WebSphere

# IBM WebSphere Partner Gateway Enterprise および Advanced Editions

バージョン 6.2

# ハブ構成ガイド

**お願い**

本書および本書で紹介する製品をご使用になる前に、 479 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM WebSphere Partner Gateway Enterprise Edition (製品番号 5724-L69) バージョン 6.2、リリース 0、モディフィケーション 0 と Advanced Edition (製品番号 5724-L68) バージョン 6.2、リリース 0、モディフィケーション 0 および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

**原典：** WebSphere® IBM WebSphere Partner Gateway Enterprise and Advanced Editions
Version 6.2
Hub Configuration Guide

**発行：** 日本アイ・ビー・エム株式会社

**担当：** トランスレーション・サービス・センター

第1刷 2010.4

# 目次

# 第 1 章 本書について

本書では、IBM (R) WebSphere (R) Partner Gateway サーバーの構成方法について説明します。

## 対象読者

WebSphere Partner Gateway を保守する管理者。本書では、次の 2 種類の管理者を想定しています。

- ハブ管理者
- アカウント管理者

ハブ管理者は、コミュニティーのスーパー・ユーザーです。ハブ管理者は、パートナーの構成と接続を含む、ハブ・コミュニティー全体の構成および管理を担当します。アカウント管理者は、ハブ管理者機能のサブセットにアクセスすることができ、内部パートナーまたは外部パートナーの主要な管理ユーザーになっています。

**注:** ハブ管理者、外部パートナー、および内部パートナーのコンソールは、それぞれのアクセス制御/権限によって異なります。

## 表記上の規則

本書は、次の規則に従って編集されています。

*表 1. 表記上の規則*

| 規則 | 説明 |
|---|---|
| モノスペース・フォント | このフォントのテキストは、ユーザーが入力したテキスト、引数またはコマンド・オプションの値、例とサンプル・コード、またはシステムが画面に出力する情報 (メッセージ・テキストまたはプロンプト) を示します。 |
| **太字** | 太字のテキストは、表と本文に記述されたグラフィカル・ユーザー・インターフェースのコントロール (例えば、オンライン・ボタン名、メニュー名、メニュー・オプションなど) および列見出しを示します。 |
| *イタリック* | イタリックのテキストは、強調部分、本のタイトル、新規用語と本文で定義されている用語、変数名、または文字として使用されているアルファベット文字を示します。 |
| *イタリック・モノスペース・フォント* | イタリック・モノスペース・フォントのテキストは、モノスペース・フォントのテキスト内の変数名を示します。 |
| *ProductDir* | *ProductDir* は、製品のインストール先のディレクトリーを表します。IBM WebSphere Partner Gateway 製品のすべてのパス名は、IBM WebSphere Partner Gateway 製品がインストールされているシステムのインストール先の相対ディレクトリーです。 |

*表 1. 表記上の規則 (続き)*

| 規則 | 説明 |
|---|---|
| *%text%* および *$text* | パーセント記号 (%) に囲まれたテキストは、Windows(R) の text システム変数またはユーザー変数の値を示します。UNIX(R) 環境での同等の表記は、*$text* であり、UNIX の *text* 環境変数の値を示します。 |
| 下線付きのカラー・テキスト | 下線付きのカラー・テキストは、相互参照を示します。テキストをクリックすると、参照先のオブジェクトに移動します。 |
| 青色アウトラインのテキスト | (PDF ファイルのみ) テキストの周りのアウトラインは、相互参照を示します。アウトライン内のテキストをクリックすると、参照先のオブジェクトに移動します。この規則は、この表内の PDF ファイルに関する「下線付きのカラー・テキスト」規則に相当します。 |
| 『 』 (かぎ括弧) | (PDF ファイルのみ) かぎ括弧で囲まれた部分は、この文書の他のセクションへの相互参照です。 |
| { } | 構文の記述行の場合、中括弧 { } で囲まれた部分は、選択対象のオプションです。1 つのオプションのみを選択する必要があります。 |
| [ ] | 構文の記述行の場合、大括弧 [ ] で囲まれた部分は、オプショナル・パラメーターです。 |
| < > | 不等号括弧で囲まれた部分は名前を構成する変数要素であり、各要素を区別する目的で使用しています。例えば、*<server_name><connector_name>*tmp.log のように表記されています。 |
| / または ¥ | ディレクトリー・パスを区切る文字として、Windows インストールでは円記号 (¥) を使用しています。UNIX インストールの場合は、円記号の代わりにスラッシュ (/) を使用します。 |

## 関連文書

本製品には完全な資料のセットが提供されており、これらの資料では、WebSphere Partner Gateway Enterprise Edition および Advanced Edition のインストール、構成、管理、および使用について包括的に説明しています。

この資料は、次のサイトからダウンロードするか、オンラインで直接閲覧できます。

http://www.ibm.com/software/integration/wspartnergateway/library/

**注:** 本書の発行後に公開されたテクニカル・サポートの技術情報や速報に、本書の対象製品に関する重要な情報が記載されている場合があります。これらは次の WebSphere Business Integration サポート Web サイトにあります。

http://www.ibm.com/software/integration/wspartnergateway/support/

関心のあるコンポーネント・エリアを選択し、「Technotes」セクションと「Flashes」セクションを参照してください。

## リリース 6.2 の新機能

WebSphere Partner Gateway V6.2 では、以下の新機能がサポートされています。

- WebSphere Partner Gateway の拡張フレームワークを使用した WebSphere Transformation Extender との統合
- ログ・ファイル収集および送信のための ISA V4 のサポート
- 証明書のアップロードおよび構成の機能拡張
- メッセージ詳細でのエラー・メッセージへのリンク
- WebSphere Partner Gateway ファースト・ステップ・ページの機能拡張
- 再配置および再デプロイメントのために WebSphere Partner Gateway 設定を更新するためのスクリプト
- WebSphere Partner Gateway コンポーネントのインストール終了時にインストール検査テスト (IVT) を実行するための機能
- 完全な WebSphere Partner Gateway 構成をエクスポートおよびインポートするための機能
- 手動でのアップグレード作業を最小化するための自動アップグレードのサポート
- スケジューラー付きのコンソール・ベースのアーカイバー
- 既存の WebSphere Application Server セルに統合するための機能
- セキュア・ファイル転送プロトコル (SFTP) のサポート
- ebXML Message Service (ebMS) 用の CPP/CPA エディター
- **機能拡張**
  - アーカイバーのパフォーマンスの向上
  - AS2 および大容量ファイルの場合の文書スループット性能の向上

6.2 の新機能について詳しくは、http://www-01.ibm.com/software/integration/wspartnergateway/about/を参照してください。

# 第 2 章 ハブ構成の概要

WebSphere Partner Gateway をインストールしたら、内部パートナーと外部パートナー間で文書を交換する前に、WebSphere Partner Gateway サーバー (ハブ) を構成する必要があります。

この章では以下のトピックを扱います。

- 『ハブ構成の概要』
- 6 ページの『ハブの設定に必要な情報』
- 12 ページの『文書処理の概要』
- 15 ページの『ハンドラーを使用した文書処理コンポーネントの構成』
- 21 ページの『ハブの構成の概要』

## ハブ構成の概要

ハブ構成の目的は、内部パートナーと外部パートナーの間で文書または文書のセットを (電子的に) 送受信できるようにすることです。ハブは、文書の受信、他の形式への変換 (必要な場合)、および文書の配信を管理します。また、文書の着信時と発信時のセキュリティーを保護するようにハブを構成することも可能です。

ハブとパートナーの間で交換される文書は、通常は標準形式で、特定のビジネス・インタラクションを表しています。例えば、パートナーは、購入注文要求を RosettaNet 3A4 PIP、cXML OrderRequest 文書、または 850 トランザクションとの EDI-X12 交換として送信します。ハブは、内部パートナーのアプリケーションが使用できる形式に文書を変換します。同様に、内部パートナーのバックエンド・アプリケーションは、購入注文応答を独自のカスタム形式で送信し、それが標準形式に変換されます。その後、変換された文書がパートナーに送信されます。

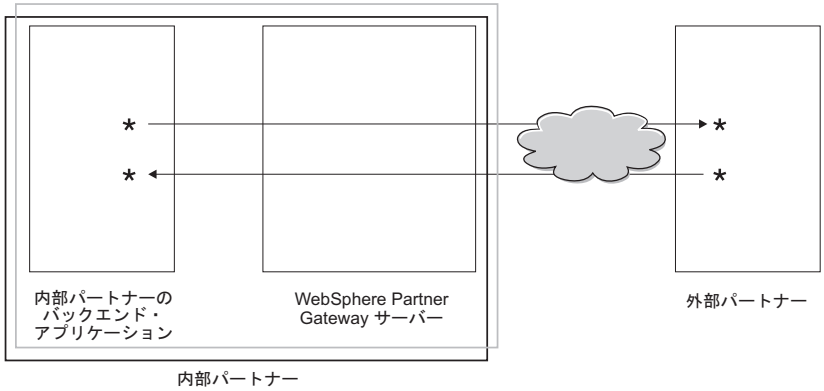



*図 1. ハブを介した文書フロー*

本書では、ハブの構成方法について説明した後、パートナーのセットアップ方法について説明します。さらに、ハブのセキュリティーを構成する方法についても説明します。

5 ページの図 1 では、WebSphere Partner Gateway サーバーおよび内部パートナーのバックエンド・アプリケーションが、すべて内部パートナーによって所有されていることに注意してください。内部パートナーは、ハブを所有する会社です。以降の章で説明するとおり、内部パートナーのプロファイルは、外部パートナーの場合と同様にして定義します。

**注:** 本書では、内部パートナーのバックエンド・アプリケーションからパートナー宛先への接続、および外部パートナーから内部パートナー宛先への接続を作成する方法について説明します。文書が内部パートナー宛先に到着すると、一般に、それらの文書を WebSphere InterChange Server または WebSphere MQ Broker などのバックエンド・アプリケーションに組み込みます。このようなバックエンド・アプリケーションと WebSphere Partner Gateway の間で組み込みを実行するために必要な作業については、「*WebSphere Partner Gateway エンタープライズ統合ガイド*」で説明されています。

## ハブの設定に必要な情報

ハブをセットアップするには、内部パートナーが参加する交換のタイプに関する情報が必要です。例えば、以下の情報が必要です。

- 内部パートナーとその外部パートナーがハブを介して送信する文書のタイプ (EDI-X12 やカスタム XML など)
- 内部パートナーとその外部パートナーが文書の送信に使用するトランスポートのタイプ (HTTP や FTP など)
- ハブに到着する文書を複数の文書に分割する必要があるかどうか、またはハブに到着する個々の文書を送信する前にグループ化する必要があるかどうか
- 文書が配信前に変換されるかどうか
- 文書が配信前に検証されるかどうか
- 文書の配信前に文書の重複がチェックされるかどうか
- 文書に暗号化やデジタル署名などのセキュリティー技法を使用するかどうか

これらの情報を決定したら、ハブの設定を始めることができます。

ハブを定義したら、外部パートナーから提供された情報 (IP アドレスや DUNS 番号) を使用して、外部パートナーを定義します。さらに、前述のとおり、内部パートナーもハブの特殊なタイプのパートナーとして定義します。

## トランスポートの概要

さまざまなトランスポートを使用して、パートナーから WebSphere Partner Gateway (ハブ) に文書を送信できます。パートナーは、
HTTP、HTTPS、JMS、FTP、FTPS、FTP スクリプト記述、SMTP、SFTP、またはファイル・ディレクトリーを使用して、文書をパブリック・ネットワークで送信できます。パートナーは、FTP スクリプト・トランスポートを使用して、文書をプライベート・ネットワークである付加価値通信網 (VAN) で送信できます。独自のトランスポートを作成することもできます。

**注:** パートナーとハブの間でファイル・ディレクトリー・トランスポートが使用されている場合、管理者はセキュリティー関連のすべての問題を処理する必要があります。

同様に、ハブは、さまざまなトランスポートを使用して、文書をバックエンド・アプリケーションに送信します。ハブとバックエンド・アプリケーションの間で最もよく使用されるトランスポートは、HTTP、HTTPS、JMS、ファイル・ディレクトリー、FTP スクリプト、FTP、SFTP、および SMTP です。

図 2 に、HTTP、HTTPS、JMS、およびファイル・ディレクトリーの各トランスポートを示します。

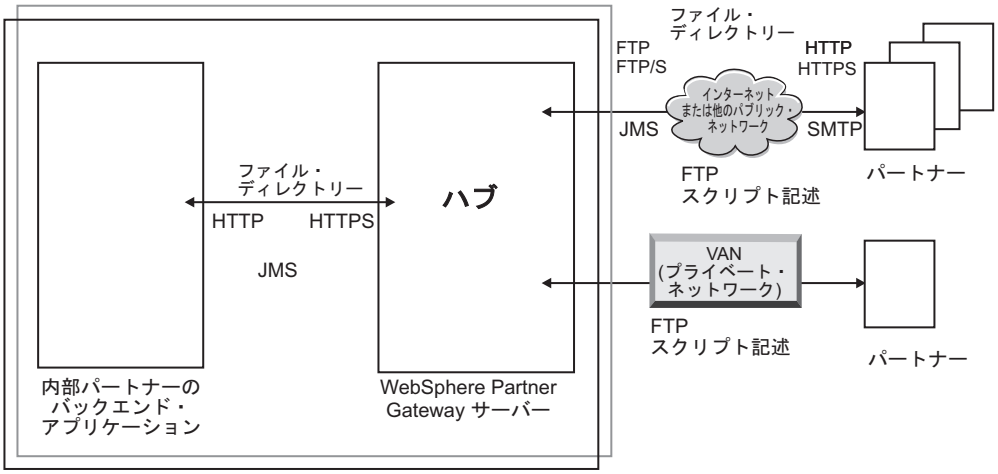



*図 2. WebSphere Partner Gateway がサポートする最も一般的なトランスポート*

文書の送受信に使用するトランスポートのタイプによって、受信側および宛先のセットアップの方法が異なります。*受信側* は、ハブの入り口点 (パートナーまたはバックエンド・アプリケーションによって送信される文書がハブで受信される場所) です。*宛先* は、パートナーのコンピューターまたはバックエンド・システムの入り口点 (ハブが文書を送信する場所) です。FTP、FTPS、FTP スクリプト、JMS、およびファイル・ディレクトリーのトランスポートを使用できるように準備するには、セットアップ作業を行う必要があります。35 ページの『第 4 章 ハブを構成するための準備』を参照してください。

## 文書定義の概要

外部パートナーと内部パートナーの間で文書を交換するための設定を行う場合、文書について以下の事項を指定します。

- 文書の*パッケージ化*
- いくつかの共通の特性を共有する文書のクラスを定義するビジネス・*プロトコル*
- ビジネス・プロトコルによって提供される文書の 1 つを示す*文書タイプ*

*文書定義* は、文書のパッケージ化、文書のプロトコル、および文書タイプで構成されます。製品が提供する以下の文書定義を使用するものとします。

- パッケージ化: AS
- プロトコル: EDI-X12

- 文書タイプ: ISA

このルーティング定義に準拠する文書を受け取ったときに行われる処理を以下に説明します。ハブが文書を受け取ると、固定インバウンド・ワークフローのアンパック・ステップで、文書が AS パッケージ化を使用していることが判別されます。これは、AS パッケージ化用に指定されたトランスポート・ヘッダーが存在するためです。その他のパッケージ化タイプは、同じようにして (通常文書に付属するトランスポート・ヘッダーを調べて) ハブによって検出されます。どのパッケージ化タイプとも一致しない場合は、「なし」パッケージ化タイプが文書に割り当てられます。AS パッケージ化の場合、メッセージ・トランスポート・ヘッダーから送信側ビジネス ID および受信側ビジネス ID が取得されます。AS トランスポート・ヘッダーには、メッセージの暗号化の有無、圧縮の有無、または署名の有無を指定できるその他のヘッダーも含まれます。

パッケージ化を識別したら、ハブの固定インバウンド・ワークフローのプロトコル解析ステップで、文書のプロトコルと文書タイプが判別されます。これは、実際のメッセージ内容を調べ、プロトコルと文書タイプを示す特性を文書内で探すことによって実行されます。プロトコル解析ワークフロー・ステップでは、使用されるプロトコルに応じて、文書からその他の情報も取り出します。

文書が特定のパッケージ、プロトコル、および文書タイプを使用していることが分かると、ハブは文書の処理を続行することができます。この時点で、パッケージ、プロトコル、および文書タイプに加えて、送信側ビジネス ID および受信側ビジネス ID も分かります。ハブはこの情報により、送信側パートナーおよび受信側パートナー間の、インバウンド・パッケージ、プロトコル、および文書タイプを持つ接続を検索できます。

接続が検出されると、以下の追加情報を検出できるため、ハブは文書のルーティング方法と処理方法を認識します。

- 送信側パートナーおよび受信側パートナーの証明書 (必要な場合)
- 送信側ルーティングおよび受信側ルーティングの属性設定
- 文書のルーティング時に実行するアクション
- 適用可能な変換マップ (存在する場合)
- 適用可能な検証マップ (存在する場合)

## パッケージ化

パッケージ化によって、文書の伝送に関する情報が提供されます。前述のとおり、パッケージ化が AS の場合、ハブは AS ヘッダーの情報を使用して文書のソースおよび宛先を判別します。パートナーが RosettaNet PIP を内部パートナーに送信する場合、PIP は RNIF としてパッケージ化されます。

9 ページの図 3 は、ハブと外部パートナーの間、およびハブとバックエンド・アプリケーションの間で交換される文書に設定可能なパッケージ化タイプを示しています。

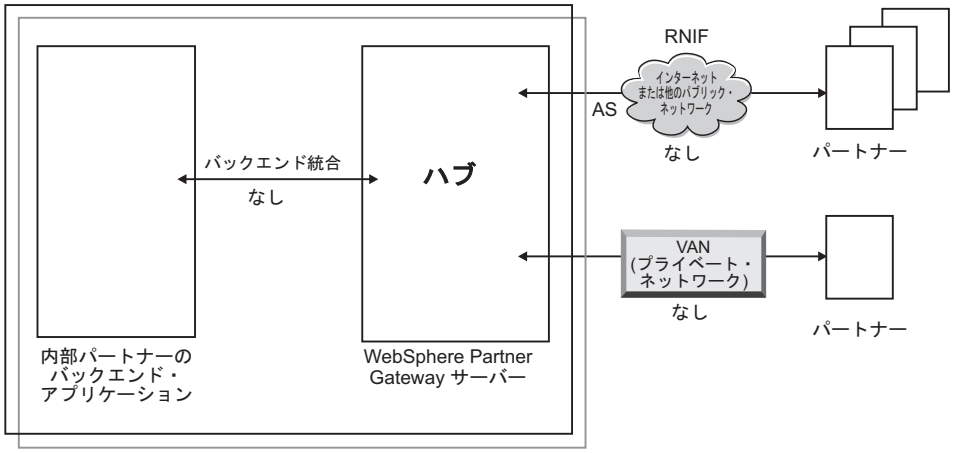



*図 3. 文書パッケージ化タイプ*

パッケージは、特定のプロトコルに関連付けられています。例えば、パートナーは、RosettaNet 文書をハブに送信する場合に RNIF パッケージ化を指定する必要があります。

**バックエンド統合:** 図 3 に示されているとおり、バックエンド統合はハブとバックエンド・アプリケーションの間でのみ使用可能です。バックエンド統合パッケージ化を指定すると、ハブによってバックエンド・システムに送信される文書に特殊なヘッダー情報が追加されます。同様に、バックエンド・アプリケーションが、バックエンド統合のパッケージ化で文書をハブに送信する場合、ヘッダー情報を追加する必要があります。バックエンド統合パッケージ、およびヘッダー情報の要件については、「*WebSphere Partner Gateway エンタープライズ統合ガイド*」で説明されています。

**AS:** AS パッケージは、パートナーとハブの間で最も多く使用されます。AS パッケージは、AS1、AS2、および AS3 規格に準拠する文書に使用できます。 AS1 は SMTP を介して文書を安全に送信するために使用される規格であり、AS2 は HTTP または HTTPS を介して文書を安全に送信するために使用される規格です。AS3 は、FTP または FTPS を介して文書を安全に送信するために使用される新しい規格です。AS のパッケージ化を使用してパートナーが送信する文書には、AS1、AS2、または AS3 ヘッダー情報が含まれます。AS1、AS2、または AS3 ヘッダーを期待するパートナーに送信される文書は、(ハブで) AS としてパッケージ化する必要があります。

**なし:** なしパッケージは、ハブとパートナーの間、およびハブとバックエンド・アプリケーションの間で文書を送受信するために使用できます。文書がなしとしてパッケージ化される場合、ヘッダー情報は追加されません (期待されません)。

**RNIF:** RNIF パッケージは、インストール・メディア上で提供されます。RNIF パッケージを (交換する PIP とともに) アップロードします。方法については、 115 ページの『RosettaNet 文書』で説明しています。RNIF パッケージは、RosettaNet 文書をパートナーとハブの間で送信する場合に使用されます。

**ebMS:** ebXML Message Service (ebMS) メカニズムは、ebXML 取引先間でビジネス・メッセージを交換する標準的な方法を提供します。専有のテクノロジーおよびソリューションに頼ることなくビジネス・メッセージを交換するための、信頼性の

高い手段を提供します。ebXML メッセージには、メッセージ・ヘッダーの構造 (ルーティングおよび配信に必要) およびペイロード・セクションが含まれています。

ebMS は、ebXML 取引先間でビジネス・メッセージを交換する標準的な方法を提供します。ebXML メッセージは、通信プロトコルに依存しない MIME/Multipart メッセージ・エンベロープです。

**N/A:** WebSphere Partner Gateway 内で終了するか、または WebSphere Partner Gateway 内部から発生する文書タイプがあります。WebSphere Partner Gateway 内で終了する文書タイプの場合、パッケージ化は必要ありません。WebSphere Partner Gateway 内部から発生する文書タイプでは、ソースのパッケージ化はありません。したがって、そのようなフローでは、パッケージ化は N/A として指定されます。

外部パートナーから内部パートナー (または、逆方向) の片方向伝送では、ほとんどの場合、WebSphere Partner Gateway が外部パートナーから文書を受信し、それを内部パートナーに送信します。WebSphere Partner Gateway では、パートナー接続の作成時に、WebSphere Partner Gateway が文書を受信するパッケージ化と WebSphere Partner Gateway が文書を送信する際に使用するパッケージ化を指定します。図 4 では、AS としてパッケージ化された文書が、外部パートナーから内部パートナー・バックエンドへ流れています。文書はトランスポート・ヘッダーなしで内部パートナー宛先に配信されます。図 4 では、1 つのアクティビティーが文書の交換と関連付けられています。

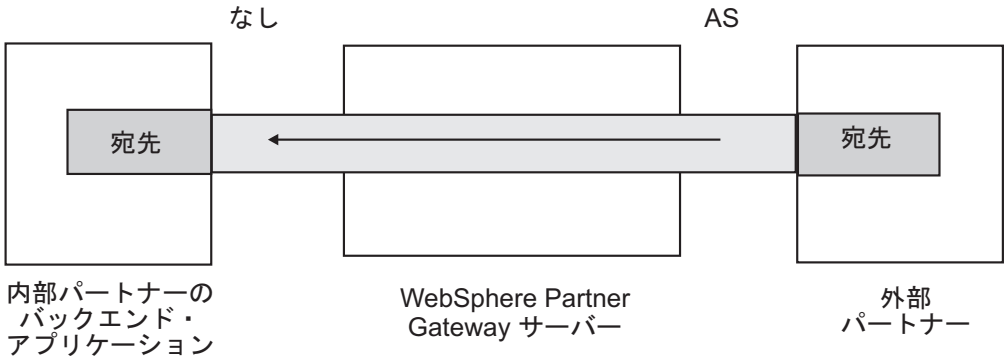



*図 4. 標準的な片方向接続*

ただし、プロトコルによっては複数のアクティビティー (エンベロープ解除、変換など) が含まれ、その中には交換全体の中間部分として発生するものもあります。例えば、パートナーが EDI 交換をハブに送信する場合 (最終的な配信先は内部パートナー) 、交換はエンベロープ解除され、個々の EDI トランザクションが処理されます。元の EDI 交換には、パートナーから送信されるときにパッケージが関連付けられています。ただし、交換自体は内部パートナーに配信されないため (ハブ内でエンベロープ解除され、交換に対する追加処理は発生しません)、交換のパッケージ化は適用されません。したがって、エンベロープ解除のステップの対話をセットアップする場合、送信側でパッケージを入力しますが、受信側には「N/A」を指定します。

EDI 交換で必要な文書定義をセットアップするプロセスについては、175 ページの『第 10 章 EDI 文書フローの構成』で説明されています。

## プロトコル

システムに準備されているプロトコルは、以下のとおりです。

- バイナリー

  バイナリー・プロトコルは、AS、なし、およびバックエンド統合パッケージで使用できます。バイナリー文書には、文書のソースまたは宛先についてのデータは含まれていません。

- EDI-X12、EDI-Consent、EDI-FACT

  これらの EDI プロトコルは、AS またはなしパッケージで使用できます。 10 ページの『 N/A』で説明されているように、EDI トランザクションまたは交換がハブから発生する場合、またはハブで終了する場合、パッケージに「N/A」を指定します。X12 および EDIFACT は、データ交換に使用される EDI 標準です。EDI-Consent とは、EDI-Consent 仕様に指定されているコンテンツ・タイプを指します。

- Web サービス

  Web サービス・プロトコルは、なしパッケージでのみ使用できます。

- cXML

  cXML プロトコルは、なしパッケージでのみ使用できます。

- XMLEvent

  XMLEvent は、バックエンド・アプリケーションへ流れる文書、またはバックエンド・アプリケーションから流れる文書にイベント通知を提供するために使用される特殊なプロトコルです。これは、バックエンド統合パッケージでのみ使用できます。このプロトコルについては、「*WebSphere Partner Gateway エンタープライズ統合ガイド*」で説明されています。

RNIF パッケージをアップロードすると、関連したプロトコル (RosettaNet および RNSC) も取得できます。RosettaNet (パートナーとハブの間で使用されるプロトコル) は、RNIF パッケージに関連付けられています。RNSC (ハブと内部パートナーのバックエンド・アプリケーションの間で使用されるプロトコル) は、バックエンド統合パッケージに関連付けられています。

EDI トランザクション、XML 文書、または ROD 文書を変換する場合は、Data Interchange Services クライアント (DIS) または WTX design studio が変換マップの作成に使用されます。

Data Interchange Services クライアントでは、この変換に関連したプロトコルに対してディクショナリーが定義されています。ディクショナリーには、EDI 文書定義、セグメント、複合データ・エレメント、データ・エレメントなど、EDI 規格を構成するすべてに関する情報が含まれています。EDI 用のソース文書の定義は WDI によって提供されますが、ROD および XML の場合は DIS クライアントで作成する必要があります。バージョン 6.2 以降では、標準および変換マップを別個にコンパイルできます。特定の EDI 規格の詳細については、該当する EDI 規格マニュアルを参照してください。Data Interchange Services クライアントについては、「*WebSphere Partner Gateway Mapping Guide*」または Data Interchange Services クライアントに付属のオンライン・ヘルプを参照してください。

**注:** 送信側 ID および受信側 ID は、変換マップに関連付けられている ROD 文書定義に含まれている必要があります。また、文書タイプおよびディクショナリー値を判別するために必要な情報も、文書定義に含まれている必要があります。変換マップを作成する場合、Data Interchange Services クライアントのマッピング担当者が、これらの要件を把握していることを確認してください。

カスタム・プロトコルを作成して、文書をどのように構造化するかを正確に定義することができます。XML 文書の場合は、 162 ページの『カスタム XML 文書処理』の説明に従って XML 形式を定義します。

### 文書タイプ

文書には、さまざまな形式があります。製品が提供する文書タイプおよびそれらの関連プロトコルは、以下のとおりです。

- バイナリー。バイナリー・プロトコルで使用できます。
- ISA。X12 交換 (エンベロープ) を表し、EDI-X12 プロトコルに関連します。
- BG。EDI Consent エンベロープを表し、EDI-Consent プロトコルに関連します。
- UNB。EDIFACT エンベロープを表し、EDI-EDIFACT プロトコルに関連します。
- XMLEvent。XMLEvent プロトコルで使用できます。

以下のリストは、他のタイプの文書および定義のソースを示しています。

- RosettaNet PIP (インストール・メディアからアップロード)。RosettaNet プロトコルで使用できます。
- Web サービス (WSDL ファイルとしてアップロード)。Web サービス・プロトコルで使用できます。
- cXML 文書 (cXML 文書のタイプを指定して作成)。
- 特定の EDI 標準トランザクション。Data Interchange Services クライアントからインポートします。
- レコード指向データ (ROD) または XML 文書。Data Interchange Services クライアントからインポートします。

162 ページの『カスタム XML 文書処理』に説明されているように、独自の文書タイプを作成することもできます。

## 文書処理の概要

ハブの設定を始める前に、WebSphere Partner Gateway のコンポーネントと、文書処理に各コンポーネントがどのように使われるのかを確認しておきましょう。

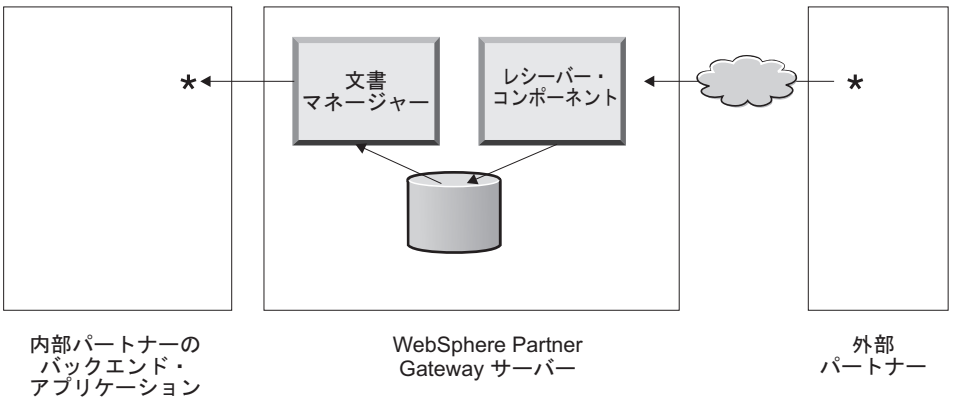



*図 5. レシーバー・コンポーネントと文書マネージャー・コンポーネント*

図 5 は、文書がパートナーから送信され、ハブで受信されて処理された後、内部パートナーのバックエンド・アプリケーションに送信される仕組みの例を示しています。

**注:** 説明の便宜上、この文書の図では、1 つのレシーバー・コンポーネントと 1 つの文書マネージャーが同じサーバー・マシンにインストールされています。 (3 番目のコンポーネントであるコンソールは表示されていません。コンソールは、WebSphere Partner Gateway へのインターフェースです。) 実際には、これらのコンポーネントが複数回出現したり、別々のサーバーにインストールされている場合があります。すべてのコンポーネントが同一の共通ファイル・システムを使用する必要があります。WebSphere Partner Gateway のセットアップに使用できる他のトポロジーについては、「*WebSphere Partner Gateway インストール・ガイド*」を参照してください。

WebSphere Partner Gateway は、レシーバー・コンポーネントによって文書を受信します。レシーバー・コンポーネントは、インバウンド文書のトランスポートをモニターし、到着した文書を取り出し、文書に対するいくつかの基本的な処理を実行してから、文書マネージャーが文書を取り出すことができるキューに文書を入れます。

レシーバー・インスタンスは、トランスポート固有です。レシーバーは、ハブがサポートするトランスポートのタイプごとに設定します。例えば、パートナーが HTTP で文書を送信する場合、それらの文書を受信するには HTTP レシーバーを設定する必要があります。

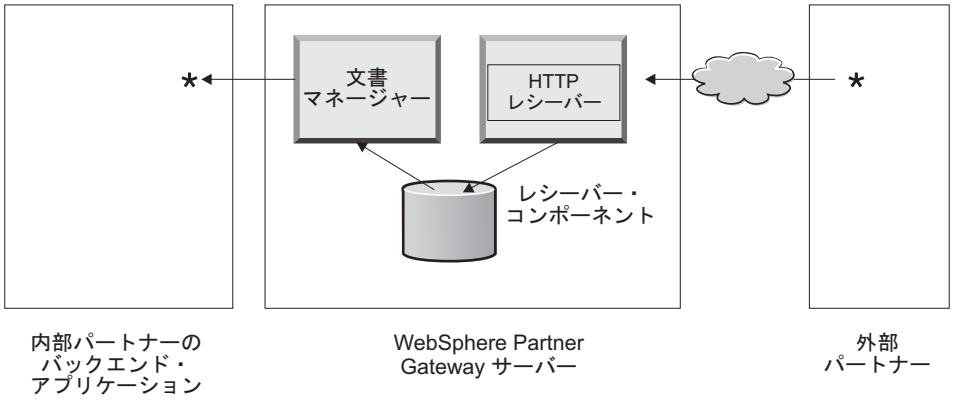



*図 6. HTTP レシーバー*

内部パートナーのバックエンド・アプリケーションが JMS で文書を送信する場合、それらの文書を受信するためにハブで JMS レシーバーを設定します。

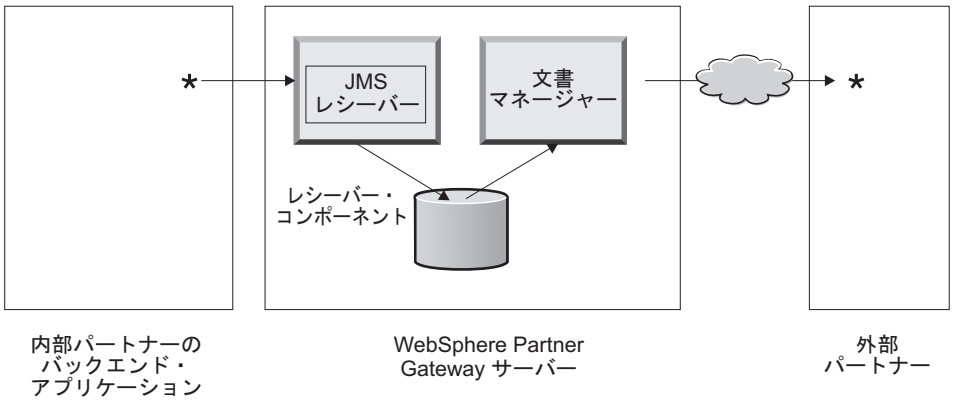



*図 7. JMS レシーバー*

6 ページの『トランスポートの概要』で説明されているとおり、WebSphere Partner Gateway ではさまざまなトランスポートをサポートしていますが、レシーバーを定義する独自のユーザー定義トランスポートをアップロードすることもできます (77 ページの『 ユーザー定義トランスポートのレシーバーの設定』を参照してください)。

レシーバー・コンポーネントは、文書をファイル共用システムに送信します。複数の文書が単一ファイルに含まれている場合 (例えば、XML または ROD 文書、あるいは EDI 交換が一緒に送信される場合)、レシーバーは文書または交換を分割してから、それらをファイル共用システムに送信します。文書マネージャー・コンポーネントは、このファイル・システムから文書を取り出し、ルーティング情報や、変換が必要かどうかを判断します。

例えば、パートナーは AS2 パッケージ化の EDI-X12 文書を期待していたにもかかわらず、内部パートナーがそのパートナーへの配信用にハブに送信した EDI-X12 文書が、パッケージ化されていない可能性があります。パートナーは AS2 パッケージ化文書を配信する HTTP URL を指定し、文書マネージャーはパートナーの期待通りに文書をパッケージ化します。文書マネージャーはそのパートナーの宛先の構成

(これは、パートナーが AS2 文書の受信を期待する HTTP URL に対してセットアップされている必要があります) を使用して文書をパートナーに送信します。

## ハンドラーを使用した文書処理コンポーネントの構成

ここでは、WebSphere Partner Gateway の各コンポーネントについて詳しく説明するとともに、製品で指定された各コンポーネントのビジネス文書処理の動作を変更可能な (または変更する必要がある) さまざまなポイントを示します。

製品で指定されたレシーバー、宛先、固定ワークフロー・ステップ、およびアクションの動作を変更するには、ハンドラー を使用します。ハンドラーには、WebSphere Partner Gateway で提供されるものとユーザー定義のものの 2 タイプがあります。ハンドラーの作成については、「*WebSphere Partner Gateway Programmer Guide*」を参照してください。

ハンドラーを作成したら、それをアップロードして使用可能にします。ユーザー定義のハンドラーのみをアップロードします。WebSphere Partner Gateway で提供されているハンドラーは、既に使用可能です。

以下のセクションでは、ハンドラーを指定できる処理ポイントについて説明します。

### レシーバー

レシーバーには、ハンドラーを指定できる 3 つの*構成ポイント* (前処理、同期検査、および後処理) があります。

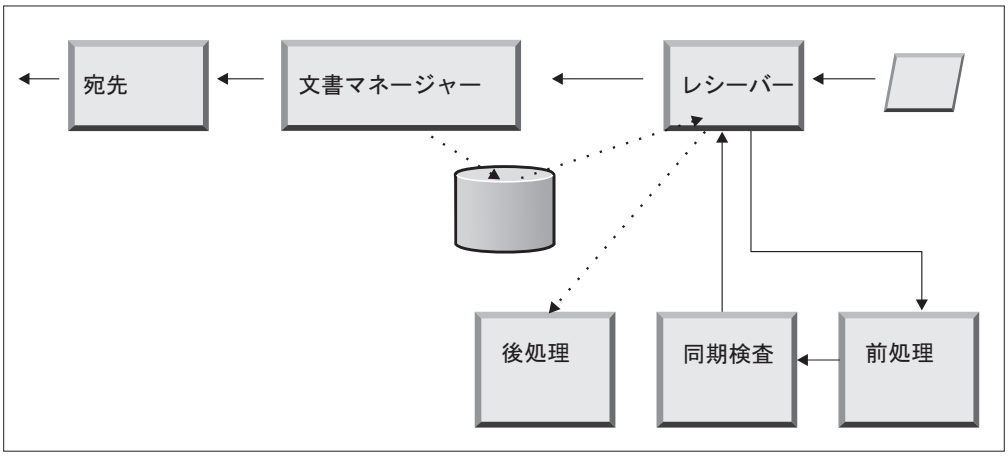



*図 8. レシーバーの構成ポイント*

処理は、以下の順序で発生します。

1. レシーバー・コンポーネントが、文書の受信後に、前処理ステップおよび同期検査ステップを呼び出します。
2. 次に、レシーバーが、文書を処理するために文書マネージャーを呼び出します。
3. 同期フローの場合、文書マネージャーが同期応答を提供します。次に、レシーバー・コンポーネントが、文書マネージャーから戻された応答で後処理ステップを呼び出します。

これらのステップについて、以下のセクションで説明します。

- 前処理

  前処理ステップは、通常、文書マネージャーが文書を処理する前に完了する必要のある文書処理に使用されます。 例えば、複数の ROD 文書を単一ファイルで受信する場合は、レシーバーを定義するときに ROD スプリッター・ハンドラーを構成します。レシーバーをセットアップする場合、ROD スプリッターと、製品が提供する他の 2 つのスプリッターを使用できます。前処理ステップ用の追加のハンドラーを作成する場合、それらのハンドラーも使用できます。

  前処理構成ポイントの構成については、 78 ページの『 前処理』を参照してください。

- 同期検査

  同期検査は、WebSphere Partner Gateway が文書を同期または非同期のどちらで処理するかを決めるために使用されます。例えば、HTTP を介して受信された AS2 文書の場合、MDN (メッセージ処理通知) が同じ HTTP 接続を介して同期的に戻されるかどうかを決定します。WebSphere Partner Gateway には、同期検査用のさまざまなハンドラーがあります。レシーバーに関連付けられているトランスポートによって、ハンドラーのリストは異なります。

  同期検査は、同期伝送をサポートするトランスポート (HTTP、HTTPS、JMS など) にのみ適用されます。

  **注:** 同期交換で使用される AS2、cXML、RNIF、または SOAP 文書の場合、関連した同期検査ハンドラーを HTTP または HTTPS レシーバーで指定する必要があります。

  同期検査構成ポイントの構成については、 82 ページの『 同期検査』を参照してください。

- 後処理

  後処理は、同期トランザクションの結果としてハブが送信する応答文書の処理に使用されます。

  後処理構成ポイントの構成については、 83 ページの『 後処理』を参照してください。

## 文書マネージャー

レシーバーが受信した文書は、文書マネージャーが、さらに処理するために共通ファイル・システムから取り出します。文書マネージャーは、パートナー接続を使用して文書をルーティングします。文書マネージャーを介したすべての文書フローが、固定インバウンド・ワークフロー、可変ワークフロー、および固定アウトバウンド・ワークフローなど、一連のワークフローを通過します。インバウンド・ワークフローの終わりに、パートナー接続が決定されます。パートナー接続は、この文書に対して実行するアクションを指定します。可変ワークフローの実行後、文書マネージャーはこの文書に対して固定アウトバウンド・ワークフローを処理します。

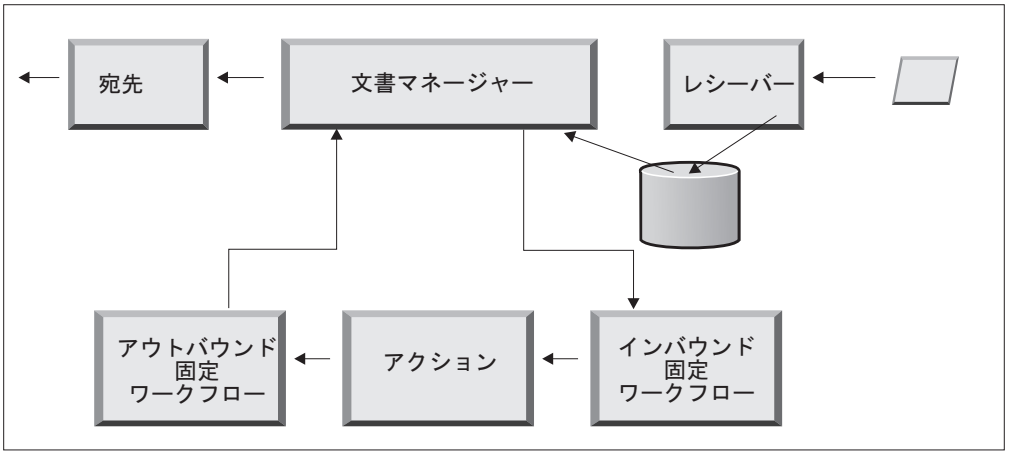



*図 9. 固定ワークフローとアクション*

図 9 は、RosettaNet PIP または Web サービスなどの文書が通るパスを示しています。ただし、一部の文書では、複数の構成フローが必要です。例えば、EDI 交換は、複数のトランザクションで構成される場合があります。最初のフローでは、個々のトランザクションのセットをエンベロープ解除するためのアクションが使用されます。これらの各トランザクションは、独自の構成フローに再導入され処理されます。

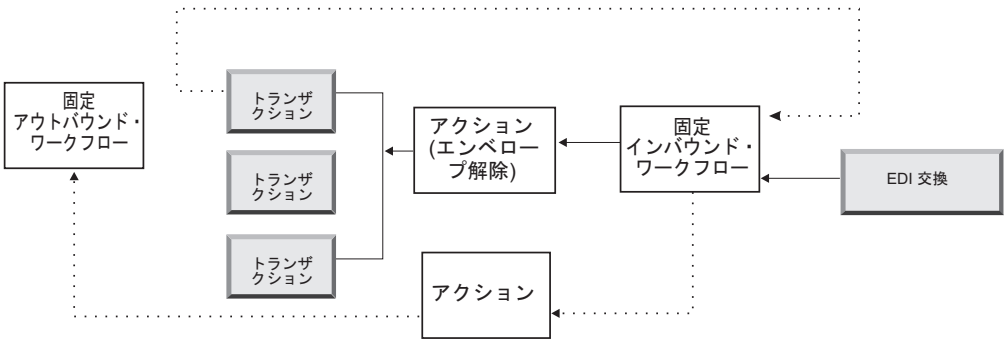



*図 10. EDI 交換用の固定ワークフローとアクション*

## インバウンド固定ワークフロー

インバウンド固定ワークフローは、レシーバーから文書マネージャーに着信するすべての文書に対して実行される処理ステップの標準セットで構成されます。ステップの数とタイプが常に同じであるため、ワークフローは固定です。ただし、ユーザー出口を介して、プロトコル・アンパック・ステップおよびプロトコル処理ステップを処理するためのカスタマイズされたハンドラーを提供できます。インバウンド固定ワークフローの最後のステップでは、パートナー接続検索が実行され、このビジネス文書に対して実行される可変ワークフローが決定されます。

例えば、AS2 メッセージが受信された場合は、このメッセージが暗号化解除され、送信側と受信側のビジネス ID が取り出されます。インバウンド固定ワークフロー・ステップでは、WebSphere Partner Gateway でさらに処理するために AS2 文書をプレーン・テキストに変換し、メッセージに対するアクションを決定するための

情報を抽出します。

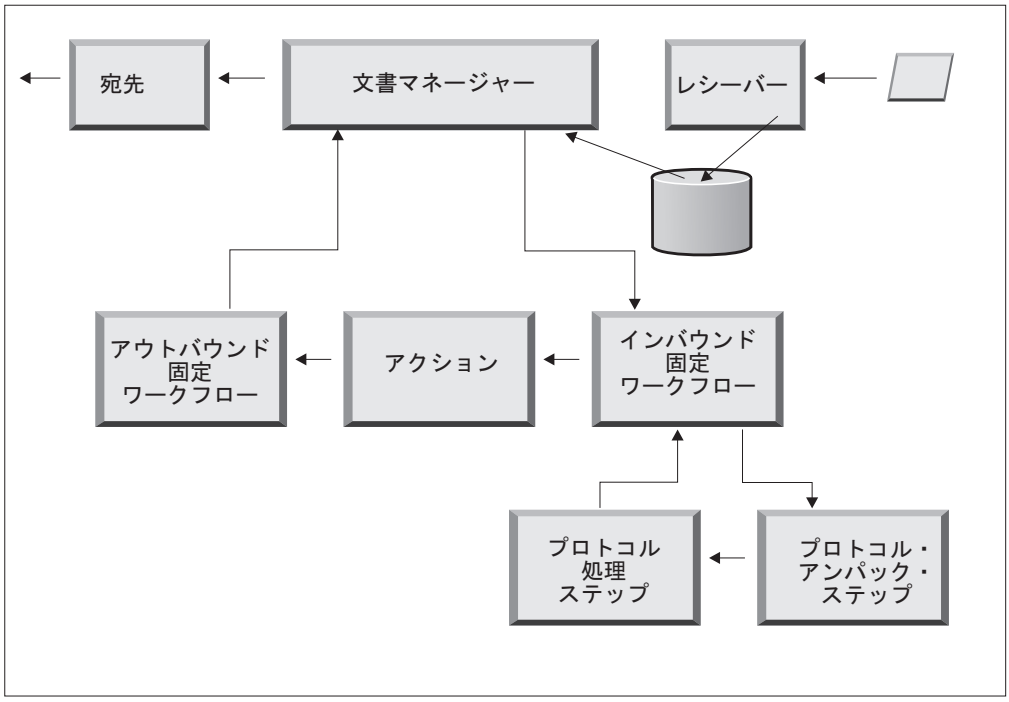



*図 11. インバウンド固定ワークフロー・ステップ*

**プロトコル・アンパック:** プロトコル・アンパックでは、文書をさらに処理できるようにするために文書がアンパックされます。このプロセスには、暗号化解除、圧縮解除、署名検証、ルーティング情報の抽出、ユーザー認証、またはビジネス文書パートの抽出などが含まれます。

WebSphere Partner Gateway には、RNIF、AS、バックエンド統合、およびなしパッケージ化用のハンドラーがあります。他のパッケージ化プロトコル用のハンドラーが必要な場合は、ユーザー出口として開発することができます。ユーザー出口の作成については、「*WebSphere Partner Gateway Programmer Guide*」を参照してください。

プロトコル・アンパック・ステップは変更できませんが、ハンドラーを追加して、ビジネス・ロジックをステップに追加することはできます。

このステップの構成については、86 ページの『固定ワークフローの構成』を参照してください。

**プロトコル処理ステップ:** プロトコル処理では、プロトコル固有の情報が判別されます。これには、ルーティング情報 (送信側 ID、受信側 ID など)、プロトコル情報、および文書タイプ情報を判別するためのメッセージの構文解析が含まれる場合があります。WebSphere Partner Gateway には、さまざまなプロトコル用の処理があります (87 ページの『 プロトコル処理ハンドラー』のリストを参照)。CSV (comma-separated value) などの他のプロトコルの処理は、ユーザー出口を使用して提供できます。

プロトコル処理ステップは変更できませんが、ハンドラーを追加して、ビジネス・ロジックをステップに追加することはできます。

このステップの構成については、 86 ページの『固定ワークフローの構成』を参照してください。

文書のプロトコルに適用されるデフォルトのハンドラーを使用することもでき、プロトコル・アンパックおよびプロトコル処理の固定ワークフロー・ステップに対して異なるハンドラーを指定することもできます。

## アクション

処理シーケンスにおける次のステップは、文書交換に関して設定されたアクションに基づいて行われます。アクションは、文書に対して実行できる多数のステップで構成されます。アクションの例としては、文書の検証 (文書が特定の規則セットに従っているかどうか) や、受信側が必要とする形式に文書を変換する処理などがあります。

文書で特定のステップを必要としない場合は、製品が提供するパススルー・アクションを使用できます。このアクションは文書に何の変更も加えません。

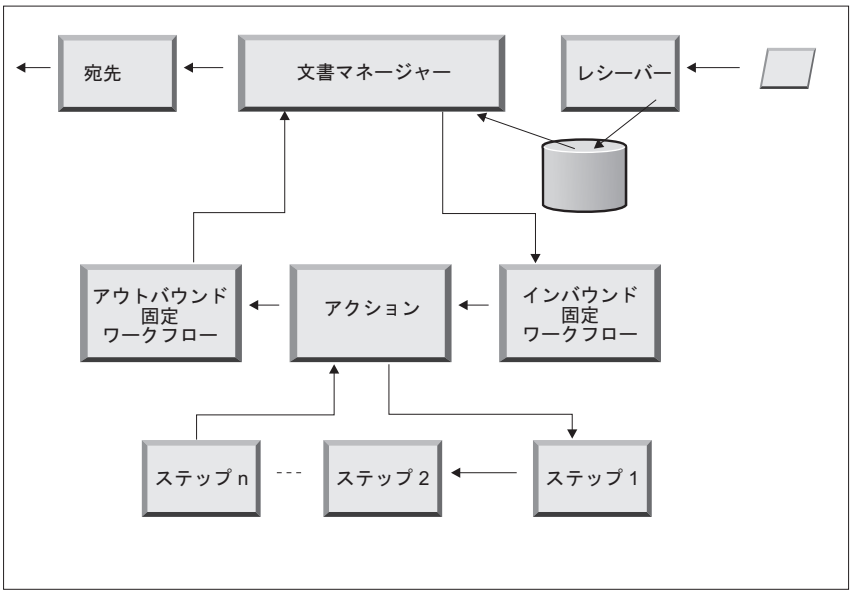



*図 12. アクションのステップ*

製品が提供するアクションは変更できません。ただし、アクションを作成して構成済みリストにハンドラーを追加したり、製品で提供するアクションをコピーしてからハンドラーのリストを変更したりすることができます。

製品で提供するアクションの作成またはコピー、またはユーザー定義アクションの構成については、 88 ページの『アクションの構成』を参照してください。

## アウトバウンド固定ワークフロー

アウトバウンド固定ワークフローは、プロトコル情報を使って文書をパッケージ化するステップだけで構成されます。例えば、バックエンド統合パッケージ化を使用してバックエンド・アプリケーションが文書を受信するように設定されている場合

は、文書が宛先に渡される前に、何らかのヘッダー情報が文書に追加されます。

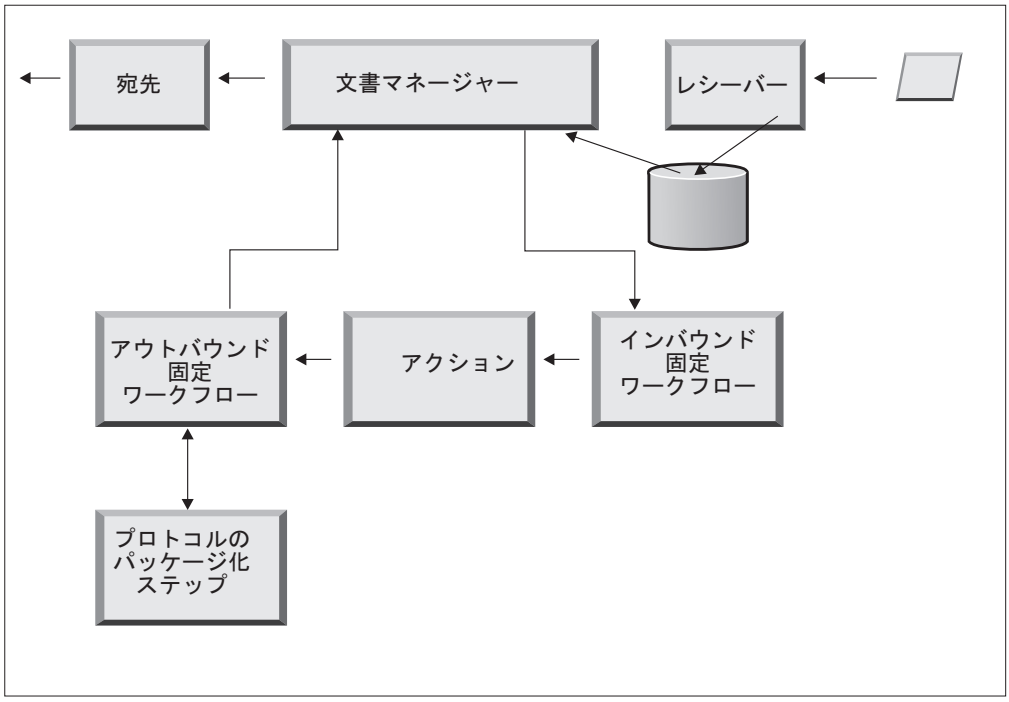



*図 13. アウトバウンド固定ワークフロー・ステップ*

WebSphere Partner Gateway には、さまざまなパッケージおよびプロトコル用のハンドラーがあります (88 ページの『アウトバウンド・ワークフロー』のリストを参照)。他のパッケージ化ハンドラーが必要な場合は、ユーザー出口として開発できます。通常、これらのステップでは、以下の 1 つ以上の処理が行われます。

- アセンブルまたはエンベロープ
- 暗号化
- 署名
- 圧縮
- ビジネス・プロトコル固有のトランスポート・ヘッダーの設定

プロトコル・パッケージ化ステップは変更できませんが、ハンドラーを追加して、ビジネス・ロジックをステップに追加することはできます。

このワークフロー・ステップの構成については、 86 ページの『固定ワークフローの構成』を参照してください。

## 宛先

宛先は、メッセージを送信する必要のあるパートナーごとに、コンソールで構成されます。宛先の構成には、メッセージの送信に使用されるトランスポートと、パートナーの受信プロセスの URL などの、送信に必要な構成が含まれます。

文書は文書マネージャーを出ると、宛先を使用して目的の受信側に送信されます。宛先には、前処理と後処理の 2 つの構成ポイントがあります。

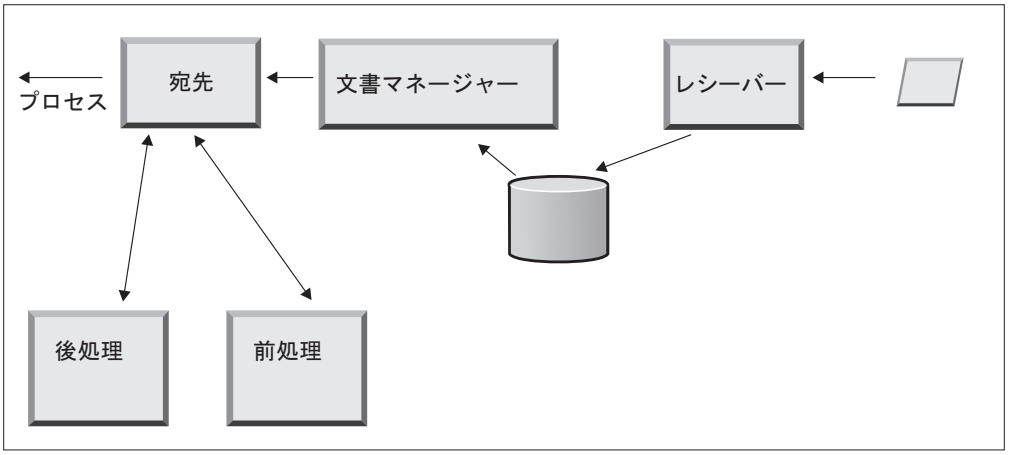



*図 14. 宛先の構成ポイント*

- 前処理

  前処理は、受信側に送信される前の文書の処理に影響を与えます。(プロセスでは、実際に文書を送信します。) システムには前処理ステップを構成するためのハンドラーはありませんが、ユーザー定義のハンドラーをアップロードできます。
- 後処理

  後処理は、文書送信の結果に対して (例えば、同期伝送時に受信側から受信する応答に対して) 作用します。システムには後処理ステップを構成するためのハンドラーはありませんが、ユーザー定義のハンドラーをアップロードできます。

前処理ステップおよび後処理ステップの構成については、250 ページの『ハンドラーの構成』を参照してください。

## ハブの構成の概要

ビジネス・ニーズを分析したら (6 ページの『ハブの設定に必要な情報』を参照)、ハブをセットアップし、パートナー・プロファイルを作成します。ここでは、関係する作業の概要を示します。

**注:** ハブを構成している場合、イベント・コードとトラブルシューティングのヒントについては、「*WebSphere Partner Gateway 管理ガイド*」を参照してください。

### ハブの設定

#### このタスクについて

ハブ管理者は、以下の作業を実行してハブを設定します。

1. 使用するトランスポートの事前セットアップを実行します (必要な場合)。事前セットアップについては、35 ページの『第 4 章 ハブを構成するための準備』で説明します。
2. オプションで、コンソールをカスタマイズし、デフォルトのパスワードおよびアクセス権ポリシーを変更します。この作業については、53 ページの『第 6 章 コミュニティー・コンソールの構成』で説明します。

3. ハブで文書を (内部パートナーおよび外部パートナーから) 受信するために使用するトランスポートのタイプのレシーバーを作成します。レシーバーの作成については、 59 ページの『第 7 章 レシーバーの定義』で説明します。

   **注:** ユーザー定義のハンドラーを使用してレシーバーを構成する場合は、レシーバーを作成する前にハンドラーをアップロードする必要があります。ハンドラーのアップロードについては、 60 ページの『ユーザー定義ハンドラーのアップロード』で説明します。
4. インバウンド・ワークフローのステップまたはアクションを構成します。これはオプションの ステップで、WebSphere Partner Gateway で提供されていない文書処理が特に必要な場合にのみ必要です。製品で提供するワークフローまたはアクションの動作を変更する必要がなければ、このステップは省略してください。ワークフロー・ステップおよびアクションの構成については、 85 ページの『第 8 章 固定ワークフロー・ステップおよびアクションの構成』で説明します。

   **注:** ユーザー定義のハンドラーは、ワークフローまたはアクションを構成する前にアップロードする必要があります。ユーザー定義のハンドラーのアップロードについては、 85 ページの『ハンドラーのアップロード』で説明します。
5. ハブで送受信できる文書のタイプを定義するために文書定義を作成します (または、必要な定義が既に使用可能になっていることを確認します)。
6. 2 つの文書定義の有効な組み合わせを示すためにインタラクションを作成します。

   文書定義の作成およびインタラクションの作成については、 109 ページの『第 9 章 文書タイプの構成』および 175 ページの『第 10 章 EDI 文書フローの構成』で説明しています。
7. 内部パートナー用のプロファイルを作成します。その際、内部パートナーについての情報を提供し、内部パートナーが送受信できる文書のタイプ (内部パートナーの B2B 機能) を設定します。プロファイルの作成については、 25 ページの『第 3 章 パートナーの作成とセットアップ』で説明します。

## パートナーの作成

ハブをセットアップしたら、内部パートナーと文書を交換する外部パートナーごとにプロファイルを作成します。パートナーを作成できるのは、ハブ管理者のみです。

ハブ管理者は、パートナーの B2B 機能のセットアップ、パートナーの宛先の設定、およびパートナーのセキュリティー・プロファイルの設定も行うことができます。これらのステップは、パートナーが自分で行うことも可能です。

パートナーの作成については、 25 ページの『第 3 章 パートナーの作成とセットアップ』で説明します。宛先の作成については、 227 ページの『第 11 章 宛先の作成』で説明します。セキュリティー・プロファイルのセットアップについては、 257 ページの『第 13 章 文書交換のセキュリティーの使用可能化』で説明します。

## 文書接続の設定

ハブを構成して、パートナー・プロファイルを作成したら、接続をセットアップできます。接続は、送信側と受信側の有効な組み合わせ、および交換できる文書を示します。接続の管理については、 253 ページの『第 12 章 接続の管理』で説明します。

# 第 3 章 パートナーの作成とセットアップ

パートナーには内部パートナーと外部パートナーの 2 種類があります。通常は、WebSphere Partner Gateway サーバーを所有し、そのサーバーを使用して他社と通信している会社が内部パートナーになります。内部パートナーはバックエンド・アプリケーション (所有する会社の内部アプリケーション) を所有しています。内部パートナーの数に制限はありませんが、通常は最初に定義されたパートナーがデフォルト・パートナーになります。内部パートナーが通信する他社が外部パートナーです。

文書交換の相手となるパートナーごとに、パートナー・プロファイルを作成する必要があります。プロファイルの作成だけでなく、プロファイルのセットアップも必要です。セットアップとは、いくつかの必須ステップとオプション・ステップで構成されるプロセスです。

この章では、パートナー・プロファイルの作成および設定の基本的な手順について、概要を説明します。各ステップの詳細については、そのステップまたはセクションの最後にある参照先を参照してください。この章では以下のセクションを扱います。

- 『パートナー・プロファイルの作成』
- 27 ページの『宛先の作成』
- 28 ページの『B2B 機能の設定』
- 29 ページの『証明書のロード』
- 30 ページの『ユーザーの作成』
- 31 ページの『FTP ユーザーの構成』
- 32 ページの『グループの作成』
- 33 ページの『連絡先の作成』
- 34 ページの『住所の作成』

**注:** WebSphere Partner Gateway の構成変更を行う場合は、必ず、コミュニティー・コンソールにログインしたときと同じブラウザー・インスタンスを使用してください。複数のブラウザー・インスタンスを同時に使用すると、構成変更が無効になる可能性があります。

## パートナー・プロファイルの作成

### このタスクについて

WebSphere Partner Gateway でパートナーを定義する場合、これが最初のステップです。このステップでは、パートナーの基本情報 (名前、ログイン名。ビジネス ID など) を定義します。

パートナーを作成するには、パートナーに関する以下の情報が必要です。

- パートナーが使用するビジネス ID。以下のものを使用できます。

– DUNS - 各会社に割り当てられた標準の Dun & Bradstreet 番号。
– DUNS+4 - DUNS 番号の拡張版。
– フリー・フォーム - パートナーが会社の識別に使用する任意の番号。

ハブ・コミュニティーに追加したいパートナーごとに、以下の手順を実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**作成**」をクリックします。
3. 「**会社ログイン名**」を入力します。これは、パートナーがハブへのログイン時に「会社」フィールドに使用する名前です。「会社ログイン名」には、空白スペースを使用できません。
4. 「**パートナー表示名**」では、パートナーの会社名または他の記述名を入力します。これが、「**パートナー検索**」リストに表示される名前です。
5. パートナーのタイプを選択します。これが最初のパートナーなら、WebSphere Partner Gateway を所有する会社のセットアップを行うことになるでしょう。したがって、「**内部パートナー**」を選択します。この現行の内部パートナーをデフォルトに設定したい場合は、パートナー構成画面で「**デフォルト内部パートナー**」チェック・ボックスを選択します。他のパートナーに対してこのチェック・ボックスを選択すると、この内部パートナーから自動的にデフォルト選択が除去されます。このページで選択をクリアすることはできません。最初に作成された内部パートナーの場合、このチェック・ボックスはデフォルトで選択されています。
6. (オプション) 管理者の管理ユーザー名を入力します。ユーザー「管理ユーザー名」は、すべてのパートナーにわたって固有です。パートナーの管理者は、このパートナーに対する管理アクティビティー (宛先、B2B 機能、ユーザーなどの管理) を実行できます。ハブ・オペレーターは、常に、パートナー管理に対する全アクセス権限を持っています。
7. パートナーの状況を選択します。パートナーの状況が「使用不可」の場合は、「**使用可能**」を選択します。「**使用可能**」が、パートナーのデフォルトの状況です。
8. (オプション) 「**ベンダー・タイプ**」フィールドに、会社のタイプを入力します。
9. (オプション) パートナーの「**Web サイト**」を入力します。
10. 「**ビジネス ID**」>「**新規**」をクリックします。
11. リストからタイプを指定し、適切な ID を入力します。WebSphere Partner Gateway では、ここで入力した番号を使用して、パートナーへ (またはパートナーから) の文書をルーティングします。

    ID を入力する際には、以下のガイドラインに従ってください。

    a. DUNS 番号は 9 桁であること。
    b. DUNS+4 は 13 桁であること。
    c. フリー・フォーム ID 番号は 60 文字以内の英数字および特殊文字で構成すること。

**注:** パートナーには、複数のビジネス ID を割り当てることができます。複数のビジネス ID が必要になる場合もあります。例えば、ハブが EDI X12 および EDIFACT 文書を送受信する場合は、文書交換時に DUNS およびフリー・フォーム ID が使用されます。

このタイプの文書フローに関わる内部パートナーと外部パートナーは、DUNS およびフリー・フォーム ID を持っている必要があります。フリー・フォーム ID は、ID と修飾子の両方を持つ EDI ID を表すために使用されます。例えば、EDI 修飾子が「ZZ」で、EDI ID が「810810810」であるとします。フリー・フォーム ID は ZZ-810810810 として指定できます。

12. (オプション) パートナーの IP アドレスを入力します。IP アドレスは、「クライアント IP の検証」が構成されている場合に宛先と連動して使用されます。以下のステップを実行して、IP アドレスを入力します。
    a. 「**IP アドレス**」の下の「**新規**」をクリックします。
    b. 動作モードを指定します。
    c. パートナーの IP アドレスを入力します。
13. 「**保管**」をクリックします。
14. 管理ユーザー名を入力した場合は、パートナーがハブにログオンするときに使用するパスワードが表示されます。そのパスワードを書き留めます。それを後でパートナー管理ユーザーに渡します。

## 宛先の作成

### このタスクについて

パートナーのプロファイルを作成したら、ハブがそのパートナーに文書を送信するときに使用する宛先を設定する必要があります。

パートナーの宛先を作成するには、以下の手順を実行します。

1. 宛先を作成するパートナー・プロファイルが選択されていることを確認します。

   プロファイルを作成したばかりの場合は、そのプロファイルが既に選択されています。選択されていない場合は次の手順を実行してください。
   a. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」の順にクリックします。
   b. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
   c. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
2. 「**宛先**」をクリックします。
3. 「**作成**」をクリックします。
4. 「**宛先名**」を入力して、宛先を識別します。
5. (オプション) 宛先の**状況**を指定します。
6. (オプション) 宛先が**オンライン**か**オフライン**かを指定します。
7. (オプション) 宛先の**説明**を入力します。
8. 「**トランスポート**」を選択します。

9. トランスポートを選択すると、このページの「**宛先構成**」セクションがそのトランスポート固有の表示になります。トランスポートごとにこのセクションに記入する方法については、以下のセクションのいずれかを参照してください。
   - 228 ページの『グローバルなトランスポート値の設定』

     **注:** これらの値は、FTP スクリプト記述宛先でのみ必要になるものです。
   - 230 ページの『HTTP 宛先の設定』
   - 232 ページの『HTTPS 宛先の設定』
   - 234 ページの『FTP 宛先の設定』
   - 236 ページの『SMTP 宛先の設定』
   - 237 ページの『JMS 宛先の設定』
   - 240 ページの『ファイル・ディレクトリー宛先の設定』
   - 241 ページの『FTPS 宛先の設定』
   - 244 ページの『FTP スクリプト記述宛先の設定』
   - 243 ページの『SFTP 宛先の設定』

## B2B 機能の設定

### このタスクについて

各パートナーには、送受信できる文書のタイプを定義する B2B 機能が備わっています。

ハブ管理者は各パートナーの B2B 機能を設定できますが、パートナー各自がこのタスクを実行することも可能です。B2B 機能は、パートナーの B2B 機能を文書定義に関連付けるために使用します。

各パートナーの B2B 機能を設定するには、以下の手順を実行します。

1. B2B 機能を構成するパートナー・プロファイルが選択されていることを確認します。選択したプロファイルは、「**プロファイル**」の後のページの上に表示されます。

   プロファイルを作成したばかりの場合は、そのプロファイルが既に選択されています。選択されていない場合は次の手順で選択してください。

   a. 「**アカウント管理**」をクリックします。
   b. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
   c. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
2. 「**B2B 機能**」をクリックします。「B2B 機能」ページが表示されます。このページの右側には、文書定義としてシステムでサポートされているパッケージ、プロトコル、文書が表示されます。
3. パッケージの「**ソースの設定**」列の下の「**役割はアクティブではありません**」アイコンをクリックします。パッケージには、外部パートナーが内部パートナーに送信する文書が格納されています。

4. パートナーが同じ文書を送受信する場合は、「**ソースの設定**」と「**ターゲットの設定**」の両方を選択します。文書定義が使用可能な場合は、コンソールにチェック・マークが表示されます。

   **注:** 「ソースの設定」の選択項目は、2 方向 PIP のどのアクションでも同じになります。これは、あるパートナーから要求が発信され、別のパートナーから対応する確認が発信される場合でも同じです。また、これは「ターゲットの設定」にも該当します。
5. 「**パッケージ**」レベルで「**展開**」アイコンをクリックして、個々のノードを適切な文書定義レベルまで展開します。あるいは、「**0**」**から**「**4**」の数値または「**すべて**」を選択して、表示されているすべての文書定義を選択済みのレベルまで展開します。
6. 再度、システムがサポートする文書定義ごとに、低レベルの「**プロトコル**」および「**文書タイプ**」の各レベルに対して、「**ソースの設定**」または「**ターゲットの設定**」、あるいはその両方の役割を選択します。

   「**文書タイプ**」レベルで定義をアクティブにした場合は、「**アクション**」および「**アクティビティー**」の定義も (存在する場合)、自動的にアクティブになります。
7. (オプション) 「**使用可能**」列の下の「**使用可能**」をクリックして、文書定義をオフラインにします。(「**ソースの設定**」または「**ターゲットの設定**」を選択すると、レコードが自動的に使用可能になります。) オンラインにするには、「**使用不可**」をクリックします。

   パッケージが使用不可の場合は、同じノード内にある低レベルの文書定義が、個々の状況が使用可能であるかどうかにかかわらず、すべて使用不可になります。低レベルの文書定義を使用不可にした場合、同じコンテキスト内にある高レベルの定義はすべて使用可能なままになります。文書定義が使用不可になると、それまでに存在していた接続や属性はすべて機能しなくなります。
8. (オプション) プロトコル、パッケージ、文書タイプ、アクション、アクティビティー、またはシグナルの属性を編集する場合は、「**編集**」アイコンをクリックします。これにより、属性がある場合は、属性の設定が表示されます。属性を変更するには、値を入力するか、または「**更新**」列から値を選択して、「**保存**」をクリックします。

# 証明書のロード

## このタスクについて

証明書を使用すれば、パートナーは、暗号化、デジタル署名、SSL などの方法でセキュア文書を送受信することができます。パートナーが別のパートナーから証明書を受け取ると、そのパートナーはこれらのうち、任意の方法を使用して文書を送信できます。

パートナー向けの証明書をアップロードするには、292 ページの『ウィザードを使用した証明書のアップロード』で説明されているステップを使用してください。

証明書の使用について詳しくは、257 ページの『第 13 章 文書交換のセキュリティーの使用可能化』を参照してください。

# ユーザーの作成

## このタスクについて

ユーザーとは、ログインしてこのパートナーの管理タスクを実行する人のことです。LDAP サーバーおよび WAS 管理コンソールに追加される新規ユーザーは、アクティブにするために、WebSphere Partner Gateway コンソールにも追加する必要があります。

パートナーのユーザーを作成するには、以下の手順を実行します。

1. ユーザーを作成するパートナー・プロファイルが選択されていることを確認します。選択したプロファイルは、「**プロファイル**」>の後のページの上に表示されます。プロファイル名が選択されていない場合は次の手順でプロファイルを作成してください。
   a. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
   b. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
   c. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
2. 「**ユーザー**」をクリックします。
3. 「**作成**」をクリックします。
4. ユーザーの名前を入力します。

   **注:** ユーザー名は、システム内のすべてのパートナーで固有でなければなりません。
5. 状況が「**有効**」であることを確認してください。
6. (オプション) 姓、名、およびユーザーのその他の個人情報を入力します。
7. ユーザーの「**言語**」、「**書式ロケール**」、および「**時間帯**」を選択します。
8. ユーザー状況の「アラート状況」を「**有効**」に変更します。
9. ユーザーの「サブスクライブ済み可視化 (Subscribed Visibility)」を選択します。
10. 「**パスワードの自動生成**」をクリックしてそのユーザーのパスワードを作成するか、パスワードを入力し、再入力します。
11. 「**保存**」をクリックします。

**注:**

1. LDAP サーバーでは固有のユーザー名が必須であるため、WebSphere Partner Gateway でもユーザー名は固有でなければなりません。新規ユーザーを作成したときにそのユーザー名が同一パートナーまたは別パートナーで既に使用されている場合は、「**この名前のユーザーはすでに存在します**」というエラー・メッセージが表示されます。
2. ユーザー名の制限がない旧バージョンから WebSphere Partner Gateway にマイグレーションする場合は、重複するユーザー名の横に二重アスタリスク (**) が表示されて、このユーザー名が同一のパートナー・プロファイル、または別のパートナー・プロファイルに既に存在することを知らせます。ユーザー名が互いに固有になるように、いずれか一方のユーザー名を変更してください。LDAP サーバ

ーおよび WAS 管理コンソールに追加される新規ユーザーおよびグループは、アクティブにするために、WebSphere Partner Gateway コンソールにも追加する必要があります。

LDAP を WebSphere Partner Gateway で使用できるようにするには、WebSphere Application Server コンソールから LDAP サーバー認証をセットアップし、WebSphere Partner Gateway コミュニティー・コンソールから LDAP ユーザー許可をセットアップする必要があります。LDAP 認証のセットアップについては、「*WebSphere Partner Gateway インストール・ガイド*」を参照してください。ユーザーの管理および LDAP ユーザー許可の設定方法については、「*WebSphere Partner Gateway E/A 管理ガイド*」を参照してください。

ユーザーの管理について詳しくは、「*WebSphere Partner Gateway パートナー・ガイド*」の『ユーザーの管理』を参照してください。

## FTP ユーザーの構成

### このタスクについて

現在のユーザーを FTP ユーザーとして使用可能にするには、以下の手順を実行します。

1. 「**アカウント管理**」>「**FTP ユーザー管理**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのユーザーのリストを表示します。
3. 連絡先について「状況」列が使用不可になっている場合は、アイコンをクリックして使用可能にします。アイコンは使用可能と使用不可の状態を切り替えることができます。
4. FTP アクセスを構成する対象のユーザーに対する「**詳細の表示**」アイコンをクリックします。ユーザーの詳細ページが表示されます。
5. 「**FTP 構成**」を編集します。
6. 「**ホーム・ディレクトリー**」を入力します。これは bcg.ftp.config.rootdirectory に指定された値からの相対パスです。このフィールドは必須です。
7. ホーム・ディレクトリーへの「**書き込みアクセス権**」を使用可能または使用不可にします。
8. 「**ディレクトリーの作成/除去**」を使用可能または使用不可にします。
9. 「**最大ログイン回数**」を選択します。これは、許可される並行ログインの最大数です。「カスタム制限」を選択した場合は、テキスト・ボックスにカスタマイズされた値を入力してください。
10. 「**同一 IP からの最大ログイン回数**」を選択します。これは、同一の IP アドレスから許可される並行ログインの最大数です。リストから「カスタム制限」を選択した場合は、テキスト・ボックスにカスタマイズされた値を入力してください。
11. 「**最大アイドル時間**」を選択します。これは、ユーザー接続が廃棄されるまでの最大アイドル時間 (秒単位) です。リストから「カスタム制限」を選択した場合は、テキスト・ボックスにカスタマイズされた値を入力してください。

12. 「**最大アップロード**」を選択します。これは、アップロードの最大速度 (バイト/秒) です。リストから「カスタム制限」を選択した場合は、テキスト・ボックスにカスタマイズされた値を入力してください。
13. 「**最大ダウンロード**」を選択します。これは、ダウンロードの最大速度 (バイト/秒) です。リストから「カスタム制限」を選択した場合は、テキスト・ボックスにカスタマイズされた値を入力してください。
14. 「**保存**」をクリックします。

## グループの作成

### このタスクについて

ユーザーをグループ化すると、複数のユーザーのアクセス権を同時に管理できます。LDAP サーバーおよび WebSphere Application Server 管理コンソールに追加される新規グループは、アクティブにするために、WebSphere Partner Gateway コンソールにも追加する必要があります。

パートナーごとにグループを作成するには、以下の手順を実行します。

1. グループを作成するパートナー・プロファイルが選択されていることを確認します。

   プロファイルを作成したばかりの場合は、そのプロファイルが既に選択されています。選択されていない場合は次の手順で選択してください。

   a. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」の順にクリックします。
   b. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
   c. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
2. 「**グループ**」をクリックします。
3. 「**作成**」をクリックします。
4. このグループの名前を入力します。
5. 「**保存**」をクリックします。
6. このグループにユーザーを追加するには、「**メンバーシップ**」リンクをクリックします。

   このパートナーに関連付けられているユーザーが、「**グループ外のユーザー**」または「**グループ内のユーザー**」の下に表示されます。ユーザーをグループに追加するには、以下を実行します。

   a. グループの横の「**レコードの編集 (Edit Record)**」アイコンをクリックします。
   b. 追加するユーザーを選択して、「**グループへの追加**」をクリックします。
   c. 「**保存**」をクリックします。
7. このグループ内のユーザーのアクセス権を変更するには、「**アクセス権**」リンクをクリックします。

このグループのユーザーのアクセス権が、**モジュール**別に表示されます。このグループのアクセス権を変更するには、以下を実行します。

a. グループの横の「**レコードの編集 (Edit Record)**」アイコンをクリックします。
b. 各モジュール右側のラジオ・ボタンをクリックして、アクセス権を「**アクセスなし**」、「**読み取り専用**」、「**読み取り/書き込み**」のいずれかに指定します。
c. 「**保存**」をクリックします。

**注:** ユーザーは複数のグループに所属できます。その場合、グループごとにアクセス権が異なると、ユーザーはすべてのグループでそのユーザーに割り当てられているアクセス権のうち最もレベルが高いアクセス権を継承します。

**注:** hubadmin グループのすべてのメンバーは、スーパーユーザーのアクセス権を持ちます。このため、パスワード・セキュリティーの保守に際しては、複数のユーザーで hubadmin の責任を共用できます。

グループの管理について詳しくは、「*WebSphere Partner Gateway パートナー・ガイド*」の『グループの管理』を参照してください。

## 連絡先の作成

### このタスクについて

WebSphere Partner Gateway では、各種のイベントが発生した場合に通知できるように、連絡先を作成することができます。パートナーごとに連絡先を作成するには、以下の手順を実行します。

1. 連絡先を作成するパートナー・プロファイルが選択されていることを確認します。選択したプロファイルは、「**プロファイル**」>の後のページの上に表示されます。

   プロファイルが選択されていない場合は、以下のステップを実行します。

   a. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
   b. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
   c. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
2. 「**連絡先**」をクリックします。
3. 「**作成**」をクリックします。
4. この連絡先の「**名**」および「**姓**」を入力します。
5. (オプション) この連絡先の「**アドレス**」を入力します。
6. (オプション) 「**連絡先タイプ**」を選択します。
7. (オプション) この連絡先の「**E メール**」アドレス、「**電話番号**」、「**FAX 番号**」を入力します。
8. 連絡先の「**言語**」、「**書式ロケール**」、および「**時間帯**」を選択します。
9. ユーザー状況の「**アラート状況**」を「**有効**」に変更します。

10. ユーザーの「**サブスクライブ済み可視化 (Subscribed Visibility)**」を選択します。
11. 「**保存**」をクリックします。

連絡先の管理について詳しくは、「*WebSphere Partner Gateway パートナー・ガイド*」の『連絡先の管理』を参照してください。

## 住所の作成

### このタスクについて

WebSphere Partner Gateway では、パートナーのアドレスを作成できます。パートナーのアドレスを作成するには、以下の手順を実行します。

1. アドレスを作成するパートナー・プロファイルが選択されていることを確認します。選択したプロファイルは、「**プロファイル**」>の後のページの上に表示されます。

   プロファイルを作成したばかりの場合は、そのプロファイルが既に選択されています。選択されていない場合は次の手順で選択してください。

   a. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
   b. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
   c. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
2. 「**住所**」をクリックします。
3. 「**新規住所の作成**」をクリックします。
4. 「**住所のタイプ**」を選択します。
5. (オプション) 「**アドレス**」を入力します。
6. 「**保存**」をクリックします。

アドレスの管理について詳しくは、「*WebSphere Partner Gateway パートナー・ガイド*」の『住所の管理』を参照してください。

# 第 4 章 ハブを構成するための準備

次章以降では、 5 ページの『第 2 章 ハブ構成の概要』で説明したレシーバーおよび宛先の設定を行います。文書の送受信に使用するトランスポートのタイプによって、受信側および宛先をセットアップする必要があります。

この章では以下のトピックを扱います。

- 『 ファイル・ディレクトリー宛先の作成』
- 『文書を受信する FTP サーバーの構成』
- 39 ページの『JMS トランスポート・プロトコル用のハブの構成』
- 46 ページの『RNIF 圧縮の構成』

また、FTP スクリプト記述レシーバーおよび宛先で必要な FTP スクリプトの概要を取り上げ、Data Interchange Services クライアントについて説明します。このクライアントは、変換や検証を作成したり、EDI、XML、およびレコード指向データ (ROD) 文書の機能確認通知マップを作成したりするために使用できます。

- 46 ページの『FTP スクリプト記述レシーバーおよび宛先用の FTP スクリプトの使用』
- 47 ページの『Data Interchange Services クライアントのマップの使用』

これらのタイプのレシーバーや宛先の設定を予定していない場合は、この章を省略して 49 ページの『第 5 章 サーバーの始動およびコミュニティー・コンソールの表示』に進んでください。

## ファイル・ディレクトリー宛先の作成

必要な場合、ファイル・ディレクトリー宛先に指定したディレクトリーが、ユーザーに代わって作成されるようになりました。既に存在する場合、宛先にそれが使用されます。

## 文書を受信する FTP サーバーの構成

**注:** このセクションは、パートナーから FTP または FTPS を介して文書を受信する場合にのみ適用されます。パートナーへの文書の送信については、 234 ページの『FTP 宛先の設定』および 241 ページの『FTPS 宛先の設定』で説明しています。

着信文書用のトランスポートとして FTP または FTPS を使用する場合は、FTP サーバーをインストールしておく必要があります。FTP を使用する予定で、サーバーをまだインストールしていない場合は、次のステップに進む前に、ここでインストールを行ってください。また、ご使用のシステムが、以下のいずれかのシナリオに該当することを確認してください。

- FTP サーバーが、WebSphere Partner Gateway がインストールされているのと同じマシンにインストールされている。

- WebSphere Partner Gateway マシンの bcguser には、FTP サーバーがファイルを保管する場所にアクセスするための読み取り/書き込みアクセス権限がある。

**注:** 複数のマシンにインストール済み環境がセットアップされている場合、FTP サーバーは、受信側がインストールされているマシンにインストールする必要があります。

## FTP サーバーの必要なディレクトリー構造の構成

### このタスクについて

FTP サーバーをインストールしたら、FTP サーバーのホーム・ディレクトリーの下に、必要なディレクトリー構造を作成します。WebSphere Partner Gateway では、着信文書を送信しているパートナーを正しく識別するためにレシーバー・コンポーネントおよび文書マネージャー・コンポーネントが使用する、特定のディレクトリー構造が必要となります。構造は 図 15 に示されています。

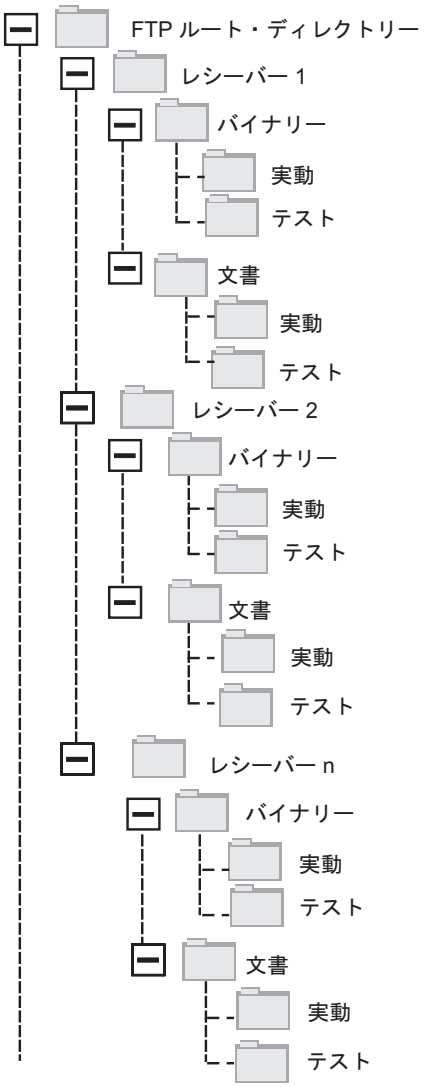



*図 15. FTP ディレクトリー構造*

各パートナーのディレクトリーには、「バイナリー」ディレクトリーと「文書」ディレクトリーが含まれています。また、「バイナリー」ディレクトリーと「文書」ディレクトリーのどちらにも、「実動」ディレクトリーと「テスト」ディレクトリーが含まれています。

「文書」ディレクトリーは、パートナーが完全なルーティング情報を含む XML 文書を (FTP を使用して) ハブに送信する際に使用されます。それには、カスタム XML 定義を作成する必要があります。また、このディレクトリーを使用して電子データ交換 (EDI) 文書を送信できます。

「バイナリー」ディレクトリーは、パートナーがそれ以外の文書を (FTP を使用して ) ハブに送信する際に使用されます。

FTP を使用して文書を送受信するパートナーごとに、FTP サーバーのルート・ディレクトリーから以下のフォルダーを作成します。

1. パートナー用のフォルダーを作成します。

   **注:** フォルダーの名前は、パートナーの作成時に「**会社ログイン名**」に指定した名前と一致しなければなりません。パートナーの作成については、25 ページの『パートナー・プロファイルの作成』で説明します。
2. パートナー用のフォルダーの下に、「**バイナリー**」と「**文書**」という名前のサブフォルダーを作成します。
3. 「バイナリー」フォルダーと「文書」フォルダーの下に、「**実動**」と「**テスト**」という名前のサブフォルダーを作成します。

## FTP 経由で送信されるファイルの処理

FTP サーバーがバイナリー・ファイルや XML ファイルを処理する方法を理解しておくことは重要です。

### バイナリー・ファイル

バイナリー・ファイルは文書マネージャーでは一切検査されないため、特定のファイル名構造を使用する必要があります。

ファイル名構造は、*<To_PartnerID>.<Unique_Filename>* のようになります。

レシーバー・コンポーネントで検出されたバイナリー・ファイルは共用ストレージに書き込まれ、処理を行うために文書マネージャーに渡されます。

ファイルが検出されたディレクトリーの名前は、「送信元パートナー名 (From Partner Name)」の評価に使用され、ファイル名の最初の部分は「送信先パートナー名 (To Partner Name)」の評価に使用されます。ディレクトリー構造におけるディレクトリーの位置は、当該トランザクションが実動トランザクションなのかテスト・トランザクションなのかを評価する際に使用されます。

例えば、123456789.abcdefg1234567 という名前のファイルが ¥ftproot¥partnerTwo¥binary¥production ディレクトリーで検出されたとします。文書マネージャーは以下の情報を認識します。

- 「送信元パートナー名 (From Partner Name)」は partnerTwo である (ディレクトリー・ツリーの partnerTwo 部分でファイルが検出されたため)。

- 「送信先パートナー名 (To Partner Name)」は partnerOne である (ファイル名の最初の部分が 123456789 で、これが partnerOne の DUNS ID であるため)。

  **注:** この例および本書全体を通して、DUNS 番号はすべて例として示されています。WebSphere Partner Gateway では、<To_PartnerID> が受信側パートナー DUNS と一致する必要があります。Duns ID が見つからない場合は、チャネル検索が失敗します。
- トランザクション・タイプは実動である。

文書マネージャーは、実動タイプのパートナー接続を検索します。

- パッケージ: なし (N/A)
- プロトコル: バイナリー (1.0)
- 文書タイプ: バイナリー (1.0)

文書マネージャーは次にファイルを処理します。

バイナリー・ファイルは、汎用前処理ハンドラーまたは FileNamePartnerId ハンドラーを使用して FTP により転送することもできます。詳細については、 80 ページの『前処理構成ポイントの変更』を参照してください。

### XML ファイル

カスタム XML 仕様を使用してルーティングされた XML ファイルは、文書マネージャーによって検査され、ルーティング情報が文書自体から取り出されるため、ファイル名要件がありません。

レシーバー・コンポーネントで検出された XML ファイルは共用ストレージに書き込まれ、文書マネージャーに渡されて処理されます。

文書マネージャーは XML ファイルを定義済みの XML 形式と比較し、必要な XML 形式を選択します。(XML 形式のセットアップについては、 162 ページの『カスタム XML 文書処理』で説明します。) 送信元パートナー名、送信先パートナー名、およびルーティング情報は、XML ファイルから抽出されます。

ディレクトリー構造におけるディレクトリーの位置は、当該トランザクションが実動トランザクションなのかテスト・トランザクションなのかを評価する際に使用されます。

文書マネージャーはこの情報を使って正しいパートナー接続を見つけてから、ファイルを処理します。

## 追加の FTP サーバー構成

### このタスクについて

必要なディレクトリー構造を作成したら、ハブ・コミュニティーのパートナーごとに FTP サーバーを構成します。FTP サーバーを構成する方法は、使用するサーバーによって異なります。FTP サーバーのマニュアルを参照して、以下のタスクを実行してください。

1. 新規のグループ (例えば Partners) を追加します。

2. FTP で文書を送受信する各パートナーを示すユーザーを、新規作成したグループに追加します。
3. 各パートナーに対して、FTP サーバーをセットアップし、 36 ページの『 FTP サーバーの必要なディレクトリー構造の構成』でパートナーに対して作成したディレクトリー構造に着信パートナーをマップします。詳しくは、ご使用の FTP サーバーのマニュアルを参照してください。

### FTPS サーバーのセキュリティー考慮事項

FTPS サーバーを使用して着信文書を受信する場合、SSL セッションに関するセキュリティー考慮事項は、パートナーが使用する FTPS サーバーおよびクライアントでのみ処理されます。着信 FTPS 文書での WebSphere Partner Gateway に固有のセキュリティー構成はありません。WebSphere Partner Gateway は、サーバーがセキュア・チャネルを正常に折衝し、文書を受け取った後で、FTP レシーバー ( 64 ページの『 FTP レシーバーの設定』を参照) から文書を取り出します。FTPS サーバーのマニュアルを参照して、パートナーが接続できるセキュア・チャネルを正常に構成するために必要な証明書 (およびどこで証明書が必要か) を判別してください。

サーバー認証の場合、レシーバー・コンポーネントの証明書をパートナーに提供します。証明書が認証局 (CA) によって発行される場合、CA 証明書チェーンも提供します。クライアント認証が FTPS サーバーによってサポートされる場合、パートナーのクライアント認証証明書を FTPS サーバーで指定する必要があります。クライアント認証およびクライアント認証証明書の指定については、FTPS サーバーの資料を参照してください。

## JMS トランスポート・プロトコル用のハブの構成

ここでは、JMS トランスポートを使用するようハブをセットアップする方法について説明します。JMS トランスポートを使用してハブで文書を送受信する場合は、ここで説明する手順に従ってください。JMS トランスポートを使用しない場合は、この部分を省略してください。

**注:** ここで示す手順では、WebSphere MQ の JMS インプリメンテーションを使用して、JMS 環境を設定する方法について説明します。この手順では、ローカル・キューのセットアップ方法も説明します。伝送およびリモート・キューをセットアップする場合は、WebSphere MQ 文書を参照してください。

このセクションの説明は WebSphere MQ 固有ですが、他の JMS プロバイダーでも類似の手順が必要になります。 WebSphere Platform Messaging の場合は、「*WebSphere Partner Gateway 統合ガイド*」の『第 5 章 トランスポートとしての JMS と WebSphere Process Server の統合』の『WebSphere Partner Gateway を WebSphere Application Server にインストールする場合の JMS の構成』を参照してください。

JMS レシーバーまたは宛先 (あるいは両方) を設定する方法については、本書の後のセクションで取り上げます。これらの作業については、 67 ページの『 JMS レシーバーの設定』、および 237 ページの『JMS 宛先の設定』で説明します。

## JMS 用のディレクトリーの作成

### このタスクについて

まず JMS 用のディレクトリーを作成します。例えば、Windows のインストール環境で、c:¥temp ディレクトリー内に JMS という名前のディレクトリーを作成したいとします。これを行うには、以下のステップを実行します。

1. Windows のエクスプローラーを開きます。
2. C:¥temp ディレクトリーを開きます。
3. JMS という名前のフォルダーを新規作成します。

## デフォルトの JMS 構成の変更

### このタスクについて

ここでは、WebSphere MQ のインストールに含まれる JMSAdmin.config ファイルを更新して、コンテキスト・ファクトリーおよびプロバイダー URL を変更します。

1. WebSphere MQ の Java¥bin ディレクトリーに移動します。例えば、Windows のインストール環境では C:¥IBM¥MQ¥Java¥bin に移動します。
2. メモ帳や vi などのプレーン・テキスト・エディターを使用して、JMSAdmin.config ファイルを開きます。
3. 以下の行の前に「#」文字を追加します。

   ```
   INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
   PROVIDER_URL=ldap://polaris/o=ibm,c=us
   ```

4. 以下の行の前にある「#」文字を削除します。

   ```
   #INITIAL_CONTEXT_FACTORY=com.sun.jndi.fscontext.RefFSContextFactory
   #PROVIDER_URL=file:/C:/JNDI-Directory
   ```

5. PROVIDER_URL=file:/C:/JNDI-Directory という行を、『 JMS 用のディレクトリーの作成』で設定した JMS ディレクトリーの名前に変更します。例えば、c:/temp/JMS ディレクトリーを設定する場合は、この行が以下のようになります。

   ```
   PROVIDER_URL=file:/c:/temp/JMS
   ```

6. ファイルを保存します。

## キューおよびチャネルの作成

ここでは、WebSphere MQ を使用して、文書の送受信に使われるキューおよびこの通信のチャネルを作成します。キュー・マネージャーが作成されていることが前提となっています。キュー・マネージャーの名前は、以下のステップの *<queue_manager_name>* に入ります。また、このキュー・マネージャーのリスナーが TCP ポート 1414 で開始されていることも前提となっています。

1. コマンド・プロンプトを開きます。
2. 以下のコマンドを入力して、WebSphere MQ コマンド・サーバーを開始します。

   ```
   strmqcsv <queue_manager_name>
   ```

3. 以下のコマンドを入力して、WebSphere MQ コマンド環境を開始します。

   ```
   runmqsc <queue_manager_name>
   ```

4. 以下のコマンドを入力して、ハブに送信される着信文書を保持するための WebSphere MQ キューを作成します。

```
def ql(<queue_name>)
```

例えば、JMSIN という名前のキューを作成するには、以下のように入力します。

```
def ql(JMSIN)
```

5. 以下のコマンドを入力して、ハブから送信される文書を保持するための WebSphere MQ キューを作成します。

```
def ql(<queue_name>)
```

例えば、JMSOUT という名前のキューを作成するには、以下のように入力します。

```
def ql(JMSOUT)
```

6. 以下のコマンドを入力して、ハブから送受信される文書が使用する WebSphere MQ チャネルを作成します。

```
def channel(<channel_name>) CHLTYPE(SVRCONN)
```

例えば、java.channel という名前のチャネルを作成するには、以下のように入力します。

```
def channel(java.channel) CHLTYPE(SVRCONN)
```

7. 以下のコマンドを入力して、WebSphere MQ コマンド環境を終了します。

```
end
```

## 現行環境への Java ランタイムの追加

### このタスクについて

現行のシステム・パスに Java(TM) ランタイムを追加するには、以下のコマンドを入力します。

```
set PATH=<ProductDir>¥_jvm¥jre¥bin
```

ここで、*ProductDir* は、WebSphere Partner Gateway がインストールされているディレクトリーを表します。

## JMS 構成の定義

### このタスクについて

JMS 構成を定義するには、以下のステップを実行します。

1. WebSphere MQ Java ディレクトリー (ディレクトリー (*<path_to_Websphere_MQ_installation_directory>*¥java¥bin) に移動します。
2. 以下のコマンドを入力して、JMSAdmin アプリケーションを始動します。

```
JMSAdmin
```

3. InitCtx> プロンプトから以下のコマンドを入力して、新規 JMS コンテキストを定義します。

```
define ctx(<context_name>)
change ctx(<context_name>)
```

例えば、*context_name* が JMS である場合、コマンドは次のようになります。

```
define ctx(JMS)
```

```
change ctx(JMS)
```

4. InitCtx/jms> プロンプトから以下の JMS 構成を入力します。

```
define qcf(connection_factory_name)
    tran(CLIENT)
    host(<your_IP_address>)
    port(1414)
    chan(java.channel)
    qmgr(<queue_manager_name>)

define q(<name>) queue(<queue_name>) qmgr(<queue_manager_name>)

define q(<name>) queue(<queue_name>) qmgr(<queue_manager_name>)

end
```

**注:**

- MQ および WebSphere Partner Gateway が 2 つの別々のマシンにインストールされている場合は、CLIENT のトランスポート・タイプを選択してください。
- MQ と WebSphere Partner Gateway が同じマシンにインストールされている場合は、トランスポート・タイプは BINDINGS でなければなりません。

前のステップでは .bindings ファイルを作成しました。これは、ステップ 5 (40 ページ) で指定したフォルダーのサブフォルダーにあります。サブフォルダーの名前は、JMS コンテキストに対して指定した名前です。

例えば、以下の JMSAdmin セッションを使用して、MQ キュー・マネージャーがある sample.ibm.com の IP アドレスを指定して、Hub としてキュー接続ファクトリーを定義します (<*queue_manager_name*>は sample.queue.manager)。この例では、40 ページの『キューおよびチャネルの作成』で作成した JMS キュー名およびチャネル名が使用されています。ユーザー入力は、> プロンプトの後に行います。

```
InitCtx> define ctx(jms)
InitCtx> change ctx(jms)
InitCtx/jms> define qcf(Hub)
    tran(CLIENT)
    host(sample.ibm.com)
    port(1414)
    chan(java.channel)
    qmgr(sample.queue.manager)
InitCtx/jms> define q(inQ) queue(JMSIN) qmgr(sample.queue.manager)
InitCtx/jms> define q(outQ) queue(JMSOUT) qmgr(sample.queue.manager)
InitCtx/jms>end
```

この例では、.bindings ファイルはディレクトリー c:/temp/JMS/JMS にあります。ここで、c:/temp/JMS は PROVIDER_URL、JMS はコンテキスト名です。

## ランタイム・ライブラリーの構成

JMS レシーバーまたは JMS 宛先の場合は、WebSphere Partner Gateway で表示する必要がある WebSphere MQ JAR ファイルが多数あります。このような JAR ファイルを表示できるようにするには、これらのファイルをクラス・パスに組み込みます。MQ バインディング・モードで MQ にアクセスする場合は、MQ ネイティブ・ライブラリーもクラス・パスに組み込む必要があります。MQ JAR ファイルと JMS のネイティブ・ライブラリーの詳細については、WebSphere MQ の資料を参照してください。

JAR ファイルを Websphere Partner Gateway クラス・パスに追加する方法は数種類あります。ユーザー出口ディレクトリーにこれらのファイルを格納する方法と、WebSphere Application Server 共用ライブラリーを使用してこれらのファイルを関連付ける方法があります。

### ユーザー出口ディレクトリーを使用する方法:

この方法では、指定された JAR ファイルを適切なユーザー出口ディレクトリーに格納します。

- JMS レシーバーの場合は <WPG-Install root>/receiver/lib/userexits ディレクトリーに格納します。
- JMS 宛先の場合は <WPG-Install root>/router/lib/userexits ディレクトリーに格納します。

### WebSphere Application Server 共用ライブラリーを使用する方法:

#### このタスクについて

この方法を使用するには、共用ライブラリー変数を作成し、この変数にレシーバーまたは文書マネージャー・アプリケーションを関連付けます。この手順の概要を以下に示します。この手順の詳細については、WebSphere Application Server の資料を参照してください。

1. WebSphere Application Server 管理コンソールにログインします。
2. 以下の手順で共用ライブラリー変数を作成します。
   a. 「**環境**」>「**共用ライブラリー**」にナビゲートします。
   b. 「**スコープ**」(一般にはノード) を選択して「**新規**」をクリックします。
   c. 変数名 (MQ_LIBRARIES など) を入力し、MQ JAR ファイルのクラス・パスのエントリーを入力し、「**OK**」をクリックします。
3. 以下の手順に従い、作成した共用ライブラリー変数に WebSphere Partner Gateway コンポーネントを関連付けます。
   a. 「**アプリケーション**」>「**エンタープライズ・アプリケーション**」にナビゲートします。
   b. 「**BCGReceiver**」 (JMS レシーバーの場合) または「**BCGDocMgr**」 (JMS 宛先の場合) を選択します。
   c. 「**共用ライブラリー参照**」を選択します。
   d. アプリケーションを選択し、「**参照共用ライブラリー**」をクリックします。
   e. 「使用可能」リストから、作成した共用ライブラリー変数 (MQ_LIBRARIES など) を選択し、この変数を「選択済み」リストへ移動します。「**OK**」をクリックします。

### 外部 MQ での JMS ゲートウェイおよびレシーバーの構成

#### このタスクについて

以下は、WebSphere Application Server 管理コンソールを使用して WebSphere Partner Gateway と MQ の間の通信ブリッジを作成するためのステップを示したものです。

1. JMS キュー接続ファクトリーを作成します。

a. WebSphere Application Server 管理コンソールにログインします。
b. 「**リソース**」>「**JMS**」>「**キュー接続ファクトリー**」にナビゲートします。
c. 「**スコープ**」を選択し、「**新規**」をクリックします。
   - ゲートウェイ構成の場合は、文書マネージャー・サーバー/ノードのスコープを選択します。 (ノード・スコープは、クラスターの場合に有用です。シンプル・モードの場合は、サーバー・スコープを選択します。)
   - レシーバーの構成の場合は、レシーバー・サーバー/ノードのスコープを選択します。 (ノード・スコープは、クラスターの場合に有用です。シンプル・モードの場合は、サーバー・スコープを選択します。)
d. 「**WebSphere MQ メッセージング・プロバイダー**」オプションを選択し、「**OK**」をクリックします。
e. 「**名前**」と「**JNDI 名**」を入力します。これらは必須の値です。
f. 「**キュー・マネージャー**」、「**ホスト**」 (キュー・マネージャーが実行されているマシンの IP)、「**ポート**」、「**チャネル**」、および「**トランスポート・タイプ**」に適切な値を入力します。残りのフィールドは任意指定です。

   **注:**
   - MQ および WebSphere Partner Gateway が 2 つの別々のマシンにインストールされている場合は、CLIENT のトランスポート・タイプを選択してください。
   - MQ と WebSphere Partner Gateway が同じマシンにインストールされている場合は、トランスポート・タイプは BINDINGS でなければなりません。

   詳細情報については、WebSphere Application Server インフォメーション・センター (http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multipla...) を参照してください。

2. JMS キューを作成します。
   a. WebSphere Application Server 管理コンソールにログインします。
   b. 「**リソース**」>「**JMS**」>「**キュー**」にナビゲートします。
   c. 「**スコープ**」を選択し、「**新規**」をクリックします。
      - ゲートウェイ構成の場合は、文書マネージャー・サーバー/ノードのスコープを選択します。 (ノード・スコープは、クラスターの場合に有用です。シンプル・モードの場合は、サーバー・スコープを選択します。)
      - レシーバーの構成の場合は、レシーバー・サーバー/ノードのスコープを選択します。 (ノード・スコープは、クラスターの場合に有用です。シンプル・モードの場合は、サーバー・スコープを選択します。)
   d. 「**名前**」と「**JNDI 名**」を入力します。これらは必須の値です。
   e. 「**キュー・マネージャー**」、「**ホスト**」 (キュー・マネージャーが実行されているマシンの IP)、「**ポート**」、「**チャネル**」、および「**トランスポート・タイプ**」に適切な値を入力します。残りのフィールドは任意指定です。
   f. 変更が行われたサーバーを再始動します。例えば、シンプル分散インストールの場合は、DocumentManager/Receiver/bcgserver。
3. WebSphere Partner Gateway 上に JMS ゲートウェイを構成します。
   a. WebSphere Partner Gateway 管理コンソールにログインします。

b. 「**アカウント管理**」>「**プロファイル**」>「**宛先**」をクリックします。
c. 「**作成**」をクリックします。
d. 「**宛先名**」を入力します。このフィールドは必須です。
e. 「トランスポート」フィールドで「**JMS**」を選択します。
f. 次の必須フィールドの値を入力します。
   - アドレス: WebSphere Application Server に作成されたキュー接続ファクトリーまたはキュー・オブジェクトの適切なホスト名およびポートを提供して宛先アドレスを入力します。このアドレスのフォーマットは、corbaloc:iiop: <hostname>: <bootstrapportnumber> でなければなりません。ここで、
     – corbaloc:iiop - クライアント (WebSphere Partner Gateway) とサーバー・ルックアップ (WebSphere Application Server) の間の通信に使用されるプロトコルを示します。
     – <hostname> - WebSphere Application Server がインストールされているマシンのホスト名または IP アドレス。このマシンに対してキュー接続ファクトリーおよびキュー・オブジェクトが作成されています。
     – <bootstrapportnumber> - キュー接続ファクトリーとキュー・オブジェクトがバインドされているサーバーのブートストラップ・ポート番号。ブートストラップ・ポート番号を知るには、WebSphere Application Server 管理コンソールにログインし、「**サーバー**」> 「**アプリケーション・サーバー**」 > **<サーバー名>** >「**ポート**」にナビゲートして、ブートストラップ・アドレスを確認することができます。配布モードの場合、ポート番号はレシーバーとゲートウェイとで異なります。正しいブートストラップ・ポート番号を得るためには、対応するサーバー (レシーバーの場合は bcgreceiver、ゲートウェイの場合は bcgdocmgr) にアクセスしてください。
   - JMS ファクトリー名: JMS キュー接続ファクトリーに提供されている JNDI 名。
   - JMS キュー名: JMS キューに提供されている JNDI 名。
   - JMS JNDI ファクトリー名: JNDI 通信に使用されるファクトリー。WebSphere Application Server を使用するので、この値には com.ibm.websphere.naming.WsnInitialContextFactory と指定することができます。

4. WebSphere Partner Gateway 上に JMS レシーバーを構成します。
   a. WebSphere Partner Gateway 管理コンソールにログインします。
   b. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックします。
   c. 「**レシーバーの作成**」をクリックします。
   d. 「**レシーバー名**」を入力します。このフィールドは必須です。
   e. 「トランスポート」フィールドで「**JMS**」を選択します。
   f. ステップ 3f の説明に従って、必須フィールドに適切な値を入力してください。

## RNIF 圧縮の構成

Rosettanet Business メッセージおよび添付ファイルは、大きい文書を転送するために、S/MIME エンベロープを使用して圧縮およびパッケージ化されます。また、Rosettanet Business メッセージに対する解凍サポートも提供されています。ペイロードを単独で圧縮するか、または添付ファイル付きで圧縮するかを選択するオプションが提供されています。パフォーマンスを向上させるためには、暗号化、署名、または転送エンコードの前に、Rosettanet 2.0 Technical Advisory Specification に従ってサービス・コンテンツと添付ファイルを圧縮してください。Rosettanet WebSphere Partner Gateway の適切なチャネルの下で、次のいずれかの値をルーティング・オブジェクト属性圧縮の値として選択します。

- なし
- ペイロード
- ペイロードおよび添付ファイル

選択された圧縮オプションのほかに、「**圧縮コンテンツ・タイプ**」および「**圧縮サイズ**」など、追加のフィルター基準属性も選択することができます。フィルター基準の使用により、圧縮するペイロードまたは添付ファイルを、添付ファイルのプールから選択することができます。「**圧縮コンテンツ・タイプ**」には、「すべて」か、コンマで区切られた有効な MIME タイプが入ります。基本圧縮で「**ペイロード**」オプションを選択した場合、「**圧縮コンテンツ・タイプ**」ルーティング・オブジェクト属性に指定された値に関係なく、ペイロードが圧縮されます。指定したコンテンツ・タイプに応じた圧縮の対象として、添付ファイルのみが選択されます。ルーティング・オブジェクト属性「**圧縮サイズ**」には、「すべて」か、有効なサイズ制限が入ります。有効なサイズ制限は、圧縮条件を満たす最小サイズを示します。

圧縮された Rosettanet 文書が送信されると、サービス・コンテンツと添付ファイルに対して S/MIME 解凍が実行されます。

## FTP スクリプト記述レシーバーおよび宛先用の FTP スクリプトの使用

FTP スクリプト・トランスポートを使用すると、付加価値通信網 (VAN) を含む任意の FTP サービスにデータを送信できます。FTP サーバー上の操作を制御するには、FTP コマンドを含むスクリプト・ファイルを使用します。

このスクリプトは、FTP スクリプト記述レシーバーまたは宛先の作成時に指定します。FTP スクリプトのプレースホルダーのレシーバーまたは宛先の作成時に入力する実際の値が、WebSphere Partner Gateway によって置き換えられます。

入力スクリプトに定義されている操作は、FTP サーバーに対するアクションに変換されます。入力スクリプトは、サポートされる FTP コマンドのグループで構成されます。これらのコマンドのパラメーターは変数の形をとる場合があります。その場合、実行時に値が入力されます。

FTP スクリプト記述レシーバーの FTP スクリプトの作成については、70 ページの『 FTP スクリプト記述レシーバーの設定』を参照してください。FTP スクリプト記述宛先の FTP スクリプトの作成については、244 ページの『FTP スクリプト記述宛先の設定』を参照してください。

## Data Interchange Services クライアントのマップの使用

EDI エンベロープ解除、変換、および検証を実行したり、ROD、XML、および EDI 間で変換を行うには、Data Interchange Services クライアントから関連したマップをインポートする必要があります。Data Interchange Services は、別個にインストールするプログラムです。これは、通常、WebSphere Partner Gateway が稼働するコンピューターとは別のコンピューターに常駐します。

Data Interchange Services のマッピング担当者は、特定の文書を変換および検証する方法を記述するマップを作成します。

マップを作成するには、ソース文書およびターゲット文書の定義が必要です。EDI の場合、ソース文書の定義は WDI によって提供されますが、ROD および XML の場合は DIS クライアントで作成する必要があります。EDI の場合は、.eif ファイル (標準ファイル) を DIS クライアントにインポートします。ROD の場合は、DIS クライアントを使用して標準を作成します。DTD/XSD をインポートし、XML 用の標準を作成します。標準および変換マップは別個にコンパイルできます。

例えば、バックエンド・アプリケーションが購入注文を作成し、これを変換して、標準の EDI X12 購入注文 (850) として外部パートナーに送信するとします。Data Interchange Services のマッピング担当者は、各フィールドまたはデータをプログラムから X12 形式に変換する方法の詳細を示すマップを作成します。次に、マップを WebSphere Partner Gateway に直接エクスポートします。または、マップをファイルにエクスポートして、コマンド・スクリプトを使用してインポートします。

Data Interchange Services クライアントからマップをインポートする方法について詳しくは、211 ページの『 手動によるマップのインポート』で説明します。

**注:** DIS クライアントには独自のデータベースがあります。DIS クライアントでマップの作成を完了したら、それを .EIF ファイルとしてエクスポートします。WebSphere Partner Gateway のコンソールから、この .EIF ファイルをインポートします。これは、WebSphere Partner Gateway データベースに情報を格納します。

## インストール後の構成作業の実行

WebSphere Partner Gateway のインストールが完了したら、この WebSphere Partner Gateway を構成する必要があります。一般にこの構成では、WebSphere Partner Gateway 管理コンソールでハブをセットアップする作業が行われます。取引コミュニティーの要件によっては、 WebSphere Partner Gateway コンポーネントをホストする WebSphere Application Server インフラストラクチャーを構成する必要もあります。これらの作業を以下に示します。それぞれの項目は、詳しい手順にリンクしています。

- 267 ページの『暗号の強度の変更』
- 269 ページの『クライアント認証による SSL の構成』

# 第 5 章 サーバーの始動およびコミュニティー・コンソールの表示

この章では、WebSphere Partner Gateway サーバーの始動方法とコミュニティー・コンソールの表示方法について説明します。以下のトピックを扱います。

- 『WebSphere Partner Gateway のコンポーネントの始動』
- 51 ページの『 コミュニティー・コンソールへのログイン』

WebSphere Application Server Network Deployment 管理コンソールからクラスターを始動する方法については、「*WebSphere Partner Gateway E/A 管理ガイド*」の『第 1 章 WebSphere Partner Gateway コンポーネント・アプリケーションの管理』を参照してください。

## WebSphere Partner Gateway のコンポーネントの始動

### このタスクについて

サーバーを始動するには、WebSphere Partner Gateway のコンソール、文書マネージャー、およびレシーバーの 3 つのコンポーネントをそれぞれ始動する必要があります。

シンプル・モードでは、すべての WebSphere Partner Gateway コンポーネントは、WebSphere Application Server の同じインスタンス上にインストールされます。すべてのコンポーネントは、スクリプトと WebSphere Application Server 管理コンソールを使用して開始および停止します。シンプル・モード・システムで WebSphere Partner Gateway コンポーネントを開始するには、次のスクリプトを実行します。

```
<INSTALL DIR>/bin/bcgStartServer.sh
```

シンプル・モード・システムで WebSphere Partner Gateway コンポーネントを停止するには、次のスクリプトを実行します。

```
<INSTALL DIR>/bin/bcgStopServer.sh
```

**注:** シンプル・モードでインストールするときには、サーバー名を指定する必要はありません。シンプル・モードでインストールする場合、サーバー名は常に server1 です。

**注: temp** ディレクトリーの容量が少ないときにインストーラーを実行して、製品を正常にインストールできなかった場合は、**temp** ディレクトリーの容量を増やしてから、製品をアンインストールし、再インストールしてください。

1. http://<computer name or IP address>:58080/console と入力すると、Web ブラウザーにウェルカム・ページが表示されます。以下の情報を使用して、WebSphere Partner Gateway にログインします。
   - 「**ユーザー名**」フィールドには次のように入力します。

     ```
     hubadmin
     ```

   - 「**パスワード**」フィールドには次のように入力します。

```
Pa55word
```

- 「**会社ログイン名**」フィールドには次のように入力します。

```
Operator
```

「**ログイン**」をクリックします。

2. はじめてログインしたときには、新規パスワードを作成する必要があります。新規パスワードを入力し、「**検証**」フィールドにもう一度新規パスワードを入力します。
3. 「**保存**」をクリックします。Community Console の初期入力ウィンドウが表示されます。

WebSphere Partner Gateway アプリケーションをインストールするときに、ファースト・ステップ・アプリケーションと、インストール検査テスト・アプリケーションがデフォルトでインストールされます。これは、WebSphere Partner Gateway の最後のコンポーネントがマシンにある間は、インストールされたままです。ファースト・ステップ・ページでは、各コンポーネントの検証テストを別個に実行するために、インストール済みコンポーネントのデータが設定されます。

ファースト・ステップ・ページは、<install_dir>/FirstSteps/bin フォルダーにあるコマンド **bcgFirstSteps. sh** を使用して起動できます。

コンソールのファースト・ステップ・ページから、すべてのインストール済みコンポーネントに対して開始オプションと停止オプションを切り替えることができます。例えば、ハブが実行中の場合、停止オプションがリストされます。実行中でない場合、開始オプションがリストされます。トポロジーに基づく、コンポーネントの開始オプションと停止オプションを以下に示します。

- Web Sphere Process Gateway の開始と停止は、シンプル・トポロジーとシンプル配布トポロジーの場合に使用できます。
- MAS の開始と停止は、完全配布トポロジーの場合に使用できます。
- Deployment Manager の開始と停止は、完全配布トポロジーの場合に使用できます。

  **注:** このオプションは、WebSphere Partner Gateway のインストーラーを使用して Deployment Manager がインストールされた場合にのみ使用できます。
- コンソール、レシーバー、およびルーターの開始と停止は、完全配布トポロジーの場合に使用できます。
- FTP 管理の開始と停止は、すべてのトポロジーで使用できます。

これらのオプションは、マシンにインストールされている場合に限り、示されたトポロジーで使用できます。サーバー・ログを確認して、アクションが正常終了したかどうかを確認する必要があります。状況を確認するために、コマンド行ウィンドウを使用することもできます。ファースト・ステップ・パネルで「**WPG の開始**」リンクをクリックすると、DOS コマンド・プロンプトで開始コマンドが発行されます。ファースト・ステップ・パネルでは、コマンドの正常 (または異常) 終了は通知されません。

インストール検査テスト (IVT) オプションが起動されると、マシンにインストールされている WebSphere Partner Gateway コンポーネントの妥当性が検査されます。この検証テストは、コマンド行から **LaunchIVT.sh** コマンドを使用することで起動

することもできます。このコマンドは、<installdir>/FirstSteps/ivt/bin フォルダーにあります。検査が完了すると、IVT では、すべてのインストール済み WebSphere Partner Gateway コンポーネントの詳細を含むレポートを生成します。また、この操作中に作成された一時ファイルを削除し、この操作中に開始されたサーバーとノードをすべて停止します。いずれかのコンポーネントが失敗したことを示すために、必要なログ・ファイルが <installdir>/FirstSteps/ivt/logs フォルダーに生成されます。

**注:** 配布トポロジーでは、異なるマシンにインストールされたコンポーネントは、IVT で検査されません。

デフォルトの暗号方式より強固な暗号方式の証明書をアップロードしようとすると、証明書のアップロードに失敗する場合があります。

## コミュニティー・コンソールへのログイン

### このタスクについて

このセクションでは、コミュニティー・コンソールの表示とログインの手順について説明します。推奨画面解像度は 1024x768 です。

**注:** WebSphere Partner Gateway コミュニティー・コンソールでは、セッション情報を維持するために Cookie サポートをオンにする必要があります。Cookie には個人情報は保管されず、ブラウザーがクローズすると有効期限が切れます。

1. Web ブラウザーを開き、以下の URL を入力して、コンソールを表示します。

   http://<*hostname*>.<*domain*>:58080/console (unsecure)

   https://<*hostname*>.<*domain*>:58443/console (secure)

   <*hostname*> および <*domain*> は、コミュニティー・コンソール・コンポーネントをホスティングするコンピューターの名前およびロケーションです。

   **注:** これらの URL では、デフォルト・ポート番号が使用されていることを想定しています。デフォルト・ポート番号を変更した場合は、指定した値でこのデフォルト番号を置き換えます。

ほとんどの場合、ハブ管理者から送られてくるユーザー名、初期パスワード、および会社ログイン名を使用して、コミュニティー・コンソールへログインします。この情報は次の手順で必要です。この情報を受け取っていない場合は、ハブ管理者にお問い合わせください。

コミュニティー・コンソールへのログイン方法 (この説明は外部パートナーと内部パートナーに適用):

1. 会社の「**ユーザー名**」を入力します。
2. 会社の「**パスワード**」を入力します。
3. 例えば「IBM」のような、「**会社ログイン名**」を入力します。
4. 「**ログイン**」をクリックします。はじめてログインする場合、新規パスワードを作成する必要があります。
5. 新規パスワードを入力し、「検証」テキスト・ボックスにもう一度新規パスワードを入力します。

6. 「**保存**」をクリックします。コンソールの初期入力画面が表示されます。

**注:** WebSphere Partner Gateway が LDAP を使用して構成される場合、「LDAP ユーザー名」および「パスワード」を入力する必要があります。「会社ログイン名」は、この情報の入力を要求するプロンプトが出されないので、このシナリオでは該当しません。また、システムはご使用のパスワードを変更するプロンプトも出しません。

# 第 6 章 コミュニティー・コンソールの構成

この章では、コミュニティー・コンソールを構成して、パートナーが表示できる内容、パートナーがコンソールにログインする方法、およびさまざまなコンソール・タスクに必要なパートナーのアクセス権を指定する方法について説明します。この章では以下のトピックを扱います。

- 『ロケール情報およびコンソールのブランドの指定』
- 55 ページの『パスワード・ポリシーの設定』
- 56 ページの『アクセス権の構成』
- 57 ページの『コンソールのタイムアウト値の設定』

WebSphere Partner Gateway により提供されたデフォルト設定を使用する場合は、これらのタスクを実行する必要はありません。

**注:** WebSphere Partner Gateway の構成変更を行う場合は、必ず、コミュニティー・コンソールにログインしたときと同じブラウザー・インスタンスを使用してください。複数のブラウザー・インスタンスを同時に使用すると、構成変更が無効になる可能性があります。

## ロケール情報およびコンソールのブランドの指定

### このタスクについて

デフォルトでは、コミュニティー・コンソールのページは、英語で表示されます。IBM は、内容の他言語への翻訳を、アップロード可能な一連のファイルとして提供しています。さまざまなロケールに対して IBM が提供するその他のコンソール項目は、バナー・グラフィックスです。オプションで、独自のロゴ・グラフィックスをアップロードできます。また、ページ上のテキストをフォーマットするためのカスタム・スタイル・シートをアップロードすることもできます。

このタスクは、「ロケールのアップロード」ページを使用して行います。「ロケールのアップロード」ページを表示するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**コンソール構成**」>「**ロケール構成**」をクリックします。
2. 「**作成**」をクリックします。
3. 「**ロケール**」リストからロケールを選択します。

コンソールに「ロケールのアップロード」ページが表示されます。

「ロケールのアップロード」ページから、以下のタスクを実行することができます。

- 固有のバナーまたはロゴ (あるいはその両方) をアップロードして、コンソールのブランドを設定する。
- IBM が提供するファイルをアップロードする。これにより、コンソール上のエレメントの内容をローカライズできます。

## コンソールのブランド設定

### このタスクについて

ブランド・イメージを変更して、コミュニティー・コンソールの外観をカスタマイズすることができます。コミュニティー・コンソールのブランド設定では、ヘッダーの背景と会社のロゴの 2 つのイメージがインポートされます。

- ヘッダーの背景は、コミュニティー・コンソールの最上部一帯に表示されます。
- 会社のロゴは、コミュニティー・コンソールの右上に表示されます。

これらのイメージは .JPG 形式のファイルで、コミュニティー・コンソールのウィンドウに収まるように一定の仕様に従っていなければなりません。

- バナーとロゴに必要な仕様を参照するには、「ロケールのアップロード」ウィンドウで「**イメージ指定**」をクリックします。
- ヘッダーやロゴのイメージのサンプルを参照するには、ページの「**サンプル・イメージ**」部分までスクロールダウンし、**sample_headerback.jpg** または **sample_logo.jpg** をクリックします。
- 独自のバナーやロゴを作成するためのテンプレートとして使用するサンプルをダウンロードするには、「**サンプル・イメージ (ヘッダーの背景および会社のロゴ)**」をクリックします。

バナーまたはロゴ (あるいはその両方) を作成したら、以下のステップを実行します。

1. カスタマイズされたバナーをアップロードするには、以下のいずれかのタスクを実行します。
   - 「**バナー**」フィールドに、ヘッダー/バナーに使用するイメージ・ファイルのパスと名前を入力します。
   - 「**参照**」をクリックし、バナーが入っている .jpg ファイルへ移動して、ファイルを選択します。
2. カスタマイズされたロゴをアップロードするには、以下のいずれかのステップを実行します。
   - 「**ロゴ**」フィールドに、会社のロゴに使用するファイルのパスと名前を入力します。
   - 「**参照**」をクリックし、ロゴが入っている .jpg ファイルへ移動して、ファイルを選択します。
3. 「**アップロード**」をクリックします。

**注:** 置き換えたヘッダーの背景や会社のロゴを有効にするには、コミュニティー・コンソールを再始動する必要があります。

## スタイル・シートの変更

### このタスクについて

デフォルトと異なるスタイル・シートを指定する場合 (例えば、異なるフォント・サイズまたは色にする場合) は、以下のタスクを実行します。

1. 以下のいずれかのタスクを実行します。

- 「**CSS**」フィールドに、カスタマイズされたスタイル・シートが入っているファイルのパスと名前を入力します。
- 「**参照**」をクリックし、スタイル・シートが入っているファイルへ移動して、ファイルを選択します。

2. 「**アップロード**」をクリックします。

## コンソール上のデータのローカライズ

### このタスクについて

リソース・バンドルまたは他のロケール・ファイルを IBM から受信した場合は、「ロケールのアップロード」ページを使用して、これらのファイルをアップロードできます。リソース・バンドルには、以下の情報が含まれています。

- 「**コンソール・ラベル**」- インターフェース上のすべてのテキストを表すテキスト・ストリングが含まれています。
- 「**イベント記述**」- イベントの詳細を表示する際に使用されるテキスト・ストリング (「重複する接続を作成しようとしました」など)が含まれています。
- 「**イベント名**」- イベント名を表すテキスト・ストリング (「接続は既に存在します」など) が含まれています。
- 「**EDI イベント記述**」- EDI イベントの詳細を表示する際に使用されるテキスト・ストリング (「FA の調整に失敗しました。EDI 確認通知内にトランザクションのアクティビティー ID がありません。」など) が含まれています。
- 「**EDI イベント名**」- EDI イベント名を表すテキスト・ストリング (「FA の調整に失敗しました」など) が含まれています。
- 「**拡張イベント・テキスト**」- イベントに関する補足情報 (イベントの原因やトラブルシューティング情報など) を示すテキスト・ストリングが含まれています。

リソース・バンドルまたは他のロケール・ファイルをアップロードするには、以下のステップを実行します。

1. リソース・バンドルまたはファイルごとに、以下のいずれかのタスクを実行します。
   - ファイルのパスおよび名前を入力します。
   - 「**参照**」をクリックし、使用するファイルへ移動して、ファイルを選択します。
2. ファイルのアップロードが終了したら、「**アップロード**」をクリックします。

# パスワード・ポリシーの設定

システム設定されたデフォルト値以外の値を使用したい場合は、ハブ・コミュニティーのパスワード・ポリシーを設定します。パスワード・ポリシーは、コミュニティー・コンソールにログインするすべてのユーザーに適用されます。

パスワード・ポリシーの以下のエレメントを変更することができます。

- 「最小の長さ」- パートナーがパスワードに最低限使用しなければならない文字数を表します。デフォルトは 8 文字です。
- 「有効期限」- パスワードが期限切れになるまでの日数を表します。デフォルトは 30 日です。

- 「固有性」- ヒストリー・ファイルに保持されるパスワードの数を指定します。パートナーは、ヒストリー・ファイル内にある旧パスワードを使用できません。デフォルトのパスワード数は 10 です。
- 「特殊文字」- これを選択すると、以下のタイプの特殊文字のうち、少なくとも 3 つがパスワードに含まれていなければならないことを示します。
  - 大文字
  - 小文字
  - 数字
  - 特殊文字

  パスワードが英字 (ASCII) で構成される場合は、この設定をすることで、より厳しいセキュリティー要件を設けることができます。デフォルト設定はオフです。パスワードが各国文字で構成される場合は、「特殊文字」をオフにしておくことをお勧めします。英語以外の言語の文字セットには、4 つの文字タイプのうち必要となる 3 つが含まれていない場合もあります。

  システムでサポートされている特殊文字は、「#」、「@」、「$」、「&」、「+」です。
- 「名前の差異を検査」- これを選択すると、ユーザーのログイン名や氏名から推測されやすいパスワードを使用できなくなります。このフィールドは、デフォルトで選択されています。

デフォルト値を変更するには、以下のステップを実行します。

1. **「ハブ管理」>「コンソール構成」>「パスワード・ポリシー」**をクリックします。「パスワード・ポリシー」ページが表示されます。
2. **「編集」**アイコンをクリックします。
3. 任意のデフォルト値を、パスワード・ポリシーに使用したい値に変更します。
4. **「保存」**をクリックします。

# アクセス権の構成

アクセス権とは、ユーザーがコンソールの各種モジュールにアクセスするために必要な権限です。

## ユーザーへのアクセス権の付与方法

アクセス権を構成する前に、個々のユーザーへのアクセス権の付与方法について理解しておくと役立ちます。ハブ・コミュニティー内の 3 つのタイプのエンティティー (ハブ管理者、内部パートナー、および外部パートナー) は、いずれも管理ユーザーを持つことができます。内部パートナーまたはパートナーを作成する場合、そのエンティティーの管理ユーザーも作成できます。

**注:** Hub オペレーター・パートナーの場合は、インストール時に Admin ユーザーと hubadmin ユーザーという 2 つの管理ユーザーが自動的に作成されます。

パートナーを作成する場合 (25 ページの『パートナー・プロファイルの作成』を参照) は、パートナーのログイン情報 (ログインに使用する名前やパスワードなど) を指定します。パートナーは、ログインした後に、組織内の追加ユーザーを作成しま

す。また、パートナーは、グループを作成して、ユーザーをそのグループに割り当てます。例えば、文書ボリュームをモニターするユーザーのグループが組織で必要となる場合があります。パートナーは、ボリューム・グループを作成して、このグループにユーザーを割り当てます。

**注:** ハブ管理者は、パートナーに対してユーザーおよびグループを定義することもできます。

次に、パートナーの管理ユーザーが、ユーザーのグループにアクセス権を割り当てます。例えば、管理ユーザーは、ボリューム・グループが文書ボリューム・レポートと文書分析レポートのみを参照するようにすることができます。また、管理ユーザーは、「グループの詳細」ページを使用して、ボリューム・グループの文書レポート・モジュールを使用可能に、その他のモジュールを使用不可にすることができます。

ハブ管理者が「アクセス権」ページで行った設定によって、「グループの詳細」ページにモジュールがリストされるかどうかが決定されます。

一部のモジュールはハブ・コミュニティーの特定のメンバー (hubadmin のようなハブ管理者など) に制限されています。したがって、このようなモジュールをパートナーに対して使用可能に設定しても、モジュールはパートナーの「グループの詳細」ページには表示されません。

## アクセス権の使用可能化と使用不可化

### このタスクについて

「アクセス権リスト」ページからアクセス権を使用可能または使用不可することにより、ユーザーのグループに割り当てられるアクセス権を決定することができます。ただし、新しいアクセス権を定義することはできません。

デフォルトのアクセス権を変更するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**コンソール構成**」>「**アクセス権**」をクリックします。「アクセス権リスト」が表示されます。
2. デフォルトを変更したい場合は、以下のステップを実行します。
   a. 現在の設定 (「**有効**」または「**無効**」) をクリックして、設定を変更します。
   b. 変更を確認するプロンプトが出されたら、「**OK**」をクリックします。

# コンソールのタイムアウト値の設定

デフォルトのセッション・タイムアウト値である 30 分は、以下のシナリオでは受け入れられない場合があります。

- セキュアな環境のユーザーは、セキュリティーを確保するために、より短いセッション・タイムアウト期間を必要とする場合があります。これは、マシンを離れるのに、コンソールからログオフすることを忘れたときにもあてはまります。
- アクセシビリティーの理由により、通常のユーザーより応答が遅い場合、より長いセッション・タイムアウト期間を必要とする場合があります。

WebSphere Partner Gateway コンソールのタイムアウト値を設定するには、以下のステップを実行します。

1. WebSphere Application Server コンソールを開きます。
2. 「**サーバー**」>「**アプリケーション・サーバー**」>「**bcgserver**」>「**Web コンテナー設定**」>「**Web コンテナー**」>「**セッション管理**」の順にクリックします。
3. 「**セッション管理**」ページで、「**タイムアウトの設定**」セクションの「**タイムアウトの設定**」を選択します。
4. 分単位で値を入力します。デフォルトは、30 分です。
5. 「**適用**」をクリックします。

# 第 7 章 レシーバーの定義

この章では、WebSphere Partner Gateway にレシーバーを設定する方法について説明します。以下のトピックを扱います。



**注:** WebSphere Partner Gateway の構成変更を行う場合は、必ず、コミュニティー・コンソールにログインしたときと同じブラウザー・インスタンスを使用してください。複数のブラウザー・インスタンスを同時に使用すると、構成変更が無効になる可能性があります。

## レシーバーの概要

12 ページの『文書処理の概要』に記載されているように、*レシーバー* は特定のトランスポートからのインバウンド文書を受信します。レシーバー・インスタンスは特定のデプロイメント用に構成されます。

ハブ上のレシーバーで受信される文書は、外部パートナーから送信される (最終的には内部パートナーに配信される) 場合もあれば、内部パートナーのバックエンド・アプリケーションから送信される (最終的には外部パートナーに配信される) 場合もあります。

60 ページの図 16 に、4 つのレシーバーがセットアップされた WebSphere Partner Gateway サーバーを示します。レシーバーのうち 2 つ (HTTP/S および FTP/S) はパートナーから発信される文書用です。これらの 2 つのレシーバーは HTTP URI および FTP ディレクトリーを表します。パートナーが文書をユーザーに送信する場所を指定するために、これらのレシーバーに関する情報をパートナーに提供します。その他の 2 つのレシーバー (JMS およびファイル・ディレクトリー) は、内部パートナーのバックエンド・アプリケーションから発信される文書用です。これらのレシーバーはキューおよびディレクトリーを表します。

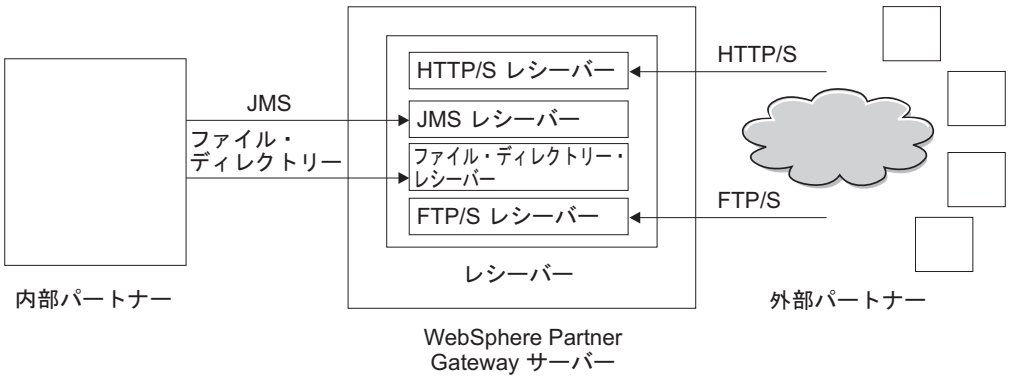



*図 16. トランスポートおよび関連付けられたレシーバー*

ハブへの文書の送信に使用するトランスポートのタイプごとに、少なくとも 1 つのレシーバーを設定する必要があります。例えば、HTTP または HTTPS トランスポートで送信される文書を受信するには、HTTP レシーバーを設定します。外部パートナーが FTP で文書を送信する場合は、FTP レシーバーを設定します。

受信されるいくつかの文書に特殊な要件がある場合、特定のトランスポート用に複数のレシーバーをセットアップする必要があります。この場合、パートナーにこれらの要件を通知し、正しいレシーバー処理を実行できるようにそうした文書を特定のアドレスに送信するよう依頼します。

レシーバー・コンポーネントは、レシーバーの 1 つにメッセージが着信した時期を検出します。一部のレシーバーは、新規メッセージが着信したかどうかを判別するためにトランスポートを定期的に、またはスケジュールに従ってポーリングし、メッセージを検出します。ポーリング・ベースの WebSphere Partner Gateway レシーバーは、JMS、FTP、SMTP、File、および FTP スクリプト記述です。HTTP/S レシーバーはコールバック・ベースです。これは、メッセージが着信すると、トランスポートから通知を受信することを意味します。ユーザー定義のトランスポートは、ポーリング・ベースまたはコールバック・ベースのいずれかに設定できます。

## ユーザー定義ハンドラーのアップロード

### このタスクについて

レシーバーの構成ポイントを変更するには、レシーバーのハンドラーを指定します。WebSphere Partner Gateway 提供のハンドラー、またはユーザー定義のハンドラーを使用できます。ここでは、ユーザー定義のハンドラーをアップロードする方法について説明します。このセクションでは、ユーザー定義のハンドラーの場合のみ使用します。WebSphere Partner Gateway 提供のハンドラーは、既に使用可能です。

ハンドラーをアップロードするには、以下のステップを実行します。

1. メインメニューから、「**ハブ管理**」>「**ハブ構成**」>「**ハンドラー**」をクリックします。
2. 「**レシーバー**」をクリックします。

レシーバーに対して現在定義されているハンドラーのリストが表示されます。WebSphere Partner Gateway から提供されているハンドラーのプロバイダー ID は「**製品**」となっています。

3. 「ハンドラー・リスト」ページで、「**インポート**」をクリックします。
4. 「ハンドラーのインポート」ページで、目的のハンドラーが記述されている XML ファイルへのパスを指定するか、または「**参照**」を使用してその XML ファイルを検索します。

ハンドラーがアップロードされたら、そのハンドラーを使用して、レシーバーの構成ポイントをカスタマイズすることができます。

## 汎用前処理ハンドラー

前処理構成ハンドラーは、すべてのタイプのレシーバーで使用できますが、SMTP レシーバーには適用されません。以下の表は、汎用前処理ハンドラーに設定できる属性について説明したものです。

*表 2. 汎用前処理ハンドラー*

| 属性 | 説明 |
|---|---|
| 送信元パッケージ名 (From Packaging Name) | この属性は、文書と関連付けられたパッケージ化を示します。この値は、文書定義で指定されたパッケージ化と一致している必要があります。 |
| 送信元パッケージ・バージョン (From Packaging Version) | この属性は、「**送信元パッケージ名 (From Packaging Name)**」に指定されているパッケージ化のバージョンを示します。例えば、文書のパッケージ化が「なし (None)」の場合、この値は N/A となります。 |
| 送信元プロトコル名 (From Protocol Name) | この属性は、文書と関連付けられたプロトコルを示します。この値は、文書定義で指定されたプロトコルと一致している必要があります。 |
| 送信元プロトコル・バージョン (From Protocol Version) | この属性は、「**送信元プロトコル名 (From Protocol Name)**」に指定されているプロトコルのバージョンを示します。 |
| 送信元プロセス・コード (From Process Code) | この属性は、この文書と関連付けられたプロセス (文書タイプ) を示します。この値は、文書定義内の文書タイプと一致している必要があります。 |
| 送信元プロセス・バージョン (From Process Version) | この属性は、「**送信元プロセス・コード (From Process Code)**」に指定されているプロセスのバージョンを示します。 |
| METADICTIONARY | この属性は、文書定義が関連付けられているディクショナリーの名前を示します。この値は、「送信元プロトコル名 (From Protocol Name)」フィールドに指定されたプロトコルと一致していなければなりません。 |
| METADOCUMENT | この属性は、この文書と関連付けられた文書定義名を示します。この値は、「送信元プロセス・コード (From Process Code)」フィールドに指定されたプロセスと一致していなければなりません。 |

*表 2. 汎用前処理ハンドラー (続き)*

| 属性 | 説明 |
|---|---|
| METASYNTAX | この属性は、このレシーバーで処理される文書の構文を示します。許可される値は、ediIchg (EDI 交換) / xml / rod (フラット・ファイル) です。 |
| ENCODING | この属性は、文書の文字エンコードを示します。デフォルト値は ASCII です。 |
| BCG_BATCHDOCS | 文書をバッチで処理したい場合は、この属性を **ON** に設定します。 |
| SenderId、ReceiverId | この属性は、受信側 ID、送信側 ID を示します。これらの ID はプロファイルに構成されているパートナーのビジネス ID です。 |

## グローバルなトランスポート値の設定

### このタスクについて

FTP スクリプト記述受信側に適用されるグローバル・トランスポート属性を設定します。FTP スクリプト記述受信側を定義しない場合、このセクションの記述は必要ありません。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックして、「レシーバー・リスト」を表示します。
2. 「**グローバル・トランスポート属性**」リンクをクリックします。
3. デフォルト値がご使用の構成に対して適切である場合は、「**キャンセル**」をクリックします。それ以外の場合は、このセクションの残りのステップを継続します。
4. 「**カテゴリー別にリストされたグローバル属性**」の横にある「**編集**」アイコンをクリックします。
5. 「**FTP スクリプト・トランスポート**」および「**FTP スクリプト記述: 受信側および宛先**」値を検討し、必要に応じて変更します。

   FTP スクリプト・トランスポートではロック・メカニズムを使用しており、複数の FTP スクリプト記述インスタンスが同じレシーバーに同時にアクセスすることができないようになっています。文書の送信準備を終えた FTP スクリプト・トランスポートには、このロックが必要です。ロックを取得するまでにレシーバー・インスタンスが待機する時間や、ロックが使用中の場合にロックを取得するために試行する回数などに、デフォルト値が設定されています。これらのデフォルト値を使用することも、変更することもできます。1 つ以上の値を変更するには、新しい値を入力します。以下の値を変更できます。

   - 「**FTP スクリプト・トランスポート**」値
     - 「**ロック再試行カウント**」。ロックが現在使用されている場合にレシーバーがロックの取得を試みる回数を指定します。デフォルトは 3 です。
     - 「**ロック再試行間隔 (秒)**」。ロックの取得を試みてから次に試みるまでの経過時間を指定します。デフォルトは 260 秒です。
   - 「**FTP スクリプト記述: 受信側および宛先**」値

– 「**最大ロック時間 (秒)**」。レシーバーがロックを保持できる時間を指定します。デフォルト値は 240 秒です。
– 「**最大キュー存続期間 (秒)**」。レシーバーがロックを取得するためにキューに待機する期間を指定します。デフォルトは 740 秒です。

6. 「**保存**」をクリックします。

---

# HTTP/S レシーバーの設定

## このタスクについて

レシーバー・コンポーネントには、事前定義された bcgreceiver サーブレットがあります。これは HTTP/S POST メッセージの受信に使用されます。サーブレットが受信したメッセージにアクセスするには、HTTP レシーバーを 1 つ以上作成します。

HTTP/S レシーバーに必要な情報を指定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックして、「レシーバー・リスト」ページを表示します。
2. 「レシーバー・リスト」ページで、「**レシーバーの作成**」をクリックします。

## レシーバーの詳細

### このタスクについて

「**レシーバーの詳細**」セクションで、以下のステップを実行します。

1. レシーバーの名前を入力します。例えば、HttpReceiver1 というレシーバー名を付けます。このフィールドは必須です。ここで入力した名前は「レシーバー」リストに表示されます。
2. (オプション) レシーバーの状況を指定します。デフォルトは「**有効**」です。使用可能状態のレシーバーは、文書を受信することができます。無効状態のレシーバーは、文書を受信できません。
3. (オプション) レシーバーの説明を入力します。
4. 「**トランスポート**」リストから、「**SFTP**」を選択します。

## レシーバーの構成

### このタスクについて

「**レシーバーの構成**」セクションで、以下のステップを実行します。

1. (オプション) 動作モードを指定します。動作モードによって、送信の性質が定義されます。例えば、文書交換を製品に書き込む前にテストする場合は、「**テスト**」を指定します。デフォルトは「**実動**」です。
2. HTTP/S レシーバーの URI を入力します。この名前は **bcgreceiver** で始める必要があります。例えば、/bcgreceiver/Receiver と入力します。これにより、HTTP/S を介してサーバーに到着した文書は、/bcgreceiver/Receiver で受信されます。
3. ヘッダー属性を使用して HTTP/S レシーバーを認証するには、「**基本認証の使用可能化 (Enable basic authentication)**」フラグを true に設定してください。デフォルト値は false です。

4. 「**HTTP/S トランスポート**」値を検討し、必要に応じて変更します。以下の値を変更できます。
   - 「**最大同期タイムアウト (秒)**」。同期接続を開いたまま保持できる秒数を指定します。デフォルトは 300 秒です。
   - 「**最大同時同期接続数**」。システムで使用できる同期接続数を指定します。デフォルトは、100 個の接続です。

**注:** 「**同期ルーティング**」の値を編集することができます。

## ハンドラー

分割が必要な複数の EDI 交換または XML や ROD 文書を含むファイルを受信した場合は、前処理構成ポイントに適切なスプリッター・ハンドラーを構成します。

同期交換を通して特定のタイプのビジネス文書 (RosettaNet、cXML、SOAP、および AS2)を送受信する場合は、同期検査構成ポイントで関連するプロトコルのハンドラーを指定します。

レシーバーの後処理構成ポイントを変更することもできます。

構成ポイントを変更する場合は、78 ページの『構成ポイントの変更』に進みます。それ以外の場合は、「**保存**」をクリックします。

---

# FTP レシーバーの設定

### このタスクについて

FTP レシーバーは設定された間隔で FTP サーバーをポーリングし、新規文書を検索します。

FTP レシーバーに必要な情報を指定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックして、「レシーバー・リスト」ページを表示します。
2. 「レシーバー・リスト」ページで、「**レシーバーの作成**」をクリックします。

### タスクの結果

## レシーバーの詳細

### このタスクについて

「**レシーバーの詳細**」セクションで、以下のステップを実行します。

1. レシーバーの名前を入力します。例えば、FTPReceiver1 というレシーバー名を付けます。このフィールドは必須です。ここで入力した名前は「レシーバー」リストに表示されます。
2. (オプション) レシーバーの状況を指定します。デフォルトは「**有効**」です。使用可能状態のレシーバーは、文書を受信することができます。無効状態のレシーバーは、文書を受信できません。
3. (オプション) レシーバーの説明を入力します。
4. 「**トランスポート**」リストから、「**FTP ディレクトリー**」を選択します。

## レシーバーの構成

### このタスクについて

「**レシーバーの構成**」セクションで、以下のステップを実行します。

1. 「**FTP ルート・ディレクトリー**」フィールドに、FTP サーバーのルート・ディレクトリーを入力します。文書マネージャーは FTP ルート・ディレクトリー内でパートナーのサブディレクトリーを自動的にポーリングして、文書ルーティングを行います。このフィールドは必須です。FTP サーバーのディレクトリーの設定については、35 ページの『文書を受信する FTP サーバーの構成』を参照してください。

   **注:** ルート FTP ディレクトリーで終了するディレクトリー・パスを入力します。パートナーのサブディレクトリーは含めないでください。

2. (オプション) 「**ファイル未変更間隔**」に、ファイル・サイズが未変更の状態を保つ時間 (秒数) を指定します。この時間を過ぎると、文書マネージャーが処理する文書を取り出します。この未変更間隔期間により、文書マネージャーが文書を取得する場合に、文書の送信が完了し、転送されていない状態が確保されます。デフォルト値は 3 秒です。
3. (オプション) 「**スレッド数**」に、文書マネージャーが同時に処理できる文書の数を指定します。デフォルト値の 1 を使用することをお勧めします。
4. (オプション) 「**除外するファイル拡張子**」に、文書マネージャーが FTP ディレクトリー内で文書を検出した場合に無視する (処理対象から除外する) 文書のタイプを指定します。例えば、文書マネージャーがスプレッドシート・ファイルを無視するようにしたい場合は、そのファイルの拡張子を入力します。拡張子を入力したら、「**追加**」をクリックします。無視するファイル拡張子リストに拡張子が追加されます。デフォルトでは、どのファイル・タイプも除外されません。

   **注:** ファイル名拡張子の前にドットを使用しないでください (.exe または .txt など)。ファイル拡張子を示す文字列のみを使用します。

## ハンドラー

分割が必要な複数の EDI 交換または XML や ROD 文書を含むファイルを受信した場合は、前処理構成ポイントに適切なスプリッター・ハンドラーを構成します。

前処理構成ポイントを変更する場合は、78 ページの『構成ポイントの変更』に進みます。それ以外の場合は、「**保存**」をクリックします。

# SMTP (POP3) レシーバーの設定

### このタスクについて

SMTP レシーバーは (指定されたスケジュールに従って) POP3 メール・サーバーをポーリングして、新規文書を検索します。

SMTP (POP3) レシーバーに必要な情報を指定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックして、「レシーバー・リスト」ページを表示します。

2. 「レシーバー・リスト」ページで、「**レシーバーの作成**」をクリックします。

### タスクの結果

## レシーバーの詳細

### このタスクについて

「**レシーバーの詳細**」セクションで、以下のステップを実行します。

1. レシーバーの名前を入力します。例えば、POP3Receiver1 というレシーバー名を付けます。このフィールドは必須です。ここで入力した名前は「レシーバー」リストに表示されます。
2. (オプション) レシーバーの状況を指定します。デフォルトは「**有効**」です。使用可能状態のレシーバーは、文書を受信することができます。無効状態のレシーバーは、文書を受信できません。
3. (オプション) レシーバーの説明を入力します。
4. 「**トランスポート**」リストから、「**POP3**」を選択します。

## レシーバーの構成

### このタスクについて

ページの「**レシーバーの構成**」セクションで、以下のステップを実行します。

1. (オプション) 動作モードを指定します。動作モードによって、送信の性質が定義されます。例えば、文書交換を製品に書き込む前にテストする場合は、「**テスト**」を指定します。デフォルトは「**実動**」です。
2. メールを配信する POP3 サーバーの場所を入力します。例えば、IP アドレスを入力します。
3. (オプション) ポート番号を入力します。何も入力しなかった場合は、値 110 が使用されます。
4. ユーザー ID とパスワードが必要な場合は、メール・サーバーへのアクセスに必要なユーザー ID とパスワードを入力します。
5. 「**スレッド数**」は読み取り専用モードです。これは、文書マネージャーが同時に処理できる文書の数を示します。

## スケジュール

### このタスクについて

ページの「**スケジュール**」セクションで、以下のステップを実行します。

1. 「**間隔ベースのスケジューリング**」または「**カレンダー・ベースのスケジューリング**」を選択します。
2. 以下のいずれかのステップを実行します。
   - 「**間隔ベースのスケジューリング**」を選択した場合は、POP3 サーバーを再びポーリングするまでの経過時間を秒数で選択します (またはデフォルト値を受け入れます)。デフォルト値を受け入れた場合、POP3 サーバーは 5 秒おきにポーリングされます。

- 「**カレンダー・ベースのスケジューリング**」を選択した場合は、スケジューリングのタイプ (「**日次スケジュール**」、「**週次スケジュール**」、または「**カスタム・スケジュール**」) を選択します。
  - 「**日次スケジュール**」を選択した場合は、POP3 サーバーがポーリングされる時刻 (時分) を選択します。
  - 「**週次スケジュール**」を選択した場合は、時刻のほかに曜日を 1 つ以上選択します。
  - 「**カスタム・スケジュール**」を選択した場合は、まず時刻を選択し、次に週および月について「**範囲**」または「**選択できる日**」を選択します。「**範囲**」では、開始日と終了日を指定します。(例えば、平日の特定の時刻にのみサーバーをポーリングする場合は、「**月**」 および「**金**」をクリックしてください。) 「**選択できる日**」では、週および月の特定の日付を選択します。

### ハンドラー

分割が必要な複数の EDI 交換または XML や ROD 文書を含むファイルを受信した場合は、前処理構成ポイントに適切なスプリッター・ハンドラーを構成します。

前処理構成ポイントを変更する場合は、78 ページの『構成ポイントの変更』に進みます。それ以外の場合は、「**保存**」をクリックします。

## JMS レシーバーの設定

### このタスクについて

JMS レシーバーは (指定されたスケジュールに従って) JMS キューをポーリングして、新規文書を検索します。

JMS レシーバーに必要な情報を指定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックして、「レシーバー・リスト」ページを表示します。
2. 「レシーバー・リスト」ページで、「**レシーバーの作成**」をクリックします。

**注:** 必要な WebSphere MQ JAR ファイルを WebSphere Partner Gateway で表示できるようにするためのランタイム・ライブラリーの構成については、42 ページの『ランタイム・ライブラリーの構成』を参照してください。

### レシーバーの詳細

### このタスクについて

「**レシーバーの詳細**」セクションで、以下のステップを実行します。

1. レシーバーの名前を入力します。例えば、JMSReceiver1 というレシーバー名を付けます。このフィールドは必須です。ここで入力した名前は「レシーバー」リストに表示されます。
2. (オプション) レシーバーの状況を指定します。デフォルトは「**有効**」です。使用可能状態のレシーバーは、文書を受信することができます。無効状態のレシーバーは、文書を受信できません。

3. (オプション) レシーバーの説明を入力します。
4. 「**トランスポート**」リストから、「**JMS**」を選択します。

## レシーバーの構成

### このタスクについて

ページの「**レシーバーの構成**」セクションで、以下のステップを実行します。

1. (オプション) **操作タイプ**を指定します。操作タイプによって、送信の性質が定義されます。例えば、文書交換を製品に書き込む前にテストする場合は、「**テスト**」を指定します。デフォルトは「*実動*」です。
2. **JMS プロバイダーの URL** を入力します。これは、WebSphere Partner Gateway を JMS 対応として構成した際に入力した値 (バインディング・ファイルのファイル・システム・パス) と一致していなければなりません (ステップ 5 (40 ページ))。また、JMS コンテキストのサブフォルダーを JMS プロバイダー URL の一部として指定することもできます。

   例えば、JMS コンテキストを指定しない場合、`c:/temp/JMS` と入力します。JMS コンテキストを指定する場合は、`c:/temp/JMS/JMS` と入力します。
3. **ユーザー ID** と**パスワード**が必要な場合は、JMS キューへのアクセスに必要なユーザー ID とパスワードを入力します。
4. **JMS キュー名**の値を入力します。このフィールドは必須です。この名前は、バインディング・ファイルの作成時 (ステップ 4 (42 ページ)) に `define q` コマンドで指定した名前と一致している必要があります。

   ステップ 2 で JMS コンテキストのサブフォルダーを入力した場合、ここではキュー名だけを入力します (例えば、`inQ`)。JMS プロバイダー URL で JMS コンテキストのサブフォルダーを入力しなかった場合は、ファクトリー名の前にサブフォルダーを指定します (例えば、`JMS/inQ`)。
5. **JMS ファクトリー名**の値を入力します。このフィールドは必須です。この名前は、バインディング・ファイルの作成時 (ステップ 4 (42 ページ)) に `define qcf` コマンドで指定した名前と一致している必要があります。

   ステップ 2 で JMS コンテキストのサブフォルダーを入力した場合、ここではファクトリー名だけを入力します (例えば、`Hub`)。JMS プロバイダー URL で JMS コンテキストのサブフォルダーを入力しなかった場合は、ファクトリー名の前にサブフォルダーを指定します (例えば、`JMS/Hub`)。
6. (オプション) **プロバイダー URL パッケージ**を入力します。
7. 「**JNDI ファクトリー名**」を入力します。このフィールドは必須です。 39 ページの『JMS トランスポート・プロトコル用のハブの構成』の説明に従い独自の WebSphere MQ の JMS 構成を設定した場合、使用する値は、おそらく com.sun.jndi.fscontext.RefFSContextFactory です。
8. 「**JMS ユーザー名**」 および 「**JMS パスワード**」を入力します。
9. (オプション) 「**タイムアウト**」に、レシーバーが文書を調べるために JMS キューをモニターする時間 (秒数) を指定します。このフィールドはオプションです。

10. (オプション) 「**スレッド数**」に、文書マネージャーが同時に処理する文書の数を指定します。デフォルト値の 1 を使用することをお勧めします。

例えば、 39 ページの『JMS トランスポート・プロトコル用のハブの構成』の JMS 構成例と一致するように JMS レシーバーを設定したい場合は、以下のようにします。

1. 「**レシーバー名**」ボックスに、値 **JMSReceiver** を入力します。
2. 次のいずれかの値を「**JMS プロバイダー URL**」ボックスに入力します。
   - Windows の場合: **file:///C:/TEMP/JMS/JMS**
   - UNIX の場合: **file:///opt/temp**
3. 「**JMS キュー名**」ボックスに、値 **inQ** を入力します。
4. 「**JMS ファクトリー名**」ボックスに、値 **Hub** を入力します。

### ハンドラー

分割が必要な複数の EDI 交換または XML や ROD 文書を含むファイルを受信した場合は、前処理構成ポイントに適切なスプリッター・ハンドラーを構成します。

このレシーバーの構成ポイントを変更する場合は、 78 ページの『構成ポイントの変更』に進みます。それ以外の場合は、「**保管**」をクリックします。

## ファイル・ディレクトリー・レシーバーの設定

### このタスクについて

ファイル・ディレクトリー・レシーバーは、設定された間隔でディレクトリーをポーリングし、新規文書を検索します。

ファイル・ディレクトリー・レシーバーに必要な情報を指定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックして、「レシーバー・リスト」ページを表示します。
2. 「レシーバー・リスト」ページで、「**レシーバーの作成**」をクリックします。

### レシーバーの詳細

### このタスクについて

「**レシーバーの詳細**」セクションで、以下のステップを実行します。

1. レシーバーの名前を入力します。例えば、FileReceiver1 というレシーバー名を付けます。このフィールドは必須です。ここで入力した名前は「レシーバー」リストに表示されます。
2. (オプション) レシーバーの状況を指定します。デフォルトは「**有効**」です。使用可能状態のレシーバーは、文書を受信することができます。無効状態のレシーバーは、文書を受信できません。
3. (オプション) レシーバーの説明を入力します。
4. 「**トランスポート**」リストから、「**ファイル・ディレクトリー**」を選択します。

## レシーバーの構成

### このタスクについて

ページの「**レシーバーの構成**」セクションで、以下のステップを実行します。

1. 「**文書ルート・パス**」に、文書を受信する場所を指定します。

   ルート・ディレクトリーが存在しない場合は、レシーバーのために新規ディレクトリーが作成されます。しかし、ルート・ディレクトリーが既に存在する場合は、レシーバーによって既存のディレクトリーが使用されます。このことは、WebSphere Partner Gateway 6.1.1 以降に適用されます。

   `file://` プレフィックスはオプションです。

   例えば、ディレクトリー `c:¥wpg¥receivers¥file1` を文書ルート・パスとして指定する場合は、`c:¥wpg¥receivers¥file1` または `file://c:¥wpg¥receivers¥file1` を入力してください。
2. (オプション) 「**ポーリング間隔**」に、新しい文書を調べるためにディレクトリーをポーリングする間隔を指定します。何も入力しなかった場合は、5 秒間隔でディレクトリーがポーリングされます。
3. (オプション) 「**ファイル未変更間隔**」に、ファイル・サイズが未変更の状態を保つ時間 (秒数) を指定します。この時間を過ぎると、文書マネージャーが処理する文書を取り出します。この未変更間隔期間により、文書マネージャーが文書を取得する場合に、文書の送信が完了し、転送されていない状態が確保されます。デフォルト値は 3 秒です。
4. (オプション) 「**スレッド数**」に、文書マネージャーが同時に処理できる文書の数を指定します。デフォルト値の 1 を使用することをお勧めします。

## ハンドラー

分割が必要な複数の EDI 交換または XML や ROD 文書を含むファイルを受信した場合は、前処理構成ポイントに適切なスプリッター・ハンドラーを構成します。

前処理構成ポイントを変更する場合は、78 ページの『構成ポイントの変更』に進みます。それ以外の場合は、「**保管**」をクリックします。

---

# FTP スクリプト記述レシーバーの設定

### このタスクについて

FTP スクリプト記述レシーバーは、設定されたスケジュールに従って動作するポーリング・レシーバーです。FTP スクリプト記述レシーバーの動作は、FTP コマンド・スクリプトで制御します。

ご使用の FTP サーバーのディレクトリーをポーリングする FTP レシーバーと異なり、FTP スクリプト記述レシーバーは別のサーバー (VAN など) のディレクトリーをポーリングします。

**注:**

1. データベースがダウンし、「ロック・ユーザー」が「はい」に設定されている場合、FTP スクリプト記述レシーバーはデータベースからロックを取得しないため、作動しないことがあります。
2. パートナーは、FTP スクリプト記述レシーバーが受信できるように、確実に文書を完成させる必要があります。このためには、文書が完成するまで FTP サーバーでこの文書をロックするか、またはパートナーが文書を一時ディレクトリーに書き込み、完成した文書を FTP スクリプト記述レシーバーが使用するディレクトリーに移動します。

## FTP スクリプトの作成

### このタスクについて

FTP サーバーには、受け入れられるコマンドに関する具体的な要件を保持できます。FTP スクリプト記述レシーバーを使用するには、接続先の FTP サーバーで必要な FTP コマンドをすべて含むファイルを作成します。(FTP サーバー管理者からこの情報を入手する必要があります。)

1. レシーバーに対して実行するアクションを指定したスクリプトを作成します。次のスクリプトは、(名前およびパスワードを指定して) 指定された FTP サーバーに接続し、FTP サーバー上の指定ディレクトリーに移動して、このディレクトリー内のすべてのファイルを受信する例です。

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
cd %BCGOPTION1%
mget *
quit
```

   FTP スクリプト記述レシーバーの特定のインスタンスを作成するとき入力した値に応じてレシーバーを処理する場合は、プレースホルダー (%BCGSERVERIP% など) が置き換えられます。この例の %BCGOPTION% は、cd コマンド内のディレクトリー名です。スクリプト・パラメーターおよび関連する FTP スクリプト記述レシーバー・フィールドを 表 3 に示します。

*表 3. スクリプト・パラメーターと FTP スクリプト記述レシーバーのフィールド項目との対応*

| スクリプト・パラメーター | FTP スクリプト記述レシーバーのフィールド項目 |
|---|---|
| %BCGSERVERIP% | サーバー IP |
| %BCGUSERID% | ユーザー ID |
| %BCGPASSWORD% | パスワード |
| %BCGOPTIONx% | **ユーザー定義属性の下のオプション** *x* |

2. ファイルを保存します。

## FTP スクリプト記述コマンド

スクリプトを作成する場合は、以下のコマンドを使用できます。

- ascii、binary、passive、epsv

これらのコマンドは FTP サーバーに送信されません。各コマンドにより、FTP サーバーへの転送モード (ASCII、バイナリー、またはパッシブ) が変更されます。

- cd

  指定されたディレクトリーに移動します。

- delete

  FTP サーバーからファイルを削除します。

- get

  このコマンドは、リモート・システムから取得するファイルの名前である単一の引数を取ります。要求されたファイルが WebSphere Partner Gateway に転送されます。このコマンドは、名前が既知である単一ファイルを取り出す場合にのみ使用します。それ以外の場合は、`mget` コマンドをワイルドカードとともに使用します。

- getdel

  このコマンドは、WebSphere Partner Gateway が処理用のファイルを取得するときにリモート・システムからファイルが除去される点を除き、`get` コマンドと同じです。

- mget

  このコマンドは、取得するファイルのグループについて説明する単一の引数を取ります。説明には、標準のワイルドカード文字 (「*」および「?」) を含めることができます。1 つ以上のファイルがリモート・システムから取得されます。

- mgetdel

  このコマンドは、FTP サーバーから取得し、その後サーバー上から削除するファイルのグループについて説明する単一の引数を取ります。説明には、標準のワイルドカード文字 (「*」および「?」) を含めることができます。1 つ以上のファイルがリモート・システムから取得され、その後リモート・システムから削除されます。

- mkdir

  FTP サーバー上にディレクトリーを作成します。

- mputren

  このコマンドは、mput と rename コマンドの組み合わせです。例えば、**mputren * *.tmp /destination/*** コマンドは、**.tmp** という拡張子を使用して、宛先から FTP サーバーにファイルをコピーします。文書のダウンロード・プロセスが完了すると、ファイルは名前変更され、FTP ルート上の **/destination** ディレクトリーにコピーされます。

- open

  このコマンドは、FTP サーバー IP アドレス、ユーザー名、およびパスワードの 3 つのパラメーターを取ります。これらのパラメーターは、%BCGSERVERIP%、%BCGUSERID%、および %BCGPASSWORD% 変数に対応します。

したがって、FTP スクリプト記述レシーバー・スクリプトの最初の行は、以下のようになります。

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
```

- quit

  FTP サーバーへの既存の接続を終了します。

- quote

  QUOTE の後に指定されているものをすべてコマンドとしてリモート・システムに送信するように指定します。これにより、標準の FTP プロトコルに定義されていないコマンドをリモート FTP サーバーに送信できるようになります。

- rename

  FTP サーバー上のファイルの名前を変更します。

- rmdir

  FTP サーバーからディレクトリーを削除します。

- site

  このコマンドは、サイト固有のコマンドをリモート・システムに発行するときに使用できます。リモート・システムは、このコマンドの内容が有効かどうかを判別します。

## レシーバーの詳細

### このタスクについて

FTP スクリプト記述レシーバーに必要な情報を指定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックして、「レシーバー・リスト」ページを表示します。
2. 「レシーバー・リスト」ページで、「**レシーバーの作成**」をクリックします。

「**レシーバーの詳細**」セクションで、以下のステップを実行します。

1. レシーバーの名前を入力します。例えば、FTPScriptingReceiver1 というレシーバー名を付けます。このフィールドは必須です。ここで入力した名前は「レシーバー」リストに表示されます。
2. (オプション) レシーバーの状況を指定します。デフォルトは「**有効**」です。使用可能状態のレシーバーは、文書を受信することができます。無効状態のレシーバーは、文書を受信できません。
3. (オプション) レシーバーの説明を入力します。
4. 「トランスポート」リストから、「**FTP スクリプト記述**」を選択します。

## レシーバーの構成

### このタスクについて

ページの「**レシーバーの構成**」セクションで、以下のステップを実行します。

1. (オプション) **動作モード**を指定します。操作タイプによって、送信の性質が定義されます。例えば、文書交換を製品に書き込む前にテストする場合は、「**テスト**」を指定します。デフォルトは「**実動**」です。
2. 接続先の FTP サーバーの**サーバー IP** アドレスを入力します。FTP スクリプトが実行されると、ここに入力した値で %BCGSERVERIP% が置き換えられます。
3. サーバーにアクセスするために使用する**ユーザー ID** および**パスワード**を入力します。FTP スクリプトが実行されると、ここに入力した値で %BCGUSERID% および %BCGPASSWORD% が置き換えられます。
4. 「**FTPS モード**」には、「はい」または「いいえ」を選択してください。これは、レシーバーが Secure Sockets Layer (SSL) モードで動作するかどうかを指定します。このモードで動作する場合は、パートナーと証明書を交換する必要があります ( 257 ページの『第 13 章 文書交換のセキュリティーの使用可能化』を参照)。
5. 以下のステップを実行して、スクリプト・ファイルをアップロードします。
   a. 「**スクリプト・ファイルのアップロード**」をクリックします。
   b. 文書を処理するスクリプトが格納されたファイルの名前を入力するか、または「**参照**」 を使用して、ファイルにナビゲートします。
   c. 「**スクリプト・ファイルのエンコード・タイプ**」を選択します。
   d. 「**ファイルのロード**」をクリックして、スクリプト・ファイルを「**現在ロードされているスクリプト・ファイル**」テキスト・ボックスにロードします。
   e. このスクリプト・ファイルを使用したい場合は、「**保存**」をクリックします。
   f. 「**ウィンドウを閉じる**」をクリックします。
6. 「**接続タイムアウト**」に、トラフィックがなくてもソケットを開いたままにしておく時間 (秒数) を入力します。
7. 「**ロック・ユーザー**」フィールドに、レシーバーがロックを要求して、FTP スクリプト記述レシーバーの他のインスタンスが同時に同じ FTP サーバー・ディレクトリーにアクセスできないようにするかどうかを指定します。

### タスクの結果

**注:** 「**グローバル FTP スクリプト記述属性**」には既に値が入っており、このページから編集することはできません。これらの値を変更するには、「グローバル・トランスポート属性」ページを使用します ( 62 ページの『 グローバルなトランスポート値の設定』を参照)。

## ユーザー定義属性

### このタスクについて

追加の属性を指定する場合は、以下のステップを実行します。FTP スクリプトが実行されると、オプションに入力した値で %BCGOPTION*x*% が置き換えられます (*x* はオプション番号に対応します)。

1. 「**新規**」をクリックします。
2. 「**オプション 1**」の横に値を入力します。

3. 追加の属性を指定する場合は、「**新規**」を再びクリックして、値を入力します。
4. 必要なだけステップ 3 を繰り返して、すべての属性を定義します。

例えば、FTP スクリプトが次のようになっているとします。

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
          cd %BCGOPTION1%
          mget *
          quit
```

この場合、%BCGOPTION% はディレクトリー名です。

### スケジュール

間隔ベースのスケジューリングとカレンダー・ベースのスケジューリングのどちらが必要なのかを指定します。

- 「**間隔ベースのスケジューリング**」を選択した場合は、FTP サーバーをポーリングするまでの経過時間を秒数で選択します (またはデフォルト値を受け入れます)。
- 「**カレンダー・ベースのスケジューリング**」を選択した場合は、スケジューリングのタイプ (「**日次スケジュール**」、「**週次スケジュール**」、または「**カスタム・スケジュール**」) を選択します。
  - 「**日次スケジュール**」を選択した場合は、FTP サーバーがポーリングされる時刻を入力します。
  - 「**週次スケジュール**」を選択した場合は、時刻のほかに曜日を 1 つ以上選択します。
  - 「**カスタム・スケジュール**」を選択した場合は、まず時刻を選択し、次に週および月について「**範囲**」または「**選択できる日**」を選択します。「**範囲**」では、開始日と終了日を指定します。(例えば、平日の特定の時刻にのみサーバーをポーリングする場合は、「**月**」 および「**金**」をクリックしてください。) 「**選択できる日**」では、週および月の特定の日付を選択します。

### ハンドラー

分割が必要な複数の EDI 交換または XML や ROD 文書を含むファイルを受信した場合は、前処理構成ポイントに適切なスプリッター・ハンドラーを構成します。

前処理構成ポイントを変更する場合は、78 ページの『構成ポイントの変更』に進みます。それ以外の場合は、「**保管**」をクリックします。

## SFTP レシーバーの設定

### このタスクについて

このセクションでは、プロトコルとして SFTP (SSH-FTP) を使用してビジネス文書を転送する方法を詳しく説明します。SFTP は、データの機密性、認証、およびメッセージ保全性を提供します。

SFTP レシーバーは、SFTP サーバーのポーリング、SFTP サーバーからのファイルの取得、およびローカル・ディレクトリーへのファイルの格納を行います。ポーリングされる SFTP サーバーのディレクトリーは、リモート・イベント・ディレクト

リーと呼ばれます。取得したファイルが格納されるディレクトリーは、ローカル・イベント・ディレクトリーと呼ばれます。SFTP レシーバーに必要な情報を指定するには、以下のステップを実行します。

SFTP レシーバーに必要な情報を指定するには、以下のステップを実行します。

1. 「**ハブ管理**」 > 「**ハブ構成**」 > 「**レシーバー**」をクリックして、「レシーバー・リスト」ページを表示します。
2. 「レシーバー・リスト」ページで、「**レシーバーの作成**」をクリックします。

## レシーバーの詳細

### このタスクについて

「**レシーバーの詳細**」セクションで、以下のステップを実行します。

1. レシーバーの名前を入力します。例えば、 SFTPReceiver1 というレシーバー名を付けます。このフィールドは必須です。ここで入力した名前は「レシーバー」リストに表示されます。
2. (オプション) レシーバーの状況を指定します。デフォルトは「**有効**」です。有効状態のレシーバーは、文書を受信することができます。無効状態のレシーバーは、文書を受信できません。
3. (オプション) レシーバーの説明を入力します。
4. 「**トランスポート**」リストから、「**SFTP**」を選択します。

## レシーバーの構成

### このタスクについて

「**レシーバーの詳細**」セクションで、以下のステップを実行します。

1. 「**動作モード**」を入力します。ドロップダウン・リストから選択するか、「**新規**」をクリックしてモードを作成します。
2. 「**SFTP ホスト IP**」フィールドに SFTP サーバーのホスト名を入力します。最大文字数は 100 文字です。IP アドレス、IPv4 アドレス、および IPv6 アドレスを入力することもできます。
3. 「**ポート番号**」の値を入力します。デフォルト値は 22 です。
4. 「**リモート・イベント・ディレクトリー**」は、アダプターが SFTP サイトからイベント・ファイルをダウンロードする元のディレクトリーです。
5. 「**認証タイプ**」で、「**ユーザー名/パスワード (username/password)**」または「**秘密鍵認証 (private key authentication)**」を選択します。
6. ユーザー名/パスワードの場合は、「**ユーザー ID**」および「**パスワード**」を入力します。「認証タイプ」が「秘密鍵認証 (private key authentication)」である場合は、ユーザー名、秘密鍵ファイル、およびパスフレーズを入力します。秘密鍵ファイルは、OpenSSH の形式で指定する必要があります。
7. 「**SFTP ポーリング間隔**」に、時間をミリ秒で入力します。これは、ローカル・イベント・ディレクトリーをポーリング中にアダプターが待機する所要時間です。この時間と、ローカル・イベント・ディレクトリーで文書を処理するための時間は、ポーリング周期と呼ばれます。

8. 「**ポーリング数量**」は、それぞれのポーリング周期中にレシーバーが処理するイベント (文書) の数です。
9. 「**再試行間隔**」は、インバウンド操作中にエラーが発生した後、新しい接続の確立を試行してから次に試行するまでアダプターが待機するミリ秒単位の時間です。
10. 「**再試行制限**」は、エラーが発生した後、アダプターがインバウンド接続の再確立を試行する回数です。
11. 「**EIS エンコード**」は FTP サーバーのエンコードです。この値は、FTP サーバーに対する制御接続のエンコードを設定するために使用します。
12. 「**サーバー認証の有効化 (Enable server authentication)**」を有効にすると、接続が確立される先のサーバーを認証できます。サーバー認証を有効にする場合は、ホスト・キー・ファイル・パスを入力します。ホスト・キー・ファイルは、OpenSSH の形式で指定する必要があります。
13. 必要に応じて、ハンドラーを構成します。
14. 「**保存**」をクリックして、構成を保存します。

### ハンドラー

分割が必要な複数の EDI 交換または XML や ROD 文書を含むファイルを受信した場合は、前処理構成ポイントに適切なスプリッター・ハンドラーを構成します。

前処理構成ポイントを変更する場合は、78 ページの『構成ポイントの変更』に進みます。それ以外の場合は、「**保管**」をクリックします。

## ユーザー定義トランスポートのレシーバーの設定

### このタスクについて

ユーザー定義トランスポートのレシーバーを定義する場合、フィールド名およびその他の情報はトランスポートを記述するファイル内で定義します。

以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックします。
2. 「**トランスポート・タイプの管理**」をクリックします。
3. トランスポートを定義する XML ファイルの名前を入力します (または、「**参照**」を使用して、必要なファイルへ移動します)。
4. 「**アップロード**」をクリックします。

   **注:** 「レシーバー・リスト」から、ユーザー定義のトランスポート・タイプを削除することもできます。WebSphere Partner Gateway で提供されているトランスポートは、削除できません。また、レシーバーを作成するときに使用されたユーザー定義のトランスポートも削除することはできません。
5. 「**レシーバーの作成**」をクリックします。
6. レシーバーの名前を入力します。このフィールドは必須です。ここで入力した名前は「レシーバー」リストに表示されます。

7. (オプション) レシーバーの状況を指定します。デフォルトは「**有効**」です。使用可能状態のレシーバーは、文書を受信することができます。無効状態のレシーバーは、文書を受信できません。
8. (オプション) レシーバーの説明を入力します。
9. リストからユーザー定義トランスポートを選択します。
10. フィールドに情報を入力します (フィールドはユーザー定義トランスポートごとに固有です)。
11. このレシーバーの構成ポイントを変更する場合は、『構成ポイントの変更』に進みます。それ以外の場合は、「**保管**」をクリックします。

## 構成ポイントの変更

使用できる構成ポイント数、およびこれらの構成ポイントの関連ハンドラー数は、セットアップ中のレシーバー・タイプに応じて変わります。例えば、同期検査構成ポイントは HTTP/S および JMS レシーバーの場合にのみ使用できます。

同期交換に関与する特定のビジネス・プロトコル (RosettaNet、cXML、SOAP、および AS2) に対して、同期検査構成ポイント内でそのプロトコルに対するハンドラーを指定する必要があります。また、レシーバーの前処理または後処理ポイントにアップロードされたユーザー定義ハンドラー (または製品提供のプロセス) を適用して、レシーバーの文書処理方法を変更することもできます。

これらの構成ポイントにユーザーが作成したハンドラーを適用するには、まず 60 ページの『ユーザー定義ハンドラーのアップロード』の説明に従って、ハンドラーをアップロードする必要があります。また、製品提供のハンドラーを使用することも可能です。このハンドラーは、既に使用可能であり、アップロードする必要はありません。

### 前処理

前処理構成ハンドラーは、すべてのタイプのレシーバーで使用できますが、SMTP レシーバーには適用されません。

#### 前処理属性

79 ページの表 4で、前処理ハンドラーに対して設定できる属性について説明し、属性が適用するスプリッター・ハンドラーをリストします。

この表で例として使用される ROD 属性は、377 ページの『 ROD から EDI への例』で使用されるものと対応しています。この例では、ROD 属性はマップ S_DT_ROD_TO_EDI.eif に含まれています。これには、次の文書定義が含まれています。

- パッケージ: なし (バージョン N/A)
- プロトコル: ROD_TO_EDI_DICT (バージョン ALL)
- 文書タイプ: DTROD-TO-EDI_ROD (バージョン ALL)

このフローに関連する ROD メタ・ディレクトリーおよびメタ文書は ROD_TO_EDI_DICT と DTROD-TO-EDI_ROD です。

*表 4. スプリッター・ハンドラーの属性*

| 属性 | 説明 | スプリッター・ハンドラー |
|---|---|---|
| エンコード | 文書の文字エンコード。デフォルトは ASCII です。 | ROD Generic XML EDI |
| BATCHDOCS | BCG_BATCHDOCS がオンである場合、スプリッターは文書の分割後にバッチ ID を文書に追加します。エンベロープされる EDI トランザクションに文書が変換される場合、エンベローパーはバッチ ID を使用して、トランザクションが配信前に確実に同じ EDI 交換 (可能な場合) に入れられるようにします。エンベローパーでは、バッチ属性が「**オン**」 (デフォルト値) に設定されている必要があります。 195 ページの『バッチ・モード』を参照してください。 | ROD Generic XML |
| 送信元パッケージ名 (From Packaging Name) | 文書に関連するパッケージ化。この値は、文書定義で指定されたパッケージ化と一致している必要があります。例えば、パッケージ化がなしである文書の場合、この値は「**なし**」である必要があります。 | ROD Generic |
| 送信元パッケージ・バージョン (From Packaging Version) | 「送信元パッケージ名 (From Packaging Name)」で指定したパッケージ化のバージョン。例えば、パッケージ化がなしである文書の場合、この値は「**N/A**」である必要があります。 | ROD Generic |
| 送信元プロトコル名 (From Protocol Name) | 文書に関連するプロトコル。この値は、文書定義で指定されたプロトコルと一致している必要があります。例えば、ROD 文書の場合、この値は **ROD-TO-EDI_DICT** のようになります。 | ROD Generic |
| 送信元プロトコル・バージョン (From Protocol Version) | 「送信元プロトコル名 (From Protocol Name)」で指定したプロトコルのバージョン。例えば、ROD-TO-EDI_DICT プロトコルの場合、値は **ALL** になります。 | ROD Generic |
| 送信元プロセス・コード (From Process Code) | この文書に関連するプロセス (文書タイプ)。この値は、文書定義内の文書タイプと一致している必要があります。例えば、ROD 文書の場合、この値は DTROD-TO-EDI_ROD のようになります。 | ROD Generic |
| 送信元プロセス・バージョン (From Process Version) | 「送信元プロセス・コード (From Process Code)」で指定したプロセスのバージョン。例えば、DTROD-TO-EDI_ROD の場合、この値は **ALL** になります。 | ROD Generic |
| メタディクショナリー (Metadictionary) | メタディクショナリーは、WebSphere Partner Gateway でデータを解釈するための情報を提供します。例えば、ROD 文書の場合、この値は **ROD-TO-EDI_DICT** のようになります。 | ROD Generic |
| メタ文書 (Metadocument) | メタ文書は、WebSphere Partner Gateway でデータを解釈するための情報を提供します。例えば、ROD 文書の場合、この値は **DTROD-TO-EDI_ROD** のようになります。 | ROD Generic |
| メタ構文 (Metasyntax) | メタ構文は、分割中の文書のフォーマットを示します。デフォルト値は **rod** です。 | ROD Generic |

表 4. スプリッター・ハンドラーの属性 (続き)

| 属性 | 説明 | スプリッター・ハンドラー |
|---|---|---|
| SenderId | 送信側パートナーの ID。 | 汎用 |
| ReceiverId | 受信側パートナーの ID。 | 汎用 |

**注:**

1. サポートされる ROD 文書タイプはレシーバー・インスタンスごとに 1 つだけです。
2. レシーバーで複数のスプリッター・ハンドラーが構成されている場合 (例えば、ROD、XML、および EDI スプリッター・ハンドラーが構成されている場合)、ROD スプリッター・ハンドラーは「**構成済みリスト**」内の最後の 1 つである必要があります。

## 前処理構成ポイントの変更

### このタスクについて

前処理構成ポイントを変更するには、以下のステップを実行します。

1. 「**構成ポイント・ハンドラー**」リストから「**前処理**」を選択します。

   5 つの前処理ハンドラーが (デフォルトで) 用意されており、「**使用可能リスト**」に示されています。

   - com.ibm.bcg.edi.receiver.preprocesshandler.EDISplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.GenericDocumentFlowHandler
   - com.ibm.bcg.server.receiver.preprocesshandler.FileNamePartnerId

   **注:** 前処理ハンドラーは SMTP レシーバーに適用されません。
2. 分割が必要な複数の EDI 交換または XML や ROD 文書を受信する場合は、適切なスプリッター・ハンドラーを選択します。前処理ステップを構成するには、次のようにします。
   a. 「**使用可能リスト**」でハンドラーを選択して、「**追加**」をクリックします。ハンドラーが「**使用可能リスト**」から「**構成済みリスト**」に移動することに注意してください ( 81 ページの図 17 を参照)。

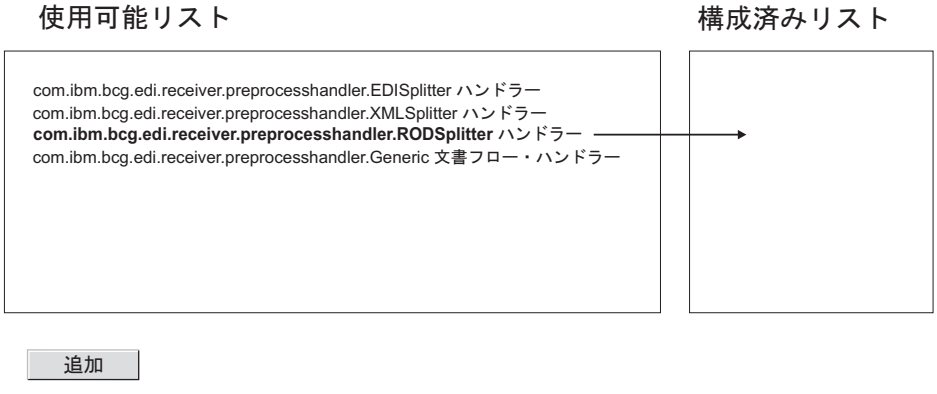



*図 17. レシーバーの前処理ステップの構成*

b. 構成リストに追加するハンドラーごとに、このステップを繰り返します。

   レシーバーの場合、ハンドラーは、「**構成済みリスト**」に表示されている順序で呼び出されます。最初に適用可能なハンドラーが要求を処理し、リストの以降のハンドラーは呼び出されません。

c. ハンドラーを選択し、「**構成**」をクリックして、ハンドラーを構成します。
   - EDISplitterHandler を追加する場合は、その属性であるエンコード (Encoding) を変更できます。エンコードのデフォルトは ASCII です。
   - XMLSplitterHandler を追加する場合は、その属性である BCGBATCHDOC を変更できます。デフォルトは「**オン**」です。この属性については、78 ページの『前処理属性』を参照してください。
   - RODSplitterHandler を追加する場合は、11 の属性値を指定できます。エンコードの BATCHDOCS およびメタ構文にはデフォルト値があります。その他の属性である送信元パッケージ名 (From Packaging Name)、送信元パッケージ・バージョン (From Packaging Version)、送信元プロトコル名 (From Protocol Name)、送信元プロトコル・バージョン (From Protocol Version)、送信元プロセス・コード (From Process Code) 、送信元プロセス・バージョン (From Process Version)、メタディクショナリー (Metadictionary)、およびメタ文書 (Metadocument) には、値を入力する必要があります。これらの属性については、78 ページの『前処理属性』を参照してください。
   - GenericDocumentFlowHandler を追加した場合は、13 の属性の値を指定することができます。エンコード (Encoding) および BATCHDOCS にはデフォルト値があります。SenderId 属性と ReceiverId 属性は、GenericDocumentFlowHandler に対して事前に定義されています (デフォルト値はありません)。その他の属性である送信元パッケージ名 (From Packaging Name)、送信元パッケージ・バージョン (From Packaging Version)、送信元プロトコル名 (From Protocol Name)、送信元プロトコル・バージョン (From Protocol Version)、送信元プロセス・コード (From Process Code) 、送信元プロセス・バージョン (From Process Version)、メタディクショナリー (Metadictionary)、メタ文書 (Metadocument)、およびメタ構文 (Metasyntax) には、値を入力する必要があります。これらの属性については、78 ページの『前処理属性』を参照してください。

- FileNamePartnerId を追加した場合、構成パラメーターは必要ありません。受信されたファイルは以下の命名規則に従う必要があります。

  ```
  <anystring>bcgrcv<Receiver ID>bcgsdr<Sender ID>bcgend<anystring>
  ```

  ここで

  *Receiver ID*、*Sender ID*
  プロファイル内で構成されたパートナーのビジネス ID。

  **bcgrcv, bcgsdr**
  受信側および送信側のビジネス ID の開始を示すストリング定数。

  **bcgend**
  必要な命名規則ストリングの終了を判別するストリング定数。

  *anystring*
  ユーザーが選択した任意の英数字。

  このハンドラーは、FTP スクリプト記述レシーバーまたはファイル・ディレクトリー・フィールド用にのみ構成できます。FTP スクリプト記述またはファイル・ディレクトリー上でバイナリー・ファイルを受信するには、このハンドラーをレシーバー用に構成できます。

## 同期検査

### このタスクについて

同期検査構成ポイントは、HTTP/S および JMS レシーバーの場合にのみ使用できます。

同期交換に関与するビジネス・プロトコル用のハンドラーを指定するには、以下のステップを実行します。

1. 「**構成ポイント・ハンドラー**」リストから「**同期検査**」を選択します。

   HTTP/S レシーバー用の 6 つの同期検査ハンドラーが (デフォルトで) 用意されています。これらのハンドラーは、「**使用可能リスト**」に表示されます。

   - com.ibm.bcg.server.sync.As2SyncHdlr
   - com.ibm.bcg.server.sync.CxmlSyncHdlr
   - com.ibm.bcg.server.sync.RnifSyncHdlr
   - com.ibm.bcg.server.sync.SoapSyncHdlr
   - com.ibm.bcg.server.sync.DefaultAsynchronousSyncCheckHandler
   - com.ibm.bcg.server.sync.DefaultSynchronousSyncCheckHandler
   - com.ibm.bcg.server.sync.EBMSSyncCheckHandler

   例えば、HTTP/S レシーバーを構成する場合、「使用可能リスト」は次のようになります。

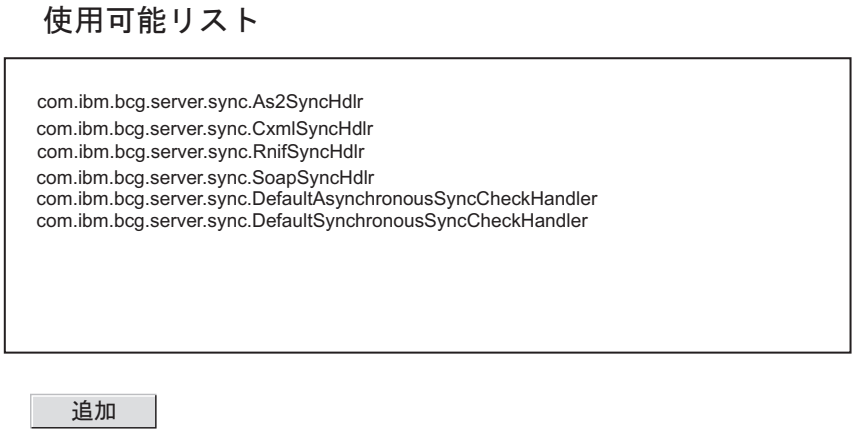



*図 18. HTTP/S 同期検査構成ポイントで使用可能なハンドラーのリスト*

命名規則からわかるように、最初の 4 つのハンドラーは、同期トランザクションに使用できる 4 つの文書タイプに固有です。
DefaultAsynchronousSyncCheckHandler を使用する要求は、非同期要求として処理されます。DefaultSynchronousSyncCheckHandler を使用する要求は、同期要求として処理されます。

DefaultAsynchronousSyncCheckHandler および
DefaultSynchronousSyncCheckHandler は他のレシーバー (JMS レシーバーなど) と併用できます。

2. このレシーバーで同期文書を受信する場合は、以下のステップを実行します。
   a. 「**使用可能リスト**」でハンドラーを 1 つ以上選択して、「**追加**」をクリックします。
   b. このリストにさらにハンドラーを追加する場合は、このステップを繰り返します。レシーバーの場合、ハンドラーは、「**構成済みリスト**」に表示されている順序で呼び出されます。最初に使用可能なハンドラーが要求を処理し、リストの以降のハンドラーは呼び出されません。

   HTTP および HTTPS レシーバーの場合は、特定の同期検査ハンドラー (例えば、AS2 トランザクションの com.ibm.bcg.server.sync.As2SyncHdlr) をリストしてからデフォルトの同期検査ハンドラーをリストすることをお勧めします。

# 後処理

## このタスクについて

後処理ステップにはデフォルトのハンドラーが用意されていないため、デフォルトでは「**使用可能リスト**」にハンドラーが 1 つもリストされません。ただし、同期通信をサポートするすべてのレシーバー・タイプに対して、この構成ポイント用のハンドラーをアップロードすることができます。後処理ステップで使用可能なハンドラー・タイプは、次のとおりです。

- RECEIVER.SYNCRESPONSEPROCESS.JMS
- RECEIVER.SYNCRESPONSEPROCESS.HttpS

これらのハンドラー・タイプの 1 つに準拠するハンドラーをアップロードして、後処理ハンドラーを追加します。「ハンドラー・リスト」ページの「**インポート**」選

択項目を使用して、ユーザー定義のハンドラーをアップロードします。ユーザー定義のレシーバー・ハンドラーをアップロードすると、このハンドラーが「ハンドラー・リスト」に追加されます。また、このハンドラーは、関連する構成ポイントのタイプの「使用可能リスト」にも表示されます。

後処理構成ポイントを変更するには、以下のステップを実行します。

1. 「**構成ポイント・ハンドラー**」リストから「**Postprocess**」を選択します。
2. 「**使用可能リスト**」でユーザー定義ハンドラーを選択して、「**追加**」をクリックします。ハンドラーが「**使用可能リスト**」から「**構成済みリスト**」に移動することに注意してください。

## 構成済みリストの変更

### このタスクについて

ハンドラーの順序を変更したり、ハンドラーを削除したり、ハンドラーの属性を構成したりする必要がある場合は、該当するステップを実行します。

- 「**構成済みリスト**」からハンドラーを選択し、「**除去**」をクリックして、ハンドラーを除去します。ハンドラーが「**使用可能リスト**」に移動します。
- ハンドラーを選択し、「**上に移動**」または「**下に移動**」をクリックして、ハンドラーが使用される順序を変更します。
- 「**構成済みリスト**」からハンドラーを選択し、「**構成**」をクリックして、ハンドラーを構成します。構成可能な属性のリストが表示されます。

# 第 8 章 固定ワークフロー・ステップおよびアクションの構成

この章では、インバウンドおよびアウトバウンドの固定ワークフローとアクションを構成するために実行するオプションの作業について説明します。製品で提供するワークフローまたはアクションの動作を変更する必要がなければ、この章は省略してください。

この章では以下のトピックを扱います。

- 『ハンドラーのアップロード』
- 86 ページの『固定ワークフローの構成』
- 88 ページの『アクションの構成』

**注:** WebSphere Partner Gateway の構成変更を行う場合は、必ず、コミュニティー・コンソールにログインしたときと同じブラウザー・インスタンスを使用してください。複数のブラウザー・インスタンスを同時に使用すると、構成変更が無効になる可能性があります。

## ハンドラーのアップロード

### このタスクについて

コンポーネントに変更を加える場合は、まずそれらのコンポーネントのハンドラーをアップロードしてから、コンポーネントを作成または構成する必要があります。アップロードする必要があるのは、コンポーネントで必要とされるユーザー定義のハンドラーのみです。例えば、独自の検証ステップを追加する場合は、「**ハンドラー**」の「アクション」ページから目的のハンドラーをアップロードする必要があります (ステップ 1 (86 ページ) から 4 (86 ページ) までを参照)。

**注:** 15 ページの『ハンドラーを使用した文書処理コンポーネントの構成』で説明されているように、ユーザー定義のハンドラーのみをアップロードします。WebSphere Partner Gateway で提供されているハンドラーは、既に使用可能です。

固定ワークフローとアクションを変更したり、新たにアクションを作成したりできます。これらのコンポーネントは、これらのコンポーネントに関連付けたハンドラーによって変更します。

**注:** アクションおよび固定ワークフローの有効なハンドラー・タイプをリストするには、「**ハブ管理**」>「**ハブ構成**」>「**ハンドラー**」>「**アクション**」>「**ハンドラー・タイプ**」をクリックするか、または「**ハブ管理**」>「**ハブ構成**」>「**ハンドラー**」>「**固定ワークフロー**」>「**ハンドラー・タイプ**」をクリックします。このリストを使用して、ハンドラーが有効なタイプであることを確認してから、ハンドラーをアップロードしてください。ハンドラーは、許可されているタイプではない場合、正常にアップロードされません。

ハンドラーをアップロードするには、以下のステップを実行します。

1. メインメニューから、「**ハブ管理**」>「**ハブ構成**」>「**ハンドラー**」をクリックします。
2. ハンドラーのタイプを選択します (「**アクション**」または「**固定ワークフロー**」)。

   特定のコンポーネントに対して現在定義されているハンドラーのリストが表示されます。WebSphere Partner Gateway で提供されているハンドラーがリストされていることに注意してください。これらのプロバイダー ID は「**製品**」となっています。
3. 「ハンドラー・リスト」ページで、「**インポート**」をクリックします。
4. 「ハンドラーのインポート」ページで、目的のハンドラーが記述されている XML ファイルへのパスを指定するか、または「**参照**」を使用してその XML ファイルを検索します。
5. 「**アップロード**」をクリックします。

ハンドラーをアップロードしたら、そのハンドラーを使用してアクションおよびワークフローを新たに作成できます。

**注:** ユーザー定義のハンドラーを更新するには、変更した XML ファイルをアップロードします。例えば、アクション・ハンドラーの場合は、「**ハブ管理**」>「**ハブ構成**」>「**ハンドラー**」>「**アクション**」をクリックし、「**インポート**」をクリックします。

WebSphere Partner Gateway で提供されているハンドラーは、変更したり、削除したりすることはできません。

## 固定ワークフローの構成

### このタスクについて

5 ページの『第 2 章 ハブ構成の概要』では、構成可能な 2 つの固定インバウンド・ワークフロー・ステップについて説明しました。1 つはプロトコルのアンパックで、もう 1 つはプロトコルの構文解析です。アウトバウンド・ワークフローの場合は、プロトコルのパッケージ化のステップが 1 つあります。

ユーザー定義のハンドラーを使用してワークフロー・ステップを構成する場合は、85 ページの『ハンドラーのアップロード』の説明に従って、ハンドラーをアップロードしてください。

固定ワークフローを構成するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**固定ワークフロー**」をクリックします。
2. 「**インバウンド**」または「**アウトバウンド**」をクリックします。
3. 構成するステップの名前の横にある「**詳細の表示**」アイコンをクリックします。

   ステップが、そのステップの構成済みハンドラーのリストと共にリストされます。デフォルトのハンドラーのリストについては、87 ページの『インバウンド・ワークフロー』および 88 ページの『アウトバウンド・ワークフロー』を参照してください。
4. ハンドラーのリストを編集するには、「**編集**」アイコンをクリックします。

5. 変更するステップごとに、以下の作業を 1 つ以上実行します。
   a. 「**使用可能リスト**」からハンドラーを選択し、「**追加**」をクリックして、ハンドラーを追加します。(「**使用可能リスト**」にハンドラーが表示されるのは、ユーザー定義のハンドラーをアップロードした場合や、以前に「**構成済みリスト**」からハンドラーを削除した場合です。) ハンドラーが「**構成済みリスト**」に移動します。
   b. 「**構成済みリスト**」からハンドラーを選択し、「**除去**」をクリックして、ハンドラーを除去します。ハンドラーが「**使用可能リスト**」に移動します。
   c. ハンドラーを選択し、「**上に移動**」または「**下に移動**」をクリックして、ハンドラーが呼び出される順序を変更します。

      ハンドラーは、「**構成済みリスト**」にリストされている順序で呼び出されます。要求を処理できる最初の使用可能なハンドラーのみが、要求を処理します。特定のタイプの文書 (例えば、ROD 文書) の大量受信が見込まれる場合は、その文書のタイプに関連付けられたハンドラー (この例では com.ibm.bcg.edi.business.process.RODScannerHandler) をリストの最上位に移動しておくことができます。
6. 「**保存**」をクリックします。

# インバウンド・ワークフロー

ここでは、インバウンド・ワークフロー向けに構成されているハンドラーをリストします。

## プロトコル・アンパック・ハンドラー

デフォルトでは、プロトコル・アンパック・ステップには以下のハンドラーが構成されています。

- com.ibm.bcg.ediint.ASUnpackagingHandler
- com.ibm.bcg.server.pkg.NullUnpackagingHandler
- com.ibm.bcg.server.pkg.MIMEMultipartUnpackagingHandler
- com.ibm.bcg.eai.EAIUnpackagingHandler

## プロトコル処理ハンドラー

デフォルトでは、プロトコル処理ステップには以下のハンドラーが構成されています。

- com.ibm.bcg.server.RNOChannelParseHandler
- com.ibm.bcg.server.RNSignalChannelParseHandler
- com.ibm.bcg.server.RNSCChannelParseHandler
- com.ibm.bcg.server.BinaryChannelParseHandler
- com.ibm.bcg.cxml.cXMLChannelParseHandler
- com.ibm.bcg.soap.SOAPChannelParseHandler
- com.ibm.bcg.server.XMLRouterBizProcessHandler
- com.ibm.bcg.edi.EDIRouterBizProcessHandler
- com.ibm.bcg.edi.business.process.RODScannerHandler
- com.ibm.bcg.edi.business.process.NetworkAckHandler

- com.ibm.bcg.server.EBMSProtocolParseHandler
- com.ibm.bcg.server.BackendChannelParseHandler

「Content-Types」属性は、BinaryChannelParseHandler、XMLRouterBizHandler、EDIRouterBizProcessHandler、および cXMLChannelParseHandler に関連付けられています。これらのハンドラーでは、デフォルトのコンテンツ・タイプのリストが定義済みです。受信した文書に上記のハンドラーのいずれかに対応して構成されたコンテンツ・タイプ・ヘッダーが含まれる場合、そのハンドラーが適用されます。

### アウトバウンド・ワークフロー

デフォルトでは、プロトコル・パッケージ化ステップには以下のハンドラーが構成されています。

- com.ibm.bcg.server.pkg.NullPackagingHandler
- com.ibm.bcg.ediint.ASPackagingHandler
- com.ibm.bcg.edi.server.EDITransactionHandler
- com.ibm.bcg.rosettanet.pkg.RNOPPackagingHandler
- com.ibm.bcg.server.pkg.RNPassThruPackagingHandler
- com.ibm.bcg.cxml.cXMLPackagingHandler
- com.ibm.bcg.soap.SOAPPackagingHandler
- com.ibm.bcg.eai.EAIPackagingHandler

## アクションの構成

5 ページの『第 2 章 ハブ構成の概要』に表示されているように、アクションは 1 つ以上のステップで構成されます。WebSphere Partner Gateway には、一連のデフォルトのアクションがあります。1 つ以上のアクション・ハンドラー (アクション内のステップ) をアップロードして、アクションのリストに追加することができます。このアクション・ハンドラーは、その後、アクションで使用できます。新規アクションを作成することもできます。 106 ページの『アクションの作成』を参照してください。

**注:** WebSphere Partner Gateway により提供されたアクションを変更することはできませんが、このようなアクションをコピーして変更することはできます。 107 ページの『アクションのコピー』を参照してください。

ユーザー定義のハンドラーを使用してアクションを構成する場合は、 85 ページの『ハンドラーのアップロード』の説明に従って、ハンドラーをアップロードしてください。

### 製品が提供するアクション

このセクションでは、Websphere Partner Gateway 製品で提供されるアクションの目的と、それらを使用するために必要な構成について詳細に説明します。 109 ページの『第 9 章 文書タイプの構成』で、これらのアクションのいくつかを使用するタイミングについてさらに詳細に説明しています。

一部のアクションの名前には、「双方向」が含まれます。*双方向* とは、ソース形式とターゲット形式を逆にしても、アクションを使用できることを意味します。例え

ば、「RosettaNet と XML の間の双方向変換 (検証あり)」というアクションの場合、ソース文書が RosettaNet でターゲット文書が XML であっても、ソース文書が XML でターゲット文書が RosettaNet であってもかまいません。

WebSphere Partner Gateway で提供されるさまざまなアクションを以下に示します。

- 『パススルー』
- 90 ページの『RosettaNet プロセスの内部パートナーによるキャンセル』
- 91 ページの『RosettaNet パススルー (プロセス・ロギングあり)』
- 91 ページの『RosettaNet と RosettaNet サービス・コンテンツの間の双方向変換 (検証あり)』
- 93 ページの『RosettaNet と RosettaNet サービス・コンテンツ間の双方向変換 (コンテンツ検証なし)』
- 94 ページの『内部パートナーのカスタム XML から RosettaNet への双方向変換 (コンテンツ重複検査および検証あり)』
- 92 ページの『RosettaNet と XML の間の双方向変換 (検証あり)』
- 95 ページの『カスタム XML の双方向変換 (検証あり)』
- 96 ページの『カスタム XML の双方向変換 (重複検査および検証あり)』
- 97 ページの『カスタム XML パススルー (重複検査および検証あり)』
- 97 ページの『カスタム XML パススルー (重複検査あり)』
- 98 ページの『カスタム XML パススルー (検証あり)』
- 98 ページの『EDI エンベロープ解除』
- 99 ページの『EDI 検証および EDI 変換』
- 100 ページの『ROD (FlatFile) 変換および EDI 検証』
- 100 ページの『XML 変換および EDI 検証』
- 101 ページの『ebMS の分割および解析』
- 103 ページの『SOAP エンベロープの検証』
- 104 ページの『SOAP 本体の検証』
- 104 ページの『SOAP エンベロープ解除』
- 102 ページの『EDI 交換の検証』
- 102 ページの『WTX 変換』
- 103 ページの『EDI リエンベローパー』

## パススルー

このアクションは、文書に対して検証や変換などの特別な処理が実行される予定がない場合に使用されます。ソース文書は、そのままの状態でターゲット・ロケーションに送信されます。

### 構成

不要。

### 変更

このアクションは、新規アクションにコピーできます。既存のステップの前に、新しいステップを追加できます。例えば、ソース文書を検証するカスタム検証ステップや、その他のカスタム処理です。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.passthrough.No_op** – ターゲット文書のコンテンツ・タイプを、文書のコンテンツから引き出してはならないことを示すために使用します。
2. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## RosettaNet プロセスの内部パートナーによるキャンセル

### 目的

このアクションは、内部パートナー (バックエンド) により RosettaNet RNIF プロセスを取り消すものです。バックエンド・アプリケーション (内部パートナー) が、イベント・コード 800/801 の XML イベント文書を送信すると、このステップで 0A1 文書が作成されて外部パートナーに送信され、対応する PIP プロセスはキャンセルされます。

### 構成

キャンセルされる RNIF プロセスは、WebSphere Partner Gateway で既に構成されていなければならず、WebSphere Partner Gateway は、キャンセルされるプロセスを開始した RosettaNet 文書を既に受信していなければなりません。

### 変更

このアクションは、RosettaNet PIP プロセスのキャンセルに固有のものであるため、変更またはコピーできません。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - RNIF の正しいアンパック・クラスを判別するか、または文書を RNIF 以外であると見なしてアンパックを実行しません。
2. **com.ibm.bcg.validation.ValidationFactory** - ソース RN 文書で、RNIF サービス・コンテンツが正しいかどうかを検証します。
3. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## RosettaNet パススルー (プロセス・ロギングあり)

このアクションは、RosettaNet ソース RNIF 文書が WebSphere Partner Gateway でパススルーされるときに使用されます。RNIF 文書のサービス・コンテンツが抽出も変換もされない場合に、このステップを使用します。これはパススルーですが、RNIF 処理は実行され、受信確認が生成されます。

### 構成

不要。

### 変更

このアクションは、コピーおよび変更できます。追加のカスタム処理用に、新規のステップを既存のステップの前に追加できます。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.rosettanet.passthru.ProcessLoggingFactory** - このステップは、RosettaNet 文書のメタデータをビジネス文書オブジェクト (BDO) 内に設定します。
2. **com.ibm.bcg.passthrough.No_op** - ターゲット文書のコンテンツ・タイプを、文書のコンテンツから引き出してはならないことを示すために使用します。
3. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## RosettaNet と RosettaNet サービス・コンテンツの間の双方向変換 (検証あり)

このアクションは、RosettaNet RNIF 文書に使用されます。外部パートナーから RNIF 文書を受信すると、ペイロード (RNSC - RosettaNet サービス・コンテンツ) が RNIF パッケージ化文書から抽出され、バックエンド・アプリケーション (内部パートナー) に送信されます。RNSC を含む RNIF 文書に対して検証が行われます。バックエンド・アプリケーション (内部パートナー) から着信したときに、RNSC 文書が検証されます。

### 構成

RosettaNet 文書用の RosettaNet PIP パッケージがロードされている必要があります。

### 変更

このアクションは、コピーおよび変更できません。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - RNIF の正しいアンパック・クラスを判別するか、または文書を RNIF 以外であると見なしてアンパックを実行しません。
2. **com.ibm.bcg.validation.ValidationFactory** - 検証を実行して、RNIF 1.1、RNIF 2.0、および RNSC 文書の検証のために以下のビジネス・プロセスを利用します。- RNSignal0A1Validation (WebSphere Partner Gateway が生成した RNIF シグナルまたは 0A1 メッセージを検証する) - ValidationNoOp (何も処理を行うことなく単に BusinessDocument を戻すもので、WBIC が RNIF シグナルまたは 0A1 メッセージを再試行する際に呼び出される) - RN11Validation (RNIF 1.1 メッセージを検証する) - RN20Validation (RNIF 2.0 メッセージを検証する) - RNSCValidation (XML イベントおよび RNSC メッセージを検証する)
3. **com.ibm.bcg.translation.protocol.StdRNandRNSCProtFactory** - RNIF 文書から RNSC を取り出すため、または RNSC 用の RNIF 情報を作成するために使用されます。
4. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - RosettaNet 状態エンジンを更新するために RosettaNet 0A1 文書を処理する際に使用します。
5. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## RosettaNet と XML の間の双方向変換 (検証あり)

このアクションは、カスタム XML 文書に変換する必要のある RosettaNet RNIF 文書 (またはその逆の場合) に使用されます。外部パートナーから RNIF 文書を受信すると、ペイロード (RNSC - RNIF サービス・コンテンツ) が RNIF パッケージから抽出され、検証され、XML 文書に変換されて、その変換済みターゲット文書が検証された上で、バックエンド・アプリケーション (内部パートナー) に送信されます。バックエンド・アプリケーション (内部パートナー) から着信したときに、XML が検証されて RNSC に変換され、その RNSC が検証されます。

### 構成

- RosettaNet 文書用の RosettaNet PIP パッケージがロードされている必要があります。
- ソースまたはターゲット XML 文書のいずれかにおいて、検証マップ (XML SCHEMA) が構成される必要があります。
- このアクションに対して XSLT 変換マップが構成される必要があります。

### 変更

このアクションは、コピーおよび変更できません。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - RNIF の正しいアンパック・クラスを判別するか、または文書を RNIF 以外であると見なしてアンパックを実行しません。
2. **com.ibm.bcg.validation.ValidationFactory** – ソース RNIF 文書または XML 文書を検証します。
3. **com.ibm.bcg.translation.protocol.RNXsltProtFactory** – RNSC から XML に、または XML から RNSC に変換します。
4. **com.ibm.bcg.validation.OutboundValidationFactory** - 結果として生成された変換済み XML 文書を検証します。
5. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - RosettaNet 状態エンジンを更新するために RosettaNet 0A1 文書を処理する際に使用します。
6. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## RosettaNet と RosettaNet サービス・コンテンツ間の双方向変換 (コンテンツ検証なし)

このアクションは、RosettaNet (RNIF) 文書に使用されます。外部パートナーから RNIF 文書を受信すると、ペイロード (RNSC - RNIF サービス・コンテンツ) が RNIF パッケージから抽出されます。この抽出されたペイロードは、検証され、XML 文書に変換されてから、バックエンド・アプリケーション (内部パートナー) に送信されます。バックエンド・アプリケーション (内部パートナー) から XML 文書を受信すると、それに対して以下のステップが実行されます。

1. 重複 ID チェック
2. 検証
3. RNSC への変換
4. RNSC の検証

### 構成

RosettaNet 文書用の RosettaNet PIP パッケージがロードされている必要があります。

### 変更

このアクションは、コピーおよび変更できません。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - RNIF の正しいアンパック・クラスを判別するか、または文書を RNIF 以外であると見なしてアンパックを実行しません。
2. **com.ibm.bcg.validation.ValidationWithoutContentFactory** – RNSC 以外で検証を実行します。
3. **com.ibm.bcg.translation.protocol.StdRNandRNSCProtFactory** - RNIF 文書から RNSC を取り出すため、または RNSC 用の RNIF 情報を作成するために使用されます。
4. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - RosettaNet 状態エンジンを更新するために RosettaNet 0A1 文書を処理する際に使用します。
5. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## 内部パートナーのカスタム XML から RosettaNet への双方向変換 (コンテンツ重複検査および検証あり)

このアクションは、カスタム XML 文書に変換する必要のある RosettaNet RNIF 文書 (またはその逆の場合) に使用されます。外部パートナーから RNIF 文書を受信すると、ペイロード (RNSC - RNIF サービス・コンテンツ) が RNIF パッケージから抽出され、検証され、XML 文書に変換されて、バックエンド・アプリケーション (内部パートナー) に送信されます。バックエンド・アプリケーション (内部パートナー) から着信したとき、XML に対して重複 ID 検査が実行されてから、XML が検証されて RNSC に変換され、さらに検証が実行されます。「RosettaNet と XML の間の双方向変換 (検証あり)」アクションに類似していますが、ソース XML に対する重複検査が追加されます。

### 構成

- ソース文書の XML 形式では、重複検査キーを構成する必要があります。
- RosettaNet 文書用の RosettaNet PIP パッケージがロードされている必要があります。
- ソースまたはターゲット XML 文書のいずれかにおいて、検証マップ (XML SCHEMA) が構成される必要があります。
- このアクションに対して XSLT 変換マップが構成される必要があります。

### 変更

このアクションは、RNIF 文書に固有であるため、コピーおよび変更できません。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - 受信したカスタム XML に重複 ID 検査を実行します。

2. **com.ibm.bcg.server.pkg.UnPackagingFactory** - RNIF の正しいアンパック・クラスを判別するか、または文書を RNIF 以外であると見なしてアンパックを実行しません。
3. **com.ibm.bcg.validation.ValidationFactory** – ソース RNIF 文書または XML 文書を検証します。
4. **com.ibm.bcg.translation.protocol.RNXsltProtFactory** – RNSC から XML に、または XML から RNSC に変換します。
5. **com.ibm.bcg.validation.OutboundValidationFactory** - 結果として生成された変換済み XML 文書を検証します。
6. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - RosettaNet 状態エンジンを更新するために RosettaNet 0A1 文書を処理する際に使用します。
7. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## カスタム XML の双方向変換 (検証あり)

このアクションは、外部パートナーまたは内部パートナーから着信したカスタム XML 文書で使用します。ソース文書が検証されてターゲット文書に変換され、さらにターゲット文書が検証されます。

### 構成

- ソース文書において、検証マップ (XML SCHEMA) が構成される必要があります。
- このアクションに対して XSLT 変換マップが構成される必要があります。
- ターゲット文書において、検証マップ (XML SCHEMA) が構成される必要があります。

### 変更

このアクションは、コピーおよび変更できます。変換ステップまたは検証ステップをユーザー定義ステップに置き換えることができ、ユーザー定義ステップを加算追加することもできます。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.validation.ValidationFactory** – このステップでは、受信したカスタム XML 文書を検証します。
2. **com.ibm.bcg.translation.protocol.translators.xslt.XSLTranslationFactory** – 変換を実行します。
3. **com.ibm.bcg.validation.OutboundValidationFactory** - 結果として生成された変換済み XML 文書を検証します。
4. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のス

テップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## カスタム XML の双方向変換 (重複検査および検証あり)

このアクションは、カスタム XML 文書で使用されます。外部パートナーまたは内部パートナーから着信した文書に使用できます。ソース文書で重複 ID 検査が実行され、ソース文書が検証され、ソース文書がターゲット文書に変換され、ターゲット文書が検証されます。このアクションは、「カスタム XML の双方向変換 (検証あり)」に類似していますが、重複検査が追加されている点が異なります。

### 構成

- ソース文書の XML 形式では、重複検査キーを構成する必要があります。
- ソース文書において、検証マップ (XML SCHEMA) が構成される必要があります。
- このアクションに対して XSLT 変換マップが構成される必要があります。
- ターゲット文書において、検証マップ (XML SCHEMA) が構成される必要があります。

### 変更

このアクションは、コピーおよび変更できます。ユーザー定義ステップに置き換えることが可能なステップは、ValidationFactory、XSLTTranslationFactory および OutboundValidationFactory です。またはユーザー定義ステップを追加できます。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - 文書 ID に基づいて重複文書があるかどうかをチェックします。
2. **com.ibm.bcg.validation.ValidationFactory** - このステップでは、受信したカスタム XML 文書を検証します。
3. **com.ibm.bcg.translation.protocol.translators.xslt.XSLTranslationFactory** - このステップでは、受信したカスタム XML 文書をターゲット XML 形式に変換します。
4. **com.ibm.bcg.validation.OutboundValidationFactory** - このステップでは、直前の変換ステップからの変換済みターゲット XML 文書を検証します。
5. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## カスタム XML パススルー (重複検査および検証あり)

### 目的

このアクションは、カスタム XML 文書で使用されます。外部パートナーまたは内部パートナーから発信された文書に使用できます。重複 ID 検査が実行され、ソース文書が検証されます。このアクションは、「カスタム XML パススルー (重複検査あり)」に類似していますが、ソース文書検証も実行される点が異なります。

### 構成

- ソース文書の XML 形式では、重複検査キーを構成する必要があります。
- ソース XML 文書において、検証マップ (XML SCHEMA) が構成される必要があります。

### 変更

このアクションは、コピーおよび変更できます。ユーザー定義ステップに置き換えることが可能なステップは、ValidationFactory です。またはユーザー定義ステップを追加できます。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - 文書 ID に基づいて重複文書があるかどうかをチェックします。このソース文書の XML 形式には、重複 ID 構成が必要です。
2. **com.ibm.bcg.validation.ValidationFactory** - このステップでは、ソース・カスタム XML 文書を検証します。
3. **com.ibm.bcg.passthrough.No_op** - ターゲット文書のコンテンツ・タイプを、文書のコンテンツから引き出してはならないことを示すために使用します。
4. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## カスタム XML パススルー (重複検査あり)

このアクションは、カスタム XML 文書で使用されます。外部パートナーまたは内部パートナーから発信された文書に使用できます。ソース文書に対して重複 ID 検査が実行されます。

### 構成

ソース文書の XML 形式では、重複検査キーを構成する必要があります。

### 変更

可能な変更は、「カスタム XML パススルー (重複検査および検証あり)」アクションで定義された検証ステップの追加であるため、このアクションは、新規アクションにコピーできません。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - 文書 ID に基づいて重複文書があるかどうかをチェックします。このソース文書の XML 形式には、重複 ID 構成が必要です。
2. **com.ibm.bcg.passthrough.No_op** - ターゲット文書のコンテンツ・タイプを、文書のコンテンツから引き出してはならないことを示すために使用します。
3. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## カスタム XML パススルー (検証あり)

このアクションは、外部パートナーまたは内部パートナーから着信したカスタム XML 文書で使用します。ソース文書に対して検証が実行されます。

### 構成

ソース XML 文書において、検証マップ (XML SCHEMA) が構成される必要があります。

### 変更

このアクションは、コピーおよび変更できます。ValidationFactory をユーザー定義ステップに置き換えることができ、ユーザー定義ステップを追加することもできます。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.validation.ValidationFactory** - このステップでは、ソース・カスタム XML 文書を検証します。
2. **com.ibm.bcg.passthrough.No_op** - ターゲット文書のコンテンツ・タイプを、文書のコンテンツから引き出してはならないことを示すために使用します。
3. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## EDI エンベロープ解除

このアクションは、外部パートナーから着信した EDI 交換で使用します。EDI 交換のエンベロープが解除され (EDI トランザクションが抽出される)、これらの EDI トランザクションは再び WebSphere Partner Gateway に導入されて、個別に処理されます。EDI 交換文書は WebSphere Partner Gateway 内ではそれ以上処理されません。

### 構成

文書定義でのオプションの構成。

### 変更

このアクションは、コピーおよび変更できません。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.edi.business.process.EDIDenvFactory** – EDI 交換のエンベロープ解除を実行します。
2. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## EDI 検証および EDI 変換

このアクションは、EDI エンベロープ解除アクションによって EDI 交換からエンベロープ解除された EDI トランザクションに使用されます。これらのトランザクションは外部パートナーからのものです。EDI トランザクション文書が、検証されてから変換されます。

### 構成

- 文書定義でのオプションの構成
- DIS クライアントまたは WTX design studio からのソース EDI トランザクション用のオプションの検証マップ。
- DIS クライアントまたは WTX design studio からの変換マップ。
- 任意のパッケージ/EDI - Any/Any からなし/EDI - Any/Any への参加者接続を、EDI エンベロープ解除として定義されたアクションでセットアップする必要があります。

### 変更

このアクションは、ユーザー出口ステップを追加するためにコピーおよび変更することができます。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.edi.business.process.EDISourceValidationFactory** – EDI トランザクションを検証します。また、このステップでは、EDI 交換からのすべての EDI トランザクションを処理した後に、EDI FA を発行します。
2. **com.ibm.bcg.edi.business.process.EDITranslatorFactory** – EDI トランザクションをターゲット文書に変換します。

3. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## XML 変換および EDI 検証

### 目的

このアクションは、内部パートナーからのカスタム XML 文書に使用されます。ソース XML 文書は EDI トランザクションに変換され、検証されます。その後、バックエンドまたは外部パートナーのいずれかに送信されます。ルーティング情報を指定するために、XML 形式を使用します。

### 構成

- 文書定義でのオプションの構成。
- DIS クライアントからのターゲット EDI トランザクション用のオプションの検証マップ。
- DIS クライアントまたは WDI design studio からの変換マップ。

### 変更

このアクションは、EDITargetValidationFactory を除去するため、またはユーザー出口ステップを追加するためにコピーおよび変更することができます。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.edi.business.process.XMLTranslatorFactory** – ソース XML 文書をターゲット EDI トランザクションに変換します。
2. **com.ibm.bcg.edi.business.process.EDITargetValidationFactory** – ターゲット EDI トランザクションを検証します。
3. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## ROD (FlatFile) 変換および EDI 検証

このアクションは、内部パートナーからのレコード指向文書 (ROD/フラット・ファイル) に使用されます。ソース ROD 文書は EDI トランザクションに変換され、検証されます。

### 構成

- 文書定義でのオプションの構成。
- DIS クライアントからのターゲット EDI トランザクション用のオプションの検証マップ。

- ROD 標準は、DIS クライアントで定義し、ダミーの変換マップを使用してコンパイルする必要があります。
- レシーバーのプロセス・ハンドラーに応じて ROD スプリッター/Generic Document Processor を追加する必要があります。これは、ディクショナリー文書および形式を認識させるためです。

### 変更

このアクションは、EDITargetValidationFactory を除去するため、またはユーザー出口ステップを追加するためにコピーおよび変更することができます。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.edi.business.process.RODTranslatorFactory** – ソース ROD 文書をターゲット EDI トランザクションに変換します。
2. **com.ibm.bcg.edi.business.process.EDITargetValidationFactory** – ターゲット EDI トランザクションを検証します。
3. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## ebMS の分割および解析

このアクションは、外部パートナーからの ebMS 文書に使用されます。ペイロード添付ファイルが抽出され、再び WebSphere Partner Gateway に導入されて個別に処理されます。ebMS 文書は WebSphere Partner Gateway 内ではそれ以上処理されません。

### 構成

追加の構成は不要です。

### 変更

このアクションは、コピーおよび変更できません。

### ステップ

このアクションには、以下のステップが含まれ、順番に実行されます。

1. **com.ibm.bcg.server.EBMSSplitAndParse** – ペイロード添付ファイルは、個別の文書に抽出されます。
2. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway の必須の処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## EDI 交換の検証

EDI 交換の検証は、WTX との非同期統合中に使用されます。交換をエンベロープ解除することにより、個々のトランザクションが交換から抽出されます。エンベロープ解除アクションにより、各トランザクションが交換から抽出されます。各トランザクションによって文書が生成され、その文書が検証対象として直接渡されます。

### 構成

- <any package>/EDI – xxxx/XXX からなし/EDI – xxxx/XXX への参加者接続を、「EDI 交換の検証」として定義されたアクションでセットアップする必要があります。
- オプションで、FA ユーザーは FA マップを構成できます。
- 機能確認通知を流すためのチャネルを定義する必要があります。

## WTX 変換

EDI、XML、および ROD またはフラット・ファイルは、WTX を使用して変換します。

WTX を使用した EDI の変換は、非同期的または同期的に実行できます。同期実行は、ほとんどの場合、エンベロープ解除して検証したトランザクションを WTX に送信して処理する場合に使用しますが、WTX で処理するために必要であれば、トランザクションがエンベロープし直されます。EDI トランザクションは、検証に成功すると WTX 変換 EDI トランザクション・アクションに渡されます。非同期モードでは、EDI トランザクションがバックエンドで変換されます。ここで、WTX が WESB/WMB または WTX ランチャーにデプロイされます。

### 同期実行の場合の構成

- <any package>/EDI – xxxx/XXX からなし/EDI – xxxx/XXX への参加者接続を EDI エンベロープ解除として定義されたアクションでセットアップする必要があります。
- <N/A>/XXXXXXX/YYYYY からなし/ZZZZZZ/BBBBBBB への参加者接続を、「EDI 検証」および「WTX 変換 EDI トランザクション」として定義されたアクションでセットアップする必要があります。
- WTX 変換マップをこのチャネルにも関連付ける必要があります。

### 非同期実行の場合の構成

- <any package>/EDI – xxxx/XXX からなし/EDI – xxxx/XXX への参加者接続を EDI エンベロープ解除として定義されたアクションでセットアップする必要があります。
- <N/A>/<edi version>/トランザクションから <N/A>/<edi version>/トランザクションへの参加者接続を、EDI 検証として定義されたアクションでセットアップする必要があります。
- <N/A>/<edi version>/トランザクションから <BI>/<edi interchange>/<ISA>/<UNB>/<UCS> への参加者接続を、EDI 検証および EDI 再エンベロープとして定義されたアクションでセットアップする必要があります。

### ROD および XML の場合の構成

- ROD 変換 - <any package>/<any protocol (flat file)>/<any flat file> から <Any>/<ANY>/<Any> Format への参加者接続を、「WTX 変換」として定義されたアクションでセットアップする必要があります。
- XML 変換 - <any package>/<any protocol>/<any XML> から <Any>/<ANY>/<Any> Format への参加者接続を、「WTX 変換」として定義されたアクションでセットアップする必要があります。

## WTX エンベロープ

### 目的

非同期モードで WTX を使用する場合は、WTX 変換の後に変換して EDI トランザクションを生成します。これがエンベロープ対象として WebSphere Partner Gateway に送信されます。

### 構成

- ターゲット・エンドでのパススルー構成エンベローパー・プロファイルのアクションを持つ <Backend>/<EDI Dictionary>/<EDI document> {EDI Trx} から <N/A>/<EDI X12/EDIFACT>/<EDI ISA/UNB> への接続。(チャネル A)。
- アクションがパススルーである、<NA>/<EDI Interchange>/<EDI ISA/UNB> から <ANY PACKAGE>/<EDI X12/EDIFACT>/<EDI ISA/UNB> への接続。(チャネル B)
-

## EDI リエンベローパー

リエンベローパーは、個々のトランザクションをエンベロープするために使用します。リエンベローパーは、ソース・エンベロープからエンベローパー・ヘッダーを取得し、エンベロープ解除された各トランザクションをそのヘッダーでラップします。

### 構成

- ソース (トランザクション) とターゲット (エンベロープ・プロファイルが設定された EDI 交換) の間の接続。
- アクションを EDI リエンベローパーとして設定します。

# SOAP エンベロープの検証

業界標準に従って、Web サービス要求全体が SOAP1.1 スキーマに対して検証されます。アクション SOAP エンベロープには、以下のステップがあります。ステップは順番に実行されます。

1. **com.ibm.bcg.validation.WebserviceFactory**– Web サービス要求の妥当性検査を行い、WebserviceValidation ハンドラーを戻します。
2. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway に必要な処理を実行します。これが最後のステップであり、コンソールによって自動的に、既存のアクションまたは新規作成されたアクションに追加されます。このステップは、構成済みハンドラー・リストには表示されません。

## SOAP 本体の検証

このフィーチャーは、SOAP エンベロープの下にある SOAP 本体またはペイロードの妥当性検査を行います。ペイロードの妥当性検査は、SOAP エンベロープ内の XML ペイロードに対してのみサポートされています。ペイロード XML の下にある業界標準のスキーマ・ロケーション・ポインターは、スキーマ・ベースの妥当性検査に利用されます。オプションで、ペイロードの妥当性検査を行うために、スキーマを該当する Web サービス接続と関連付けることができます。明示的に Web サービス接続と関連付けたスキーマは、ペイロード XML の下に配置されたスキーマに優先します。ペイロード XML にスキーマ・ロケーション・ポインターがない場合は、Web サービス接続の下のスキーマを関連付けます。Web サービスの要求および応答のルーティング・オブジェクト属性は、次のとおりです。

- **ResponseValidation** – 応答文書の妥当性検査を行わない場合は、この属性の値をターゲット・サイドで「No」に設定します。この属性のデフォルト値は、「Yes」です。
- **ContentValidation** – この属性を使用すると、ペイロード XML でのコンテンツ妥当性検査を使用可能または使用不可にすることができます。デフォルトでは、コンテンツ妥当性検査は使用可能になっています。これを「No」に設定すると、文法の妥当性検査が実行されます。

アクション SOAP 本体には、次のステップが含まれています。ステップは順番に実行されます。

1. **com.ibm.bcg.validation.ValidationFactory** – Web サービス要求の妥当性検査を実行します。
2. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway に必要な処理を実行します。これが最後のステップで、コンソールにより既存のアクションまたは新規作成されたアクションに自動的に追加されます。このステップは、構成済みハンドラー・リストには表示されません。

SOAP エンベロープの下のペイロードの妥当性検査のフィーチャーを組み込むように WebSphere Partner Gateway をアップグレードするには、「E/A 管理ガイド」を参照してください。

## SOAP エンベロープ解除

SOAP エンベロープをエンベロープ解除し、さらなる処理のために SOAP 本体を導入する必要があります。SOAP エンベロープをエンベロープ解除するためのルーティング・オブジェクト属性は、次のとおりです。

- **SOAP エンベロープのエンベロープ解除 (De-Envelope SOAP Envelope)** - 非同期通信のみをサポートします。これは一方向の Web サービス基本プロファイル・サポートであるため、SOAP 障害または SOAP 応答は戻されません。同期通信の場合、文書に対する SOAP エンベロープのエンベロープ解除は失敗し、エラー・イベントがログに記録されます。
- **エンベロープ解除された文書の再ルーティング (Re-route De-enveloped Document)** - これは、**SOAP エンベロープのエンベロープ解除**アクションの、リンクされたルーティング・オブジェクト属性です。ルーティング・オブジェクト属性が「はい (Yes)」に設定されている場合、**SOAP エンベロープのエンベロープ解除**アクションは、SOAP エンベロープから抽出された SOAP 本体を、新規文

書として WebSphere Partner Gateway に導入しなければなりません。さらに、添付ファイルも新規文書として導入する必要があります。新たに導入された文書はすべて、パッケージ N/A の下に分類されます。それらをさらにルーティングするためには、抽出されたペイロードおよび添付文書用の N/A パッケージ・ベースのチャネルを構成する必要があります。

- **ConsumePayload** - この属性は「**エンベロープ解除文書の転送**」属性にリンクしています。抽出後にペイロードを抑制する場合に使用します。この属性の値および「**エンベロープ解除文書の転送**」の値を「はい」に設定した場合、ペイロードは SOAP エンベロープから抽出されず、送信もされません。添付ファイルは単独で送信されます。この属性を「いいえ」に設定し、「**エンベロープ解除文書の転送**」を「はい」に設定した場合は、ペイロードと添付ファイルが別個に送信されます。この属性のデフォルト値は、「いいえ」です。

「SOAP エンベロープのエンベロープ解除」アクションには、次のステップが含まれています。ステップは順番に実行されます。

1. **com.ibm.bcg.validation.SOAPDeEnveloperFactory** – Web サービス要求の妥当性検査を行い、SOAPDeEnveloper ハンドラーを戻します。
2. **com.ibm.bcg.outbound.OutboundDocFactory** - 常に必須です。ターゲット文書に対して WebSphere Partner Gateway に必要な処理を実行します。これが最後のステップで、コンソールにより既存のアクションまたは新規作成されたアクションに自動的に追加されます。このステップは、構成済みハンドラー・リストには表示されません。

添付ファイル付きの SOAP をエンベロープ解除し、SOAP 本体のペイロードではなく、添付ファイルのみを送信する場合の構成は以下のようになります。

- bcg.soap.ConsumePayload = Y (デフォルトではこの値は N です)
- bcg.soap.Re-RouteDe-EnvelopedDocument = Y (デフォルトではこの値は Y です)

添付ファイル付きの SOAP をエンベロープ解除し、ペイロードと添付ファイルを別個に送信する場合の構成は以下のようになります。

- bcg.soap.ConsumePayload = N (デフォルトではこの値は N です)
- bcg.soap.Re-RouteDe-EnvelopedDocument = Y (デフォルトではこの値は Y です)

SOAP エンベロープの下のペイロードの妥当性検査のフィーチャーを組み込むように WebSphere Partner Gateway をアップグレードするには、「*WebSphere Partner Gateway E/A 管理ガイド*」を参照してください。

## ユーザー定義のアクションの変更

### このタスクについて

ユーザー定義のアクションを構成するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**アクション**」をクリックします。
2. 構成するユーザー定義のアクションの名前の横にある「**詳細の表示**」アイコンをクリックします。

   アクションが、そのアクションの構成済みハンドラー (アクション・ステップ) のリストと共にリストされます。

3. 変更する各アクションに対して、以下のステップを 1 つ以上実行します。
   a. 「**使用可能リスト**」から関連付けられたハンドラーを選択し、「**追加**」をクリックして、ステップを追加します。ハンドラーが「**構成済みリスト**」に移動します。
   b. 「**構成済みリスト**」からハンドラーを選択し、「**除去**」をクリックして、ハンドラーを除去します。ハンドラーが「**使用可能リスト**」に移動します。
   c. ハンドラーを選択し、「**上に移動**」または「**下に移動**」をクリックして、ハンドラーが呼び出される順序を変更します。
   d. ハンドラーを選択し、「**繰り返し**」をクリックして、ハンドラーが複数回処理されるようにします。

      アクションに対して構成されているハンドラーがすべて呼び出され、それぞれのハンドラーに関連付けられた各ステップが「**構成済みリスト**」に表示されている順序で実行されます。
   e. 「**構成済みリスト**」からハンドラーを選択し、「**構成**」をクリックして、ハンドラーを構成します。構成可能な属性のリストが表示されます。
4. 「**保存**」をクリックします。

## アクションの作成

以下のいずれかの方法でアクションを作成できます。

- 新規アクションを作成し、そのアクションにハンドラーを関連付けます。
- 製品提供のアクションをコピーし、必要に応じてそのアクションに関連付けられているハンドラーを変更します。

### 新規アクションの作成

#### このタスクについて

新規アクションを作成するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**アクション**」をクリックします。
2. 「**作成**」をクリックします。
3. アクションの名前を入力します。このフィールドは必須です。
4. (オプション) アクションの説明を入力します。
5. アクションが使用可能かどうかを指定します。
6. アクションの一部として呼び出されるステップごとに、「**使用可能リスト**」から関連付けられたハンドラーを選択し、「**追加**」をクリックして、そのハンドラーを追加します。ハンドラーが「**構成済みリスト**」に移動します。

   アクションは、「**構成済みリスト**」に表示されている順に各ハンドラーを呼び出します。どのハンドラーも正しい順序に並んでいることを確認してください。「**上に移動**」または「**下に移動**」を使用して、ハンドラーの順序を変更するか、または「**繰り返し**」を使用して、ハンドラーが複数回処理されるようにします。
7. 「**構成済みリスト**」からハンドラーを選択し、「**構成**」をクリックして、ハンドラーを構成します。構成可能な属性のリストが表示されます。
8. 「**保存**」をクリックします。

## アクションのコピー
### このタスクについて

既存のアクションをコピーすることにより、アクションを作成するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**アクション**」をクリックします。
2. 「アクション」リストで、コピーするアクションの横にある「**コピー**」アイコンをクリックします。
3. アクションの名前を入力します。このフィールドは必須です。
4. (オプション) アクションの説明を入力します。
5. アクションが使用可能かどうかを指定します。
6. 「**構成済みリスト**」に既に 1 つ以上のステップが表示されていることに注意してください。これが、コピーしたアクションに関連付けられているステップです。例えば、製品が提供する「RosettaNet プロセスの内部パートナーによるキャンセル」アクションのクローンを作成した場合は、以下のように使用可能な構成済みのハンドラーのリストが表示されます。

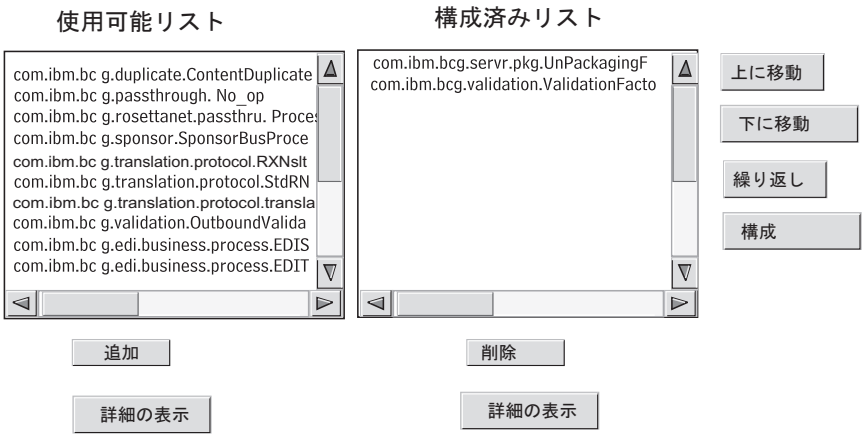



*図 19. アクションのクローン作成*

「**構成済みリスト**」を変更するには、以下のステップを 1 つ以上実行します。

a. 「**使用可能リスト**」から関連付けられたハンドラーを選択し、「**追加**」をクリックして、ステップを追加します。ハンドラーが「**構成済みリスト**」に移動します。

b. 「**構成済みリスト**」から関連付けられたハンドラーを選択し、「**削除**」をクリックして、ステップを削除します。ハンドラーが「**使用可能リスト**」に移動します。

c. ハンドラーを選択し、「**上に移動**」または「**下に移動**」をクリックして、ハンドラーが呼び出される順序を変更します。

   アクションに対して構成されているハンドラーがすべて呼び出され、それぞれのハンドラーに関連付けられた各ステップが「**構成済みリスト**」に表示されている順序で実行されます。

d. 「**構成済みリスト**」からステップを選択し、「**構成**」をクリックして、ステップを構成します。構成可能な属性のリストが表示されます。

7. 「**保存**」をクリックします。

# 第 9 章 文書タイプの構成

この章では、外部パートナーおよびバックエンド・アプリケーションと交換する EDI 以外の文書の構成方法について説明します。EDI 文書の文書タイプおよびインタラクションの構成方法 (パススルー中の EDI 文書は除く) については、 175 ページの『第 10 章 EDI 文書フローの構成』で説明します。 175 ページの『第 10 章 EDI 文書フローの構成』では、XML およびレコード指向データ (ROD) 文書の文書タイプとインタラクションを構成する方法についても説明します。

この章では以下のトピックを扱います。

- 『文書タイプの概要』
- 113 ページの『バイナリー文書』
- 113 ページの『パススルー・アクションによる EDI 文書』
- 115 ページの『RosettaNet 文書』
- 130 ページの『ebMS 文書』
- 152 ページの『Web サービス』
- 157 ページの『cXML 文書』
- 162 ページの『カスタム XML 文書処理』

**注:** WebSphere Partner Gateway の構成変更を行う場合は、必ず、コミュニティー・コンソールにログインしたときと同じブラウザー・インスタンスを使用してください。複数のブラウザー・インスタンスを同時に使用すると、構成変更が無効になる可能性があります。

## 文書タイプの概要

文書定義は、少なくともパッケージ、プロトコル、文書タイプで構成されています。プロトコルによっては、アクティビティー、アクション、シグナルを指定できる場合もあります。文書定義では、WebSphere Partner Gateway で処理される文書のタイプを指定します。

パッケージ化とは、AS2 などの仕様に従って文書をパッケージ化するために必要なロジックです。プロトコル・フローとは、EDI-X12 など特定のプロトコルに準拠する文書を処理するために必要なロジックです。文書タイプとは、文書がどのようになっているかを記述したものです。

以下のセクションでは、内部パートナーとパートナー間の文書タイプを設定するためのステップ全体について概説します。

### ステップ 1: 文書定義が使用可能であることを確認する

#### このタスクについて

(システムによって事前に定義された文書の) 文書定義が存在しているかを確認します。文書フローが存在しない場合は、必要なファイルをアップロードするか、またはカスタム定義を手動で作成して、文書フローを作成します。

文書定義を作成するときに、いくつかの属性を変更することができます。属性は、検証や暗号化の検査、再試行カウントなどのさまざまな文書処理やルーティングの機能を実行する目的で使用されます。 文書定義レベルで設定した属性は、関連するパッケージ、プロトコル、または文書タイプのグローバル設定となります。使用可能な属性は、文書定義によって異なります。例えば、EDI 文書定義の属性は、RosettaNet 文書定義の属性とは異なります。

例えば、AS パッケージの「**応答のための時間**」値を指定すると、AS によってパッケージ化されたすべての文書にこの値が適用されます。(「**応答のための時間**」は、元の要求を再送するまでに、MDN (メッセージ処理通知) 確認通知を待つ時間を示します。) その後、「**応答のための時間**」属性を B2B 機能レベルで設定すると、文書定義レベルで設定された値がこの設定によってオーバーライドされます。

文書定義のすべてのレベルで設定可能な属性では、文書タイプ・レベルで設定された値がプロトコル・レベルで設定された値よりも優先し、プロトコル・レベルで設定された属性がパッケージ・レベルで設定された属性よりも優先します。

インタラクションを作成する前に、「文書定義の管理」ページに文書タイプをリストする必要があります。文書定義を管理するには、*「WebSphere Partner Gateway E/A 管理ガイド」の『ハブ管理者のタスク』の章*

## ステップ 2: 対話を作成する

### このタスクについて

定義済みの文書タイプのインタラクションを作成します。対話では、文書に関して実行するアクションを WebSphere Partner Gateway に指定します。交換によっては、(パートナーまたは内部パートナーから送信されて) ハブで受信される文書を記述するフローと、ハブから (外部パートナーまたは内部パートナーに) 送信される文書を記述するフローの 2 つのフローのみが必要な場合があります。ただし、ハブで送受信する EDI 交換が個々のトランザクションに分割されたり、確認通知を必要としたりするものである場合は、実際には EDI 交換を実行する対話を複数に分けて作成します。対話を管理するには、*「WebSphere Partner Gateway E/A 管理ガイド」の『ハブ管理者のタスク』の章*を参照してください。

## ステップ 3: パートナーのプロファイル、宛先、および B2B 機能を作成する

### このタスクについて

内部パートナーおよび外部パートナーのパートナー・プロファイルを作成します。(文書の送信場所を決定する) 宛先および B2B 機能を定義して、内部パートナーおよび外部パートナーが送受信できる文書を指定します。「B2B 機能」ページには、既に定義されている文書タイプがすべて表示されます。

B2B 機能レベルで属性を設定できます。このレベルで設定した属性は、文書定義レベルで設定された属性をオーバーライドします。例えば、AS パッケージの「**応答のための時間**」を文書定義レベルで 30 に設定してから、B2B 機能レベルで 60 に設定した場合は、値 60 が使用されます。B2B レベルで設定された属性は、特定のパートナーに合わせて調整できます。

## ステップ 4: 接続をアクティブ化する

### このタスクについて

内部パートナーおよび外部パートナー間の接続をアクティブ化します。使用可能な接続は、作成された対話が基になります。対話は、B2B 機能を基にしています。インタラクションは、使用可能な文書定義によって異なります。

交換によっては、接続が 1 つだけ必要になることがあります。例えば、パートナーが内部パートナーのバックエンド・アプリケーションにバイナリー文書を送信する場合、必要な接続は 1 つのみです。ただし、EDI 交換のうち、エンベロープが解除されるものや、個々のトランザクションが変換されるものでは、複数の接続を確立します。

**注:** そのままの状態でやり取りされる EDI 交換では、必要な接続は 1 つのみです。

属性は接続レベルで設定できます。このレベルで設定された属性は、B2B 機能レベルで設定された属性をオーバーライドします。例えば、AS2 パッケージの「**応答のための時間**」を B2B 機能レベルで 60 に設定してから、120 に設定すると、値 120 が使用されます。接続レベルで属性に値を設定することで、関連するパートナーとアプリケーションのルーティングの要件に応じて、属性をさらに調整することができます。

## フローの例

### このタスクについて

デフォルトでは、複数のパッケージ化方法が使用可能です。文書定義を確立する手順全体を示すために、EDI-X12 標準に準拠する EDI 交換を受信するように、外部パートナーと合意している場合を考えます。パートナーは文書を AS2 パッケージ化内で送信します。ユーザーは交換をパッケージ化しないで (変換しないで) バックエンド・アプリケーションに送信するように指定します。

1. 「文書定義の管理」ページで、(パートナーからハブに流れる文書タイプを記述する) 文書定義が使用可能であるかを確認します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**パッケージ: AS**」の横にある「**展開 (Expand)**」アイコンをクリックします。**EDI-X12** が既にリストされていることに注意してください。
   c. 「**プロトコル: EDI-X12**」の横にある「**展開 (Expand)**」アイコンをクリックします。「**文書タイプ: ISA**」が既にリストされていることに注意してください。
2. 「文書定義の管理」ページがまだ表示されている場合は、2 番目の文書定義 (バックエンド・アプリケーションに流れる文書タイプを記述する) が使用可能であるかを確認します。
   a. 「**パッケージ: なし**」の横にある「**展開 (Expand)**」アイコンをクリックします。**EDI-X12** が既にリストされていることに注意してください。
   b. 「**プロトコル: EDI-X12**」の横にある「**展開 (Expand)**」アイコンをクリックします。「**文書タイプ: ISA**」が既にリストされていることに注意してください。

3. 文書タイプがソース・タイプであるか、それともレシーバー・タイプであるかを記述するインタラクションを作成します。
   a. 「文書定義の管理」ページがまだ表示されている場合は、「**インタラクションの管理**」リンクをクリックします。
   b. 「ソース」列で、「**パッケージ: AS**」、「**プロトコル: EDI-X12 (すべて)**」を展開し、「**文書タイプ: ISA**」をクリックして、ラジオ・ボタンが選択されるようにします。
   c. 「ターゲット」列で、「**パッケージ:なし**」、「**プロトコル: EDI-X12 (すべて)**」を展開し、「**文書タイプ: ISA**」をクリックして、ラジオ・ボタンが選択されるようにします。
   d. この例では、変換は発生しません。したがって、「**変換マップ**」リストで何も選択しないでください。
   e. 「**アクション**」**リスト**から「**パススルー**」を選択します。
   f. 「**保存**」をクリックします。

この時点で、ハブが AS としてパッケージ化された EDI-X12 交換 (ISA 標準) を受け入れることができるように指定されています。また、ハブがパッケージ化しなくても EDI-X12 交換 (ISA 標準) を送信できるように指定されています。さらに、交換する場合に変換が発生しないように指定されています。交換は (AS ヘッダーが削除されたあとに) バックエンド・アプリケーションに単にパススルーされます。

このタイプの交換をハブに送信できるパートナーは、まだ指定されていません。このパートナーは、パートナー・プロファイルおよびパートナーの B2B 機能をセットアップするときに定義します。(内部パートナーのバックエンド・システムのプロファイルおよび B2B 機能も定義します)。これらのタスクを実行したら、パートナーとバックエンド・アプリケーション間の接続を作成します。図 20 に、この例に対応する、パートナーと内部パートナーのバックエンド・アプリケーション間の接続を示します。

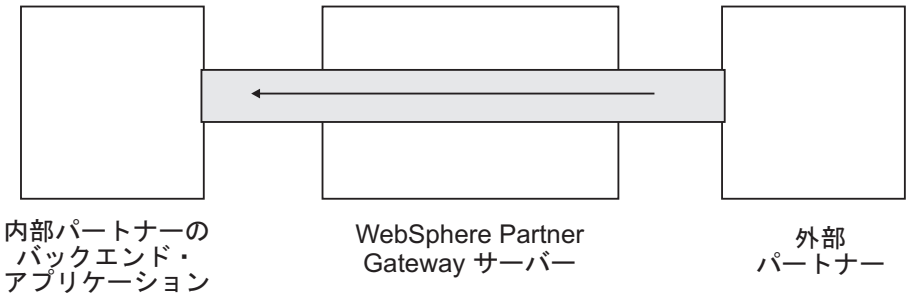



*図 20. パートナーから内部パートナーへの片方向接続*

接続が存在するかどうかは、「接続の管理」ページ (「**アカウント管理**」>「**接続**」>「**パートナー接続**」) を使用して確認します。「接続の管理」ページの「**ソース**」リストでパートナーを、「**ターゲット**」リストで内部パートナーを選択し、「**検索**」をクリックします。使用可能な接続が 1 つリストされます。以降のセクションで説明するように、必要に応じて属性およびアクションを変更できます。

文書定義には 3 つのタイプがあります。コンソールから選択できるシステム提供の定義、定義済みであるにもかかわらずコミュニティー・コンソールに表示されてい

ない定義 (WebSphere Partner Gateway インストール・メディアまたは別の場所からこれらの定義をアップロードします)、およびユーザーが独自に作成する定義です。文書定義のタイプごとに、属性を指定したり、文書タイプを詳細に定義するマップをアップロードしたりすることができます (場合によってはこの作業が必須です)。

## バイナリー文書

バイナリー文書はそのままハブ内をパススルーされるため、外部パートナーと内部パートナーのバックエンド・アプリケーション間のバイナリー文書交換は簡単に処理されます。内部パートナーおよび外部パートナーのプロファイルと B2B 機能を定義してから、これらの間の接続を作成する必要があります。デフォルトの内部パートナーを使用しない場合は、内部パートナーの receiverID を明示的に設定する必要があります。基本認証を使用してバイナリー文書が HTTP トランスポートを通して転送される場合、receiverID は **X-aux-receiver-id** 属性を通して渡すことができます。バイナリー文書は、外部パートナーにより FTP プロトコルを使用してハブに送信することもできます。AS、なし、および バックエンド統合パッケージに対してバイナリー・プロトコルは既に使用可能であるため、 109 ページの『ステップ 1: 文書定義が使用可能であることを確認する』は既に実行済みです。

**注:** 任意のレベル (パッケージ、プロトコル、または文書タイプ) で属性を追加して、デフォルト処理を変更するには、「**属性値の編集**」アイコンをクリックします。デフォルトでは、どの属性もバイナリー・プロトコルまたは文書タイプに関連していません。

同様に、バイナリー文書を含む 4 つの対話がデフォルトで提供されていて、これらの対話には 110 ページの『ステップ 2: 対話を作成する』を実行する必要がありません。対話は以下の交換用に提供されます。

*表 5. 製品で提供されるインタラクション*

| ソース・パッケージ/プロトコル/文書タイプ | ターゲット・パッケージ/プロトコル/文書タイプ |
|---|---|
| AS/バイナリー/バイナリー | バックエンド統合/バイナリー/バイナリー |
| バックエンド統合/バイナリー/バイナリー | AS/バイナリー/バイナリー |
| AS/バイナリー/バイナリー | なし/バイナリー/バイナリー |
| なし/バイナリー/バイナリー | AS/バイナリー/バイナリー |

バイナリー文書の交換では、以下の処理を実行する必要があります。

- 110 ページの『ステップ 3: パートナーのプロファイル、宛先、および B2B 機能を作成する』 ( 25 ページの『第 3 章 パートナーの作成とセットアップ』、および 227 ページの『第 11 章 宛先の作成』を参照)
- 111 ページの『ステップ 4: 接続をアクティブ化する』 ( 253 ページの『第 12 章 接続の管理』を参照)

## パススルー・アクションによる EDI 文書

WebSphere Partner Gateway には、EDI 交換のエンベロープを解除して、変換する機能があります (プロセスについては、 175 ページの『第 10 章 EDI 文書フローの構成』を参照)。

図 21 に、パートナーから内部パートナーにパススルーされている EDI 交換のフローを示します。

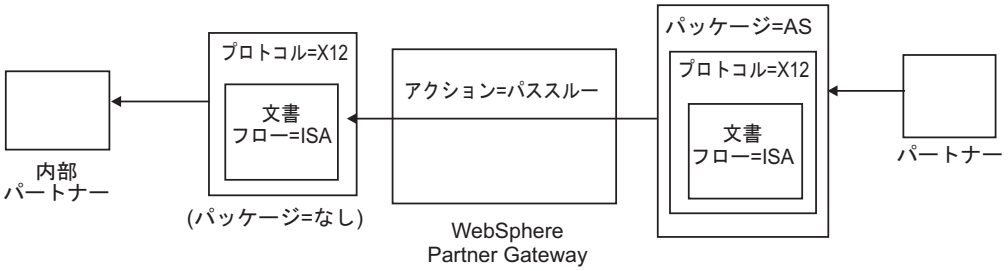



*図 21. パススルー・アクションによる着信 EDI 交換*

この例では AS2 ヘッダーが削除されますが、それ以外は交換がそのまま残り、システムを経由して内部パートナーの宛先に流れます。

WTX (EDI から Any) を使用した EDI トランザクションの同期変換では、トランザクションが複数の出力を持つ場合に、再送信フラグに基づいて、子が直接アウトバウンド・ワークフローに渡されるか、固定のインバウンド・ワークフローに再送信され、新しいチャネルにパススルーされます。非同期の場合、WTX は EDI トランザクションをエンベロープ対象として WPG に送信します。2 つのチャネル (<none>/<EDI Dictionary>/<EDI document > パススルーによる {EDI Trx} および <NA>/<EDI interchange>/<,EDI ISA/UNB>) から <Any Package>/<EDI X12/<FACT>/<EDI ISA/UNB に対する接続を、アクションをパススルーとして設定する必要があります。

# 文書定義の作成

## このタスクについて

EDI パススルー交換の文書タイプは、「文書定義の管理」ページに (デフォルトで) 表示されています ( 111 ページの『フローの例』を参照)。デフォルト値を持つ属性を変更したり、値が割り当てられていない属性を設定する場合は、「文書定義の管理」ページを使用して、このタスクを実行できます。

例えば、AS でパッケージ化された EDI 文書の「**応答のための時間**」属性を変更するとします。これを行うには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**パッケージ: AS**」の横にある「**属性値の編集**」アイコンをクリックします。
3. 「**文書定義コンテキスト属性**」というタイトルのページのセクションが表示されるまでスクロールダウンします。
4. 「**応答のための時間**」行の「**更新**」列に、別の値を入力します。
5. 「**保存**」をクリックします。

この例では、パッケージ属性を変更しました。プロトコル (EDI-X12 など) および文書タイプ (ISA など) の属性は、パススルー・アクションには関係しません。このパッケージ属性は、AS パッケージ化でラップされたすべての文書に適用されます。

## インタラクションの作成

### このタスクについて

パススルー・アクションでの EDI 交換の対話を作成するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」リンクをクリックします。
3. 「**ソース**」の下で、「**パッケージ: AS**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
4. 「**ターゲット**」の下で、「**パッケージ: なし**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
5. 「**アクション**」リストから「**パススルー**」を選択します。

ステップ 1 から 5 により、WebSphere Partner Gateway は、ソース・パートナーからの AS としてパッケージ化された EDI-X12 交換を受信したり、パッケージ化されていない EDI-X12 交換をターゲット・パートナーに送信したり、ソースからターゲットに交換をパススルーしたりできるようになりました。

なし/EDI-X12/ISA としてパッケージ化されたソース文書および AS/EDI-X12/ISA としてパッケージ化されたターゲット文書を含む対話を設定する場合は、ステップ 3 で「**パッケージ: なし**」を展開し (「**ソース**」列内)、ステップ 4 で「**パッケージ: AS**」 を展開します (「**ターゲット**」列内)。

---

## RosettaNet 文書

RosettaNet は、パートナー間でのビジネス・メッセージの交換をサポートするためのオープン・スタンダードを規定する組織です。RosettaNet について詳しくは、http://www.rosettanet.org を参照してください。この標準には、RosettaNet Implementation Framework (RNIF) および Partner Interface Process (PIP) 仕様が含まれます。RNIF はメッセージ・パッケージ化、転送プロトコル、およびセキュリティーのフレームワークを提供することにより、パートナーのメッセージ交換方法を定義します。公開されているバージョンは 1.1 と 2.0 の 2 つがあります。PIP は、パブリック・ビジネス・プロセス、およびこのプロセスをサポートするための XML ベースのメッセージ・フォーマットを定義します。

WebSphere Partner Gateway では、RNIF 1.1 および 2.0 を使用する RosettaNet メッセージングをサポートします。PIP メッセージを受信すると、ハブはメッセージを検証し、変換して、適切なバックエンド・システムに送信します。 WebSphere Partner Gateway には、変換されたメッセージをバックエンド・システムが処理可能な RosettaNet Service Content (RNSC) メッセージにパッケージ化するためのプロトコルが備わっています。ルーティング情報を提供するためにこれらのメッセージで使用されるパッケージ化については、「*WebSphere Partner Gateway エンタープライズ統合ガイド*」を参照してください。

ハブはバックエンド・システムから RNSC メッセージを受信し、適切な PIP メッセージを作成して、適切な取引先 (パートナー) にメッセージを送信することもできます。使用する RNIF のバージョンおよび PIP 用の文書定義を準備してください。

WebSphere Partner Gateway は RosettaNet メッセージのルーティング機能を提供するだけでなく、処理する各メッセージの状態を維持します。これにより、試行回数が指定されたしきい値に到達するまで、失敗したメッセージを再送信できます。PIP メッセージを配信できない場合は、イベント通知メカニズムによってバックエンド・システムにアラートが送信されます。また、ハブはバックエンド・システムから特定のイベント通知メッセージを受信した場合に、自動的に 0A1 PIP を生成して、適切なパートナーに送信できます。イベント通知については、「*WebSphere Partner Gateway エンタープライズ統合ガイド*」を参照してください。

## RNIF および PIP の文書タイプ・パッケージ

RosettaNet メッセージングをサポートするために、WebSphere Partner Gateway にはパッケージと呼ばれる 2 組の ZIP ファイルが用意されています。RNIF パッケージは、RNIF プロトコルをサポートするために必要な文書定義で構成されます。これらのパッケージは B2BIntegrate ディレクトリーに格納されています。

RNIF V1.1 の場合、パッケージは以下のとおりです。

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip

RNIF V02.00 の場合、パッケージは以下のとおりです。

- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_V02.00.zip

各ペアの最初のパッケージは、パートナーとの RosettaNet 通信をサポートするために必要な文書定義を提供し、2 番目のパッケージは、バックエンド・システムとの RosettaNet 通信をサポートするために必要な文書定義を提供します。

2 組目のパッケージは、PIP 文書タイプ・パッケージで構成されています。各 PIP 文書タイプ・パッケージには、XML ファイルが格納された Packages ディレクトリー、および XSD ファイルが格納された GuidelineMaps ディレクトリーが含まれます。XML ファイルでは、WebSphere Partner Gateway が PIP を処理する方法、および交換されるメッセージや信号を定義する文書定義を指定します。XSD ファイルでは、PIP メッセージのフォーマットを指定し、メッセージ内の XML エレメントの許容値を定義します。0A1 PIP の ZIP ファイルには、0A1 文書を作成するためのテンプレートとしてハブが使用する XML ファイルも含まれています。

WebSphere Partner Gateway が PIP 文書タイプ・パッケージを提供している PIP は、次のとおりです。

- PIP 0A1 Notification of Failure v1.0
- PIP 0A1 Notification of Failure V02.00.00
- PIP 2A1 Distribute New Product Information V02.00.00
- PIP 2A12 Distribute Product Master V01.03.00
- PIP 3A1 Request Quote V02.00.00
- PIP 3A2 Request Price and Availability R02.01.00
- PIP 3A4 Request Purchase Order V02.02.00
- PIP 3A4 Request Purchase Order V02.00

- PIP 3A5 Query Order Status R02.00.00
- PIP 3A6 Distribute Order Status V02.02.00
- PIP 3A7 Notify of Purchase OrderUpdate V02.02.00
- PIP 3A8 Request Purchase Order Change V01.02.00
- PIP 3A8 Request Purchase Order Change V01.03.00
- PIP 3A9 Request Purchase Order Cancellation V01.01.00
- PIP 3B2 Notify of Advance Shipment V01.01.00
- PIP 3B3 Distribute Shipment Status R01.00.00
- PIP 3B11 Notify of Shipping Order R01.00.00A
- PIP 3B12 Request Shipping Order V01.01.00
- PIP 3B13 Notify of Shipping Order Confirmation V01.01.00
- PIP 3B14 Request Shipping Order Cancellation V01.00.00
- PIP 3B18 Notify of Shipping Documentation V01.00.00
- PIP 3C1 Return Product V01.00.00
- PIP 3C3 Notify of Invoice V01.01.00
- PIP 3C4 Notify of Invoice Reject V01.00.00
- PIP 3C6 Notify of Remittance Advice V01.00.00
- PIP 3C7 Notify of Self-Billing Invoice V01.00.00
- PIP 3D8 Distribute Work in Process V01.00.00
- PIP 4A1 Notify of Strategic Forecast V02.00.00
- PIP 4A3 Notify of Threshold Release Forecast V02.00.00
- PIP 4A4 Notify of Planning Release Forecast R02.00.00A
- PIP 4A5 Notify of Forecast Reply V02.00.00
- PIP 4B2 Notify of Shipment Receipt V01.00.00
- PIP 4B3 Notify of Consumption V01.00.00
- PIP 4C1 Distribute Inventory Report V02.03.00
- PIP 4C1 Distribute Inventory Report V02.01
- PIP 5C1 Distribute Product List V01.00.00
- PIP 5C2 Request Design Registration V01.00.00
- PIP 5C4 Distribute Registration Status V01.02.00
- PIP 5D1 Request Ship From Stock And Debit Authorization V01.00.00
- PIP 6C1 Query Service Entitlement V01.00.00
- PIP 6C2 Request Warranty Claim V01.00.00
- PIP 7B1 Distribute Work in Process V01.00.00
- PIP 7B5 Notify of Manufacturing Work Order V01.00.00
- PIP 7B6 Notify of Manufacturing Work Order Reply V01.00.00

PIP ごとに 4 つの PIP 文書タイプ・パッケージがあります。

- パートナーとの RNIF 1.1 メッセージング用
- バックエンド・システムとの RNIF 1.1 メッセージング用

- パートナーとの RNIF 2.0 メッセージング用
- バックエンド・システムとの RNIF 2.0 メッセージング用

パッケージが WebSphere Partner Gateway とパートナー間のメッセージに対応しているのか、それとも WebSphere Partner Gateway とバックエンド・システム間のメッセージに対応しているかを識別する場合に使用できる特定の命名規則に、各 PIP 文書タイプ・パッケージは従っています。この命名規則により、RNIF のバージョン、PIP、およびパッケージがサポートする PIP のバージョンも識別されます。WebSphere Partner Gateway とパートナー間のメッセージングに使用される PIP 文書タイプ・パッケージのフォーマットは、次のとおりです。

```
BCG_Package_RNIF<RNIF_version>_<PIP><PIP_version>.zip
```

WebSphere Partner Gateway とバックエンド・システム間のメッセージングに使用される PIP 文書タイプ・パッケージのフォーマットは、次のとおりです。

```
BCG_Package_RNSC<Backend_Integration_version>_RNIF<RNIF_version>_
<PIP><PIP_version>.zip
```

例えば、BCG_Package_RNIF1.1_3A4V02.02.zip は、RNIF 1.1 プロトコルを使用してパートナーと WebSphere Partner Gateway 間で送信される、バージョン 02.02 の 3A4 PIP について文書を検証します。バックエンド・システムとの通信に関する PIP 文書タイプ・パッケージの場合は、RosettaNet の内容をバックエンド・システムに送信するためのプロトコルも、パッケージ名で指定する必要があります。これらのメッセージで使用されるパッケージ化については、「*WebSphere Partner Gateway エンタープライズ統合ガイド*」を参照してください。

# 文書定義の作成

## このタスクについて

WebSphere Partner Gateway で RosettaNet メッセージングを処理するには、メッセージの送信に使用される RNIF のバージョンに対応する RNIF パッケージが必要です。WebSphere Partner Gateway がサポートする PIP ごとに、RNIF のバージョンに対応する 2 つの PIP 文書タイプ・パッケージが必要です。例えば、RNIF 2.0 で 3A4 PIP をサポートするには、WebSphere Partner Gateway に次のパッケージが必要です。

- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_V02.00.zip
- BCG_Package_RNIFV02.00_3A4V02.02.zip
- BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip

最初のパッケージはパートナーとの RosettaNet メッセージングを、2 番目のパッケージはバックエンド・システムとの RosettaNet メッセージングをサポートします。3 番目と 4 番目のパッケージは、WebSphere Partner Gateway に、RNIF 2.0 を使用してパートナーとバックエンド・システム間で 3A4 メッセージの受け渡しを行うための機能を提供します。

RosettaNet パッケージをアップロードするには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**パッケージのアップロード/ダウンロード**」をクリックします。

3. 「**WSDL パッケージ**」に対して「**いいえ**」を選択します。
4. 「**参照**」をクリックし、パートナーと通信するための RNIF パッケージを選択します。

   RNIF パッケージは、デフォルトで、インストール・メディアの B2BIntegrate/Rosettanet ディレクトリー内にあります。例えば、RNIF バージョン 2.00 パッケージをアップロードする場合は、B2BIntegrate/Rosettanet ディレクトリーを参照して、Package_RNIF_V0200.zip を選択します。
5. 「**データベースへコミットする**」が「**はい**」に設定されていることを確認します。
6. 「**アップロード**」をクリックします。
7. 「**参照**」を再度クリックし、バックエンド・アプリケーションと通信するための RNIF パッケージを選択します。

   例えば、RNIF バージョン 2.00 パッケージをアップロードする場合は、B2BIntegrate/Rosettanet ディレクトリーを参照して、Package_RNSC_1.0_RNIF_V02.00.zip を選択します。
8. 「**アップロード**」をクリックします。

   パートナーまたはバックエンド・システムと通信するために必要なパッケージは、システムにインストールされました。「文書定義の管理」ページを調べる場合は、パートナーとの通信用のパッケージ化を表す「**パッケージ: RNIF/プロトコル: RosettaNet (Package: RNIF/Protocol: RosettaNet)**」、およびバックエンド・アプリケーションとの通信用のパッケージ化を表す「**パッケージ: バックエンド統合/プロトコル: RNSC (Package: Backend Integration/Protocol: RNSC)**」の項目を参照します。
9. サポートする PIP ごとに、以下のステップを実行します。PIP およびサポートする RNIF のバージョンに対応する PIP 文書タイプ・パッケージをアップロードします。例えば、3C6 PIP (送金通知の通知) をアップロードしてパートナーに送信するには、以下のステップを実行します。
   a. 「**参照**」をクリックし、B2BIntegrate/Rosettanet ディレクトリーから BCG_Package_RNIFV02.00_3C6V02.02 を選択します。
   b. 「**データベースへコミットする**」が「**はい**」に設定されていることを確認します。
   c. 「**アップロード**」をクリックします。

   3C6V02.02 PIP が、「文書定義の管理」ページの「**パッケージ: RNIF/プロトコル: RosettaNet (Package: RNIF/Protocol: RosettaNet)**」の下に文書タイプとして表示されます。アクティビティー、アクション、および 2 つのシグナルも表示されます。これらは PIP のアップロードに含まれます。

   3A6 PIP をアップロードしてバックエンド・アプリケーションに送信するには、以下のステップを実行します。
   a. 「**参照**」をクリックし、BCG_Package_RNSC1.0_RNIFV02.00_3C6V02.02.zip を選択します。
   b. 「**データベースへコミットする**」が「**はい**」に設定されていることを確認します。

c. 「**アップロード**」をクリックします。

3C6V02.02 PIP が、「文書定義の管理」ページの「**パッケージ: バックエンド統合/プロトコル: RNSC (Package: Backend Integration/Protocol: RNSC)**」の下に文書タイプとして表示されます。 使用する PIP または PIP のバージョンに対応するパッケージが WebSphere Partner Gateway に用意されていない場合は、独自のパッケージを作成して、アップロードできます。詳しくは、 389 ページの『PIP 文書定義パッケージの作成』を参照してください。

## 属性値の構成

### このタスクについて

PIP 文書定義の場合、ほとんどの属性値は既に設定されているため、設定する必要はありません。ただし、以下の属性を設定する必要があります。

RNIF (1.0) パッケージ

- **GlobalSupplyChainCode** - パートナーが使用するサプライ・チェーンのタイプを識別します。タイプは電子部品、情報技術、および半導体製造です。この属性にはデフォルト値がありません。

RNIF (V02.00) パッケージ

- **暗号化** - PIP のペイロードを暗号化するか、コンテナーとペイロードを暗号化するか、または暗号化しないかを設定します。デフォルト値は「なし」です。
- **同期応答が必要** - パートナーが受信確認通知の受信を必要とする場合は、「はい」に設定します。200 を要求する場合は、「いいえ」に設定します。
- **同期サポートあり** - PIP が同期メッセージ交換をサポートするかどうかを設定します。デフォルト値は「いいえ」です。

WebSphere Partner Gateway が PIP 文書タイプ・パッケージを提供している PIP は、同期されないことに注意してください。したがって、これらの PIP の「同期応答が必要」および「同期サポートあり」属性を変更する必要はありません。

**注:** 「同期応答が必要」属性の動作は、1 方向 PIP と 2 方向 PIP では異なります。2 方向 PIP の場合、「同期応答が必要」を「いいえ」に設定すると、この設定は「受信の否認防止」の「はい」設定よりも優先します。例えば、次の設定を使用して 3A7 を送信するとします。

- SiqReq=Y
- NonRepofRec=Y
- SyncSupported=Y
- SyncAckReq=N

2 方向 PIP の場合は、着信文書に関するエラー・メッセージが表示されます。ただし、1 方向 PIP の場合は、コンソールに着信文書が表示され、0KB 200 がパートナーに戻されます。

属性を設定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。

2. 「**展開**」アイコンをクリックして個々にノードを適切な文書定義レベルまで展開するか、「**すべて**」を選択して表示されたすべての文書定義のノードを展開します。
3. 「**アクション**」列で、編集するパッケージ(「パッケージ: RNIF (1.1)」や「パッケージ: RNIF (V02.00)」など) の「**属性値の編集**」アイコンをクリックします。
4. 「**文書定義コンテキスト属性**」セクションで、設定する属性の「**更新**」列に移動し、値を選択するか、または新しい値を入力します。設定する属性ごとに、この手順を繰り返します。
5. 「**保存**」をクリックします。

**注:** ソースまたはターゲットの「**属性**」をクリックしてから、「**更新**」列で値を入力するかまたは値を変更して、RosettaNet 属性を接続レベルで更新することもできます。 254 ページの『属性の指定または変更』を参照してください。

## インタラクションの作成

### このタスクについて

次のプロセスでは、バックエンド・システムとパートナーとの間のインタラクションを作成する方法について説明します。送信する PIP および受信する PIP ごとに、対話を 1 つ作成する必要があることに注意してください。

開始する前に、適切な RNIF 文書定義がアップロードされ、使用する PIP に対応したパッケージがアップロードされていることを確認してください。0A1 PIP (Notification of Failure) を生成する機能が必要な場合は、その PIP がステップ 9 (119 ページ) の説明に従ってアップロードされていることを確認してください。

特定の PIP の対話を作成するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの作成**」をクリックします。
3. 「**ソース**」ツリーを「**アクション**」レベルまで展開し、「**ターゲット**」ツリーを「**アクション**」レベルまで展開します。
4. ツリー内で、ソース・コンテキストおよびターゲット・コンテキストに使用する文書定義を選択します。例えば、パートナーが 3C6 PIP (1 アクション PIP) を開始する場合は、次の文書定義を選択します。

*表 6. パートナーが開始する 3C6 PIP*

| ソース | ターゲット |
|---|---|
| パッケージ: RNIF (V02.00) | パッケージ: バックエンド統合 (1.0) |
| プロトコル: RosettaNet (V02.00) | プロトコル: RNSC (1.0) |
| 文書タイプ: 3C6 (V01.00) | 文書タイプ: 3C6 (V01.00) |
| アクティビティー: 送金通知の通知 | アクティビティー: 送金通知の通知 |
| アクション: 送金通知の通知アクション | アクション: 送金通知の通知アクション |

バックエンド・システムが 3C6 PIP を開始する場合は、次の文書定義を選択します。

*表 7. バックエンド・システムが開始する 3C6 PIP*

| ソース | ターゲット |
|---|---|
| パッケージ: バックエンド統合 (1.0) | パッケージ: RNIF (V02.00) |
| プロトコル: RNSC (1.0) | プロトコル: RosettaNet (V02.00) |
| 文書タイプ: 3C6 (V01.00) | 文書タイプ: 3C6 (V01.00) |
| アクティビティー: 送金通知の通知 | アクティビティー: 送金通知の通知 |
| アクション: 送金通知の通知アクション | アクション: 送金通知の通知アクション |

パートナーが 3A4 などの 2 アクション PIP を開始する場合は、最初のアクションに次の文書定義を選択します。

*表 8. パートナーが開始する 3A4 PIP*

| ソース | ターゲット |
|---|---|
| パッケージ: RNIF (V02.00) | パッケージ: バックエンド統合 (1.0) |
| プロトコル: RosettaNet (V02.00) | プロトコル: RNSC (1.0) |
| 文書タイプ: 3A4 (V02.02) | 文書タイプ: 3A4 (V02.02) |
| アクティビティー: 仕入れ注文の要求 | アクティビティー: 仕入れ注文の要求 |
| アクション: 仕入れ注文の要求アクション | アクション: 仕入れ注文の要求アクション |

バックエンド・システムが 2 アクション 3A4 PIP を開始する場合は、最初のアクションに次の文書定義を選択します。

*表 9. バックエンド・システムが開始する 3A4 PIP*

| ソース | ターゲット |
|---|---|
| パッケージ: バックエンド統合 (1.0) | パッケージ: RNIF (V02.00) |
| プロトコル: RNSC (1.0) | プロトコル: RosettaNet (V02.00) |
| 文書タイプ: 3A4 (V02.02) | 文書タイプ: 3A4 (V02.02) |
| アクティビティー: 仕入れ注文の要求 | アクティビティー: 仕入れ注文の要求 |
| アクション: 仕入れ注文の要求アクション | アクション: 仕入れ注文の要求アクション |

5. 「アクション」フィールドで、「**RosettaNet と RosettaNet サービス・コンテンツの間の双方向変換 (検証あり)**」を選択します。
6. 「**保存**」をクリックします。
7. 2 アクション PIP を設定する場合は、必要なステップを繰り返して、2 番目のアクション用の対話を作成します。例えば、パートナーが開始する 3A4 PIP の 2 番目のアクションに対して、次の文書定義を選択します。このアクションで、バックエンド・システムは応答を送信します。

*表 10. パートナーが開始する 3A4 PIP (2 番目のアクション)*

| ソース | ターゲット |
|---|---|
| パッケージ: バックエンド統合 (1.0) | パッケージ: RNIF (V02.00) |
| プロトコル: RNSC (1.0) | プロトコル: RosettaNet (V02.00) |
| 文書タイプ: 3A4 (V02.02) | 文書タイプ: 3A4 (V02.02) |
| アクティビティー: 仕入れ注文の要求 | アクティビティー: 仕入れ注文の要求 |

*表 10. パートナーが開始する 3A4 PIP (2 番目のアクション) (続き)*

| ソース | ターゲット |
|---|---|
| アクション: 仕入れ注文の確認アクション | アクション: 仕入れ注文の確認アクション |

バックエンド・システムが開始する 3A4 PIP の 2 番目のアクションに対して、次の文書定義を選択します。

*表 11. バックエンド・システムが開始する 3A4 PIP (2 番目のアクション)*

| ソース | ターゲット |
|---|---|
| パッケージ: RNIF (V02.00) | パッケージ: バックエンド統合 (1.0) |
| プロトコル: RosettaNet (V02.00) | プロトコル: RNSC (1.0) |
| 文書タイプ: 3A4 (V02.02) | 文書タイプ: 3A4 (V02.02) |
| アクティビティー: 仕入れ注文の要求 | アクティビティー: 仕入れ注文の要求 |
| アクション: 仕入れ注文の確認アクション | アクション: 仕入れ注文の確認アクション |

8. 0A1 Notification of Failure を生成する場合は、XMLEvent の対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。
   c. 「**ソース**」ツリーを「**文書タイプ**」レベルまで展開し、「**ターゲット**」ツリーを「**文書タイプ**」レベルまで展開します。
   d. 以下の文書定義を選択します。

*表 12. XML Event 文書定義*

| ソース | ターゲット |
|---|---|
| パッケージ: バックエンド統合 (1.0) | パッケージ: バックエンド統合 (1.0) |
| プロトコル: XMLEvent (1.0) | プロトコル: XMLEvent (1.0) |
| 文書タイプ: XMLEvent (1.0) | 文書タイプ: XMLEvent (1.0) |

   e. 「アクション」フィールドで、「**パススルー**」を選択します。
   f. 「**保存**」をクリックします。
9. 0A1 RNSC に対する XMLEvent の対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。
   c. 「**ソース**」ツリーを「**文書タイプ**」レベルまで展開し、「**ターゲット**」ツリーを「**アクティビティー**」レベルまで展開します。
   d. 以下の文書定義を選択します。

*表 13. 0A1 に対する XML Event の文書定義*

| ソース | ターゲット |
|---|---|
| パッケージ: バックエンド統合 (1.0) | パッケージ: バックエンド統合 (1.0) |
| プロトコル: XMLEvent (1.0) | プロトコル: RNSC (1.0) |
| 文書タイプ: XMLEvent (1.0) | 文書タイプ: 0A1 (V02.00) |
| | アクティビティー: 障害通知の配布 |

e. 「アクション」フィールドで、「**RosettaNet と XML の間の双方向変換 (検証あり)**」を選択します。

f. 「**保存**」をクリックします。

**注:** XMLEvent の使用可能または使用不可にするには、「*エンタープライズ統合ガイド*」の『XMLEvent の使用可能化または使用不可化』のセクションを参照してください。

## RosettaNet 文書の表示

### このタスクについて

RosettaNet ビューアーは、RosettaNet 文書に関する情報を表示します。ロー文書とそれに関連する文書処理の詳細およびイベントを、特定の検索条件を使用して表示することができます。文書が正常に配信されたかどうかを調べたり、問題の原因を判別するときに、この情報が役に立ちます。

RosettaNet ビューアーを表示するには、以下を実行します。

1. 「**ビューアー**」>「**RosettaNet ビューアー**」をクリックします。
2. 表 14の説明に従って、リストから適切な検索基準を選択します。

*表 14. RosettaNet 検索条件*

| 値 | 説明 |
|---|---|
| 開始日時 | 開始されたプロセスの日時。 |
| 終了日時 | 終了されたプロセスの日時。 |
| ソースおよびターゲット・パートナー | ソース (開始側) およびターゲット (受信側) パートナーを識別します (内部パートナーのみ)。 |
| パートナー | 検索がすべてのパートナーに適用されるか、あるいは内部パートナーのみに適用されるかを示します。 |
| 自分の役割は以下 | パートナーがターゲットまたはソースである文書の検索が行われるかどうかを示します。 |
| ソース・ビジネス ID | 開始側パートナーのビジネス識別番号。例えば、DUNS など。 |
| 動作モード | 実動またはテスト。テストは、テスト動作モードをサポートしているシステムでのみ使用可能です。 |
| プロトコル | パートナーが使用できるプロトコル。 |
| 文書タイプ | 特定のビジネス・プロセス。 |
| プロセス・インスタンス ID | プロセスに割り当てられた固有の識別番号。基準にはアスタリスク (*) のワイルドカードを含めることができます。 |
| ソート順 | 以下の順に結果をソート:<br>• ターゲット・タイム・スタンプ<br>• 文書タイプ<br><br>デフォルトは、ターゲット・タイム・スタンプです。 |
| 降順または昇順 | 降順は、最新のタイム・スタンプ、または先頭のアルファベットの初めを表示します。<br><br>昇順は、最も古いタイム・スタンプ、または先頭のアルファベットの終わりを表示します。<br><br>デフォルトは、降順です。 |
| ページごとの結果件数 | 1 ページに表示される結果の数を指定します。 |

3. 「**検索**」をクリックします。

## CIDX 文書

CIDX は堅固な産業団体および標準化団体で、その任務は化学薬品会社とその取引相手の間でビジネスを電子的に行う容易さ、速度、およびコストを改善することです。CIDX は、化学業界の標準を推進するさまざまなイニシアチブを持っています。本書では、CIDX の Chem eStandards イニシアチブに焦点を当てます。Chem eStandard は、化学薬品の購入、販売、および配送を専門として開発されたデータ交換の統一標準です。Chem eStandards は以下のもので構成されます。

- ChemXML または Chem eStandards メッセージ仕様: v2.0、v2.0.1、v2.0.2、v3.0 および v4.0
- Chem eStandards エンベロープおよびセキュリティー仕様: v2.0 および v3.0

パッケージ化の場合、CIDX は常に RNIF 1.1 を使用します。RNIF 1.1 は常に非同期であることを覚えておくのは重要です。そのため、CIDX 文書交換は常に非同期です。

CIDX はパッケージ化とトランザクションで構成されるのに対して、RosettaNet はパッケージ化と PIP (partner interchange process) で構成されます。CIDX は RNIF 1.1 パッケージ化を使用します。トランザクションは ChemXML 標準で定義されたとおりです。ChemXML 標準の各バージョンがトランザクションを定義します。特定の ChemXML 標準バージョンで定義された ChemXML のすべてのトランザクションは、ChemXML 標準のトランザクションと同じバージョンです。RosettaNet とは異なり、CIDX は定義を処理するのに規格合致を必要としません。CIDX はそれよりもトランザクションの構造や安全な方法でのメッセージ交換に取り組んでいます。

比較を続けると、RosettaNet は RosettaNet 標準の管理権限であり、同様に CIDX は CIDX 標準の管理権限です。RosettaNet は RNIF パッケージ化および PIP を定義します。RosettaNet メッセージは RNIF 1.1 または RNIF 2.0 を使用できます。RosettaNet が定義した PIP はメッセージ・セットを提供し、コレオグラフィーを処理します。CIDX は常に RosettaNet によって定義された RNIF 1.1 を使用します。CIDX は管理ボディであるため、RNIF エンベロープは Chem eStandards エンベロープおよびセキュリティー仕様によって定義されたとおりに構成される必要があります。この仕様は RosettaNet のインプリメンテーションに基づいています。CIDX は RosettaNet によって定義された PIP を使用しません。その代わりに、CIDX は Chem eStandards メッセージ仕様を使用します。

CIDX について詳しくは、http://www.cidx.org を参照してください。CIDX 標準は、http://www.cidx.org からダウンロードできます。Chem eStandards Envelope and Security バージョン 3.0 は、http://www.cidx.org/Portals/0/Publications/Envelope_and_Security_v3.0.pdf にあります。

WebSphere Partner Gateway では、以下の Chem eStandards がサポートされています。

- Chem eStandards エンベロープおよびセキュリティー仕様 v3.0
- ChemXML または Chem eStandards メッセージ仕様 v4.0

## CIDX の RNIF および PIP 文書タイプ・パッケージ

CIDX は RNIF1.1 を使用します。CIDX をサポートするために、WebSphere Partner Gateway にはパッケージと呼ばれる 2 組の ZIP ファイルが用意されています。RNIF パッケージは、RNIF プロトコルをサポートするために必要な文書定義で構成されます。これらのパッケージは B2BIntegrate ディレクトリーに格納されています。

RNIF V1.1 の場合、パッケージは以下のとおりです。

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip

最初のパッケージは、パートナーとの CIDX 通信をサポートするために必要な文書定義を提供し、2 番目のパッケージは、バックエンド・システムとの CIDX 通信をサポートするために必要な文書定義を提供します。

2 組目のパッケージは、PIP 文書タイプ・パッケージで構成されています。各 PIP 文書タイプ・パッケージには、XML ファイルが格納された Packages ディレクトリー、および XSD ファイルが格納された GuidelineMaps ディレクトリーが含まれます。XML ファイルでは、WebSphere Partner Gateway が PIP を処理する方法、および交換されるメッセージや信号を定義する文書定義を指定します。XSD ファイルでは、PIP メッセージのフォーマットを指定し、メッセージ内の XML エレメントの許容値を定義します。0A1 PIP の ZIP ファイルには、0A1 文書を作成するためのテンプレートとしてハブが使用する XML ファイルも含まれています。

CIDX の場合、WebSphere Partner Gateway は、E41 ChemXML Version 4.0 Order Create および E42 ChemXML Version 4.0 Order Response に対応した文書タイプ・パッケージを提供します。

提供される CIDX パッケージの命名規則は、RosettaNet 用に提供されたパッケージのものと同じです。例えば、BCG_Package_RNIF1.1_E414.0.zip は、RNIF1.1 を使用してパートナーと WPG 間で送信される、v4.0 の E41 PIP について文書を検証します。

## 文書定義の作成

### このタスクについて

WebSphere Partner Gateway で CIDX メッセージングを処理するには、メッセージの送信に使用されるバージョンの RNIF に対応する RNIF パッケージが必要です。WebSphere Partner Gateway がサポートする PIP ごとに、RNIF のバージョンに対応する 2 つの PIP 文書タイプ・パッケージが必要です。例えば、RNIF1.1 で E41 PIP をサポートするには、WebSphere Partner Gateway に次のパッケージが必要です。

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip
- BCG_Package_RNIF1.1_E414.0.zip
- BCG_Package_RNSC1.0RNIF1.1_E414.0.zip

最初のパッケージはパートナーとの CIDX メッセージングを、2 番目のパッケージはバックエンド・システムとの CIDX メッセージングをサポートします。3 番目と 4 番目のパッケージは、WebSphere Partner Gateway に、パートナーとバックエンド間で E41 メッセージの受け渡しを行うための機能を提供します。

CIDX パッケージをアップロードするには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**パッケージのアップロード/ダウンロード**」をクリックします。
3. 「**WSDL パッケージ**」に対して「**いいえ**」を選択します。
4. 「**参照**」をクリックし、パートナーと通信するための RNIF パッケージを選択します。

   RNIF パッケージは、デフォルトで、インストール・メディアの B2BIntegrate/rosettanet ディレクトリー内にあります。例えば、RNIF バージョン 2.00 パッケージをアップロードする場合は、B2BIntegrate/rosettanet ディレクトリーを参照して、Package_RNIF_V0200.zip を選択します。
5. 「**データベースへコミットする**」が「**はい**」に設定されていることを確認します。
6. 「**アップロード**」をクリックします。
7. 「**参照**」を再度クリックし、バックエンド・アプリケーションと通信するための RNIF パッケージを選択します。

   例えば、RNIF バージョン 2.00 パッケージをアップロードする場合は、B2BIntegrate/rosettanet ディレクトリーを参照して、Package_RNSC_1.0_RNIF_V02.00.zip を選択します。
8. 「**アップロード**」をクリックします。

   パートナーまたはバックエンド・システムと通信するために必要なパッケージは、システムにインストールされました。「文書定義の管理」ページを調べる場合は、パートナーとの通信用のパッケージ化を表す「**パッケージ: RNIF/プロトコル: Rosettanet (Package: RNIF/Protocol: Rosettanet)**」、およびバックエンド・アプリケーションとの通信用のパッケージ化を表す「**パッケージ: バックエンド統合/プロトコル: RNSC (Package: Backend Integration/Protocol: RNSC)**」の項目を参照します。
9. サポートする PIP ごとに、PIP およびサポートする RNIF のバージョンに対応する PIP 文書タイプ・パッケージをアップロードします。

   例えば、E41 CIDX PIP (Order Create) をアップロードしてパートナーに送信するには、以下のステップを実行します。

   a. 「**参照**」をクリックし、B2BIntegrate/Rosettanet ディレクトリーから **BCG_Package_RNIF1.1_E414.0.zip** を選択します。
   b. 「**データベースへコミットする**」が「**はい**」に設定されていることを確認します。
   c. 「**アップロード**」をクリックします。

   E41 PIP が、「文書定義の管理」ページの「パッケージ: RNIF/プロトコル: RosettaNet (Package: RNIF/Protocol: RosettaNet)」の下に文書タイプとして表示さ

れます。アクティビティー、アクション、および 2 つのシグナルも表示されます。これらは PIP のアップロードに含まれます。

E41 PIP をアップロードしてバックエンド・アプリケーションに送信するには、以下のステップを実行します。

a. 「**参照**」をクリックし、**BCG_Package_RNSC1.0RNIF1.1_E414.0.zip** を選択します。

b. 「**データベースへコミットする**」が「**はい**」に設定されていることを確認します。

c. 「**アップロード**」をクリックします。

E41 PIP が、「文書定義の管理」ページの「パッケージ: バックエンド統合/プロトコル: RNSC (Package: Backend Integration/Protocol: RNSC)」の下に文書タイプとして表示されます。

## 属性値の構成

### このタスクについて

RNIF 文書定義の場合、ほとんどの属性値は既に設定されているため、構成する必要はありません。ただし、以下の属性を設定する必要があります。

RNIF (1.1) パッケージ

- **GlobalSupplyChainCode** - パートナーが使用するサプライ・チェーンのタイプを識別します。タイプは電子部品、情報技術、および半導体製造です。この属性にはデフォルト値がありません。

属性を設定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**展開**」アイコンをクリックして個々にノードを適切な文書定義レベルまで展開するか、「**すべて**」を選択して表示されたすべての文書定義のノードを展開します。
3. 「**アクション**」列で、編集するパッケージ(「パッケージ: RNIF (1.1)」や「パッケージ: RNIF (V02.00)」など) の「**属性値の編集**」アイコンをクリックします。
4. 「**文書定義コンテキスト属性**」セクションで、設定する属性の「**更新**」列に移動し、値を選択するか、または新しい値を入力します。設定する属性ごとに、この手順を繰り返します。
5. 「**保存**」をクリックします。

**注:** ソースまたはターゲットの「**属性**」をクリックしてから、「**更新**」列で値を入力するかまたは値を変更して、RosettaNet 属性を接続レベルで更新することもできます。 254 ページの『属性の指定または変更』を参照してください。

## インタラクションの作成

### このタスクについて

次のプロセスでは、バックエンド・システムとパートナーとの間のインタラクションを作成する方法について説明します。送信する PIP および受信する PIP ごとに、対話を 1 つ作成する必要があることに注意してください。

開始する前に、適切な RNIF 文書定義がアップロードされ、使用する PIP に対応したパッケージがアップロードされていることを確認してください。

特定の PIP の対話を作成するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの作成**」をクリックします。
3. 「**ソース**」ツリーを「**アクション**」レベルまで展開し、「**ターゲット**」ツリーを「**アクション**」レベルまで展開します。
4. ツリー内で、ソース・コンテキストおよびターゲット・コンテキストに使用する文書定義を選択します。例えば、パートナーが E41 PIP を開始する場合は、次の文書定義を選択します。

*表 15. パートナーが開始する 3C6 PIP*

| ソース | ターゲット |
|---|---|
| パッケージ: RNIF (1.1) | パッケージ： バックエンド統合 (1.1) |
| プロトコル: RosettaNet (1.1) | プロトコル: RNSC (1.0) |
| 文書タイプ: E41 (4.0) | 文書タイプ: E41 (4.0) |
| アクティビティー: OrderCreate | アクティビティー: OrderCreate |
| アクション: Order Create | アクション: Order Create |

パートナーが 3A4 などの 2 アクション PIP を開始する場合は、最初のアクションに次の文書定義を選択します。

*表 16. パートナーが開始する 3A4 PIP*

| ソース | ターゲット |
|---|---|
| パッケージ: RNIF (V02.00) | パッケージ: バックエンド統合 (1.0) |
| プロトコル: RosettaNet (V02.00) | プロトコル: RNSC (1.0) |
| 文書タイプ: 3A4 (V02.02) | 文書タイプ: 3A4 (V02.02) |
| アクティビティー: 仕入れ注文の要求 | アクティビティー: 仕入れ注文の要求 |
| アクション: 仕入れ注文の要求アクション | アクション: 仕入れ注文の要求アクション |

5. 「アクション」フィールドで、「**RosettaNet と RosettaNet サービス・コンテンツの間の双方向変換 (検証あり)**」を選択します。
6. 「**保存**」をクリックします。

# CIDX 文書の表示

## このタスクについて

RosettaNet ビューアーは、CIDX 文書に関する情報を表示します。ロー文書とそれに関連する文書処理の詳細およびイベントを、特定の検索条件を使用して表示することができます。文書が正常に配信されたかどうかを調べたり、問題の原因を判別するときに、この情報が役に立ちます。

RosettaNet ビューアーを表示するには、以下を実行します。

1. 「**ビューアー**」>「**RosettaNet ビューアー**」をクリックします。
2. 該当する検索条件を選択してください。

3. 「**検索**」をクリックします。

# ebMS 文書

ebMS メカニズムは、ebXML 取引先間でビジネス・メッセージを交換するための標準的な方法を提供します。ebXML メッセージング・サービスは、所有テクノロジーおよびソリューションに依存しないでビジネス・メッセージを交換するための信頼できる手段を提供します。このセクションでは、文書定義やこれらの文書のインタラクションをセットアップする方法について説明します。

## 文書定義の作成

### このタスクについて

ebMS メッセージングでは、文書を定義する前に、Collaboration Profile Agreement (CPA) XML ファイルをアップロードする必要があります。

CPA XML ファイルをアップロードするには、以下を実行します。

1. 「**ハブ管理**」 > 「**ハブ構成**」 > 「**ebMS**」をクリックします。
2. 「**CPA のアップロード**」をクリックします。
3. 「**参照**」をクリックし、該当の CPA パッケージを選択します。
4. 「**ebMS バージョン**」の 2.0 が選択されていることを確認してください。
5. 「**アップロード**」をクリックします。

CPA のアップロード・プロセス中に、CPA にあるパートナーから内部パートナーを選択するかどうか尋ねられます。内部パートナーは ebMS フロー内でマネージャーと見なされ、ebMS フロー内の内部パートナーのすべてのターゲットは「バックエンド統合」または「N/A」のパッケージを使用します。ただし、コンソール上では、パートナーは外部パートナーのみとして示されます。

ebMS は、「文書定義の管理」ページの「ebMS」および「パッケージ: バックエンド統合 (Package: Backend Integration)」の下のプロトコルと同様に、パッケージとして表示されます。

また、ebMS フローは CPA がなくても WebSphere Partner Gateway で構成することができます。そうするには、 109 ページの『文書タイプの概要』の説明に従って、ebMS 文書定義、B2B 機能を WebSphere Partner Gateway コンソールから作成します。実際、CPA をアップロードしている間に、すべての構成が自動的に行われます。CPA がない場合は、このセクションに記載された手順に従ってください。

## 属性値の構成

### このタスクについて

ebMS 文書定義の場合、ほとんどの属性値は既に設定されているため、設定する必要はありません。ただし、以下の属性を設定する必要があります。

**ebMS パッケージ**

- **応答のための時間 (分単位)** - 元の要求を再送する前に確認通知を待つ時間を設定します。この属性は、「再試行カウント」と連動します。単位は分です。デフォルト値は 30 です。
- **再試行カウント** - 確認通知が受信されない場合に要求を送信する回数を設定します。この属性は、「応答のための時間」と連動します。デフォルト値は 3 です。
- **否認防止が必要** - 否認防止ストアに元の文書を保管するかどうかを設定します。デフォルト値は「はい」です。

  **注:** WebSphere Partner Gateway 6.2 では、否認防止情報はパートナー接続パラメーターから取得されます。パートナー接続パラメーターは、パートナー接続検索が正常に行われた後に取得されます。デフォルトでは、否認防止は「はい」に設定されています。この設定では、なんらかの理由で情報がパートナー接続から提供されない場合、文書は否認防止ストアに格納されます。
- **メッセージ・ストアが必要** - 文書をメッセージ・ストアに保管するかどうかを設定します。デフォルト値は「はい」です。

  **注:** メッセージ・ストア情報がパートナー接続パラメーターから取得されます。パートナー接続パラメーターは、パートナー接続検索が正常に行われた後に取得されます。デフォルトでは、メッセージ・ストアは「はい」に設定されています。つまり、文書はメッセージ・ストア内に存続されます。
- **受信の否認防止** - 否認防止ストアに受信を保管するかどうかを設定します。デフォルト値は「はい」です。
- **再試行間隔** - システムが再試行を待機する間隔を設定します。この属性は、「再試行カウント」と連動します。デフォルトは 5 分です。

属性を設定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**展開**」アイコンをクリックして個々にノードを適切な文書定義レベルまで展開するか、「**すべて**」を選択して表示されたすべての文書定義のノードを展開します。
3. 「**アクション**」列で、編集するパッケージの「**属性値の編集**」アイコンをクリックします。
4. 「**文書定義コンテキスト属性**」セクションで、設定する属性の「**更新**」列に移動し、値を選択するか、または新しい値を入力します。設定する属性ごとに、この手順を繰り返します。
5. 「**保存**」をクリックします。

**注:** ソースまたはターゲットの「**属性**」をクリックしてから、「**更新**」列で値を入力するかまたは値を変更して、ebMS 属性を接続レベルで更新することもできます。254 ページの『属性の指定または変更』を参照してください。

## インタラクションの作成

### このタスクについて

次のプロセスでは、バックエンド・システムとパートナーとの間のインタラクションを作成する方法について説明します。

開始する前に、適切な ebMS 文書定義がアップロードされていることを確認してください。

特定のパートナーのインタラクションを作成するには、以下のステップを実行します。

1. 「**ハブ管理**」 >「**ハブ構成**」 >「**文書定義**」をクリックします。
2. 「**インタラクションの作成**」をクリックします。
3. 「ソース」ツリーを「アクション」レベルまで展開し、「ターゲット」ツリーを「アクション」レベルまで展開します。
4. ツリー内で、ソース・コンテキストおよびターゲット・コンテキストに使用する文書定義を選択します。例えば、パートナーが ebMS を開始する場合は、次の文書定義を選択します。

*表 17. パートナーが開始する ebMS*

| ソース | ターゲット |
|---|---|
| パッケージ: ebMS | パッケージ: バックエンド統合 (1.0) |
| プロトコル: ebMS | プロトコル: ebMS |
| 文書タイプ: ALMService | 文書タイプ: ALMService |
| アクティビティー: ALMService | アクティビティー: ALMService |
| アクション: Remittance ALMBusiness | アクション: ALMBusiness |

バックエンド・システムが ebMS を開始する場合は、次の文書定義を選択します。

*表 18. バックエンド・システムが開始する ebMS*

| ソース | ターゲット |
|---|---|
| パッケージ: バックエンド統合 (1.0) | パッケージ: ebMS |
| プロトコル: ebMS | プロトコル: ebMS |
| 文書タイプ: ALMService | 文書タイプ: ALMService |
| アクティビティー: ALMService | アクティビティー: ALMService |
| アクション: ALMBusiness | アクション: Remittance ALMBusiness |

5. オプションで、「アクション」フィールドで「**ebMS の分割および解析**」を選択します。

   このハンドラーを選択すると、パートナーから送られる ebMS メッセージからペイロードが取り出され、それがパートナーから別々に送られているかのようにフローに戻されます。バックエンド・システムがメッセージを開始している場合は、このハンドラーを選択しないでください。このハンドラーを選択していない場合は、アクション・フィールドに「パススルー」を選択します。
6. 「**保存**」をクリックします。

   **注:** いくつかの ebMS フロー (例えば、STAR 仕様での場合) では、ebMS サービス・エレメント (ebMS サービス値は WPG チャネル文書フロー定義値と同じ) が URI ではなく、ストリングです。そのような場合、ebMS 2.0 仕様のように、型属性が ebMS SOAP メッセージでサービス・エレメントを示す必要があります。例えば、STAR 仕様では、型属性の値は「STARBOD」でなければなり

ません。文書フロー定義属性のターゲット側でそうした属性を構成できます。( 148 ページの表 20 を参照してください。)

## ebMS CPA の WebSphere Partner Gateway 構成へのマッピング

### このタスクについて

このセクションでは、Collaboration Profile Agreement (CPA) と WebSphere Partner Gateway UI 構成の間のマッピングを提供します。フィーチャーは、対応する WebSphere Partner Gateway UI 構成とともにリストされています。

**1.**

**フィーチャー**
**エレメント/属性**

**1.1 CPAId 1**

**インポート済み/手動構成済み**: インポート済み

**WebSphere Partner Gateway UI 構成:**

CPAID は、2 つのパートナー間に関連付けられたチャネルを通じて構成されます。この値を表示するには、WebSphere Partner Gateway コンソールで「**ハブ管理**」>「**ebMS**」にナビゲートします。「検索」をクリックし、表示された検索結果から「詳細の表示」アイコンをクリックします。

**2.**

**フィーチャー**
**エレメント/属性**

**1.2. Status 1**

**インポート済み/手動構成済み**: インポート済み。ただし、WebSphere Partner Gateway には保管されていません。また、これは手動で構成することはできません。

**WebSphere Partner Gateway UI 構成:**

この属性は、WebSphere Partner Gateway では構成できません。この値は、CPA からのインポート中に検査されます。インポート中、次のいずれかの状況が表示されます。

- Agreed (同意): CPA はインポートできます。
- Signed (署名): CPA はインポートでき、インポートの前に署名が検証されます。
- Proposed (提案): CPA はインポートできません。

**3.**

**フィーチャー**
**エレメント/属性**

**1.3 Start 1**

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

この属性は、WebSphere Partner Gateway では構成できません。これは CPA インポートからのみ設定できます。この値を表示するには、WebSphere Partner Gateway コンソールで「**ハブ管理**」>「**ebMS**」にナビゲートします。「検索」をクリックし、表示された検索結果から「詳細の表示」アイコンをクリックします。

**4.**

**フィーチャー**
　　**エレメント/属性**

**1.4 End 1**

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

この属性は、WebSphere Partner Gateway では構成できません。これは CPA インポートからのみ設定できます。この値を表示するには、WebSphere Partner Gateway コンソールで「**ハブ管理**」>「**ebMS**」にナビゲートします。「検索」をクリックし、表示された検索結果から「詳細の表示」アイコンをクリックします。

**5.**

**フィーチャー**
　　**エレメント/属性**

**1.5 Conversation Constraints 0, 1 (9.5) - invocationLimit 0,1 - concurrentConversations 0, 1**

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

この属性は、WebSphere Partner Gateway では構成できません。これは CPA インポートからのみ設定できます。この値を表示するには、WebSphere Partner Gateway コンソールで「**ハブ管理**」>「**ebMS**」にナビゲートします。「検索」をクリックし、表示された検索結果から「詳細の表示」アイコンをクリックします。

**6.**

**フィーチャー**
　　**エレメント/属性**

**1.6 PartyInfo 2**
　　partyName 1

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

値を表示するには、**「アカウント管理」>「プロファイル」>「パートナー」**にナビゲートします。「検索」をクリックし、CPA のパートナーに対して表示された検索結果から「詳細の表示」アイコンをクリックします。

**7.**

**フィーチャー**
**エレメント/属性**

**1.6 PartyInfo 2**
defaultMshChannelId 1

**インポート済み/手動構成済み**: インポート済み。ただし、WebSphere Partner Gateway には保管されていません。また、これは手動で構成することはできません。

**WebSphere Partner Gateway UI 構成:**

これらの値は、**Activity- MSHService** シグナル・エレメント (Ping、Status request、MessageError、および Acknowledgment など) に対するチャネル属性を設定するための CPA をインポートするときに使用されます。これらのチャネル値は、特定のアクション・エレメントに対して CPA に「OverrideMshActionBinding」エレメントが存在する場合、再びオーバーライドされます。

**8.**

**フィーチャー**
**エレメント/属性**

**1.6 PartyInfo 2**
defautMshPackageId 1

**インポート済み/手動構成済み**: インポート済み。ただし、WebSphere Partner Gateway には保管されていません。また、これは手動で構成することはできません。

**WebSphere Partner Gateway UI 構成:**

これらの値は、**Activity- MSHService** シグナル・エレメント (Ping、Status request、MessageError、および Acknowledgment など) に対するチャネル属性を設定するための CPA をインポートするときに使用されます。これらのチャネル値は、特定のアクション・エレメントに対して CPA に「OverrideMshActionBinding」エレメントが存在する場合、再びオーバーライドされます。

**9.**

**フィーチャー**
**エレメント/属性**

**1.6 PartyInfo 2**
PartyId 1, *

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

値を表示するには、「**アカウント管理**」>「**プロファイル**」>「**パートナー**」にナビゲートします。「検索」をクリックし、CPA のパートナーに対して表示された検索結果から「詳細の表示」アイコンをクリックします。

**10.**

**フィーチャー**
**エレメント/属性**

**1.6 PartyInfo 2**
type

**インポート済み/手動構成済み**: インポートされていません。また構成できません。

**11.**

**フィーチャー**
**エレメント/属性**

**1.6 PartyInfo 2**
PartyRef 1,*= (8.4.2)
- xlink:type F
- xlink:href 1
- type Fixed
- schemaLocation Implied

**インポート済み/手動構成済み**: インポートされていません。また構成できません。

**12.**

**フィーチャー**
**エレメント/属性**

**1.6 PartyInfo 2**
1.6.3 CollaborationRole 1,*

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

WebSphere Partner Gateway では、複数のコラボレーション役割エレメントがサポートされています。

**13.**

**フィーチャー**
**エレメント/属性**

**1.6 PartyInfo 2**
.6.3.1 ProcessSpecification 1
- name 1
- version 1
- xlink:type 1
- xlink:href
1 - uuid ImpliedReference 0,* (8.4.4.6)
- URI 0, 1
Transforms 1

```
  Transform
1 - Algorithm Fixed
 DigestMethod 1
  DigestValue 1
```

**インポート済み/手動構成済み**: インポートされていません。

**WebSphere Partner Gateway UI 構成:**

構成できません。

**14.**

**フィーチャー**
**エレメント/属性**

**1.6 PartyInfo 2**

```
1.6.3.2 Role 1   (8.4.5)
- name 1
- xlink:type Fixed
- xlink:href 1
```

**インポート済み/手動構成済み**: 属性 **xlink:href** はインポートです。他の属性はインポートされていません。

**WebSphere Partner Gateway UI 構成:**

値はチャネル属性 (「**アカウント管理**」>「**接続**」>「**パートナー接続**」) で構成することができます。チャネルを検索し、チャネル属性 (**Role**) にアクセスします。

**15.**

**フィーチャー**
**エレメント/属性**

**1.6 PartyInfo 2**

```
1.6.3.3  ApplicationCertificateRef 0,1  (8.4.6)
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

値は構成できません。属性 **certId** に対して指定された証明書はファイル・システムにロードされますが、WebSphere Partner Gateway にはロードされません。

**16.**

**フィーチャー**
**エレメント/属性**

**1.6 PartyInfo 2**

```
1.6.3.4  ApplicationSecurityDetailsRef 0, 1 (8.4.7)
- securityId 1
```

**インポート済み/手動構成済み**: インポートされていません。

**WebSphere Partner Gateway UI 構成:**

構成できません。

**17.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5 ServiceBinding 1**
1.6.3.5.1 Service 1 (8.4.9)
- type  Implied

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

- **サービス**: 文書定義の名前です。値を表示するには、「**ハブ管理**」>「**文書定義**」にナビゲートします。サービスの値は、ebMS パッケージとバックエンド統合パッケージの下に、文書タイプおよびアクティビティーとして表示されます。
- **タイプ**: タイプは、チャネル属性として使用されます (「**アカウント管理**」>「**接続**」>「**パートナー接続**」)。チャネルを検索し、チャネル属性 (**サービス・タイプ**) にアクセスします。

**18.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5 ServiceBinding 1**
1.6.3.5.1 Service 1 (8.4.9)
- type  Implied

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

- **サービス**: 文書定義の名前です。値を表示するには、「**ハブ管理**」>「**文書定義**」にナビゲートします。サービスの値は、ebMS パッケージとバックエンド統合パッケージの下に、文書タイプおよびアクティビティーとして表示されます。
- **タイプ**: タイプは、チャネル属性として使用されます (「**アカウント管理**」>「**接続**」>「**パートナー接続**」)。チャネルを検索し、チャネル属性 (**サービス・タイプ**) にアクセスします。

**19.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**
ThisPartyActionBinding 1
- action 1
- packageId 1
- xlink:href  Implied -
xlink:type Fixed
BusinessTransactionCharacteristics 1
- isNonRepudiationRequired
  All implied
isNonRepudiationReceiptRequired
- isConfidential
- isAuthenticated

```
- isAuthorizationRequired
- isTamperProof
- isIntelligibleCheckRequired
- timeToAcknowledgeReceipt
- timeToAcknowledgeAcceptance
- timeToPerform
- retryCountChannelId 1,*
ActionContext 0, 1
- binaryCollaboration 1
- businessTransactionActivity 1
- requestOrResponseAction 1
CollaborationActivity 0, 1
- name 1
OtherPartyActionBinding 0, 1
CanReceive 0, 1
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

- **CanSend** – チャネルは、「**バックエンド統合**」>「**ebMS**」>「**サービス名**」>「**partnerA のアクション**」から「**ebMS**」>「**サービス名**」>「**partnerB のアクション**」に作成されます (partnerB は、**OtherPartyActionBinding** エレメントを通じてバインドされている **CanReceive** エレメントを持っています)。
- **Action** – インポートされており、文書定義の「**アクティビティー**」の下に Action エレメントとして作成されます。
- **packageId** – 参照パッケージ ID 属性は、チャネル属性として保管されます。
- Xlink:href および xlink:type: インポートされておらず、構成できません。
- **isNonRepudiationRequired**、 **isNonRepudiationReceiptRequired**、 **isIntelligibleCheckRequired**、 **timeToAcknowledgeReceipt**、 **timeToPerform**: これらの属性はチャネル属性として構成されています。
- **isConfidential**、 **isAuthenticated**、 **isTamperProof**、 **isAuthorizationRequired**、 **timeToAcknowledgeAcceptance**、 **retryCount** - インポートされておらず、 構成できません。
- **ChannelId** 1, * : WebSphere Partner Gateway に対して 1 つの値のみ受け入れられます。参照属性はチャネル属性として設定されます。
- **binaryCollaboration**、 **businessTransactionActivity**、 **requestOrResponseAction**、 **CollaborationActivity** – インポートされておらず、構成できません。
- **OtherPartyActionBinding** - インポート済み。この参照を使用してチャネルが作成されます。
- **CanReceive** - インポート済み。同一接続に他のチャネルが存在する場合、同期として扱われます。

**20.**

**フィーチャー**

**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.6.3.5.3 CanReceive 0, *  (8.4.11)
ThisPartyActionBinding 1
OtherPartyActionBinding 0, 1
CanSend 0, 1
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

- **CanReceive** – チャネルは、「**ebMS**」>「**サービス名**」>「**partnerA のアクション**」から「**バックエンド統合**」>「**ebMS**」>「**サービス名**」>「**partnerB のアクション**」に作成されます (partnerB は、**OtherPartyActionBinding** エレメントを通じてバインドされている **CanSend** エレメントを持っています)。
- **OtherPartyActionBinding** - インポート済み。この参照を使用してチャネルが作成されます。
- **CanSend** - インポート済み。同一接続に他のチャネルが存在する場合、同期として扱われます。

**21.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**
1.6.4 Certificate 1, * (8.4.18)
- certId  KeyInfo

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

証明書はファイル・システムに保管され、手動で WebSphere Partner Gateway にロードしなければなりません (「**アカウント管理**」>「**プロファイル**」>「**証明書**」)。

**22.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**
1.6.5 SecurityDetails 0, *  (8.4.18)
- securityId 1 TrustedAnchor 0, *
AnchorCertificateRef 1, *
SecurityPolicy 0, 1

**インポート済み/手動構成済み**: インポートされていません。参照証明書のみがファイル・システムにロードされます。

**23.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**
1.6.6 DeliveryChannel 1, * (8.4.22)
- channelId 1
- transportId 1
- docExchangeId1
MessagingCharacteristics 1
- syncReplyMode All implied

```
- ackRequested attribute
- ackSignatureRequested
- duplicateElimination
- actor
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

- **channelId** : 参照属性はチャネル属性として設定されます。
- **transportId**: 参照属性はゲートウェイの作成に使用され、チャネルのデフォルト・ゲートウェイとして設定されます。
- **docExchangeId**: 参照属性はチャネル属性として設定されます。
- **syncReplyMode、 ackRequested、 ackSignatureRequested、 duplicateElimination、 actor** : これらの属性はインポートされており、チャネル属性として構成されています。

**24.**

**フィーチャー**

**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.6.7 Transport 1, * (8.4.24)
- transportId 1
TransportSender 0, 1 (8.4.25)
TransportProtocol 1
- version 1
ImpliedAccessAuthentication 0, *
TransportClientSecurity 0, 1
TransportSecurityProtocol 1
- version 1
ImpliedClientCertificateRef  0, 1
- certId 1
ServerSecurityDetailsRef 0, 1
- securityId 1
EncryptionAlgorithm 0, *
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

**インポート済み/手動構成済み**: インポートされていません。

**25.**

**フィーチャー**

**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.6.7 Transport 1, * (8.4.24)
TransportReceiver 0, 1 (8.4.33)
TransportProtocol 1
- version 1
ImpliedEndpoint 1, *
- uri 1
- type  ImpliedAccessAuthentication 0, *
TransportServerSecurity 0, 1
TransportSecurityProtocol 1
- version 1
ServerCertificateRef 1
```

```
- certId 1
ClientSecurityDetailsRef 0, 1
- SecurityId 1
EncryptionAlgorithm 0, *
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

- **トランスポート・プロトコル**: ゲートウェイ・プロトコルを定義します。
- **バージョン**: ゲートウェイのプロトコル・バージョンを定義します。
- **URL**: ゲートウェイ URL を定義します。これらの値は、「**アカウント管理**」> 「**プロファイル**」>「**PartnerSearch**」で表示できます。すべてのパートナーおよび選択したパートナーに対して、「**宛先**」タブをクリックします。残りの属性値はインポートされていません。

**26.**

**フィーチャー**

**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.6.8 DocExchange (8.4.39)
- docExchangeId 1 1.6.8.2.1
ebXMLSenderBinding 0, 1 (8.4.40)
- version ReliableMessaging 0, 1
Retries 0, 1
RetryInterval 0, 1
MessageOrderSemantics 1
PersistDuration 0, 1
SenderNonRepudiation 0, 1
NonRepudiationProtocol 1
- version 1 Implied
HashFunction 1
SignatureAlgorithm 1
- oid All implied
- w3c
- enumeratedType
SigningCertificateRef 1
- certId 1
SenderDigitalEnvelope 0, 1
DigitalEnvelopeProtocol 1
- version 1  EncryptionAlgorithm 1
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

**Retries、 RetryInterval、 MessageOrderSemantics、 PersistDuration、 HashFunction、 SignatureAlgorithm、 DigitalEnvelopeProtocol、 EncryptionAlgorithm** : これらの値はインポートされ、 チャネル属性として保管さ

れています (**「アカウント管理」>「接続」>「パートナー接続」**)。チャネルを検索し、**「チャネル属性」**を選択します。残りの値はインポートされておらず、構成できません。

**27.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.6.8.2 ebXMLReceiverBinding 0, 1 (8.4.53)
- version 1
ReliableMessaging 0, 1
Retries 0, 1
RetryInterval 0, 1
MessageOrderSemantics 1
ReceiverNonRepudiation 0, 1
NonRepudiationProtocol 1
- version 1
HashFunction 1
SigningAlgorithm 1
- oid All Implied
- w3c
- enumeratedType
SigningSecurityDetailsRef 1
- securityId 1
ReceiverDigitalEnvelope 0, 1
DigitalEnvelopeProtocol 1
- version 1
EncryptionAlgorithm 1
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
EncryptionCertificateRef 1
- certId 1
NamespaceSupported 0, *
- location 1
- version Implied
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

**Retries、 RetryInterval、 MessageOrderSemantics、 PersistDuration、 HashFunction、 SignatureAlgorithm、 DigitalEnvelopeProtocol、 EncryptionAlgorithm** : これらの値はインポートされ、 チャネル属性として保管されています (**「アカウント管理」>「接続」>「パートナー接続」**)。チャネルを検索し、**「チャネル属性」**を選択します。残りの値はインポートされておらず、構成できません。

**28.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.6.9  OverrideMshActionBinding 0, *  (8.4.58)
- action 1
- channelId
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

指定されたアクションに対して、チャネル属性は参照チャネル ID を使用して設定されます。

**29.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.7 SimplePart (8.5)
- id 1
- mimetype 1
- mimparameters  Implied
- xlink:role
 ImpliedNamespaceSupported 0, *
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

**Mimetype** : 値はインポートされており、チャネル属性として保管されます。残りの値はインポートされておらず、構成できません。

**30.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.8 Packaging (8.6)
- id 1
ProcessingCapabilities 1, *
- parse 1
- generate 1
CompositeList 0, *
Composite 0, *
- mimetype 1
- id 1
- mimeparameters ImpliedConstituent 1, *
- idref 1
- excludeFromSignature Implied
- minOccurs Implied
- maxOccurs Implied
SignatureTransform 0, 1
Transform 1, *
EncryptionTransform 0, 1
Transform 1, *
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

**Composite : mimetype、 mimeparameters、 Constituent-idref、 Constituent-excludeFromSignature、 signatureTransform、 encryptionTransform、 Algorithm**: これらの値はインポートされ、 チャネル属性として保管されています (「**アカウン**

**ト管理」>「接続」>「パートナー接続」**)。チャネルを検索し、「**チャネル属性**」を選択します。残りの値はインポートされておらず、構成できません。

**31.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
Encapsulation 0, *
- mimetype 1
- id 1
- mimeparameters  ImpliedConstituent 1
- idref 1
- excludeFromSignature Implied
- minOccurs Implied
- maxOccurs Implied
SignatureTransform 0, 1
Transform 1, *
EncryptionTransform 0, 1
Transform 1, *
```

**インポート済み/手動構成済み**: インポート済み。

**WebSphere Partner Gateway UI 構成:**

**Encapsulation : mimetype、 mimeparameters、 Constituent-idref、 Constituent-excludeFromSignature、 signatureTransform、 encryptionTransform、 Algorithm**: これらの値はインポートされ、 チャネル属性として保管されています (「**アカウント管理」>「接続」>「パートナー接続**」)。チャネルを検索し、「**チャネル属性**」を選択します。残りの値はインポートされておらず、構成できません。

**32.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.9 Signature 0, 1 (8.7)
ds:Signature 1,3
SignedInfo 1
CanonicalizationMethod 0, 1
SignatureMethod 1
- AlgorithmReference 1, *
- URI FixedTransforms 1
Transform 1
- Algorithm Fixed
```

**インポート済み/手動構成済み**: インポートされていません。

**WebSphere Partner Gateway UI 構成:**

構成できません。

**33.**

**フィーチャー**
**エレメント/属性**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.10 Comments 0, * (8.8)
- xml:lang
```

**インポート済み/手動構成済み**: インポートされていません。

**WebSphere Partner Gateway UI 構成:**

構成できません。

## 接続属性

以下の表は、ebMS パッケージ化のメッセージのビジネス・チャネルで見られるルーティング・オブジェクト属性を提供します。

「**アカウント管理**」>「**接続**」>「**パートナー接続**」をクリックし、「ソース」と「ターゲット」を選択します。チャネルがインバウンド ebMS メッセージ用の場合は、ソース・サイドの「**属性**」をクリックします。そしてチャネルがアウトバウンド ebMS メッセージ用の場合は、ターゲット・サイドの「**属性**」をクリックします。結果の画面をスクロールダウンし、「**アクション**」フォルダーをクリックします。

*表 19. 接続属性*

| CPA XML 属性 | デフォルト値 | 可能な値 | WebSphere Partner Gateway での表示テキスト |
|---|---|---|---|
| isNonRepudiationRequired | False | True/false - Yes/No にマップ | 否認防止が必要 |
| isNonRepudiationReceiptRequired | False | True/false - Yes/No にマップ | 受信の否認防止 |
| timeToAcknowledgeReceipt | | | 応答のための時間 |
| Retries | 3 | 任意の数値 | 再試行カウント |
| MessageOrderSemantics | Not Guaranteed | ″Guaranteed″ ″NotGuaranteed″ | メッセージ順序セマンティクス |
| PersistDuration | P1D | | 持続期間 |
| syncReplyMode | なし | ″mshSignalsOnly″<br><br>″signalsOnly″<br><br>″responseOnly″<br><br>″signalsAndResponse″<br><br>″none″<br><br>(フェーズ 2 に移動) | 同期応答モード |
| ackRequested | Per Message | ″always″ - 常に確認応答を要求することを暗黙指定。<br><br>″never″ - 確認応答を要求しないことを暗黙指定。<br><br>「perMessage」 - ebXML 文書の ack エレメントに応じて確認応答を要求できるかできないかを暗黙指定。 | 確認通知要求済み |

*表 19. 接続属性 (続き)*

| CPA XML 属性 | デフォルト値 | 可能な値 | WebSphere Partner Gateway での表示テキスト |
|---|---|---|---|
| ackSignatureRequested | Per Message | ″always″<br>″never″<br>″perMessage″ | 確認通知署名要求済み |
| duplicateElimination | Per Message | ″always″<br>″never″<br>″perMessage″ | 重複の除去 |
| アクター | ″urn:oasis:names:tc:ebxml-msg:actor:nextMSH″ | ″urn:oasis:names:tc:ebxml-msg:actor:nextMSH″″urn:oasis:names:tc:ebxml-msg:actor:toPartyMSH″ | アクター |
| PartyRole | - | CPA での役割 | 役割 |
| 再試行間隔 | 270 | - | 再試行間隔 |
| NonRepudiationProtocol | - | http://www.w3.org/2000/09/xmldsig# | 署名プロトコル |
| SignatureAlgorithm | - | 1. http://www.w3.org.2000/09/xmldsig#dsa-sha1<br>2. http://www.w3.org/2000/09/xmldsig#hmac-sha1<br>3. http://www.w3.org/2000/09/xmldsig#rsa-sha1 | 署名アルゴリズム |
| isEncryptionRequired | いいえ | True/false - Yes/no にマップ | EncryptionRequired |
| isCompressionRequired | いいえ | True/false - Yes/no にマップ | 圧縮が必要 |
| /Packaging/CompositeList /Encapsulation/Constituent: mimetype | - | | 圧縮 Mimeype |
| /tp:SenderDigitalEnvelope /tp:DigitalEnvelopeProtocol | - | SMIME XMLEncryption | EncryptionProtocol |
| /tp:SenderDigitalEnvelope /EncryptionAlgorithm | - | 3des-cbc, aes128-cbc, aes-256-cbc | 暗号化アルゴリズム |
| /tp:ReceiverDigitalEnvelope /tp:DigitalEnvelopeProtocol | - | SMIME XMLEncryption | EncryptionProtocol |
| /tp:ReceiverDigitalEnvelope /EncryptionAlgorithm | - | 3des-cbc, aes128-cbc, aes-256-cbc | 暗号化アルゴリズム |
| /Packaging/CompositeList /Encapsulation tp:MimeType | - | text/xml application/pkcs7-mime | 暗号化 Mime タイプ |
| /Packaging/CompositeList /Encapsulation- tp:mimeparameters | - | | 暗号化 Mime パラメーター |
| /Packaging/CompositeList /Encapsulation/Constituent: mimetype | - | | 暗号化構成要素 |
| /Packaging/CompositeList / Composite/ tp:mimeparameters | - | | パッケージ Mime パラメーター |
| /Packaging/CompositeList / Composite /Constituent: mimetype | - | | PackagingConstituent |

表 19. 接続属性 (続き)

| CPA XML 属性 | デフォルト値 | 可能な値 | WebSphere Partner Gateway での表示テキスト |
|---|---|---|---|
| /Packaging/CompositeList /Composite/Contituent /excludeFromSignature: mimetype | - | | 署名から除外 |
| /Packaging/CompositeList / Composite/Contituent/ SignatureTransform | - | 1. BASE64<br>2. ENVELOPED<br>3. XPATH<br>4. XPATH2<br>5. XSLT | 署名変換アルゴリズム |
| /Packaging/CompositeList /Composite/Contituent/ EncryptionTransform | - | 1. BASE64<br>2. ENVELOPED<br>3. XPATH<br>4. XPATH2<br>5. XSLT | 暗号化変換アルゴリズム |

### 制限

CPA を WebSphere Partner Gateway にマップする場合、以下の制限があります。

1. CPA からの証明書は WebSphere Partner Gateway にインポートされません。それらの証明書はファイル・システムに保管され、管理者が手動でそれらを妥当性検査して、WebSphere Partner Gateway にアップロードしなければなりません。
2. WebSphere Partner Gateway は CPA からの同期フローおよび非同期フローをアドレッシングすることができますが、同じアクション値の複数のバインディングをアドレッシングすることはできません。
3. 9 桁の数字の DUNS ID のみがサポートされます (Freeform はサポートされません)。

## ebMS SOAP ヘッダーの WebSphere Partner Gateway ヘッダーへのマッピング

ebMS spec 2.0 は、ebMS SOAP メッセージになければならない必須ヘッダーのセットを定義します。以下の表は、これらの ebMS 必須ヘッダーの一部とそれらの値が取られる WebSphere Partner Gateway ヘッダーの間のマッピングを示します。

表 20. ebMS SOAP ヘッダーと対応する WebSphere Partner Gateway ヘッダー

| シリアル番号 | ebMS SOAP メッセージ内のヘッダー名 | WebSphere Partner Gateway 内の対応するヘッダー名 |
|---|---|---|
| 1 | 元 PartyId | バックエンド・システムによって設定される「x-aux-sender-id」。 |
| 2 | 送信側役割 | 文書定義属性のソース側の役割属性 |
| 3 | 元 PartyId タイプ | ユーザーは構成できません。PartyId が DUNS の場合、「type」値は「urn:duns」です。それ以外の場合、「string」です。 |

表 20. ebMS SOAP ヘッダーと対応する WebSphere Partner Gateway ヘッダー (続き)

| シリアル番号 | ebMS SOAP メッセージ内のヘッダー名 | WebSphere Partner Gateway 内の対応するヘッダー名 |
|---|---|---|
| 4 | 宛先 PartyId | バックエンド・システムによって設定される「x-aux-receiver-id」。 |
| 5 | 受信側役割 | 文書定義属性のターゲット側の役割属性 |
| 6 | 宛先 PartyId タイプ | ユーザーは構成できません。PartyId が duns の場合、「type」値は「urn:duns」です。そうでない場合、「string」です。 |
| 7 | CPAId | CPA がデータベース内にある場合、WebSphere Partner Gateway は CPA 内にある CPA-ID を使用します。データベース内にない場合、ユーザーは文書定義属性のターゲット側にある CPA ID 属性を構成できます。ユーザーがこの属性を構成しておらず、CPA がない場合、WebSphere Partner Gateway はパートナー ID に基づいて CPA ID を生成します。 |
| 8 | 会話 ID | バックエンド・システムによって設定された「x-aux-process-instance-id」。バックエンド・システムがこれを設定しない場合、WebSphere Partner Gateway はその独自の会話 ID を生成します。 |
| 9 | サービス | ターゲット・パートナー接続での文書定義値。<br>**注:** 文書定義とアクティビティーは ebMS フロー内で同じです。 |
| 10 | サービス・タイプ | 文書定義属性のターゲット側のサービス・タイプ属性 |
| 11 | アクション | ターゲット・パートナー接続でのアクション値 |
| 12 | MessageId | バックエンド・システムによって設定された「x-aux-msg-id」。バックエンド・システムがこれを設定しない場合、WebSphere Partner Gateway はその独自のメッセージ ID を生成します。 |

ebMS 同期応答を ebMS 要求文書に送信している場合、バックエンド・システムは応答文書で「x-aux-request-msg-id」ヘッダーを設定する必要があります。このヘッダーの値は要求メッセージのメッセージ ID です。さらに、応答文書は要求文書と同じ会話内になければなりません。これは、応答の「x-aux-process-instance-id」が要求の ConversationId と同じでなければならないことを意味します。

要求文書の ConversationId と MessageId はそれぞれ「x-aux-process-instance-id」および「x-aux-msg-id」としてバックエンドに送信されます。

## ebMS 文書の表示

### このタスクについて

ebMS ビューアーは、ebMS 文書に関する情報を表示します。ロー文書とそれに関連する文書処理の詳細およびイベントを、特定の検索条件を使用して表示することができます。文書が正常に配信されたかどうかを調べたり、問題の原因を判別するときに、この情報が役に立ちます。

ebMS ビューアーを表示するには、以下を実行します。

1. 「**ビューアー**」>「**ebMS ビューアー**」をクリックします。
2. 該当する検索条件を選択してください。
3. 「**検索**」をクリックします。

ebMS ビューアーで、文書は会話 ID に基づいて編成されます。これは、同じ会話 ID のすべての文書が一緒にグループ化され、会話 ID の各行の左側にある「詳細 (More details)」アイコンをクリックして、それらを表示できることを意味します。「詳細 (More details)」アイコンをクリックすると、その会話内のすべてのメッセージを示す新規ページが表示されます。ページの上部に「会話状況」という属性があります。この属性の値が、その会話で次に予期されるメッセージです。

## ebMS メッセージの状況の要求

### このタスクについて

ebMS メッセージの状況を要求するには、以下のステップを実行します。

1. 調べたい ebMS 文書を見つけた後、その隣にある「**詳細の表示**」アイコンをクリックします。
2. 「状況の要求」をクリックします。その文書の状況が表示されます。

状況を最新表示するには、「**状況の表示**」をクリックします。

ebMS の Status Request 文書と Status Response 文書を構成する際には、以下の点を考慮してください。

- 作成する必要がある接続は Status Request 接続のみです。Status Response 接続では、既存の Status Request 接続が使用されます。
- 内部パートナーから外部パートナーへの Status Request 接続では、接続のソース宛先は使用されません。
- 外部パートナーから内部パートナーへの Status Request 接続では、Status Response 応答文書を外部パートナーに送信するときに、接続のソース宛先が使用されます。
- ユーザーに CPA がない場合は、B2B 機能を使用可能にし、ebMS Status Request メッセージのチャネルを以下のように作成します。
  - インバウンド ebMS Status Request メッセージ

    ソース側の B2B 機能は以下のようになります。

    パッケージ: N/A (N/A)
    プロトコル: ebMS (2.0)
    文書タイプ: MSHService (2.0)
    アクティビティー: MSHService (2.0)
    アクション: StatusRequest(N/A)

    ターゲット側の B2B 機能は以下のようになります。

    パッケージ: ebMS (2.0)
    プロトコル: ebMS (2.0)

文書タイプ: MSHService (2.0)
アクティビティー: MSHService (2.0)
アクション: StatusRequest(N/A)

– アウトバウンド ebMS Status Request メッセージ

ソース側の B2B 機能は以下のようになります。

パッケージ: ebMS (2.0)
プロトコル: ebMS (2.0)
文書タイプ: MSHService (2.0)
アクティビティー: MSHService (2.0)
アクション: StatusRequest(N/A)

ターゲット側の B2B 機能は以下のようになります。

パッケージ: N/A (N/A)
プロトコル: ebMS (2.0)
文書タイプ: MSHService (2.0)
アクティビティー: MSHService (2.0)
アクション: StatusRequest(N/A)

次にユーザーはチャネルをアクティブにし、パートナー接続ページで宛先を設定します。

**注:** この情報は、ebMS エラーおよび確認通知にも適用されます。この場合、これらのチャネルに対するアクションがそれぞれ MessageError と Acknowledgment に変更されます。

## ebMS パートナーの ping

### このタスクについて

「パートナー接続のテスト」ページで、ebMS パートナーに対して ping を実行できます。 これは、ping メッセージをパートナーに送信できることを意味し、パートナーが起動して受信する準備ができている場合、パートナーは pong メッセージで応答します。CPA をアップロードすると、ping-pong チャネルが作成されます。

ping を機能させるには、関係するパートナーとの接続を定義する必要があります。詳細については、*「WebSphere Partner Gateway E/A ハブ構成ガイド」*で、ebMS パートナーの ping のセクションを参照してください。

ebMS パートナーに ping するには、以下を実行します。

1. **「ツール」 > 「パートナー接続のテスト」**をクリックします。
2. **「コマンド」**に、**「PING ebMS」** を選択します。
3. **「送信側パートナー」**および**「受信側パートナー」**を選択してください。
4. (オプション) **「宛先」**を選択するか、**URL** を入力します。
5. **「テスト」**をクリックして、ping メッセージを送信します。

ping メッセージの状況を判別するには、**「ping 状況」**をクリックします。 最終 ping 要求の状況が「結果」の下に表示されます。

**注:** 最後の ping 要求は、「パートナー接続のテスト」から開始されていることも、既存の ping 文書の文書ビューアーの再送から開始されていることもあります。

# Web サービス

パートナーは、内部パートナーがホストする Web サービスを呼び出すことができます。同様に、内部パートナーは、パートナーがホストする Web サービスを呼び出すことができます。パートナーまたは内部パートナーは、WebSphere Partner Gateway サーバーを通して Web サービスを呼び出します。WebSphere Partner Gateway は、プロキシーとして動作し、Web サービス要求を Web サービス・プロバイダーに渡し、プロバイダーからの同期的な応答をリクエスターに戻します。

ここでは、パートナーや内部パートナーが使用する Web サービスの設定に関する以下の情報について説明します。

- Web サービスのパートナーの識別
- Web サービスに対する文書定義の設定
- パートナーの B2B 機能への文書定義の追加
- Web サービス・サポートの制限

## Web サービスのパートナーの識別

パートナーが使用する Web サービスを内部パートナーが提供する場合、WebSphere Partner Gateway は内部パートナーと外部パートナー両方の ID を要求します。WebSphere Partner Gateway では、複数の内部パートナーを作成できます。そしてそのうちの 1 つがデフォルトの内部パートナーとして設定されます。デフォルトの内部パートナーをオーバーライドして、内部パートナーを選択するには、WebSphere Partner Gateway レシーバーに追加のパラメーター (アウトバウンド・フローかインバウンド・フローかに応じて、**FromPartnerBusinessId** または **ToPartnerBusinessId** など) を送信してください。エラー条件は、基本認証と URL を通じて 2 つの異なる外部パートナー ID が提供されている場合に、基本認証が優先されることです。アウトバウンド・フローに使用可能な各種照会ストリング: `<Receiver-URL>?to=<business id>` および `<Receiver-URL?to=<business id>&from=<business id>`。インバウンド・フローに使用可能な各種照会ストリング:`<Receiver-URL` および `Receiver-URL?to=business id`。インバウンドの場合、**基本認証**は必須です。

## 文書定義の作成

文書定義を設定するには、Web サービスを定義する WSDL (Web サービス記述言語) ファイルをアップロードするか、コミュニティー・コンソールを通して同等な文書定義を手動で入力します。

### Web サービスの WSDL ファイルのアップロード

#### このタスクについて

Web サービスの定義は、拡張子 `.wsdl` の 1 次 WSDL ファイルに含まれている必要があります。この定義では、インポート・エレメントを使用して追加 WSDL ファイルをインポートすることができます。インポートするファイルがある場合、これらのファイルは、以下のいずれかの方法を使用して、1 次ファイルと共にアップロードできます。

- 各インポート・エレメントの location 属性のファイル・パスまたは (HTTP) URL がコミュニティー・コンソールのサーバー (ユーザーのマシンではなく) から到達可能である場合、1 次ファイルを直接アップロードすることができ、インポートされるファイルは自動的にアップロードされます。
- インポート・ファイルと 1 次ファイルがすべて 1 つの ZIP ファイルに圧縮され、各ファイルのパスがインポートの location 属性のパス (ある場合) に対応している場合は、ZIP ファイルをアップロードすると、含まれている 1 次 WSDL ファイルおよびインポート WSDL ファイルがすべてアップロードされます。

例えば、1 次 WSDL ファイル helloworldRPC.wsdl に、次のインポート・エレメントが含まれているものとします。

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl" location=
"bindingRPC.wsdl"/>

<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl" location=
"port/porttypeRPC.wsdl"/>
```

また、インポートされる WSDL ファイル bindingRPC.wsdl に、以下のインポート・エレメントが含まれているものとします。

ファイルには、以下が含まれている必要があります。

```
Name                    Path

helloworldRPC.wsdl

bindingRPC.wsdl

porttypeRPC.wsdl                port¥
```

Web サービスの WSDL ファイル定義がアップロードされると、元の WSDL は検証マップとして保管されます。(Web サービス・メッセージは、実際に WebSphere Partner Gateway により WSDL に照らし合わせて検証されることはありません)。この WSDL は、プライベート WSDL と呼ばれます。

また、パブリック WSDL は、「パッケージのアップロード/ダウンロード」ページで指定されたターゲット URL で置き換えられたプライベート URL と共に保管されます。パブリック WSDL は、ターゲットの URL (パブリック URL) で Web サービスを呼び出す Web サービスのユーザーに提供されます。WebSphere Partner Gateway は、その後、元の Web サービス・プロバイダーのプライベート URL である宛先に Web サービス要求を送付します。WebSphere Partner Gateway は、プロキシーとして動作し、プライベート・プロバイダー URL (Web サービス利用者には表示されない) に Web サービス要求を転送します。

プライベート WSDL およびパブリック WSDL (インポート・ファイルを含む) は、WSDL がアップロードされた後にコミュニティー・コンソールからダウンロードできます。

**コミュニティー・コンソールを使用した WSDL ファイルのアップロード:**
WebSphere Partner Gateway では、WSDL ファイルをインポートすることができます。 Web サービスが単一の WSDL ファイルに定義されている場合は、WSDL ファイルを直接アップロードできます。Web サービスが複数の WSDL ファイルを使用して定義されている場合 (1 次 WSDL ファイル内に WSDL ファイルをインポートした場合)、WSDL ファイルは、ZIP アーカイブの形式でアップロードされます。

**重要:** ZIP アーカイブに格納された WSDL ファイルは、WSDL インポート・エレメントに指定されているディレクトリーに入れる必要があります。例えば、以下のインポート・エレメントがあるものとします。

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl"
location="path1/bindingRPC.wsdl"/>
```

ZIP アーカイブ内のディレクトリー構造は、path1/bindingRPC.wsdl になります。

ここで、以下の例を考えて見ます。

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl"
 location="bindingRPC.wsdl"/>.
```

bindingRPC.wsdl ファイルは、ZIP アーカイブ内のルート・レベルにあります。

単一の WSDL ファイルまたは ZIP アーカイブをアップロードするには、以下の手順を実行します。

1. 「**ハブ管理**」 >「**ハブ構成**」 >「**文書定義**」をクリックします。
2. 「**パッケージのアップロード/ダウンロード**」をクリックします。
3. 「**WSDL パッケージ**」の場合は、「**はい**」をクリックします。
4. 「**Web サービス・パブリック URL**」の場合は、以下のステップの 1 つを実行します。
   - Web サービスが (パートナーから呼び出された) 内部パートナーによって提供される場合は、Web サービスのパブリック URL を入力します。以下に例を示します。

     https://*<target_host:port>*/bcgreceiver/Receiver

     この URL は一般に、ターゲットに定義されている実動 HTTP ターゲットと同じになります。
   - Web サービスが (内部パートナーから呼び出された) パートナーによって提供される場合は、パートナーのパブリック URL と照会ストリングを入力します。以下に例を示します。

     https://*<target_host:port>*/bcgreceiver/Receiver?to=*<partner_business_ID>*
5. 「**参照**」をクリックし、WSDL ファイルまたは ZIP アーカイブを選択します。
6. ファイルをテスト・モードでアップロードする場合は、「**データベースへコミットする**」で「**いいえ**」を選択します。「**いいえ**」を選択すると、ファイルはシステムにインストールされません。「メッセージ」ボックスに表示されているシステム生成メッセージを使用して、アップロード・エラーのトラブルシューティングを行います。システム・データベースにファイルをアップロードするには、「**はい**」を選択します。
7. 現在データベース内にあるデータを置き換える場合は、「**データの上書き**」で「**はい**」を選択します。データベースにファイルを追加する場合は、「**いいえ**」を選択します。
8. 「**アップロード**」をクリックします。WSDL ファイルがシステムにインストールされます。

**スキーマ・ファイルを使用したパッケージの検証:** コンソールを使用してアップロードできる XML ファイルを記述する一連の XML スキーマが、WebSphere Partner Gateway のインストール・メディアで提供されています。アップロード・ファイル

は、このスキーマと照合して検証されます。スキーマ・ファイルは、XML に準拠していないためにファイルをアップロードできない場合、エラーの原因を判断するのに役立つリファレンスです。ファイルは、wsdl.xsd、wsdlhttp.xsd、および wsdlsoap.xsd で、有効な Web サービス記述言語 (WSDL) ファイルを記述するスキーマが含まれています。

ファイルは B2BIntegrate¥packagingSchemas にあります。

## 文書定義の手動作成

同等の文書定義を手動で入力する場合は、このセクションの手順に従います。また、「**プロトコル: Web サービス**」で文書タイプ、アクティビティー、およびアクションの各項目を作成する必要もあります。アクションの要件およびその受信 SOAP メッセージとの関係に特に注意してください。

文書定義のパッケージ/プロトコル/文書タイプ/アクティビティー/アクション階層では、サポートされている Web サービスは以下のように表されます。

- **パッケージ: なし**
- **プロトコル: Web サービス (1.0)**
- **文書タイプ:** {*<Web_service_namespace>*:*<Web_service_name>*} (名前とコード)。Web サービス・プロトコルの文書タイプの間で固有である必要があります。これは通常は WSDL のネーム・スペースと名前です。
- **アクティビティー:** 各 Web サービス操作に対するアクティビティー (名前とコード)

  {*<operation_namespace>*}:*<operation_name>*
- **アクション**: 各操作の入力メッセージに対するアクション (名前とコード)

  {*<namespace_of_identifying_xml_element = namespace_of_first_child_of_soap:body>*}:
  *<name_of _identifying_xml_element = name_of_first_child_of_soap:body>*

WebSphere Partner Gateway はアクションのネーム・スペースおよび名前を使用して、着信 Web サービス要求 SOAP メッセージを識別し、定義されたパートナー接続に基づいて適切に送付するため、アクションは重要な定義となります。受信した SOAP メッセージの soap:body エレメントの最初の XML 子エレメントのネーム・スペースおよび名前は、WebSphere Partner Gateway の文書定義の既知のアクションのネーム・スペースおよび名前と一致する必要があります。

例えば、文書リテラル SOAP バインディングの場合の Web サービス要求 SOAP メッセージが以下のようになるものとします。

```
<?xml version="1.0" encoding="UTF-8"?>

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd=
"http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
 <soapenv:Body>
  <nameAndAddressElt xmlns="http://www.helloworld.com/xsd/helloDocLitSchema">
   <titleElt xmlns="">Mr</titleElt>
   <nameElt xmlns="">Joe Smith</nameElt>
   <addressElt xmlns="">
    <numberElt>123</numberElt>
    <streetElt>Elm St</streetElt>
    <cityElt>Peoria</cityElt>
```

```
   </addressElt>
  </nameAndAddressElt>
 </soapenv:Body>
</soapenv:Envelope>
```

WebSphere Partner Gateway は、以下のコードで定義されている Web サービス・アクションを探します。

```
{http://www.helloworld.com/xsd/helloDocLitSchema}:nameAndAddressElt
```

RPC バインディング・スタイル SOAP 要求メッセージは、以下のようになります。

```
<?xml version="1.0" encoding="UTF-8"?>

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd=
"http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1:helloWorldRPC soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/ xmlns:ns1="http://www.helloworld.com/helloRPC">
   <name xsi:type="xsd:string">Joe Smith</name>
  </ns1:helloWorldRPC>
 </soapenv:Body>
</soapenv:Envelope>
```

WebSphere Partner Gateway は、以下のコードで定義されている Web サービス・アクションを探します。

```
{http://www.helloworld.com/helloRPC}:helloWorldRPC
```

RPC バインディングでは、SOAP 要求メッセージの soap:body の最初の子エレメントのネーム・スペースおよび名前が、関連 Web サービス操作のネーム・スペースおよび名前である必要があります。

文書リテラル・バインディングでは、SOAP 要求メッセージの soap:body の最初の子エレメントのネーム・スペースおよび名前が、Web サービスの入力「message」定義の 「part」 エレメントの XML 「element」 属性のネーム・スペースおよび名前である必要があります。

## インタラクションの作成

### このタスクについて

Web サービスのインタラクションを作成するには、ソースとターゲットの両方に同じ Web サービス文書タイプ・アクションを使用します。

対話を作成するには、以下の手順を実行します。

1. 「**ハブ管理**」 >「**ハブ構成**」 >「**文書定義**」をクリックします。
2. 「**インタラクションの作成**」をクリックします。
3. 「**ソース**」の下で、「**パッケージ: なし**」>「**プロトコル: Web サービス**」>「**文書タイプ:** < *document type*」> >「**アクション:** <*action*>」を展開します。
4. 前のステップを「**ターゲット**」列で繰り返します。
5. ページの下部にある「**アクション**」リストから、「**パススルー**」を選択します (「**パススルー**」は、Web サービスに対して WebSphere Partner Gateway でサポートされている、唯一有効なオプションです)。

## Web サービス・サポートの制限

WebSphere Partner Gateway では、以下の標準がサポートされています。

- WSDL 1.1
- SOAP 1.1
- WS-I Basic Profile v. 1.0 (文書リテラル・バインディングの SOAP メッセージの形式に関する重要な制限を含む)

**注:**

- WebSphere Partner Gateway では、Basic Profile 1.0 を部分的にサポートしています。
- SOAP/HTTP バインディングはサポートされています。
- 再バインドはサポートされていません。
- RPC エンコード/RPC リテラルおよび文書リテラル・バインディング・スタイルはサポートされています (WS-I Basic Profile の制限に従います)。

103 ページの『SOAP エンベロープの検証』および 104 ページの『SOAP エンベロープ解除』を参照してください。

# cXML 文書

WebSphere Partner Gateway 文書マネージャーは、XML 文書のルート・エレメント名 cXML および cXML DOCTYPE (DTD) によって識別されるバージョンにより、cXML 文書を識別します。例えば、以下の DOCTYPE は、cXML バージョン 1.2.009 用です。

```
<!DOCTYPE cXML SYSTEM "http://xml.cXML.org/schemas/cXML/1.2.009/cXML.dtd">
```

文書マネージャーが cXML 文書に対する DTD 検証を実行しますが、WebSphere Partner Gateway は cXML DTD を提供していません。これは、www.cxml.org からダウンロードし、コミュニティー・コンソールの検証マップ・モジュールを使用して WebSphere Partner Gateway にアップロードすることができます。DTD をアップロードした後に、cXML 文書タイプと関連付けます。DTD の cXML 文書タイプへの関連付けについて詳しくは、172 ページの『マップと文書定義の関連付け』を参照してください。

文書マネージャーは、文書管理のために cXML ルート・エレメントの 2 つの属性 payloadID と timestamp を使用します。cXML payloadID と timestamp は、文書 ID 番号および文書タイム・スタンプとして使用されます。いずれも文書管理用にコミュニティー・コンソールで表示可能です。

cXML ヘッダー内の From エレメントと To エレメントには、文書のルーティングおよび認証に使用される Credential エレメントが含まれます。以下の例は、cXML 文書のソースおよび宛先としての From エレメントと To エレメントを示しています。

**注:** この例および本書全体を通して、DUNS 番号はすべて例として示されています。

```
<Header>
<From>
```

```
            <Credential domain="AcmeUserId">
                <Identity>admin@acme.com</Identity>
            </Credential>
            <Credential domain="DUNS">
                <Identity>130313038</Identity>
            </Credential>
</From
<To>
            <Credential domain="DUNS">
                <Identity>987654321</Identity>
            </Credential>
            <Credential domain="IBMUserId">
                <Identity>test@ibm.com</Identity>
            </Credential>
</To>
```

複数の Credential エレメントが使用されている場合、文書マネージャーは、ルーティングおよび認証のビジネス ID として DUNS 番号を使用します。指定されている DUNS 番号がない場合は、最初の信任状が使用されます。

WebSphere Partner Gateway は、Sender エレメントの情報を使用しません。

同期トランザクションでは、cXML 応答文書に From および To ヘッダーは使用されません。応答文書は、要求文書によって確立されたのと同じ HTTP 接続を使用して送信されます。

## cXML 文書タイプ

cXML 文書は、要求、応答、またはメッセージという 3 つタイプのいずれかになります。

### 要求

cXML 要求には、多くのタイプがあります。cXML 文書内の**要求**エレメントは、WebSphere Partner Gateway の文書タイプに対応します。標準的な要求エレメントは、以下のとおりです。

- OrderRequest
- ProfileRequest
- PunchOutSetupRequest
- StatusUpdateRequest
- GetPendingRequest
- ConfirmationRequest
- ShipNoticeRequest

以下の表は、cXML 要求文書のエレメントと WebSphere Partner Gateway 内の文書定義の間の関係を示しています。

**cXML エレメント**
　　**文書定義**

**cXML DOCTYPE**
　　プロトコル

**DTD バージョン**
　　プロトコル・バージョン

**要求 (タイプ) 例: OrderRequest**
文書タイプ

## 応答

ターゲット・パートナーは、cXML 応答を送信して、ソース・パートナーに cXML 要求の結果を通知します。一部の要求の結果にはデータがない場合があるため、応答エレメントにはオプションで状況エレメントのみを含めることができます。また、応答エレメントには、アプリケーション・レベルのデータが含まれることがあります。例えば、PunchOut 時には、PunchOutSetupResponse エレメントにアプリケーション・レベルのデータが含まれます。標準的な応答エレメントは、以下のとおりです。

- ProfileResponse
- PunchOutSetupResponse
- GetPendingResponse

以下の表は、cXML 応答文書のエレメントと WebSphere Partner Gateway 内の文書定義の間の関係を示しています。

**cXML エレメント**
**文書定義**

**cXML DOCTYPE**
プロトコル

**DTD バージョン**
プロトコル・バージョン

**応答 (タイプ) 例: ProfileResponse**
文書タイプ

## メッセージ

cXML メッセージでは、cXML メッセージ・エレメントに WebSphere Partner Gateway 文書タイプ情報が含まれます。このエレメントには、応答エレメント内にあるのと同じオプションの状況エレメントを含めることができます。この状況エレメントは、要求メッセージへの応答となるメッセージで使用されます。

メッセージの内容は、ユーザーのビジネス・ニーズによってカスタム定義されます。<Message> エレメントのすぐ下のエレメントは、WebSphere Partner Gateway で作成された文書タイプに対応しています。以下の例の SubscriptionChangeMessage は文書タイプです。

```
<Message>
<SubscriptionChangeMessage type="new">
           <Subscription>
                <InternalID>1234</InternalID>
                <Name xml:lang="en-US">Q2 Prices</Name>
                <Changetime>1999-03-12T18:39:09-08:00</Changetime>
                <SupplierID domain="DUNS">942888711</SupplierID>
                <Format version="2.1">CIF</Format>
            </Subscription>
</SubscriptionChangeMessage>
</Message>
```

以下の表は、cXML メッセージのエレメントと WebSphere Partner Gateway 内の文書定義の間の関係を示しています。

**cXML エレメント**
**文書定義**

**cXML DOCTYPE**
プロトコル

**DTD バージョン**
プロトコル・バージョン

**メッセージ**
文書タイプ

片方向メッセージと要求/応答文書の違いは、簡単に言うと、要求エレメントや応答エレメントではなく、メッセージ・エレメントがあることです。

メッセージは、以下の属性を持つことができます。

- `deploymentMode`: メッセージがテスト文書であるか、実動文書であるかを示します。指定可能な値は、production (デフォルト) または test です。
- `inReplyTo`: このメッセージが応答するメッセージを指定します。`inReplyTo` 属性の内容は、先に受信したメッセージの payloadID です。この属性は、多くのメッセージを持つ両方向トランザクションを構成する場合に使用します。

## Content-Type ヘッダーと添付文書

すべての cXML 文書には、Content-Type ヘッダーが含まれている必要があります。添付ファイルのない cXML 文書の場合は、以下の Content-Type ヘッダーが使用されます。

- Content-Type: text/xml
- Content-Type: application/xml

cXML プロトコルは、MIME を介して、外部ファイルの添付をサポートしています。例えば、バイヤーは、通常、対応するメモ、図面、FAX などによって仕入れ注文を明確にしなければならない場合があります。添付ファイルを含む cXML 文書では、以下にリストした Content-Type ヘッダーのいずれかを使用する必要があります。

- Content-Type: multipart/related; boundary=<*something_unique*>
- Content-Type: multipart/mixed; boundary=<*something_unique*>

`boundary` エレメントは、MIME メッセージの本文とペイロード部分を区切るために使用される固有のテキストです。詳しくは、www.cxml.org にある「cXML User Guide」を参照してください。

## 有効な cXML 対話

WebSphere Partner Gateway では、以下の cXML 文書定義のインタラクションがサポートされています。

- 外部パートナーから内部パートナーへ: なし/cXML からなし/cXML (パススルーおよび検証あり)

- 内部パートナーから外部パートナーへ:
  - なし/cXML からなし/cXML (パススルーおよび検証あり)
  - なし/XML からなし/cXML (パススルー、検証、および変形あり)

# 文書定義の作成

## このタスクについて

以下のプロセスに従って、cXML 文書の新規文書定義を作成します。

**注:** cXML 文書定義を作成する前に、正しいバージョンの cXML が定義されていることを確認してください。デフォルトはバージョン 1.2.009 です。

1. 「**ハブ管理**」 >「**ハブ構成**」 >「**文書定義**」をクリックします。
2. 「**文書定義の作成**」をクリックします。「文書定義の作成」ページが表示されます。
3. 文書タイプの「**文書タイプ**」を選択します。
4. 文書のタイプに応じて、以下のいずれかのタスクを実行します。
   - 要求の場合は、「**名前**」フィールドに要求タイプ (`OrderRequest` など) を入力します。
   - 応答の場合は、応答に `<Status>` 以外の子タグがない場合は、`Response` と入力します。それ以外の場合は、`<Status>` の後に次のタグ名を入力します。以下の例では、最初の応答エレメントに `Response` を、2 番目の応答エレメントに `Profile Response` と入力します。

```
<cXML>
    <Response>
        <Status code="200" text="OK"/>
    </Response>
</cXML>
<cXML>
    <Response>
        <Status code="200" text="OK"/>
   </ProfileResponse>
    </Response>
</cXML>
```

5. 「**バージョン**」に **1.0** と入力します。

   バージョン番号は参照用です。実際のプロトコル・バージョンは、cXML 文書内の DTD バージョンから派生しています。
6. オプションの「**説明**」を入力します。
7. 「**文書レベル**」に対して「**はい**」を選択します。
8. 「**状況**」に対して「**有効**」を選択します。
9. 「**可視**」のすべての属性に対して「**はい**」を選択します。
10. 「**パッケージ: なし**」フォルダーをクリックして、パッケージ選択オプションを展開します。
11. 「**プロトコル: cXML (1.2.009): cXML**」を選択します。
12. 「**保存**」をクリックします。

## インタラクションの作成

### このタスクについて

文書定義を作成したら、cXML 文書のインタラクションをセットアップします。

対話を作成するには、以下の手順を実行します。

1. 「**ハブ管理**」 >「**ハブ構成**」 >「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」リンクをクリックします。
3. cXML 文書がソースの場合は、「**ソース**」の下で「**パッケージ: なし**」および「**プロトコル: cXML**」を展開し、「**文書タイプ:**<*document _flow*>」を選択します。cXML 文書がターゲットの場合は、「**パッケージ: なし**」および「**プロトコル: cXML**」を展開し、「**ターゲット**」列で「**文書タイプ:** <*document_flow*>」を選択します。
4. もう半分のインタラクション (cXML に変換される文書または cXML から変換される文書) のソースまたはターゲット列を展開し、パッケージおよびプロトコルを展開して、文書タイプを選択します。
5. ページの下部にある「**アクション**」リストから、「**パススルー**」を選択します (「**パススルー**」は、cXML 文書に対してサポートされている、唯一有効なオプションです)。

---

# カスタム XML 文書処理

このセクションでは、他の組み込みルーティング・プロトコルのいずれかで処理されない XML 文書を経路指定するようにハブを構成する方法について説明します。

カスタム *XML* は、組み込みプロトコルのいずれかで処理されない XML 文書を指すために使用される WebSphere Partner Gateway 用語です。

カスタム XML 文書の識別は、消去プロセスによって行われます。固定インバウンド・ワークフロー・プロトコル解析ステップの順序に基づいて、カスタム XML を処理するプロトコル解析ステップが呼び出される前に、ハブは XML 文書をそれぞれの標準プロトコルに一致させようとします。カスタム XML ハンドラーは、標準の XML 文書タイプのいずれにも一致しない XML 文書について呼び出されます。

カスタム XML 文書を処理するには、プロトコル・パーサーが文書から情報を取り出す必要があります。カスタム XML プロトコル・パーサーは、XML 形式、文書プロトコル定義、および文書タイプ定義の集合から、構成を使用する文書を認識および処理するのに必要とする情報を取得します。

カスタム XML プロトコルが作動する方法の概略を示します。

1. XML 文書が解析され、文書 DTD 名、ルート・タグ・ネーム・スペース、およびルート・タグ名の値のうちで存在するものがあれば取得します。
2. 最初のステップで取得された ID に基づいて、XML 形式を含む文書ファミリーのセットが考えられる文書の一致として識別されます。文書ファミリーおよび XML 形式の作成方法については、この後の 163 ページの『XML 形式の作成』で説明します。

3. ファミリーから一致すると考えられる各 XML 形式が文書に適用され、その XML 形式が文書に一致するかどうかが調べられます。一致については、このセクションの後の方で説明します。
4. 一致する XML 形式が見つかった場合、ハブでの文書の処理に使用される文書からデータを取り出すためにその XML 形式が使用されます。一致する XML 形式で構成される文書ファミリーによって、ルーティングに使用される文書プロトコルが決定します。一致する XML 形式自体は、ルーティングに使用される文書タイプを使用して決定を行います。

「XML プロトコルの管理 (Manage XML Protocols)」ページを使用して、文書プロトコルに関連付けられる文書ファミリーを作成できます。次いで、形式ファミリーに文書タイプに関連した XML 形式を取り込むことができます。

XML 形式は以下の 2 つのタイプの情報で構成されます。

- XML 文書から情報を取り出すために使用される XPath 式。
- 定数値として使用されるリテラル・データ。

文書マネージャーは XML 形式を使用して、着信文書を一意的に識別し、正しいルーティングと処理に必要な文書内の情報にアクセスする値を取り出します。

カスタム XML ルーティングのセットアップは複数のステップからなるプロセスです。これを行うには、以下を実行する必要があります。

1. 関連文書のセットを経路指定し、それをパッケージ (複数可) に関連付けるために使用されるプロトコルを作成します。
2. 形式の文書タイプを作成し、それを新規作成したプロトコルと関連付けます。
3. プロトコルで経路指定される文書に一致した XML 形式のセットを保持するための文書ファミリーを作成します。
4. XML 形式を、ファミリー・プロトコルの文書タイプのいずれかにそれぞれ関連付けられたファミリーに追加します。

接続を行えるように、新規文書タイプ間のインタラクションを作成します。

これらのステップについては、以降のセクションで説明します。また、これらのステップの例については、342 ページの『カスタム XML 文書用のハブ設定』を参照してください。

## XML 形式の作成

XML 形式は、カスタム XML 文書からのデータを識別し、それを処理できるように取り出すために使用されます。XML 形式は文書ファミリーに含まれています。文書ファミリーは、共通 DTD 名、ルート・エレメント・タグ、またはルート・エレメント・ネーム・スペースを共有する関連した XML 形式の集合です。したがって、文書ファミリーには、DTD ファミリー、ルート・タグ・ファミリー、およびネーム・スペース・ファミリーという 3 つのタイプがあります。

文書ファミリーには 2 つの役割があります。

- 文書が経路指定される方法を判別できます。実行時に、文書が XML 形式に一致すると、その形式のファミリーに関連したルーティング・プロトコルおよびバージョンを使用して文書が経路指定されます。

- システム内の XML 形式を編成するのに役立ちます。システムを構成する場合、XML 形式をファミリーごとに編成できます。例えば、購買メッセージを Purchasing messages という名前のファミリーにグループ化してから、特定のファミリー内にある形式にアクセスするための文書ファミリーを検索できます。

## 文書ファミリーの作成

### このタスクについて

関連した XML 形式をファミリーにグループ化するには、最初にファミリーを作成する必要があります。文書ファミリーを作成するには、以下を実行します。

1. 「**ハブ管理**」 >「**ハブ構成**」 >「**XML 形式**」をクリックします。
2. 「**文書ファミリーの作成**」をクリックします。
3. 「新規文書ファミリー」ビューで、「**ファミリー名**」を入力します。

   **注:** 複数のファミリーが同じ ID または名前を持つことができます。ID の型と名前の組み合わせによって、固有のファミリー・キーが形成されます。例えば、カスタム XML ハンドラーを使用して SOAP メッセージを経路指定するとします。複数の異なる種類の SOAP メッセージがある場合、すべてがルート・タグ ID としてエンベロープを持つ異なる名前のファミリーにそれらを分類できます。
4. システム内の使用可能なプロトコルのリストから「**プロトコル**」を選択します。カスタム・プロトコルを定義してから、それを使用するファミリーを定義する必要があります。ファミリーの作成後はそのファミリーのプロトコルを変更できないため、事前に計画してください。
5. 「**ラージ・ファイル・オプション**」を選択します。これは、「なし」、「ラージ・ファイル・プロセッサーの使用」、または「ネーム・スペース認識ラージ・ファイル・プロセッサーの使用」のいずれかです。

   「**なし**」は、ファミリー内の XML 形式は XPath バージョン 1.0 式を使用できますが、処理できるファイルのサイズはいくつかの要因によって制限されることを意味します。その要因としては、文書マネージャーのメモリー構成、文書マネージャーの作業負荷、および処理される文書の構造があります。

   「**ラージ・ファイル・プロセッサーの使用**」または「**ネーム・スペース認識ラージ・ファイル・プロセッサーの使用**」は、ファイル・サイズに制限はないものの、ファミリーのメンバーである XML 形式で単純エレメント・パス式を使用することに限定されることを意味します。

   完全な XPath プロセッサーを使用して処理できない大きな文書に一致する XML 形式を作成している場合は、「ラージ・ファイル・オプション」を使用します。「ネーム・スペース認識」オプションを選択する場合、エレメント・パスが文書内に表示される際に、そこにはネーム・スペース・プレフィックスが含まれます。
6. リストから文書の「**ファミリー・タイプ**」である、DTD、ルート・タグ、またはネーム・スペースのいずれかを選択します。

7. 作成しているファミリーのタイプの「**ファミリー ID**」を入力します。

*表 21. ファミリー・タイプの ID*

| ファミリーのタイプ | ID として入力するもの |
|---|---|
| DTD | DTD 名 |
| ルート・タグ | そのファミリー内にあるメッセージのルート・タグ<br>**注:** ネーム・スペース・プレフィックスがある場合は、省略します。 |
| ネーム・スペース | ルート・タグのネーム・スペース |

この ID は XML 形式のファミリーを選択するために実行時に使用されます。その XML 形式のいずれかが文書と突き合わされ、そこから処理情報を取り出すために使用されます。同じ ID を使用する複数のファミリーがある場合、一致するものが見つかるまで、そのすべてのファミリーの形式がメッセージと突き合わせて検査されることに注意してください。

8. 「**保存**」をクリックして新規ファミリーを保存するか、「**キャンセル**」をクリックして文書ファミリーの作成を停止するか、または「**戻る**」をクリックして初期ビューに戻ります。

## 文書ファミリーの検索

### このタスクについて

文書ファミリーを表示するには、最初にそれを検索する必要があります。文書ファミリーを検索するには、以下を実行します。

1. 「**ハブ管理**」 >「**ハブ構成**」 >「**XML 形式**」をクリックします。
2. 表示する文書ファミリーのプロトコルを選択します。
3. ファミリー名が分かっている場合は、入力します。ワイルドカード検索を実行するには、アスタリスク (*) を使用できます。
4. ファミリー・タイプを、「すべてのタイプ」、「DTD」、「ネーム・スペース」、または「ルート・タグ」の中から選択します。
5. ラージ・ファイル・オプションを、「なし」、「ラージ・ファイル・プロセッサーの使用」、または「ネーム・スペース認識ラージ・ファイル・プロセッサーの使用」の中から選択します。
6. 「**検索**」をクリックします。検索条件に一致するすべての文書ファミリーが「検索」ボタンの下に表示されます。
7. 文書ファミリーの詳細を見るには、そのそばにある「**詳細の表示**」アイコンをクリックします。

## 文書ファミリーの編集

### このタスクについて

文書ファミリーの詳細ウィンドウで、ファミリーのプロパティーを編集できます。これを行うには、以下を実行します。

1. ファミリーの詳細ビューにある鉛筆ボタンをクリックして、文書ファミリーの編集ビューを表示します。このビューではプロトコルを変更できないことに注意し

てください。これは、ファミリー内に形式を使用して経路指定されたメッセージがあり、ファミリーに関連したプロトコルが変更されるとデバッグが難しくなることがあるためです。

2. 文書ファミリーの編集ビューで、ファミリー名、ファミリー・タイプ、およびファミリー ID を変更できます。
3. 変更を加えたら、「**保存**」をクリックして変更を保存します。「**キャンセル**」または消された鉛筆ボタンをクリックして、変更を保存せずにファミリーの詳細ビューに戻ります。

## ファミリーへの新規 XML 形式の追加

### このタスクについて

文書ファミリーを作成したら、新規の XML 形式をそのファミリーに追加できます。これを行うには、以下を実行します。

**注:** このセクションでは、XPath 式という用語が頻繁に使用されます。XML 形式がラージ・ファイル・オプションを使用する場合、この用語はエレメント・パス式を意味するために用いられます。これは、文書のルートから値を持つエレメントへの単純パスです。

1. 文書ファミリーの詳細ビューから「**XML 形式の作成**」をクリックします。「XML フォーマット定義」ビューが表示されます。このページは、「**文書タイプ定義**」、「**文書タイプ定義基準**」、「**文書属性**」、および「**ユーザー定義属性**」のヘッダーの下で 4 つのセクションに分割されます。
2. 「**文書タイプ定義**」セクションに入力します。

   「文書タイプ定義」セクションには、文書ファミリーに関連したプロトコルに含まれる文書タイプを載せた選択リストがあります。このリストから「**文書タイプ**」を選択します。文書が XML 形式に一致すると、文書ファミリーに関連したプロトコルおよび形式に関連した文書タイプを使用して文書が経路指定されます。
3. 「**文書タイプ定義基準**」セクションに入力します。

   「**文書タイプ定義基準**」セクションと「**文書属性**」セクションには、ラージ・ファイル・オプションを使用する場合に値およびエレメント・パスを入力するフィールド、またはそれを使用しない場合に XPath 式、プレフィックス・ネーム・スペース、および戻りの型を入力するフィールドがあります。

   **値** このフィールドに、形式 ID の値を入力します。このフィールドは必須です。

   **エレメント・パス**
   このフィールドに、エレメント・パスを入力します。このフィールドは必須です。エレメント・パスは、ラージ・ファイル・オプションを使用する形式にのみ該当することに注意してください。

   **XPath 式**
   このフィールドで、形式に一致する文書の有効な XPath 式、またはすべての文書について定数として戻されるリテラル・ストリング値のいずれ

かを入力します。このフィールドは必須です。XPath 式は、ラージ・ファイル・オプションを使用しない形式でのみ使用されることに注意してください。

**「プレフィックス・ネーム・スペース」フィールド**
このフィールドで、XPath 式で使用される最新のネーム・スペース・プレフィックス (ある場合) の定義を入力します。これは、プレフィックス = ネーム・スペース修飾子の形式で入力されます。例えば、式の最新のネーム・スペース・プレフィックスが SOAPENV で、その修飾子が http://schemas.xmlsoap.org/soap/envelope/ である場合、ネーム・スペース・プレフィックスには SOAPENV=http://schemas.xmlsoap.org/soap/envelope/ を入力します。ラージ・ファイル・オプションを使用する形式には、プレフィックス・ネーム・スペース・フィールドが定義の一部として含まれないことに注意してください。

**戻りの型**
このフィールドで、選択リストから定数、テキスト、またはエレメント・タグ名のいずれかを選択します。すべての文書について XPath 式フィールドをストリング・リテラルとして解釈する場合は、「定数」を使用します。XPath 評価エンジンを使用して文書のコンテキストで式を評価するには、「テキスト」を使用します。式の XPath 評価によって戻される最初のエレメントのエレメント名を取得する場合は、「エレメント・タグ名」を使用します。ラージ・ファイル・オプションを使用する形式には、戻りの型としてエレメント・タグ名がないことに注意してください。

「文書タイプ定義基準」セクションで、値および XPath 式を入力します。文書が処理されて XML 形式が文書に一致するかどうかが判別されるときに、値と式の評価結果が比較されます。文書と形式の間に一致が検出される場合、および形式を使用してソース・ビジネス ID とターゲット・ビジネス ID を検出できる場合、「文書タイプ定義」セクションで指定されたプロトコルおよび文書タイプを使用して文書が経路指定されます。このセクションのフィールドの詳細については、168 ページの表 22を参照してください。

表 22. 「文書タイプ定義基準」フィールド

| フィールド | 必須/オプション | アクション |
|---|---|---|
| フォーマット ID | 必須 | XML 文書内で文書を固有に識別する内容へのパスを定義する XPath 式またはエレメント・パスを入力します。例えば、購入注文用のルート・タグが <PurchasingMessage type=″Purchase Order″> で確認用のルート・タグが <PurchasingMessage type=″Order Confirmation″> の場合、XPath 式 /PurchasingMessage/@type は、一部のメッセージについてはテキスト「Purchase Order」を戻し、その他のメッセージについては「Order Confirmation」を戻します。2 つの XML 形式 (1 つは注文用で、もう 1 つは確認用) が作成され、注文用の「Value」フィールドは「Purchase Order」を表示し、確認用の「Value」フィールドは「Order Confirmation」を表示します。実行時に、適切な形式がシステムによって見つけられます。なぜなら、システムは式評価が値に一致する結果を示す形式を探すからです。一致が検出されると、形式に関連付けられたルーティング文書タイプがシステムによって使用されます。 |
| フォーマット・バージョン | 必須 | 形式バージョンを定義する XPath 式またはエレメント・パスを入力します。形式バージョンは、形式 ID に使用される場合と同様の方法で評価されます。バージョンの式が形式内のバージョン値と一致する場合、ID も一致する場合にはその形式が使用されます。文書のバージョンが 1 つしかない場合、戻りの型が「定数」である式に「1」を入力し、値に「1」を入力できます。これは、バージョンが常に一致しており、一致する形式を判別するのに ID だけが使用されることを意味します。 |

4. 「**文書属性**」セクションに入力します。

   「**文書属性**」セクションで、「**文書タイプ定義基準**」セクションで入力したように値および XPath 式を入力します。このセクションのフィールドの詳細については、表 23を参照してください。

表 23. 「文書属性」フィールド

| フィールド | 必須/オプション | アクション |
|---|---|---|
| ソース・ビジネス ID | 必須 | XML 文書内でソース・ビジネス ID のパスを定義する XPath 式またはエレメント・パスを入力します。これは、ルーティングの目的でソース・パートナーを識別するために使用されます。このデータは使用する形式について検出されなければならないことに注意してください。 |
| ターゲット・ビジネス ID | 必須 | XML 文書内でターゲット・ビジネス ID のパスを定義する XPath 式またはエレメント・パスを入力します。これは、ルーティングの目的でターゲット・パートナーを識別するために使用されます。このデータは使用する形式について検出されなければならないことに注意してください。 |

*表 23. 「文書属性」フィールド (続き)*

| フィールド | 必須/オプション | アクション |
|---|---|---|
| 文書 ID | オプション | XML 文書内で文書 ID 番号のパスを定義する XPath 式またはエレメント・パスを入力します。この値は文書ビューアーで表示されます。 |
| 文書タイム・スタンプ | オプション | XML 文書内で文書作成タイム・スタンプのパスを定義する XPath 式またはエレメント・パスを入力します。この値は文書ビューアーで表示されます。 |
| 重複検査キー 1 から 5 | オプション | 文書が固有かまたは重複かを識別するために使用されるパスを定義する XPath 式またはエレメント・パスを入力します。 |
| 同期フラグ | オプション | この文書タイプに同期応答が必要かどうかを示す *true* または *false* に評価する XPath 式またはエレメント・パスを入力します。値を設定するために文書内容を使用する XPath 式を入力するか、または戻りの型に定数を指定したストリング・リテラル true または false を入力できます。属性 BCGDocumentConstants.BCG_GET_SYNC_RESPONSE は、このフィールドが true に設定される場合に、チャネル解析処理中に BDO で設定されます。 |
| 検証ルート・エレメント | オプション | XML 文書内でエンベロープに入れられたメッセージの内容のルート・ノード (ペイロード) を定義する XPath 式を入力します。WebSphere Partner Gateway は文書の検証をこのエレメントから始めます。これが作動するためには、検証を実行するアクションを指定する必要があります。このフィールドは、ラージ・ファイル・オプションを使用する形式では表示されません。 |
| 関連文書 ID | オプション | 現在の文書が関連付けられている、以前に経路指定された文書の文書 ID を提供する XPath 式またはエレメント・パスを入力します。例えば、Order Confirmation は通常 Purchase Order に関連付けられます。Purchase Order 文書 ID 値は XPath 式を使用して取得できます (上記を参照)。Order Confirmation に Purchase Order ID が含まれる場合、関連した文書 ID 式を使用してそれを取得できます。このようにして、文書ビューアーで文書がリンクされます。 |
| 検索フィールド 1 から 10 | オプション | XML 文書内でカスタム検索に使用する文書内容へのパスを定義する XPath 式またはエレメント・パスを入力します。文書ビューアーで、これらのフィールドの値に基づいて文書を検索できます。 |

5. 「**ユーザー定義属性**」セクションに入力します。

   「**ユーザー定義属性**」セクションで、カスタム・ユーザー定義属性を追加できます。属性を追加するには、入力フィールドにその名前を入力して、「**追加**」をクリックします。次に、該当すれば XPath 式、エレメント・パス、プレフィックス・ネーム・スペースを入力し、この属性の戻りの型を選択して、その他の標準属性に定義したようにこの新規属性を定義します。

属性を追加したら、標準属性が使用された方法と同様にして、これらの属性も使用されます。形式からユーザー定義属性を除去する場合、名前の隣に表示される赤い X をクリックします。ユーザー定義属性は、文書を処理するユーザー作成ハンドラーで使用されることを意図しています。文書が処理されると、属性名とその値がビジネス文書に追加されます。ハンドラー・コードは、定義された名前を使用してビジネス文書から属性名とその値を取得することにより、それらにアクセスできます。詳しくは、「*WebSphere Partner Gateway Programmer Guide*」を参照してください。

6. このビューで値を入力した後、下にスクロールし、「**保存**」をクリックして変更を保存します。変更をキャンセルしてファミリー要約ビューに戻るには、「**キャンセル**」または消された鉛筆ボタンをクリックします。

## プロトコル定義の作成

### このタスクについて

ここでは、カスタム XML プロトコル定義形式の作成方法について説明します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」>「**文書定義の作成**」をクリックします。
2. 「**文書定義タイプ**」で、「**プロトコル**」を選択します。
3. 「**名前**」に、文書定義の ID を入力します。例えば、カスタム XML プロトコルの場合は、Custom_XML と入力します。このフィールドは必須です。
4. 「**バージョン**」に、プロトコルのバージョンの値を入力します。数値またはストリング値が許可されます。
5. (オプション) プロトコルの説明を入力します。
6. 文書タイプではなくプロトコルを定義するため、「**文書レベル**」を「**いいえ**」に設定します (文書タイプの定義については、次のセクションを参照してください)。
7. 「**状況**」を「**有効**」に設定します。
8. このプロトコルの「**可視/不可視**」を設定します。一般には、すべてのパートナーに対して可視に設定します。
9. この新規プロトコルがラップされるパッケージを選択します。例えば、このプロトコルを AS、なし、バックエンド統合の各パッケージに関連付ける場合は、「**パッケージ: AS**」、「**パッケージ: なし**」、「**パッケージ: バックエンド統合**」を選択します。
10. 「**保存**」をクリックします。

## 文書タイプ定義の作成

### このタスクについて

次に、再度「文書定義の作成」ページを使用して、文書タイプを作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」>「**文書定義の作成**」をクリックします。
2. 「**文書定義タイプ**」で、「**文書タイプ**」を選択します。
3. 「**名前**」に、文書定義の ID を入力します。例えば、文書タイプの名前として `Purchase order` を入力します。このフィールドは必須です。

4. 「**バージョン**」に、文書タイプのバージョンの値を入力します。数値またはストリング値が許可されます。
5. 文書タイプのオプションの説明を入力します。
6. 「**文書レベル**」を「**はい**」に設定します (実際の文書に対応するルーティング・オブジェクトを定義しているため)。
7. 「**状況**」を「**有効**」に設定します。
8. このフローの「**可視/不可視**」を設定します。一般には、すべてのパートナーに対して可視に設定します。
9. ステップ 9 (170 ページ) で選択した各パッケージを展開するために、「**展開 (Expand)**」アイコンをクリックします。フォルダーを展開し、前のセクションで作成したプロトコルの名前を選択します (例: プロトコル: Custom XML)。
10. 「**保存**」をクリックします。

例の値を使用した場合、「文書定義の管理」ページには、AS、なし、およびバックエンド統合パッケージの下に、文書タイプ Purchase order およびプロトコル Custom XML が含まれるようになります。

## 構成の終了

プロトコル定義が定義された後、XML 文書ファミリーに使用するためのルーティング・プロトコルとしてそれを選択できます。文書タイプをプロトコルに追加した後、それらを文書ファミリーにある XML 形式定義に割り当てることができます。ファミリー内の形式に一致するメッセージは、そのファミリーに関連したプロトコルおよび一致する形式に関連した文書タイプを使用して経路指定されます。

新規定義を使用するチャネルを定義するには、その前に新規プロトコルおよび文書タイプとその他のプロトコルおよび文書タイプの間のインタラクションを有効にする必要があります。また、パートナーの B2B 機能を有効にして、パートナーが新規プロトコルおよび文書タイプを使用して文書を送受信できるようにする必要もあります。

## カスタム XML ファイルの XSD ファイルに対する検証

カスタム XML の基本的なセットアップ (文書タイプ定義、XML ファミリーと XML 形式、B2B 機能、および接続の作成) が完了し、単純なアクション「パススルー」を使用して XML をルーティングする準備が整ったら、以下のステップを実行して、パススルー前に XML を検証できるようにします。

1. 「**接続**」ページで、「*カスタム XML パススルー (検証あり)*」を新規アクションとして設定します。
2. 「**ハブ管理**」 >「**ハブ構成**」 >「**文書定義**」にナビゲートします。
3. カスタム XML 文書の「**属性値の編集**」アイコン (青い矢印) をクリックします。
4. 「**マップのアップロード**」を選択します。
5. 対応する XSD ファイルを選択し、「**アップロード**」をクリックします。
6. ステップ 2 から 3 を繰り返します。
7. 「**属性の追加**」をクリックして、文書定義コンテキスト属性を追加します。
8. 「**検証マップ**」を選択し、「**保存**」をクリックします。

9. 「**アカウント管理**」>「**接続**」で、接続を検索します。
10. 接続の**ソース**側で「**属性**」をクリックします。
11. 縮小されたノード・アイコン (青いフォルダー) を展開して、文書タイプを探します。
12. 「**検証マップ**」ドロップダウンから XSD 検証マップを選択し、「**保存**」をクリックします。

XSD ファイルのより新しいバージョンをアップロードする必要がある場合、古いバージョンをまず削除する必要があります。これは、「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**検証マップ**」ページで実行できます。新規マップをアップロードしたら、ステップ 12 を繰り返してください。マップを削除すると、この接続属性がリセットされるためです。

# 検証マップの使用

WebSphere Partner Gateway では、検証マップを使用して特定の文書の構造を検証します。検証マップと文書を関連付けるには、最初にその検証マップが WebSphere Partner Gateway で使用可能であることを確認します (『検証マップの追加』を参照)。検証マップの管理については、*「WebSphere Partner Gateway E/A 管理ガイド」の『ハブ管理者タスク』の章*を参照してください。

## 検証マップの追加

### このタスクについて

宛先のパートナーやバックエンド・システムが文書を構文解析できるように、アクションに検証マップを関連付けることができます。なお、検証マップは文書の*構造*のみを検証することに注意してください。メッセージの内容については検証されません。

**注:** 検証マップと文書定義を一度関連付けたら、その関連付けを解除することはできません。

新しい検証マップをハブに追加するには、以下の手順を実行します。

1. 検証マップ・ファイルをハブに保管するか、WebSphere Partner Gateway がファイルを読み取ることのできる場所に保管します。
2. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**検証マップ**」をクリックします。
3. 「**作成**」をクリックします。
4. 検証マップの説明を入力します。
5. 文書の検証に使用するスキーマ・ファイルにナビゲートして、「**オープン**」をクリックします。
6. 「**保管**」をクリックします。

## マップと文書定義の関連付け

### このタスクについて

検証マップと文書定義を関連付けるには、以下の手順を実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**検証マップ**」をクリックします。

2. 文書定義と関連付ける検証マップの横にある「**詳細の表示**」アイコンをクリックします。
3. パッケージの横にある「**展開 (Expand)**」アイコンをクリックして、個々に適切なレベルまで (例えば、RosettaNet 文書では「**アクション**」など) 展開します。
4. 検証マップと関連付ける文書定義を選択します。
5. 「**保存**」をクリックします。

## 変換マップの使用

### このタスクについて

WebSphere Partner Gateway は変換マップを使用して、文書を 1 つの形式から別の形式に変換します(例えば、XML 文書を EDI に変換)。

以下は、変換マップを使用するためのステップを示したものです。

1. WebSphere Partner Gateway 管理コンソールにログインします。
2. 「**ウィザード**」をクリックします。
3. EIF インポート・ウィザードで、**ブラウズ**して、.EIF ファイルのロケーションを指定します。
4. 「**インポート**」をクリックします。
5. 「要約をインポートする」ページで、「**次へ**」をクリックします。
6. 「変換マップを検討し、作成されるインタラクションを変更する」画面で変換マップを選択し、インタラクションを追加し、作成されたインタラクションのアクションを選択します。
7. 「**終了**」をクリックします。

## 文書の表示

### このタスクについて

文書ビューアーは、文書タイプを構成する文書に関する情報を表示します。ロー文書とそれに関連する文書処理の詳細およびイベントを、特定の検索条件を使用して表示することができます。文書が正常に配信されたかどうかを調べたり、問題の原因を判別するときに、この情報が役に立ちます。

文書ビューアーを表示するには、以下を実行します。

1. 「**ビューアー**」>「**文書ビューアー**」をクリックします。
2. 該当する検索条件を選択してください。
3. 「**検索**」をクリックします。

文書ビューアーの使用法については、「*WebSphere Partner Gateway E/A 管理ガイド*」を参照してください。

## 否認防止ロギングの構成

メッセージの否認防止ロギングを構成するには、文書の送付に使用されるパッケージ、プロトコル、または文書フローの属性を使用します。これは「否認防止が必要」属性です。この属性の値は「はい」または「いいえ」です。属性定義はルーティング・オブジェクト・レベルで行われていますが、B2B 機能レベルまたは接続レベルで変更することによりオーバーライドすることができます。

## メッセージ・ストアの構成

文書のルーティングに使用されるパッケージ、プロトコル、または文書フローの属性を使用して、メッセージ・ストアを構成することができます。この属性の名前は「メッセージ・ストアが必要」で、属性の値は「はい」または「いいえ」です。この属性はルーティング・オブジェクト・レベルで定義されていますが、B2B 機能レベルまたは接続レベルで変更することによりオーバーライドすることができます。

# 第 10 章 EDI 文書フローの構成

この章では、標準の EDI 交換向けに文書定義とインタラクションを構成する方法について説明します。また、XML 文書とレコード指向データ (ROD) 文書の受信および変換についてもこの章で説明します。この章では以下のトピックを扱います。

- 『EDI の概要』
- 179 ページの『XML 文書と ROD 文書の概要』
- 180 ページの『文書タイプ作成と属性設定の概要』
- 182 ページの『有効なフローの概要』
- 187 ページの『変換エンジンの概要』
- 188 ページの『 バックエンドからのトランザクションのエンベロープ』
- 192 ページの『WTX 統合およびポリモアフィック・マップのエンベロープ』
- 188 ページの『 EDI 交換の処理方法』
- 192 ページの『 XML 文書または ROD 文書の処理方法』
- 194 ページの『EDI 環境の設定』
- 207 ページの『文書交換の定義』
- 225 ページの『 EDI 交換およびトランザクションの表示』

EDI 交換では、エンベロープ解除や変換を実施しなくても、情報をやり取りできます。このタイプの交換に必要な対話を作成するステップについては、113 ページの『パススルー・アクションによる EDI 文書』を参照してください。

**注:** WebSphere Partner Gateway の構成変更を行う場合は、必ず、コミュニティー・コンソールにログインしたときと同じブラウザー・インスタンスを使用してください。複数のブラウザー・インスタンスを同時に使用すると、構成変更が無効になる可能性があります。

## EDI の概要

EDI とは、承認済みの国家標準または業界標準で情報を変換および交換することに同意した仕事関係者間でビジネス情報をネットワーク経由で伝送する手段のことです。WebSphere Partner Gateway は、以下の EDI 標準に対してエンベロープ解除、変換、およびエンベロープを実施する機能を備えています。

- X12。米国規格協会で承認されている共通の EDI 標準です。
- UN/EDIFACT (United Nations Electronic Data Interchange for Administration Commerce and Support)。
- UCS (Uniform Communication Standard)

以下のセクションでは、X12、EDIFACT、および UCS 標準に準拠した EDI 交換と、それぞれの EDI 交換に含まれるトランザクションおよびグループについて概説します。また、XML 文書、ROD 文書、および EDI 交換がどのように変換されるのかについても説明します。

## EDI 交換の構造

EDI 交換には、1 つ以上のビジネス・トランザクションが含まれています。X12 およびその関連する標準では、ビジネス・トランザクションは*トランザクション集合*と呼ばれています。EDIFACT およびその関連する標準では、ビジネス・トランザクションはメッセージと呼ばれています。本書では、通常、X12 または UCS のトランザクション集合や EDIFACT メッセージのことを*トランザクション* または*ビジネス・トランザクション* と呼びます。

EDI 交換はいくつかのセグメントで構成されており、各セグメントにはデータ・エレメントが含まれています。データ・エレメントとは、具体的には名前、数量、日付、時間などのことです。セグメントとは、関連するデータ・エレメントが 1 つにまとめられたグループのことです。セグメントは、その先頭に表示されるセグメント名またはセグメント・タグで識別されます。(データ・エレメントは、名前では識別されません。その代わり、区切ることを目的として予約された特殊な区切り文字で区切られています。)

トランザクション内の詳細またはデータ・セグメントを管理目的用に使用するその他のセグメントと区別すると、便利な場合があります。管理目的のセグメントは、X12 では*制御セグメント*と呼ばれ、EDIFACT ではサービス・セグメントと呼ばれています。EDI 交換の境界を区切るエンベロープ・セグメントは、こうした制御セグメントやサービス・セグメントの一例です。

EDI 交換に含まれるセグメントには、3 つのレベルがあります。どのレベルでも、先頭にはヘッダー・セグメントがあり、末尾にはトレーラー・セグメントがあります。

どの交換にも、交換ヘッダー・セグメントと、交換トレーラー・セグメントがあります。

交換には、1 つ以上のグループを含めることができます。各グループには、1 つ以上の関連するトランザクションが含まれています。グループにもレベルがあり、EDIFACT ではオプションですが、X12 およびその関連する標準では必須です。複数のグループが含まれている場合、それぞれのグループごとにグループ・ヘッダーとグループ・トレーラー・セグメントがあります。

グループ (グループが存在しない場合には交換) には、1 つ以上のトランザクションが含まれています。各トランザクションには、トランザクション集合ヘッダーおよびトランザクション集合トレーラーがあります。

トランザクションは、購入注文などのビジネス・ドキュメントになります。ビジネス・ドキュメントの内容は、トランザクション集合ヘッダー・セグメントとトランザクション集合トレーラー・セグメントの間にある明細セグメントで示されます。

各 EDI 標準では、交換内にデータを表示する方法をそれぞれ独自に規定しています。以下の表は、サポートされている 3 つの EDI 標準のセグメントを示しています。

*表 24. サポートされている EDI 標準のセグメント*

| 標準のセグメント | X12 | UCS | EDIFACT |
|---|---|---|---|
| 交換開始 | ISA | BG | UNB |
| 交換終了 | IEA | EG | UNZ |
| グループ開始 | GS | GS | UNG |
| グループ終了 | GE | GE | UNE |
| トランザクション開始 | ST | ST | UNH |
| トランザクション終了 | SE | SE | UNT |

図 22 では、X12 交換とそれを構成するセグメントの例を紹介しています。

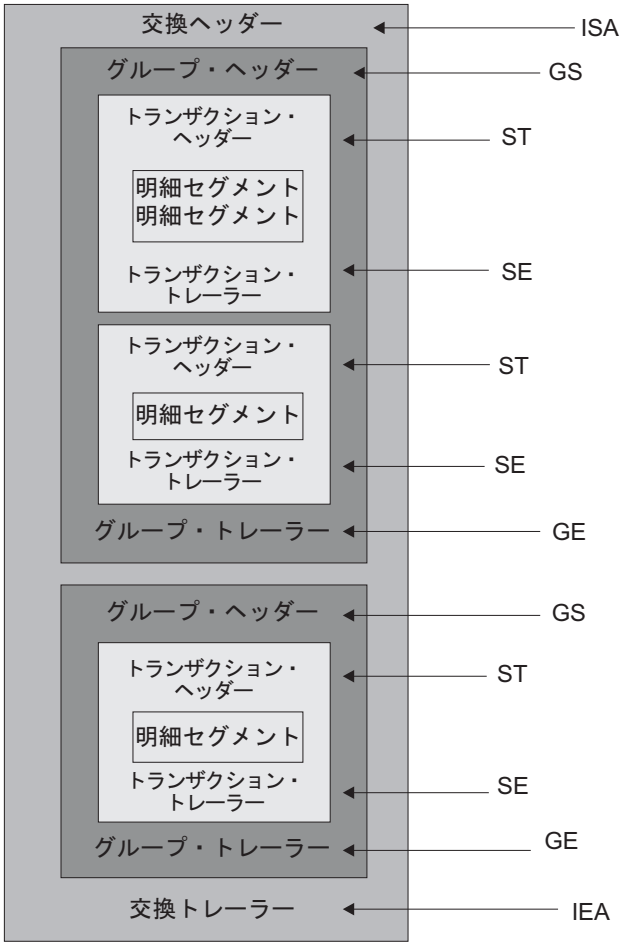



*図 22. 交換エンベロープ*

## マップ

Data Interchange Services クライアントのマッピング担当者が、形式の異なる文書間の変換方法を記述した変換マップを作成します。例えば、X12 トランザクションを EDIFACT メッセージに変更する変換マップなどがあります。また、EDI トランザクションを XML 文書またはレコード指向データ文書に変換することもできます。

マップは、DIS または WTX design studio を使用して作成します。DIS は WDI 変換用のマップを作成するために使用し、WTX design studio は WTX 変換の場合に使用します。DIS を使用して作成したマップは WTX 変換用にマイグレーションできず、再書き込みする必要があります。両方とも動作可能な場合は、アクションに応じて変換エンジンが選択されます。

マップを作成するには、ソース文書およびターゲット文書の定義が必要です。EDI 用のソース文書の定義は WDI 自体によって提供されますが、ROD および XML の場合は DIS クライアントを使用して作成する必要があります。この標準をランタイム・コードで使用するために、コンパイルする必要があります。以前のバージョンでは標準に対する変換マップが必要でしたが、このバージョンでは変換マップがなくてもコンパイルできます。EDI の標準の EIF をインポートしますが、ROD の場合は DIS クライアントを使用して作成します。XML の場合、DTD/XSD は開発データベースにインポートします。EDI の場合は、管理コンソールで EDI ウィザードに移動します。EIF ファイルで使用可能なデータ形式/標準が表示されます。すべて一括してインポートすることも、1 つ以上を選択してインポートすることもできます。正常に選択されている場合は、標準の制御ストリングが実行時データベースにインポートされます。

変換マップでは、1 つの文書から複数の文書を作成することもできます。このタイプのマップでは、マップ・チェーニング を使用して、単一トランザクションから複数の出力を生成します。マップ・チェーニングでは、ソース文書が正常にターゲット文書に変換された後、後続のマップを使用して再度そのソース文書が別のターゲット文書を生成するために変換されます。これを何度も繰り返して、必要な数だけの文書を生成できます。

変換マップのほかに、機能確認通知マップと検証マップも使用できます。機能確認通知マップは、機能確認通知の生成方法に関する指示を記載したものです (機能確認通知は、EDI 文書が相手に届いたことを送信側に通知するものです)。WebSphere Partner Gateway をインストールすると、EDI 標準の機能確認通知マップがいくつかインストールされます。この各マップのリストについては、222 ページの『確認通知の設定』を参照してください。

送信時には、ハブは機能確認通知を必要とします。確認通知時間内に機能確認通知を受信しなかった場合は、元の文書が再送されます。再試行の回数および再試行間隔は構成可能です。この機能は、デフォルトではオンになっていません。EDI プロパティーの値を手動で設定する必要があります。「確認通知までの時間 (Time to acknowledgement)」を「はい」に設定する場合は、再試行の回数および間隔の値も設定する必要があります。再試行イベントは、モニターの目的でログに記録されます。FA なしで再試行回数の上限に達した場合は、モニターの目的で該当するイベントがログに記録されます。

Data Interchange Services クライアントのマッピング担当者は、このほかに別の機能確認通知マップを作成することもできます。WebSphere Partner Gateway は、EDI トランザクションが検証されたときに、EDI トランザクションに関連する機能確認通知マップがあれば、機能確認通知を生成します。ソース文書は、EDI 文書でなければなりません。

WebSphere Partner Gateway では、標準レベルの検証で EDI 文書が検証されます。機能確認通知を生成しようとすると、EDI 文書の検証結果が保管されます。EDI 文

書に対してさらに検証を行うには、検証マップを作成します。機能確認通知の生成時には、機能確認通知マップと EDI 文書の検証結果が使用されます。機能確認通知マップにはマッピング・コマンドが記載されており、特定の機能確認通知を作成するために検証結果をどのように使用するかを示します。検証プロセスが文書を変換対象として承認すると、適切なデータ変換マップを使用してソース文書が変換されます。

## XML 文書と ROD 文書の概要

Data Interchange Services クライアントのマッピング担当者は、XML 文書およびレコード指向データ文書の文書定義を作成し、それぞれのタイプの文書を別のタイプの文書に変換する変換マップを作成できます。

### XML 文書

XML 文書は、XML DTD または XML スキーマによって定義されます。Data Interchange Services クライアントのマッピング担当者は、この DTD またはスキーマに基づいて変換マップを作成し、XML 文書を別の形式にどのように変換するかを記述します。XML 文書は、別の XML 文書、レコード指向データ文書、または EDI トランザクションに変換できます。

### ROD 文書

レコード指向データ (ROD) とは、専有の形式に準拠した文書のことです。Data Interchange Services クライアントのマッピング担当者が ROD 文書定義を定義します。これは、ビジネス・アプリケーションが文書内のデータを構造化する方法を定義したものです。文書定義を定義したら、マッピング担当者は ROD 文書を別の ROD 文書、XML 文書、または EDI トランザクションに変換するためのマップを作成できます。

### スプリッターと複数の文書

XML 文書または ROD 文書は、個々の文書として、または同じファイル内の文書のグループとして、ハブに参加させることができます。同じファイルに複数の文書が存在する場合があります。例えば、パートナーまたは内部パートナーのスケジュールされたジョブによって送信対象の文書が定期的にアップロードされる場合などです。複数の XML 文書または ROD 文書が 1 つのファイルで届いた場合は、レシーバーが関連するスプリッター・ハンドラー (XMLSplitterHander または RODSplitterHandler) を呼び出してその一連の文書を分割します。 (スプリッター・ハンドラーは、ターゲットを作成すると構成されます。78 ページの『 前処理』を参照してください。) その後文書が再び文書マネージャーに導入されて、個別に処理されることになります。

**注:** 送信側 ID および受信側 ID は、変換マップに関連付けられている ROD 文書定義に含まれている必要があります。また、文書タイプおよびディクショナリー値を判別するために必要な情報も、文書定義に含まれている必要があります。変換マップを作成する場合、Data Interchange Services クライアントのマッピング担当者が、これらの要件を把握していることを確認してください。

1 つのファイルで複数の EDI 交換を送信することもできます。複数の EDI 交換が 1 つのファイルで届いた場合は、レシーバーが EDISplitterHandler を呼び出してその一連の交換を分割します。その後交換が再び文書マネージャーに導入されて、個別に処理されることになります。

**注:** 分割は、交換について分割が行われるのであって、交換内の個々のトランザクションについて行われるわけではありません。交換内のトランザクションには、エンベロープ解除が行われます。

## 文書タイプ作成と属性設定の概要

文書定義は、少なくともパッケージ、プロトコル、文書タイプで構成されています。文書定義では、WebSphere Partner Gateway で処理される文書のタイプを指定します。

パッケージ化とは、AS2 などの仕様に従って文書をパッケージ化するために必要なロジックです。プロトコル・フローとは、EDI-X12 など特定のプロトコルに準拠する文書を処理するために必要なロジックです。文書タイプとは、文書がどのようになっているかを記述したものです。

以下のセクションでは、内部パートナーと外部パートナー間の文書フローを設定するためのステップ全体について概説します。また、これらのセクションでは属性を設定できるポイントについても説明します。

### ステップ 1: 文書定義が使用可能であることを確認する

#### このタスクについて

どの文書も、文書に対して文書定義を定義しなければ送受信できません。WebSphere Partner Gateway には、機能確認通知を表すものも含め、デフォルトの文書定義がいくつか用意されています。EDI トランザクション、XML 文書、または ROD 文書の変換マップをインポートすると、それに関連付けられた文書定義が「文書定義」ページに表示されます。同じく、まだ定義されていない機能確認通知マップをインポートすると、その確認通知の文書定義が「文書定義」ページに表示されます。文書定義は、独自に作成することもできます。

文書定義を作成するときに、いくつかの属性を変更することができます。属性は、検証や暗号化の検査、再試行カウントなどのさまざまな文書処理やルーティングの機能を実行する目的で使用されます。文書定義レベルで設定した属性は、関連するパッケージ、プロトコル、または文書タイプのグローバル設定となります。使用可能な属性は、文書定義によって異なります。EDI 文書定義の属性は、RosettaNet 文書定義の属性とは異なります。

例えば、ISA 文書タイプ・レベルで「**TA1 要求を許可**」の値を指定した場合、その設定値はすべての ISA 文書に適用されます。その後、パートナーまたは内部パートナーの B2B 機能レベルで「**TA1 許可属性**」を設定した場合は、その値で文書定義レベルの値がオーバーライドされます。

文書定義の複数のレベルで設定可能な属性では、文書タイプ・レベルで設定された値がプロトコル・レベルで設定された値よりも優先し、プロトコル・レベルで設定された属性がパッケージ・レベルで設定された属性よりも優先します。例えば、

&X44TA1 プロトコル・レベルでエンベロープ・プロファイルを指定し、さらに TA1 文書タイプ・レベルでも別のエンベロープ・プロファイルを指定している場合、TA1 文書タイプ・レベルで指定したエンベロープ・プロファイルが使用されます。

インタラクションを作成する前に、「文書定義の管理」ページに文書タイプをリストする必要があります。

## ステップ 2: 対話を作成する

### このタスクについて

次のステップとして、インタラクションを設定します。インタラクションは、パートナーの接続を作成するためのテンプレートとなります。対話により、文書の着信の仕方、文書に対して実行される処理、文書をハブから送信する方法を通知します。

プロトコルによっては、(パートナーまたは内部パートナーから送信されて) ハブで受信される文書を記述するフローと、ハブから (パートナーまたは内部パートナーに) 送信される文書を記述するフローの 2 つのフローのみが必要な場合があります。ただし、ハブで送受信する EDI 交換がエンベロープ解除されて個々のトランザクションに分割されたり、確認通知を必要としたりするものである場合は、実際には複数の対話を作成します。例えば、ハブで EDI 交換を受信する場合、交換をハブに送信する方法、およびそれをハブで処理する方法を記述した対話を作成します。また、ハブ内のトランザクションごとに、トランザクションの処理方法を記述した対話も作成することになります。ハブから送信される EDI 交換では、交換のエンベロープを宛先に送信する方法を記述した対話を作成します。

## ステップ 3: パートナーのプロファイル、宛先、および B2B 機能を作成する

### このタスクについて

次に、内部パートナーおよび外部パートナーのパートナー・プロファイルを作成します。宛先と B2B 機能も定義します。宛先は文書の送信先を決定するもので、B2B 機能は内部パートナーまたはパートナーが送受信可能な文書を指定するものです。「B2B 機能」ページには、既に定義されている文書タイプがすべて表示されます。

B2B 機能レベルで属性を設定できます。このレベルで設定した属性は、文書定義レベルで設定された属性をオーバーライドします。例えば、「**TA1 要求を許可**」を ISA 文書の文書定義レベルで「**いいえ**」に、B2B 機能レベルでは「**はい**」に設定した場合、「**はい**」の値が使用されます。B2B レベルで設定された属性は、特定のパートナーに合わせて調整できます。

プロトコル・レベルまたは文書タイプ・レベルでエンベロープ・プロファイルを設定し (つまり、「文書定義の管理」ページで設定)、次に「B2B 機能」ページで同じエンベロープ・プロファイルに別の値を設定した場合、後者の値が使用されます。

内部パートナーおよび外部パートナーのプロファイルと B2B 機能を定義してから、これらの間の接続を作成する必要があります。

## ステップ 4: 接続をアクティブ化する

### このタスクについて

最後に、内部パートナーおよび外部パートナー間の接続をアクティブ化します。使用可能な接続は、パートナーの B2B 機能と作成したインタラクションに基づいて決まります。インタラクションは、使用可能な文書定義によって異なります。

交換によっては、接続が 1 つだけ必要になることがあります。例えば、パートナーが内部パートナーのバックエンド・アプリケーションにバイナリー文書を送信する場合、必要な接続は 1 つのみです。ただし、EDI 交換のうち、エンベロープが解除されるものや、個々のトランザクションが変換されるものでは、複数の接続を確立します。

**注:** そのままの状態でやり取りされる EDI 交換では、必要な接続は 1 つのみです。

属性は接続レベルで設定できます。このレベルで設定した属性は、B2B 属性レベルで設定された属性をオーバーライドします。例えば、「**TA1 要求を許可**」を B2B 機能レベルでは「**はい**」に、接続レベルでは「**いいえ**」に設定した場合、「**いいえ**」の値が使用されます。接続レベルで属性に値を設定することで、関連するパートナーとアプリケーションのルーティングの要件に応じて、属性をさらに調整することができます。

# 有効なフローの概要

ここでは、WebSphere Partner Gateway で実行可能な変換のタイプについて概説します。これらの変換の詳細と設定に必要な作業については、207 ページの『文書交換の定義』で説明します。

## EDI 間のフロー

WebSphere Partner Gateway では、パートナーまたは内部パートナーから EDI 交換を受信し、それをタイプの異なる EDI 交換に変換し (例えば、EDI-X12 から EDIFACT への変換など)、変換後の文書を内部パートナーまたはパートナーに送信することができます。EDI 交換が別の EDI 交換に変換されるときには、以下のステップが実行されます。

1. ハブに届いた EDI 交換のエンベロープが解除されます。
2. EDI 交換内の個々のトランザクションが受信側の EDI 形式に変換されます。
3. 変換された EDI トランザクションがエンベロープされて受信側に送信されます。

183 ページの図 23 は、3 つのトランザクションがエンベロープ解除される X12 交換を示しています。まず各トランザクションが EDIFACT 形式に変換され、その後エンベロープされてパートナーに送信されます。

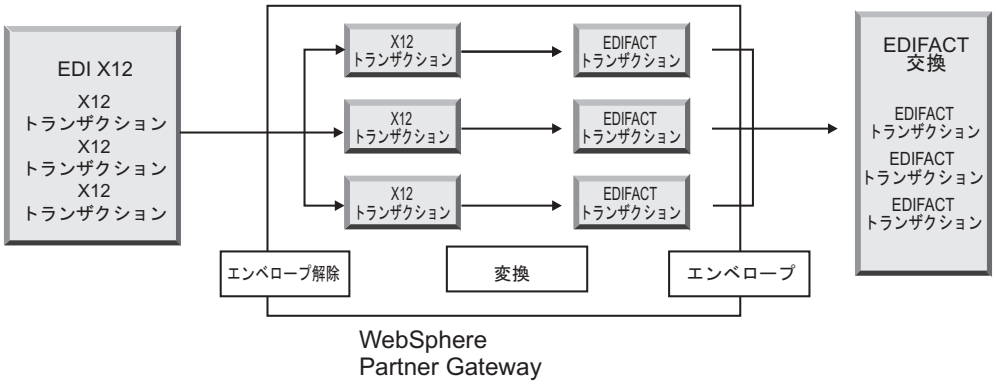



*図 23. EDI 交換間のフロー*

トランザクションのそれぞれに変換マップが関連付けられており、そのマップにはトランザクションをどのように変換するかが指定されています。トランザクションは、単一トランザクションに変換することができます。マップの作成時にマップ・チェーニングが使用されている場合は、複数のトランザクションに変換できます。エンベローパーのバッチ機能がオンになっている場合、1 つのエンベロープとしてハブに入るトランザクションは、1 つのエンベロープとしてハブから出ます。ただし、エンベロープのブレークポイントがある場合 (例えば、EDI 属性に異なる値が指定されている場合やエンベロープ・プロファイルが異なる場合)、またはバッチ機能がオフの場合、トランザクションは別々のエンベロープとしてハブから送信されます。エンベローパー (パートナーに送信される一連のトランザクションを収集し、それらをエンベロープに包んで送信するコンポーネント) の一般的な説明は、194 ページの『エンベローパー』を参照してください。バッチ機能についての詳細は、 195 ページの『バッチ・モード』を参照してください。

また、トランザクションに検証マップを関連付けることもできます。

## EDI から XML または ROD へのフロー

WebSphere Partner Gateway では、パートナーまたは内部パートナーから EDI 交換を受信し、その交換のエンベロープを解除し、解除後の EDI トランザクションを XML 文書または ROD 文書に変換することができます。

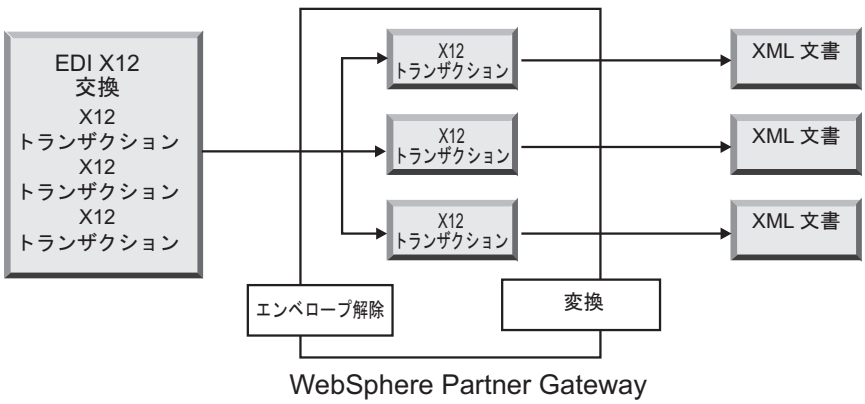



*図 24. EDI 交換から XML 文書へのフロー*

トランザクションは、単一文書に変換することができます。マップの作成時にマップ・チェーニングが使用されている場合は、複数の文書に変換できます。

## XML または ROD から EDI へのフロー

WebSphere Partner Gateway では、パートナーまたは内部パートナーから XML 文書または ROD 文書を受信し、それを EDI トランザクションに変換し、そのトランザクションをエンベロープして内部パートナーまたはパートナーに送信することができます。

図 25 に、XML 文書が X12 トランザクションに変換され、その後エンベロープされる様子を示します。

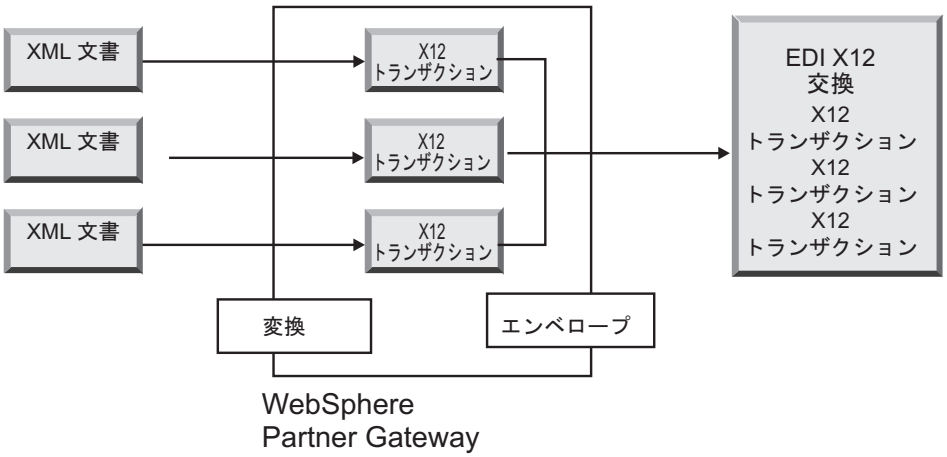



*図 25. XML 文書から EDI 交換へのフロー*

1 つの文書を複数のトランザクションに変換することができ (マップ・チェーニングを使用してマップが作成された場合)、その各トランザクションを別の交換としてエンベロープすることができます。図 26 は、3 つの X12 トランザクションに変換される XML 文書を示しています。このうちの 2 つのトランザクションは、一緒にエンベロープされます。残りの 1 つは、別のエンベロープに含められます。

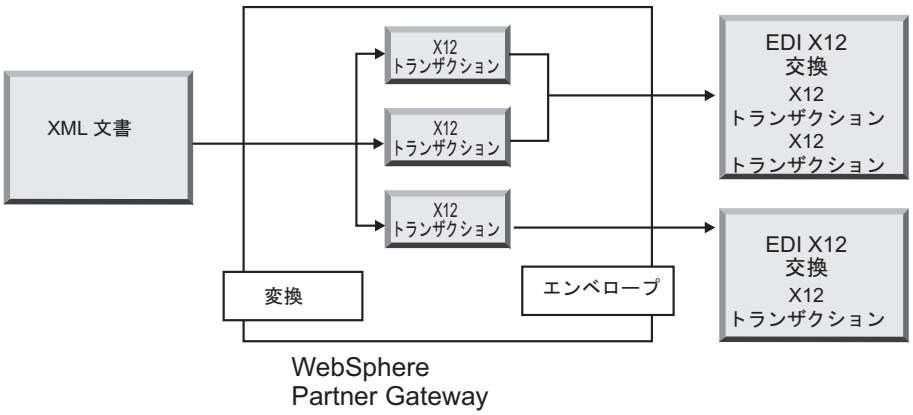



*図 26. XML 文書から複数の EDI トランザクションへのフロー*

## 複数の XML 文書または ROD 文書から EDI 交換へのフロー

WebSphere Partner Gateway では、パートナーまたは内部パートナーから 1 つ以上の XML 文書または ROD 文書からなるファイルを受信し、文書を EDI トランザクションに変換し、その EDI トランザクションを複数のエンベロープに包んで内部パートナーまたはパートナーに送信することができます。

各文書は、単一トランザクションに変換することができます。マップの作成時にマップ・チェーニングが使用されている場合は、複数のトランザクションに変換できます。

**注:**

1. 1 つのファイルで送信する各文書は、タイプが同じである必要があります。XML 文書か ROD 文書のどちらか一方のみで、両者を混在させることはできません。
2. どの ROD 文書も、同じタイプのものである必要があります。

図 27 は、個々の XML 文書に分割される一連の XML 文書を示しています。各 XML 文書が X12 トランザクションに変換され、それぞれのトランザクションがエンベロープされます。

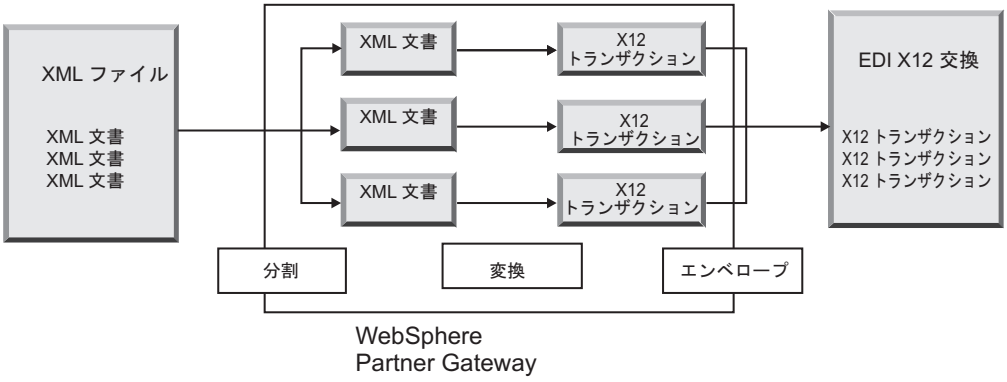



*図 27. 複数の XML 文書から EDI 交換へのフロー*

図 27 では、文書は (XML スプリッター・ハンドラーによって) 分割され、変換されたトランザクションが一緒にエンベロープされます。このシナリオを実行するためには、XML スプリッター・ハンドラーの BCG_BATCHDOCS オプションがオン (デフォルト値) に設定されていることが必要です。BCG_BATCHDOCS がオンに設定されており、エンベローパーのバッチ・モードがオンであれば、これらのトランザクションを同じ EDI エンベロープに入れることができます。エンベローパーのバッチ・モード属性については、 195 ページの『バッチ・モード』で説明します。

## XML から ROD、または ROD から XML へのフロー

WebSphere Partner Gateway では、パートナーまたは内部パートナーから XML 文書または ROD 文書を受信し、それを他のタイプの文書に変換し (XML から ROD、または ROD から XML への変換)、その文書をパートナーまたは内部パートナーに送信することができます。

186 ページの図 28 は、ROD 文書に変換される一連の XML 文書を示しています。

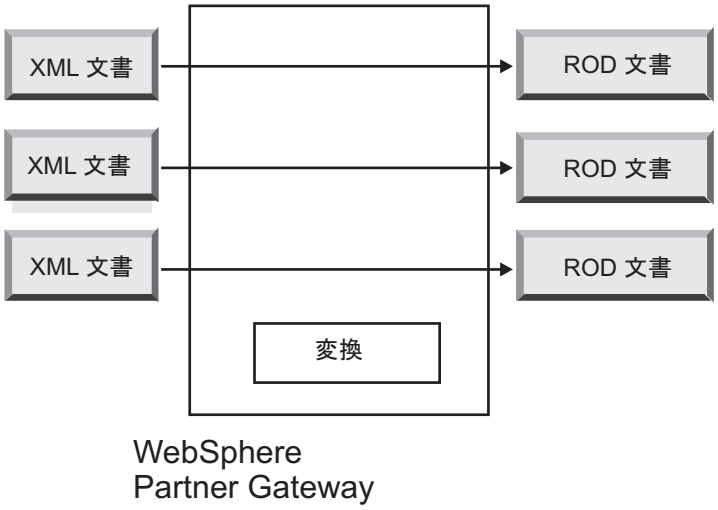



*図 28. XML 文書から ROD 文書へのフロー*

文書は、単一文書に変換することができます。マップの作成時にマップ・チェーニングが使用されている場合は、複数の文書に変換できます。

## XML から XML、または ROD から ROD へのフロー

WebSphere Partner Gateway では、パートナーまたは内部パートナーから XML 文書または ROD 文書を受信し、それを同じタイプの文書に変換し (XML から XML、または ROD から ROD への変換)、その文書をパートナーまたは内部パートナーに送信することができます。

図 29 は、別の形式の XML 文書に変換される XML 文書を示しています。

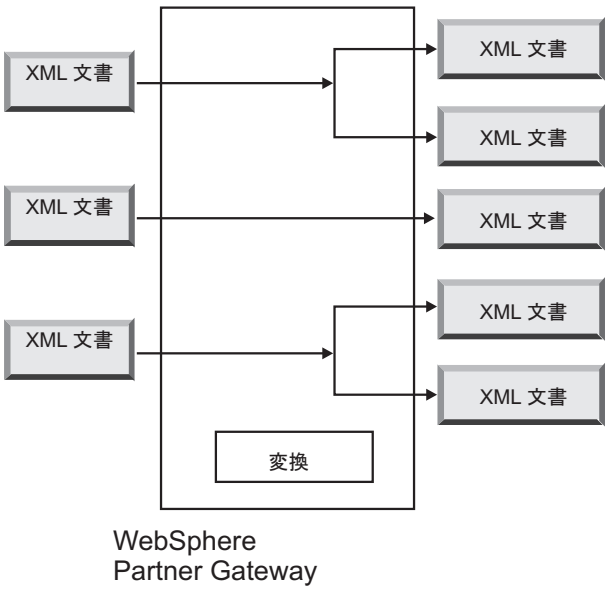


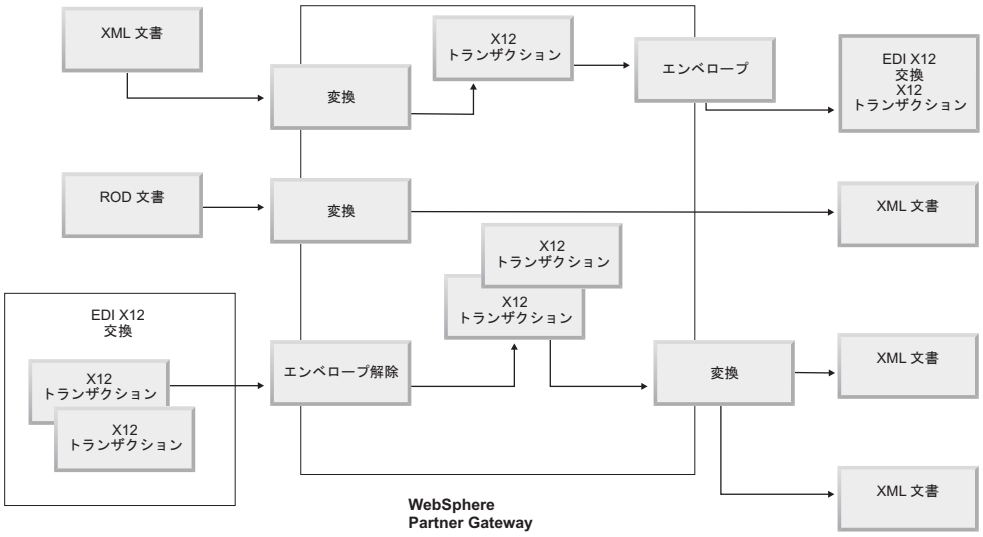

*図 29. XML 文書から XML 文書へのフロー*

文書は、単一文書に変換することができます。マップの作成時にマップ・チェーニングが使用されている場合は、複数の文書に変換できます。

## Any から Any へのフロー

WTX では、任意の形式を任意の形式に変換できます。マップの作成には WTX design studio を使用します。フローには、ROD から Any、XML から Any、および EDI から Any があります。必要な場合は、必ず文書を分割するためのスプリッターを構成してください。ROD がソース文書である場合は、ルーティング情報も設定する必要があります。XML がソース文書の場合は、XML 形式で必要なルーティング情報が提供されます。フローによってアクションは以下のように異なります。

- ROD から Any - WTX 変換
- XML から Any - WTX 変換
- EDI から Any - EDI エンベロープ解除 (交換をトランザクションにエンベロープ解除する場合)。その後、EDI リエンベローパーおよび WTX 変換のアクションを使用して、トランザクションを再エンベロープし、それらを EDI - Any 形式に変換します。トランザクションを検証する必要がある場合は、EDI 検証を行います。エンベロープ解除せずに交換を検証する場合は、EDI 交換の検証を行います。




## 変換エンジンの概要

WebSphere Partner Gateway は、ネイティブ WDI および WTX の 2 種類の変換エンジンをサポートしています。

**ネイティブ WDI** - ネイティブ WDI の場合、変換マップは DIS クライアントで作成します。WebSphere Partner Gateway は、WDI と統合するための各種アクション (EDI エンベロープ解除、EDI 変換、EDI 検証、EDI 再エンベロープ、EDI エンベロープ、ROD 変換、および XML 変換) を提供しています。ネイティブの WDI であるため、統合のために別途構成する必要はありません。

**WTX** - WTX design studio を使用して変換マップを作成します。WebSphere Partner Gateway は、WTX と統合するための各種アクション (WTX 変換、EDI 交換の検証、EDI エンベロープ解除、EDI 検証、EDI 再エンベロープ、および EDI エンベロープ) を提供しています。WTX の場合は、RMI とネイティブの 2 つの方法があります。WebSphere Partner Gateway と同じマシンに WTX をインストールしていない場合は、RMI をお勧めします。WTX をリモート側から呼び出すための手順は以下のとおりです。

1. DTXHome ディレクトリーで rmiserver.properties ファイルを開き、プロパティーを変更します。例えば、ポート番号を設定できます。
2. DTXHome ディレクトリーから startrmiserver.bat を実行します。
3. 「コンソール共通 (Console Common)」プロパティーにホスト名 (RMI サーバーが稼働しているホスト) およびポート番号を指定します。RMI サーバーのオプションを「はい」に設定します。
4. マップの物理的な場所を指定します。

ネイティブの場合は、WTX ホーム・ディレクトリーとしてシステム・パスを設定します。また、rmiuseserver のプロパティーを「いいえ」に設定します。

## バックエンドからのトランザクションのエンベロープ

非同期の場合に WTX を使用するとき、バックエンド・アプリケーションは、WTX によって生成された EDI トランザクションをコンシュームし、バックエンド・パッケージ化標準でエンベロープするために WebSphere Partner Gateway に送信します。トランザクションの詳細を指定するために、デフォルトのバックエンド・ヘッダーが使用されます (x-aux-senderid、x-aux-receiverid、x-aux-protocol、x-aux-protocol-version、x-aux-process-type、x-aux-process-version、および BCG_DOCSYNTAX)。バックエンド・パッケージ・ヘッダーには、EDI ディクショナリー/プロトコル (X12v4R1 など) に関する情報と、上記で規定されているヘッダーに対するプロセス・トランザクション情報 (850 など) が入れられます。WTX エンベロープ・アクションのセクションを参照してください。

## EDI 交換の処理方法

一般的に、ハブに届いた EDI 交換は、エンベロープ解除され、それから個々のトランザクションが処理されます。多くの場合、標準の EDI トランザクション (X12 850 や EDIFACT ORDERS (購入注文) など) は、バックエンド・アプリケーションが認識する形に変換されます。また、相手に交換が届いたことを示す機能確認通知がパートナーに送信されるのが普通です。したがって、EDI 交換のやり取りでは複数のアクション (EDI エンベロープ解除、EDI 変換、EDI 検証、EDI エンベロープ、EDI 検証交換、EDI 再エンベロープ、WTX 変換、WTX エンベロープ) が必要になります。例えば、交換に 2 つのトランザクションが含まれている場合に、確認通知を必要なしとすると、WebSphere Partner Gateway は以下のアクションを実行します。

1. 交換のエンベロープを解除します。

   WebSphere Partner Gateway は、交換レベル、グループ・レベル、およびトランザクション・レベルでエンベロープ・ヘッダーおよびトレーラー・セグメントから交換に関する情報を抽出します。これには以下の情報が含まれています。

- 交換レベルでは、送信側および受信側であるパートナーのビジネス ID、使用標識 (交換が実稼働環境向けか、テスト環境向けかを指定するもの)、および交換が作成された日時です。
- グループ・レベルでは、送信側および受信側のアプリケーション ID、およびグループが作成された日時です。
- トランザクション・レベルでは、トランザクションのタイプです (X12 850 や EDIFACT ORDERS など)。
- 個々のトランザクションに対する検証が必要な場合は、EDI がエンベロープ解除されます。検証が完了すると、検証されたトランザクションがエンベロープされ、変換エンジン (WDI または WTX での処理) またはアクションに応じた宛先に送信されます。

2. 関連付けられたマップに従って最初のトランザクションを変換します。
3. 関連付けられたマップに従って 2 番目のトランザクションを変換します。
4. 変換後の文書をバックエンド・アプリケーションに配信します。

同じく、内部パートナーのバックエンド・アプリケーションで生成された文書をハブが送信するときにも、文書は標準の EDI トランザクションに変換されます。変換後の EDI トランザクションは、エンベロープされてからパートナーに送信されます。EDI 交換を受信する場合と同じように、EDI 交換を作成し、エンベロープし、送信する場合にも、複数のアクションが必要になります。

個々のトランザクション、グループ、および交換は、制御番号で識別されます。交換が発生すると、WebSphere Partner Gateway がこの制御番号を設定します。ただし、制御番号は 204 ページの『制御番号』に示すように、カスタマイズすることもできます。

以下の図は、AS としてパッケージ化されている EDI 交換がパートナーから送信される全体像を示しています。その最終目的は、変換された 2 つの XML 文書を内部パートナーのバックエンド・システムの 2 つの異なる宛先に配信することです。この例では、850 トランザクションが、バックエンド・アプリケーションが処理できる購入注文に変換されます。890 トランザクションは、バックエンド・アプリケーションが処理できる倉庫出荷命令に変換されます。

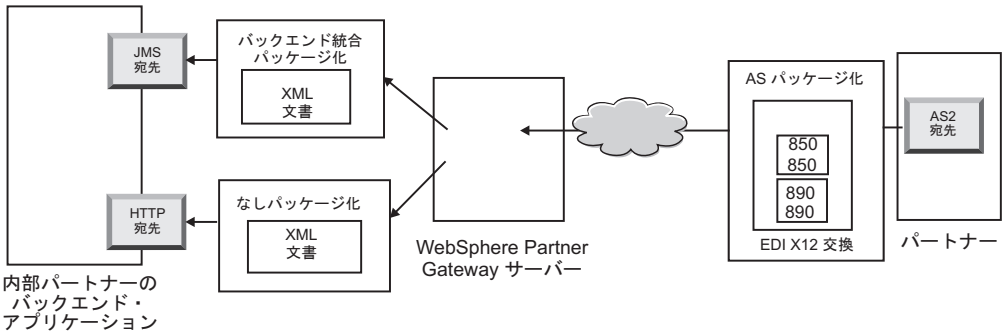



*図 30. パートナーから内部パートナーへのフローの全体像*

この交換では、パートナーから内部パートナーまで 1 つの接続ではなく、3 つの接続を必要としています。

- 1 つはパートナーからハブまでの接続で、交換のエンベロープを解除するためのものです。これは中間ステップであるため (交換はエンベロープ解除されますが、パートナーに配信されません)、パートナー接続のターゲット側は該当なしです。

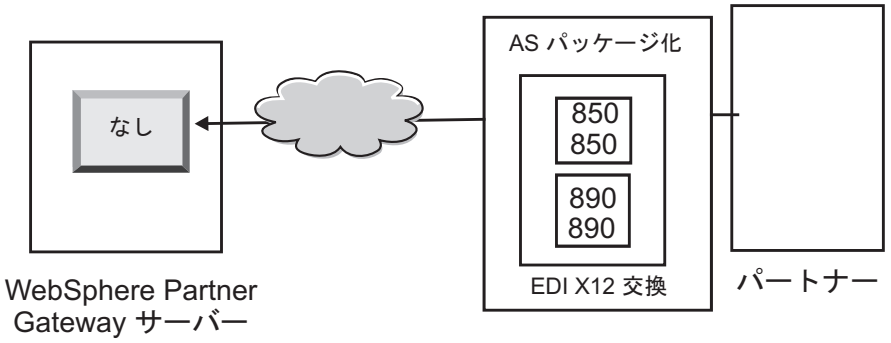



*図 31. エンベロープ解除の接続*

- 2 つ目は最初のトランザクションを変換して内部パートナーの JMS 宛先に配信するための接続で、3 つ目は 2 番目のトランザクションを変換して内部パートナーの HTTP 宛先に配信するための接続です。

  トランザクションは、システムによってエンベロープ解除された元の交換に届いているため、ソース・パッケージ化は適用されません。したがって、トランザクションのソース側で、パートナー接続に「**パッケージ化: N/A (Packaging: N/A)**」を指定する必要があります。

  XML に変換され、JMS を介してバックエンド・アプリケーションに送信されるトランザクションの場合、このトランザクションのパートナー接続のターゲット宛先を内部パートナーの JMS 宛先として指定する必要があります。XML に変換され、HTTP を介してバックエンド・アプリケーションに送信されるトランザクションの場合は、このトランザクションのパートナー接続のターゲット宛先を HTTP 宛先として指定する必要があります。

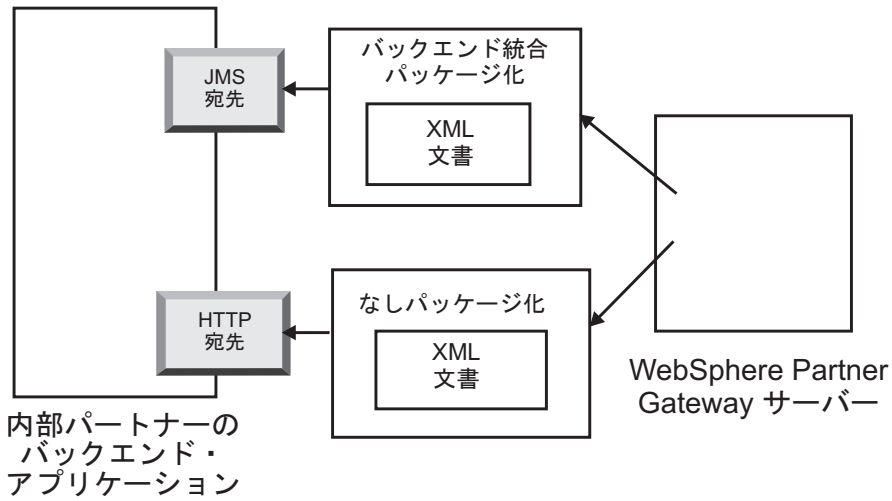



*図 32. 個々のトランザクション用の接続*

交換と個々のトランザクションを表示する場合に、文書ビューアーを使用することができます。個々のトランザクションは文書ビューアーから見れば、交換の子 です。文書ビューアーを使用すると、ソース交換またはターゲット交換に関連付けられた子、および子に関連付けられたイベントを表示することができます。文書ビューアーについては、「*WebSphere Partner Gateway E/A 管理ガイド*」の『イベントおよび文書の表示』のセクションを参照してください。

送信側から確認通知を求められた場合は、さらに接続を追加する必要があります。

- 各確認通知をパートナーに送り返すための接続です。機能確認通知はシステムによって生成されるため、パートナー接続のソース側で「**パッケージ化: N/A (Packaging: N/A)**」を指定する必要があります。機能確認通知は、エンベロープされた後配信されるため、パートナー接続のターゲット側でも、「**パッケージ化: N/A (Packaging: N/A)**」を指定する必要があります。スケジュールを設定しておけば、エンベローパーがそのスケジュールに従って各確認通知を収集します。スケジュールの設定については、 194 ページの『エンベローパー』を参照してください。
- パートナーに送り返す前に確認通知をエンベロープするための接続も必要です。エンベロープはシステムによって生成されるため、パートナー接続のソース側で「**パッケージ化: NA (Packaging: NA)**」を指定する必要があります。パートナー接続のターゲット側では、ターゲット宛先をパートナーの宛先に設定する必要があります。この場合、「**パッケージ化: AS**」を指定します。エンベロープは、EDI 標準のデフォルトのものを使用することも、カスタマイズすることもできます。エンベロープのカスタマイズについては、 196 ページの『 エンベロープ・プロファイル』を参照してください。

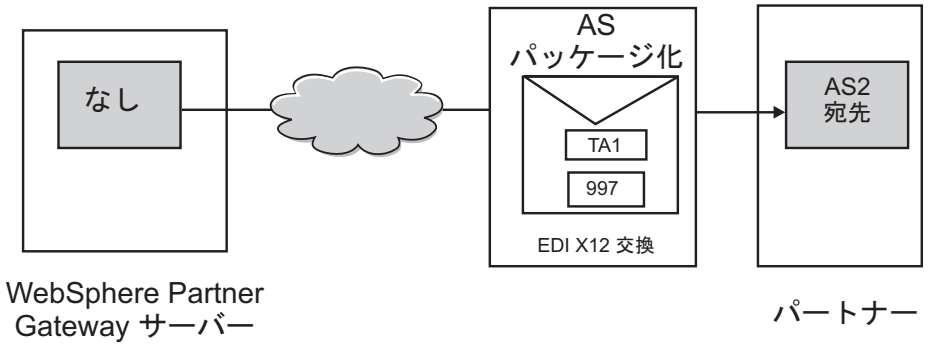



*図 33. 確認通知のエンベロープおよびオリジネーターへの送信*

## 同期的な変換

WTX は、単一のマップを使用して任意の形式を任意の形式に変換する機能を提供します。変換のために WTX API を直接呼び出すためのオプションが提供されています。エンベロープ解除されて検証されたトランザクションは、エンベロープ後に WTX に送信されて処理されます。

**注:** 使用可能な各種の EDI 形式については、 175 ページの『EDI の概要』を参照してください。

**単一の出力** - 再送信属性により、出力文書をワークフローに再導入するか、アウトバウンド・ワークフローに直接送信して処理するかが決定されます。

**複数の出力** - 再送信フラグに基づいて、子が直接アウトバウンド・ワークフローに渡されるか、固定のインバウンド・ワークフローに再送信され、新しいチャネルにパススルーされます。

### 非同期の変換

内部パートナーが外部パートナーに非同期的にメッセージを送信する場合、外部パートナーは、変換のために WESB/WMB または WTX を使用できます。WTX は JMS 宛先と見なされるため、構成は不要です。WTX は、処理後の文書をバックエンドに送信します。WebSphere Partner Gateway に情報は返されません。JMS ゲートウェイに正常に送達されると、EDI 文書に送信済みのマークが付けられます。

## XML 文書または ROD 文書の処理方法

XML 文書または ROD 文書は、個々の文書または同じファイル内の文書のグループとしてハブで受信されます。同じファイル内の文書のグループとしてハブに届いたときには、WebSphere Partner Gateway は以下のアクションを実行します。

1. 文書のセットを個々の文書に分割します。
2. 関連付けられたマップに従って各文書を変換します。
3. 文書を EDI トランザクションに変換する場合は、そのトランザクションをエンベロープしてバックエンド・アプリケーションに配信します。文書を XML 文書または ROD 文書に変換する場合は、変換後の文書をそのままバックエンド・アプリケーションに配信します。

XML 文書または ROD 文書が単一の文書として届いた場合には、WebSphere Partner Gateway は以下のアクションを実行します。

1. 関連付けられたマップに従ってその文書を変換します。
2. 文書を EDI トランザクションに変換する場合は、そのトランザクションをエンベロープしてバックエンド・アプリケーションに配信します。文書を別の XML 文書または ROD 文書に変換する場合は、その文書をバックエンド・アプリケーションに配信します。

同じく、内部パートナーのバックエンド・アプリケーションで生成された文書をハブが送信するときにも、文書は XML 文書、ROD 文書、または EDI トランザクションに変換されます。EDI トランザクションの場合は、エンベロープされてからパートナーに送信されます。EDI 交換を受信する場合と同じように、文書を変換する場合、変換後のトランザクションをエンベロープする場合、および EDI 交換を送信する場合にも、複数のアクションが必要になります。

## WTX 統合およびポリモアフィック・マップのエンベロープ

WebSphere Partner Gateway では、メタデータ・タイプ・ツリーが定義されています。各カードにデータの種類を構成し、それに関する情報を設定することができます。一般に、以下のプロパティーを構成することが期待されます。プロパティーの名前および値は、大/小文字が区別されます。ブール値に限り、大/小文字が区別されません。

*表 25. メタデータ・タイプ・ツリーのプロパティー*

| プロパティー名 | プロパティー値 | 説明 |
|---|---|---|
| BCG_DOCSYNTAX | EDI_INTERCHANGE<br>EDI_TRANSACTION<br>XML ROD | 出力がエンベロープされた EDI 交換の場合は、EDI_INTERCHANGE を設定する必要があります。出力が EDI トランザクションであり、エンベロープされていない場合は、EDI_TRANSACTION を設定する必要があります。XML および ROD 出力の場合は、それに応じて XML および ROD を設定する必要があります。 |
| BCG_REENVELOPE | true/false | この値が true で、BCG_DOCSYNTAX が EDI_INTERCHANGE の場合は、EDI エンベロープがエンベロープ解除されます。エンベロープ解除後、生成された各トランザクションは、今後のステップに使用可能な個別の文書とみなされます。 |
| BCG_REROUTE | true/false | この値が true の場合、文書は転送されます。値が false で、出力が単一の場合は、既存の BDO が新規ファイルに更新されて送信されます。 |
| ProtocolName | 適宜 | 出力文書のプロトコル名。ReRoute が true に設定されている場合は必須です。これは、転送される文書のチャネルを選出するために使用されます。 |
| ProtocolVersion | 適宜 | 出力文書のプロトコル・バージョン。ReRoute が true に設定されている場合は必須です。これは、転送される文書のチャネルを選出するために使用されます。 |
| ProcessCode | 適宜 | 出力文書のプロセス・コード。ReRoute が true に設定されている場合は必須です。これは、転送される文書のチャネルを選出するために使用されます。 |
| ProcessVersion | 適宜 | 出力文書のプロセス・バージョン。ReRoute が true に設定されている場合は必須です。これは、転送される文書のチャネルを選出するために使用されます。 |
| SegmentCountElementName | SE01/UNT01 | 出力が EDI_TRANSACTION の場合は、この属性を指定する必要があります。この属性は、目的とするエンベロープの種類に応じて設定する必要があります。 |
| SegmentCount | 適宜 | 出力が EDI_TRANSACTION の場合は、この属性を指定する必要があります。この属性には、トランザクションのセグメント数に関する情報が設定されます。 |

変換後のターゲットが EDI の場合は、外部パートナーに送信する前にエンベロープする必要があります。変換された出力文書では、形式を任意に組み合わせることができます。これは、メタデータ・カードのカード番号に何がコード化されるかによって異なります。これには、他のカード詳細のプロパティーが含まれます。マップの作成者がカードをコード化します。検討の対象となる属性は、ReRoute、ReEnvelope、および DocSyntax です。ReRoute および ReEnvelope には True または False 値を設定できるのに対し、DocSyntax にはユーザーによって入力される任意の値を設定できます。DocSyntax の値が ediInchg の場合のみ、エンベロ

ープ解除対象とみなされます。 ReRoute 値および ReEnvelope 値のそれぞれの組み合わせで考えられる結果について、以下に説明します。docSyntax は EDI_INTERCHANGE に設定されていることを前提とします。

- ReRoute = True、ReEnvelope = False: 文書はその他の文書 (XML または ROD) と同様に処理されます。
- ReRoute = False、ReEnvelope = False: 文書はその他の文書 (XML または ROD) と同様に処理されます。
- Reroute = True, ReEnvelope = True: 文書は最初にエンベロープ解除されます。子トランザクションごとに、子 bdo が作成されます。ディクショナリーおよび文書は、プロトコルおよびプロセスとして設定されます。この ChildBDO (トランザクション) がそれぞれ N/A パッケージを使用して転送されます。適切なチャネルが存在しなければなりません。このチャネルのターゲット属性にエンベローパー・プロファイルを構成できます。エンベロープが流れるための別個のチャネルを作成する必要があります。
- Reroute = False、Reenvelope = True: 文書は最初にエンベロープ解除されます。出力として単一トランザクションが生成される場合は、ロケーションとしてビジネス文書がこのトランザクション・ファイルに更新され、送信されます。出力として多数のトランザクションが生成される場合は、子 BDO が非転送として作成され、送信されます。このチャネルのターゲット属性は、エンベローパー・プロファイルに応じて適切に構成されていることが求められます。エンベローパーが流れるチャネルが存在しなければなりません。

## EDI 環境の設定

前のセクションで触れたように、EDI 交換のやり取りに関連する数多くの属性を指定できます。例えば、製品提供のエンベロープ・プロファイルを変更したり、特定の接続に使用する固有のエンベロープを定義したり、交換の各要素に割り当てられる制御番号を設定したり、同じ交換を異なる方法で配信できるように接続プロファイルを設定したりできます。ここでは、この各作業について説明します。

### エンベローパー

エンベローパーは、パートナーに送信される一連のトランザクションを収集し、それらをエンベロープに包んで送信するコンポーネントです。送信待機中のトランザクションをいつエンベローパーで探すかを WebSphere Partner Gateway に指示する必要があるため、エンベローパーをスケジュールします (デフォルトのスケジュールのままでもかまいません)。また、ロック時間、キュー存続期間、およびバッチ・モードのデフォルト値を更新することもできます。

**注:** エンベローパーの設定はオプションです。エンベローパーのどの値も変更しない場合は、製品提供のデフォルト値が使用されます。

#### ロック

文書マネージャーのインスタンスごとにエンベローパーが用意されます。文書マネージャーを 2 つシステムにインストールすれば、エンベローパーも 2 つになります。したがって、エンベローパーのインスタンスを 2 つ以上使用して、エンベロープ待機中のトランザクションをポーリングすることも可能です。特定のトランザクションが 1 つだけのエンベローパーによってポーリングされるように設定するため

に、ロックが使用されます。ロックによって、複数のエンベローパーが関与する場合に、1 つのエンベローパーのみが特定のトランザクションをポーリングし、処理するように設定できます。複数のエンベローパーが同時にポーリングしますが、別々のトランザクションに対して機能します。

ロックには、制限時間が設定されます。エンベローパーのインスタンスがロックを保持できる時間のデフォルト値は 240 秒です。

ロックの待機が必要な場合、エンベローパーはキューに入れられます。最大キュー存続期間 (エンベローパーが待機しなければならない時間) は 740 秒です。

通常は、ロック用のデフォルト値を変更する必要はありません。

## バッチ・モード

1 つのファイルで到着した複数の文書は、その文書のタイプに設定してあるスプリッター・ハンドラーに従って分割されます。(ターゲットの定義の一部であるスプリッター・ハンドラーの構成については、 78 ページの『構成ポイントの変更』で説明しています。) スプリッター・ハンドラーの属性の 1 つに BCG_BATCHDOCS があります。BCG_BATCHDOCS をオン (デフォルト値) に設定すると、スプリッターは文書の分割後に文書にバッチ ID を追加します。

エンベローパーには、BCG_BATCHDOCS 属性に関連したバッチ・モード用の属性があります。個々の文書にバッチ ID が割り当てられている場合に、バッチ・モードのデフォルト値 (オン) を受け入れると、エンベローパーは、トランザクションが一緒にエンベロープされるように、同じファイルで一緒に到着した文書すべてを処理してからエンベロープして送信します。例えば、5 つの XML 文書が同じファイルで届いたとします。各 XML 文書は、EDI トランザクションに変換されて、同じ受信側に配信されることになります。この文書を 3 つのみ変換した時点で、エンベローパーがあらかじめスケジュールされたトランザクションのポーリングを開始します。バッチ・モードを選択していれば、準備の整った 3 つのトランザクションをエンベローパーが処理 (エンベロープ) することはありません。そうではなく、5 つすべてのトランザクションの処理が完了するまで待機し、それから各トランザクションをエンベロープして送信します。適用可能な EDI 標準で回避していないかぎり、各トランザクションは同じエンベロープに包まれます。

## デフォルト値の変更

### このタスクについて

エンベローパーのデフォルト値を変更するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**EDI**」>「**エンベローパー**」をクリックします。
2. 「**編集**」アイコンをクリックします。
3. 「**最大ロック時間 (秒)**」属性および「**最大キュー存続期間 (秒)**」属性に割り当てられている時間を増減する場合は、新しい値を入力します。

   **注:** 通常は、デフォルト値を変更する必要はありません。
4. バッチ・モードをオフにする場合は、「**バッチ・モードの使用**」の横にあるチェックを外します。
5. 送信待機中のトランザクションをエンベローパーがチェックする回数を変更する場合は、以下の一連の作業のいずれかを実行します。

- 間隔ベースのスケジューリング (デフォルト値) の時間を変更するには、「**間隔**」の横に新しい時間を入力します。例えば、この値を 30 秒に変更すると、エンベローパーが 30 秒おきに文書をチェックし、対象の文書をエンベロープして受信側に送信するようになります。
- カレンダー・ベースのスケジューリングを使用するには、以下の作業を実行します。
  a. 「**カレンダー・ベースのスケジューリング**」をクリックします。
  b. スケジューリングのタイプ (「**日次スケジュール**」、「**週次スケジュール**」、または「**カスタム・スケジュール**」) を選択します。
     – 「**日次スケジュール**」を選択した場合は、エンベローパーが文書をチェックする時刻 (時分) を選択します。
     – 「**週次スケジュール**」を選択した場合は、時刻のほかに曜日を 1 つ以上選択します。
     – 「**カスタム・スケジュール**」を選択した場合は、まず時刻を選択し、次に週および月について「**範囲**」または「**選択できる日**」を選択します。「**範囲**」では、開始日と終了日を指定します。(例えば、平日の特定の時刻にのみエンベローパーに文書をチェックさせる場合は、「**月**」および「**金**」をクリックしてください。) 「**選択できる日**」では、週および月の特定の日付を選択します。

6. 「**保存**」をクリックします。

## エンベロープ・プロファイル

エンベロープ・プロファイルによって、エンベロープの特定のエレメントに配置される値が決まります。エンベロープ・プロファイルは、文書定義の「**エンベロープ・プロファイル**」属性で EDI トランザクションに割り当てます。 WebSphere Partner Gateway には、サポートされている標準 (X12、EDIFACT、または UCS) ごとに定義済みのエンベロープ・プロファイルが用意されています。この定義済みの各エンベロープ・プロファイルを直接使用することも、変更することも、新しいエンベロープ・プロファイルにコピーすることもできます。エンベロープ・プロファイルを変更または作成するステップについては、 197 ページの『デフォルト値の変更』を参照してください。

エンベロープ・プロファイルには、エンベロープ標準のエレメントごとに 1 つのフィールドがあります。また、プロファイルには、トランザクション集合、メッセージ、機能グループ、および交換のヘッダーまたはトレーラー・セグメントとなるリテラル・データまたは定数データを用意しておくことができます。ここで用意する値は、取り込む必要があり、かつ別のソースに用意されていない値のみにします。

フィールド名が、容易に相互参照できるように意図されています。例えば、UNB03 フィールドは UNB セグメントの 3 番目のデータ・エレメントです。

197 ページの『 エンベロープ属性』で説明しているように、エンベロープ・プロファイルで設定した値よりも、他の場所で設定した属性の方が優先されます。属性の中には、文書定義関連の属性またはマップでオーバーライドできるものもあります。

## エンベロープ属性

エンベロープ属性は、構成プロセス中にいくつかの異なるポイントで設定することができます。また、文書に関連付けられた変換マップに設定することもできます。例えば、Data Interchange Services クライアントのマッピング担当者は、マップの定義時に CtlNumFlag プロパティーを指定できます。このプロパティーは、エンベロープ・プロファイルの一部として (「**トランザクション ID 別制御番号**」フィールドで) 設定することもできます。変換マップで設定した属性は、コミュニティー・コンソールで設定した関連する値よりも優先されます。例えば、変換マップで CtlNumFlag に **N** (いいえ) を設定し、「**トランザクション ID 別制御番号**」フィールドに **Y** (はい) の値を入力した場合、この項目の値として使用されるのは **N** の値です。

エンベロープ・プロファイルは、このほか、プロトコル・レベルで設定したり (パートナーに関連付けられた「文書定義の管理」ページまたは「B2B 機能」ページ)、接続の一部として設定したりすることもできます。優先順位は、以下のようになっています。

1. 変換マップで設定したプロパティーは、コミュニティー・コンソールで設定した関連する属性よりも優先されます。
2. 接続レベルで設定した属性は、B2B 機能レベルで設定した属性よりも優先されます。
3. B2B 機能レベルで設定した属性は、文書定義レベルで設定した属性よりも優先されます。
4. どこで設定した属性も (変換マップ、文書定義レベル、B2B 機能レベル、または接続レベル)、エンベロープ・プロファイルで設定した値よりも優先されます。

変換マップのプロパティーおよび関連するコミュニティー・コンソール属性のリストについては、461 ページの『Data Interchange Services クライアント・プロパティー』を参照してください。

## デフォルト値の変更

### このタスクについて

449 ページの『 エンベロープ・プロファイル属性』では、プロファイルに値を入力しない場合やプロファイルを作成しない場合に、EDI 標準の各エンベロープ属性で使用されるデフォルト値を表にまとめています。使用するエンベロープ・プロファイルに、実行時にシステムによって提供されない必須エレメントを必ず指定してください。

エンベロープ・プロファイルを設定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**EDI**」>「**エンベロープ・プロファイル**」の順にクリックします。
2. 以下のステップのいずれかを実行します。
   - エンベロープの作成
     a. 「**作成**」をクリックします。
     b. エンベロープ・プロファイルの名前を入力します。この名前が、「エンベロープ・プロファイル」リストに表示されることになります。
     c. (オプション) プロファイルの**説明**を入力します。

d. エンベロープが準拠する「**EDI 標準**」をクリックします。例えば、EDI-X12 標準に準拠した文書を交換する場合は、「**X12**」をクリックします。

- エンベロープを変更します。
  a. プロファイルの名前の横にある「**詳細の表示**」アイコンをクリックして、既存のエンベロープ・プロファイルのいずれかを選択します。
  b. 「**編集**」アイコンをクリックします。

3. デフォルトでは、「**一般**」ボタンが選択されています。ENVTYPE を除くどのフィールドにも値を入力できます。ENVTYPE には、ステップ 2d で選択した標準が事前に入力されています。

   値を追加できるフィールドは、次のとおりです。
   - 「**交換制御番号の長さ**」。エンベロープ内の交換に制御番号を割り当てるときに使用する文字数です。
   - 「**グループ制御番号の長さ**」。エンベロープ内のグループに制御番号を割り当てるときに使用する文字数です。
   - 「**トランザクション制御番号の長さ**」。エンベロープ内のトランザクションに制御番号を割り当てるときに使用する文字数です。
   - 「**最大トランザクション番号**」。このエンベロープで許可されている最大トランザクション数です。
   - 「**トランザクション ID 別制御番号**」。設定された番号をデータベース内で検索するときにトランザクション ID を (キーの一部として) 使用するかどうかを示します。使用する場合は、トランザクション ID ごとに別個の制御番号セットが使用されます。

   一般エンベロープ・プロファイルの上記の各フィールドは、3 つのどの標準でも同じです。ただし、EDIFACT にはもう 1 つ別のフィールドがあります。「**EDI 用のグループの作成**」です。

   「一般」ページで何らかの変更を加えた場合は、「**保存**」をクリックします。

4. 交換の値を指定するには、「**交換**」をクリックします。新たに一連のフィールドがページに表示されます。表示されるフィールドは、EDI 標準によって異なります。一部のフィールドには既に値が入っており、また実行時に値が設定されるフィールドもあります。
   - EDI-X12 標準の場合は、以下のフィールドを変更できます。
     - **ISA01: 許可情報修飾子**。ISA02 内の情報のタイプを表すコードです。
     - **ISA02: 許可情報**。交換データの送信側をさらに識別または許可するための情報です。
     - **ISA03: セキュリティー情報修飾子**。ISA04 内の情報のタイプを表すコードです。有効な値は、以下のとおりです。

       **00** ISA04 は意味のある情報ではありません

       **01** ISA04 にはパスワードが含まれています
     - **ISA04: セキュリティー情報**。送信側または交換データに関するセキュリティー情報です。ISA03 内のコードは、情報のタイプを定義します。

– **ISA11: 交換標準 ID**。交換を管理する機関を表すコードです。有効な値: **U** (米国の EDI コミュニティー ASC X12)、**TDCC**、および **UCS**。

**注:** この属性は、X12 の 4010 までのバージョンで使用されます。X12 4020 では、ISA11 エレメントが反復分離記号として使用されます。

– **ISA12: 交換バージョン ID**。交換と機能グループ制御セグメントで使用される構文のバージョン番号です。

– **ISA14: 応答要求済み**。確認通知を要求するための送信側のコードです。有効な値は、以下のとおりです。

**0** 確認通知を要求しません

**1** ISA および IEA セグメントが受信され、認識されたという確認通知を要求します

– **ISA15: テスト標識**。交換がテスト用であるか、実動用であるかを示す標識です。有効な値は、以下のとおりです。

**T** テスト・データの場合

**P** 実動データの場合

- UCS 標準の場合は、以下のフィールドを変更できます。
  – **BG01: 通信 ID**。送信する側の会社の ID です。
  – **BG02: 通信パスワード**。受信側が割り当てたパスワードで、パートナーとの合意に従って使用されます。
- EDIFACT 標準の場合は、以下のフィールドを変更できます。
  – **UNB0101: 構文 ID**。使用される構文を管理する機関の ID です。制御機関は UNO です。レベルは A または B です。
  – **UNB0102: 構文バージョン**。構文 ID によって識別される構文のバージョン番号です。
  – **UNB0601: 受信側参照/パスワード**。受信側が割り当てたパスワードで、パートナーとの合意に従って使用されます。
  – **UNB0602: 受信側参照/パスワード修飾子**。受信側のパスワードに対する修飾子で、パートナーとの合意に従って使用されます。
  – **UNB07: アプリケーション参照**。交換メッセージが関係する機能領域の送信側の ID です。
  – **UNB08: 優先順位**。処理の優先順位を決めるための送信側のコードで、パートナーとの合意に従って使用されます。コード A が最も高い優先順位です。
  – **UNB09: 確認通知要求**。確認通知を要求するための送信側のコードです。
  – **UNB10: 通信契約 ID**。この交換で使用される契約のタイプを表す名前またはコードで、パートナーとの合意に従って使用されます。
  – **UNB11: テスト標識 (使用標識)**。交換がテスト目的であることを示す標識です。「1」はテスト交換を示します。

「交換」ページで何らかの変更を加えた場合は、「**保存**」をクリックします。

5. 交換内のグループの値を指定するには、「**グループ**」をクリックします。新たに一連のフィールドが表示されます。表示されるフィールドは、EDI 標準によって異なります。

このページの各フィールドでは、グループの送信側と受信側を定義するのが一般的です。

- EDI-X12 標準および UCS 標準の場合は、以下のフィールドに値を入力できます。
  - **GS01: 機能グループ ID**。グループ内のトランザクション集合のタイプの ID です。
  - **GS02: アプリケーション送信側**。送信側の会社の特定の部門を表す名前またはコードです。
  - **GS03: アプリケーション受信側**。グループを受信する受信側の会社の特定の部門を表す名前またはコードです。
  - **GS07: グループ機関**。標準を管理する機関を示すために GS08 と共に使用されるコードです。
  - **GS08: グループ・バージョン**。標準のバージョン、リリース、および業界を表すコードです。
- EDIFACT 標準の場合は、以下のフィールドに値を入力できます。
  - **UNG01: 機能グループ ID**。グループ内のメッセージのタイプの ID です。
  - **UNG0201: アプリケーション送信側 ID**。送信側の会社の特定の部門を表す名前またはコードです。
  - **UNG0202: アプリケーション送信側 ID 修飾子**。送信側 ID コードの修飾子です。このコードの修飾子については、データ・エレメント・ディレクトリーを参照してください。
  - **UNG0301: アプリケーション受信側 ID**。グループを受信する受信側の会社の特定の部門を表す名前またはコードです。
  - **UNG0302: アプリケーション受信側 ID 修飾子**。受信側 ID コードの修飾子です。このコードの修飾子については、データ・エレメント・ディレクトリーを参照してください。
  - **UNG06: 制御機関**。機能グループ内のメッセージ・タイプを管理している機関を示すコードです。
  - **UNG0701: メッセージ・バージョン**。メッセージ・タイプのバージョン番号です。
  - **UNG0702: メッセージ・リリース**。メッセージ・タイプのバージョン番号の中のリリース番号です。
  - **UNG0703: 関連割り当て済み**。メッセージ・タイプをさらに識別するために担当関連によって割り当てられたコードです。
  - **UNG08: アプリケーション・パスワード**。受信側の会社の特定の部門が割り当てたパスワードです。

「グループ」ページで何らかの変更を加えた場合は、「**保存**」をクリックします。

6. グループ内のトランザクションの値を指定するには、「**トランザクション**」をクリックします。ただし、EDIFACT の場合は「**メッセージ**」をクリックします。新たに一連のフィールドが表示されます。表示されるフィールドは、EDI 標準によって異なります。

- EDI-X12 または USC 標準の場合は、「**ST03: インプリメンテーション規則 ID ストリング**」の値を入力できます。
- EDIFACT 標準の場合は、以下のフィールドに値を入力できます。
  - **UNH0201: メッセージ・タイプ**。メッセージ・タイプを識別するために制御機関が割り当てたコードです。
  - **UNH0202: メッセージ・バージョン**。メッセージ・タイプのバージョン番号です。
  - **UNH0203: メッセージ・リリース**。メッセージ・タイプのバージョン番号の中のリリース番号です。
  - **UNH0204: 制御機関**。メッセージ・タイプを管理している機関を表すコードです。
  - **UNH0205: 関連割り当て済みコード**。メッセージ・タイプをさらに識別するために担当関連によって割り当てられたコードです。
  - **UNH03: 共通アクセス参照**。後続のすべてのデータ転送を共通のファイルに関連付けるキーです。パートナーは、複数の要素からなるキーの使用に同意できますが、サブエレメント区切り記号を使用することはできません。

「トランザクション」ページで何らかの変更を加えた場合は、「**保存**」をクリックします。

7. 「**保存**」をクリックします。
8. ほかに定義または変更するエンベロープ・プロファイルがある場合は、そのプロファイルごとに、ステップ 2 (197 ページ) から 7 を繰り返します。

定義したエンベロープ・プロファイルは、「エンベロープ・プロファイル」リストに表示されます。このリストから、目的のプロファイルを選択し、「**使用箇所**」アイコンをクリックして、そのプロファイルを使用する接続を決定できます。

## 接続プロファイル

接続プロファイルは、エンベロープ解除されたトランザクションと併用する場合と、エンベローパー作成の EDI 交換と併用する場合があります。トランザクションの場合、接続プロファイルで、エンベロープ解除後にトランザクションをどのように処理するかを決定します。交換の場合、接続プロファイルでは交換をどのように配信するかを決定します。

「接続プロファイル」ウィンドウを使用して、新規プロファイルを作成したり、既存のプロファイル情報を編集したりします。現在定義されている各プロファイルの名前およびその説明がある場合には、それらが「接続プロファイル・リスト」に表示されます。接続プロファイルの詳細については、「*WebSphere Partner Gateway E/A ハブ構成ガイド*」を参照してください。

### トランザクション

WebSphere Partner Gateway に EDI 交換が届いた場合、通常、その交換のエンベロープを解除して個々のトランザクションにするというのが最初のアクションです。トランザクションが作成されると、エンベロープ解除アクションによって「**交換の使用標識**」とグループ情報 (**グループ・アプリケーション送信側 ID**、**グループ・アプリケーション受信側 ID**、および**グループ・アプリケーション・パスワード**) がト

ランザクション・メタデータに設定されます。次に、WebSphere Partner Gateway が独自のワークフローで各トランザクションを再処理します。

例えば、同じタイプのトランザクション (850 など) が 2 つあり、それぞれを所属グループまたは交換の使用標識の値に応じて別々に処理する必要があるとします。「**使用標識**」が実動 (**P**) の場合は、1 つ目のマップ (A) を使用し、「**使用指標**」がテスト (**T**) の場合は、2 つ目のマップ (B) を使用するものとします。この 850 トランザクションを処理するには、同種の接続が 2 つ必要になります。1 つはマップ A を使用し、もう 1 つはマップ B を使用するという点のみが異なります。

この点を除けば 2 つのトランザクションはまったく同じなので (ソース・パートナー、ターゲット・パートナー、パッケージ、プロトコル、および文書タイプは同じです)、文書マネージャーではどの接続を使用するのかを判断する手段が必要になります。これは、既に設定した接続プロファイル属性をトランザクション・メタデータとマッチングすることによって行います。この例で言うと、接続プロファイルを 2 つ作成し、その 1 つ (CPProduction) では「**EDI 使用タイプ**」を **P** に設定し、もう 1 つ (CPTest) では「**EDI 使用タイプ**」を **T** に設定した場合、文書マネージャーでは使用標識が P のトランザクションが CPProduction プロファイルと一致します。したがって、文書マネージャーはマップ A を使用してトランザクションを変換すればよいと認識します。

このセクションで挙げた例では「**交換の使用標識**」属性を使用しましたが、トランザクションの識別要因としてはこのほかにも「**グループ・アプリケーション送信側 ID**」、「**グループ・アプリケーション受信側 ID**」、「**グループ・アプリケーション・パスワード**」の各属性を使用することができます。

## 交換

交換の場合は、「**接続プロファイル修飾子 1**」属性を使用します。

例えば、現在、社内で VAN (「なし」パッケージ化) またはインターネット (「AS2」パッケージ化) からのマイグレーションを進めているとします。840 (見積依頼) トランザクションでは VAN を使用し、850 (購入注文) トランザクションではインターネットを使用したいと考えています。パートナー接続を 2 つ設定します。どちらでも、ソース交換は同じですが、ターゲットは異なります (1 つは「なし」パッケージ化で、もう 1 つは「AS2」パッケージ化です)。接続プロファイルが、この 2 つの接続を区別するのに役立ちます。

交換用の接続プロファイルを設定するには、いくつかのステップを踏む必要があります。この例の 2 つの接続プロファイルを作成するには、以下のステップを実行します。

1. トランザクションに必要な 2 つの接続を確立します。どちらの接続でも、「受信」側で「**接続プロファイル修飾子 1**」属性を設定します。この値は、分かりやすいものにしてください (例えば、ConNone や ConAS2 など)。
2. 接続プロファイルを 2 つ定義します (例えば、CPNone および CPAS2)。各プロファイルでは、「**修飾子 1**」 の値を、ステップ 1 で設定した「**接続プロファイル修飾子 1**」属性と一致する値 (ConNone および ConAS2) に設定します。
3. 交換に必要な 2 つの接続を確立します。各接続では、ソース・パッケージ化は同じです (「N/A」) が、ターゲット・パッケージ化は異なります (「なし」および「AS2」)。接続プロファイル CPNone を持つパートナー接続では、ターゲッ

ト宛先は、VAN に接続可能な FTP スクリプト記述宛先に設定されます。接続プロファイル CPAS2 を持つパートナー接続では、ターゲット・パッケージ化は AS に設定されます。

4. 適切な接続プロファイルを各接続に関連付けます。

エンベローパーでは、パートナー接続の「受信」側の「**接続プロファイル修飾子 1**」属性がエンベロープのブレークポイントとして使用されます。したがって、「**接続プロファイル修飾子 1**」属性の値が異なるトランザクションは、別々のエンベロープに入れられます。トランザクションに異なる値を設定した場合、エンベローパーは 840 トランザクションと 850 トランザクションを同じ交換にエンベロープすることはありません。

文書マネージャーが接続を検索すると、接続が 2 つ見つかりますが、接続プロファイルの一致する 1 つのみが使用されます。

## 接続プロファイルの設定

### このタスクについて

接続プロファイルの設定はオプションです。パートナーで交換する文書のタイプに合わせて接続を複数確立する必要がない場合には、このセクションを省略してください。

接続プロファイルを設定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**EDI**」>「**接続プロファイル**」をクリックします。
2. 「**接続プロファイルの作成**」をクリックします。
3. 「接続プロファイルの詳細」ページで、この接続プロファイルの名前を入力します (必須)。
4. (オプション) 接続プロファイルの説明を入力します。

   名前と説明 (説明を入力した場合) が「接続プロファイル・リスト (Connection Profile List)」ページに表示されます。
5. (オプション) 「**修飾子 1**」の値を入力します。この値によって、EDI 交換で使用する接続が決まります。「**修飾子 1**」の使用例については、 202 ページの『交換』を参照してください。
6. (オプション) これがテスト、実動、または情報交換なのかを示す値を「**EDI 使用タイプ**」に入力します。「**EDI 使用タイプ**」の使用例については、 201 ページの『 トランザクション』を参照してください。
7. (オプション) グループの送信側に関連付けられたアプリケーションまたは会社部門を示す値を「**アプリケーション送信側 ID**」に入力します。
8. (オプション) グループの受信側に関連付けられたアプリケーションまたは会社部門を示す値を「**アプリケーション受信側 ID**」に入力します。
9. (オプション) アプリケーション送信側とアプリケーション受信側間でパスワードが必要な場合には、「**パスワード**」に値を入力します。
10. 「**保存**」をクリックします。

特定の交換のエンベロープに入れるトランザクションでは、「**接続プロファイル修飾子 1**」属性値を、同じ「**修飾子 1**」属性値を持つ接続プロファイルに対応するように指定することができます。「**接続プロファイル修飾子 1**」属性は、文書定義のプロトコル・レベルで設定できます (例えば、「文書定義の管理」ページで X12V5R1 プロトコルの属性を編集して、対応する「**接続プロファイル修飾子 1**」属性値をクリックすることによって、使用する接続プロファイルを示すように設定することができます)。この後、交換接続をアクティブ化したときに、「**接続プロファイル**」ボタンをクリックしてリストからプロファイルを選択することによって、接続プロファイルを関連付けます。

## 制御番号

エンベローパーでは、エンベロープ内の交換、グループ、およびトランザクションに固有の番号付けを行うために、制御番号を使用しています。制御番号は、内部パートナーと外部パートナーに対して設定されます。文書の交換が行われるときにも、パートナーのペアに対して制御番号が生成されます。

EDI B2B 機能を備えるパートナーごとに、制御番号用の一連の初期シード値があります。各値は、はじめて EDI 交換が作成されてパートナー・ペア間で送信されるときに使用されます。交換の送信先となるパートナーに、この初期シード値が適用されます。パートナー間で文書の送信が完了したら、最後に使用された番号を「現行制御番号」ページで参照できます。「**トランザクション ID 別制御番号**」を **Y** に設定している場合は、特定のパートナーのペアに対していくつかの項目を作成してもかまいません。作成された項目は、新しい制御番号の生成に使用されます。

制御番号を初期化するときに、マスクを使用して、エンベローパーによる通常の制御番号生成を変更できます。マスクは、交換またはグループの制御番号に基づいた制御番号を生成するために使用します。マスクとは、以下のようなものです。編集マスク内の「*n*」は、制御番号値の生成に使用するバイト数に置き換えてください。使用可能なコードの説明については、表 26 を参照してください。

*表 26. 制御番号マスク*

| コード | 制御番号 | 説明 |
|---|---|---|
| G | トランザクション | トランザクション制御番号は、グループ制御番号と同じです。グループごとに 1 つのトランザクションのみが許可されます。 |
| G*n* | トランザクション | グループ制御番号から *n* バイトが取得されます。残りのトランザクション制御番号には、その最大サイズまでゼロが埋め込まれます。グループごとに 1 つのトランザクションのみが許可されます。 |
| C | グループ、トランザクション | グループまたはトランザクションの制御番号フィールドの残りのバイトが、このパートナーの制御番号の保守に使用されます。 |
| V | グループ、トランザクション | 先頭のグループまたはトランザクションの値が 1、2 番目の値が 2 という具合になるように、増分値が使用されます。 |
| V*n* | トランザクション | 先頭のトランザクションの値が 1、2 番目の値が 2 という具合になるように、*n* バイトの長さの増分値が使用されます。 |

*表 26. 制御番号マスク (続き)*

| コード | 制御番号 | 説明 |
|---|---|---|
| G*n*C | トランザクション | グループ制御番号から *n* バイトが取得され、トランザクション制御番号フィールドの残りのバイトが制御番号の保守に使用されます。残りの位置の数によって、制御番号の最大値が決まります。例えば、G5C の場合は 4 つの位置が残るので、最大値は 9999 になります。最大値に達すると、制御番号は 1 へと循環します。 |
| G*n*V | トランザクション | グループ制御番号から *n* バイトが取得されます。トランザクション制御番号フィールドの残りのバイトでは、先頭のトランザクションの値が 1、2 番目の値が 2 という具合になるように、増分値が使用されます。 |
| G*n*V*m* | トランザクション | グループ制御番号から *n* バイトが取得されます。トランザクション制御番号フィールドの残りのバイトでは、最大 *m* バイトまで、先頭のトランザクションの値が 1、2 番目の値が 2 という具合になるように、増分値が使用されます。 |
| I | グループ、トランザクション | グループまたはトランザクションの制御番号が、交換制御番号と同じである必要があります。交換では 1 つのグループのみが許可され、グループまたは交換では 1 つのトランザクションのみが許可されます。 |
| I*n* | グループ、トランザクション | 交換制御番号から *n* バイトが取得されます。残りのグループ制御番号またはトランザクション制御番号フィールドには、その最大サイズまでゼロが埋め込まれます。交換ごとに 1 つのグループのみが許可され、グループごとに 1 つのトランザクションのみが許可されます。 |
| I*n*C | グループ、トランザクション | 交換制御番号から *n* バイトが取得されます。グループまたはトランザクション制御番号フィールドの残りのバイトが、制御番号の保守に使用されます。残りの位置の数によって、制御番号の最大値が決まります。例えば、I5C の場合は 4 つの位置が残るので、最大値は 9999 になります。最大値に達すると、制御番号は 1 へと循環します。 |
| I*n*V | グループ、トランザクション | 交換制御番号から *n* バイトが取得されます。グループ制御番号またはトランザクション制御番号フィールドの残りのバイトでは、先頭のグループまたはトランザクションの値が 1、2 番目の値が 2 という具合になるように、増分値が使用されます。 |
| I*n*V*m* | トランザクション | 交換制御番号から *n* バイトが取得されます。トランザクション制御番号フィールドの残りのバイトでは、最大 *m* バイトまで、先頭のトランザクションの値が 1、2 番目の値が 2 という具合になるように、増分値が使用されます。 |

*表 26. 制御番号マスク (続き)*

| コード | 制御番号 | 説明 |
|---|---|---|
| I*n*G*m* | トランザクション | 交換制御番号から *n* バイトが取得され、グループ制御番号から最大で *m* バイトが取得されます。*n* と *m* の合計が 9 を超える場合は、グループ制御番号から 9 - *n* バイトのみが取得されます。例えば、I4G6 の場合は、交換から 4 バイトが取得されます。 |
| I*n*G*m*C | トランザクション | 交換制御番号から *n* バイトが取得され、グループ制御番号から *m* バイトが取得されます。トランザクション制御番号フィールドの残りのバイトが、制御番号の保守に使用されます。残りの位置の数によって、制御番号の最大値が決まります。例えば、I2G4C の場合は 3 つの位置が残るので、最大値は 999 になります。最大値に達すると、制御番号は 1 へと循環します。 |
| I*n*G*m*V | トランザクション | 交換制御番号から *n* バイトが取得され、グループ制御番号から *m* バイトが取得されます。トランザクション制御番号フィールドの残りのバイトでは、先頭のトランザクションの値が 1、2 番目の値が 2 という具合になるように、増分値が使用されます。 |
| I*n*G*m*V*o* | トランザクション | 交換制御番号から *n* バイトが取得され、グループ制御番号から *m* バイトが取得されます。トランザクション制御番号フィールドの残りのバイトでは、最大 *0* バイトまで、先頭のトランザクションの値が 1、2 番目の値が 2 という具合になるように、増分値が使用されます。 |

# 制御番号初期化

## このタスクについて

エンベローパーが使用する制御番号を構成するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**EDI**」>「**制御番号の初期化**」をクリックします。
2. パートナーの名前を入力して「**検索**」をクリックするか、または名前を入力しないで「**検索**」をクリックしてすべてのパートナーを表示します。「**EDI 対応 (EDI-capable)**」にチェック・マークを付けておくと、検索対象が EDI 文書 B2B 機能を備えたパートナーに限定されます。このチェック・マークを外すと、すべてのパートナーが検索されます。
3. パートナーの横にある「**詳細の表示**」アイコンをクリックします。
4. パートナーの現行の制御番号割り当てが「制御番号構成の詳細」ページにリストされます (割り当てがある場合)。「**編集**」アイコンをクリックして、値を追加または変更します。
5. 交換用の制御番号生成の初期化に使用する番号を「**交換**」の横に入力 (または変更) します。

6. グループ用の制御番号生成の初期化に使用する番号を「**グループ**」の横に入力 (または変更) します。この方法以外に、「**マスク**」をクリックし、固定値ではなく、使用するマスクを入力することもできます。
7. トランザクション用の制御番号生成の初期化に使用する番号を「**トランザクション**」の横に入力 (または変更) します。この方法以外に、「**マスク**」をクリックし、固定値ではなく、使用するマスクを入力することもできます。
8. 「**保存**」をクリックします。

### 現行の制御番号

パートナー・ペアのデータが既に制御テーブルに存在する場合は、制御番号生成を変更できます。以下の処理を実行できます。

- パートナー・ペアの制御番号生成を初期状態にリセットします。
- 交換、グループ、またはトランザクションの番号 (あるいは、これらの番号の組み合わせ) を編集し、新しい値で保管します。

**注:** 制御番号生成をリセットしたり、グループまたはマスクを編集したりするときには、番号の順序が崩れたり、制御番号の重複問題が発生したりしないように十分に注意してください。こうしたアクションを実行するのは、テスト段階のときか、パートナーから特に別の制御番号が要求された場合のみにすることをお勧めします。

どのパートナーにどんな制御番号が割り当てられているのかを判断するには、現行制御番号という機能を使用します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**EDI**」>「**現行制御番号**」をクリックします。
2. 以下のステップのいずれかを実行します。
   - すべてのパートナーの現状を参照する場合は、パートナー・リストの「**任意のパートナー**」を選択状態のままにしておき、「**現在の状況の表示**」をクリックします。
   - 選択したパートナーの状態を表示する場合は、以下のステップを実行します。
     a. ソース・パートナーおよびターゲット・パートナーの名前を入力し、「**検索**」をクリックします。EDI 文書を交換しているパートナーのみに検索結果を限定する場合は、「**EDI 対応の検索**」にチェック・マークを付けたままにしておきます。
     b. 検索結果のリストから、1 つ以上のパートナーを選択し、「**現在の状況の表示**」をクリックします。

## 文書交換の定義

文書交換の定義は、手動でまたはウィザードを使用して行えます。ウィザードを使用して接続を定義する場合は、『ウィザードを使用した文書交換の定義』を参照してください。接続の定義を手動で行うか、または接続を手動で変更する場合は、210 ページの『手動による文書交換の定義』を参照してください。

### ウィザードを使用した文書交換の定義

WebSphere Partner Gateway には、文書交換を定義するのに役立つ 2 つのウィザードがあります。それは、EIF インポート・ウィザードと EDI 接続ウィザードです。

EIF インポート・ウィザードは、EIF ファイルに入っているマップをインポートするのに必要なステップをガイドし、アップロードされたマップの詳細を表示します。さらに、それらのマップを正しいルーティング・オブジェクトに関連付けて、論理インタラクションを作成します。ウィザードが完了すると、新規のマップがアップロードされ、必要なインタラクションがシステムに作成されます。その後、EDI 接続ウィザードを使用して、新規にアップロードされたマップによる接続を作成します。

**注:** 混乱を避けるために、一度に 1 人のユーザーだけが EIF インポート・ウィザードを使用できます。

EDI 接続ウィザードは EIF ウィザードの後に使用され、EDI インタラクション (EDI 文書の送信または受信) を構成するのに必要なステップをガイドします。ウィザードが完了すると、選択されたパートナーについて、EDI インタラクションのための構成が完成します。これには、B2B 機能の有効化、有効なインタラクションの作成、パートナー接続の作成、および必要な EDI 属性の割り当てが含まれます。接続ウィザードにより、入力に基づいて提案されたパートナー接続が生成されます。生成される可能性のある接続の全リストが以下に示されます。

- 基本メッセージ用のデエンベローパー
- 変換
- 基本メッセージ用のエンベローパー
- TA1 生成
- FA 生成
- TA1 または FA (あるいはその両方) 用のエンベローパー
- TA1 または FA (あるいはその両方) 用のデエンベローパー

これらのウィザードはどちらも、コンソールの「ウィザード」タブの下にあります。

## EIF インポート・ウィザードを使用したマップのインポート

### このタスクについて

EIF インポート・ウィザードを使用してマップをインポートするには、以下のステップを実行します。

1. WebSphere Partner Gateway コンソールを始動します。
2. 「**ウィザード**」をクリックします。
3. 「**EIF インポート・ウィザード**」をクリックします。
4. インポートするファイルの名前を入力するか、「**参照**」をクリックしてファイルを見つけます。

   **注:** 複数のマップを含む EIF ファイルをインポートする場合、ファイルに含まれるマップ名が固有であることを確かめてください。複数のマップを同じマップ名で同じ EIF ファイルにアップロードすると、データベース内のマップは、後から一致するマップによって上書きされてしまいます。
5. 「**インポート**」をクリックします。

6. 正常にインポートされたマップのリストが表示されます。「**終了**」をクリックしてデフォルト値を受け入れるか、「**次へ**」をクリックしてそれを表示または変更します。
7. 「**次へ**」をクリックした場合、変換マップを確認し、インタラクションを変更するかどうか尋ねられます。変換マップを選択します。インタラクションがある場合、読み取り専用として表示されます。インタラクションを追加するには、「**インタラクションの追加**」をクリックします。
8. 「インタラクションの追加」ウィンドウで、インタラクションを選択し、「**このインタラクションの追加**」をクリックして、インタラクションをリストに追加します。
9. 変換マップの確認が終わったら、「**次へ**」をクリックして検証マップを確認します。
10. インポートされた検証マップを確認します。問題がない場合、「**終了**」をクリックします。FA マップを表示する場合は、「**次へ**」をクリックします。
11. インポートされた FA マップを確認し、「**終了**」をクリックします。正常にインポートされたマップおよび作成されたインタラクションを示す最後のウィンドウが表示されます。

## EDI 接続ウィザードを使用した接続の設定

### このタスクについて

EDI 接続ウィザードを使用して接続を設定する前に、以下を作成しておく必要があります。

- 内部パートナー
- 少なくとも 1 つの外部パートナー
- パートナーごとの EDI ビジネス ID。このウィザードで、EDI ビジネス ID は *qq-xxxxxxxxx* というフォームのフリー・フォーム・ビジネス ID として定義されます。ここで、*qq* は 2 桁の EDI 交換修飾子で、*xxxxxxxxx* は 9 桁の EDI 交換 ID です。
- 宛先およびデフォルト宛先
- エンベロープ・プロファイル

EDI フローが正常に実行できるようになる前に、いくつかの追加の構成ステップが必要です。以下に例を示します。

- XML 形式の構成 (XML を送信または受信している場合)
- ROD スプリッターを持つ受信側の構成 (ROD を受信している場合)
- AS または AS2 用の追加の接続属性の構成 (AS パッケージ化を使用している場合)

EDI 接続ウィザードを使用して接続を作成するには、以下のステップを実行します。

1. WebSphere Partner Gateway コンソールを始動します。
2. 「**ウィザード**」をクリックします。
3. 「**EDI 接続ウィザード**」をクリックします。

4. 構成するタスクのタイプ (「**EDI 文書を EDI パートナーに送信します**」または「**EDI 文書を EDI パートナーから受信します**」) をクリックして、「**次へ**」をクリックします。
5. 「**EDI 文書を EDI パートナーに送信します**」または「**EDI 文書を EDI パートナーから受信します**」のどちらを選択したかに応じて、ソースまたはターゲットのパートナーを入力し、「**検索**」をクリックします。
6. ドロップダウン・リストからソースまたはターゲットのパートナーを選択し、「**次へ**」をクリックします。
7. ソースまたはターゲットのパートナーの一般プロパティーを選択します。構文が EDI の場合は、EDI プロパティーも指定する必要があります。必要なすべてのプロパティーを選択したら、「**次へ**」を選択します。

   **注:**

   a. TA1 および FA プロパティーは、ソースが外部パートナーの場合にのみ表示されます。 FA 必要時間は、ターゲットが外部パートナーの場合にのみ表示されます。

   b. EDI 接続ウィザードには、EDI 区切り文字値として使用される共通値のリストが含まれます。提供されたリストにない値を使用する場合、ウィザードを終了してから接続属性を手動で編集する必要があります。接続属性は、「**アカウント管理**」>「**接続**」をクリックして変更することができます。

   c. 動作モードごとに宛先を指定するように強制されます。これは、ブランク (「宛先は選択されていません」) オプションを選択できないことを意味します。この追加の接続構成を強制しても、文書の送受信の大抵の状況には悪影響を与えません。接続から宛先の指定を除去する必要がある場合は、ウィザードを終了した後に、「**アカウント管理**」>「**接続**」をクリックして行うことができます。
8. ソースまたはターゲットの「**検証マップ**」、「**アクション**」、およびソースまたはターゲットのパートナーの「**変換マップ**」を選択します。マップを選択した後で、マップ記述が表示されます。AS パッケージを使用する EDI のような場合の混乱を避けるため、パッケージはブランクにします。これらを選択したら、「**次へ**」をクリックします。
9. 提案された接続を確認し、「**属性**」、「**アクション**」、または「**宛先**」をクリックして、これらの設定を確認します。

   **注:** 既に存在しており、作成されていない接続はぼかし表示されます。これらの接続にもその隣に「存在」アイコンがあり、「作成」チェック・ボックスはありません。接続が既に存在する場合、このウィザードでは上書きされません。この場合、この状態を説明する警告が表示されます。
   接続を変更する必要がある場合、「**戻る**」をクリックします。リストされている接続で間に合う場合、「**終了**」をクリックします。変更する必要がある場合、「**戻る**」をクリックします。正常に作成された接続を示す最後のウィンドウが表示されます。

## 手動による文書交換の定義

EIF インポート・ウィザードおよび EDI 接続ウィザードは、文書交換を定義するのに役立ちます (これらのウィザードの詳細については、207 ページの『ウィザードを使用した文書交換の定義』を参照してください)。ただし、文書は手動で定義する

こともできます。ここでは、ハブを EDI 交換に参加させ、ハブで文書またはトランザクションを変換し、ハブから EDI 交換を送信できるように文書交換を設定するために必要な作業についてに概説します。以下のセクションで示すステップは、一般的なものであり、マップのインポートと対話の設定にのみ適用されるものです。パートナーの B2B 機能を使用可能にする一般的なステップ (あらゆるタイプの文書交換に適用されます) については、28 ページの『B2B 機能の設定』を参照してください。接続の管理に関する一般的なステップ (あらゆるタイプの文書交換に適用されます) については、253 ページの『第 12 章 接続の管理』を参照してください。マップのインポートから接続の管理まで EDI 文書交換の包括的な例を参照する場合は、347 ページの『第 19 章 EDI の例』を参照してください。付録には、以下の例が掲載されています。

- 347 ページの『 EDI から ROD への例』
- 363 ページの『 EDI から XML への例』
- 377 ページの『 ROD から EDI への例』
- 369 ページの『 XML から EDI への例』

## 手動によるマップのインポート

### このタスクについて

EDI 文書、XML 文書、またはレコード指向データ (ROD) 文書用の変換マップは、Data Interchange Services クライアント・プログラムで作成できます。Data Interchange Services クライアントは、XML スキーマ文書定義、XML DTD 文書定義、EDI 標準、ROD 文書定義、およびマップを作成および保守するために使用するプログラムです。

WTX マップは、WTX Design studio を使用して作成し、WebSphere Partner Gateway にインポートします。

Data Interchange Services クライアントは、単独でインストールされるプログラムとして WebSphere Partner Gateway のメディアに収録されていますが、別のコンピューターに常駐するのが一般的です。Data Interchange Services クライアントのマッピング担当者が、ある文書のエレメントを形式の異なる別の文書のエレメントにどのように移動するかということを指示するマップを作成します。Data Interchange Services は、文書の形式を文書を一つの形式から別の形式にどのように変換するかという指示を保持するほか、ソース文書とターゲット文書のレイアウト (形式) を認識している必要があります。Data Interchange Services では、文書のレイアウトが文書定義になります。

変換マップを WebSphere Partner Gateway にインポートすると、Data Interchange Services で作成した文書定義が「変換マップ」ページと「文書定義の管理」ページに文書定義 (パッケージ、プロトコル、および文書タイプ) として表示されます。

例えば、XML 文書を X12 トランザクションに変換する場合は、XML と X12 のトランザクション文書定義、および変換の内容が定義されているマップをインポートします。

Data Interchange Services からマップ・ファイルを受け取る方法は 2 つあります。Data Interchange Services クライアントから WebSphere Partner Gateway データベースに直接接続できる場合は、Data Interchange Services クライアントのマッピング担

当者がマップ・ファイルをデータベースに直接エクスポートできます。一般には、マップ・ファイルを E メールまたは FTP 転送で受け取るという方法が取られます。マップ・ファイルを FTP 経由で受け取る場合は、ファイル形式がバイナリーである必要があります。

Data Interchange Services クライアントからのマップのエクスポート時にエラーが発生した場合でも、コミュニティー・コンソールにはマップ名が表示されている場合があります。このマップを使用して、文書を変換することはできません。このマップを使用して文書を変換するためには、Data Interchange Services クライアントのマッピング担当者に、エクスポートの問題を知らせて、マッピング担当者にマップの再エクスポートを依頼することが必要になります。

マップをインポートするには、以下のステップを実行します。

1. コマンド・ウィンドウを開きます。
2. 以下のコマンドまたはスクリプトを入力します。
   - UNIX システムの場合:

     `<ProductDir>/bin/bcgDISImport.sh <control_string_map>`
   - Windows システムの場合:

     `<ProductDir>¥bin¥bcgDISImport.bat <control_string_map>`

     ここで、*<database_user_ID>* と *<password>* は、WebSphere Partner Gateway のインストール作業の一部としてデータベースをインストールしたときに使用した値です。*<control_string_map>* は、Data Interchange Services クライアントからエクスポートしたマップ制御ストリング・ファイルの完全パスです。
3. 変換マップの場合は、文書定義がインポートされたことを確認します。
   a. **「ハブ管理」>「ハブ構成」>「マップ」>「変換マップ」**の順にクリックします。
   b. 「変換マップ」ページから、Data Interchange Services のマップの横にある**「詳細の表示」**アイコンをクリックします。ソースおよびターゲットの文書定義が表示され、ハブで受信する文書の形式とハブから配信される文書の形式を知ることができます。
   c. **「ハブ管理」>「ハブ構成」>「文書定義」**をクリックします。
   d. 「変換マップ」ページに表示された文書定義に関連付けられているパッケージとプロトコルを展開して、「文書定義の管理」ページに文書タイプが表示されていることを確認します。

変換マップと共に検証マップを使用すると、EDI 標準を必要とする変換プロセスに EDI 標準の検証を追加できます。検証マップでは、EDI 文書の検証を完全に制御できます。

Data Interchange Services クライアントからエクスポートした変換マップおよび検証マップ、または bcgDISImport ユーティリティーを使用してインポートした変換マップおよび検証マップは、WebSphere Partner Gateway コミュニティー・コンソールからはダウンロードできないことに注意してください。Data Interchange Services クライアントのマッピング担当者は、Data Interchange Services クライアントを介して WebSphere Partner Gateway データベースに接続することにより、これらのマップを管理します。

## WTX マップのインポート

### このタスクについて

WTX design studio を使用して作成した WTX マップは、WebSphere Partner Gateway にインポートする必要があります。これにより、特定の参加者接続に関連付けられるようになります。DFD は手動で作成する必要があります。作成した DFD は、ネイティブ・オペレーティング・システム用にコンパイルされたマップの形式で、WTX design studio からエクスポートされます。これを WebSphere Partner Gateway にインポートするには、「**ハブ管理**」 > 「**マップ**」 > 「**変換マップ**」にナビゲートして「**作成**」をクリックします。インポートしたマップは、共通ファイル・システムの WTX マップ専用のフォルダー (common/maps) に格納されます。

## WDI 標準 EIF のインポート

### このタスクについて

WebSphere Partner Gateway で EDI トランザクションを検証するためには、コンパイル済みの EDI 標準が WebSphere Partner Gateway で使用可能でなければなりません。このコンパイル済みの標準制御ストリングを作成するには、以下を実行します。

1. WDI サポート Web サイトから EDI 標準をダウンロードします。
2. 変換用のデータ変換マップを作成し、WebSphere Partner Gateway で検証する EDI トランザクションを選択します。例えば、X12V4R1 のトランザクション 810 を検証する場合は、X12V4R1-810 から X12V4R1-810 へのデータ変換マップを作成します。
3. 必須セグメント 1 つだけをマップして変換マップをコンパイルします。
4. データ変換マップの制御ストリングを文書マネージャー・データベースにエクスポートします。これにより、コンパイル後の標準も文書マネージャー・データベースにエクスポートされ、検証に使用できるようになります。

**注:** 代わりに、コンパイル済みの標準制御ストリングのみを含むサンプル EIF もいくつか用意されています。

## EDI 間フローの設定

### このタスクについて

ここでは、EDI 交換の受信、EDI 交換のエンベロープ解除、EDI 形式間でのトランザクションの変換、トランザクションのエンベロープ、およびトランザクションの配信に必要な対話について説明します。

1. ハブで受信する EDI 交換用の文書定義が存在することを確認します。交換がエンベロープ解除された後は、元のエンベロープが処理されなくなる点に注意してください。 つまり、配信ポイントがなくなります。したがって、ターゲットの対話ではパッケージに対して「**N/A**」を使用することになります。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 既に文書定義が存在しているかどうかをチェックします。例えば、パートナーが AS パッケージ化、EDI-X12 プロトコル、および ISA 文書タイプで EDI 交換を送信しようとしている場合、その定義は既に使用可能になっています。同じく、N/A/EDI-X12/ISA 文書定義も既に存在しています。

c. プロファイルに関連付ける属性の値を入力します (あるいは、リストから値を選択します)。例えば、いずれかのトランザクションでエラーが発生したらエンベロープを廃棄するように指定する場合は、「**文書定義**」の横にある「**属性値の編集**」アイコンをクリックします。「**エラーが発生した場合はエンベロープを廃棄**」行で、リストから「**はい**」を選択します。

d. 文書定義がまだ存在していない場合は、「パッケージ」、「プロトコル」、および「文書タイプ」を選択して作成します。

**注:** 接続内のアクションが「EDI 交換の検証」の場合は、属性「エラー時にエンベロープを破棄」を使用できません。

2. 交換に必要な対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」を選択します。
   c. ソースとターゲットの文書定義を選択します。パッケージ化を除き (パッケージ化では、ターゲットが「**N/A**」になります)、文書定義は同じになります。
   d. 「アクション」リストから、「**EDI エンベロープ解除**」を選択します。
3. EDI トランザクションの文書定義と EDI 形式間でのトランザクション変換方法について記述されている変換マップをインポートします。211 ページの『 手動によるマップのインポート』を参照してください。

   交換に複数のトランザクションが含まれている場合は、トランザクションごとにこのステップを繰り返します。
4. マップに関連付けられた文書定義の属性を編集する場合は、以下のステップを実行します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. プロトコルの横にある「**属性値の編集**」アイコンをクリックします。EDI プロトコルの場合は、設定可能な属性が数多く記載されたリストが表示されます。
   c. プロトコルに関連付ける属性の値を入力します (あるいは、リストから値を選択します)。
   d. 文書定義の横にある「**属性値の編集**」アイコンをクリックします。通常は、プロトコルに関連したものよりも数が少ない属性のリストが表示されます。
   e. 文書タイプに関連付ける属性の値を入力します (あるいは、リストから値を選択します)。例えば、文書タイプに関連付けられた「**検証マップ**」を変更できます。

      トランザクションには必ずエンベロープ・プロファイルを選択してください。
5. 今インポートしたマップの対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。
   c. 「**ソース**」で、トランザクションに関連付けられた文書タイプを選択します。パッケージとプロトコルを展開し、目的の文書タイプを選択します。通常、これは「**N/A**」 (トランザクション自体はパートナーから発せられたもの

ではないため)、マップに定義されているプロトコル (例えば、**X12V4R1** など)、およびマップに定義されている実際の EDI 文書 (例えば、**850** など) になります。

d. 「**ターゲット**」の下で、変換した文書の文書定義を選択します。パッケージとプロトコルを展開し、目的の文書タイプを選択します。トランザクションがエンベロープされるため (そして直接にはパートナーに配信されないため)、パッケージ化も再び「**N/A**」になります。

e. 変換マップ・リストから、この文書の変換方法が定義されているマップを選択します。

f. ネイティブ WDI の場合は、「アクション」リストから「**EDI 検証および EDI 変換**」を選択します。WTX の場合は「**EDI 検証および WTX 変換 (EDI Validate and WTX Transformation)**」を選択します。

6. ハブから送信される EDI 交換用の文書定義が存在することを確認し、その EDI 交換に関連付ける属性を設定します。

a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。

b. 既に文書定義が存在しているかどうかをチェックします。ソース・パッケージは「N/A」になり、そのプロトコルと文書タイプは交換の配信に使用されるプロトコルと文書タイプになります。例えば、EDI 交換が AS/EDI-X12/ISA として配信される場合、ソースは N/A/EDI-X12/ISA になります。

c. 配信対象の交換に適用する属性を編集します。

d. 文書定義がまだ存在していない場合は、「パッケージ」、「プロトコル」、および「文書タイプ」を選択して作成します。

7. トランザクションの変換後にハブから送信される EDI 交換用の対話を作成します。

a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。

b. 「**インタラクションの作成**」をクリックします。

c. ソースとターゲットの文書をそれぞれ選択します。パッケージ化を除き (パッケージ化では、ソース文書が「**N/A**」になります)、文書定義は同じになります。

d. 「**アクション**」リストから「**パススルー**」を選択します。

フローに確認通知を追加するには、 222 ページの『確認通知の設定』を参照してください。

インタラクションを設定したら、パートナー用の B2B 機能を作成します。

- ソース・パートナーでは、(「**ソースの設定**」の下で) 3 つの文書定義 (ソース文書タイプ用、EDI トランザクション用、およびエンベロープ用の各文書定義) を使用可能にします。
- ターゲット・パートナーでは、(「**ターゲットの設定**」の下で) 3 つの文書定義 (エンベロープ解除された文書タイプ用、変換された EDI トランザクション用、および EDI エンベロープ用の各文書定義) を使用可能にします。

B2B 機能を作成するための詳細な手順については、 28 ページの『B2B 機能の設定』で説明します。

パートナー用の B2B 機能を設定したら、接続を作成します。以下の 3 つの接続が必要です。

- ソース・パートナーからハブへのエンベロープのための接続。
- ソース EDI トランザクションからターゲット EDI トランザクションへの接続。
- ハブからターゲット・パートナーへのエンベロープのための接続。

接続を作成するための詳細な手順については、253 ページの『第 12 章 接続の管理』で説明します。

## EDI から XML または ROD へのフローの設定

### このタスクについて

ここでは、EDI 交換の受信、EDI 交換のエンベロープ解除、EDI 形式から XML 文書または ROD 文書へのトランザクションの変換、およびトランザクションの配信に必要な対話について説明します。

**注:** EDI から XML へのフローの包括的な例については、363 ページの『 EDI から XML への例』を参照してください。 EDI から ROD へのフローの包括的な例については、347 ページの『 EDI から ROD への例』を参照してください。

1. ハブで受信する EDI 交換用の文書定義が存在することを確認します。交換のエンベロープが解除された後は、エンベロープが処理されなくなる点に注意してください。つまり、配信ポイントがなくなります。したがって、ターゲットの対話ではパッケージに対して「**N/A**」を使用することになります。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 既に文書定義が存在しているかどうかをチェックします。例えば、パートナーが AS パッケージ化、EDI-X12 プロトコル、および ISA 文書タイプで EDI 交換を送信しようとしている場合、その定義は既に使用可能になっています。同じく、N/A/EDI-X12/ISA 文書定義も既に存在しています。
   c. 文書定義がまだ存在していない場合は作成します。
2. ハブで受信する EDI 交換用の対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」を選択します。
   c. ソースとターゲットの文書をそれぞれ選択します。パッケージ化を除き (パッケージ化では、ターゲットが「**N/A**」になります)、文書定義は同じになります。
   d. 「アクション」リストから、「**EDI エンベロープ解除**」を選択します。
3. EDI トランザクションの文書定義、XML 文書または ROD 文書の定義、および XML 文書または ROD 文書へのトランザクション変換方法について記述されている変換マップをインポートします。211 ページの『 手動によるマップのインポート』を参照してください。

   交換に複数のトランザクションが含まれている場合は、トランザクションごとにこのステップを繰り返します。
4. 今インポートしたマップの対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。

c. 「**ソース**」で、トランザクションに関連付けられた文書タイプを選択します。パッケージとプロトコルを展開し、目的の文書タイプを選択します。通常、これは「**N/A**」 (トランザクション自体はパートナーから発せられたものではないため)、マップに定義されているプロトコル (例えば、**X12V4R1** など)、およびマップに定義されている実際の EDI 文書 (例えば、**850** など) になります。

d. 「**ターゲット**」の下で、変換した (XML または ROD) 文書の文書定義を選択します。パッケージとプロトコルを展開し、目的の文書タイプを選択します。

e. 変換マップ・リストから、この文書の変換方法が定義されているマップを選択します。

f. ネイティブ WDI の場合は、「アクション」リストから「**EDI 検証および EDI 変換**」を選択します。WTX の場合は「**EDI 検証および WTX 変換 (EDI Validate and WTX Transformation)**」を選択します。

フローに確認通知を追加するには、 222 ページの『確認通知の設定』を参照してください。

インタラクションを設定したら、パートナー用の B2B 機能を作成します。

- ソース・パートナーでは、(「**ソースの設定**」の下で) 2 つの文書定義 (エンベロープ用、および EDI トランザクション用の各文書定義) を使用可能にします。
- ターゲット・パートナーでは、(「**ターゲットの設定**」の下で) 2 つの文書定義 (EDI エンベロープ用、および XML または ROD 文書用の各文書定義) を使用可能にします。

B2B 機能を作成するための詳細な手順については、 28 ページの『B2B 機能の設定』で説明します。

パートナー用の B2B 機能を設定したら、接続を作成します。以下の 2 つの接続が必要です。

- ソース・パートナーからハブへのエンベロープのための接続。
- ソース EDI トランザクションから XML または ROD 文書への接続。

接続を作成するための詳細な手順については、 253 ページの『第 12 章 接続の管理』で説明します。

## XML または ROD から EDI へのフローの設定

### このタスクについて

ここでは、XML 文書または ROD 文書の受信、その文書の EDI トランザクションへの変換、トランザクションのエンベロープ、およびトランザクションの配信に必要な対話について説明します。

**注:** XML から EDI へのフローの包括的な例については、 369 ページの『 XML から EDI への例』を参照してください。 ROD から EDI へのフローの包括的な例については、 377 ページの『 ROD から EDI への例』を参照してください。

1. XML 文書または ROD 文書の定義、EDI トランザクションの文書定義、およびその文書の EDI トランザクションへの変換方法について記述されている変換マップをインポートします。 211 ページの『 手動によるマップのインポート』を参照してください。
2. 今インポートしたマップの対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。
   c. 「**ソース**」の下で、XML 文書または ROD 文書に関連付けられた文書定義を選択します。パッケージとプロトコルを展開し、目的の文書タイプを選択します。
   d. 「**ターゲット**」の下で、EDI トランザクションに関連付けられた文書タイプを選択します。パッケージとプロトコルを展開し、目的の文書タイプを選択します。トランザクションは直接には配信されないため (配信の前にエンベロープに入れられます)、「パッケージ」には「**N/A**」がリストされます。
   e. 変換マップ・リストから、この文書の変換方法が定義されているマップを選択します。
   f. ネイティブ WDI の場合は、「アクション」リストから「**XML 変換および EDI 検証**」または「**ROD 変換および EDI 検証**」を選択します。WTX の場合は「**WTX 変換**」を選択します。
3. ハブから送信される EDI 交換用の文書定義が存在することを確認し、その EDI 交換に関連付ける属性を設定します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 既に文書定義が存在しているかどうかをチェックします。ソース文書 (ハブから送信される交換) の「パッケージ」には、「**N/A**」を使用する必要があります。
   c. 配信対象の交換に適用する属性を編集します。
   d. 文書定義がまだ存在していない場合は、「パッケージ」、「プロトコル」、および「文書タイプ」を選択して作成します。
4. 文書の変換後にハブから送信される EDI 交換用の対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。
   c. ソースとターゲットの文書をそれぞれ選択します。ソース文書とターゲット文書のパッケージ化は異なりますが (ソース文書のパッケージは「N/A」)、同じプロトコル (EDI-X12 など) および文書タイプ (ISA など) にする必要があります。
   d. 「アクション」リストから「**パススルー**」を選択します。

インタラクションを設定したら、パートナー用の B2B 機能を作成します。

- ソース・パートナーでは、(「**ソースの設定**」の下で) 設定する必要のある文書定義の数は、文書タイプによって異なります。
  - 例えば、文書タイプが ICGPO、変換後の EDI トランザクションが MX12V3R1 である XML 文書の場合は、「**ソースの設定**」の下で、3 つの文書定義 (XML (ICGPO) 文書用、EDI トランザクション (MX12V3R1) 用、およびハブから送信されるエンベロープ用の各文書定義) を使用可能にします。

– その他の XML 文書および ROD 文書では、(「**ソースの設定**」の下で) 2 つの文書定義 (XML または ROD 文書用、およびハブから送信されるエンベロープ用の各文書定義) を使用可能にします。

- ターゲット・パートナーでは、(「**ターゲットの設定**」の下で) 2 つの文書定義 (EDI トランザクション用、および受信した EDI エンベロープ用の各文書定義) を使用可能にします。EDI トランザクションでは、プロトコルの横にある「**属性値の編集**」アイコンをクリックして、エンベロープ・プロファイルを指定します。ほかの属性も同様に指定することができます。

B2B 機能を作成するための詳細な手順については、 28 ページの『B2B 機能の設定』で説明します。

パートナー用の B2B 機能を設定したら、接続を作成します。以下の 2 つの接続が必要です。

- ソース XML または ROD 文書から EDI トランザクションへの接続。
- ハブからパートナーへのエンベロープのための接続。

接続を作成するための詳細な手順については、 253 ページの『第 12 章 接続の管理』で説明します。

## 1 つのファイル内の複数の XML 文書または ROD 文書から EDI へのフローの設定

### このタスクについて

このセクションでは、複数の XML 文書または ROD 文書を 1 つのファイルで受信し、その各文書を EDI トランザクションへ変換し、トランザクションをエンベロープして、EDI 交換を配信するために必要な対話について説明します。

1. XML 文書または ROD 文書の定義、EDI トランザクションの文書定義、および変換について記述されている変換マップをインポートします。 211 ページの『手動によるマップのインポート』を参照してください。
2. ソース文書とターゲット文書用の対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。
   c. ネイティブ WDI の場合は、ソース文書とターゲット文書を選択し、「アクション」リストから「**XML 変換および EDI 検証**」または「**ROD 変換および EDI 検証**」を選択します。WTX の場合は、「**WTX 変換**」および「**EDI 検証 (EDI validate)**」を選択します。
3. 変換マップで生成されるソース文書とターゲット文書ごとにステップ 2 を繰り返します。
4. ハブから送信される EDI 交換用の文書定義が存在することを確認し、その EDI 交換に関連付ける属性を設定します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 既に文書定義が存在しているかどうかをチェックします。ソースは「N/A」になり、そのプロトコルと文書タイプは交換の配信に使用されるプロトコルと文書タイプになります。例えば、EDI 交換が AS/EDI-X12/ISA として配信される場合、ソースは N/A/EDI-X12/ISA になります。
   c. 配信対象の交換に適用する属性を編集します。

d. 文書定義がまだ存在していない場合は、「パッケージ」、「プロトコル」、および「文書タイプ」を選択して作成します。

5. トランザクションの変換後にハブから送信される EDI 交換用の対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。
   c. ソースとターゲットの文書をそれぞれ選択します。ソース文書とターゲット文書のパッケージ化は異なりますが (ソース文書のパッケージは「N/A」)、同じプロトコル (EDI-X12 など) および文書タイプ (ISA など) にする必要があります。
   d. 「アクション」リストから「**パススルー**」を選択します。

インタラクションを設定したら、パートナー用の B2B 機能を作成します。

- ソース・パートナーでは、(「**ソースの設定**」の下で) 設定する必要のある文書定義の数は、文書タイプによって異なります。
  - 例えば、文書タイプが ICGPO、変換後の EDI トランザクションが MX12V3R1 である XML 文書の場合は、「**ソースの設定**」の下で、3 つの文書定義 (XML (ICGPO) 文書用、EDI トランザクション (MX12V3R1) 用、およびハブから送信されるエンベロープ用の各文書定義) を使用可能にします。
  - その他の XML 文書および ROD 文書では、(「**ソースの設定**」の下で) 2 つの文書定義 (XML または ROD 文書用、およびハブから送信されるエンベロープ用の各文書定義) を使用可能にします。

B2B 機能を作成するための詳細な手順については、28 ページの『B2B 機能の設定』で説明します。

パートナー用の B2B 機能を設定したら、接続を作成します。以下のいくつかの接続が必要です。

- EDI トランザクションに変換される各 XML または ROD 文書用の接続。
- ハブからパートナーへのエンベロープのための接続。

接続を作成するための詳細な手順については、253 ページの『第 12 章 接続の管理』で説明します。

## XML から ROD または ROD から XML への文書フローの設定

### このタスクについて

ここでは、XML 文書または ROD 文書の受信、その文書の他の文書タイプ (XML から ROD または ROD から XML) への変換、およびその文書の配信に必要な対話について説明します。

1. XML 文書と ROD 文書の定義、および文書の変換方法について記述されている変換マップをインポートします。211 ページの『 手動によるマップのインポート』を参照してください。
2. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**変換マップ**」をクリックし、今インポートしたマップの横にある「**詳細の表示**」アイコンをクリックします。
3. 今インポートしたマップの対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。

b. 「**インタラクションの作成**」をクリックします。

4. ソース文書とターゲット文書を選択し、「アクション」リストから「**WTX 変換**」 (WTX の場合) または「**ROD 変換および EDI 検証**」を選択します。

インタラクションを設定したら、パートナー用の B2B 機能を作成します。

- ソース・パートナーでは、(「**ソースの設定**」の下で) XML または ROD 文書用の文書定義を使用可能にします。
- ターゲット・パートナーでは、(「**ターゲットの設定**」の下で) XML または ROD 文書用の文書定義を使用可能にします。

B2B 機能を作成するための詳細な手順については、 28 ページの『B2B 機能の設定』で説明します。

パートナー用の B2B 機能を設定したら、接続を作成します。XML から ROD へのフロー、または ROD から XML へのフロー用の接続が 1 つ必要です。接続を作成するための詳細な手順については、 253 ページの『第 12 章 接続の管理』で説明します。

## XML から XML または ROD から ROD へのフローの設定

### このタスクについて

ここでは、XML 文書または ROD 文書の受信、その文書の同じ文書タイプ (XML から XML または ROD から ROD) への変換、およびその文書の配信に必要な対話について説明します。

1. XML 文書または ROD 文書の定義、および文書の変換方法について記述されている変換マップをインポートします。 211 ページの『 手動によるマップのインポート』を参照してください。
2. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**変換マップ**」をクリックし、今インポートしたマップの横にある「**詳細の表示**」アイコンをクリックします。
3. 今インポートしたマップの対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。
   c. ソースとターゲットの文書をそれぞれ選択します。
   d. ネイティブ WDI の場合は、「アクション」リストから「**XML 変換および EDI 検証**」 または「**ROD 変換および EDI 検証**」を選択します。WTX の場合は、「**WTX 変換**」および「**EDI 交換の検証**」を選択します。

インタラクションを設定したら、パートナー用の B2B 機能を作成します。

- ソース・パートナーでは、(「**ソースの設定**」の下で) XML または ROD 文書用の 1 つの文書定義を使用可能にします。
- ターゲット・パートナーでは、(「**ターゲットの設定**」の下で) XML または ROD 文書用の 1 つの文書定義を使用可能にします。

B2B 機能を作成するための詳細な手順については、 28 ページの『B2B 機能の設定』で説明します。

パートナー用の B2B 機能を設定したら、接続を作成します。XML から XML へのフロー、または ROD から ROD へのフロー用の接続が 1 つの要です。接続を作成

するための詳細な手順については、 253 ページの『第 12 章 接続の管理』で説明します。

## 確認通知の設定

ここでは、交換またはトランザクションの受信側の確認通知を文書のオリジネーターに送信するために必要な対話の設定方法について説明します。

### 機能確認通知

機能確認通知マップは、パートナーから受け取った EDI 文書に応答するときに、機能確認通知を生成する目的で使用します。WebSphere Partner Gateway には、よく使用される EDI 機能確認通知を生成する機能確認通知マップ・セットが用意されています。ただし、マッピング担当者が FA マップと検証マップを作成することもできます。この場合、作成されたマップは WebSphere Partner Gateway にアップロードされます。

**注:** 機能確認通知マップを作成するのは、カスタム機能確認通知が必要なときのみにしてください。

WebSphere Partner Gateway に用意されている機能確認通知マップのほかに、&FUNC_ACK_METADATA_DICTIONARY プロトコルおよび関連する &FUNC_ACK_META も用意されています。いずれも、「文書定義」ページの「**パッケージ: なし**」にリストされます。&FUNC_ACK_META は、すべての機能確認通知マップに共通のソース文書定義です。このマップは、機能確認通知の構造を備えています。機能確認通知はパートナーに送信され、機能確認通知マップによりシステムに、確認通知の生成方法が通知されます。 ソース文書定義の名前は変更できません。Data Interchange Services クライアントのマッピング担当者は、データベースにソース文書定義がなければ、機能確認通知マップを作成できません。

機能確認通知マップのターゲット文書定義は、機能確認通知のレイアウトを記述したものです。これは、997、999、または CONTRL という名前が付けられた EDI 文書定義である必要があります。

以下の機能確認通知マップが WebSphere Partner Gateway と共にインストールされ、「文書定義の管理」ページの「**パッケージ: N/A**」の下に表示されます。

*表 27. 製品提供の機能確認通知マップ*

| プロトコル | 文書タイプ | 説明 |
|---|---|---|
| &DTCTL21 | CONTRL | 機能確認通知 CONTRL – UN/EDIFACT バージョン 2 リリース 1 (D94B) |
| &DTCTL | CONTRL | 機能確認通知 CONTRL – UN/EDIFACT (D94B より前) |
| &DT99933 | 999 | 機能確認通知 999 – UCS バージョン 3 リリース 3 |
| &DT99737 | 997 | 機能確認通知 997 – X12 バージョン 3 リリース 7 |
| &DT99735 | 997 | 機能確認通知 997 – X12 バージョン 3 リリース 5 |

*表 27. 製品提供の機能確認通知マップ (続き)*

| プロトコル | 文書タイプ | 説明 |
|---|---|---|
| &DT99724 | 997 | 機能確認通知 997 – X12 バージョン 2 リリース 4 |

また、&X44TA1 プロトコル (および関連する TA1 文書タイプ) が「**パッケージ: N/A**」の下にリストされます。このマップは TA1 を生成するために使用されます。TA1 は、受信した X12 交換用に生成される機能確認通知です。

&WDIEVAL プロトコル (および関連する X12ENV) も、「**パッケージ: N/A**」の下に用意されています。

EDI トランザクションと同じく、機能確認通知も、必ず配信前に EDI 交換に含められます。

### TA1 確認通知

TA1 は、X12 交換確認通知を提供する EDI セグメントです。その役割は、X12 交換ヘッダーおよびトレーラー (ISA および IEA) のペアの受信と構文の正確さを確認することです。送信側は、ISA 交換制御ヘッダーの要素 14 を **1** に設定することによって、受信側に TA1 を要求できます。TA1 の交換制御番号が同じ制御番号の以前に送信済みの X12 交換と一致すると、確認通知プロセスが完了します。

EDI トランザクションおよび機能確認通知と同じく、TA1 も、必ず配信前に EDI 交換に含められます。

## 文書タイプへの確認通知の追加

### このタスクについて

確認通知をフローに追加するには、以下のステップを実行します。

1. WebSphere Partner Gateway が機能確認通知マップを提供しない場合は、Data Interchange Services クライアントからマップをインポートします。 211 ページの『 手動によるマップのインポート』を参照してください。
2. FA マップと文書定義を関連付けます。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**EDI FA マップ**」の順にクリックします。
   b. マップの横にある「**詳細の表示**」アイコンをクリックします。
   c. パッケージの横にある「**展開 (Expand)**」アイコンをクリックして、個々に適切なレベルまで展開します (例えば、「**パッケージ**」および「**プロトコル**」のフォルダーを展開して、トランザクションを選択します)。
   d. 「**保存**」をクリックします。
3. 今インポートしたマップの対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。
   c. 「**ソース**」で、機能確認通知に関連付けられた文書タイプを選択します。パッケージとプロトコルを展開し、目的の文書タイプを選択します。
   d. 「**ターゲット**」で、同じ値を選択します。

e. 「アクション」リストから「**パススルー**」を選択します。

4. ハブから送信される EDI 交換用の文書定義が存在することを確認し、その EDI 交換に関連付ける属性を設定します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 既に文書定義が存在しているかどうかをチェックします。ソースは「N/A」になり、そのプロトコルと文書タイプは交換の配信に使用されるプロトコルと文書タイプになります。例えば、EDI 交換が AS/EDI-X12/ISA として配信される場合、ソースは N/A/EDI-X12/ISA になります。
   c. 配信対象の交換に適用する属性を編集します。
   d. 文書定義がまだ存在していない場合は、「パッケージ」、「プロトコル」、および「文書タイプ」を選択して作成します。
5. 文書の変換後にハブから送信される EDI 交換用の対話を作成します。
   a. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
   b. 「**インタラクションの作成**」をクリックします。
   c. ソースとターゲットの文書をそれぞれ選択します。
   d. 「**アクション**」リストから「**パススルー**」を選択します。

## タスクの結果

インタラクションを設定したら、パートナー用の B2B 機能を作成します。機能確認通知送信のターゲット・パートナーは、元の EDI 文書のソース・パートナーであることに注意してください。

- ソース・パートナーでは、(「**ソースの設定**」の下で) 機能確認通知用の文書定義を使用可能にします。また、ハブから送信されるエンベロープ用の文書定義も使用可能にします。
- ターゲット・パートナーでは、(「**ターゲットの設定**」の下で) 機能確認通知用の文書定義を使用可能にします。また、受信する EDI エンベロープ用の文書定義も使用可能にします。

  機能確認通知では、プロトコルの横にある「**属性値の編集**」アイコンをクリックして、エンベロープ・プロファイルを指定します。

B2B 機能を作成するための詳細な手順については、28 ページの『B2B 機能の設定』で説明します。

パートナー用の B2B 機能を設定したら、接続を作成します。以下の 2 つの接続が必要です。

- 機能確認通知用の接続。
- ハブからパートナーへのエンベロープのための接続。

接続を作成するための詳細な手順については、253 ページの『第 12 章 接続の管理』で説明します。

# EDI 交換およびトランザクションの表示

## このタスクについて

この章で既に述べたように、文書フローを構成する EDI 交換やトランザクションについての情報を表示する場合に、文書ビューアーを使用できます。ロー文書とそれに関連する文書処理の詳細およびイベントを、特定の検索条件を使用して表示することができます。EDI 交換が正常に配信されたかどうかを調べたり、問題の原因を判別するときにこの情報が役に立ちます。

文書ビューアーを表示するには、以下を実行します。

1. 「**ビューアー**」>「**文書ビューアー**」をクリックします。
2. 該当する検索条件を選択してください。
3. 「**検索**」をクリックします。

文書ビューアーの使用法については、「*WebSphere Partner Gateway E/A 管理ガイド*」を参照してください。

# 第 11 章 宛先の作成

パートナーを作成したら、パートナーの宛先を定義します。宛先は、パートナーのシステムへの入り口点を定義するものです。

この章では以下のトピックを扱います。



**注:** WebSphere Partner Gateway の構成変更を行う場合は、必ず、コミュニティー・コンソールにログインしたときと同じブラウザー・インスタンスを使用してください。複数のブラウザー・インスタンスを同時に使用すると、構成変更が無効になる可能性があります。

## 宛先の概要

WebSphere Partner Gateway では、宛先を使用して文書を正しい宛先にルーティングします。受信側は外部パートナーまたは内部パートナーにすることができます。

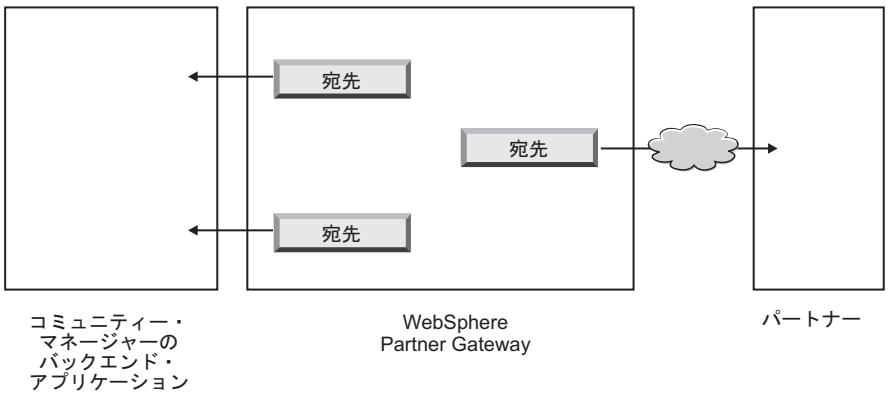



*図 34. 内部パートナーおよび外部パートナーへの宛先*

宛先の構成時にどの情報を使用するかは、アウトバウンド・トランスポート・プロトコルによって決まります。

パートナー宛先のトランスポートとしてデフォルトでサポートされているのは、次のとおりです。

- HTTP/1.1
- HTTPS/1.0
- HTTPS/1.1
- FTP
- FTPS
- JMS
- SMTP

  **注:** SMTP 宛先は、外部パートナーに対してのみ定義できます (内部パートナーに対しては定義できません)。
- SFTP
- ファイル・ディレクトリー
- FTP スクリプト記述

また、宛先の作成時にユーザー定義のトランスポートをアップロードして、それを指定することも可能です。

ハブ管理者は各パートナーの宛先を設定できますが、パートナー各自がこのタスクを実行することも可能です。ここでは、パートナーの代わりにタスクを実行する方法について説明します。宛先の管理については、*「E/A 管理ガイド」の『ハブ管理者のタスク』の章*を参照してください。

## グローバルなトランスポート値の設定

### このタスクについて

すべての FTP スクリプト記述宛先に適用されるグローバル・トランスポート属性を設定します。FTP スクリプト記述宛先を 1 つも定義しない場合には、このセクションの記述は必要ありません。

FTP スクリプト・トランスポートには、複数の FTP スクリプト記述インスタンスが同じ宛先に同時にアクセスできないようにする、ロック機構が使用されています。ゲートウェイ・インスタンスがロックを取得するまでに待機する時間や、ロックが使用されている場合にロックの取得を試みる回数などについては、デフォルト値が用意されています。これらのデフォルト値を使用することも、変更することもできます。

1. 「**アカウント管理**」>「**プロファイル**」をクリックします。
2. 「**宛先**」をクリックします。
3. 「宛先の詳細」から「**グローバル・トランスポート属性**」を選択します。

   ターゲットの作成時にグローバルなトランスポート値を指定したとき、「**最大ロック時間 (秒)**」または「**最大キュー時間 (秒) (Maximum Queue Time (Seconds))**」を更新した場合は、ここにその更新された値が反映されます。
4. デフォルト値がご使用の構成に対して適切である場合は、「**キャンセル**」をクリックします。それ以外の場合は、このセクションの残りのステップを継続します。
5. 「**FTP スクリプト・トランスポート**」の横にある「**編集**」アイコンをクリックします。
6. 1 つ以上の値を変更するには、新しい値を入力します。以下の値を変更できます。
   - 「**ロック再試行カウント**」。ロックが現在使用中である場合に、ロックを取得するために宛先が試行する回数を指定します。デフォルトは 3 です。
   - 「**ロック再試行間隔 (秒)**」。ロックの取得を試みてから次に試みるまでの経過時間を指定します。デフォルトは 260 秒です。
   - 「**最大ロック時間 (秒)**」。宛先がロックを保持できる期間を指定します。ターゲットの作成時に変更されていないかぎり、デフォルトは 240 秒です。
   - 「**最大キュー存続期間 (秒)**」。ターゲットがロックを取得するためにキューに待機する期間を指定します。ターゲットの作成時に変更されていないかぎり、デフォルトは 740 秒です。
7. 「**保存**」をクリックします。

## 順方向プロキシーの構成

### このタスクについて

HTTP トランスポートには、構成済みのプロキシー・サーバー経由で文書が送信されるように、順方向プロキシー・サポートをセットアップすることができます。WebSphere Partner Gateway では、次のタイプのサポートを設定できます。

- HTTP 経由のプロキシー・サポート
- 認証付き HTTP 経由のプロキシー・サポート
- SOCKS 経由のプロキシー・サポート

**注:** WebSphere Partner Gateway は、HTTP ポートでのみプロキシー・サーバーに接続します。

順方向プロキシーを設定したら、それをデフォルトの宛先にすると、トランスポートでグローバルに利用することができます (例えば、すべての HTTP 宛先がその順方向プロキシーを利用するなどです)。

順方向プロキシーを設定するには、以下のステップを実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**宛先**」をクリックします。
3. 「**順方向プロキシーのサポート**」をクリックします。
4. 「順方向プロキシー・リスト」ページで、「**作成**」をクリックします。
5. プロキシーの名前を入力します。
6. (オプション) プロキシーの説明を入力します。
7. リストからトランスポート・タイプを選択します。

   **注:** 選択できるトランスポートは、HTTP および HTTPS です。
8. 以下の情報を入力します。「プロキシー・ホスト」と「プロキシー・ポート」または「Socks プロキシー・ホスト」と「Socks プロキシー・ポート」のいずれかを入力します。
   - 「**プロキシー・ホスト**」には、使用するプロキシー・サーバー (例えば、http://proxy.abc.com) を入力します。
   - 「**プロキシー・ポート**」には、ポート番号を入力します。
   - プロキシー・サーバーにユーザー名とパスワードが必要な場合は、「**ユーザー名**」フィールドおよび「**パスワード**」フィールドにそれぞれ指定します。
   - 「**Socks プロキシー・ホスト**」には、使用する Socks プロキシー・サーバーを入力します。
   - 「**Socks プロキシー・ポート**」には、ポート番号を入力します。
9. このプロキシーをデフォルトのプロキシーにする場合は、チェック・ボックスを選択します (プロキシー・サポートが指定されているすべてのパートナーがそのプロキシーを使用できるようになります)。
10. 「**保存**」をクリックします。

**注:** 順方向プロキシーでは HTTP トンネリング技法が使用されますが、セキュア順方向プロキシーに対するサポートはありません。HTTP トンネルはプロキシー・サーバーと共に作成されます。どのタイプのデータ (HTTP または HTTPS) をエンド・パートナーに渡す場合でも、事前に接続を確認する必要があります。データは SSL 暗号化されています。順方向プロキシーに使用するポートは、HTTP ポート 80 でなければなりません。これは基本的には、WebSphere Partner Gateway とパートナーの間での SSL ハンドシェークのパススルーです。

## HTTP 宛先の設定

### このタスクについて

ハブからパートナーの IP アドレスに文書を送信できるように、HTTP 宛先を設定します。HTTP 宛先を設定するとき、構成済みのプロキシー・サーバー経由で文書が送信されるように指定することもできます。

HTTP 宛先の作成プロセスを開始するには、以下の手順を実行します。

1. 「**アカウント管理**」>「**プロファイル**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
3. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
4. 「**宛先**」をクリックします。
5. 「**作成**」をクリックします。

## 宛先の詳細

### このタスクについて

「**宛先リスト**」ページから、以下のステップを実行します。

1. 宛先を識別する名前を入力します。このフィールドは必須です。この名前が、宛先のリストに表示されることになります。
2. (オプション) 宛先の状況を指定します。デフォルトは「**有効**」です。有効状態の宛先は、文書を送信することができます。無効状態の宛先は、文書を送信できません。
3. (オプション) 宛先がオンラインかオフラインかを指定します。デフォルトは「**オンライン**」です。
4. (オプション) 宛先の説明を入力します。

## 宛先構成

### このタスクについて

ページの「**宛先構成**」セクションで、以下のステップを実行します。

1. (オプション) 使用するプロキシー・サーバーを選択します。「**順方向プロキシー・リスト**」には、デフォルトのプロキシー・サーバーも含め、既に作成したプロキシー・サーバーがすべて掲載されています。このフィールドのデフォルト値は、「**デフォルトの順方向プロキシーの使用**」です。選択したパートナーに別のプロキシー・サーバーを使用させる場合は、リストからそのサーバーを選択します。選択したパートナーにこの機能を使用させない場合は、「**順方向プロキシーを使用しない**」を選択します。
2. 「**アドレス**」フィールドに、文書の配信先となる URI を入力します。このフィールドは必須です。

   形式は、http://<*server_name*>:<*optional_port*>/<*path*> です。

   例えば、以下のような形式になります。

   ```
   http://anotherserver.ibm.com:57080/bcgreceiver/Receiver
   ```

   **注:** IPv6 アドレスを指定している場合、マシン名またはホスト名ではなく、数値形式を指定してください。

   IPv6 アドレスの例は以下のようになります。

```
http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
http://[1080:0:0:0:8:800:200C:417A]/index.html
http://[3ffe:2a00:100:7031::1]
http://[1080::8:800:200C:417A]/foo
http://[::192.9.5.5]/ipng
http://[::FFFF:129.144.52.38]:80/index.html
http://[2010:836B:4179::836B:4179]
```

Web サービス用に使用する宛先を設定するときは、Web サービス・プロバイダーから提供されたプライベート URL を指定します。この URL は、WebSphere Partner Gateway が Web サービス・プロバイダーのプロキシーとして動作する際に、Web サービスを呼び出す URL です。

3. (オプション) HTTP サーバーへのアクセスにユーザー名とパスワードが必要な場合は、ユーザー名とパスワードを入力します。
4. 「**再試行カウント**」フィールドに、宛先が文書の送信を試行する回数を入力します。この回数を超えると送信エラーとなります。デフォルトは 3 です。
5. 「**再試行間隔**」フィールドに、宛先が文書の再送信を試行するまでの待ち時間を入力します。デフォルトは 300 秒です。
6. 「**スレッド数**」フィールドに、同時に処理可能な文書の数を入力します。デフォルトは 3 です。
7. 文書を処理する前に送信者の IP アドレスを検証するには、「**クライアント IP の検証**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。
8. 指定した回数の再試行が終わって配信エラーになりそうな場合に、宛先を自動的にオフラインにするには、「**自動キュー**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。

   「**自動キュー**」を選択した場合は、宛先を手動でオンラインにするまで、すべての文書がキューに入ったままになります。
9. 「**接続タイムアウト**」フィールドに、トラフィックがない場合にソケットがオープン状態を保つ時間 (秒数) を入力します。デフォルトは 120 秒です。
10. 宛先の前処理または後処理ステップを構成する場合は、250 ページの『ハンドラーの構成』を参照してください。それ以外の場合は、「**保存**」をクリックします。

## HTTPS 宛先の設定

### このタスクについて

ハブからパートナーの IP アドレスに文書を送信できるように、HTTPS 宛先を設定します。HTTPS 宛先を設定するとき、構成済みのプロキシー・サーバー経由で文書が送信されるように指定することもできます。

HTTPS 宛先を作成するには、以下の手順を実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。

3. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
4. 「**宛先**」をクリックします。
5. 「**作成**」をクリックします。

## 宛先の詳細

### このタスクについて

「宛先の詳細」ページから、以下のステップを実行します。

1. 宛先を識別する名前を入力します。このフィールドは必須です。
2. (オプション) 宛先の状況を指定します。デフォルトは「**有効**」です。有効状態の宛先は、文書を送信することができます。無効状態の宛先は、文書を送信できません。
3. (オプション) 宛先がオンラインかオフラインかを指定します。デフォルトは「**オンライン**」です。
4. (オプション) 宛先の説明を入力します。
5. 「**トランスポート**」リストから、「**HTTPS/1.0**」または「**HTTPS/1.1**」を選択します。

## 宛先構成

### このタスクについて

ページの「**宛先構成**」セクションで、以下のステップを実行します。

1. (オプション) 使用するプロキシー・サーバーを選択します。「**順方向プロキシー・リスト**」には、デフォルトのプロキシー・サーバーも含め、既に作成したプロキシー・サーバーがすべて掲載されています。このフィールドのデフォルト値は、「**デフォルトの順方向プロキシーの使用**」です。選択したパートナーに別のプロキシー・サーバーを使用させる場合は、リストからそのサーバーを選択します。選択したパートナーにこの機能を使用させない場合は、「**順方向プロキシーを使用しない**」を選択します。
2. 「**アドレス**」フィールドに、文書の配信先となる URI を入力します。このフィールドは必須です。

   形式は、https://<*server_name*>:<*optional_port*>/<*path*> です。

   以下に例を示します。

   ```
   https://anotherserver.ibm.com:57443/bcgreceiver/Receiver
   ```

   **注:** IPv6 アドレスを指定している場合、マシン名またはホスト名ではなく、数値形式を指定してください。

   IPv6 アドレスの例は以下のようになります。

   ```
   https://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
   https://[1080:0:0:0:8:800:200C:417A]/index.html
   https://[3ffe:2a00:100:7031::1]
   https://[1080::8:800:200C:417A]/foo
   https://[::192.9.5.5]/ipng
   https://[::FFFF:129.144.52.38]:80/index.html
   https://[2010:836B:4179::836B:4179]
   ```

3. (オプション) セキュア HTTP サーバーへのアクセスにユーザー名とパスワードが必要な場合は、ユーザー名とパスワードを入力します。
4. 「**再試行カウント**」フィールドに、宛先が文書の送信を試行する回数を入力します。この回数を超えると送信エラーとなります。デフォルトは 3 です。
5. 「**再試行間隔**」フィールドに、宛先が文書の再送信を試行するまでの待ち時間を入力します。デフォルトは 300 秒です。
6. 「**スレッド数**」フィールドに、同時に処理可能な文書の数を入力します。デフォルトは 3 です。
7. 文書を処理する前に送信者の IP アドレスを検証するには、「**クライアント IP の検証**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。
8. 文書に関連付けられたビジネス ID と照合して、送信パートナーのデジタル証明書を検証する場合は、「**クライアント SSL 証明書の検証**」フィールドで「**はい**」を選択します。デフォルトは「**いいえ**」です。
9. 指定した回数の再試行が終わって配信エラーになりそうな場合に、宛先を自動的にオフラインにするには、「**自動キュー**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。

   「**自動キュー**」を選択した場合は、宛先を手動でオンラインにするまで、すべての文書がキューに入ったままになります。
10. 「**接続タイムアウト**」フィールドに、トラフィックがない場合にソケットがオープン状態を保つ時間 (秒数) を入力します。デフォルトは 120 秒です。
11. 宛先の前処理または後処理ステップを構成する場合は、250 ページの『ハンドラーの構成』を参照してください。それ以外の場合は、「**保存**」をクリックします。

## FTP 宛先の設定

### このタスクについて

FTP 宛先を作成するには、以下の手順を実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
3. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
4. 「**宛先**」をクリックします。
5. 「**作成**」をクリックします。

**注:** FTP 受動モードはサポートされていません。受動モードのサポートについては、244 ページの『FTP スクリプト記述宛先の設定』を参照してください。

## 宛先の詳細

### このタスクについて

「宛先の詳細」ページから、以下のステップを実行します。

1. 宛先を識別する名前を入力します。このフィールドは必須です。
2. (オプション) 宛先の状況を指定します。デフォルトは「**有効**」です。有効状態の宛先は、文書を送信することができます。無効状態の宛先は、文書を送信できません。
3. (オプション) 宛先がオンラインかオフラインかを指定します。デフォルトは「**オンライン**」です。
4. (オプション) 宛先の説明を入力します。

## 宛先構成

### このタスクについて

ページの「**宛先構成**」セクションで、以下のステップを実行します。

1. 「**アドレス**」フィールドに、文書の配信先となる URI を入力します。このフィールドは必須です。

   形式は、ftp://*<ftp_server_name>*:*<portno>* です。

   以下に例を示します。

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   ポート番号を入力しなかった場合は、標準の FTP ポートが使用されます。

   **注:** IPv6 アドレスを指定している場合、マシン名またはホスト名ではなく、数値形式を指定してください。

   IPv6 アドレスの例は以下のようになります。

   ```
   ftp://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:21
   ftp://[1080:0:0:0:8:800:200C:417A]:21
   ftp://[3ffe:2a00:100:7031::1]:21
   ftp://[1080::8:800:200C:417A]:21
   ftp://[::192.9.5.5]:21
   ftp://[::FFFF:129.144.52.38]:21
   ftp://[2010:836B:4179::836B:4179]:21
   ```

2. (オプション) FTP サーバーへのアクセスにユーザー名とパスワードが必要な場合は、ユーザー名とパスワードを入力します。
3. 「**再試行カウント**」フィールドに、宛先が文書の送信を試行する回数を入力します。この回数を超えると送信エラーとなります。デフォルトは 3 です。
4. 「**再試行間隔**」フィールドに、宛先が文書の再送信を試行するまでの待ち時間を入力します。デフォルトは 300 秒です。
5. 「**スレッド数**」フィールドに、同時に処理可能な文書の数を入力します。デフォルトは 3 です。
6. 文書を処理する前に送信者の IP アドレスを検証するには、「**クライアント IP の検証**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。

7. 指定した回数の再試行が終わって配信エラーになりそうな場合に、宛先を自動的にオフラインにするには、「**自動キュー**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。

   「**自動キュー**」を選択した場合は、宛先を手動でオンラインにするまで、すべての文書がキューに入ったままになります。
8. 「**接続タイムアウト**」フィールドに、トラフィックがない場合にソケットがオープン状態を保つ時間 (秒数) を入力します。デフォルトは 120 秒です。
9. 文書が宛先に送信されるときに、その文書が元の名前を持つようにする場合は、「**固有ファイル名の使用**」を選択しないでください。 WebSphere Partner Gateway でファイルに名前を割り当てる場合は、これを選択してください。
10. 宛先の前処理または後処理ステップを構成する場合は、250 ページの『ハンドラーの構成』を参照してください。それ以外の場合は、「**保存**」をクリックします。

## SMTP 宛先の設定

### このタスクについて

SMTP 宛先を作成するには、以下の手順を実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
3. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
4. 「**宛先**」をクリックします。
5. 「**作成**」をクリックします。

## 宛先の詳細

### このタスクについて

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を識別する名前を入力します。このフィールドは必須です。
2. (オプション) 宛先の状況を指定します。デフォルトは「**有効**」です。有効状態の宛先は、文書を送信することができます。無効状態の宛先は、文書を送信できません。
3. (オプション) 宛先がオンラインかオフラインかを指定します。デフォルトは「**オンライン**」です。
4. (オプション) 宛先の説明を入力します。

## 宛先構成

### このタスクについて

ページの「**宛先構成**」セクションで、以下のステップを実行します。

1. 「**アドレス**」フィールドに、文書の配信先となる URI を入力します。このフィールドは必須です。

   形式は、mailto:<*user@server_name*> です。

   以下に例を示します。

   ```
   mailto:admin@anotherserver.ibm.com
   ```

2. (オプション) SMTP サーバーへのアクセスにユーザー名とパスワードが必要な場合は、ユーザー名とパスワードを入力します。
3. 「**再試行カウント**」フィールドに、宛先が文書の送信を試行する回数を入力します。この回数を超えると送信エラーとなります。デフォルトは 3 です。
4. 「**再試行間隔**」フィールドに、宛先が文書の再送信を試行するまでの待ち時間を入力します。デフォルトは 300 秒です。
5. 「**スレッド数**」フィールドに、同時に処理可能な文書の数を入力します。デフォルトは 3 です。
6. 文書を処理する前に送信者の IP アドレスを検証するには、「**クライアント IP の検証**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。
7. 指定した回数の再試行が終わって配信エラーになりそうな場合に、宛先を自動的にオフラインにするには、「**自動キュー**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。

   「**自動キュー**」を選択した場合は、宛先を手動でオンラインにするまで、すべての文書がキューに入ったままになります。
8. 「**認証が必要**」フィールドで、文書にユーザー名とパスワードが必要かどうかを指定します。デフォルトは「**いいえ**」です。
9. 宛先の前処理または後処理ステップを構成する場合は、250 ページの『ハンドラーの構成』を参照してください。それ以外の場合は、「**保存**」をクリックします。

## JMS 宛先の設定

### このタスクについて

JMS 宛先を作成するには、以下の手順を実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
3. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
4. 「**宛先**」をクリックします。
5. 「**作成**」をクリックします。

**注:** 必要な WebSphere MQ JAR ファイルを WebSphere Partner Gateway で表示できるようにするためのランタイム・ライブラリーの構成については、42 ページの『ランタイム・ライブラリーの構成』を参照してください。

## 宛先の詳細

### このタスクについて

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を識別する名前を入力します。このフィールドは必須です。
2. (オプション) 宛先の状況を指定します。デフォルトは「**有効**」です。有効状態の宛先は、文書を送信することができます。無効状態の宛先は、文書を送信できません。
3. (オプション) 宛先がオンラインかオフラインかを指定します。デフォルトは「**オンライン**」です。
4. (オプション) 宛先の説明を入力します。

## 宛先構成

### このタスクについて

ページの「**宛先構成**」セクションで、以下のステップを実行します。

1. 「**アドレス**」フィールドに文書の配信先の URL を入力します。このフィールドは必須です。

   WebSphere MQ JMS の場合、ターゲット URL の形式は以下のようになります。

   ```
   file:///<user_defined_MQ_JNDI_bindings_path>
   ```

   以下に例を示します。

   ```
   file:///opt/JNDI-Directory in case of UNIX and
   file://c:/temp/ in case of Windows.
   ```

   このディレクトリーには、ファイル・ベースの JNDI の「.bindings」ファイルが含まれています。このファイルは、WebSphere Partner Gateway が目的の宛先に文書をルーティングする方法を示します。

   - 内部 JMS 宛先 (バックエンド・システムに対する宛先) では、これは WebSphere Partner Gateway を JMS 対応として構成した際 (ステップ 5 (40 ページ) を参照) に入力した値 (バインディング・ファイルのファイル・システム・パス) と一致していなければなりません。また、JMS コンテキストのサブフォルダーを JMS プロバイダー URL の一部として指定することもできます。

     例えば、JMS コンテキストを指定しない場合、`c:/temp/JMS` と入力します。JMS コンテキストを指定する場合は、`c:/temp/JMS/JMS` と入力します。
   - パートナー宛先の場合、パートナーが「.bindings」ファイルを指定する可能性があります。

   このフィールドは必須です。
2. (オプション) JMS キューへのアクセスにユーザー名とパスワードが必要な場合は、ユーザー名とパスワードを入力します。
3. 「**再試行カウント**」フィールドに、宛先が文書の送信を試行する回数を入力します。この回数を超えると送信エラーとなります。デフォルトは 3 です。

4. 「**再試行間隔**」フィールドに、宛先が文書の再送信を試行するまでの待ち時間を入力します。デフォルトは 300 秒です。
5. 「**スレッド数**」フィールドに、同時に処理可能な文書の数を入力します。デフォルトは 3 です。
6. 文書を処理する前に送信者の IP アドレスを検証するには、「**クライアント IP の検証**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。
7. 指定した回数の再試行が終わって配信エラーになりそうな場合に、宛先を自動的にオフラインにするには、「**自動キュー**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。

   「**自動キュー**」を選択した場合は、宛先を手動でオンラインにするまで、すべての文書がキューに入ったままになります。
8. 「**認証が必要**」フィールドで、文書にユーザー名とパスワードが必要かどうかを指定します。デフォルトは「**いいえ**」です。
9. 「**JMS ファクトリー名**」フィールドに、JMS プロバイダーが JMS キューへの接続に使用する Java クラスの名前を入力します。このフィールドは必須です。

   内部 JMS 宛先の場合、この名前は、バインディング・ファイルの作成時 (ステップ 4 (42 ページ)) に `define qcf` コマンドで指定した名前と一致していなければなりません。

   ステップ 1 (238 ページ) で JMS コンテキストのサブフォルダーを入力した場合、ここではファクトリー名だけを入力します (例えば、`Hub`)。「**アドレス**」フィールドに JMS コンテキストのサブフォルダーを入力しなかった場合は、ファクトリー名の前にサブフォルダーを指定してください (例えば、`JMS/Hub` )。
10. 「**JMS メッセージ・クラス**」フィールドにメッセージ・クラスを入力します。TextMessage や BytesMessage など、有効な JMS メッセージ・クラスを入力します。このフィールドは必須です。
11. 「**JMS メッセージ・タイプ**」フィールドに、メッセージのタイプを入力します。これはオプションのフィールドです。
12. 「**プロバイダー URL パッケージ**」フィールドに、Java で JMS コンテキスト URL を認識するために使用するクラス (または JAR ファイル) の名前を入力します。このフィールドはオプションです。値を指定しなかった場合は、バインディング・ファイルのファイル・システム・パスが使用されます。
13. 「**JMS キュー名**」フィールドに、文書を送信する JMS キューの名前を入力します。このフィールドは必須です。

    内部 JMS 宛先の場合、この名前は、バインディング・ファイルの作成時 (ステップ 4 (42 ページ)) に `define q` コマンドで指定した名前と一致していなければなりません。

    ステップ 1 (238 ページ) で JMS コンテキストのサブフォルダーを入力した場合、ここではキュー名だけを入力します (例えば、`outQ`)。JMS プロバイダー URL に JMS コンテキストのサブフォルダーを入力しなかった場合は、ファクトリー名の前にサブフォルダーを指定してください (例えば、`JMS/outQ`)。

14. 「**JMS JNDI ファクトリー名**」フィールドに、ネーム・サービスへの接続に使用するファクトリー名を入力します。このフィールドは必須です。 39 ページの『JMS トランスポート・プロトコル用のハブの構成』の説明に従い独自の WebSphere MQ の JMS 構成を設定した場合、使用する値は、おそらく com.sun.jndi.fscontext.RefFSContextFactory です。
15. 宛先の前処理または後処理ステップを構成する場合は、 250 ページの『ハンドラーの構成』を参照してください。それ以外の場合は、「**保管**」をクリックします。

## ファイル・ディレクトリー宛先の設定

### このタスクについて

ファイル・ディレクトリー宛先を作成するには、以下の手順を実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
3. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
4. 「**宛先**」をクリックします。
5. 「**作成**」をクリックします。

## 宛先の詳細

### このタスクについて

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を識別する名前を入力します。このフィールドは必須です。
2. (オプション) 宛先の状況を指定します。デフォルトは「**有効**」です。有効状態の宛先は、文書を送信することができます。無効状態の宛先は、文書を送信できません。
3. (オプション) 宛先がオンラインかオフラインかを指定します。デフォルトは「**オンライン**」です。
4. (オプション) 宛先の説明を入力します。

## 宛先構成

### このタスクについて

ページの「**宛先構成**」セクションで、以下のステップを実行します。

1. 「**アドレス**」フィールドに、文書の配信先となる URI を入力します。このフィールドは必須です。

   WebSphere Partner Gateway がインストールされているドライブと同じドライブにファイル・ディレクトリーがある UNIX および Windows システムの場合、形式は file://<*path_to_target_directory*> になります。

   以下に例を示します。

file://localfiledir

ここで、*localfiledir* は、ルート・ディレクトリー以外のディレクトリーです。

ファイル・ディレクトリーの宛先を、WebSphere Partner Gateway がインストールされているドライブ「以外」の Windows ドライブに作成する必要がある場合、パスは次のようになります。file:///<*drive_letter*>:/<*path*>

2. 「**再試行カウント**」フィールドに、宛先が文書の送信を試行する回数を入力します。この回数を超えると送信エラーとなります。デフォルトは 3 です。
3. 「**再試行間隔**」フィールドに、宛先が文書の再送信を試行するまでの待ち時間を入力します。デフォルトは 300 秒です。
4. 「**スレッド数**」フィールドに、同時に処理する文書の数を入力します。デフォルトは 3 です。
5. 文書を処理する前に送信者の IP アドレスを検証するには、「**クライアント IP の検証**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。
6. 指定した回数の再試行が終わって配信エラーになりそうな場合に、宛先を自動的にオフラインにするには、「**自動キュー**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。

   「**自動キュー**」を選択した場合は、宛先を手動でオンラインにするまで、すべての文書がキューに入ったままになります。
7. 文書が宛先に送信されるときに、その文書が元の名前を持つようにする場合は、「**固有ファイル名の使用**」を選択しないでください。 WebSphere Partner Gateway でファイルに名前を割り当てる場合は、これを選択してください。
8. 宛先の前処理または後処理ステップを構成する場合は、 250 ページの『ハンドラーの構成』を参照してください。それ以外の場合は、「**保存**」をクリックします。

## FTPS 宛先の設定

### このタスクについて

FTPS 宛先を作成するには、以下の手順を実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
3. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
4. 「**宛先**」をクリックします。
5. 「**作成**」をクリックします。

**注:** FTPS 受動モードはサポートされていません。受動モードのサポートについては、 244 ページの『FTP スクリプト記述宛先の設定』を参照してください。

## 宛先の詳細

### このタスクについて

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を識別する名前を入力します。このフィールドは必須です。
2. (オプション) 宛先の状況を指定します。デフォルトは「**有効**」です。有効状態の宛先は、文書を送信することができます。無効状態の宛先は、文書を送信できません。
3. (オプション) 宛先がオンラインかオフラインかを指定します。デフォルトは「**オンライン**」です。
4. (オプション) 宛先の説明を入力します。

## 宛先構成

### このタスクについて

ページの「**宛先構成**」セクションで、以下のステップを実行します。

1. 「**アドレス**」フィールドに、文書の配信先となる URI を入力します。このフィールドは必須です。

   形式は、ftp://<*ftp_server_name*>:<*portno*> です。

   以下に例を示します。

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   ポート番号を入力しなかった場合は、標準の FTP ポートが使用されます。
2. (オプション) セキュア FTP サーバーへのアクセスにユーザー名とパスワードが必要な場合は、ユーザー名とパスワードを入力します。
3. 「**再試行カウント**」フィールドに、宛先が文書の送信を試行する回数を入力します。この回数を超えると送信エラーとなります。デフォルトは 3 です。
4. 「**再試行間隔**」フィールドに、宛先が文書の再送信を試行するまでの待ち時間を入力します。デフォルトは 300 秒です。
5. 「**スレッド数**」フィールドに、同時に処理する文書の数を入力します。デフォルトは 3 です。
6. 文書を処理する前に送信者の IP アドレスを検証するには、「**クライアント IP の検証**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。
7. 指定した回数の再試行が終わって配信エラーになりそうな場合に、宛先を自動的にオフラインにするには、「**自動キュー**」フィールドで「**はい**」を選択します。それ以外の場合は、「**いいえ**」を選択します。デフォルトは「**いいえ**」です。

   「**自動キュー**」を選択した場合は、宛先を手動でオンラインにするまで、すべての文書がキューに入ったままになります。
8. 「**接続タイムアウト**」フィールドに、トラフィックがない場合にソケットがオープン状態を保つ時間 (秒数) を入力します。デフォルトは 120 秒です。

9. 文書が宛先に送信されるときに、その文書が元の名前を持つようにする場合は、「**固有ファイル名の使用**」を選択しないでください。 WebSphere Partner Gateway でファイルに名前を割り当てる場合は、これを選択してください。
10. 宛先の前処理または後処理ステップを構成する場合は、 250 ページの『ハンドラーの構成』を参照してください。それ以外の場合は、「**保存**」をクリックします。

## SFTP 宛先の設定

### このタスクについて

ハブからパートナーの IP アドレスに文書を送信できるように、SFTP 宛先を設定します。アダプターは、SFTP サーバーに接続して SFTP サーバーに文書を送信します。文書データは、ストリームとしてアダプターに提供されます。

SFTP 宛先を作成するには、以下の手順を実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
3. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
4. 「**宛先**」をクリックします。
5. 「**作成**」をクリックします。

## 宛先の詳細

### このタスクについて

「宛先の詳細」ページで、以下のステップを実行します。

1. 宛先を識別する名前を入力します。このフィールドは必須です。
2. (オプション) 宛先の状況を指定します。デフォルトは「**有効**」です。有効状態の宛先は、文書を送信することができます。無効状態の宛先は、文書を送信できません。
3. (オプション) 宛先がオンラインかオフラインかを指定します。デフォルトは「**オンライン**」です。
4. (オプション) 宛先の説明を入力します。
5. 「**トランスポート**」リストから、「**SFTP**」を選択します。

## 宛先構成

### このタスクについて

ページの「**宛先構成**」セクションで、以下のステップを実行します。

1. 「**SFTP ホスト IP / ホスト名**」を入力します。最大文字数は 100 文字です。IP アドレス、IPv4 アドレス、および IPv6 アドレスを入力することもできます。
2. 「**ポート番号**」を入力します。最小値は 1、最大値は 65535 です。デフォルト値は 22 です。

3. 「**出力ディレクトリー**」を入力します。最大文字数は 100 文字です。ロケールに応じた文字を使用できます。
4. 「**認証タイプ**」で、「ユーザー名/パスワード (username/password)」または「秘密鍵認証 (private key authentication)」を選択します。
5. ユーザー名/パスワードの場合は、「**ユーザー名**」および「**パスワード**」を入力します。「認証タイプ」が「秘密鍵認証 (private key authentication)」である場合は、「**ユーザー名**」、「**秘密鍵ファイル**」、および「**パスフレーズ**」を入力します。「**秘密鍵ファイル**」は、OpenSSH 形式の秘密鍵ファイルのパスです。
6. 「**再試行カウント**」を入力します。これは、接続が成功しなかったときに、レシーバーが SFTP サーバーへの接続を試行する回数です。
7. 「**再試行間隔**」を入力します。これは、各再試行の間のレシーバーの待ち時間です。
8. 「**スレッド数**」を入力します。
9. 「**EIS エンコード**」は FTP サーバーのエンコードです。この値は、FTP サーバーの制御接続のエンコードを設定するために使用します。
10. 「**サーバー認証の有効化 (Enable server authentication)**」を有効にすると、接続を確立する先のサーバーを認証できます。サーバー認証を有効にする場合は、ホスト・キー・ファイル・パスを入力します。ホスト・キー・ファイルは、OpenSSH の形式で指定する必要があります。
11. 「**保存**」をクリックして、構成を保存します。
12. ハンドラーの構成を入力し、「**保存**」をクリックして構成の詳細を保存します。

**注:** 構成の保存後、以下のようにして、対応するサーバーを再始動してください。

- シンプル・モードでは、bcgserver サーバーを再始動します
- シンプル配布モードでは、bcgserver クラスターを再始動します
- 完全配布モードでは、BCGDocMgr クラスターを再始動します

## FTP スクリプト記述宛先の設定

FTP スクリプト記述宛先は、設定されたスケジュールに従って動作します。FTP スクリプト記述宛先の動作は、FTP コマンド・スクリプトによって管理されます。

**注:** データベースがダウンし、「ロック・ユーザー」が「はい」に設定されている場合、FTP スクリプト記述宛先はデータベースからロックを取得しないため、作動しないことがあります。

**注:** AIX プラットフォームでは、トランザクション量が多い文書を送信する場合はパッシブ・モードを使用してください。ファイル転送操作で、スクリプトにパッシブ・モードを指定してください。これは、FTP スクリプト記述宛先で使用されます。スクリプトでは、'passive' コマンドと 'pasv' コマンドのいずれも同じように使用できます。アクティブ・モードを使用すると、エラーが発生します。

# FTP スクリプトの作成

## このタスクについて

FTP スクリプト記述宛先を使用するには、必要な FTP コマンドのうち、ご使用の FTP サーバーで認められているものをすべて記載したファイルを作成します。

1. 宛先のスクリプトを作成して、実行するアクションを指定します。例えば、以下のスクリプトは、名前とパスワードで指定された FTP サーバーに接続して、FTP サーバー上で指定のディレクトリーに移動し、その中のすべてのファイルをサーバー上の指定のディレクトリーに送信するという例です。

   ```
   open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% %BCGOPTIONx%
   cd %BCGOPTIONx%
   mput *
   quit
   ```

   宛先がサービスを提供するとき、プレースホルダー (例えば、%BCGSERVERIP% など) は、FTP スクリプト記述宛先の特定のインスタンスを作成するときに入力した値に置き換えられます (以下の表を参照してください)。

   *表 28. スクリプト・パラメーターと FTP スクリプト記述宛先フィールドの項目のマッピング*

| スクリプト・パラメーター | FTP スクリプト記述宛先フィールドの項目 |
|---|---|
| %BCGSERVERIP% | サーバー IP |
| %BCGUSERID% | ユーザー ID |
| %BCGPASSWORD% | パスワード |
| %BCGOPTIONx% | **ユーザー定義属性**の下のオプション *x* |

   ユーザー定義オプションは、最大 10 個まで設定できます。
2. ファイルを保存します。

# FTP スクリプト・コマンド

スクリプトを作成する場合は、以下のコマンドを使用できます。

- ascii、binary、passive、epsv

  これらのコマンドは FTP サーバーに送信されません。各コマンドにより、FTP サーバーへの転送モード (ASCII、バイナリー、またはパッシブ) が変更されます。
- cd

  指定されたディレクトリーに移動します。
- delete

  FTP サーバーからファイルを削除します。
- mkdir

  FTP サーバー上にディレクトリーを作成します。
- mput

このコマンドは、リモート・システムに転送する 1 つ以上のファイルを指定する単一の引数を取ります。この引数に標準のワイルドカード文字 (「*」および「?」) を指定して、複数のファイルを示すことができます。

- mputren

  このコマンドは、<source>、<temporary>、および <target> という 3 つの引数を取ります。アスタリスク (*) は処理中の現行ファイルの名前を表します。

  **source** FTP サーバーに格納されるファイルの名前。想定される値はアスタリスク (*) です。

  **temporary**
  <source> を FTP サーバーに格納するときに使用される一時ファイル名。

  **ターゲット**
  <temporary> の名前変更後のファイル名。名前変更後は、一時ファイルは存在しません。

  **例:**

  **mputren * *.tmp ***
  この例では、現行ファイルに拡張子 .tmp を付けたものが FTP サーバーに格納されます。サーバーへのファイルの格納後に、ファイル名が元の名前に変更されます。

  **mputren * *.tmp *.ready**
  この例では、現行ファイルに拡張子 .tmp を付けたものが FTP サーバーに格納されます。サーバーへのファイルの格納後に、ファイル名が元の名前に .ready 拡張子を付けたものに変更されます。

  **mputren * *.tmp /complete/***
  この例では、現行ファイルに拡張子 .tmp を付けたものが FTP サーバーに格納されます。サーバーへのファイルの格納後に、ファイル名が元の名前に変更され、/complete ディレクトリーに保管されます。この時点以降、一時ファイル *.tmp は存在しません。

  **mputren * *.tmp /complete/*.final**
  この例では、現行ファイルに拡張子 .tmp を付けたものが FTP サーバーに格納されます。サーバーへのファイルの格納後に、ファイル名が元の名前に変更され、.final 拡張子を付けたものが /complete ディレクトリーに保管されます。この時点以降、一時ファイル *.tmp は存在しません。

- open

  このコマンドは、FTP サーバー IP アドレス、ユーザー名、およびパスワードの 3 つのパラメーターを取ります。これらのパラメーターは、%BCGSERVERIP%、%BCGUSERID%、および %BCGPASSWORD% 変数に対応します。

  したがって、FTP スクリプト記述宛先スクリプトの最初の行は次のようになります。

  ```
  open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
  ```

- quit

  FTP サーバーへの既存の接続を終了します。

- quote

  QUOTE の後に指定されているものをすべてコマンドとしてリモート・システムに送信するように指定します。これにより、標準の FTP プロトコルに定義されていないコマンドをリモート FTP サーバーに送信できるようになります。

- rmdir

  FTP サーバーからディレクトリーを削除します。

- site

  このコマンドは、サイト固有のコマンドをリモート・システムに発行するときに使用できます。リモート・システムは、このコマンドの内容が有効かどうかを判別します。

## FTP スクリプト記述宛先

### このタスクについて

FTP スクリプト記述宛先を使用する場合は、以下の作業を実行します。

FTP スクリプト記述宛先を作成するには、以下の手順を実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
3. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
4. 「**宛先**」をクリックします。
5. 「**作成**」をクリックします。

## 宛先の詳細

### このタスクについて

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を識別する名前を入力します。このフィールドは必須です。
2. (オプション) 宛先の状況を指定します。デフォルトは「**有効**」です。有効状態の宛先は、文書を送信することができます。無効状態の宛先は、文書を送信できません。
3. (オプション) 宛先がオンラインかオフラインかを指定します。デフォルトは「**オンライン**」です。
4. (オプション) 宛先の説明を入力します。

## 宛先構成

### このタスクについて

ページの「**宛先構成**」セクションで、以下のステップを実行します。

1. 文書の送信先となる FTP サーバーの IP アドレスを入力します。FTP スクリプトが実行されると、ここに入力した値で %BCGSERVERIP% が置き換えられます。

   **注:** IPv6 アドレスを指定している場合、マシン名またはホスト名ではなく、数値形式を指定してください。

   IPv6 アドレスの例は以下のようになります。

   ```
   FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
   1080:0:0:0:8:800:200C:417A
   3ffe:2a00:100:7031::1
   1080::8:800:200C:417A
   ::192.9.5.5
   ::FFFF:129.144.52.38
   2010:836B:4179::836B:4179
   ```

2. FTP サーバーへのアクセスに必要なユーザー ID とパスワードを入力します。FTP スクリプトが実行されると、ここに入力した値で %BCGUSERID% および %BCGPASSWORD% が置き換えられます。
3. ターゲットがセキュア・モードの場合は、「**FTPS モード**」に対して「**はい**」をクリックしてください。それ以外の場合は、デフォルトの「**いいえ**」を使用します。
4. 以下のステップを実行して、スクリプト・ファイルをアップロードします。
   a. 「**スクリプト・ファイルのアップロード**」をクリックします。
   b. 文書を処理するスクリプトが格納されたファイルの名前を入力するか、または「**参照**」 を使用して、ファイルにナビゲートします。
   c. 「**スクリプト・ファイルのエンコード・タイプ**」を選択します。
   d. 「**ファイルのロード**」をクリックして、スクリプト・ファイルを「**現在ロードされているスクリプト・ファイル**」テキスト・ボックスにロードします。
   e. このスクリプト・ファイルを使用したい場合は、「**保存**」をクリックします。
   f. 「**ウィンドウを閉じる**」をクリックします。
5. 「**再試行カウント**」フィールドに、宛先が文書の送信を試行する回数を入力します。この回数を超えると送信エラーとなります。デフォルトは 3 です。
6. 「**再試行間隔**」フィールドに、宛先が文書の再送信を試行するまでの待ち時間を入力します。デフォルトは 300 秒です。
7. 「**接続タイムアウト**」に、トラフィックがなくてもソケットを開いたままにしておく時間 (秒数) を入力します。デフォルトは 120 秒です。
8. 「**ロック・ユーザー**」フィールドに、宛先がロックを要求して、FTP スクリプト記述宛先の他のインスタンスが同時に同じ FTP サーバー・ディレクトリーにアクセスできないようにするかどうかを指定します。

**注:** 「**グローバル FTP スクリプト記述属性**」には既に値が入っており、このページから編集することはできません。これらの値を変更するには、「グローバル・トランスポート属性」ページを使用します ( 228 ページの『グローバルなトランスポート値の設定』を参照)。

## ユーザー定義属性

### このタスクについて

追加の属性を指定する場合は、以下のステップを実行します。FTP スクリプトが実行されると、オプションに入力した値で %BCGOPTION*x*% が置き換えられます (*x* はオプション番号に対応します)。

1. 「**新規**」をクリックします。
2. 「**オプション 1**」の横に値を入力します。
3. 追加の属性を指定する場合は、「**新規**」を再びクリックして、値を入力します。
4. 必要なだけステップ 3 を繰り返して、すべての属性を定義します。

例えば、FTP スクリプトが次のようになっているとします。

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
          cd %BCGOPTION1%
          mput *
          quit
```

この場合、%BCGOPTION% はディレクトリー名です。

## スケジュール

### このタスクについて

このページの「スケジュール」セクションから、以下のステップを実行します。

1. 間隔ベースのスケジューリングとカレンダー・ベースのスケジューリングのどちらが必要なのかを指定します。
   - 「**間隔ベースのスケジューリング**」を選択した場合は、宛先がポーリングされるまでの経過秒数を選択します (またはデフォルト値を受け入れます)。
   - 「**カレンダー・ベースのスケジューリング**」を選択した場合は、スケジューリングのタイプ (「**日次スケジュール**」、「**週次スケジュール**」、または「**カスタム・スケジュール**」) を選択します。
     - 「**日次スケジュール**」を選択した場合は、宛先がポーリングされる時刻を入力します。
     - 「**週次スケジュール**」を選択した場合は、時刻のほかに曜日を 1 つ以上選択します。
     - 「**カスタム・スケジュール**」を選択した場合は、まず時刻を選択し、次に週および月について「**範囲**」または「**選択できる日**」を選択します。「**範囲**」では、開始日と終了日を指定します。(例えば、特定の曜日にのみサーバーをポーリングする場合は、「**月**」および「**金**」をクリックします。)「**選択できる日**」では、週および月の特定の日付を選択します。
2. 宛先の前処理または後処理ステップを構成する場合は、250 ページの『ハンドラーの構成』を参照してください。それ以外の場合は、「**保管**」をクリックします。

## ハンドラーの構成

### このタスクについて

宛先の 2 つの処理ポイント (プリプロセスおよびポストプロセス) を変更できます。

前処理または後処理ステップにはデフォルトのハンドラーが用意されていないため、デフォルトでは「**使用可能リスト**」にハンドラーが 1 つもリストされません。ハンドラーを既にアップロードしている場合には、そのハンドラーを選択し、「**構成済みリスト**」に移動できます。

これらの構成ポイントにユーザーが作成したハンドラーを適用するには、まずハンドラーをアップロードする必要があります。ハンドラーのアップロードの手順については、「*E/A ハブ構成ガイド*」を参照してください。次に、以下のステップを実行します。

1. 「**構成ポイント・ハンドラー**」リストから、「**前処理**」または「**後処理**」を選択します。
2. 「**使用可能リスト**」からハンドラーを選択し、「**追加**」をクリックします。
3. ハンドラーの属性を変更する場合は、「**構成済みリスト**」からそのハンドラーを選択し、「**構成**」をクリックします。変更可能な属性のリストが表示されます。必要な変更を加え、「**値の設定 (Set Values)**」をクリックします。
4. 「**保存**」をクリックします。

「**構成済みリスト**」では、以下のようにさらに変更を加えることもできます。

- 「**構成済みリスト**」からハンドラーを選択し、「**除去**」をクリックして、ハンドラーを除去します。ハンドラーが「**使用可能リスト**」に移動します。
- ハンドラーを選択し、「**上に移動**」または「**下に移動**」をクリックして、ハンドラーが処理される順序を変更します。

## ユーザー定義トランスポートの宛先の設定

### このタスクについて

ユーザー定義のトランスポートをアップロードする場合は、以下のステップを実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**宛先**」をクリックします。
3. 「**トランスポート・タイプの管理**」をクリックします。
4. トランスポートを定義する XML ファイルの名前を入力します (または、「**参照**」を使用して、必要なファイルへ移動します)。
5. 「**データベースへコミットする**」では、デフォルトの「**はい**」を使用します。実動に移す前にこのトランスポートをテストする場合には、「**いいえ**」を選択します。
6. データベースに既に同じ名前のファイルが存在した場合、このファイルに置き換えるかどうかを指定します。
7. 「**アップロード**」をクリックします。

**注:** 「トランスポート・タイプの管理」ページから、ユーザー定義のトランスポート・タイプを削除することもできます。WebSphere Partner Gateway で提供されているトランスポートは、削除できません。また、ユーザー定義のトランスポートを使用して宛先を作成した後は、このユーザー定義のトランスポートを削除できません。

8. 「**作成**」をクリックします。
9. 宛先を識別する名前を入力します。このフィールドは必須です。
10. (オプション) 宛先の状況を指定します。デフォルトは「**有効**」です。有効状態の宛先は、文書を送信することができます。無効状態の宛先は、文書を送信できません。
11. (オプション) 宛先がオンラインかオフラインかを指定します。デフォルトは「**オンライン**」です。
12. (オプション) 宛先の説明を入力します。
13. フィールド (フィールドの内容はユーザー定義のトランスポートごとに固有) に情報を入力し、「**保存**」をクリックします。

## デフォルト宛先の指定

### このタスクについて

内部パートナーまたはパートナーの宛先を作成した後、その宛先の 1 つをデフォルト宛先として選択します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 検索条件を入力し、「**検索**」をクリックするか、または検索条件を入力せずに「**検索**」をクリックして、すべてのパートナーのリストを表示します。
3. 「**詳細の表示**」アイコンをクリックして、パートナーのプロファイルを表示します。
4. 「**宛先**」をクリックします。
5. 「**デフォルト宛先の表示**」をクリックします。

   パートナーに対して定義されている宛先のリストが表示されます。
6. 「**実動**」リストから、このパートナーのデフォルトにする宛先を選択します。デフォルト宛先は、「**テスト**」など他のタイプの宛先に対しても設定できます。
7. 「**保存**」をクリックします。

# 第 12 章 接続の管理

パートナーの B2B 機能を作成し、対話を作成したら、内部パートナーと外部パートナー間の接続を確立します。この章では以下のトピックを扱います。

- 『接続の概要』
- 『パートナー接続のアクティブ化』
- 254 ページの『属性の指定または変更』

**注:** WebSphere Partner Gateway の構成変更を行う場合は、必ず、コミュニティー・コンソールにログインしたときと同じブラウザー・インスタンスを使用してください。複数のブラウザー・インスタンスを同時に使用すると、構成変更が無効になる可能性があります。

## 接続の概要

接続は、交換される文書のタイプごとにパートナー間で設定します。例えば、パッケージ化、プロトコル、文書タイプ、アクション、またはマップが異なる場合があるため、内部パートナーから同じ 1 人のパートナーに対して複数の接続を確立することもあります。

接続をアクティブ化するときに、ソース・パートナーまたはターゲット・パートナーの属性を指定できます。接続レベルで設定した属性は、特定のパートナーの B2B 機能レベルや、文書定義レベルで設定した属性よりも優先されます。

EDI、XML、ROD の各文書を交換するときにエンベロープまたは変換が伴う場合は、それぞれの交換ごとに接続を確立します。接続に関連付けられたプロファイルのセットからプロファイルを選択して、これらの文書タイプに応じた接続を詳しく定義することができます。詳細については、201 ページの『接続プロファイル』を参照してください。

## 複数の内部パートナーの構成

WebSphere Partner Gateway では、内部パートナーの数に制限はありません。FTPScript サポート・フィーチャーに流れている Web サービスおよびバイナリー文書の後方互換性を提供するためには、デフォルト内部パートナーの構成が必要です。複数の内部パートナーに対する Web サービスおよびバイナリー文書の構成について詳しくは、文書タイプの構成に関する章を参照してください。

## パートナー接続のアクティブ化

### このタスクについて

パートナー接続には、文書タイプごとに正しい交換を行うために必要な情報が含まれています。文書をルーティングするには、内部パートナーと、いずれかの外部パートナーの間で接続が確立されていなければなりません。

システムは、内部パートナーと外部パートナーの B2B 機能および対話を基に、両者の間の接続を自動的に作成します。

これらの接続をアクティブ化するには、まず接続を検索する必要があります。

ソースとターゲットを選択する際には、ソースが固有であることを確認してください。

基本的な接続検索を実行し、接続をアクティブ化するには、以下の手順を実行します。

1. 「**アカウント管理**」>「**接続**」をクリックします。「接続の管理」ページが表示されます。
2. 「**ソース**」の下で、ソースを選択します。例えば、内部パートナーから発信される交換を設定する場合は、その内部パートナーを選択します。
3. 「**ターゲット**」の下で、ターゲットを選択します。例えば、パートナーが受信する交換を設定する場合は、そのパートナーを選択します。

   **注:** 新規接続を作成する場合は、ソースおよびターゲットは一意である必要があります。
4. 「**検索**」をクリックし、基準を満たす接続を検索します。

   **注:** より詳細な検索条件を入力する場合は、「拡張検索」ページを使用します。
5. 接続をアクティブ化するには、「**アクティブ化**」をクリックします。「接続の管理」ページが再度表示され、今度は接続が緑色で強調表示されます。このページに、ソースとターゲットのパッケージ、プロトコル、文書タイプが表示されます。また、ここに表示されるボタンをクリックすると、パートナー接続の状況やパラメーターを表示し、変更することができます。
6. ソースまたはターゲットの属性を指定したり、接続プロファイルを選択したりするには、『属性の指定または変更』を参照してください。

2 アクション PIP の場合は、双方向の接続をアクティブ化して、2 番目の PIP アクションをサポートするようにします。そのためには、2 番目のアクションのソースおよびターゲットを最初のアクションのソースおよびターゲットと反対にします。

EDI、XML、または ROD の文書に既に複数の対話を定義している場合は、それぞれの対話に関連付けられた接続をすべてアクティブ化してください。

## 属性の指定または変更

### このタスクについて

接続をアクティブ化すると、属性を設定したり、以前に定義された属性を変更したりできます。接続の属性を指定または変更するには、以下のステップを実行します。

1. 属性値を表示または変更するには、「**属性**」をクリックします。

   例えば、内部パートナーが「なし」としてパッケージ化されている文書をパートナーに送信しようとしているとします。パートナーは AS としてパッケージ化さ

れている文書を受け取ろうとしています。内部パートナーは複数のビジネス ID を文書に割り当てることができます。使用する ID を WebSphere Partner Gateway に指示するには、以下のステップを実行します。

a. 接続のソース側で「**属性**」をクリックします。

b. 「接続属性」ページが表示されたら、「**なし**」フォルダーを展開します。

c. 「**更新**」リストから、パートナーに送信する AS ID を選択します。

d. 「**保存**」をクリックします。

**注:** 以前に AS ID を指定している場合は (例えば、「B2B 機能」ページなどで)、ここで入力した値で以前の値がオーバーライドされます。

また、パートナーから AS としてパッケージ化されている文書を受け取るときには MDN アドレスの値を入力しますが、これも属性を設定する一例です。このアドレスには、MDN の配信先を指定します。

2. この接続に関連付けられたアクションまたは変換マップを表示または変更する場合は、「**アクション**」をクリックします。そのアクションまたはマップに既に値が設定してある場合は、ここで変更した値でオーバーライドされます。
3. ソースまたはターゲット宛先を表示または変更するには、「**宛先**」をクリックします。
4. 「**接続プロファイルの追加**」ボタンおよび「**アクティブ・プロファイル**」リストが表示された場合は、以前に定義した特定のプロファイルにこの接続を関連付けることができます。

接続レベルで設定した属性は、プロトコル・レベルまたは文書タイプ・レベルで設定した属性よりも優先されます。パッケージ、プロトコル、および文書タイプに属性が関連付けられている場合、文書タイプの値で、パッケージとプロトコルに設定されている値がオーバーライドされます。

# 第 13 章 文書交換のセキュリティーの使用可能化

WebSphere Partner Gateway では、インバウンド・トランザクションおよびアウトバウンド・トランザクションを保護する複数のタイプの証明書をインストールし、使用することができます。この章では以下のトピックを扱います。



WebSphere Partner Gateway において、証明書およびセキュリティー・プロトコルを使用すると、以下のようなセキュリティー上の利点があります。

- 文書を誰が送信しているかに関して確認する
- 転送中に文書が変更されていないことを確認する
- 他のユーザーが文書の内容を表示できないようにする
- 文書を送信しているユーザーが文書を送信する権限を持つことを確認する

**注:** WebSphere Partner Gateway の構成変更を行う場合は、必ず、コミュニティー・コンソールにログインしたときと同じブラウザー・インスタンスを使用してください。複数のブラウザー・インスタンスを同時に使用すると、構成変更が無効になる可能性があります。

# セキュリティーの概要

## WebSphere Partner Gateway で使用されるセキュリティーのメカニズムとプロトコル

WebSphere Partner Gateway は、ビジネス・プロトコルに応じて、証明書を使用することで以下のメカニズムを使用可能にして、文書交換のセキュリティーを維持します。

**暗号化および暗号化解除**

暗号化は、暗号化解除されるまでデータを読めないように、データを変更する方法です。WebSphere Partner Gateway は、公開鍵暗号化と呼ばれる暗号システムを使用して、パートナーとハブの間の通信を保護します。AS2 または RosettaNet などのさまざまなビジネス・プロトコルに、暗号化の要件があります。また、SSL も暗号化を使用します。この章では、特に断りがある場合を除き、*暗号化* という用語の使用は、ビジネス・プロトコルに適用されます。

暗号化解除は、暗号化されたデータを復号してデータを読み取り可能にする方法です。暗号化解除は、インバウンド文書に対して実行されます。

**デジタル署名およびデジタル署名の検証**

デジタル署名は、誰が文書を送信したか、および転送中に文書が変更されていないことを確認するためのメカニズムです。これは、否認防止の保証にも役立ちます。否認防止とは、パートナーがメッセージを生成して送信したことを否認できないことを意味します。また、パートナーはメッセージを受信したことも否認できません。

**注:** 否認防止情報がパートナー接続パラメーターから取得されます。パートナー接続パラメーターは、パートナー接続検索が正常に行われた後に取得されます。デフォルトでは、否認防止は「はい」に設定されています。この設定では、なんらかの理由で情報がパートナー接続から提供されない場合、文書は否認防止ストアに格納されます。

**SSL** SSL は、インターネットのセキュリティーを管理するためによく利用されるプロトコルです。 SSL は、ネットワーク接続を介してリンクされている 2 つのアプリケーションがそれぞれ信頼できることを確認できるようにし、データを暗号化して機密性を保証することで、セキュア接続を提供します。暗号化は、データ型に依存しません。SSL は、HTTP や FTP などのトランスポート上で使用されます。

**基本認証**

着信メッセージが HTTP または HTTPS で送信された場合、受信側は基本認証の資格情報によって送信側のパートナーを認証することができます。ユーザー ID とパスワードは HTTP ヘッダーで渡されます。パスワードも送信する場合は、SSL/TLS に基本認証を使用して必ずヘッダーを暗号化します。認証は、Base64 エンコード形式で Bussiness ID/username:password または Username:password のいずれかを使用して提供されます。HTTP ヘッダーの値は、「**基本認証の使用可能化 (Enable basic authentication)**」が true に設定されている場合にのみ考慮されます。コンソールの「レシーバーの詳細」ページで「基本認証」を選択して、「真」に設定します。

認証が失敗すると、認証失敗応答が送信側に戻されます。そうでない場合、文書はさらなる処理のために送信されます。 SSL クライアント認証の場合、送信側パートナーのビジネス ID が識別されます。受信側は文書を受信すると、証明書がいずれかのパートナーと関連付けられているか確認します。一致するパートナーがいない場合、文書は失敗します。後方互換性のために、基本認証により SOAP メッセージを送信しているときには、受信側で「**基本認証の使用可能化 (Enable Basic Authentication)**」フラグを「No」に設定します。文書は、受信側で文書の認証が失敗した場合を除き、文書ビューアーで表示することができます。基本認証は、次の文書に対してサポートされています。

- EDI/XML 文書
- バイナリー/EDI/XML ペイロードの AS2 文書
- Web サービス要求
- Rosettanet メッセージ
- ebMS メッセージ

セキュリティーは、トランスポートまたはビジネス・プロトコルのいずれかで実現できます。受信側でのユーザーの認証では、HTTP での外部パートナーからのバイナリー文書がサポートされています。送信側パートナーは、基本認証の資格情報または SSL クライアント認証の資格情報のいずれかを使用して識別されます。

## 証明書およびセキュリティー・メカニズム

証明書は、暗号化、デジタル署名、および SSL という、セキュリティーに対する 3 つのアプローチのすべての基礎となります。証明書によって、WebSphere Partner Gateway でこれらのアプローチを使用できます。証明書を使用すると、伝送中に文書のセキュリティーを保つことができます。

各パートナーは、WebSphere Partner Gateway と文書の送受信を行うための 1 つ以上の証明書を持ち、ハブ・オペレーターで表される WebSphere Partner Gateway は、パートナーと文書の送受信を行うための 1 つ以上の証明書を持っています。

**注:** パートナーまたはハブ・オペレーターに使用される同一の証明書が、すべての文書に適用されます。証明書は、文書タイプによって変わることはありません。

### 証明書および暗号化

証明書には、数学的に関連した公開鍵と秘密鍵ペアの公開鍵の部分が含まれています。公開鍵は、文書が送信される前に文書を「ロック」すなわち暗号化します。文書の送信後に、秘密鍵のみが文書を「アンロック」すなわち暗号化解除できるようになっています。公開鍵は、暗号化された文書を送信するパートナーと共有するため、公開鍵と呼ばれます。一方、秘密鍵は、自分が文書を暗号化解除できるように、他人に教えないようにします。証明書には公開鍵が格納されており、公開鍵をサブジェクト名 (証明書の所有者であるエンド・エンティティーの名前) にバインドします。

証明書はパートナーが生成し、パートナーによって自己署名されるか、または CA で発行されます。CA 発行の証明書は、パートナーが証明書署名要求 (CSR) を使用して要求し、認証局 (CA) から受け取った証明書です。CA 発行の証明書は、パー

トナーではなく CA によって署名されます。各パートナーは、文書の送受信で使用する証明書を、少なくとも 1 つ持っています。

ビジネス文書暗号化は、ビジネス標準が暗号化をサポートする場合のみ適用されます。すべての標準が暗号化をサポートするわけではありません。暗号化をサポートする標準では、各標準の暗号化の適用方法は異なっています。WebSphere Partner Gateway は、標準ごとの差異と、暗号化の適用方法を理解しています。

WebSphere Partner Gateway がパートナーに文書を送信する場合、そのパートナーの証明書を使用して、文書が暗号化されます。このようにすると、パートナーは、自分の秘密鍵を使用して文書を暗号化解除し、内容を読み取ることができます。使用される証明書は、WebSphere Partner Gateway にロードされてそのパートナーの暗号化証明書になります。

パートナーが WebSphere Partner Gateway に文書を送信する場合、そのパートナーはハブ・オペレーターの証明書を使用して文書を暗号化します。このようにすると、秘密鍵を持つハブ・オペレーターのみが、文書を暗号化解除して、内容を読み取ることができます。使用される秘密鍵は、「PKCS12 のロード」オプションでハブ・オペレーター用にロードされたものです。ハブ・オペレーターの証明書は、管理者がパートナーに渡す必要があります。

**注:**

1. WebSphere Partner Gateway では、RC2 および TripleDES アルゴリズムがサポートされています。RC5 アルゴリズムはサポートされません。以前のリリースで RC5 アルゴリズムを使用していた場合は、サポートされているアルゴリズムに切り替えてください。
2. WebSphere Partner Gateway では、以下のアルゴリズムもサポートされます。
   - AES、TripleDES、および RC2: 送信および受信済み ebMS 文書に対して。
   - TripleDES および RC2: RNIF 文書に対して。
   - DES: ebMS に対して。ただし、RC2、TripleDES、または AES など、より強力なアルゴリズムの使用が推奨されます

   これらのアルゴリズムは、WebSphere Partner Gateway コンソールの「システム管理」>「DocMgr 管理」>「セキュリティー」ビューで設定するか、またはユーザー出口内のセキュリティー・サービス API を使用して設定できます。セキュリティー・プロパティーの詳細については、「*WebSphere Partner Gateway 管理ガイド*」を参照してください。SecurityService については、「*WebSphere Partner Gateway Programmer Guide*」を参照してください。

### 基本的手順

暗号化された文書を受け取るには、以下の基本的な手順を実行する必要があります。完全な手順については、269 ページの『証明書を使用した暗号化および暗号化解除の使用可能化』を参照してください。

1. 公開鍵/秘密鍵ペアを取得します。自分で生成するか、または CA から鍵ペアを受け取ります。

2. 秘密鍵を WebSphere Partner Gateway サーバーのハブ・オペレーター (すべての内部パートナーが鍵を使用できる) または内部パートナー (特定の内部パートナーのみが鍵を使用できる) の下にアップロードして、サーバーが着信文書を暗号化解除できるようにします。
3. 公開証明書を取引先に提供することにより、そのパートナーが証明書を自分のサーバーにアップロードできるようにして、文書をこちらに送信する前に暗号化できるようにします。

この手順を実行すると、このパートナーは、証明書を使用して、こちらだけが暗号化解除できるように暗号化した文書を送信できるようになります。パートナーに暗号化された文書を送信するには、この手順を逆にして、パートナーの証明書をアップロードし、それらの証明書を使用してパートナーに送信する文書を暗号化します。

## 証明書およびデジタル署名

WebSphere Partner Gateway は、B2B プロトコルに必要な場合、デジタル署名をサポートしています。証明書は署名を行うために使用します。これは暗号化証明書を使用する場合と似ています (ただし、方向は逆になります)。デジタル署名された文書をパートナーに送信するための証明書を作成する必要はありますが、その逆は必要ありません。

デジタル署名は、文書の実際の送信者を確認するため、および文書が転送中に変更されていないことを証明するために使用します。ビジネス標準がデジタル署名をサポートする場合のみ適用されます。すべての標準がデジタル署名をサポートするわけではありません。デジタル署名をサポートする標準では、各標準のデジタル署名の適用方法は異なっています。WebSphere Partner Gateway は、標準間の差異と、デジタル署名の適用方法を理解しています。

WebSphere Partner Gateway がパートナーに文書を送信する場合、「PKCS12 のロード」オプションでロードされたハブ・オペレーターの秘密鍵を使用して、文書に署名します。パートナーは、ハブ・オペレーター証明書を使用して、WebSphere Partner Gateway が文書に署名したことを確認します。文書の署名にハブ・オペレーターの秘密鍵を使用しなかった場合、パートナーが持っているハブ・オペレーター証明書は、署名を検証する機能を果たしません。ハブ・オペレーターの証明書は、管理者がパートナーに渡す必要があります。

パートナーが WebSphere Partner Gateway に文書を送信する場合、WebSphere Partner Gateway は、パートナーのデジタル署名証明書を使用して、文書に署名したのがパートナーであることを確認します。文書の署名にパートナーの秘密鍵を使用しなかった場合、WebSphere Partner Gateway が持っているそのパートナーの証明書は、署名を検証する機能を果たしません。

### 基本的な手順:

デジタル署名した文書を送信するには、以下の基本的な手順を実行する必要があります。完全な手順については、275 ページの『証明書を使用したデジタル署名の使用可能化』を参照してください。

1. 公開鍵/秘密鍵ペアを取得します。自分で生成するか、または CA から鍵ペアを受け取ります。

2. ハブ・オペレーターの下の自分の WebSphere Partner Gateway サーバーに秘密鍵をアップロードして、送信される文書にサーバーが署名できるようにします。
3. 公開証明書を取引先に提供することにより、そのパートナーが証明書を自分のサーバーにアップロードでき、こちらから受信した文書を検証できるようにします。

この手順を完了すると、秘密鍵を使用して、デジタル署名された文書を送信することができ、これにより文書を送信したのが他の誰でもないことをパートナーが認識できます。同様に署名された文書をパートナーから受信するには、この手順を逆にして、パートナーの証明書をアップロードし、それらを使用して文書の発信元を確認する必要があります。

## 証明書および SSL/TLS

文書の送信時に、SSL を使用して、受信者のみが文書を読み取ることができる (そのためデータの機密性が保証される) ように文書を暗号化することができます。

SSL では、クライアント およびサーバー の概念があります。クライアントは、サーバーに文書を送信するためにサーバーに接続します。クライアントがサーバーに接続すると、サーバーは、文書の暗号化に使用する証明書をクライアントへ送信します。このサーバー証明書は、サーバー認証の一部でもあります。サーバーは、その証明書を使用して、クライアントに対してサーバー自体を認証します。サーバーがクライアントからの証明書を要求する場合もあります。これはクライアント認証と呼ばれ、サーバーにとってクライアントが既知であることを確認するためにサーバーが使用します。

WebSphere Partner Gateway がパートナーに文書を送信しているときは、WebSphere Partner Gateway はクライアントであり、パートナーはサーバーです (すなわち、文書はパートナーのサーバーに送信されています)。

**注:** パートナーのサーバーは、このパートナー用に WebSphere Partner Gateway で定義された宛先です。

パートナーが WebSphere Partner Gateway に文書を送信しているときは、パートナーがクライアント、WebSphere Partner Gateway がサーバーです。

**注:** これは、WebSphere Partner Gateway で定義されているレシーバーです。

パートナーが SSL を使用して WebSphere Partner Gateway に文書を送信しているときは、パートナーの実際の身元 (ID) はわかりません。クライアント認証が使用されている場合でも、パートナーの ID は分かりません。ただし、このパートナーが WebSphere Partner Gateway への文書の送信元として信頼できることはわかります。WebSphere Partner Gateway には、パートナーが提供したクライアント認証証明書からパートナーを識別する追加機能もあります。

WebSphere Partner Gateway がパートナーに文書を送信している場合、そのパートナーの証明書を使用して、文書が暗号化されます。そのため、そのパートナーのみが、自分の秘密鍵を使用して文書を暗号化解除し、内容を読み取ることができます。実行時の SSL の一部として、パートナーは、暗号化に使用する証明書を WebSphere Partner Gateway に動的に送信します。WebSphere Partner Gateway は、

ハブ・オペレーターの下のルート/中間証明書としてロードされた証明書を使用して認証パスの構築と検証を行うことによって、その証明書が有効であることを確認します。

SSL には、送信側を検証するためのクライアント認証という 2 つ目のオプション部分があります。ここでパートナーが WebSphere Partner Gateway から証明書を要求します。WebSphere Partner Gateway は、ハブ・オペレーターの下にロードされたクライアント認証証明書を送信します。クライアント認証に使用するハブ・オペレーターの証明書は、管理者がパートナーに渡す必要があります。クライアント認証証明書が自己署名証明書である場合は、自己署名証明書をパートナーに渡す必要があります。クライアント認証証明書が CA 証明書であり、パートナーがその CA 証明書をまだ持っていない場合は、パートナーに CA 証明書を渡す必要があります。

パートナー が SSL を使用して WebSphere Partner Gateway に文書を送信している場合、WebSphere Partner Gateway 証明書を使用して文書が暗号化されます。そのため、WebSphere Partner Gateway のみが、自分の秘密鍵を使用して文書を暗号化解除し、内容を読み取ることができます。実行時の SSL の一部として、WebSphere Partner Gateway は、暗号化に使用する証明書をパートナーに動的に送信します。パートナーは、管理者が以前パートナーに渡した証明書と比較することによって、証明書が有効であることを確認します。SSL には、送信側を検証するためのクライアント認証という 2 つ目のオプション部分があります。ここで WebSphere Partner Gateway がパートナーから証明書を要求します。パートナーが WebSphere Partner Gateway にクライアント認証証明書を送信し、この証明書はパートナーが以前管理者に渡した証明書と照合されます。

**注:** SSL を使用してパートナーから文書を受信するため、WebSphere Partner Gateway は、下層の WebSphere Application Server 機能を使用します。そのため、実行時に使用される証明書は、WebSphere Partner Gateway コンソールを使用してアップロードされるのではなく、WebSphere Application Server 鍵ストアおよびトラストストアにロードされます。

クライアント認証を使用する場合、WebSphere Partner Gateway は、SSL トランスポートの外部で追加のパートナー識別を実行します。パートナーから提供されたクライアント認証証明書が WebSphere Partner Gateway に渡されると、WebSphere Partner Gateway はこれを、そのパートナーの SSL クライアント用にロードされた証明書と比較して、パートナーの身元を識別しようとします。

クライアントが HTTP ベースの SSL 接続を開始する場合は必ず、http:// ではなく https:// で始まる URL が使用されます。SSL 接続はハンドシェークによって開始されます。このステージでアプリケーションは、証明書を交換し、使用する暗号化アルゴリズムに同意して、残りのセッションで使用される暗号鍵を生成します。

### 基本的な手順

SSL を使用した文書を*送信* するには、以下の基本的な手順を実行する必要があります。完全な手順については、280 ページの『証明書を使用した SSL の使用可能化』を参照してください。

1. パートナーから証明書を取得して、WebSphere Application Server トラストストアにロードします。

2. パートナーへのクライアント認証用の公開鍵/秘密鍵ペアを取得します。自分で生成するか、または CA から鍵ペアを受け取ります。
3. 自分の WebSphere Application Server 鍵ストアに秘密鍵と公開証明書をアップロードします。
4. 公開証明書を取引パートナーに提供することにより、そのパートナーが証明書を自分のサーバーにアップロードできるようにして、SSL ランタイム通信中にクライアント認証証明書をこちらから受け取ったことを確認できるようにします。

SSL を使用した文書を*受信* するには、以下の基本的な手順を実行する必要があります。完全な手順については、280 ページの『証明書を使用した SSL の使用可能化』を参照してください。

1. 公開鍵/秘密鍵ペアを取得します。自分で生成するか、または CA から鍵ペアを受け取ります。
2. 自分の WebSphere Application Server 鍵ストアに秘密鍵と公開証明書をアップロードします。
3. 公開証明書を取引パートナーに提供することにより、そのパートナーが証明書を自分のサーバーにアップロードできるようにして、SSL ランタイム通信中にサーバー証明書をこちらから受け取ったことを確認できるようにします。
4. クライアント認証用にパートナーから証明書を取得して、WebSphere Application Server トラストストアにロードします。これは、SSL ランタイム通信中に使用されます。
5. WebSphere Partner Gateway コンソールでクライアント認証証明書からパートナーを識別するためには、パートナーのクライアント認証にパートナーの証明書をアップロードします。

## 鍵ストアとトラストストアでの証明書の保管

WebSphere Partner Gateway では、証明書を保管する方法は 2 つあります。 SSL を使用してパートナーから WebSphere Partner Gateway に送信される文書の場合、証明書は WebSphere Application Server 鍵ストアおよびトラストストアに保管されます。トラストストアは、信頼できる証明書を保管するために使用します。その証明書は、パートナーから受け取った証明書が有効であることを確認するために使用されます。鍵ストアは、WebSphere Partner Gateway ハブ・オペレーターの公開鍵および秘密鍵を保管するために使用します。ビジネス文書のセキュリティーのために使用される証明書は、WebSphere Partner Gateway コンソールを通じてロードすることによって保管されます。このセクションでは、WebSphere Application Server と共に使用される鍵ストアおよびトラストストアについて説明します。WebSphere Partner Gateway をインストールすると、レシーバーとコンソールがインストールされている WebSphere Application Server 用に、鍵ストアとトラストストアが作成されます。

- 鍵ストア: 公開鍵と秘密鍵が含まれているファイル。
- トラストストア: パートナーの自己署名証明書および CA 証明書の公開鍵が含まれている鍵データベース・ファイル。公開鍵は、署名者証明書として保管されます。商業用の CA の場合は、CA ルート証明書が追加されています。トラストストア・ファイルは秘密鍵を含まないため、トラストストア・ファイルは鍵ストア・ファイルよりも公にアクセス可能です。

- iKeyman を使用して、鍵ストアおよびトラストストアが管理されます。このユーティリティーについては、これを使用する必要のあるセクションで説明しています。

  **注:** WebSphere Application Server 管理コンソールを使用して、レシーバーおよびコンソールの証明書、鍵ストア、およびトラストストアを管理することもできます。WebSphere Application Server 管理コンソールを使用して証明書および鍵ストアを管理する方法について詳しくは、WebSphere Application Server Information Center の『アプリケーションとその環境の保護』を参照してください。

デフォルトでは、鍵ストアおよびトラストストアは、*<ProductDir>*/common/security/keystore ディレクトリーに作成されます。名前は、以下のとおりです。

- bcgSecurity.jks
- bcgSecurityTrust.jks

### デフォルトのパスワードの変更

上記のストアにアクセスするためのデフォルトのパスワードは WebAS です。WebSphere Application Server は、これらのストアを使用するように構成されています。iKeyman ユーティリティーを使用してパスワードを変更できます。keytool コマンドを使用して、鍵ストア・ファイルのパスワードを変更することもできます。UNIX の場合は、次のようなコマンドを使用します。

```
/<WAS_Installation_Dir>/java/bin/keytool
 -storepasswd -new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$
 -storepass $CURRENT_PASSWORD$ -storetype JKS
```

Windows の場合、前述のコマンドを使用しますが、スラッシュの代わりに円記号を使用し、ドライブ名を指定します。

鍵ストア・パスワードを変更する場合は、各 WebSphere Application Server インスタンスの構成も変更する必要があります。この場合、bcgChgPassword.jacl スクリプトを使用します。コンソール・インスタンスにおいて、以下のディレクトリーに移動します。

```
/<ProductDir>/bin
```

次に、以下のコマンドを発行します。

```
./bcgwsadmin.sh -f /<ProductDir>/scripts/
bcgChgPassword.jacl -conntype NONE
```

レシーバーおよび文書マネージャーの WebSphere Application Server インスタンスに対して、このコマンドを繰り返します。

**注:** Windows インストールの場合は、./bcgwsadmin.sh の代わりに bcgwsadmin.bat を使用します。

新規パスワードを求めるプロンプトが出されます。

### 期限切れ証明書の置換

トラストストアの証明書の有効期限が切れている場合は、以下の手順に従って、新規証明書を追加し、証明書を置き換える必要があります。

1. IKEYMAN が実行されていない場合は、開始します。

2. トラストストア・ファイルを開きます。
3. パスワードを入力し、「**OK**」をクリックします。
4. メニューから、「**署名者証明書**」を選択します。
5. 「**追加**」をクリックします。
6. 「**データ・タイプ**」をクリックし、Base64 でエンコードされた ASCII データなどのデータ・タイプを選択します。

   このデータ・タイプは、インポートする証明書のデータ・タイプと一致している必要があります。
7. 証明書ファイルの名前および CA ルート・デジタル証明書の場所を入力するか、または「**参照**」をクリックして、名前と場所を選択します。
8. 「**OK**」をクリックします。
9. インポートする証明書のラベルを入力します。
10. 「**OK**」をクリックします。

## 証明書チェーンの使用

証明書チェーンは、パートナーの証明書およびその証明書の認証に使用された証明書で構成されています。例えば、ある CA を使用してパートナーの証明書を作成した場合、その CA 自体も既に別の CA によって認証されていることがあります。トラストのチェーンは、*ルート* CA (トラスト・アンカー) から始まります。ルート CA のデジタル証明書は自己署名です。つまり、認証局が自身の秘密鍵を使用してデジタル証明書に署名します。トラスト・アンカーとパートナーの証明書 (ターゲット証明書) の間にある証明書が、*中間*証明書です。

CA で発行された証明書には必ず、チェーン内のすべての証明書を追加する必要があります。例えば、A (トラスト・アンカー) が B の発行者で、B が C (ターゲット証明書) の発行者となっている証明書チェーンの場合、証明書 A および B は CA 証明書としてアップロードする必要があります。

WebSphere Partner Gateway では、すべての自己署名証明書がトラスト・アンカーとして扱われます。自己署名証明書は、認証局 (CA) のものであることもあれば、パートナーが生成した自己署名証明書であることもあります。

インバウンド SSL の場合、すべてのルート (トラスト・アンカー) 証明書および中間証明書は、前述のように WebSphere Application Server トラストストアに保持されます。すべてのパートナーの証明書について、ルート (トラスト・アンカー) 証明書および中間証明書は、ハブ・オペレーターの下にアップロードされます。

## 1 次および 2 次証明書の使用

特定のタイプの証明書を複数作成し、そのうちの 1 つを 1 次証明書として、また別の 1 つを 2 次証明書として指定することができます。1 次証明書の有効期限が切れた場合や、他の理由で 1 次証明書を使用できない場合は、WebSphere Partner Gateway によって 2 次証明書に切り替えられます。

**注:** この機能を使用すると、サーバーを停止せずに、古い証明書から新しい証明書に移行できます。
どの証明書が 1 次で、どの証明書が 2 次かは、コミュニティー・コンソールで指定します。

1 次証明書と 2 次証明書という機能は、以下の証明書に用意されています。

- パートナーの暗号化証明書
- ハブ・オペレーターの署名証明書
- ハブ・オペレーターの SSL クライアント証明書

## 暗号の強度の変更

WebSphere Partner Gateway に同梱されている Java ランタイム環境 (JRE) では、使用可能な暗号アルゴリズムおよび最大暗号強度が制限されています。例えば、許容される長さを制限ポリシーで規定して、結果として暗号鍵の強度を制限します。こうした制限は、*管轄権ポリシー・ファイル* というファイルで指定します。最大許容長は 2048 バイトです。

2048 バイトを超える鍵サイズの証明書をサポートする場合には、強度に制約や制限のない管轄権ポリシー・ファイルを使用してください。JRE のインストール先のサブディレクトリーに新しいポリシー・ファイルをインストールすれば、強度が高く制約のないポリシーを使用できるようになります。

3DES など、対称鍵アルゴリズムに対する暗号化制限もあります。強度が高い対称鍵アルゴリズムが必要な場合は、管轄権ポリシー・ファイルを置換すると、対称鍵の制限も除去されます。例えば、AES アルゴリズムを使用する場合は、無制限の暗号化ポリシー・ファイルが必要です。詳細については、http://www.ibm.com/developerworks/java/jdk/security/50のリンクを参照してください。

ただし、インポート制御の制限により、Java 5 Development Kit 用 IBM SDK に同梱されている権限ポリシー・ファイルでは、**強力**だが制限された暗号化の使用が許可されます。以下の表は、この**強力**な権限ポリシー・ファイルのバージョンよって許可される最大鍵サイズを提供します。

*表 29. 強力な権限ポリシー・ファイルで使用されるアルゴリズムの最大鍵サイズ*

| アルゴリズム | 最大キー・サイズ |
|---|---|
| DES | 64 |
| DESede | 112 (実効) または 168 (実効) |
| RC2 | 128 |
| RSA | 2048 |
| * (他のすべて) | 128 |

**注:** 以下のパラメーターを持つルーティングされた ebMS メッセージを暗号化するときに、「暗号化の失敗 XMLEncryptionException」例外が発生します。

- 暗号化アルゴリズム :aes-192-cbc または aes-256-cbc
- 暗号化プロトコル : Xml 暗号化

この問題を解決するには、無制限の暗号化ポリシー・ファイルをインストールします。ただし、法的に許可されている場合に限られます。

### Windows、Linux、および AIX オペレーティング・システムへのインストール手順

制限のない管轄権ポリシー・ファイルを WebSphere Partner Gateway にインストールする場合は、次のステップを実行します。

1. Web サイト http://www.ibm.com/developerworks/java/jdk/security/50/ の「**IBM SDK Policy files**」リンクから制限のない管轄権強度ポリシー・ファイルをダウンロードします。
2. ダウンロードしたファイルを一時フォルダーに unzip します。
3. 一時フォルダーから local_policy.jar および US_export_policy.jar をコピーします。
4. 構成する WebSphere Application Server のインスタンスによってホストされているすべてのサーバーを停止します。
5. <*WASInstallationDir*>¥java¥jre¥lib¥security フォルダーに移動します。
6. 既存の local_policy.jar および US_export_policy.jar を local_policy.jar.bak および US_export_policy.jar.bak に名前変更します。
7. ステップ 3 でコピーした JAR ファイルを <*WASInstallationDir*>¥was¥java¥jre¥lib¥security フォルダーに貼り付けます。
8. 再構成した WebSphere Application Server のインスタンスによってホストされているすべてのサーバーを再始動します。

これらのステップは、WebSphere Partner Gateway アプリケーションをインストールするすべての WebSphere Application Server インストール済み環境に適用されます。

### HP-UX および Solaris オペレーティング・システムへのインストール手順

HP-UX および Solaris プラットフォームの場合は、次の手順を使用します。

1. Web サイト http://www.ibm.com/developerworks/java/jdk/security/50/ の「**IBM SDK Policy files**」リンクから制限のない管轄権強度ポリシー・ファイルをダウンロードします。
2. ダウンロードしたファイルを一時フォルダーに unzip します。
3. 構成する WebSphere Application Server のインスタンスによってホストされているすべてのサーバーを停止します。
4. <*WASInstallationDir*>¥java¥jre¥lib¥security フォルダーに移動します。
5. 既存の local_policy.jar および US_export_policy.jar を local_policy.jar.bak および US_export_policy.jar.bak に名前変更します。
6. local_policy.jar および US_export_policy.jar を一時フォルダーから <*WASInstallationDir*>¥java¥jre¥lib¥security フォルダーにコピーします。
7. 再構成した WebSphere Application Server のインスタンスによってホストされているすべてのサーバーを再始動します。

これらのステップは、WebSphere Partner Gateway アプリケーションをインストールするすべての WebSphere Application Server インストール済み環境に適用されます。

### クライアント認証による SSL の構成

クライアント認証による SSL を指定したトランスポート・プロトコルを使用して文書を送信する場合は、使用する JSSE プロバイダーに関して追加の変更を行う必要があります。詳しくは、「*WebSphere Partner Gateway E/A 管理ガイド*」の『第 15 章トラブルシューティング』の『証明書を受信していないために SSL ハンドシェークが失敗する』を参照してください。

### 証明書の有効期限

有効期限が切れたときに無効になるのは、暗号化、デジタル署名、および SSL に使用される証明書だけです。これらの証明書は、エンド・エンティティー証明書であり、CA 証明書ではありません。CA 証明書は、有効期限が切れても無効になりません。

サーバーが再始動されてから次に再始動されるまでの間にルートまたは中間の証明書の有効期限が切れた場合、それらの証明書は信頼できる証明書のリストから除外されます。したがって、CA 証明書が見つからなかったことが原因で認証パスを構築できなかった場合、CA 証明書の有効期限が切れている可能性があります。実行時にルートまたは中間の証明書の有効期限が切れた場合、認証パスの構築は失敗し、対応するエンド・エンティティー証明書はビジネス・トランザクションで使用されません。証明書の有効期間および状況を確認するには、WebSphere Partner Gateway コンソールの「証明書リスト」ビューを使用します。このビューでは、有効期限が切れた証明書の有効期日が赤で表示されます。

CA 証明書の有効期限が切れた場合は、発行元の CA から新しい証明書を取得できます。WebSphere Partner Gateway コンソールを使用して、新しい CA 証明書をアップロードしてください。証明書のアップロード方法については、『証明書を使用した暗号化および暗号化解除の使用可能化』、 275 ページの『証明書を使用したデジタル署名の使用可能化』、および 280 ページの『証明書を使用した SSL の使用可能化』を参照してください。

## 証明書を使用した暗号化および暗号化解除の使用可能化

ここでは、暗号化および暗号化解除証明書について説明します。

### インバウンドの暗号化解除証明書の作成とインストール

この証明書は、ハブがパートナーから受信した暗号化ファイルの暗号化を解除するときに使用されます。ハブでは、秘密鍵を使用して、文書の暗号化を解除します。暗号化によって、送信者と目的の受信者以外は、転送中の文書を参照することができません。

暗号化された AS2 メッセージをパートナーから受信するときには、次の重要な制限に注意してください。パートナーが暗号化された AS2 メッセージを送信するときに間違った証明書を使用した場合は、暗号化解除が失敗します。ただし、失敗を示す MDN がパートナーに返されません。こうした状態のときにパートナーが MDN を受信できるようにするには、以下の文書定義でパートナーへの接続を作成します。

- パッケージ: **AS** からパッケージ: **None**
- プロトコル: **Binary** からプロトコル: **Binary**
- 文書タイプ: **Binary** から文書タイプ: **Binary**

作成される接続は、「AS から None」接続でなければなりません。つまり、一方のパートナーで AS B2B 機能をアクティブにし、もう一方のパートナーで None B2B 機能をアクティブにして接続を作成します。AS サイドのソース・ゲートウェイには必ず、MDN アドレスに対して構成されている SMTP ゲートウェイ (AS1 の場合)、HTTP ゲートウェイ (AS2 の場合)、または FTP ゲートウェイ (AS3 の場合) を指定してください。これにより、暗号化解除の失敗 MDN が、この「AS から None Binary」接続により返されます。

## ステップ 1: 証明書の取得

### このタスクについて

**自己署名証明書の生成:** 暗号化解除を使用する場合は、以下の手順を実行します。

1. IKEYMAN ユーティリティーを始動します。
2. IKEYMAN を使用して、自己署名証明書および鍵ペアを生成します。
3. IKEYMAN を使用して、ご使用の公開鍵を含む証明書をファイルに抽出します。
4. パートナーに証明書を配布します。パートナーは、このファイルを暗号化証明書として使用するために、B2B 製品にインポートする必要があります。暗号化されたファイルを内部パートナーに送信する際はこのファイルを使用するようパートナーに助言してください。CA で署名された証明書の場合は、CA 証明書も提供します。
5. iKeyman を使用して、自己署名証明書と秘密鍵のペアを PKCS12 ファイルの形式で保存します。
6. **「プロファイル」 > {Hub Operator/internal partner} > 「証明書」 > 「証明書のロード」**にナビゲートします。
7. **「この証明書が属するパートナー」**ドロップダウンから、新しくアップロードされた証明書を関連付けるパートナーを選択します。
8. **「検索」**をクリックして、特定のパートナーまたはパートナーのサブセットを検索します。
9. **「証明書のロケーション」**の横の**「参照」**をクリックして証明書をアップロードします。
10. **「次へ」**をクリックします。
11. 前の「証明書の詳細の提供 (Provide certificate details)」で、次の証明書情報を入力します。**リーフ証明書、ルート CA 証明書 (Root CA certificate)** または **中間 CA 証明書 (intermediate CA certificate)**。
12. この証明書を**「暗号化解除」**に関連付けます。
13. **「証明書の使用」**で、**「1 次」**または**「2 次」**を選択します。
14. アップロード後に証明書を有効にするか無効にするかに応じて、**「状況」**で**「有効」**または **「無効」**を選択します。
15. **「動作モード」**を選択します。
16. **「終了」**をクリックして変更を保存し、ウィザードを閉じます。

**CA が署名した証明書の使用:** CA が署名した証明書を使用する場合は、以下の手順に従います。

1. IKEYMAN ユーティリティーを始動します。

2. IKEYMAN を使用して、レシーバーの認証要求および鍵ペアを生成します。
3. CA に証明書署名要求 (CSR) をサブミットします。
4. CA から署名証明書を受信したら、IKEYMAN を使用して、この署名証明書を鍵ストアに配置します。

### ステップ 2: 証明書の配布
#### このタスクについて

すべてのパートナーに署名 CA 証明書を配布します。

## アウトバウンド暗号化証明書のインストール

アウトバウンド暗号化証明書は、ハブがパートナーに暗号化された文書を送信するときに使用されます。WebSphere Partner Gateway が、パートナーの公開鍵を使用して文書を暗号化し、パートナーが、自分の秘密鍵を使用して文書を暗号化解除します。

パートナーは、暗号化証明書を複数持つことができます。そのうちの 1 つが、デフォルトで使用される 1 次証明書になります。もう一方は 2 次証明書となり、1 次証明書の有効期限が切れた場合に使用されます。

### ステップ 1: パートナーの証明書の取得
#### このタスクについて

パートナーの暗号化証明書を取得します。証明書は X.509 DER 形式でなければなりません。WebSphere Partner Gateway でサポートされているのは、X5.09 証明書のみであることに注意してください。

### ステップ 2: パートナーの証明書のインストール
#### このタスクについて

コミュニティー・コンソール使用して、証明書をパートナーのプロファイルにインストールするには、以下の手順を実行します。

1. 「**プロファイル**」>「**外部パートナー**」>「**証明書**」>「**証明書のロード**」にナビゲートします。
2. ウィザードの「**パートナー、ファイル・ロケーション、パスワードの選択**」ページから、次の値を入力します。
   - **この証明書を所有するパートナー (Which partner does this certificate(s) belongs to)**: 新たにアップロードされた証明書を関連付けるパートナーを選択します。「検索」をクリックして、特定のパートナー、またはパートナーのサブセットを検索します。パートナーがハブ・オペレーターまたは内部パートナーの場合は、証明書のロケーション、秘密鍵のロケーション、およびパスワードを入力します。あるいはトラストストアまたは鍵ストアをパスワード付きで提供します。外部パートナーの場合は、証明書のロケーションを提供するか、証明書チェーンを含むトラストストア・ロケーションを提供します。
   - **証明書ロケーション**: 「**参照**」をクリックして、証明書 (パブリック) のロケーションを選択します。

3. 「**次へ**」をクリックして、ウィザードの「**証明書の詳細**」ページに進みます。
4. ウィザードの「**証明書の詳細**」ページで、次の証明書の詳細情報を入力します。
   - **リーフ証明書名** - リーフ証明書の名前。このフィールド名は、証明書がリーフ証明書か、ルート CA 証明書か、あるいは中間 CA 証明書かによって変化します。
   - **説明** - リーフ証明書の説明。
   - **証明書タイプ** - この証明書を暗号化と関連付けます。
   - **証明書の使用** - 証明書の使用を関連付けます。値は、「1 次」と「2 次」です。
   - **動作モード** - 操作のモードを入力します。
   - **状況** - アップロードした後に証明書を使用可能にするか使用不可にするかを基に、有効または無効を選択します。「次へ」ボタンは、証明書が使用可能になっている場合にのみ有効になります。
   - **セットの管理** - 証明書を、既存のセットまたは新規セットに関連付けることができます。証明書が 2 次証明書の場合は、既存のセットにのみ関連付けることができます。証明書は、暗号化のタイプの内部パートナー、または SSL (着信クライアント認証) あるいは署名 (検証) のタイプの外部パートナーの任意のセットに関連付けることができます。
5. 「**次へ**」をクリックして、ウィザードの「セット」ページに進みます。証明書が 1 次の場合は、セットを作成してその証明書をセットおよびパートナー接続に関連付ける必要はありません。「**新規セットの作成 (Create new set)**」チェック・ボックスを選択した場合は、ウィザードの「**新規セットの作成 (Create New Set)**」ページがオープンします。それ以外の場合は、ウィザードの「**既存のセットに追加 (Add to Existing)**」 ページがオープンします。ファイルに内部パートナーの秘密鍵が含まれている場合、または SSL / デジタル署名に使用される外部パートナーの公開証明書が含まれている場合は、「**終了**」をクリックすることができます。
6. ウィザードの「**新規セットの作成 (Create New Set)**」ページで、新規セットの詳細情報を入力します。1 次証明書の場合は、セットを作成して証明書をそのセットと関連付ける必要はありません。次の値を入力します。
   - **セット名** - セットの名前。
   - **説明** - セットの説明。
   - **状況** - 有効または無効を選択。これが無効になっている場合、「**次へ**」ボタンは有効になりません。
   - **デフォルト設定にする** - このセットをデフォルトにする場合は、このチェック・ボックスを選択します。
7. ウィザードの「**既存のセットに追加**」ページで、証明書を追加するセットを選択します。次の値を入力します。
   - **選択済み証明書タイプに使用可能なセットのリストから選択 (Select from the list of Sets available for the selected Certificate type)** - リストから、証明書に追加するセットを選択します。
   - **デフォルト設定にする** - このセットをデフォルトにする場合は、このチェック・ボックスを選択します。

8. 「**新規セットの作成 (Create New Set)**」または「**既存セットに追加 (Add to Existing Set)**」から、「**次へ**」をクリックして、ウィザードの「**デフォルト設定**」ページに進みます。「**次へ**」ボタンは、セットの状況が使用可能の場合にのみ有効になります。
9. アップロード後に証明書を使用可能にするか使用不可にするかを基に、「**状況**」で「**有効**」または 「**無効**」を選択します。

   **注:** 前のページ (「新規セットの作成 (Create new set)」または「既存のセットに追加 (Add to exisiting set)」) で「**デフォルト・セットの作成 (Make default set)**」チェック・ボックスを選択した場合は、セットを動作モードに関連付ける必要があります。これは、動作モードに対する証明書の使用を表示します。内部パートナーについては、暗号化は使用不可になります。外部パートナーについては、SSL クライアントとデジタル署名が使用不可になります。
10. 「**次へ**」をクリックして、ウィザードの「構成」ページに進みます。「**終了**」をクリックしたのに、欠落しているルートまたは中間 CA 証明書がある場合は、アップロードするように求めるプロンプトが表示されます。プロンプト・ウィンドウで「はい」をクリックすると、ウィザードの最初のページがオープンします。後の段階でアップロードしたい場合は、「**キャンセル**」をクリックしてください。
11. ウィザードの「構成」ページで、次の値を入力します。

    **注:** 「構成」ページには、動作モードに対する証明書 (セット) の使用法のリストが表示されます。すべてに対して現在のセット名が定義済みですが、それらの名前はリセットすることができます。
    - **パートナーから (From Partner)** - このフィールドには、内部パートナーの値が定義済みです。
    - **パートナーへ (To Partner)** - このドロップダウンには、すべての外部パートナーのリストが定義済みです。「すべて (All)」の値を選択して、すべての外部パートナーを組み込むこともできます。
    - **パッケージから (From Package)** - ドロップダウンから、内部パートナーの文書フロー定義オブジェクトのパッケージを選択します。
    - **パッケージへ (To Package)** - リストから、外部パートナーの文書フロー定義のパッケージを選択します。
12. セットを他のパートナー接続に関連付けたい場合は、「**接続の追加を続行 (Add more connections)**」をクリックします。
13. 「**2 次証明書の追加 (Add Secondary Certificate)**」をクリックして、現行セットに 2 次証明書を追加します。
14. 「**終了**」をクリックして、証明書をアップロードします。欠落しているルートまたは中間 CA 証明書がある場合は、アップロードするように求めるプロンプトが表示されます。プロンプト・ウィンドウで「はい」をクリックすると、ウィザードの最初のページがオープンします。後の段階でアップロードしたい場合は、プロンプト・ウィンドウで「**キャンセル**」をクリックします。

パートナーが 2 つ目の暗号化証明書を持っている場合には、このステップを繰り返します。

## ステップ 3: CA 発行の証明書のインストール
### このタスクについて

証明書が既に CA で署名されているにもかかわらず、CA ルート証明書や証明書チェーンに所属するその他の証明書がまだハブ・オペレーター・プロファイルにインストールされていない場合は、ここで以下の手順を実行して、それらの証明書をインストールします。

**注:** CA 発行の証明書が既にインストールされている場合は、このステップを実行する必要がありません。

1. 「**プロファイル**」> **<Hub Operator> ユーザー>** 「**証明書**」 > 「**証明書のロード**」にナビゲートします。
2. 「**この証明書が属するパートナー**」ドロップダウンから、新しくアップロードされた証明書を関連付けるパートナーを選択します。
3. 「**検索**」をクリックして、特定のパートナーまたはパートナーのサブセットを検索します。
4. 「**トラストストア (または) 鍵ストアのロケーション**」の横の「**参照**」をクリックします。
5. 証明書とトラストストア両方とも、**パスワード**を入力します。
6. トラストストアの場合、「**鍵ストア・タイプ (Keystore type)**」を入力し、「**次へ**」をクリックします。
7. ウィザードの「**アップロードするエンド・エンティティー証明書の選択 (Select end entity certificate to upload)**」ページで、ロードする証明書を選択します。

   **注:** 複数の証明書があるトラストストアを使用して証明書をロードすると、「**アップロードするルートおよび中間 CA 証明書のリストを選択 (Select the list of root and intermediate CA Certificates to be uploaded)**」に、すべての証明書が事前に入力されています。複数の証明書をアップロードすることもできます。
8. 「**終了**」をクリックします。

## ステップ 4: 暗号化の使用可能化
### このタスクについて

パッケージ (最も高いレベル)、パートナー、または接続レベル (最も低いレベル) で暗号化を使用可能にします。この設定により、接続レベルの他の設定をオーバーライドできます。必要な属性が欠落している場合は、接続の要約によって通知されます。

例えば、パートナー接続の属性を変更するには、「**アカウント管理**」> 「**接続**」> 「**パートナー接続**」 をクリックし、パートナーを選択します。「**属性**」をクリックし、属性を編集します (「**AS 暗号化**」など)。

エラー・メッセージ「有効な暗号化証明書が見つかりません」が表示された場合は、1 次証明書も 2 次証明書も有効ではありません。証明書は、有効期限が切れているか、失効している可能性があります。証明書の有効期限が切れている場合や失効している場合は、イベント・ビューアーに、対応するイベント (「証明書が失効

しているか有効期限が切れています (Certificate revoked or expired)」) も表示されます。これら 2 つのイベントは、その他のイベントによって分離される場合があります。

イベント・ビューアーを表示するには、以下を実行します。

1. 「**ビューアー**」>「**イベント・ビューアー**」をクリックします。
2. 該当する検索条件を選択してください。
3. 「**検索**」をクリックします。

イベント・ビューアーの使用法については、「*WebSphere Partner Gateway E/A 管理ガイド*」を参照してください。

# 証明書を使用したデジタル署名の使用可能化

## アウトバウンドのシグニチャー証明書の作成

文書マネージャーは、パートナーにアウトバウンド署名文書を送信するときにこの証明書を使用します。すべてのポートおよびプロトコルに対して同じ証明書および鍵が使用されます。

デジタル署名証明書は、複数持つことができます。そのうちの 1 つが、デフォルトで使用される 1 次証明書になります。もう一方は 2 次証明書となり、1 次証明書の有効期限が切れた場合に使用されます。

### 自己署名証明書の生成

#### このタスクについて

自己署名証明書を使用する場合は、以下の手順を実行します。

1. IKEYMAN ユーティリティーを始動します。
2. IKEYMAN を使用して、自己署名証明書および鍵ペアを生成します。
3. IKEYMAN を使用して、ご使用の公開鍵を含む証明書をファイルに抽出します。
4. パートナーに証明書を配布します。配布方法としては、証明書をパスワードで保護された ZIP ファイルにして、E メールで送信することをお勧めします。パートナーは、管理者に連絡して、ZIP ファイルのパスワードを要求する必要があります。
5. IKEYMAN を使用して、自己署名証明書と秘密鍵のペアを PKCS12 ファイルの形式でエクスポートします。

### アウトバウンド自己署名証明書のインストール

#### このタスクについて

1. 「**プロファイル**」> {**ハブ・オペレーター/内部パートナー**} >「**証明書**」>「**証明書のロード**」にナビゲートします。
2. ウィザードの「**パートナー、ファイル・ロケーション、パスワードの選択**」ページから、次の値を入力します。
   - **この証明書を所有するパートナー (Which partner does this certificate(s) belongs to)**: 新たにアップロードされた証明書を関連付けるパートナーを選択します。「**検索**」をクリックして、特定のパートナー、またはパートナーの

サブセットを検索します。パートナーがハブ・オペレーターまたは内部パートナーの場合は、証明書のロケーション、秘密鍵のロケーション、およびパスワードを入力します。あるいはトラストストアまたは鍵ストアをパスワード付きで提供します。外部パートナーの場合は、証明書のロケーションを提供するか、証明書チェーンを含むトラストストア・ロケーションを提供します。

- **秘密鍵:** 「**参照**」をクリックして、証明書の秘密鍵を選択します。
- **パスワード:** 証明書にパスワードがある場合は、その値を入力します。
- **トラストストア (または) 鍵ストアのロケーション (Trust Store (or) Keystore Location):** 「**参照**」をクリックして、鍵ストアのロケーションを選択します。鍵ストアは、トラステッド・ルートと CA 証明書、および秘密鍵のコレクションです。
- **パスワード:** 鍵ストア・ロケーションのパスワードを入力します。
- **タイプ:** トラストストア (または) 鍵ストアのタイプを選択します。ドロップダウンから選択可能な値は、JKS、JCEKS、および PKCS12 です。

**注:** Web Sphere Partner Gateway では、iKeyman を使用して CMS タイプの鍵データベース (鍵ストア) を作成すると、次のエラーが表示されます。

```
CMS Java ネイティブ・ライブラリーが見つかりませんでした。 (The CMS java native library
was not found. )製品に必要な SSL コンポーネントがインストール済みであり、ライブラリー・
パスが正しく定義されていることを確認してください。 (Please make sure the SSL component
required by your product is installed and library path is defined properly.)
```

. WebSphere Application Server と Web Sphere Partner Gateway は CMS 鍵ストアを使用しないため、サポートされている鍵ストア・タイプである JKS (デフォルト)、PKCS12、または JCEKS を使用してください。

3. 「**次へ**」をクリックして、ウィザードの「**証明書の詳細**」ページに進みます。複数の証明書があるトラストストア経由で証明書をロードすると、ウィザードの「**エンド・エンティティーおよび CA 証明書の選択 (Select end entity and CA certificates)**」ページがオープンします。トラストストアで使用可能な証明書のリストが表示されます。
4. ウィザードの「**エンド・エンティティー証明書および CA 証明書の選択 (Select end entity certificate and CA Certificate)**」ページで、次の値を入力します。
   - **鍵ストアに複数のエンド・エンティティー証明書が含まれています。アップロードする証明書を選択しますか? (The keystore contains more than one End Entity certificate. Select the certificate to be uploaded?)** - ドロップダウンに、すべてのエンド・エンティティー証明書のリストがあります。アップロードする証明書を選択します。
   - **パスワード** - 鍵ストアにパスワードがある場合は、このチェック・ボックスを選択し、テキスト・ボックスにパスワードを入力します。
   - **アップロードするルートおよび中間 CA 証明書のリストの選択 (Select the List of Root and Intermediate CA certificates to be uploaded)** - リスト・ボックスから、アップロードするルートおよび中間 CA 証明書を選択します。
5. 「**次へ**」をクリックして、ウィザードの「**証明書の詳細**」ページに進みます。
6. ウィザードの「**証明書の詳細**」ページで、次の証明書の詳細情報を入力します。

- **リーフ証明書名** - リーフ証明書の名前。このフィールド名は、証明書がリーフ証明書か、ルート CA 証明書か、あるいは中間 CA 証明書かによって変化します。
- **説明** - リーフ証明書の説明。
- **証明書タイプ** - この証明書を暗号化と関連付けます。
- **証明書の使用** - 証明書の使用を関連付けます。値は、「1 次」と「2 次」です。
- **動作モード** - 操作のモードを入力します。
- **状況** - アップロードした後に証明書を使用可能にするか使用不可にするかを基に、有効または無効を選択します。「次へ」ボタンは、証明書が使用可能になっている場合にのみ有効になります。
- **セットの管理** - 証明書を、既存のセットまたは新規セットに関連付けることができます。証明書が 2 次証明書の場合は、既存のセットにのみ関連付けることができます。証明書は、暗号化のタイプの内部パートナー、または SSL (着信クライアント認証) あるいは署名 (検証) のタイプの外部パートナーの任意のセットに関連付けることができます。

  **注:** ハブ・オペレーターの場合、セット管理はありません。証明書は、作成されたデフォルト証明書に関連付けられます。

7. 「**次へ**」をクリックして、ウィザードの「セット」ページに進みます。証明書が 1 次の場合は、セットを作成してその証明書をセットおよびパートナー接続に関連付ける必要はありません。「**新規セットの作成 (Create new set)**」チェック・ボックスを選択した場合は、ウィザードの「**新規セットの作成 (Create New Set)**」ページがオープンします。それ以外の場合は、ウィザードの「**既存のセットに追加 (Add to Existing)**」 ページがオープンします。ファイルに内部パートナーの秘密鍵が含まれている場合、または SSL / デジタル署名に使用される外部パートナーの公開証明書が含まれている場合は、「**終了**」をクリックすることができます。
8. ウィザードの「**新規セットの作成 (Create New Set)**」ページで、新規セットの詳細情報を入力します。1 次証明書の場合は、セットを作成して証明書をそのセットと関連付ける必要はありません。次の値を入力します。
   - **セット名** - セットの名前。
   - **説明** - セットの説明。
   - **状況** - 有効または無効を選択。これが無効になっている場合、「**次へ**」ボタンは有効になりません。
   - **デフォルト設定にする** - このセットをデフォルトにする場合は、このチェック・ボックスを選択します。
9. ウィザードの「**既存のセットに追加**」ページで、証明書を追加するセットを選択します。次の値を入力します。
   - **選択済み証明書タイプに使用可能なセットのリストから選択 (Select from the list of Sets available for the selected Certificate type)** - リストから、証明書に追加するセットを選択します。
   - **デフォルト設定にする** - このセットをデフォルトにする場合は、このチェック・ボックスを選択します。

10. 「**新規セットの作成 (Create New Set)**」または「**既存セットに追加 (Add to Existing Set)**」から、「**次へ**」をクリックして、ウィザードの「**デフォルト設定**」ページに進みます。「**次へ**」ボタンは、セットの状況が使用可能の場合にのみ有効になります。
11. アップロード後に証明書を使用可能にするか使用不可にするかを基に、「**状況**」で「**有効**」または 「**無効**」を選択します。

    **注:** 前のページ (「新規セットの作成 (Create new set)」または「既存のセットに追加 (Add to existing set)」) で「**デフォルト・セットの作成 (Make default set)**」チェック・ボックスを選択した場合は、セットを動作モードに関連付ける必要があります。これは、動作モードに対する証明書の使用を表示します。内部パートナーについては、暗号化は使用不可になります。外部パートナーについては、SSL クライアントとデジタル署名が使用不可になります。
12. 「**次へ**」をクリックして、ウィザードの「構成」ページに進みます。「**終了**」をクリックしたのに、欠落しているルートまたは中間 CA 証明書がある場合は、アップロードするように求めるプロンプトが表示されます。プロンプト・ウィンドウで「はい」をクリックすると、ウィザードの最初のページがオープンします。後の段階でアップロードしたい場合は、「**キャンセル**」をクリックしてください。
13. ウィザードの「構成」ページで、次の値を入力します。

    **注:** 「構成」ページには、動作モードに対する証明書 (セット) の使用法のリストが表示されます。すべてに対して現在のセット名が定義済みですが、それらの名前はリセットすることができます。
    - **パートナーから (From Partner)** - このフィールドには、内部パートナーの値が定義済みです。
    - **パートナーへ (To Partner)** - このドロップダウンには、すべての外部パートナーのリストが定義済みです。「すべて (All)」の値を選択して、すべての外部パートナーを組み込むこともできます。
    - **パッケージから (From Package)** - ドロップダウンから、内部パートナーの文書フロー定義オブジェクトのパッケージを選択します。
    - **パッケージへ (To Package)** - リストから、外部パートナーの文書フロー定義のパッケージを選択します。
14. セットを他のパートナー接続に関連付けたい場合は、「**接続の追加を続行 (Add more connections)**」をクリックします。
15. 「**2 次証明書の追加 (Add Secondary Certificate)**」をクリックして、現行セットに 2 次証明書を追加します。
16. 「**終了**」をクリックして、証明書をアップロードします。欠落しているルートまたは中間 CA 証明書がある場合は、アップロードするように求めるプロンプトが表示されます。プロンプト・ウィンドウで「はい」をクリックすると、ウィザードの最初のページがオープンします。後の段階でアップロードしたい場合は、プロンプト・ウィンドウで「**キャンセル**」をクリックします。

SSL クライアント認証とデジタル署名の両方の 1 次証明書と 2 次証明書をアップロードし、さらに 1 次証明書を 2 つの異なるエントリーとしてアップロードする場合は、対応する 2 次証明書を 2 つの異なるエントリーとしてアップロードしてください。

### CA が署名した証明書の取得

#### このタスクについて

CA が署名した証明書を使用する場合は、以下の手順に従います。

1. IKEYMAN ユーティリティーを始動します。
2. IKEYMAN を使用して、レシーバーの認証要求および鍵ペアを生成します。
3. CA に証明書署名要求 (CSR) をサブミットします。
4. CA から署名証明書を受信したら、IKEYMAN を使用して、この署名証明書を鍵ストアに配置します。
5. すべてのパートナーに署名 CA 証明書を配布します。

## インバウンドのデジタル・シグニチャー検証証明書のインストール

#### このタスクについて

文書を受信すると、文書マネージャーが、パートナーの署名証明書を使用して、送信側の署名を確認します。パートナーは、自己署名証明書を X.509 DER 形式で管理者に送信します。パートナーは、コミュニティー・コンソールを使用して、パートナーの証明書をそれぞれのパートナーのプロファイルにインストールします。

証明書をインストールするには、以下の手順を実行します。

1. パートナーの X.509 シグニチャー証明書を DER 形式で受信します。
2. 「**プロファイル**」 > 「**外部パートナー**」 > 「**証明書**」 > 「**証明書のロード**」にナビゲートします。
3. 「**検索**」をクリックして、特定のパートナーまたはパートナーのサブセットを検索します。
4. 「**証明書のロケーション**」の横の「**参照**」をクリックして証明書をアップロードします。
5. 「**次へ**」をクリックして、ウィザードの「**証明書の詳細**」ページに進みます。
6. この証明書を「**デジタル署名検証**」と関連付けます。
7. アップロード後に証明書を使用可能にするか使用不可にするかを基に、「**状況**」で「**有効**」または 「**無効**」を選択します。
8. 「**動作モード**」を選択します。ハブ・オペレーターの場合は、「**動作モード**」を選択するオプションはありません。
9. 「**終了**」をクリックして変更を保存し、ウィザードを閉じます。
10. 証明書が既に CA によって署名されているにもかかわらず、CA ルート証明書や証明書チェーンに所属する証明書の中にまだハブ・オペレーター・プロファイルにインストールされていないものがある場合は、ここでそれらの証明書をインストールします。これはトラストストア/鍵ストアにのみ適用されます。
    a. 「**ハブ管理**」>「**ハブ・パートナー・プロファイル (Hub partner profile)**」>「**証明書**」をクリックして、「証明書リスト」ページを表示します。

       コミュニティー・コンソールにハブ・オペレーターとしてログインし、証明書を自分のプロファイルにインストールしてください。
    b. 「**証明書のロード**」をクリックします。
    c. 「**ルートおよび中間**」を選択します。

d. 証明書の説明を入力します (必須)。

e. 「状況」を「**有効**」に変更します。

f. 「**参照**」をクリックし、証明書の保存先のディレクトリーに移動します。

g. 証明書を選択し、「**オープン**」をクリックします。

h. 「**アップロード**」をクリックし、次に「**保存**」をクリックします。

**注:** CA 証明書が既にインストールされている場合は、このステップを実行する必要がありません。

11. パッケージ (最も高いレベル)、パートナー、または接続レベル (最も低いレベル) で署名を使用可能にします。この設定により、接続レベルの他の設定をオーバーライドできます。必要な属性が欠落している場合は、接続の要約によって通知されます。

    例えば、パートナー接続の属性を変更するには、「**アカウント管理**」>「**接続**」をクリックし、パートナーを選択します。「**属性**」をクリックし、属性を編集します (「**AS 署名済み**」など)。

# 証明書を使用した SSL の使用可能化

以降のセクションでは、WebSphere Partner Gateway で使用する SSL 証明書の作成とインストールの方法について説明します。また、SSL ハンドシェーク処理についても簡単に紹介します。コミュニティーで SSL を使用していない場合は、ハブ管理者もパートナーも、インバウンドまたはアウトバウンド SSL 証明書は必要ありません。

## SSL ハンドシェーク

### このタスクについて

各 SSL セッションは、ハンドシェークで始まります。

クライアント (パートナーまたは内部パートナー) がメッセージ交換を開始すると、以下のステップが実行されます。

1. クライアントが「client hello」メッセージを送信します。このメッセージには、クライアントの暗号機能 (SSL のバージョンなど。各機能はクライアント優先順序でソートされています)、クライアントがサポートしている暗号スイート、およびクライアントがサポートしているデータ圧縮方法がリストされています。また、メッセージには 28 バイトの乱数も含まれています。
2. サーバーが「hello done」メッセージで応答します。このメッセージには、サーバーが選択した暗号方式 (暗号スイート)とデータ圧縮方法、セッション ID、および別の乱数が記述されています。

   **注:** クライアントとサーバーで、共通の暗号スイートが少なくとも 1 つサポートされている必要があります。サポートされていない場合は、ハンドシェークが失敗します。通常は、サーバーが共通の暗号スイートの中からもっとも強度の高いものを選択します。
3. サーバーが自身のデジタル証明書を送信します。

   サーバー認証はこのステップで実行されます。

4. サーバーが「digital certificate request」メッセージを送信します。「digital certificate request」メッセージでは、サーバーは、サポートしているデジタル証明書の種類、および受け入れ可能な認証局の識別名のリストを送信します。
5. サーバーは「server hello done」メッセージを送信し、クライアントからの応答を待ちます。
6. クライアントは「server hello done」メッセージを受け取って、サーバーのデジタル証明書の妥当性を検証し、サーバーの「hello」パラメーターを受け入れることができるかどうかを確認します。
7. サーバーがクライアントのデジタル証明書を要求した場合、クライアントはデジタル証明書を送信します。適切なデジタル証明書が使用可能でなければ、クライアントは「no digital certificate」アラートを送信します。このアラートは警告のみですが、クライアント認証が必須の場合には、サーバー・アプリケーションでセッションが失敗することがあります。
8. クライアントは「client key exchange」メッセージを送信します。このメッセージには、プリマスター・シークレット (対称暗号鍵の生成に使用される 46 バイトの乱数)、およびメッセージ確認コード (MAC) 鍵 (サーバーの公開鍵で暗号化済み) が記述されています。
9. デジタル証明書をサーバーに送信した場合には、クライアントは自身の秘密鍵で署名した「digital certificate verify」メッセージを送信します。このメッセージの署名を検証することによって、サーバーはクライアント・デジタル証明書の所有権を明示的に検証できます。

   **注:** サーバー・デジタル証明書を検証するために、追加の処理は必要ありません。デジタル証明書に所属する秘密鍵がサーバーにない場合は、サーバーはプリマスター・シークレットの暗号化を解除できず、対称暗号化アルゴリズムの正しい鍵を生成できないため、ハンドシェークは失敗します。
10. クライアントが一連の暗号操作を使用してプリマスター・シークレットをマスター・シークレットに変換します。暗号化とメッセージ認証に必要な鍵材料はすべて、このマスター・シークレットから派生します。次に、新たに折衝された暗号スイートにサーバーを切り替えるため、クライアントは「change cipher spec」メッセージを送信します。この次にクライアントから送信されるメッセージ (「finished」メッセージ) が、この暗号方式と鍵で暗号化された最初のメッセージになります。
11. サーバーは、自身の「change cipher spec」メッセージと「finished」メッセージで応答します。

クライアント認証にはステップ 4、7、および 9 が必要です。

SSL ハンドシェークが終了し、暗号化されたアプリケーション・データを送信できるようになります。

## インバウンド SSL 証明書の構成

ここでは、パートナーからのインバウンド接続要求に対してサーバー認証とクライアント認証をどのように構成するかについて説明します。

インバウンド要求は、パートナーが WebSphere Partner Gateway に文書を送信する場合に出されます。コミュニティーで SSL を使用していない場合、インバウンドまたはアウトバウンド SSL 証明書は必要ありません。

**注:** インバウンド FTPS の場合、WebSphere Partner Gateway はカスタマーが提供する FTP サーバーを使用するため、インバウンド SSL 構成は、カスタマーが使用しているその特定の FTP サーバー製品ごとに行われます。

## ステップ 1: SSL 証明書の取得

### このタスクについて

WebSphere Application Server は、SSL を介してパートナーからの接続要求を受信するときに、SSL 証明書を使用します。この証明書は、レシーバーがパートナーに対してハブを識別するために示す証明書です。このサーバー証明書は、自己署名証明書または CA が署名した証明書になります。通常、セキュリティーを高めるために CA 証明書を使用します。テスト環境では、自己署名証明書を使用する可能性があります。iKeyman または WebSphere Application Server 管理コンソールを使用して、証明書および鍵ペアを生成してください。iKeyman または WebSphere Application Server 管理コンソールの使用法について詳しくは、IBM の資料を参照してください。

証明書と鍵ペアを生成したら、すべてのパートナーに対してインバウンド SSL トラフィックの証明書を使用します。レシーバーまたはコンソールが複数ある場合は、結果として作成された鍵ストアを各インスタンスにコピーします。WebSphere Application Server 管理コンソールを使用して証明書を生成した場合は、WebSphere Application Server 管理コンソールを使用して鍵および証明書を別のサーバーの別の鍵ストアにインポートできます。証明書が自己署名されている場合は、この証明書をパートナーに提供します。この証明書を取得するには、IKEYMAN を使用して、ファイルに公開証明書を抽出します。

**自己署名証明書の生成:** 自己署名サーバー証明書を使用する場合は、以下の手順を実行します。

1. /<*WAS_Installation_dir*>/bin にある iKeyman ユーティリティーを始動します。初めて IKEYMAN を使用する場合は、鍵ストアにある「ダミー」の証明書を削除します。
2. iKeyman を使用してレシーバーまたはコンソールの鍵ストアを開き、レシーバーまたはコンソールの鍵ストア用の自己署名証明書および鍵ペアを生成します。
3. IKEYMAN を使用して、ご使用の公開鍵を含む証明書をファイルに抽出します。

   鍵ストアを JKS、PKCS12、または JCEKS ファイルに保存します。
4. パートナーに証明書を配布します。配布方法としては、証明書をパスワードで保護された ZIP ファイルにして、E メールで送信することをお勧めします。パートナーは、管理者に連絡して、ZIP ファイルのパスワードを要求する必要があります。
5. WebSphere Application Server 管理コンソールを使用して、レシーバーおよびコンソールの設定値および SSL 構成で新しい証明書を設定します。これを行うには、各ノードまたはサーバーの構成で鍵ストアの新しい証明書の別名を選択します。

**CA 生成証明書の取得:** CA が署名した証明書を使用する場合は、以下の手順に従います。

1. */<WAS_Installation_dir>/*bin ディレクトリーにある iKeyman ユーティリティーを始動します。
2. IKEYMAN を使用して、レシーバーの認証要求および鍵ペアを生成します。
3. CA に証明書署名要求 (CSR) をサブミットします。
4. CA から署名証明書を受信したら、IKEYMAN を使用して、この署名証明書を鍵ストアに配置します。
5. 必要に応じて、すべてのパートナーに CA 証明書を配布します。
6. WebSphere Application Server 管理コンソールを使用して、レシーバーおよびコンソールの設定値および SSL 構成で新しい証明書を設定します。これを行うには、各ノードまたはサーバーの構成で鍵ストアの新しい証明書の別名を選択します。

   **注:** WebSphere Application Server 管理コンソールを使用して、前述の手順を実行することもできます。

## ステップ 2: クライアントの認証
### このタスクについて

文書を送信したパートナーを認証する場合は、このセクションのステップを実行します。

**クライアント証明書のインストール:**
**このタスクについて**

クライアント認証では、以下の手順に従います。

1. パートナーの証明書を取得します。
2. 証明書が自己署名証明書の場合は、iKeyman または WebSphere Application Server 管理コンソールを使用して、この証明書をトラストストアにインストールします。
3. 証明書が CA 証明書の場合は、iKeyman または WebSphere Application Server 管理コンソールを使用して、関連する CA 証明書を関連するトラストストアに追加します。

**注:** ハブ・コミュニティーにさらにパートナーを追加する場合は、iKeyman または WebSphere Application Server 管理コンソールを使用して、トラストストアにそのパートナーの証明書を追加します。パートナーがコミュニティーを出た場合は、iKeyman または WebSphere Application Server 管理コンソールを使用して、トラストストアからそのパートナーの証明書を削除します。

**クライアント認証の設定:**
**このタスクについて**

証明書をインストールしたら、ユーティリティー・スクリプト bcgClientAuth.jacl を実行して、WebSphere Application Server がクライアント認証を使用するように構成します。

1. ディレクトリー */<ProductDir>/*bin に移動します。

2. クライアント認証を有効にするには、以下のようにスクリプトを呼び出します。

```
./bcgwsadmin.sh -f /<ProductDir>/scripts/bcgClientAuth.jacl
   -conntype NONE set
```

**注:** クライアント認証を無効にするには、以下のようにスクリプトを呼び出します。

```
./bcgwsadmin.sh -f /<ProductDir>/receiver/scripts/bcgClientAuth.jacl
  -conntype NONE clear
```

これらの変更内容を有効にするには、bcgreceiver サーバーを再始動する必要があります。 WebSphere Application Server 管理コンソールを使用して、クライアント認証を有効にすることもできます。値が「サポート」の場合、サーバーはクライアント証明書を要求しますが、クライアント証明書がなくても、SSL ハンドシェークを確立できます。値が「必要」の場合は、クライアント証明書を送信する必要があります。そうしないと、SSL ハンドシェークが失敗します。

**クライアント証明書の検証:**
**このタスクについて**

SSL クライアント認証で使用できる追加機能があります。この機能を使用可能にするには、コミュニティー・コンソールを使用します。HTTPS の場合、WebSphere Partner Gateway は、証明書をインバウンド文書のビジネス ID と照合して検査します。この機能を使用するには、パートナーのプロファイルを作成し、クライアント証明書をインポートして、SSL としてフラグを立てます。

1. クライアント証明書をインポートします。
   a. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックして、パートナーのプロファイルを検索します。
   b. 「**証明書**」をクリックします。
   c. 「**証明書のロード**」をクリックします。
   d. 「**参照**」をクリックし、証明書の保存先のディレクトリーに移動します。
   e. 証明書のタイプとして「**SSL クライアント**」を選択します。
   f. 証明書の説明を入力します (必須)。
   g. 「状況」を「**有効**」に変更します。
   h. 「**実動**」 (デフォルト) 以外の動作モードを選択する場合は、リストから目的のタイプを選択します。
   i. 「**終了**」をクリックします。
2. クライアント宛先を更新します。
   a. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックして、パートナーのプロファイルを検索します。
   b. 「**宛先**」をクリックします。
   c. 以前に作成した HTTPS 宛先を選択します。まだ HTTPS 宛先を作成していない場合は、232 ページの『HTTPS 宛先の設定』を参照してください。
   d. 宛先を編集するには、「**編集**」アイコンをクリックします。
   e. 「**SSL クライアント証明書の検証 (Validate SSL Client Certificate)**」に対して、「**はい**」を選択します。
   f. 「**保存**」をクリックします。

## レシーバーとコンソールに対して別々の鍵ストアとトラストストアを構成

WebSphere Partner Gateway は、デフォルトでレシーバーとコンソールに共通の鍵ストアとトラストストアを使用します。ただし、配布モード・インストールでは、レシーバーとコンソールに別々の鍵ストアとトラストストアを構成することができます。

鍵ストアとトラストストアを構成するには、レシーバーとコンソールに別々の鍵ストアとトラストストアを作成して設定します。また、別々の SSL 構成も作成します。 SSL 構成は、クラスター・レベルまたはサーバー・レベルのいずれかで設定することができます。 SSL 構成はクラスター・レベルで設定した方が容易です。なぜなら、そうするとクラスター内のすべてのサーバーにその構成が適用され、各サーバーを別々に構成する必要がないからです。

**クラスター・レベルでの SSL 構成の設定:** 新規の鍵ストアとトラストストアを使用してクラスター・レベルで SSL 構成を設定しているときに、サーバー・レベルで設定された SSL 構成が存在することはできません。サーバー・レベルで設定された SSL 構成がある場合、クラスター・レベルの SSL 構成は使用されず、代わりにそのサーバーに対して設定された構成が使用されます。

bcgconsoleCluster に SSL 構成を設定するには、以下のステップに従ってください。

1. コンソール・クラスターの鍵ストアを作成します。「**セキュリティー**」>「**SSL 証明書および鍵管理**」>「**鍵ストアおよび証明書**」にナビゲートして、bcgconsole クラスター・スコープに鍵ストアを作成する必要があります。
2. コンソール・クラスターのトラストストアを作成します。「**セキュリティー**」>「**SSL 証明書および鍵管理**」>「**鍵ストアおよび証明書**」にナビゲートして、bcgconsole クラスター・スコープにトラストストアを作成する必要があります。
3. 「**セキュリティー**」>「**SSL 証明書および鍵管理**」>「**SSL 構成**」にナビゲートして、コンソール・クラスター・スコープにコンソール・クラスターの SSL 構成を作成します。前のステップで作成された鍵ストアとトラストストアを設定します。「**証明書別名の取得**」をクリックして証明書別名リスト内の証明書別名を更新し、サーバー認証に使用される必須の別名を選択します。トラスト・マネージャーを **IbmPKIX** に設定します。
4. 継承した SSL 構成をオーバーライドして、この SSL 構成を bcgconsoleCluster に設定します。「**証明書別名の更新**」をクリックして証明書別名を更新し、サーバー認証に使用される別名を設定します。
5. bcgconsoleCluster を再始動します。

bcgreceiverCluster に SSL 構成を設定するには、以下のステップに従ってください。

1. レシーバー・クラスターの鍵ストアを作成します。「**セキュリティー**」>「**SSL 証明書および鍵管理**」>「**鍵ストアおよび証明書**」にナビゲートして、bcgreceiver クラスター・スコープに鍵ストアを作成する必要があります。
2. レシーバー・クラスターのトラストストアを作成します。「**セキュリティー**」>「**SSL 証明書および鍵管理**」>「**鍵ストアおよび証明書**」にナビゲートして、bcgconsole クラスター・スコープにトラストストアを作成する必要があります。
3. 「**セキュリティー**」>「**SSL 証明書および鍵管理**」>「**SSL 構成**」にナビゲートして、レシーバー・クラスター・スコープにレシーバー・クラスターの SSL 構

成を作成し、前のステップで作成された鍵ストアとトラストストアを設定します。「**証明書別名の取得**」をクリックして証明書の別名を取得し、サーバー認証に使用される必須の別名を選択します。トラスト・マネージャーを **IbmPKIX** に設定します。

4. 継承した SSL 構成をオーバーライドして、この SSL 構成を bcgreceiverCluster に設定します。「**証明書別名の更新**」をクリックして証明書別名を更新し、サーバー認証に使用される別名を設定します。
5. bcgreceiverCluster を再始動します。

鍵ストア、トラストストア、SSL 構成、およびエンドポイント構成の作業について詳しくは、WebSphere Application Server 文書の『*アプリケーションとその環境の保護*』セクションを参照してください。

**配布モードで NodeDefaultSSLSetting に NodeDefaultTrustStore を設定:** この設定は、シンプル配布モードに対して行う必要があります。ただし、レシーバーとコンソールに共通の鍵ストアとトラストストアが使用される場合、この設定は完全配布モードにも適用されます。ノードがセル内で統合されている場合、そのノードからの署名者証明書が CellDefaultTrustStore に追加されます。デフォルトにより、NodeDefaultSSLSetting はトラストストアとして CellDefaultTrustStore を参照します。 WebSphere Partner Gateway レシーバーおよびコンソールの場合、他のノードからの署名者証明書を使用することは好ましくないことがあります。WebSphere Partner Gateway がインストールされているノードに対して専用のトラストストアを使用するには、NodeDefaultSSLSettings に NodeDefaultTrustStore をトラストストアとして設定することができます。

この変更を行うためのステップは、次のとおりです。

1. WebSphere Application Server 管理コンソールで、「**セキュリティー**」>「**SSL 証明書および鍵管理**」>「**エンドポイント・セキュリティー構成の管理**」> **<node_name>** > 「**SSL 構成**」> **NodeDefaultSSLSettings** にナビゲートします。
2. 「トラストストア名」フィールドで、**NodeDefaultTrustStore** を選択します。

   **注:** 使用したいトラストストアに対して NodeDefaultTrustStore が構成されていることを確認してください (例えば、bcgSecurityTrust.jks など)。
3. 「**適用 (Apply)**」をクリックします。
4. コンソールの次のページで、「**保存**」をクリックしてマスター構成への変更を更新します。
5. そのノード内のサーバーを再始動します。

**注:** 完全配布モードの場合は、bcgreceiver サーバーと bcgconsole サーバーを含むすべてのノードに対して上記の変更を行う必要があります。シンプル配布モードの場合は、bcgserver を含むすべてのノードに対してこれらの変更を行う必要があります。

**WebSphere Partner Gateway サーバーを含むノードに対して NodeDefaultTrustStore が設定されている場合、trust.p12 に署名者証明書を追加:** 現在、NodeDefaultTrustStore は trust.p12 を参照しています。WebSphere Partner Gateway サーバーを含むノードに対して NodeDefaultTrustStore が設定されている場

合、bcgSecurityTrust.jks は使用されません。必要に応じて、bcgSecurityTrust.jks からの署名者証明書を trust.p12 に追加する必要があります。

## アウトバウンド SSL 証明書の構成

アウトバウンド要求は、WebSphere Partner Gateway がパートナーに文書を送信する場合に出されます。コミュニティーで SSL を使用していない場合、インバウンドまたはアウトバウンド SSL 証明書は必要ありません。

### ステップ 1: サーバーの認証

#### このタスクについて

SSL を使用してパートナーにアウトバウンド文書を送信する場合、WebSphere Partner Gateway は、パートナーからサーバー・サイド証明書を要求します。複数のパートナーに対して同じ CA 証明書を使用することができます。証明書は X.509 DER 形式でなければなりません。

**注:** フォーマットは iKeyman ユーティリティーで変換できます。iKeyman を使用してフォーマットを変換するには、次のステップを実行します。

1. IKEYMAN を始動します。
2. 新規ブランク鍵ストアを作成するか、既存の鍵ストアを開きます。
3. 「鍵データベース・コンテンツ (Key Database Content)」で「**署名者証明書**」を選択します。
4. 「**追加**」オプションを使用して ARM 証明書を追加します。
5. 「**抽出**」オプションを使用して、バイナリー DER データと同じ証明書を抽出します。
6. iKeyman を閉じます。

パートナーの自己署名証明書をハブ・オペレーター・プロファイルにインストールします。証明書が既に CA で署名されているにもかかわらず、CA ルート証明書や証明書チェーンに所属する証明書の中にまだハブ・オペレーター・プロファイルにインストールされていないものがある場合は、それらの証明書をハブ・オペレーター・プロファイルにインストールします。

1. 「**アカウント管理**」>「**プロファイル**」>「**証明書**」をクリックして、「証明書リスト」ページを表示します。

   必ずハブ・オペレーターまたは内部パートナーとして Community Console にログインします。
2. 「**PKCS12 のロード**」をクリックします。

   **注:** アップロードされる PKCS12 ファイルには、秘密鍵が 1 つだけと、それに関連する証明書が含まれている必要があります。証明書と PKCS#8 形式の秘密鍵を別々にアップロードすることもできます。
3. 証明書のタイプとして「**SSL クライアント**」を選択します。
4. 証明書の説明を入力します (必須)。
5. 「状況」を「**有効**」に変更します。
6. 「**参照**」をクリックし、証明書の保存先のディレクトリーに移動します。

7. 証明書を選択し、「**オープン**」をクリックします。
8. パスワードを入力します。
9. 「**実動**」 (デフォルト) 以外の動作モードを選択する場合は、リストから目的のタイプを選択します。
10. SSL 証明書が 2 つある場合は、「**証明書の使用**」リストから「**1 次**」または「**2 次**」を選択して、証明書が 1 次証明書なのか 2 次証明書なのかを指定します。
11. 「**アップロード**」をクリックし、次に「**保存**」をクリックします。

**注:** CA 証明書がすでにインストールされている場合には、このステップを実行する必要はありません。

## ステップ 2: クライアントの認証

### このタスクについて

SSL クライアント認証が必要な場合には、パートナーがハブからの証明書を要求します。コミュニティー・コンソールを使用して、WebSphere Partner Gateway に証明書をインポートします。iKeyman を使用すると、証明書を生成できます。証明書が自己署名証明書の場合は、この証明書をパートナーに提供する必要があります。CA が署名した証明書の場合は、CA ルート証明書をパートナーに渡す必要があります。これにより、パートナーは、この証明書を信頼できる証明書に追加できます。

SSL 証明書は、複数持つことができます。そのうちの 1 つが、デフォルトで使用される 1 次証明書になります。もう一方は 2 次証明書となり、1 次証明書の有効期限が切れた場合に使用されます。

**自己署名証明書の使用:**

### このタスクについて

自己署名証明書を使用する場合は、以下の手順を実行します。

1. IKEYMAN ユーティリティーを始動します。
2. IKEYMAN を使用して、自己署名証明書および鍵ペアを生成します。
3. IKEYMAN を使用して、ご使用の公開鍵を含む証明書をファイルに抽出します。
4. パートナーに証明書を配布します。配布方法としては、証明書をパスワードで保護された ZIP ファイルにして、E メールで送信することをお勧めします。パートナーは、管理者に連絡して、ZIP ファイルのパスワードを要求する必要があります。
5. IKEYMAN を使用して、自己署名証明書と秘密鍵のペアを PKCS12 ファイルの形式でエクスポートします。
6. コミュニティー・コンソールを使用して、自己署名証明書と鍵をインストールします。
   a. 「**アカウント管理**」>「**プロファイル**」>「**証明書**」をクリックして、「証明書リスト」ページを表示します。

      ハブ・オペレーターとしてコミュニティー・コンソールにログインしてください。
   b. 「**PKCS12 のロード**」をクリックします。

**注:** アップロードされる PKCS12 ファイルには、秘密鍵が 1 つだけと、それに関連する証明書が含まれている必要があります。証明書と PKCS#8 形式の秘密鍵を別々にアップロードすることもできます。

c. 証明書のタイプとして「**SSL クライアント**」を選択します。

d. 証明書の説明を入力します (必須)。

e. 「状況」を「**有効**」に変更します。

f. 「**参照**」をクリックし、証明書の保存先のディレクトリーに移動します。

g. 証明書を選択し、「**オープン**」をクリックします。

h. パスワードを入力します。

i. 「**実動**」 (デフォルト) 以外の動作モードを選択する場合は、リストから目的のタイプを選択します。

j. SSL 証明書が 2 つある場合は、「**証明書の使用**」リストから「**1 次**」または「**2 次**」を選択して、証明書が 1 次証明書なのか 2 次証明書なのかを指定します。

k. 「**アップロード**」をクリックし、次に「**保存**」をクリックします。

SSL クライアント認証とデジタル署名の両方の 1 次証明書と 2 次証明書をアップロードし、さらに 1 次証明書を 2 つの異なるエントリーとしてアップロードする場合は、対応する 2 次証明書を 2 つの異なるエントリーとしてアップロードしてください。

**CA が署名した証明書の使用:**
**このタスクについて**

CA が署名した証明書を使用する場合は、以下の手順に従います。

1. IKEYMAN を使用して、レシーバーの認証要求および鍵ペアを生成します。
2. CA に証明書署名要求 (CSR) をサブミットします。
3. CA から署名証明書を受信したら、IKEYMAN を使用して、この署名証明書を鍵ストアに配置します。
4. すべてのパートナーに署名 CA 証明書を配布します。

## 証明書失効リスト (CRL) の追加

WebSphere Partner Gateway には、証明書失効リスト (CRL) 機能があります。認証局 (CA) が発行する CRL は、スケジュールされていた有効期限よりも前に失効した証明書を持つパートナーを識別します。失効した証明書を持つパートナーは、WebSphere Partner Gateway へのアクセスを拒否されます。

各失効証明書は、CRL で証明書シリアル番号によって識別されます。文書マネージャーは、60 秒ごとに CRL をスキャンし、CRL リストに含まれている証明書を拒否します。ただし、CRL ディレクトリーのスキャンを行う時間間隔を構成することができます。時間間隔は、構成プロパティー bcg.rosettanet.encrypt.CertDbRefreshInterval に対して指定されます。

デフォルトでは、CRL は */<shared_data_directory>*/security/crl に保管されます。WebSphere Partner Gateway では、「コンソール」>「システム管理」>「DocMgr の管理」>「セキュリティー」の設定値 bcg.CRLDir を使用して、CRL ディレクトリーの場所を特定します。

CRL は、CRL ディレクトリーに格納します。

## CRLDP の構成

### このタスクについて

CRLDP を構成するには、Java 仮想マシン設定を変更します。つまり、値 Dcom.ibm.security.enableCRLDP = True を設定します。

この変更は、bcgdocmgr サーバーに対して完全配布モードで行う必要があります。シンプル配布モードおよびシンプル・モードの場合は、bcgserver に対して行う必要があります。

以下の手順に従ってください。

1. WebSphere Application Server 管理コンソールにログインします。
2. 「**サーバー**」>「**アプリケーション・サーバー**」に移動して、「**サーバー**」を選択します。
3. 以下のプロセスを実行して、プロパティーを設定します。
   a. サーバーを選択します (bcgdocmgr、bcgreceiver、または bcgconsole)。
   b. 「**構成**」ページで、ページの「**サーバー・インフラストラクチャー**」セクションにある「**Java およびプロセス管理**」を展開して、「**プロセス定義**」を選択します。
   c. 「**プロセス定義構成 (Process definition configuration)**」ページで、「**追加プロパティー**」セクションの「**Java 仮想マシン**」を選択します。
   d. 「汎用 JVM 引数」フィールドの既存の値 (存在する場合) に -Dcom.ibm.security.enableCRLDP=true を追加します。
4. 「**適用**」をクリックして「保存」をクリックし、この構成を完了します。
5. サーバーを再始動します。
6. クラスター内のすべてのサーバーでこのプロパティーを設定します。

# コミュニティー・コンソールおよびレシーバー・コンポーネントに対するインバウンド SSL の構成

WebSphere Partner Gateway 鍵ストアは、WebSphere Application Server にあらかじめ構成されています。このセクションは、別の鍵ストアを使用する場合にのみ適用されます。

WebSphere Partner Gateway のコミュニティー・コンソールおよびレシーバー・コンポーネントに対して SSL を構成するには、以下の手順に従います。

1. 以下の情報を取得します。

- 鍵ファイルおよびトラスト・ファイルの絶対パス名。例えば、レシーバーの場合は <*ProductDir*>/common/security/keystore/bcgSecurity.jks および <*ProductDir*>/common/security/keystore/bcgSecurityTrust.jks です。

  これらの名前は正確に入力してください。UNIX 環境では、これらの名前は大文字と小文字が区別されます。
- 各ファイルの新規パスワード。
- 各ファイルの形式。JKS、JCEKS、または PKCS12 の値の中から選択してください。この値は、大文字で表示されているとおりに入力してください。
- スクリプト・ファイル bcgssl.jacl のパス。

2. 「コミュニティー・コンソール」ウィンドウを開き、/<*ProductDir*>/bin に移動します。パスワードを変更する際、サーバーが稼働中である必要はありません。
3. 以下のコマンドを入力します。<> で囲まれた値は適切な値に置き換えてください。すべての値を入力する必要があります。

```
./bcgwsadmin.sh -f /<ProductDir>/
scripts/bcgssl.jacl -conntype NONE install
<keyFile_pathname>
<keyFile_password> <keyFile_format> <trustFile_pathname>
<trustFile_password> <trustFile_format>
```

4. サーバーを始動します。サーバーの始動に失敗した場合は、bcgssl.jacl の実行時のエラーが原因である可能性があります。間違えた場合は、スクリプトに戻って修正します。
5. bcgClientAuth.jacl を使用して clientAuthentication SSL プロパティーを設定した場合は、bcgssl.jacl を使用した後に clientAuthentication をリセットします。これは、bcgssl.jacl がクライアント認証に対して設定された値を偽の値で上書きしてしまうためです。

**注:**

1. コンソールに対してこれらのステップを繰り返します。パス名の **receiver** は、**console** に置き換えてください。
2. WebSphere Application Server 管理コンソールを使用して、SSL、鍵ストア、およびトラストストアの構成を行うこともできます。

WebSphere Partner Gateway はデフォルトで、レシーバーとコンソールの両方に対して、1 つの鍵ストアとトラストストアをサポートします。ただし、完全配布モードでは、レシーバーとコンソールに対して別々の鍵ストアとトラストストアを使用することができます。レシーバーとコンソールに対して別々の鍵ストアとトラストストアを使用するには、WAS 管理コンソールを使用して、レシーバーに対して次の構成を行ってください。

1. レシーバー鍵ストアの鍵ストアを作成します。WAS 文書の中の『鍵ストア構成の作成』のセクションを参照してください。
2. レシーバー・トラストストアのトラストストアを作成します。WAS 文書「<*アプリケーションとその環境の保護*」の中の『<*鍵ストア構成の作成*』セクションを参照してください。
3. レシーバーの SSL 構成を作成し、その構成に前述の鍵ストアとトラストストアを設定します。鍵ストアでサーバー認証に使用される、必要な別名を選択します。トラスト・マネージャーを **IbmPKIX** に設定します。WAS 文書「アプリケーションおよび*環境の保護 (Securing applications and their environment)*」の中の

『*SSL (Secure Socket Layer) 構成の作成 (Creating a Secure Socket Layer configuration)*』セクションを参照してください。

4. 継承した SSL 構成をオーバーライドすることにより、それぞれの bcgreceiver サーバーにこの SSL 構成を設定します。サーバー認証に使用される別名を設定します。
5. それぞれの bcgreceiver サーバーを再始動します。

これらのステップは、コンソールの構成に似ています。WAS 文書「*アプリケーションおよび環境の保護 (Securing applications and their environment)*」の中の該当するセクションを参照してください。

1. コンソール鍵ストアの鍵ストアを作成します。
2. コンソール・トラストストアのトラストストアを作成します。
3. コンソールの SSL 構成を作成し、その構成に前述の鍵ストアとトラストストアを設定します。鍵ストアでサーバー認証に使用される、必要な別名を選択します。トラスト・マネージャーを **IbmPKIX** に設定します。
4. 継承した SSL 構成をオーバーライドすることにより、それぞれの bcgconsole サーバーにこの SSL 構成を設定します。サーバー認証に使用される別名を設定します。
5. それぞれの bcgconsole サーバーを再始動します。

鍵ストア、トラストストア、SSL 構成、およびエンドポイント構成の作業について詳しくは、WAS 文書「*アプリケーションおよび環境の保護 (Securing applications and their environment)*」を参照してください。

**注:** 現在、NodeDefaultTrustStore は trust.p12 を参照しています。bcg ノードに対して NodeDefaultTrustStore が設定されている場合、bcgSecurityTrust.jks は使用されません。必要に応じて、trust.p12 に bcgSecurityTrust.jks から署名者証明書を追加する必要があります。

## ウィザードを使用した証明書のアップロード

### このタスクについて

ハブ・オペレーターとして、内部または外部パートナーの証明書をアップロードすることができます。

- 内部パートナーの秘密鍵および証明書をアップロードします。
- 外部パートナーの公開証明書をアップロードします。
- ルートおよび中間 CA 証明書をアップロードします。
- トラストストアから証明書チェーンをアップロードします。

証明書をアップロードするための証明書アップロード・ウィザードが提供されています。ウィザードを使用すると、証明書と使用法 (署名/検証/暗号化/復号/SSL) との関連付け、証明書と 1 つ以上の動作モードとの関連付け、セット (既存または新規のセット) への追加、すべてのパートナー接続のデフォルトとなる証明書の選択、およびこの証明書セットが使用される特定の接続の選択をすることができます。証明書がセットに関連付けられていない場合、証明書を接続に関連付けるオプションは表示されません。証明書をアップロードしている間に、証明書が有効であり、有

効期限が切れていないことを確認してください。ウィザードを使用して (内部または外部) パートナーの証明書をアップロードするためのステップは、次のとおりです。

1. ナビゲーション・メニューから、「**アカウント管理**」 > 「**プロファイル**」 > 「**証明書**」をクリックします。
2. パートナーを選択し、「**証明書**」をクリックします。
3. 「**証明書のロード**」をクリックします。
4. ウィザードの「**パートナー、ファイル・ロケーション、パスワードの選択**」ページから、次の値を入力します。
   - **この証明書を所有するパートナー (Which partner does this certificate(s) belongs to)**: 新たにアップロードされた証明書を関連付けるパートナーを選択します。「**検索**」をクリックして、特定のパートナー、またはパートナーのサブセットを検索します。パートナーがハブ・オペレーターまたは内部パートナーの場合は、証明書のロケーション、秘密鍵のロケーション、およびパスワードを入力します。あるいはトラストストアまたは鍵ストアをパスワード付きで提供します。外部パートナーの場合は、証明書のロケーションを提供するか、証明書チェーンを含むトラストストア・ロケーションを提供します。
   - **これはルートおよび中間証明書ですか (Is this a root and intermediate certificate)**: 証明書がルートおよび中間証明書の場合、このチェック・ボックスを選択します。

     **注:** ルートおよび中間証明書タイプは、ハブ管理者プロファイルにのみ適用されるため、「ルートおよび中間証明書」チェック・ボックスは、選択されたパートナーがハブ管理者の場合にのみ可視となります。さらに、ハブ管理者プロファイルの場合、「ルートおよび中間証明書」チェック・ボックスは、「証明書のロード」を選択した場合にのみ選択可能となります。
   - **証明書ロケーション (Certificate Location)**: 「**参照**」をクリックして、証明書 (公開/プライベート) のロケーションを選択します。
   - **秘密鍵:** 「**参照**」をクリックして、証明書の秘密鍵を選択します。
   - **パスワード:** 証明書にパスワードがある場合は、その値を入力します。
   - **トラストストア (または) 鍵ストアのロケーション (Trust Store (or) Keystore Location:** 「**参照**」をクリックして、トラストストア (または) 鍵ストアのロケーションを選択します。トラストストアは、トラステッド CA およびルート証明書のコレクションを含むファイルです。鍵ストアは、トラステッド・ルートと CA 証明書、および秘密鍵のコレクションです。
   - **パスワード:** トラストストア (または) 鍵ストアのロケーションにパスワードがある場合は、その値を入力します。
   - **タイプ:** トラストストア (または) 鍵ストアのタイプを選択します。ドロップダウンから選択可能な値は、JKS、JCEKS、および PKCS12 です。
5. 「**次へ**」をクリックして、ウィザードの「**証明書の詳細**」ページに進みます。複数の証明書があるトラストストア経由で証明書をロードすると、ウィザードの「**エンド・エンティティーおよび CA 証明書の選択 (Select end entity and CA certificates)**」ページがオープンします。トラストストアで使用可能な証明書のリストが表示されます。

6. ウィザードの「**アップロードするエンド・エンティティー証明書の選択 (Select end entity certificate to upload)**」ページで証明書を選択します。鍵ストアに複数の秘密鍵があるときは、異なる場合、秘密鍵とともにその鍵のパスワードを入力する必要があります。
7. ウィザードの「**エンド・エンティティー証明書および CA 証明書の選択 (Select end entity certificate and CA Certificate)**」ページで、次の値を入力します。
   - **鍵ストアに複数のエンド・エンティティー証明書が含まれています。アップロードする証明書を選択しますか? (The keystore contains more than one End Entity certificate. Select the certificate to be uploaded?)** - ドロップダウンに、すべてのエンド・エンティティー証明書のリストがあります。アップロードする証明書を選択します。
   - **パスワード** - 鍵ストアにパスワードがある場合は、このチェック・ボックスを選択し、テキスト・ボックスにパスワードを入力します。
   - **アップロードするルートおよび中間 CA 証明書のリストの選択 (Select the List of Root and Intermediate CA certificates to be uploaded)** - リスト・ボックスから、アップロードするルートおよび中間 CA 証明書を選択します。
8. 「**次へ**」をクリックして、ウィザードの「**証明書の詳細**」ページに進みます。
9. ウィザードの「**証明書の詳細**」ページで、次の証明書の詳細情報を入力します。
   - **リーフ証明書名** - リーフ証明書の名前。このフィールド名は、証明書がリーフ証明書か、ルート CA 証明書か、あるいは中間 CA 証明書かによって変化します。
   - **説明** - リーフ証明書の説明。
   - **証明書タイプ** - この証明書を証明書タイプと関連付けます。サポートされるタイプは、「デジタル署名」、「デジタル署名の検証」、「暗号化」、「復号」、「SSL サーバー」、および「SSL クライアント」です。
   - **証明書の使用** - 証明書の使用を関連付けます。値は、「1 次」と「2 次」です。
   - **動作モード** - 操作のモードを入力します。
   - **状況** - アップロードした後に証明書を使用可能にするか使用不可にするかを基に、有効または無効を選択します。「次へ」ボタンは、証明書が使用可能になっている場合にのみ有効になります。
   - **セットの管理** - 証明書を、既存のセットまたは新規セットに関連付けることができます。証明書が 2 次証明書の場合は、既存のセットにのみ関連付けることができます。証明書は、暗号化のタイプの内部パートナー、または SSL (着信クライアント認証) あるいは署名 (検証) のタイプの外部パートナーの任意のセットに関連付けることができます。
10. 「**次へ**」をクリックして、ウィザードの「セット」ページに進みます。証明書が 1 次の場合は、セットを作成してその証明書をセットおよびパートナー接続に関連付ける必要はありません。「**新規セットの作成 (Create new set)**」チェック・ボックスを選択した場合は、ウィザードの「**新規セットの作成 (Create New Set)**」ページがオープンします。それ以外の場合は、ウィザードの「**既存のセットに追加 (Add to Existing)**」 ページがオープンします。ファイルに内

部パートナーの秘密鍵が含まれている場合、または SSL / デジタル署名に使用される外部パートナーの公開証明書が含まれている場合は、「**終了**」をクリックすることができます。

11. ウィザードの「**新規セットの作成 (Create New Set)**」ページで、新規セットの詳細情報を入力します。1 次証明書の場合は、セットを作成して証明書をそのセットと関連付ける必要はありません。次の値を入力します。
    - **セット名** - セットの名前。
    - **説明** - セットの説明。
    - **状況** - 有効または無効を選択。これが無効になっている場合、「**次へ**」ボタンは有効になりません。
    - **デフォルト設定にする** - このセットをデフォルトにする場合は、このチェック・ボックスを選択します。
12. ウィザードの「**既存のセットに追加**」ページで、証明書を追加するセットを選択します。次の値を入力します。
    - **選択済み証明書タイプに使用可能なセットのリストから選択 (Select from the list of Sets available for the selected Certificate type)** - リストから、証明書に追加するセットを選択します。
    - **デフォルト設定にする** - このセットをデフォルトにする場合は、このチェック・ボックスを選択します。
13. 「**新規セットの作成 (Create New Set)**」または「**既存セットに追加 (Add to Existing Set)**」から、「**次へ**」をクリックして、ウィザードの「**デフォルト設定**」ページに進みます。「**次へ**」ボタンは、セットの状況が使用可能の場合にのみ有効になります。
14. アップロード後に証明書を使用可能にするか使用不可にするかを基に、「**状況**」で「**有効**」または 「**無効**」を選択します。

    **注:** 前のページ (「新規セットの作成 (Create new set)」または「既存のセットに追加 (Add to exisiting set)」) で「**デフォルト・セットの作成 (Make default set)**」チェック・ボックスを選択した場合は、セットを動作モードに関連付ける必要があります。これは、動作モードに対する証明書の使用を表示します。内部パートナーについては、暗号化は使用不可になります。外部パートナーについては、SSL クライアントとデジタル署名が使用不可になります。
15. 「**次へ**」をクリックして、ウィザードの「構成」ページに進みます。「**終了**」をクリックしたのに、欠落しているルートまたは中間 CA 証明書がある場合は、アップロードするように求めるプロンプトが表示されます。プロンプト・ウィンドウで「はい」をクリックすると、ウィザードの最初のページがオープンします。後の段階でアップロードしたい場合は、「**キャンセル**」をクリックしてください。
16. ウィザードの「構成」ページで、次の値を入力します。

    **注:** 「構成」ページには、動作モードに対する証明書 (セット) の使用法のリストが表示されます。すべてに対して現在のセット名が定義済みですが、それらの名前はリセットすることができます。
    - **パートナーから (From Partner)** - このフィールドには、内部パートナーの値が定義済みです。

- **パートナーへ (To Partner)** - このドロップダウンには、すべての外部パートナーのリストが定義済みです。「すべて (All)」の値を選択して、すべての外部パートナーを組み込むこともできます。
- **パッケージから (From Package)** - ドロップダウンから、内部パートナーの文書フロー定義オブジェクトのパッケージを選択します。
- **パッケージへ (To Package)** - リストから、外部パートナーの文書フロー定義のパッケージを選択します。

17. セットを他のパートナー接続に関連付けたい場合は、「**接続の追加を続行 (Add more connections)**」をクリックします。
18. 「**2 次証明書の追加 (Add Secondary Certificate)**」をクリックして、現行セットに 2 次証明書を追加します。
19. 「**終了**」をクリックして、証明書をアップロードします。欠落しているルートまたは中間 CA 証明書がある場合は、アップロードするように求めるプロンプトが表示されます。プロンプト・ウィンドウで「はい」をクリックすると、ウィザードの最初のページがオープンします。後の段階でアップロードしたい場合は、プロンプト・ウィンドウで「**キャンセル**」をクリックします。

## 証明書セットの作成

### このタスクについて

証明書セットは、次のセキュリティー機能のために導入されました。

- 内部パートナーから外部パートナーへのアウトバウンド・メッセージの SSL クライアント認証。
- 内部パートナーから外部パートナーへのアウトバウンド・メッセージへのデジタル署名の追加。
- 内部パートナーから外部パートナーへのアウトバウンド・メッセージの暗号化。
- セットは、WebSphere Partner Gateway トラストストアでの外部パートナーの SSL クライアント認証証明書の検証、外部パートナーのデジタル署名の検証、および内部パートナー向けの暗号化されたメッセージの暗号化解除など、インバウンド・シナリオには使用されません。

新規証明書を作成するには、以下の手順に従ってください。

1. コンソールで、「**プロファイル**」 > 「**パートナー**」 > 「**証明書リスト**」 > 「**証明書セット・リスト**」 > 「**セットの作成**」 にナビゲートします。
2. 「**証明書**」 > 「**証明書セット**」 > 「**セットの作成**」をクリックします。
3. 新規証明書セットの「**セット名**」と「**説明**」を入力します。
4. 「**証明書タイプ**」を設定します。
5. 「**有効**」または「**無効**」チェック・ボックスを選択して、「**証明書セット**」を使用可能または使用不可にします。
6. 「**証明書のロード**」をクリックします。

**注:** 「**1 次証明書**」と「**2 次証明書**」ドロップダウンの項目は、選択された「**証明書タイプ**」を基にしています。既に作成されているが、どのセットにも関連付

けられていない証明書がある場合は、それらの証明書を現在作成しているセットに追加することができます。証明書リストが空の場合、ドロップダウンは空になります。

7. ドロップダウンから「**1 次証明書**」と「**2 次証明書**」を選択します。
8. 「**保存**」をクリックします。

## 証明書セットの削除

### このタスクについて

1. コンソールで、「**プロファイル**」>「**パートナー**」>「**証明書セット・リスト**」にナビゲートします。このビューには、そのパートナーに対して作成されているすべての証明書がリストされます。
2. 「**削除**」アイコンをクリックします。削除操作の前に、接続でのこのセットに対するすべての参照を変更済みであることを確認します。
3. このセットが 1 つ以上の接続によって使用されている場合は、警告メッセージが表示されます。特定の証明書がどこで使用されているかを確認するには、『証明書の使用場所』を参照してください。
4. 警告メッセージ・ウィンドウで「**OK**」をクリックして削除するか、「**キャンセル**」をクリックして証明書セットの削除を打ち切ります。

## 証明書の使用場所

コンソールで、「**プロファイル**」 > 「**パートナー**」 > 「**証明書リスト**」 > 「**証明書セット・リスト**」 > 「**使用場所**」 にナビゲートします。その結果、ビューには次の詳細が表示されます。

- パートナーから (From partner)
- パートナーへ (To Partner)
- パッケージから (From package)
- パッケージへ (To Package)
- SSL クライアント
- デジタル署名
- デジタル署名の検証
- 暗号化
- 復号
- 有効期間 (Validity)

**注:** 次の理由により、証明書が無効である場合があります。1 次証明書がない場合、1 次証明書が使用不可になっている場合、セットが使用不可になっている場合、1 次の有効期限が切れていて 2 次がない場合、および 1 次と 2 次が両方とも有効期限切れになっている場合、証明書は無効です。

## FTP スクリプト記述レシーバー/宛先用の SSL の設定

FTP スクリプト記述レシーバーについては、SSL クライアント認証がハブ・オペレーター・プロファイルにロードされます。内部パートナーに対して証明書がロードされている場合でも、それによってグローバル設定がオーバーライドされることはありません。

## すべての内部パートナーに対するデフォルト証明書セットの提供

WebSphere Partner Gateway では複数の内部パートナーがサポートされているため、それぞれの内部パートナーは秘密鍵をアップロードする必要があります。組織の部門内で証明書を組織単位と共用することを望んでいる場合は、各内部パートナーの証明書をアップロードする必要があります。これを簡単にするために、特定の証明書がすべての内部パートナーに使用されるようにデフォルト・オプションを提供することができます。

コンソールで、「**証明書**」>「**証明書のアップロード**」にナビゲートします。証明書をアップロードし、証明書タイプ、使用法、および動作モードの詳細情報を提供します。こうした情報を指定して保管すると、ハブ・オペレーター・レベルで証明書/鍵がロードされます。実行時に証明書がない場合は、ハブ・オペレーター・レベルで提供されたデフォルトが使用されます。

## 証明書の要約

表 30 に、WebSphere Partner Gateway で証明書を使用する方法を要約します。証明書のロケーションは括弧 ( ) で示されています。

*表 30. 証明書要約情報*

| メッセージ配信方法 (注 1 を参照) | ハブ・オペレーター証明書 | パートナーから証明書と CA を取得 | CA (注 2 を参照) | 証明書をパートナーに提供 (注 3 を参照) | コメント |
|---|---|---|---|---|---|
| インバウンド SSL | WebSphere Application サーバー側 SSL でインストール。(WebSphere Application Server 鍵ストアに置きます。) | パートナーの自己署名証明書。 | クライアント認証が使用されている場合のみ必要です。(CA または自己署名証明書を WebSphere Application Server トラストストアに置きます。) | 自己署名の場合はハブ・オペレーターの証明書、CA 認証の場合は必要に応じて CA ルート証明書。 | |
| アウトバウンド SSL | クライアント認証が使用されている場合。(WebSphere Partner Gateway) | パートナーのサーバー・サイド証明書または CA 認証の場合は CA ルート証明書。 | WebSphere Partner Gateway | 自己署名の場合はハブ・オペレーターの証明書、サード・パーティーによって署名されている場合は CA 証明書。 | |

*表 30. 証明書要約情報 (続き)*

| メッセージ配信方法 (注 1 を参照) | ハブ・オペレーター証明書 | パートナーから証明書と CA を取得 | CA (注 2 を参照) | 証明書をパートナーに提供 (注 3 を参照) | コメント |
|---|---|---|---|---|---|
| インバウンド復号 | 秘密鍵 (WebSphere Partner Gateway) | なし | 証明書が CA 証明書の場合、ルート/中間の証明書として CA 証明書をアップロードする必要があります。 | ハブ・オペレーター証明書 | メッセージの暗号化解除用 |
| インバウンド・デジタル署名検証 | なし | デジタル署名に使用する証明書の検証用の証明書。(WebSphere Partner Gateway) | WebSphere Partner Gateway | NA | 検証および否認防止用 |
| アウトバウンド暗号化 | なし | パートナーから取得した証明書を使用します。(証明書はパートナーのプロファイルにインストールされます) | 自己署名でない場合は、クライアント証明書の CA 証明書チェーン | なし | アウトバウンド・メッセージの暗号化用 |
| アウトバウンド署名 | 秘密鍵および証明書 (WebSphere Partner Gateway) | なし | CA 証明書チェーン。 | パートナーによってはオプションです。WebSphere Partner Gateway 証明書を提供します。 | |
| ビジネス ID 検証への証明書 | なし | パートナー・プロファイルにロード | | | SSL クライアント検査の実行時にこの証明書がこのビジネス ID 用であることを確認します。 |

**注:**

1. インバウンド・メッセージは、パートナーから WebSphere Partner Gateway に着信するメッセージです。アウトバウンド・メッセージは、WebSphere Partner Gateway からパートナーへ発信されるメッセージです。
2. 証明書が CA 発行である場合は、発行される CA 証明書を取得し保管する必要があります。これは、ハブ・オペレーター証明書またはパートナーの証明書に適用されます。
3. 秘密鍵が含まれている場合、この証明書は秘密鍵に対応しています。

# WebSphere Partner Gateway での PEM 形式の証明書と鍵の使用

このセクションでは、PEM でエンコードされた鍵と証明書の使用法について説明します。

## PEM 形式の秘密鍵の使用

PEM 形式の秘密鍵があり、それを WebSphere Partner Gateway にアップロードする場合、アップロードを可能にするにはその秘密鍵を PKCS#8 形式に変換する必要があります。

これは、OpenSSL ツールを使用して実行できます。

PEM 形式の鍵を PKCS#8 形式に変換するには、次のコマンドを使用します。

```
openssl pkcs8 -topk8 -in usr.key -out usr.p8 -outform DER
```

このコマンドは、OpenSSL を使用して作成された鍵に対して機能します。

OpenSSL は、Linux ディストリビューションで入手できます。Web サイト http://www.openssl.org からダウンロードすることもできます。

## PEM 形式の証明書の使用

WebSphere Partner Gateway では、証明書を PEM 形式でアップロードできます。OpenSSL を使用して生成された PEM 形式の証明書について、機能します。

## WebSphere Partner Gateway での PKCS#7 でエンコードされた証明書

### このタスクについて

Windows では、PKCS#7 形式でエンコードされた証明書 (.p7b ファイル) がある場合、以下のステップを実行して、.p7b ファイルから証明書を抽出します。

1. .p7b ファイルをダブルクリックします。
2. ナビゲーション・パネルで、フォルダー・ツリーを展開し、「**証明書**」をクリックします。ファイルに含まれている証明書のリストが、右側に表示されます。
3. 証明書をファイル・システムにコピーするために、証明書をダブルクリックします。証明書の詳細が表示されます。
4. 証明書の詳細で、「**詳細**」タブをクリックします。
5. 「**ファイルにコピー (Copy to file)**」をクリックして、ファイルをファイル・システムにコピーします。
6. 証明書を DER エンコード・ファイルとしてエクスポートします。

# FIPS 準拠

WebSphere Partner Gateway は FIPS (連邦情報処理標準) の標準、厳密にいうと FIPS 140-2 標準に対応しています。**IBMJCEFIPS** は、FIPS 対応の JCE プロバイダーです。**IBMJSSE2 JSSE** プロバイダーは **IBM JCE** を使用し、暗号方式のコードを含んでいません。したがって、FIPS 準拠についての認証は必要ありません。**IBMJSSEFIPS JSSE** プロバイダーは FIPS 準拠ですが、WebSphere Partner

Gateway では **IBMJSSE2** プロバイダーの使用をお勧めします。なぜなら、こちらの方が最新のプロバイダーであり、より多くのアルゴリズムをサポートしており、保守容易性が向上しているからです。製品は FIPS モードまたは非 FIPS モードのいずれでも実行できます。 FIPS モードが構成されているのに、FIPS が承認していないアルゴリズムが使用された場合は、エラー・イベントが生成され、文書のトランザクションが停止されます。PKCS#12 アルゴリズムは FIPS で承認されていません。したがって、PKCS#12 ファイルは FIPS モードでアップロードすることはできません。FIPS またはデフォルト・モードで WesbSphere Partner Gateway を実行するよう構成するためには、管理者でなければなりません。FIPS モードの場合、PKCS#12 は iKeyman を使用して JCEKS または JKS 形式で WebSphere Partner Gateway のコンソールにアップロードすることができます。

FIPS モードは JKS および JCEKS 鍵ストアをサポートしていますが、PKCS#12 鍵ストアはサポートしていません。コンソールは、JKS または JCEKS 形式での証明書および鍵のアップロードを許可します。「**鍵ストアのアップロード (Keystore upload)**」画面で、「**鍵ストアの形式 (Keystore format)**」ドロップダウンから形式を選択してください。「**鍵ストアの形式 (Keystore format)**」ドロップダウンで選択可能な値は、PKCS#12、JKS、および JCEKS です。

## FIPS モードで稼働するように WebSphere Partner Gateway を構成

### このタスクについて

FIPS モードで稼働するように WebSphere Partner Gateway を構成するには、以下の手順に従ってください。

1. **java.security** ファイルに FIPS プロバイダーを設定します。
2. WebSphere Partner Gateway のコンソールで、**bcg.FIPSMode** システム・プロパティーを「true」に設定します。
3. java.security ファイルで、IBMJCE プロバイダーの前に IBMJCEFIPS プロバイダーを設定します。java.security ファイルは、<WAS Installation>/java/jre/lib/security ディレクトリーにあります。
4. JSSE ソケット・ファクトリーおよびサーバー・ソケット・ファクトリーに対して FIPS 使用可能のソケット・ファクトリー・クラスを設定します。
5. サーバーを再始動します。

   **注:** 製品が FIPS モードで実行されていることを示す通知イベントが生成されます。

## デフォルト・モードで稼働するように WebSphere Partner Gateway を構成

### このタスクについて

デフォルト・モードで稼働するように WebSphere Partner Gateway を構成するには、以下の手順に従ってください。

1. WebSphere Partner Gateway のコンソールで、**bcg.FIPSMode** システム・プロパティーを「False」に設定します。

2. 以下の説明に従って、**java.security** ファイル内の JSSE ソケット・ファクトリー、サーバー・ソケット・ファクトリー、およびプロバイダーの設定をリセットします。
   a. 各サーバーの汎用 JVM プロパティーから **com.ibm.jsse2.JSSEFIPS=true** システム・プロパティーを除去します。
   b. 以下のプロパティーの値を元の値にリセットします。
      - ssl.SocketFactory.provider
      - ssl.SocketFactory.provider
   c. すべての WAS インストールについて、**java.security** ファイル内で IBMJCEFIPS プロバイダーをコメントし、そのプロバイダーの再番号付け (1 から開始) を行います。
3. サーバーを再始動します。

**注:** モードを示す通知イベントが生成されます。デフォルト・モードでは、FIPS が承認していないアルゴリズムを含め、サポートされるすべてのアルゴリズムを使用することができます。

## FIPS モード用に IBM JSSE プロバイダーを構成

### このタスクについて

FIPS 用に IBM JSSE プロバイダーを構成するには、以下の手順に従ってください。

1. **com.ibm.jsse2.JSSEFIPS** システム・プロパティーを「True」に設定します。これは、WAS 管理コンソールを使用してアプリケーション・サーバーの JVM システム・プロパティーを設定することにより実行できます。ページ「<Server>/Java およびプロセス管理/プロセス定義/Java 仮想計算機」にナビゲートし、プロパティー **-Dcom.ibm.jsse2.JSSEFIPS=true** を設定します。すべてのサーバーに対してこの設定を行う必要があります。
2. 以下の IBMJSSE2 プロバイダーのセキュリティー・プロパティーを、すべての JSSE 要求を処理するように設定します。
   - ssl.SocketFactory.provider = com.ibm.jsse2.SSLSocketFactoryImpl
   - ssl.ServerSocketFactory.provider = com.ibm.jsse2.SSLServerSocketFactoryImpl
3. IBMJCEFIPS provider, com.ibm.crypto.fips.provider.IBMJCEFIPS を、プロバイダー・リストの IBMJCE プロバイダーの前に追加します。IBMJCE プロバイダーは鍵ストア・サポートに必要なので、除去しないでください。

   **注:** IBMJSSE2 が FIPS モードの場合は、TLS プロトコルのみがサポートされます。

## FIPS および非 FIPS モードでサポートされるアルゴリズム

FIPS では、以下のアルゴリズムがサポートされます。

- Diffie-Hellman
- RSA、DSA
- SHA-1、SHA-256、SHA-384、SHA-512
- AES、DES、TDES (Triple DES)

- FIPS 186-2 – 疑似乱数生成のためのアルゴリズム
- Transport layer security: TLSv1
- 鍵ストア形式: JKS、JCEKS
- 鍵付きメッセージのダイジェスト・アルゴリズム: hmac-sha1

WebSphere Partner Gateway では、以下のアルゴリズムがサポートされます。

- 非対称暗号方式: RSA、DSA
- ハッシュ関数: SHA-1、MD5、SHA256、SHA512、RIPEMD160
- 対称暗号方式: AES、DES、3DES、RC2 (すべて CBC モード)
- PRNG: IBMSecureRandom
- 署名アルゴリズム: dsa-sha1、rsa-sha1
- 鍵付きメッセージのダイジェスト・アルゴリズム: hmac-sha1
- Transport Layer Security: SSLv3、TLSv1
- 鍵ストア形式: PKCS#12
- 鍵付きメッセージのダイジェスト・アルゴリズム: hmac-sha1

以下のアルゴリズムは FIPS ではサポートされていませんが、WebSphere Partner Gateway でサポートされます。

- ハッシュ関数: MD5、RIPEMD160
- 対称暗号方式: RC2、RC5
- PRNG: デフォルト PRNG アルゴリズムは FIPS に承認されていない可能性があります。
- IBMSecureRandom PRNG プロバイダー (WebSphere Partner Gateway のすべてのケース)。
- Transport Layer Security: SSLv3
- 鍵ストア形式: PKCS#12

# 第 14 章 アラートの管理

WebSphere Partner Gateway のアラートは、受信した伝送のボリュームに異常な変動が見られたことを主要な担当者に通知するため、またはビジネス文書処理のエラーが発生したときに使用します。

ビューアー・モジュールのオプションであるイベント・ビューアーは、処理エラーをさらに識別し、解決するのに役立ちます。

## アラートの概要

アラートは、サブスクライブした連絡先または主要な担当者の配布先リストに送信されるテキスト・ベースの E メール・メッセージで構成されています。アラートは、システム・イベント (イベント・ベースのアラート) の発生または予期される文書フロー・ボリューム (ボリューム・ベースのアラート) に基づいています。

- **ボリューム・ベースのアラート**は、伝送ボリュームの増加または減少の通知を受信するために使用します。

  例えば、ユーザーが外部パートナーである場合、営業日に内部パートナーから何も伝送を受信しなかった場合に通知するような、ボリューム・ベースのアラートを作成することができます (「ボリューム」を「ボリュームをゼロにリセットする」に設定し、「頻度」を「毎日」に設定し、「曜日」オプションで「月曜から金曜 (Mon through Fri)」を選択します)。このアラートにより、内部パートナーのネットワーク伝送の障害を明らかにすることができます。

  ユーザーが外部パートナーである場合、内部パートナーからの伝送数が通常のレートを超えたときに警告する、ボリューム・ベースのアラートを作成することもできます。例えば、通常 1 日におよそ 1000 回伝送を受信している場合、「予想ボリューム (Expected Volume)」を 1000 に設定し、「偏差率 (%)」を 25% に設定することができます。1 日に 1250 回を超える伝送を受信したとき、および伝送のボリュームが 750 を下回ったときに、アラートがそのことを通知します。このアラートによって、内部パートナーの部門で需要が増加し、いずれはユーザーの環境にサーバーを追加する必要が生じる可能性があることが識別できます。ボリューム・ベースのアラートについて詳しくは、309 ページの『 ボリューム・ベースのアラートの作成』を参照してください。

  **注:**

  1. ボリューム・ベースのアラートでは、アラートの作成時に選択した文書タイプに関してボリュームをモニターします。WebSphere Partner Gateway は、アラートで選択した文書タイプを含む文書のみを調べ、すべてのアラート基準が満たされた場合のみアラートを生成します。
  2. 外部パートナーは、内部パートナーへ送信された文書のボリュームについてのみボリューム・ベースのアラートを作成できます。外部パートナーが内部パートナーからの着信文書のボリュームに関してボリューム・ベースのアラートを設定するためには、外部パートナーはハブ管理者に対して、外部パートナーの代わりにボリューム・ベースのアラートを設定し、外部パートナーをアラート

所有者として指定するように依頼します。内部パートナーは、外部パートナーに送信するボリューム・ベースのアラートも作成することができます。

- **イベント・ベースのアラート**は、文書処理中のエラー発生時に通知を受信するために使用します。例えば、検証エラーのため、または重複する文書を受信したために文書の処理が失敗した場合に通知するアラートを作成できます。証明書の有効期限が近づいたときに通知するアラートを作成することもできます。

  WebSphere Partner Gateway の事前定義イベント・コードを使用して、イベント・ベースのアラートを作成します。デバッグ、情報、警告、エラー、重大という 5 つのイベント・タイプがあります。各イベント・タイプ内には、多くのイベントがあります。「アラート: イベント」ページで、事前定義イベントを表示および選択できます。例えば、「240601 AS 再試行の失敗」、「108001 証明書ではありません」などです。イベント・ベースのアラートについて詳しくは、311 ページの『 イベント・ベースのアラートの作成』を参照してください。

**ヒント:**

- 予想される外部パートナーまたは内部パートナーの伝送ボリュームが動作限界を下回る場合に通知を受信するには、ボリューム・ベースのアラートを使用します。このアラートにより、外部パートナーまたは内部パートナーのネットワーク伝送の障害を明らかにすることができます。
- 文書処理中のエラーの通知を受信するには、イベント・ベースのアラートを使用します。例えば、検証エラーにより文書の処理が失敗した場合に通知する、イベント・ベースのアラートを作成できます。

**注:** アラートを送信するには、アラートに対応するように E メール・サーバーを構成する必要があります。アラートは、「**システム管理**」 >「**DocMgr の管理**」 >「**アラート・エンジン**」をクリックすると表示される「アラート・エンジン属性」ページで構成します。アラート E メール・サーバーの構成について詳しくは、「*WebSphere Partner Gateway パートナー・ガイド*」の『アラート・メール・アドレスの更新 (Updating alert mail addresses)』を参照してください。

## アラートの詳細および連絡先の表示または編集

### このタスクについて

内部パートナーは、アラート所有者 (アラートの作成者) に関係なく、すべてのアラートを表示できます。

1. 「**アカウント管理**」 >「**アラート**」をクリックします。「アラートの検索」ページが表示されます。
2. ドロップダウン・リストから検索条件を選択し、「アラート名」を入力します。検索条件を選択せずに、「**検索**」をクリックすることもできます (すべてのアラートが表示されます)。
3. 「**検索**」をクリックします。「アラート検索結果」ページが表示されます。
4. 「詳細の表示」アイコンをクリックして、アラートの詳細を表示します。
5. 「編集」アイコンをクリックして、アラートの詳細を編集します。
6. 必要に応じて、情報を編集します。
7. 「**通知**」タブをクリックします。

8. パートナー (内部パートナーまたはハブ管理者のみ) を選択します。内部パートナーは、アラート所有者に関係なく、すべてのアラートを表示できます。
9. 必要に応じて、このアラートの連絡先を編集します。
10. 「**保存**」をクリックします。

## アラートの検索

### このタスクについて

1. 「**アカウント管理**」 >「**アラート**」をクリックします。「アラートの検索」ページが表示されます。
2. ドロップダウン・リストから検索条件を選択し、「アラート名」を入力します。検索条件を選択せずに、「**検索**」をクリックすることもできます (すべてのアラートが表示されます)。

*表 31. パートナーのアラート検索条件*

| 値 | 説明 |
|---|---|
| アラート・タイプ | ボリューム、イベント、またはすべてのアラート・タイプ。 |
| アラート名 | アラートの名前。 |
| アラート状況 | 有効なアラート、無効なアラート、またはすべてのアラート。 |
| サブスクライブ済み連絡先 | アラートの割り当てられた連絡先。選択項目は「サブスクライバーあり」、「サブスクライバーなし」、および「すべて」です。 |
| ページごとの結果件数 | 検索結果の表示方法を制御します。 |

*表 32. 内部パートナーおよびハブ管理者のアラート検索条件*

| 値 | 説明 |
|---|---|
| アラート所有者 | アラートの作成者。 |
| アラート・パートナー | アラートが適用されるパートナー。 |
| アラート・タイプ | ボリューム、イベント、またはすべてのアラート・タイプ。 |
| アラート名 | アラートの名前。 |
| アラート状況 | 有効なアラート、無効なアラート、またはすべてのアラート。 |
| サブスクライブ済み連絡先 | アラートの割り当てられた連絡先。選択項目は「サブスクライバーあり」、「サブスクライバーなし」、および「すべて」です。 |
| ページごとの結果件数 | 検索結果の表示方法を制御します。 |

3. 「**検索**」をクリックします。検索条件を満たすアラートがあれば、それらのリストが表示されます。

## アラートの使用不可化および使用可能化

1. 「**アカウント管理**」 >「**アラート**」をクリックします。「アラートの検索」ページが表示されます。
2. ドロップダウン・リストから検索条件を選択し、「アラート名」を入力します。
3. 「**検索**」をクリックします。検索条件を満たすアラートがあれば、それらのリストが表示されます。

4. アラートを探し出し、「状況」の下の「**無効**」または「**有効**」をクリックします。ハブ管理者およびアラート所有者 (アラートの作成者) のみが、アラートの状況を編集する権限を持っています。

## アラートの除去

1. 「**アカウント管理**」 >「**アラート**」をクリックします。「アラートの検索」ページが表示されます。
2. ドロップダウン・リストから検索条件を選択し、「**アラート名**」を入力します。
3. 「**検索**」をクリックします。検索条件を満たすアラートがあれば、それらのリストが表示されます。
4. アラートを探し出し、「削除」アイコンをクリックして削除します。ハブ管理者およびアラート所有者 (アラートの作成者) のみが、アラートを除去できます。

## 既存のアラートへの新規連絡先の追加

### このタスクについて

1. 「**アカウント管理**」 >「**アラート**」をクリックします。「アラートの検索」ページが表示されます。
2. ドロップダウン・リストから検索条件を入力し、「アラート名」を入力します。
3. 「**検索**」をクリックします。検索条件を満たすアラートがあれば、それらのリストが表示されます。
4. 「詳細の表示」アイコンをクリックして、アラートの詳細を表示します。
5. 「編集」アイコンをクリックして、アラートの詳細を編集します。
6. 「**通知**」タブをクリックします。
7. パートナー (内部パートナーおよびハブ管理者のみ) を選択します。
8. 追加したい連絡先が「連絡先」テキスト・ボックスにリストされている場合、その連絡先を選択して、「**サブスクライブ**」をクリックします。13 (309 ページ)に進みます。

   追加したい連絡先が「連絡先」テキスト・ボックスにリストされていない場合、「**連絡先に新規項目を追加 (Add New Entry to Contacts)**」をクリックします。「新規連絡先の作成」ポップアップ・ウィンドウが表示されます。

   「連絡先に新規項目を追加 (Add New Entry to Contacts)」リンクは、パートナーがハブ・オペレーターの場合にのみ選択可能です。
9. 連絡先の名前、E メール・アドレス、電話番号、および FAX 番号を入力します。
10. 連絡先のアラート状況を選択します。
    - システムがこのアラートを生成したときに、この連絡先に E メール・メッセージが送信されるようにするには、「**有効**」を選択します。
    - システムがこのアラートを生成したときに、この連絡先に E メール・メッセージが送信されないようにする場合は、「**無効**」を選択します。
11. 連絡先を表示する範囲を選択します。

- その連絡先が自分の組織に対してのみ表示されるようにするには、「**ローカル**」を選択します。
- その連絡先がハブ管理者および内部パートナーに対して表示されるようにするには、「**グローバル**」を選択します。これらの関係者はどちらも、連絡先をアラートにサブスクライブできます。

12. 「**保存**」をクリックして、連絡先を保存します。連絡先を保存し、このアラートの連絡先リストにその連絡先を追加するには、「**保存してサブスクライブ (Save and Subscribe)**」をクリックします。
13. 「**保存**」をクリックします。

## ボリューム・ベースのアラートの作成

### このタスクについて

1. 「**アカウント管理**」 >「**アラート**」をクリックします。「アラートの検索」ページが表示されます。
2. ページの右上隅にある「**作成**」をクリックします。「アラートの定義 (Alerts Define)」タブが表示されます。
3. 「**アラート・タイプ**」として「**ボリューム・アラート**」を選択します (これがデフォルト設定です)。ボリューム・アラート用の適切なテキスト・ボックスが表示されます。
4. アラートの「**アラート名**」を入力します。
5. 「**テキスト**」にカスタムのビジネス・テキストを入力します。アラート・イベントが生成されると、このメッセージが合わせて送信されます。
6. アラートの「**アラート所有者**」を選択します。
7. ボリューム・ベースのアラートを作成する権限を持つ「**パートナー**」 (内部パートナーおよびハブ管理者のみ) を選択します。
8. ドロップダウン・リストから、「**パッケージ**」、「**プロトコル**」、および「**文書タイプ**」を選択します。選択したパッケージ、プロトコル、および文書タイプは、ソース外部パートナーのパッケージ、プロトコル、および文書タイプと一致していなければなりません。
9. 3 つのボリューム・オプション (「予想」、「範囲」、または「ボリュームをゼロにリセットする」) のいずれかを選択してから、10 (310 ページ) に進みます。
   - 「**予想**」 - 文書タイプ・ボリュームが正確な数量から逸脱したときにアラートが生成されるようにしたい場合は、「予想」を選択します。予想される文書タイプ・ボリュームについてのアラートを作成するには、以下の手順を実行します。
     a. 「ボリューム」テキスト・ボックスに、10 (310 ページ) で選択した時間フレーム内に受信することを予想する文書タイプの数を入力します。正数のみを入力してください。負の数値を入力すると、アラートは機能しません。
     b. 「偏差率 (%)」テキスト・ボックスに、文書タイプ・ボリュームが逸脱可能な制限値 (これを超えるとアラートがアクティブになる) を定義する数値を入力します。以下に例を示します。

- 「ボリューム」が 20、「偏差率 (%)」が 10 である場合は、文書フロー・ボリュームが 18 を下回るか、22 を超えると、アラートがトリガーされます。
- 「ボリューム」が 20、「偏差率 (%)」が 0 である場合は、文書フロー・ボリュームが 20 以外であれば、アラートがトリガーされます。

- **「範囲」**。文書フロー・ボリュームが最小値から最大値までの範囲から外れる場合にアラートを生成するには、「範囲」を選択します。値の範囲に基づいてアラートを作成するには、以下の手順を実行します。
  a. 「最小」テキスト・ボックスに、10 で選択した時間フレーム内に受信することを予想する文書フローの最小数を入力します。アラートは、文書フロー・ボリュームがこの量を下回った場合のみトリガーされます。
  b. 「最大」テキスト・ボックスに、10 で選択した時間フレーム内に受信することを予想する文書フローの最大数を入力します。

  **注:** ボリューム範囲に基づいてアラートを作成する場合は、「最小」テキスト・ボックスと「最大」テキスト・ボックスの両方に入力する必要があります。
- **「ボリュームをゼロにリセットする」**。10 で選択した時間フレーム内に文書フローが発生しなかった場合にアラートをトリガーするには、「ボリュームをゼロにリセットする」を選択します。

10. アラート生成のために文書フロー・ボリュームをモニターする際にシステムが使用する時間フレーム (頻度) として、「毎日」または「範囲」のいずれかを選択します。
    - **「毎日」**。1 日以上の実際の曜日または日にちに文書フロー・ボリュームをモニターするには、「毎日」を選択します。例えば、1 日以上の特定の曜日 (月曜日、月曜日と木曜日など) または日にち (1 日と 15 日など) にのみ文書フロー・ボリュームをモニターする場合は、「毎日」を選択します。
    - **「範囲」**。ある曜日から別の曜日まで、またはある日にちから別の日にちまでの文書フロー・ボリュームをモニターするには、「範囲」を選択します。例えば、月曜から金曜まで毎日、または各月の 5 日から 20 日まで毎日、文書フロー・ボリュームをモニターするには、「範囲」を選択します。
11. 次のステップで、選択された日の文書フロー・ボリュームをシステムがモニターする**開始時刻**および**終了時刻** (24 時間表記) を選択します。「範囲」の頻度が選択されると、範囲の最初の日の開始時刻から、範囲の最後の日の終了時刻まで、文書フロー・ボリュームがモニターされるため、注意してください。
12. アラート・モニターが行われる適切な曜日または日にちを選択します。頻度として「毎日」を選択した場合は、アラート・モニターが行われる実際の曜日または日にちを選択してください。頻度として「範囲」を選択した場合は、2 つの曜日を選択するか、2 つの日にちを選択して、アラート・モニターが行われる期間を指定します。
13. このアラートの**「アラート状況」**を選択します。「有効」または「無効」のいずれかです。
14. **「保存」**をクリックします。
15. **「通知」**タブをクリックします。

16. 「**編集**」アイコンをクリックします。
17. 「**パートナー**」 (内部パートナーおよびハブ管理者のみ) を選択します。
18. 追加したい連絡先が「連絡先」テキスト・ボックスにリストされている場合、その連絡先を選択して、「**サブスクライブ**」をクリックします。23 に進みます。

    追加したい連絡先が「連絡先」テキスト・ボックスにリストされていない場合、「**連絡先に新規項目を追加 (Add New Entry to Contacts)**」をクリックします。「新規連絡先の作成」ポップアップ・ウィンドウが表示されます。

    「連絡先に新規項目を追加 (Add New Entry to Contacts)」オプションは、アラート所有者に対してのみ表示され、アラート所有者に関連付けられた連絡先を作成します。この機能では、アラート所有者がアラート・パートナーの連絡先を追加することはできません。
19. **連絡先の名前**、**E メール・アドレス**、**電話番号**、および **FAX 番号**を入力します。
20. 連絡先の**アラート状況**を選択します。
    - システムがこのアラートを生成したときに、この連絡先に E メール・メッセージが送信されるようにするには、「**有効**」を選択します。
    - システムがこのアラートを生成したときに、この連絡先に E メール・メッセージが送信されないようにする場合は、「**無効**」を選択します。
21. 連絡先を表示する範囲を選択します。
    - その連絡先が自分の組織に対してのみ表示されるようにするには、「**ローカル**」を選択します。
    - その連絡先がハブ管理者および内部パートナーに対して表示されるようにするには、「**グローバル**」を選択します。これらの関係者はどちらも、連絡先をアラートにサブスクライブできます。
22. 連絡先を保存するには「**保存**」をクリックし、このアラートの連絡先リストにその連絡先を追加するには「**保存してサブスクライブ (Save Subscribe)**」をクリックします。
23. 「**保存**」をクリックします。

    **注:** ボリューム・ベースのアラートに加えられた変更は、元のモニター期間の終了後、次のモニター期間の日に有効になります。例えば、アラートが水曜日と木曜日の午後 1 時から 3 時までモニターするようになっているとします。水曜日の午後 4 時に、アラートが午後 5 時から 7 時までモニターするように変更されました。アラートは水曜日に 2 回モニターすることはありません。変更は木曜日に有効になります。

## イベント・ベースのアラートの作成

### このタスクについて

1. 「**アカウント管理**」 >「**アラート**」をクリックします。「アラートの検索」ページが表示されます。
2. ページの右上隅にある「**作成**」をクリックします。「アラートの定義 (Alerts Define)」タブが表示されます。

3. 「**アラート・タイプ**」の「**イベント・アラート**」を選択します。イベント・ベースのアラート用の適切なテキスト・ボックスが表示されます。
4. アラートの「**アラート名**」を入力します。
5. 「**テキスト**」にカスタムのビジネス・テキストを入力します。アラート・イベントが生成されると、このメッセージが合わせて送信されます。
6. アラートの「**アラート所有者**」を選択します。
7. アラートをトリガーする「**パートナー**」を選択します (このオプションを使用できるのは、内部パートナーおよびハブ管理者のみです)。アラートを、システム内のすべてのパートナーに関連付けるには、「任意のパートナー」オプションを選択します。アラート検索を実行し、「アラート・パートナー」として「任意のパートナー」を選択すると、特定のパートナーに関連付けられていないすべてのアラートが表示されます。
8. 「**イベント・タイプ**」を選択します。「デバッグ」、「情報」、「警告」、「エラー」、「重大」、または「すべて」のいずれかです。
9. 例えば「BCG240601 AS 再試行の失敗」、「108001 証明書ではありません」などのアラートをアクティブにする「**イベント名**」を選択します。証明書の有効期限が近づいたときに通知するアラートを作成するには、以下のいずれかを選択します。
   - BCG108005 証明書の有効期限が 60 日間
   - BCG108006 証明書の有効期限が 30 日間
   - BCG108007 証明書の有効期限が 15 日間
   - BCG108008 証明書の有効期限が 7 日間
   - BCG108009 証明書の有効期限が 2 日間

   **注:** イベントをここにリストするには、イベントがアラート可能でなければなりません。イベントをアラート可能にするには、320 ページの『アラート可能イベントの指定』を参照してください。
10. このアラートの状況を選択します。「有効」または「無効」のいずれかです。
11. 「**保存**」をクリックします。
12. 「**通知**」タブをクリックします。
13. 「**通知モード**」を選択します。「すべての関係者に通知」または「サブスクライブ済み連絡先にのみ通知」のいずれかです。サブスクライブ済み連絡先は、「***サブスクライブ済み連絡先にのみ通知***」モードにより通知されます。アラートを作成しているときに、アラート通知モードに「***すべての関係者に通知***」を選択すると、そのアラートが定義されているイベントのすべての関係者に通知が送信されます。イベントの関係者は、ソース・パートナー、ターゲット・パートナー、およびアラート所有者を結合した連絡先です。
14. 「**パートナー**」 (内部パートナーおよびハブ管理者のみ) を選択します。
15. 「**連絡先**」テキスト・ボックスにリストされた連絡先から、通知を送る連絡先を選択して、「**サブスクライブ**」をクリックします。
16. 以下の「送達のモード」を選択します。
    - 「**アラートの即時送信**」。このオプションを選択すると、アラート発生時にシステムが連絡先へアラート通知を送信します。重大なアラートの場合は、このオプションを使用します。

- 「**バッチ・アラート元**」。このオプションを選択すると、連絡先がアラート通知を受け取る時期を指定できます。重大でないアラートの場合は、このオプションを使用します。

  このセクションの「カウント」および「時間」という 2 つのオプションは、同時に指定できます。

  「**カウント**」オプションを選択した場合、常に「時間」オプションを選択する必要があります。
  - 選択した制限時間 (「時間」) 内にアラート数が「カウント」に達した場合、システムはアラート通知を生成します。
  - アラートが発生したが、選択した制限時間 (「時間」) 内にアラート数が「カウント」に達しなかった場合、システムは、制限時間の終わりにアラート通知を生成します。

  「**時間**」オプションは「カウント」オプションを指定しなくても使用できますが、「カウント」オプションは常に制限時間 (「時間」) に関連付ける必要があります。
  - 「**カウント**」。このオプションを選択する場合は、「時間」オプションも使用する必要があります。数値 (n) を入力します。選択した期間 (「時間」) 中に、ここで指定した数のアラートが発生すると、システムによってアラートの連絡先にアラート通知が送信されます。

    以下の例は、これらの 2 つのオプションがどのように機能するかを示すものです。

    この例では、「バッチ・アラート元」オプションで、「カウント」に 10 (10 回のアラート) および「時間」に 2 (2 時間) が設定されています。システムは、2 時間の期間中に 10 回アラートが発生するまで、または期間の終わりに達するまで、このアラートのすべての通知を保持します。

    2 時間のうちにアラート数が 10 に達した場合、システムはこのアラートのすべてのアラート通知を連絡先に送信します。

    アラートが発生したが、制限時間 (2 時間) 内に 10 個のアラートが発生しなかった場合、システムは、制限時間の終わりにアラートの連絡先へアラート通知を送信します。
  - 「**時間**」。時間数 (n) を選択します。システムは n 時間だけアラート通知を保持します。n 時間ごとに、保持されたすべてのアラート通知をシステムが連絡先へ送信します。

    例えば 2 を入力した場合、システムは、2 時間ごとに、このアラートのすべての通知を保持します。2 時間経過すると、システムはこのアラートのすべてのアラート通知を連絡先に送信します。

17. 「**保存**」をクリックします。

# 第 15 章 エラー・フローの開始

WebSphere Partner Gateway では、管理者は文書の処理中に発生する、失敗したイベントをモニターすることができます。文書の失敗は、レシーバーまたは文書マネージャーで起こる可能性があります。失敗した文書については、対応するエラーまたは重大イベントがイベント・エンジンに記録されます。アラートを作成して、1 人以上のサブスクライバーに E メールで通知することができます。

このほかに、管理者は内部パートナーか外部パートナー、あるいはその両方のパートナーに対してエラー文書フローを実際に開始することができます。このエラー文書は、エラー・イベントまたは重大イベントを基に、失敗した文書に対して開始されます。このエラー文書フローの形式は、WebSphere Partner Gateway 形式または Web サービス形式のいずれかになります。この形式は、イベントのエラー・フロー構成で構成することができます。

## エラー・フロー文書の構成

### このタスクについて

オペレーターはコンソールの「エラー・フロー」タブにより、特定のエラー・イベントに対してエラー・フローまたは Web サービス呼び出しを設定することができます。

1. 「**アカウント管理**」> 「**エラー・フロー**」タブにナビゲートします。エラー・フロー・リストに、それぞれのエラー・フローの表示アイコンおよび削除アイコンがあります。
2. 「**表示 (View)**」アイコンをクリックすると、読み取り専用モードでエラー・フロー構成画面が起動されます。
3. 構成の表示で「**編集**」アイコンをクリックし、エラー・フロー構成を編集します。
4. 編集モードでは、次の構成値が使用可能です。
   - **名前** - エラー・フロー文書構成の名前。
   - **送信側パートナー** - パートナー検索時にクリックし、パートナー名を選択します。このパートナーは内部パートナーまたは外部パートナーの場合があります。
   - **Pパートナー・タイプ** - ドロップダウンからパートナー・タイプを選択します。
   - **エラー・イベント** - このドロップダウンには、「エラー」または「*重大*」タイプのイベントのみがリストされます。
   - **エラー・フロー・タイプ** - これは、「エラー・フロー文書」または「*Web サービスの呼び出し*」のいずれかになります。
   - **送信先** - 障害が起こった文書の受信側を選択します。「*送信側*」または「*受信側*」あるいは「*両方*」を指定できます。
5. 「**保存**」をクリックします。

6. 取り消すには「**キャンセル**」をクリックします。
7. 構成されているエラー・フローに対する B2B 機能を使用可能にします。
8. Web サービスが起動されたら、対話を作成し、パートナー接続をアクティブ化します。

WebSphere Partner Gateway では、XML および Web サービスのエラー・フロー文書定義はデフォルトでアップロードされます。パートナーに対してこれらを使用可能にし、次の接続を作成することができます。

- ErrorFlowDocument XML 接続
- 文書スタイルに対して Web サービスでの ErrorFlowDocument
- RPC スタイルに対して Web サービスでの ErrorFlowDocument

## 制限および制約事項

1. Web サービスでのエラー・フロー文書には、次の制限があります。
   - Web サービス要求は、一方向要求でなければなりません。
   - バインディング・スタイルが **document** の場合、入力パラメーター・タイプは、BCGErrorFlowSchema.xsd に定義されているエレメント **ErrorFlowDocument** になります。
   - バインディング・スタイルが **rpc** の場合、入力パラメーター・タイプは **String** になり、入力パラメーターの数は 1 つです。
2. エラー・フロー・ルーティングは、ビジネス ID が誤りの場合、機能しません。特定のイベントに対してエラー・フロー文書が要求され、誤った ID を持つビジネス文書が、同じ構成済みイベントで失敗したとしても、指定されているビジネス ID が無効なためエラー・フロー文書ルーティングは機能しません。

# 第 16 章 構成の終了

ここでは、ハブの構成時に実行できるその他のタスクについて説明します。以下のトピックを扱います。

- 『AS 文書に対するラージ・ファイル・サポート』
- 318 ページの『API の使用可能化』
- 318 ページの『イベント用に使用するキューの指定』
- 320 ページの『アラート可能イベントの指定』
- 320 ページの『 ユーザー定義のトランスポートの更新』
- 321 ページの『サンプル』

**注:** WebSphere Partner Gateway の構成変更を行う場合は、必ず、コミュニティー・コンソールにログインしたときと同じブラウザー・インスタンスを使用してください。複数のブラウザー・インスタンスを同時に使用すると、構成変更が無効になる可能性があります。

## AS 文書に対するラージ・ファイル・サポート

AS2 および AS3 に対して、GB 単位のサイズでのラージ・ファイル・サポートが拡張されました。バイト配列を使用して処理される最大ファイル・サイズが構成可能です。割り振られるメモリーの量が使用可能ヒープ・サイズを超えると、OutOfMemoryError が発生します。データのサイズが使用可能メモリーに満たない場合も、割り振られるメモリーにより使用可能メモリーの量が増加する場合、やはり OutOfMemoryError が発生します。構成されているファイル・サイズがサポート可能かどうかは、実行時に使用可能ヒープ・メモリーに基づいて判別されます。バイト配列で使用できる最大ファイル・サイズは、プロパティー **bcg.maximumFileSizeForByteArrays** を使用して指定することができます。プロパティー bcg.maximumFileSizeForByteArrays の値は、MB 単位で指定されます。ファイル・サイズがこのプロパティーの値を超える場合は、ストリームを使用して処理されます。ファイル・サイズがこのプロパティーの値より小さく、使用可能メモリーが十分でない場合は、エラー・イベント BCG210050 が生成されます。

ハブ・オペレーターとしてログインしたら、「**システム管理者**」タブ > 「**共通プロパティー**」タブにナビゲートしてください。**bcg.maximumFileSizeForByteArrays** プロパティーのデフォルト値を上書きして、バイト配列に使用する最大ファイル・サイズを指定します。パフォーマンスを改善するには、このプロパティーの値を増加してください。

## API の使用可能化

### このタスクについて

WebSphere Partner Gateway に用意されている一連の API を使用すると、コミュニティー・コンソールで一般に実行される各種機能にアクセスすることができます。これらの API については、「*WebSphere Partner Gateway Programmer Guide*」を参照してください。

XML ベースの API を使用可能にすると、パートナーが WebSphere Partner Gateway サーバーへの API 呼び出しを実行できるようになります。そのためには、以下の手順を実行します。

1. メインメニューから、「**システム管理**」>「**機能の管理**」>「**管理 API**」をクリックします。
2. 「**XML ベースの API の可能化**」の横にある「**編集**」アイコンをクリックします。
3. XML ベースの API を使用可能にするチェック・ボックスを選択します。
4. 「**保存**」をクリックします。

### タスクの結果

**注:** XML ベースの管理 API は、推奨されません。

作成作業と更新作業には、管理 API の代わりにマイグレーション・ユーティリティーも使用できます。マイグレーションのインポート・ファイルに、新規情報または更新情報が記載されています。

インポート・ファイルは、マイグレーション・ユーティリティーに組み込まれている XML スキーマにより記述されています。Rational Application Developer などの開発ツールを使用して、このスキーマに準拠するインポート XML ファイルを作成できます。マイグレーション・ユーティリティーを使用してこのファイルをインポートすることで、パートナーの連絡先とビジネス ID を含む新規パートナー定義をロードできます。既存のパートナー定義を更新することもできます。更新するには、マイグレーション・ユーティリティーを使用してこれらのパートナー定義をインポートします。管理 API では、システムの構成成果物の一部をリストできました。マイグレーション・ユーティリティーを使用してシステム全体をエクスポートすると、エクスポート XML ファイルに、パートナー機能、パートナー接続、およびレシーバー (ターゲット) がリストされます。

マイグレーション・プロセスを開始するためには、**bcgmigrate.bat/bcgmigrate.sh**バッチ・ファイルが使用されます。bcgmigrate コマンドを実行するときには必ず、(bcgmigrate.bat/bcgmigrate.sh) に対するファイルの**実行**許可があることを確認してください。このことは、UNIX プラットフォームにより当てはまります。

## イベント用に使用するキューの指定

### このタスクについて

JMS 構成を使用して構成された外部キューにイベントを送達するよう、ハブを構成することができます。

デフォルトの JMS 構成は、ハブのインストール時に設定されます。これらの値の一部は、「イベント・パブリッシュ・プロパティー」ページで確認できます。

別の JMS 構成を指定するには、WebSphere Partner Gateway/WAS の内部メッセージング・キューまたは他のメッセージング・サーバーにイベントを公開するための適切な構成値を設定します。さらに、イベントが公開されるキューの名前と一致するようにキュー名を変更します。

API イベントの送達先を指定するには、以下のステップを実行します。

1. メインメニューから、「**システム管理**」>「**DocMgr の管理**」>「**イベント・エンジン**」>「**外部イベント**」をクリックします。
2. 「**イベント送達の有効化**」の横にある「**編集**」アイコンをクリックします。
3. 「**イベント送達の有効化**」チェック・ボックスにチェック・マークを付け、イベントのパブリッシュをアクティブ化します。
4. デフォルト値がご使用のシステムに対して適切である場合は、そのままにしておきます。デフォルト値は、インストール時に構成した JMS サーバーで提供されるキュー DeliveryQ へのイベント送達をサポートします。

   イベントの送達先を変更する場合は、以下の情報を参照しながらフィールドを更新します。

   - キューにアクセスするときにユーザー ID とパスワードが必要な場合は、「**ユーザー ID**」および「**パスワード**」の値を入力します。
   - 「**JMS キュー・ファクトリー名**」に、使用している JMS .bindings ファイルの JMS キュー接続ファクトリーの名前を入力します。

     **注:** Windows のバージョン (XP 以前) によっては、デフォルトのイベント送達機能を使用する場合に、「**JMS キュー・ファクトリー名**」フィールドのデフォルト値を変更する必要があります。「**JMS キュー・ファクトリー名**」の値を `WBIC/QCF` から `WBIC¥¥QCF` へ変更します。
   - 「**JMS メッセージ・タイプ**」に、送達されるメッセージのタイプを入力します。選択項目は、バイトまたはテキストです。
   - 「**JMS キュー名**」に、イベントがパブリッシュされる JMS キューの名前を入力します。このキューは、WebSphere MQ で使用している JMS .bindings ファイルに既に定義されている必要があります。

     **注:** Windows のバージョン (XP 以前) によっては、デフォルトのイベント送達機能を使用する場合に、「**JMS キュー名**」フィールドのデフォルト値を変更する必要があります。「**JMS キュー名**」の値を `WBIC/DeliveryQ` から `WBIC¥¥DeliveryQ. WBIC/QCF` へ変更します。
   - 「**JNDI ファクトリー名**」に、.bindings ファイルにアクセスするときに使用する名前を入力します。デフォルト値は、ファイル・システムのデフォルトのバインディングへのアクセスを提供します。
   - 「**プロバイダー URL パッケージ**」に、JMS バインディング・ファイルにアクセスするための URL を入力します。この URL は、「JNDI ファクトリー名」と整合している必要があります。このフィールドはオプションであり、入力しなかった場合は、JMS バインディングのデフォルトのファイル・システム・ロケーションが使用されます。

- 「**メッセージの文字セット**」に、JMS キューに対するバイト・メッセージを作成するときに使用される文字セットを入力します。デフォルト値は、UTF-8 です。このフィールドは、バイト・メッセージにのみ関連します。
- 「**JMS プロバイダー URL**」に、JMS プロバイダーの URL を入力します。このフィールドはオプションであり、入力しなかった場合は、インストール時に指定されたデフォルトの JMS プロバイダーが使用されます。

5. 「**保存**」をクリックします。

## アラート可能イベントの指定

### このタスクについて

WebSphere Partner Gateway 内でイベントが発生すると、イベント・コードが生成されます。「イベント・コード」ページでは、イベント・コードのアラート可能状況を設定することができます。イベントがアラート可能として設定されると、「アラート」ページの「イベント名」リストにそのイベントが表示されます。この後、イベントのアラートを設定することができます。

アラート可能にするイベントを指定するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**イベント・コード**」をクリックします。「イベント・コード」ページが表示されます。
2. アラート可能にするイベントごとに、以下のステップを実行します。
   a. イベント・コードの横にある「**詳細の表示**」アイコンをクリックします。「イベント・コードの詳細」ページが表示されます。
   b. 「**アラート可能 (Alertable)**」を選択します。
   c. 「**保存**」をクリックします。

## ユーザー定義のトランスポートの更新

59 ページの『第 7 章 レシーバーの定義』および 227 ページの『第 11 章 宛先の作成』で説明されているように、ユーザー定義のトランスポートが記述されている XML ファイルをアップロードすることができます。「**トランスポート・タイプの管理**」を使用してファイルをアップロードします。XML ファイルをアップロードすると、トランスポートが使用可能になり、受信側や宛先を定義するときに使用できます。

ユーザー定義のトランスポートが記述されている XML ファイルには、トランスポートの属性が含まれています。これらの属性は、ユーザー定義のトランスポートを指定するときに、受信側または宛先のページに表示されます (「**カスタム・トランスポート属性**」セクション)。例えば、宛先用のユーザー定義のトランスポートには、属性 DestinationRetryCount が含まれています。

トランスポートが記述された XML ファイルを作成したユーザーは、(属性の追加、削除、または変更を行うことによって) 属性を更新できます。XML ファイルが変更された場合は、再び「**トランスポート・タイプの管理**」を使用してファイルをアップロードします。属性に対する変更は、宛先または受信側のページに反映されます。

# サンプル

WebSphere Partner Gateway には、カスタム機能と図示を提供するいくつかのサンプルが同梱されています。これらのサンプルのパッケージは、WebSphere Partner Gateway インストールが抽出されたディレクトリーの中の **DevelopmentKits** および**統合**フォルダーの下にあります。

DevelopmentKits フォルダーには、次のサンプルが含まれています。

- 管理 API: 管理 API は推奨されません。タスクの作成および更新には、Partner Migration utility が使用されます。
- マイグレーション: エクスポートおよびインポート構成のサンプルが含まれています。
  - エクスポート構成: コマンド行スクリプト・ファイルから java コンポーネントを使用して WebSphere Partner Gateway 構成をエクスポートする手順を示します。
  - インポート構成: コマンド行スクリプト・ファイルから java コンポーネントを使用して WebSphere Partner Gateway 構成をインポートする手順を示します。
- UserExits: 変換および妥当性検査用のカスタム・ユーザー出口コードを作成するためのサンプルで構成されています。
  - *EDITransTypeBusinessProcess* サンプルは、システムを通過する EDI 文書のカスタム機能を提供します。このサンプル・ユーザー出口は、EDI X12 文書から EDI トランザクション・タイプを解析するように設計されています。構文解析基準を変更することにより、他の値を抽出することができます。
  - *custom translation user exit* サンプルは、インバウンド XML 文書に対する変換機能を提供します。
  - *custom validation user exit* サンプルは、インバウンド XML 文書に対する妥当性検査機能を提供します。
- サンプル・シナリオ: 下記のプロトコルに対して WebSphere Partner Gateway System をセットアップするためのガイドラインを提供するサンプルで構成されています (「パッケージ化なし」および「AS パッケージ化」)。各プロトコルごとに、構成インポート・ファイルも提供されています。
  - カスタム XML
  - EDI-X12
  - バイナリー文書

統合フォルダーには、次のサンプルが含まれています。

- WebSphere Transformation Extender 統合: XML 文書をフラット・ファイルに変換するための WebSphere Transformation Extender との統合を示すためのサンプル。
- WebSphere Business Integration メッセージ・ブローカー・サンプル: WebSphere Partner Gateway がどのように WebSphere Business Integration メッセージ・ブローカーとの通信を行うかを示すためのサンプル。
- WebSphere Process Server 統合: WebSphere Partner Gateway が JMS によりどのように WebSphere Process Server と統合するかを示すためのサンプル。

- WebSphere Interchange Server 統合: WebSphere Partner Gateway が HTTP および JMS を使用してどのように Interchange Server と通信を行うかを示すためのサンプル。

# 第 17 章 CPP/CPA エディター

CPP/CPA エディターは、テンプレートからの CPP/CPA 文書の作成を支援し、ユーザーが表形式で編集できるようにするための Eclipse プラグインです。さらに、データおよびスキーマの検証も行います。

**前提条件:**

- WID/RAD バージョン 6.1 以上が必要です。
- ダウンロードした CPP/A エディター・プラグインを IDE のプラグイン・フォルダーに置きます。

Collaboration-Protocol Agreement (CPA) 文書は、2 つの Collaboration-Protocol Profile (CPP) 文書から作成することもできます。 CPP は、他者との電子ビジネスを行う当事者の能力を定義します。CPA は、2 者間でのメッセージ交換の契約内容を記述します。CPP を作成するには、エディターのユーザー・インターフェースを介して個々の XML エレメント (個々の XML エレメントは各種の属性で構成される) の値を入力します。エディターで CPA 文書を作成して、その状況が「同意 (AGREED)」になると、その文書は WebSphere Partner Gateway にインポートできます。インポートされたファイルにより、以下が自動的に作成されます。

- パートナー
- B2B ゲートウェイ
- インタラクションおよび接続

それとは別に、文書定義が自動的に定義され、必要な B2B 機能を使用できるようになります。

CPP/CPA エディターのユーザー・インターフェースを使用して、以下の操作を行うことができます。

- 324 ページの『CPP 文書の作成』
- 324 ページの『CPA 文書の作成』
- 325 ページの『エディターでの値の編集』

CPP/CPA エディターをデフォルト・エディターにするには、次のようにします。

1. Eclipse プラグイン環境で、「**ウィンドウ**」メニューをクリックして「**設定**」を選択します。
2. 「設定」ウィンドウで、「**一般**」>「**エディター**」>「**ファイルの関連付け**」をクリックします。
3. 「**ファイル・タイプ**」リストで「*.xml」を選択し、「**関連付けられたエディター**」リストで「CPPEditor マルチページ・エディター (CPPEditor Multi – page Editor)」を選択します。
4. 「**デフォルト**」をクリックします。

## CPP 文書の作成

CPP 文書を作成するには、次のようにします。

1. IDE で、「**ファイル**」>「**新規**」を選択します。
2. 「**新規**」ウィンドウで、「**CPAEditor**」> 「**CPP ファイル (Collaboration Protocol Profile file)**」を選択します。
3. 「**次へ**」をクリックして、CPP/CPA 保有者の値を入力します。
4. 「**終了**」をクリックします。指定したコンテナーの下に新規ファイルが作成されます。
5. CPAEditor をデフォルトとして構成した場合は、テンプレート内の値を変更してください。それ以外の場合は、ファイルが XML エディターで開きます。ファイルを CPAEditor で開くには、右クリックして「**アプリケーションから開く**」 > 「**CPAEditor マルチページ・エディター (CPAEditor Multi-Page Editor)**」を選択します。
6. すべてのエレメントの属性の値を入力します。一部の属性に関しては、各種のオプションから適切な値を選択できます。
7. 「**保存**」をクリックします。CPP 文書が正常に作成されたことを示すメッセージが表示されます。

## CPA 文書の作成

次の 2 つのオプションのいずれかを選択する必要があります。

- ケース 1: テンプレートを使用して CPA を作成する。これにより、エディターのユーザー・インターフェースを介して個々の XML エレメント (個々の XML エレメントは各種の属性で構成される) の値を入力できます。
- ケース 2: 2 つの CPP から CPA を作成する。

テンプレートを使用して CPA を作成するには、次のようにします。

1. IDE で、「**ファイル**」>「**新規**」を選択します。
2. 「**新規**」ウィンドウで、「**CPAEditor**」> 「**CPA ファイル (Collaboration Protocol Agreement file)**」を選択します。
3. 「**次へ**」をクリックして、CPP/CPA 保有者の値を入力します。
4. 「**終了**」をクリックします。指定したコンテナーの下に新規ファイルが作成されます。
5. CPAEditor をデフォルトとして構成した場合は、テンプレート内の値を変更してください。それ以外の場合は、ファイルが XML エディターで開きます。ファイルを CPAEditor で開くには、右クリックして「**アプリケーションから開く**」> 「**CPPEditor マルチページ・エディター (CPPEditor Multi-Page Editor)**」を選択します。
6. すべてのエレメントの属性の値を入力します。一部の属性に関しては、各種のオプションから適切な値を選択できます。
7. 「**保存**」をクリックします。CPA 文書が正常に作成されたことを示すメッセージが表示されます。

2 つの CPP から CPA を作成するには、次のようにします。

1. IDE で、「**ファイル**」> 「**新規**」 > 「**その他**」をクリックします。
2. 「**新規**」ウィンドウで、「**CPAEditor**」 > 「**CPP のマージ (Merge Collaboration Protocol Profiles)**」を選択します。
3. 「**次へ**」をクリックします。
4. CPP/CPA 保有者の値、およびマージする CPP ファイルのパスと名前を入力します。
5. 「**終了**」をクリックします。指定したコンテナーの下に、マージされたファイルが作成されます。
6. CPAEditor をデフォルトとして構成した場合は、テンプレート内の値を変更してください。それ以外の場合は、ファイルが XML エディターで開きます。ファイルを CPAEditor で開くには、右クリックして「**アプリケーションから開く**」> 「**CPPEditor マルチページ・エディター (CPPEditor Multi-Page Editor)**」を選択します。

## エディターでの値の編集

エディター・テーブルの値を編集するには、セルの上にカーソルを置いて、値を編集します。すべての PartyInfo エレメントには、固有の partyName が関連付けられています。PartyInfo の下に存在するサブエレメントとしては、
PartyId、PartyRef、Collaboration
Role、Certificate、SecurityDetails、DeliveryChannel、Transport、DocExchange、および OverrideMshActionBinding があります。これらの値は、CPP/CPA エディターのさまざまなタブで使用できます。PartyName は、PartyInfo のサブエレメントを、対応する PartyInfo エレメントと関連付けるための固有 ID となります。

例えば、PartyInfo エレメントのサブエレメントである Certificate エレメントは、1 回以上指定できます。PartyInfo エレメントは、CPP 内で複数回指定することができます。

# 第 18 章 基本的な例

この付録では、ハブの構成例を示します。以下のトピックを扱います。

- 『 基本構成 – パススルー EDI 文書の交換』
- 334 ページの『 基本構成 - インバウンドおよびアウトバウンド文書のセキュリティー設定』
- 340 ページの『基本構成の拡張』

エンベロープ解除、変換、エンベロープ化、および機能確認通知の送信を含む EDI 交換処理の例は、別の付録に記載されています。347 ページの『第 19 章 EDI の例』を参照してください。

これらの例では、システムの構成に必要なステップの概要を示します。これらの例を使用してシステムをセットアップする場合は、業務上の必要に合わせて特定の情報 (名前やビジネス ID など) を変更してください。

## 基本構成 – パススルー EDI 文書の交換

ここでは、単純なハブ構成の例を示します。定義されるレシーバーは、パートナーからハブに着信する文書用と、内部パートナーのバックエンド・システムからハブに着信する文書用の 2 つです。この例で設定される交換処理では、WebSphere Partner Gateway に用意されている文書定義を使用するため、これらのフローを基にインタラクションを作成するだけで済みます。カスタム XML は、ここでは使用しません。

この例は、内部パートナーのバックエンド・アプリケーションと外部パートナー (Partner Two) との間の交換処理を示しています。

### ハブの構成

ハブの設定では、まず 2 つのレシーバーを作成します。

- 「HttpReceiver」という名前の HTTP レシーバー: (Partner Two から) HTTP を介して内部パートナーのバックエンド・システムへ送信される文書を受信します。
- 「FileSystemReceiver」という名前のファイル・ディレクトリー・レシーバー: Partner Two に送信される文書を (内部パートナーのバックエンド・システムの) ファイル・システムから取り出します。

#### レシーバーの定義

#### このタスクについて

HTTP による文書の受取用のレシーバーを作成するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックします。
2. 「**レシーバーの作成**」をクリックします。
3. 「レシーバー名」に **HttpReceiver** と入力します。

4. 「トランスポート」リストから「**HTTP/S**」を選択します。
5. 「動作モード」には、デフォルトの「**実動**」を使用します。
6. 「URI」に **/bcgreceiver/submit** と入力します。
7. 「**保管**」をクリックします。

次に、ファイル・システム上のディレクトリーをポーリングするためのレシーバーを作成します。レシーバーを作成すると、ファイル・システム上に新規ディレクトリーが自動的に作成されます。

ファイル・システム・レシーバーを作成するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックします。
2. 「**レシーバーの作成**」をクリックします。
3. 「レシーバー名」に **FileSystemReceiver** と入力します。
4. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
5. 「デフォルトの動作モード」には、デフォルトの「**実動**」を使用します。
6. 「文書ルート・パス」に **¥temp¥FileSystemReceiver** と入力します。

   **注:** これにより、temp ディレクトリー内に FileSystemReceiver ディレクトリーが作成されます。ファイル・システム上に temp ディレクトリーがあることを確認してください。
7. 「**保存**」をクリックします。

## 文書タイプおよびインタラクションの定義

### このタスクについて

この例では、EDI-X12 標準に準拠した文書の交換処理を設定します。この例では、文書は単純にハブを経由して渡されます。EDI 交換処理のエンベロープ解除は行われず、変換は発生しません。交換処理のエンベロープ解除、トランザクションの変換、および確認通知の送信の例については、449 ページの『第 22 章 属性』を参照してください。

このセクションでは、以下の交換処理について説明します。

- パッケージ化なしでの、内部パートナーから Partner Two への EDI-X12 文書の送信。
- AS2 でパッケージ化された、Partner Two から内部パートナーへの EDI-X12 文書の送信。

パッケージ化とプロトコルが含まれているため、文書定義を新規作成する必要はありません。パッケージ、プロトコル、文書タイプは、システムで事前に定義されているものを使用します。

ただし、これらの事前定義された文書タイプに基づいて、インタラクションを定義する必要があります。

まず、1 つ目の対話 (ソースがパッケージ化なしの EDI-X12 標準準拠の ISA 形式文書で、ターゲットが AS でパッケージ化された EDI-X12 標準準拠の ISA 形式文書) を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。

2. 「**インタラクションの作成**」をクリックします。
3. 「**ソース**」列から、以下のように展開します。
   a. **パッケージ: なし**
   b. **プロトコル: EDI-X12**
4. 「**文書タイプ: ISA**」をクリックします。
5. 「**ターゲット**」列から、以下のように展開します。
   a. **パッケージ: AS**
   b. **プロトコル: EDI-X12**
6. 「**文書タイプ: ISA**」をクリックします。
7. 「**アクション**」リストから「**パススルー**」を選択します。
8. 「**保存**」をクリックします。

次に、2 つ目の対話 (ソース形式が AS でパッケージ化された EDI-X12 標準準拠の ISA 形式文書で、ターゲット形式がパッケージ化なしの EDI-X12 標準準拠の ISA 形式文書) を作成します。

1. 「**インタラクションの作成**」をクリックします。
2. 「**ソース**」列から、以下のように展開します。
   a. **パッケージ: AS**
   b. **プロトコル: EDI-X12**
3. 「**文書タイプ: ISA**」をクリックします。
4. 「**ターゲット**」列から、以下のように展開します。
   a. **パッケージ: なし**
   b. **プロトコル: EDI-X12**
5. 「**文書タイプ: ISA**」をクリックします。
6. 「**アクション**」リストから「**パススルー**」を選択します。
7. 「**保存**」をクリックします。

## パートナーおよびパートナー接続の作成

ここでは、外部パートナーと内部パートナーを作成します。パートナー用の宛先には標準のトランスポートが組み込まれており、宛先用の構成ポイントは定義されていません。

### パートナーの作成

新規パートナーを 2 つ作成します。内部パートナーを定義するには、以下のステップを実行します。

1. メインメニューから、「**アカウント管理**」をクリックします。「パートナー検索」ページがデフォルトのビューになります。
2. 「**作成**」をクリックします。
3. 「**会社ログイン名**」に **CommMan** と入力します。
4. 「**パートナー表示名**」に **Comm Man** と入力します。
5. 「**パートナー・タイプ**」に「**内部パートナー**」を選択してください。
6. 「**ビジネス ID**」の下の「**新規**」をクリックします。

7. 「**タイプ**」を「**DUNS**」のままにして、ID 値 **123456789** を入力します。

   **注:** この例および本書全体を通して、DUNS 番号はすべて例として示されています。
8. 「**ビジネス ID**」の下の「**新規**」をクリックします。
9. 「**Freeform**」を選択して、ID 値 **12-3456789** を入力します。
10. 「**保存**」をクリックします。

Partner Two を定義するには、以下のステップを実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**作成**」をクリックします。
3. 「**会社ログイン名**」に **partnerTwo** と入力します。
4. 「**パートナー表示名**」に **Partner Two** と入力します。
5. 「**パートナー・タイプ**」に「**外部パートナー**」を選択してください。
6. 「**ビジネス ID**」の下の「**新規**」をクリックします。
7. 「**タイプ**」を「**DUNS**」のままにして、ID 値 **987654321** を入力します。
8. 「**ビジネス ID**」の下の「**新規**」をクリックします。
9. 「**Freeform**」を選択して、ID 値 **98-7654321** を入力します。
10. 「**保管**」をクリックします。

これで、ハブに対して内部パートナーと Partner Two の両方が定義されました。

次に、内部パートナーと Partner Two の両方の宛先を構成します。

## 宛先の作成

### このタスクについて

内部パートナーのファイル・ディレクトリー宛先を作成する前に、この宛先で使用するディレクトリー構造を作成する必要があります。ここでは、ルート・ドライブに FileSystemDestination というディレクトリーを新規作成します。このディレクトリーは、内部パートナーが外部パートナーから受信したファイルを格納するのに使用します。

内部パートナーの場合、宛先がバックエンド・システムへの入り口点となります。

内部パートナーの宛先を作成するには、以下のステップを実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. 「**詳細の表示**」アイコンをクリックして「**内部パートナー**」を選択します。
4. 水平ナビゲーション・バーから「**宛先**」をクリックします。
5. 「**作成**」をクリックします。
6. 「**宛先名**」に **FileSystemDestination** と入力します。
7. 「**トランスポート**」で、「**ファイル・ディレクトリー**」を選択します。
8. 「**アドレス**」に **file://C:¥FileSystemDestination** と入力します。
9. 「**保存**」をクリックします。

次に、新規作成したこの宛先を内部パートナーのデフォルト宛先として設定します。

1. 「**リスト**」をクリックし、内部パートナー用に構成された宛先をすべて表示します。
2. 「**デフォルト宛先の表示**」をクリックします。
3. 「**実動**」リストから「**FileSystemDestination**」を選択します。
4. 「**保存**」をクリックします。

Partner Two の宛先を作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックし、次に「**詳細の表示**」アイコンをクリックして「**Partner Two**」を選択します。
3. 水平ナビゲーション・バーから「**宛先**」をクリックします。
4. 「**作成**」をクリックします。
5. 「**宛先名**」に **HttpDestination** と入力します。
6. 「**トランスポート**」で、「**HTTP/1.1**」を選択します。
7. 「**アドレス**」に **http://<***IP_address***>:80/input/AS2** と入力します。ここで、*<IP_address>* は Partner Two のコンピューターを表します。
8. 「**ユーザー名**」に **Comm Man** と入力します。
9. 「**パスワード**」に **commMan** と入力します。
10. 「**保存**」をクリックします。

この例の Partner Two では、パートナーがシステムにログインする際にユーザー名とパスワードが必要となる点に注意してください。

このパートナーに対しても、デフォルト宛先を定義する必要があります。

1. 「**リスト**」をクリックし、次に「**デフォルト宛先の表示**」をクリックします。
2. 「**実動**」リストから「**HttpDestination**」を選択します。
3. 「**保存**」をクリックします。

## B2B 機能の設定

### このタスクについて

次に、内部パートナーの B2B 機能を定義します。

1. メインメニューから、「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. 「**詳細の表示**」アイコンをクリックして「**内部パートナー**」を選択します。
4. 水平ナビゲーション・バーから「**B2B 機能**」をクリックします。
5. 以下のステップを実行して、「パッケージ: なし」、「プロトコル: EDI-X12」、および「文書タイプ: ISA」に対するソースとターゲットを設定します。
   a. 「**ソースの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

b. 「**ターゲットの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

c. 「**パッケージ: なし**」の横にある「**展開 (Expand)**」アイコンをクリックします。

d. ソースとターゲットの両方で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

e. 「**プロトコル: EDI-X12 (すべて)**」の横にある「**展開 (Expand)**」アイコンをクリックします。

f. ソースとターゲットの両方で、「**文書タイプ: ISA**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

次に、Partner Two の B2B 機能を設定します。

1. メインメニューから、「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. 「**詳細の表示**」アイコンをクリックして「Partner Two」を選択します。
4. 水平ナビゲーション・バーから「**B2B 機能**」をクリックします。
5. 以下のステップを実行して、「パッケージ: AS」、「プロトコル: EDI-X12」、「文書タイプ: ISA」に対する「ソースの設定」と「ターゲットの設定」を選択します。

   a. 「**ソースの設定**」の下で、「**パッケージ: AS**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

   b. 「**ターゲットの設定**」の下で、「**パッケージ: AS**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

   c. 「**パッケージ: AS**」の横にある「**展開 (Expand)**」アイコンをクリックします。

   d. ソースとターゲットの両方で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

   e. 「**プロトコル: EDI-X12 (すべて)**」の横にある「**展開 (Expand)**」アイコンをクリックします。

   f. ソースとターゲットの両方で、「**文書タイプ: ISA**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

## パートナー接続の定義

### このタスクについて

パッケージ化なしで、内部パートナーから Partner Two に配信される EDI 文書用のパートナー接続を定義します。

1. 「**アカウント管理**」>「**接続**」をクリックします。
2. 「**ソース**」リストから「**内部パートナー**」を選択します。
3. 「**ターゲット**」リストから **Partner Two** を選択します。
4. 「**検索**」をクリックします。
5. 以下の詳細情報を指定し、この接続に対して「**アクティブ化**」をクリックします。

a. **ソース**
   1) パッケージ: **なし (N/A)**
   2) プロトコル: **EDI-X12 (すべて)**
   3) 文書タイプ: **ISA (すべて)**
b. **ターゲット**
   1) パッケージ: **AS (N/A)**
   2) プロトコル: **EDI-X12 (すべて)**
   3) 文書タイプ: **ISA (すべて)**

次に、パッケージ化なしで Partner Two から内部パートナーに配信される、AS2 パッケージでラップされた EDI 文書用の接続を定義します。前のセクションで定義した接続と良く似ていますが、AS2 属性も構成する点が異なります。

1. 「**アカウント管理**」>「**接続**」をクリックします。
2. 「**ソース**」リストから **Partner Two** を選択します。
3. 「**ターゲット**」リストから「**内部パートナー**」を選択します。
4. 「**検索**」をクリックします。
5. 以下の詳細情報を指定し、この接続に対して「**アクティブ化**」をクリックします。
   a. **ソース**
      1) パッケージ: **AS (N/A)**
      2) プロトコル: **EDI-X12 (すべて)**
      3) 文書タイプ: **ISA (すべて)**
   b. **ターゲット**
      1) パッケージ: **なし (N/A)**
      2) プロトコル: **EDI-X12 (すべて)**
      3) 文書タイプ: **ISA (すべて)**

次に、Partner Two の「**パッケージ: AS (N/A)**」ボックスの横にある「属性」を選択します。

1. ページをスクロールダウンし、「**パッケージ: AS (N/A)**」の横にある「**展開 (Expand)**」アイコンをクリックして、「パッケージ: AS (N/A)」の属性を編集します。
2. 「AS MDN E-Mail Address (AS1)」の値を入力します。有効な E メール・アドレスであれば何でも構いません。
3. 「AS MDN HTTP URL (AS2)」の値を入力します。入力値は **http://<***IP_address***>:57080/bcgreceiver/submit** です。ここで、<*IP_Address*> はハブを表します。
4. 「**保管**」をクリックします。

# 基本構成 - インバウンドおよびアウトバウンド文書のセキュリティー設定

ここでは、基本構成に以下のタイプのセキュリティーを追加する方法について説明します。

- Secure Socket Layer (SSL) サーバー認証
- 暗号化
- デジタル署名

## 着信文書に対する SSL 認証の設定

### このタスクについて

ここでは、iKeyman を使用して、Partner Two が AS2 文書を HTTPS で送信できるようにサーバー認証を設定します。

サーバー認証を設定するには、以下のステップを実行します。

1. /<*ProductDir*>/was/bin ディレクトリーから ikeyman.bat ファイルを開き、IKEYMAN アプリケーションを始動します。
2. レシーバーのデフォルトの鍵ストア bcgSecurity.jks を開きます。メニュー・バーから、「**鍵データベース・ファイルのオープン (Key Database File Open)**」を選択します。デフォルトのインストールでは、bcgSecurity.jks は以下のディレクトリーにあります。<*ProductDir*>/common/security/keystore
3. プロンプトが出されたら、bcgSecurity.jks のデフォルトのパスワードを入力します。パスワードは WebAS です。
4. bcgSecurity.jks を初めて開いた場合は、「ダミー」の証明書を削除します。

次に、自己署名証明書を新規作成します。自己署名個人証明書を作成すると、サーバーの鍵ストア・ファイル内に秘密鍵と公開鍵が作成されます。

自己署名証明書を新規作成するには、以下のステップを実行します。

1. 「**新規自己署名 (New Self Signed)**」をクリックします。
2. この証明書に、鍵ストア内で証明書を一意的に識別するための鍵ラベルを付けます。ここでは **selfSignedCert** というラベルを使用します。
3. サーバーの共通名を入力します。これは、その証明書の基本的な共通 ID であり、その証明書が表すプリンシパルを一意的に識別するものでなければなりません。
4. 所属する組織名を入力します。
5. その他のデフォルトをすべて受け入れて、「**OK**」をクリックします。

Partner Two は、セキュア HTTP を使用して、AS2 で EDI メッセージを送信したいとします。これを行うには、Partner Two が公開証明書 (自己署名証明書を作成した際に作成したもの) を参照する必要があります。

Partner Two が公開証明書を使用できるようにするには、以下のステップを実行して、サーバーの鍵ストア・ファイルから公開証明書をエクスポートします。

1. IBM 鍵管理ユーティリティーから、新規作成した自己署名証明書を選択します。
2. 「**証明書の抽出 (Extract Certificate)**」をクリックします。

3. データ型を「**バイナリー DER データ (Binary DER data)**」に変更します。
4. ファイル名として **commManPublic** を指定し、「**OK**」をクリックします。

最後に、IKEYMAN を使用して、自己署名証明書と秘密鍵のペアを PKCS12 ファイルの形式でエクスポートします。この PCKS12 ファイルは、後述の暗号化で使用します。

自己署名証明書と秘密鍵のペアをエクスポートするには、以下のステップを実行します。

1. 「**エクスポート/インポート (Export/Import)**」をクリックします。
2. 鍵ファイルのタイプを「**PKCS12**」に変更します。
3. ファイル名として **commManPrivate** を指定し、「**OK**」をクリックします。
4. ターゲットの PKCS12 ファイルをプロテクトするためのパスワードを入力します。パスワードを確認し、「**OK**」をクリックします。

**注:** これらの変更内容を有効にするには、レシーバーを一旦停止して再始動します。

入力したパスワードは、後でこの秘密証明書をハブにインポートする際に使用します。

また、Partner Two で、証明書のインポートや AS2 文書の送信先アドレスの変更などの構成ステップを実行する必要もあります。例えば、Partner Two でアドレスを以下のように変更する必要があるとします。

```
https://<IP_address>:57443/bcgreceiver/submit
```

ここで、*<IP_address>* はハブを表します。

これで、Partner Two がセキュア HTTP で文書を送信する際に、レシーバーのデフォルトの鍵ストアに格納された自己署名証明書が Partner Two に提示されるようになります。

逆の状態を設定するには、Partner Two がハブに .der ファイル形式の SSL キー (この場合は partnerTwoSSL.der) を提示する必要があります。また、Partner Two で必要に応じて、HTTPS トランスポートで文書を受信できるように構成を変更してください。

Partner Two の partnerTwoSSL.der ファイルは、ルート証明書として Hub Operator のプロファイルにロードします。ルート証明書とは、証明書チェーンの確立時に利用する認証機関 (CA) から発行される証明書をいいます。この例では、PartnerTwo が生成した証明書がルート証明書としてロードされ、これにより、ハブが送信者を認識および信頼できるようになります。

partnerTwoSSL.der をハブにロードするには、以下のステップを実行します。

1. メインメニューから、「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. 「**詳細の表示**」アイコンを選択して「**ハブ・オペレーター (Hub Operator)**」を選択します。

4. 「**証明書**」をクリックし、次に「**証明書のロード**」をクリックします。
5. 「**証明書タイプ**」を「**ルートおよび中間証明書 (Root and Intermediate Certificate)**」に設定します。
6. 「説明」の内容を **Partner Two SSL Certificate** に変更します。
7. 「**状況**」を「**有効**」に設定します。
8. 「**参照**」をクリックし、partnerTwoSSL.der の保存先ディレクトリーに移動します。
9. 証明書を選択し、「**オープン**」をクリックします。
10. 「**アップロード**」をクリックし、次に「**保存**」をクリックします。

セキュア HTTP を使用するように Partner Two の宛先を変更します。

1. 水平ナビゲーション・バーから、「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックし、「**詳細の表示**」アイコンをクリックして「Partner Two」を選択します。
3. 水平ナビゲーション・バーから「**宛先**」をクリックします。次に、「**詳細の表示**」アイコンをクリックして「HttpDestination」を選択します。
4. 「**編集**」アイコンをクリックして編集します。
5. トランスポート値を **HTTPS/1.1** に変更します。
6. 読み取るアドレスの値を **https://<*IP_address*>:443/input/AS2** に変更します。ここで、*<IP_address>* は Partner Two のマシンを表します。
7. それ以外の値はすべて未変更のままで構いません。「**保存**」をクリックします。

## 暗号化の設定

### このタスクについて

ここでは、暗号化を設定するステップについて説明します。

Partner Two で、必要な構成ステップ (公開証明書および自己署名証明書のインポートなど) を実行し、ハブに送信される文書に対して暗号化を設定する必要があります。

WebSphere Partner Gateway では、文書の暗号化を解除する際に、秘密鍵を使用します。ハブがこれを実行できるようにするには、まず自己署名証明書から抽出された秘密鍵をコミュニティー・コンソールにロードする必要があります。コミュニティー・コンソールに Hub Operator としてログインしてこのタスクを実行したら、証明書を自分のプロファイルにインストールしてください。

PKCS12 ファイルをロードするには、以下のステップを実行します。

1. 水平ナビゲーション・バーから、「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. 「**詳細の表示**」アイコンをクリックして「**ハブ・オペレーター (Hub Operator)**」 を選択します。
4. 「**証明書**」をクリックし、次に「**PKCS12 のロード**」をクリックします。

5. 「**暗号化**」の左側にあるチェック・ボックスにチェック・マークを付けます。
6. 「説明」の内容を「**CommManPrivate**」に変更します。
7. 「**有効**」を選択します。
8. 「**参照**」をクリックし、PKCS12 ファイル commManPrivate.p12 の保存先ディレクトリーに移動します。
9. このファイルを選択し、「**オープン**」をクリックします。
10. PKCS12 ファイル用に提供されたパスワードを入力します。
11. 「動作モード」は「**実動**」のままにします。
12. 「**アップロード**」をクリックし、次に「**保存**」をクリックします。

パートナーがセキュア HTTP で暗号化トランザクションをハブに送信できるようにするための構成は、これで完了です。

次のセクションでは、これまでの手順とは逆に、ハブがセキュア HTTP で EDI 暗号化トランザクションを送信します。

Partner Two では、文書の暗号化を解除するための鍵ペア (この例では partnerTwoDecrypt.der) を生成し、公開証明書をハブが使用できるようにする必要があります。

前述と同様に、パートナーに送信されるトランザクションをハブが暗号化する際には、公開鍵を使用します。これを行うには、公開証明書をハブにロードします。

1. メインメニューから、「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. 「**詳細の表示**」アイコンをクリックして「Partner Two」を選択します。
4. 水平ナビゲーション・バーから「**証明書**」をクリックします。
5. 「**証明書のロード**」をクリックします。
6. 「**暗号化**」の横にあるチェック・ボックスを選択します。
7. 「説明」の内容を **Partner Two Decrypt** に変更します。
8. 「状況」を「**有効**」に設定します。
9. 「**参照**」をクリックします。
10. 暗号化解除証明書 partnerTwoDecrypt.der の保存先ディレクトリーに移動します。
11. 証明書を選択し、「**オープン**」をクリックします。
12. 「動作モード」は「**実動**」のままにします。
13. 「**アップロード**」をクリックし、次に「**保存**」をクリックします。

## タスクの結果

AS2 を使用してセキュア HTTP で暗号化メッセージを送信するためのハブ構成では、最後に内部パートナーと Partner Two 間に存在するパートナー接続を変更します。

コミュニティー・コンソールからパートナー接続を変更するには、以下のステップを実行します。

1. 水平ナビゲーション・バーから「**アカウント管理**」>「**接続**」をクリックします。
2. 「**ソース**」リストから「**Comm Man**」を選択します。
3. 「**ターゲット**」リストから **Partner Two** を選択します。
4. 「**検索**」をクリックします。
5. ターゲットの「**属性**」ボタンをクリックします。
6. 「接続の要約」で、「**AS 暗号化**」属性の現行値が「**いいえ**」になっていることに注意してください。「**パッケージ: AS (N/A)**」の横にある「**展開**」アイコンをクリックして、この値を編集します。

   **注:** このオプションを表示するには、ページをスクロールダウンしてください。
7. リストから、「**AS 暗号化**」属性を「**はい**」に変更し、「**保存**」をクリックします。

# 文書署名の設定

## このタスクについて

WebSphere Partner Gateway では、トランザクションやメッセージにデジタル署名をする際に、秘密鍵を使用して署名を作成します。メッセージの受信者は、送信者の公開鍵を使用して署名を検証します。WebSphere Partner Gateway では、デジタル署名を使用してこれを行います。

ここでは、デジタル署名で使用するハブとパートナーの両方を構成するためのステップについて説明します。

Partner Two では、必要な構成ステップ (自己署名付きの文書 (この例では partnerTwoSigning.der) を作成するなど) をすべて実行した後、文書の署名を構成する必要があります。また、Partner Two では、partnerTwoSigning.der をハブが使用できるようにする必要もあります。

デジタル証明書をハブにロードするには、以下のステップを実行します。

1. 水平ナビゲーション・バーから、「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. 「**詳細の表示**」アイコンをクリックして「Partner Two」を選択します。
4. 水平ナビゲーション・バーから「**証明書**」を選択します。
5. 「**証明書のロード**」をクリックします。
6. 「**デジタル署名**」の横にあるチェック・ボックスにチェック・マークを付けます。
7. 「説明」の内容を「**CommMan Signing**」に変更します。
8. 「**状況**」を「**有効**」に設定します。
9. 「**参照**」をクリックします。
10. デジタル証明書 partnerTwoSigning.der の保存先ディレクトリーに移動し、証明書を選択して、「**開く**」をクリックします。
11. 「**アップロード**」をクリックし、次に「**保存**」をクリックします。

デジタル署名の初期構成はこれで完了です。

パートナーは、公開証明書を使用して、ハブに送信される署名付きトランザクションを認証します。

ハブは秘密鍵を使用して、パートナーに送信されるアウトバウンド・トランザクションにデジタル署名をします。まずは、秘密鍵をデジタル署名に使用できるようにします。

秘密鍵をデジタル署名に使用できるようにするには、以下のステップを実行します。

1. 水平ナビゲーション・バーから、「**アカウント管理**」>「**プロファイル**」>「**証明書**」をクリックします。
2. 「**ハブ・オペレーター (Hub Operator)**」の横にある「**詳細の表示**」アイコンをクリックします。
3. 「**CommManPrivate**」の横にある「**詳細の表示**」アイコンをクリックします。

   **注:** これは、以前にハブにロードされた秘密証明書です。
4. 「**編集**」アイコンをクリックします。
5. 「**デジタル署名**」の横にあるチェック・ボックスにチェック・マークを付けます。

   **注:** 複数のデジタル署名証明書がある場合は、「**証明書の使用**」リストから「**1 次**」または「**2 次**」を選択して、1 次証明書と 2 次証明書を選択します。
6. 「**保存**」をクリックします。

次に、署名付き AS2 に対応できるように、内部パートナーと Partner Two 間で設定されているパートナー接続の属性を変更します。

パートナー接続の属性を変更するには、以下のステップを実行します。

1. 水平ナビゲーション・バーから「**アカウント管理**」>「**接続**」をクリックします。
2. 「**ソース**」リストから「**内部パートナー**」を選択します。
3. 「**ターゲット**」リストから **Partner Two** を選択します。
4. 「**検索**」をクリックします。
5. Partner Two の「**属性**」ボタンをクリックします。
6. 「**パッケージ: AS (N/A)**」の横にある「**展開 (Expand)**」アイコンをクリックして、「**AS 署名済み**」属性を編集します。
7. 「**AS 署名済み**」リストから「**はい**」を選択します。
8. 「**保存**」をクリックします。

署名付きの AS2 トランザクションを WebSphere Partner Gateway からパートナーに送信するために必要な構成はこれで完了です。

# 基本構成の拡張

ここでは、この付録で説明した基本構成に変更を加える方法について説明します。ここでは、前述と同じパートナーと設定 (DUNS ID 123456789 とファイル・ディレクトリー宛先を使用する内部パートナー、DUNS ID 987654321 と HTTP 宛先を使用するパートナー PartnerTwo) を使用して、以下のサポートを追加する方法について説明します。

- FTP トランスポート
- カスタム XML 文書
- バイナリー・ファイル (パッケージ化なし)

## FTP レシーバーの作成

### このタスクについて

FTP レシーバーは、ファイルを受信し、そのファイルを処理するために文書マネージャーに渡します。 35 ページの『文書を受信する FTP サーバーの構成』 で述べたように、FTP レシーバーを作成するには、FTP サーバーをインストールし、FTP ディレクトリーを作成して、FTP サーバーを構成しておく必要があります。

この例では、FTP サーバーが Partner Two 用に構成されており、ルート・ディレクトリーが c:/ftproot であるものと想定します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックします。
2. 「**レシーバーの作成**」をクリックします。
3. 以下の情報を入力します。
   a. レシーバー名: **FTP_Receiver**
   b. トランスポート: **FTP ディレクトリー**
   c. FTP ルート・ディレクトリー: **C:/ftproot**
4. 「**保存**」をクリックします。

## バイナリー・ファイルを受信するためのハブ設定

ここでは、Partner Two から内部パートナーに送信するバイナリー文書を受信するためのハブ構成に必要なステップについて説明します。

### バイナリー文書のインタラクションの作成

### このタスクについて

デフォルトでは、WebSphere Partner Gateway にはバイナリー文書を使用する 4 つの対話があります。ただし、「なし」としてパッケージ化された文書とともにパートナーに送信される、「なし」としてパッケージ化されたバイナリー文書用のインタラクションは用意されていません。ここでは、バイナリー文書がシステムをパススルーするために必要なインタラクションを作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」リンクをクリックします。
3. 「**インタラクションの管理**」ビューから「**作成**」 をクリックします。

4. 「**ソース**」から、「**パッケージ: なし**」、「**プロトコル: バイナリー (1.0)**」、「**文書タイプ: バイナリー (1.0)**」を選択します。
5. 「**ターゲット**」から、「**パッケージ: なし**」、「**プロトコル: バイナリー (1.0)**」、「**文書タイプ: バイナリー (1.0)**」を選択します。
6. (オプション) 「**変換**」マップを選択します。
7. 「**アクション**」リストから「**パススルー**」を選択します。
8. 「**保存**」をクリックします。

## 内部パートナー用の B2B 機能の更新

### このタスクについて

ここでは、バイナリー文書を受け入れられるように内部パートナーを構成する方法について説明します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. 「**Comm Man**」の横にある「**詳細の表示**」アイコンをクリックします。
4. 「**B2B 機能**」をクリックします。
5. 「**ターゲットの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
6. 「**パッケージ: なし**」の横にある「**展開 (Expand)**」アイコンをクリックします。
7. 「**ターゲットの設定**」の下で、「**プロトコル: バイナリー (1.0)**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
8. 「**プロトコル: バイナリー (1.0)**」の横にある「**展開 (Expand)**」アイコンをクリックします。
9. 「**ターゲットの設定**」の下で、「**文書タイプ: バイナリー (1.0)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

## Partner Two 用の B2B 機能の更新

### このタスクについて

ここでは、バイナリー文書を送信できるように Partner Two を構成する方法について説明します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. Partner Two の横にある「**詳細の表示**」アイコンをクリックします。
4. 「**B2B 機能**」をクリックします。
5. 「**ソースの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
6. 「**パッケージ: なし**」の横にある「**展開 (Expand)**」アイコンをクリックします。
7. 「**ソースの設定**」の下で、「**プロトコル: バイナリー (1.0)**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。

8. 「**プロトコル: バイナリー (1.0)**」の横にある「**展開 (Expand)**」アイコンをクリックします。
9. 「**ソースの設定**」の下で、「**文書タイプ: バイナリー (1.0)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

### パートナー接続の新規作成

#### このタスクについて

ここでは、バイナリー文書用に内部パートナーと Partner Two 間で新しいパートナー接続を構成する方法について説明します。

1. 「**アカウント管理**」>「**接続**」をクリックします。
2. 「**ソース**」リストから **Partner Two** を選択します。
3. 「**ターゲット**」リストから「**内部パートナー**」を選択します。
4. 「**検索**」をクリックします。
5. **なし (N/A)、バイナリー (1.0)、バイナリー (1.0)** から**なし (N/A)、バイナリー (1.0)、バイナリー (1.0)** への接続を探し、「**アクティブ化**」をクリックしてこの接続をアクティブにします。

## カスタム XML 文書用のハブ設定

162 ページの『カスタム XML 文書処理』で述べたように、カスタム XML ファイルをルーティングできるようにハブを構成する必要があります。ここでは、以下の XML 文書をルーティングできるように文書マネージャーを構成するためのステップについて説明します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Tester>
<Tester type="Test type A">
    <From>987654321</From>
    <To>123456789</To>
</Tester>
```

この例の場合、文書マネージャーは、ルート・タグを使用して XML 文書のタイプを識別します。この後、「送信元 (From)」および「送信先 (To)」フィールドから値を抽出して、「送信側パートナー」ビジネス ID と「受信側パートナー」ビジネス ID を識別します。

### カスタム XML プロトコル定義形式の作成

#### このタスクについて

まず、交換を行うカスタム XML 用のプロトコルを新規作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**文書定義の作成**」をクリックします。
3. 「**文書定義タイプ**」リストから「**プロトコル**」を選択します。
4. 以下の情報を入力します。
   a. コード: **カスタム XML**
   b. バージョン: **1.0**
   c. 説明: **プロトコル定義の例**
5. 「**文書レベル**」を「**いいえ**」に設定します。

6. 「**状況**」を「**有効**」に設定します。
7. 「**可視/不可視: ハブ管理者 (Visibility: Hub Administrator)**」を「**はい**」に設定します。
8. 「**可視/不可視: 内部パートナー (Visibility: Internal Partner)**」を「**はい**」に設定します。
9. 「**可視/不可視: パートナー (Visibility: Partner)**」を「**はい**」に設定します。
10. 以下のものを選択します。
    a. パッケージ: **AS**
    b. パッケージ: **なし**
    c. パッケージ: **バックエンド統合**
11. 「**保管**」をクリックします。

## Tester_XML 文書定義の作成

### このタスクについて

次に、新しいプロトコルの文書定義を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**文書定義の作成**」をクリックします。
3. 「**文書定義タイプ**」リストから、「**文書タイプ**」を選択します。
4. 以下の情報を入力します。
    a. 名前: **Tester_XML**
    b. バージョン: **1.0**
    c. 説明: **カスタム XML 文書タイプの例**
5. 「**文書レベル**」を「**はい**」に設定します。
6. 「**状況**」を「**有効**」に設定します。
7. 「**可視/不可視: ハブ管理者 (Visibility: Hub Administrator)**」を「**はい**」に設定します。
8. 「**可視/不可視: 内部パートナー (Visibility: Internal Partner)**」を「**はい**」に設定します。
9. 「**可視/不可視: パートナー (Visibility: Partner)**」を「**はい**」に設定します。
10. 「**パッケージ: AS**」の横にある「**展開 (Expand)**」アイコンをクリックし、「**プロトコル: CustomXML**」を選択します。
11. 「**パッケージ: なし**」の横にある「**展開 (Expand)**」アイコンをクリックし、「**プロトコル: CustomXML**」を選択します。
12. 「**パッケージ: バックエンド統合 (Package: Backend Integration)**」の横にある「**展開 (Expand)**」アイコンをクリックし、「**プロトコル: CustomXML**」を選択します。
13. 「**保存**」をクリックします。

## Tester_XML 形式の作成
### このタスクについて

最後に、新しいプロトコルと関連付ける XML 形式を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**XML 形式**」をクリックします。
2. 「**文書ファミリーの作成**」をクリックします。
3. 以下の情報を入力または選択します。
   a. ファミリー名: **Example family**
   b. プロトコル: **カスタム XML 1.0**
   c. ファミリー・タイプ: **ルート・タグ**
   d. ラージ・ファイル・オプション: **なし**
   e. ファミリー ID: **Tester**
4. 「**保存**」をクリックします。
5. 表示される「文書ファミリー」ページで、「**XML 形式の作成**」をクリックします。
6. 「文書タイプ」リストから「**Tester_XML**」を選択します。
7. 「フォーマット ID」値に、「**Test type A**」を入力します。
8. 「フォーマット ID」の「XPath 式」に、「**/Tester/@type**」を入力します。
9. 「プレフィックス・ネーム・スペース」フィールドはブランクのままにし (文書内ではネーム・スペースは使用されません)、「戻りの型」に「**テキスト**」を指定します。
10. 「フォーマット・バージョン」値フィールドと「XPath 式」フィールドの両方に **1** を入力します。「戻りの型」を「**定数**」に変更します。これは、フォーマット ID が「Tester」であるすべての文書が、このフォーマットに一致する正しいバージョンであることを意味します。これは、すべての文書のバージョンが 1 で、このフォーマットのバージョンも 1 だからです。したがって、バージョンは常に一致します。
11. 「ソース・ビジネス ID」の「XPath 式」に「**/Tester/From**」を入力します。
12. 「ターゲット・ビジネス ID」の「XPath 式」に「**/Tester/To**」を入力します。
13. 残りのフィールドは現在のフォーマットのままにします。これらはオプションであり、この例では使用しません。
14. 「**保存**」をクリックします。

## Tester_XML 文書用のインタラクションの作成
### このタスクについて

これで、インタラクションの設定に使用する新規プロトコルと文書タイプが準備できました。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの作成**」をクリックします。
3. 「**ソース**」から、以下のものを選択します。
   a. パッケージ: **なし**
   b. プロトコル: **カスタム XML (1.0)**

c. 文書タイプ: **Tester_XML (1.0)**

4. 「**ターゲット**」から、以下のものを選択します。
   a. パッケージ: **なし**
   b. プロトコル: **カスタム XML (1.0)**
   c. 文書タイプ: **Tester_XML (1.0)**
5. 「**アクション**」リストから「**パススルー**」を選択します。
6. 「**保存**」をクリックします。

## 内部パートナー用の B2B 機能の更新

### このタスクについて

カスタム XML 文書を交換できるようにするには、パートナーの B2B 機能を更新する必要があります。

最初に、内部パートナーが Tester_XML 文書を受信できる (そのターゲットになれる) ようにします。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. パートナーのリストから内部パートナーを選択します。(この例では、内部パートナーのビジネス ID が 123456789 であると想定しています。)
4. 「**B2B 機能**」をクリックします。
5. 「**ターゲットの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
6. 「**パッケージ: なし**」の横にある「**展開 (Expand)**」アイコンをクリックします。
7. 「**ターゲットの設定**」で、「**プロトコル: カスタム XML (1.0)**」 に対して「**役割はアクティブではありません**」アイコンをクリックします。
8. 「**プロトコル: カスタム XML (1.0)**」の横にある「**展開**」アイコンをクリックします。
9. 「**ターゲットの設定**」で、「**文書タイプ: Tester_XML (1.0)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

## Partner Two 用の B2B 機能の更新

### このタスクについて

新しいカスタム XML 形式を使用してメッセージの交換を実行できるようにするには、Partner Two の B2B 機能を更新します。

Partner Two が Tester_XML 文書のソースになれるようにします。(この例では、Partner Two のビジネス ID が 987654321 であると想定しています。)

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックします。
2. 「**検索**」をクリックします。
3. パートナーのリストから **Partner Two** を選択します。(この例では、Partner Two のビジネス ID が 987654321 であると想定しています。)
4. 「**B2B 機能**」をクリックします。

5. 「**ソースの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
6. 「**パッケージ: なし**」の横にある「**展開 (Expand)**」アイコンをクリックします。
7. 「**ソースの設定**」で、「**プロトコル: カスタム XML (1.0)**」 に対して「**役割はアクティブではありません**」アイコンをクリックします。
8. 「**プロトコル: カスタム XML (1.0)**」の横にある「**展開**」アイコンをクリックします。
9. 「**ソースの設定**」で、「**文書タイプ: Tester_XML (1.0)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

## パートナー接続の新規作成

### このタスクについて

最後に、パートナー接続を新規作成します。

1. 「**アカウント管理**」>「**接続**」をクリックします。
2. 「**ソース**」リストから **Partner Two** を選択します。
3. 「**ターゲット**」リストから「**内部パートナー**」を選択します。
4. 「**検索**」をクリックします。
5. **なし (N/A)、カスタム XML (1.0)、Tester_XML(1.0)** から**なし (N/A)、カスタム XML(1.0)、Tester_XML (1.0)** への接続を探し、「**アクティブ化**」をクリックしてこの接続をアクティブにします。

## カスタム XML を使用した文書のルーティング

XML の例をこの例の最初からコピーし、テキスト・エディターに貼り付けてください。ファイルに適当な名前を付けてマシンに保管します。その後、ファイル・レシーバーが使用するディレクトリーにファイルをドロップして、そのファイルをハブに送信します。文書ビューアーで調べると、定義された接続を使用して、Partner Two が内部パートナーに経路指定されていることがわかるはずです。

# 第 19 章 EDI の例

この付録では、EDI 交換を送受信し、XML 文書およびレコード指向データ (ROD) 文書に変換したり、それらの文書から変換したりする例を示します。

この付録の例は、 327 ページの『第 18 章 基本的な例』に示した例とは関係ありません。この付録では、例で使用している新しいターゲット、宛先、およびプロファイルを作成します。

**注:** 327 ページの『第 18 章 基本的な例』では、ハブを経由して渡される EDI 交換 (エンベロープ解除または変換は発生しない) の例を示しています。

これらの 4 つの例では、必要なすべての手順を示しています。例えば、EDI から XML への変換の例に従うと、その例に必要なすべての手順 (ターゲットの作成から接続のアクティブ化まで) を確認できます。

この付録のトピックは以下のとおりです。

- 『 EDI から ROD への例』
- 363 ページの『 EDI から XML への例』
- 369 ページの『 XML から EDI への例』
- 377 ページの『 ROD から EDI への例』

これらの例では、システムの構成に必要なステップの概要を示します。これらの例を使用してシステムをセットアップする場合は、業務上の必要に合わせて特定の情報 (名前やビジネス ID など) を変更してください。

## EDI から ROD への例

このセクションでは、EDI トランザクションを (エンベロープに包んで) ハブに送信する例を示します。EDI トランザクションはハブでレコード指向データ (ROD) 文書に変換され、内部パートナーに送信されます。

### EDI 交換のエンベロープ解除と変換

#### このタスクについて

この例では、Data Interchange Services のマッピング担当者が変換マップを作成したと想定しています。その変換マップは、標準の EDI 850 トランザクション (X12 のバージョン 5010 に対応した X12V5R1 ディクショナリーを使用して定義されたもの) を受け取り、レコード指向文書 (ROD) に変換します。変換された文書は、内部パートナーのバックエンド・アプリケーションによって処理されます。この例のマップは S_DT_EDI_TO_ROD.eif という名前です。

Data Interchange Services のマッピング担当者は、変換マップを WebSphere Partner Gateway データベースに直接エクスポートすることができます。あるいは、Data Interchange Services のマッピング担当者からユーザーにファイルを送信することもできます。その場合、ユーザーは bcgDISImport ユーティリティーを使用してファイ

ルを WebSphere Partner Gateway にインポートします。この付録では、後者のシナリオを想定しています。

## 変換マップのインポート

### このタスクについて

このセクションでは、EDI 入力を受け取ってレコード指向データ (ROD) 形式に変換する変換マップのインポート手順について説明します。変換マップをインポートするプロセスで、マップに関連付けられた文書定義もインポートします。

変換マップをインポートする前に、Data Interchange Services のマッピング担当者から変換マップを受信する必要があります。この一連の手順では、S_DT_EDI_TO_ROD.eif というファイルがシステムにあることを前提にしています。

1. コマンド・ウィンドウを開きます。
2. 以下のコマンドまたはスクリプトを入力します。
   - UNIX システムの場合:

     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
     <password> S_DT_EDI_TO_ROD.eif
     ```

   - Windows システムの場合:

     ```
     <ProductDir>¥bin¥bcgDISImport.bat <database_user_ID>
     <password> S_DT_EDI_TO_ROD.eif
     ```

     ここで、*<database_user_ID>* と *<password>* は、WebSphere Partner Gateway のインストール作業の一部としてデータベースをインストールしたときに使用した値です。

## 変換マップと文書定義の検証

### このタスクについて

インポートした変換マップと文書定義がコミュニティー・コンソールに表示されることを確認するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**変換マップ**」の順にクリックします。

   S_DT_EDI_TO_ROD マップが表示されます。
2. マップの横にある「**詳細の表示**」アイコンをクリックします。

   このマップが関連付けられている文書定義を確認できます。

*表 33. マップに関連付けられた文書定義*

| ソース | ターゲット |
|---|---|
| パッケージ: N/A プロトコル: X12V5R1 (すべて)文書タイプ: 850 (すべて) | パッケージ: なしプロトコル: DEMO850CL_DICTIONARY (すべて) 文書タイプ: DEMO850CLSUW (すべて) |

S_DT_EDI_TO_ROD マップは、X12 850 トランザクション (X12V5R1 規格に準拠) を読み込み、カスタム・プロトコル (DEMO850CL_DICTIONARY) および文書タイプ (DEMO850CLSUW) に変換するように定義されています。

## レシーバーの構成

### このタスクについて

このセクションでは、ハブ用のファイル・システム・ディレクトリー・レシーバーを作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックし、「**レシーバーの作成**」をクリックします。
2. 「レシーバー名」に **EDIFileTarget** と入力します。
3. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
4. 「ルート・パス (Root Path)」に **/Data/Manager/editarget** と入力します。
5. 「**保管**」をクリックします。

パートナーは、このレシーバーに EDI 交換を送信します。

## インタラクションの作成

### このタスクについて

2 つの対話を作成します。1 つは EDI エンベロープ用、もう 1 つは EDI エンベロープ内でのトランザクション用です。

EDI エンベロープを表す対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの作成**」をクリックします。
3. 「**ソース**」の下で、「**パッケージ: なし**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
4. 「**ターゲット**」の下で、「**パッケージ: N/A**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
5. 「アクション」リストから「**EDI エンベロープ解除**」を選択します。

   **注:** この対話では、変換は発生しません。EDI 交換のエンベロープ解除が行われ、個々のトランザクション (850) が取り出されます。そのため、この対話に変換マップは必要ありません。
6. 「**保存**」をクリックします。

850 トランザクションを表すソースと、変換された文書を表すターゲットを持つ対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの作成**」をクリックします。
3. 「**ソース**」の下で、「**パッケージ: N/A**」および「**プロトコル: X12V5R1**」を展開し、「**文書タイプ: 850**」を選択します。
4. 「**ターゲット**」の下で、「**パッケージ: なし**」および「**プロトコル: DEMO850CL_DICTIONARY**」を展開し、「**文書タイプ: DEMO850CLSUW**」を選択します。
5. 「変換マップ」リストから「**S_DT_EDI_TO_ROD**」を選択します。
6. 「アクション」リストから「**EDI 検証および EDI 変換**」を選択します。
7. 「**保存**」をクリックします。

この対話は、標準の EDI X12 850 トランザクションから別の形式への変換を表します。したがって、変換マップを選択する必要があります。

## パートナーの作成

### このタスクについて

この例のパートナーは、内部パートナー (Manager) と外部パートナー (TP1) の 2 つです。

内部パートナー・プロファイルを作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**作成**」をクリックします。
2. 「会社ログイン名」に **ComManager** と入力します。
3. 「パートナー表示名」に **Manager** と入力します。
4. 「パートナー・タイプ」に「**内部パートナー**」を選択してください。
5. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `000000000` を入力します。

   **注:** DUNS ではなく Freeform を必ず選択してください。
6. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `01-000000000` を入力します。
7. 「**保存**」をクリックします。

2 番目のパートナーを作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**作成**」をクリックします。
2. 「会社ログイン名」に **TP1** と入力します。
3. 「パートナー表示名」に **TP1** と入力します。
4. 「パートナー・タイプ」に「**外部パートナー**」を選択してください。
5. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `000000001` を入力します。

   **注:** DUNS ではなく Freeform を必ず選択してください。
6. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `01-000000001` を入力します。
7. 「**保存**」をクリックします。

## 宛先の作成

### このタスクについて

この例の両方のパートナー用にファイル・ディレクトリー宛先を作成します。最初に、Manager 用の宛先を作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. Manager プロファイルの横にある「**詳細の表示**」アイコンをクリックします。
3. 「**宛先**」をクリックし、次に「**作成**」をクリックします。

4. 宛先に関する以下の値を入力します。ファイル・ディレクトリー (パス全体) がファイル・システムに既に存在している必要があります。
   a. 「名前」に **ManagerFileDestination** と入力します。
   b. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
   c. 「アドレス」に **file://Data/Manager/filedestination** と入力します。
   d. 「**保存**」をクリックします。
5. 「**リスト**」をクリックし、内部パートナー用の宛先をすべてリストします。
6. 「**デフォルト宛先の表示**」をクリックします。
7. 「**実動**」リストから、ステップ 4 で作成した宛先を選択します。
8. 「**保存**」をクリックします。

次に、パートナー用の宛先を作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. 「**TP1**」の横にある「**詳細の表示**」アイコンをクリックして、この例で作成した別のパートナーを選択します。
3. 「**宛先**」をクリックし、次に「**作成**」をクリックします。
4. 宛先に関する以下の値を入力します。ファイル・ディレクトリー (パス全体) は、既存のディレクトリーである必要があります。
   a. 「名前」に **TP1FileDestination** と入力します。
   b. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
   c. 「アドレス」に **file://Data/TP1/filedestination** と入力します。
   d. 「**保存**」をクリックします。
5. 「**リスト**」をクリックし、パートナー用の宛先をすべてリストします。
6. 「**デフォルト宛先の表示**」をクリックします。
7. 「**実動**」リストから、ステップ 4 で作成した宛先を選択します。
8. 「**保存**」をクリックします。

## B2B 機能の設定

### このタスクについて

この交換処理での 2 つのパートナーの B2B 機能を使用可能に設定します。この例では、EDI 交換は外部パートナー (TP1) から発信され、内部パートナーに配信されます。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. この例のソース・パートナー (**TP1**) に対して「**詳細の表示**」アイコンをクリックします。
3. 「**B2B 機能**」をクリックします。
4. ソース・パートナーに対して 2 組の機能を使用可能に設定します。
   a. 最初に、EDI エンベロープを表す文書定義を使用可能に設定します。

1) 「**ソースの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
2) 「**パッケージ: なし**」を展開します。
3) 「**ソースの設定**」の下で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。
5) 「**ソースの設定**」の下で、「**文書タイプ: ISA (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

b. 次に、850 トランザクションを表す文書定義を使用可能に設定します。
1) 「**ソースの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
2) 「**パッケージ: N/A**」を展開します。
3) 「**ソースの設定**」の下で、「**プロトコル: X12V5R1 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
4) 「**プロトコル: X12V5R1 (すべて)**」を展開します。
5) 「**ソースの設定**」の下で、「**文書タイプ: 850**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

5. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
6. この例のターゲット・パートナー (**Manager**) に対して「**詳細の表示**」アイコンをクリックします。
7. 「**B2B 機能**」をクリックします。
8. ターゲット・パートナーに対して 2 組の機能を使用可能に設定します。
a. 最初に、エンベロープを表す文書定義を使用可能に設定します。
1) 「**ターゲットの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
2) 「**パッケージ: N/A**」を展開します。
3) 「**ターゲットの設定**」の下で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。
5) 「**ターゲットの設定**」の下で、「**文書タイプ: ISA (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

b. 次に、変換した文書を表す文書定義を使用可能に設定します。
1) 「**ターゲットの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
2) 「**パッケージ: なし**」を展開します。
3) 「**ターゲットの設定**」の下で、「**プロトコル: DEMO850CL_DICTIONARY (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
4) 「**プロトコル: DEMO850CL_DICTIONARY (すべて)**」を展開します。

5) 「**ターゲットの設定**」の下で、「**文書タイプ: DEMO850CLSUW(すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

## 接続のアクティブ化

### このタスクについて

接続をアクティブ化するには、以下のステップを実行します。

1. 「**アカウント管理**」>「**接続**」をクリックします。
2. 「ソース」リストから「**TP1**」を選択します。
3. 「ターゲット」リストから「**Manager**」を選択します。
4. 「**検索**」をクリックします。
5. エンベロープを表す接続に対して「**アクティブ化**」をクリックします。

*表 34. エンベロープ接続*

| ソース | ターゲット |
|---|---|
| パッケージ: なし (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) | パッケージ: N/A (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) |

6. 変換した文書に対する 850 トランザクションを表す接続の「**アクティブ化**」をクリックします。

*表 35. ROD 文書接続に対する EDI トランザクション*

| ソース | ターゲット |
|---|---|
| パッケージ: N/A (N/A) プロトコル: X12V5R1文書タイプ: 850 (すべて) | パッケージ: なし (N/A) プロトコル: DEMO850CL_DICTIONARY (すべて) 文書タイプ: DEMO850CLSUW (すべて) |

## 属性の追加

### このタスクについて

重複 ID を持つ文書を許可する属性を設定します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**パッケージ: なし**」の横にある「**展開 (Expand)**」アイコンをクリックします。
3. 「**プロトコル: EDI-X12**」の横にある「**属性値の編集**」アイコンをクリックします。
4. このページの「文書タイプ・コンテキスト属性 (Document Type Context Attributes)」セクションにスクロールダウンします。「**文書 ID が重複する文書の許可 (Allow documents with duplicate document ids)**」の行で、リストから「**はい**」を選択します。
5. 「**保存**」をクリックします。

この時点で、TP1 が 850 トランザクションを含む EDI 交換を内部パートナーに送信すると、EDI 交換のエンベロープが解除されて 850 トランザクションが取り出されます。850 トランザクションは次に DEMO850CLSUW 文書タイプに変換され、

変換された文書が内部パートナーの宛先に送信されます。

## 交換への TA1 の追加

X12 では、TA1 は交換の受信確認に使用されるオプションのセグメントです。送信側は、ISA 交換制御ヘッダーの要素 14 を **1** に設定することによって、受信側に TA1 を要求できます。WebSphere Partner Gateway の「TA1 要求を許可」属性を使用すると、送信側から要求があったときに TA1 を送信するかどうかを制御できます。

WebSphere Partner Gateway のインストール時に &WDI_TA1_ACK マップがインストールされるので、このマップをインポートする必要はありません。

### 関連の作成

#### このタスクについて

マップと文書定義を関連付けるには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**EDI FA マップ**」の順にクリックします。

   &WDI_TA1_ACK マップが表示されます。
2. マップの横にある「**詳細の表示**」アイコンをクリックします。

   マップに関する情報と、システムで使用可能な各タイプのパッケージが入っているフォルダーが表示されます。
3. 以下のステップを実行して、文書定義との関連を作成します。
   a. 「**パッケージ: なし**」の横にあるチェック・ボックスを選択し、フォルダーを展開します。
   b. 「**プロトコル: EDI-X12 (すべて)**」の横にあるチェック・ボックスを選択し、フォルダーを展開します。
   c. 「**文書タイプ: ISA (すべて)**」の横にあるチェック・ボックスを選択します。
   d. 「**保存**」をクリックします。

これで、&WDI_TA1_ACK1 マップとエンベロープの文書定義との関連を作成しました。

### インタラクションの作成

#### このタスクについて

TA1 トランザクションを表す対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」リンクをクリックします。
3. 「**ソース**」の下で、「**パッケージ: N/A**」および「**プロトコル: &X44TA1**」を展開し、「**文書タイプ: TA1**」を選択します。
4. 「**ターゲット**」の下で、「**パッケージ: N/A**」および「**プロトコル: &X44TA1**」を展開し、「**文書タイプ: TA1**」を選択します。
5. 「アクション」リストから「**パススルー**」を選択します。
6. 「**保存**」をクリックします。

TA1 を保持する EDI エンベロープを表すソースを持つ対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」リンクをクリックします。
3. 「**ソース**」の下で、「**パッケージ: N/A**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
4. 「**ターゲット**」の下で、「**パッケージ: なし**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
5. 「アクション」リストから「**パススルー**」を選択します。
6. 「**保存**」をクリックします。

## B2B 機能の使用可能化

### このタスクについて

次に、新規に作成したインタラクションをパートナーの B2B 機能に追加します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. この例のソース・パートナー (**Manager**) に対して「**詳細の表示**」アイコンをクリックします。

   **注:** TA1 のフローは、ROD 文書を受信するパートナーから、その文書を送信したパートナーへの流れです。この例では、Manager が TA1 のソースであり、パートナー TP1 がターゲットです。
3. 「**B2B 機能**」をクリックします。
4. ソース・パートナーに対して 2 組の機能を使用可能に設定します。
   a. 最初に、TA1 用の機能を使用可能に設定します。
      1) 「**ソースの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ソースの設定**」の下で、「**プロトコル: &X44TA1**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: &X44TA1**」を展開します。
      5) 「**ソースの設定**」の下で、「**文書タイプ: TA1 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
   b. 次に、エンベロープ用の機能を使用可能に設定します。
      1) 「**ソースの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ソースの設定**」の下で、「**プロトコル: EDI-X12**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。
      5) 「**ソースの設定**」の下で、「**文書タイプ: ISA (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
5. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。

6. この例のターゲット・パートナー (**TP1**) に対して「**詳細の表示**」アイコンをクリックします。
7. 「**B2B 機能**」をクリックします。
8. ターゲット・パートナーに対して 2 組の機能を使用可能に設定します。
   a. 最初に、TA1 を表す文書定義を使用可能に設定します。
      1) 「**ターゲットの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ターゲットの設定**」の下で、「**プロトコル: &X44TA1 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: &X44TA1 (すべて)**」を展開します。
      5) 「**ターゲットの設定**」の下で、「**文書タイプ: TA1 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
   b. 次に、EDI エンベロープを表す文書定義を使用可能に設定します。
      1) 「**ターゲットの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: なし**」を展開します。
      3) 「**ターゲットの設定**」の下で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。
      5) 「**ターゲットの設定**」の下で、「**文書タイプ: ISA (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

## エンベロープ・プロファイルの作成

### このタスクについて

次に、TA1 を包むエンベロープのプロファイルを作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**EDI**」>「**エンベロープ・プロファイル**」の順にクリックします。
2. 「**作成**」をクリックします。
3. プロファイルの名前として **EnvProf1** を入力します。
4. 「EDI 標準」リストから「**X12**」を選択します。
5. 「**一般**」ボタンがデフォルトで選択されています。エンベロープの一般属性として以下の値を入力します。
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. 「**交換**」をクリックし、交換の属性として以下の値を入力します。
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**

- ISA04: **ISA0000004**
- ISA11: **¥**
- ISA12: **00501**
- ISA15: **T**

7. 「**保存**」をクリックします。

## パートナー接続のアクティブ化
### このタスクについて

接続をアクティブ化するには、以下のステップを実行します。

1. 「**アカウント管理**」>「**接続**」をクリックします。
2. 「ソース」リストから「**Manager**」を選択します。
3. 「ターゲット」リストから「**TP1**」を選択します。
4. 「**検索**」をクリックします。
5. TA1 を表す接続をアクティブにします。

*表 36. TA1 接続*

| ソース | ターゲット |
|---|---|
| パッケージ: N/A (N/A) プロトコル: &X44TA1 (すべて) 文書タイプ: TA1 (すべて) | パッケージ: N/A (N/A) プロトコル: &X44TA1 (すべて) 文書タイプ: TA1 (すべて) |

6. エンベロープを表す接続をアクティブにします。

*表 37. エンベロープ接続*

| ソース | ターゲット |
|---|---|
| パッケージ: N/A (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) | パッケージ: なし (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) |

## 属性の構成
### このタスクについて

エンベロープ・プロファイルの属性を指定するには、以下のステップを実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. リストから「**TP1**」を選択します。
3. 「**B2B 機能**」をクリックします。
4. 「**パッケージ: なし**」の横にある「**展開 (Expand)**」アイコンをクリックします。
5. 「**プロトコル: EDI-X12 (すべて)**」の横にある「**編集**」アイコンをクリックします。
6. 「**TA1 要求を許可**」の行で、「**はい**」を選択します。
7. 「**保存**」をクリックします。

8. 「**B2B 機能**」を再度クリックします。
9. 「**パッケージ: N/A**」の横にある「**展開 (Expand)**」アイコンをクリックします。
10. 「**プロトコル: &X44TA1 (すべて)**」の横にある「**編集**」アイコンをクリックします。
11. 以下の属性を指定します。
    a. 「エンベロープ・プロファイル」の行で、リストから「**EnvProf1**」を選択します。
    b. 「交換修飾子」の行に **01** と入力します。
    c. 「交換 ID」の行に **000000001** と入力します。
    d. 「交換の使用標識」の行に **T** と入力します。
12. 「**保存**」をクリックします。

この一連のタスクで、交換に TA1 確認通知を追加しました。交換を受信すると、WebSphere Partner Gateway は送信側 (TP1) に TA1 を送信します。TA1 は、エンベロープ・プロファイル EnvProf1 に準拠したエンベロープに包まれて送信されます。

## FA マップの追加

このセクションでは、 347 ページの『 EDI から ROD への例』で説明したフローに標準の機能確認通知 (997) を追加する方法について説明します。機能確認通知により、送信側はトランザクションが受信されたことを確認できます。

**注:** この例は 354 ページの『 交換への TA1 の追加』に似ています。ただし、その例に直接的な関連はありません。代わりに、この例は、 347 ページの『 EDI から ROD への例』で実行したタスクを基に作成されています。

WebSphere Partner Gateway には、事前にインストールされた、$DT_FA で始まる一連の機能確認通知マップ名が含まれています。その後に、機能確認通知メッセージの名前およびメッセージのバージョンとリリースが続きます。例えば、997 機能確認通知メッセージのバージョン 2 リリース 4 は、$DT_997V2R4 という名前になります。WebSphere Partner Gateway に提供されているマップのリストについては、222 ページの『確認通知の設定』を参照してください。

### 関連の作成

#### このタスクについて

マップと文書定義を関連付けるには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**EDI FA マップ**」の順にクリックします。

   &DT_FA997V2R4 マップが表示されます。
2. マップの横にある「**詳細の表示**」アイコンをクリックします。

   マップに関する情報と、システムで使用可能な各タイプのパッケージが入っているフォルダーが表示されます。
3. 以下のステップを実行して、文書定義との関連を作成します。

a. 「**パッケージ: N/A**」の横にあるチェック・ボックスを選択し、フォルダーを展開します。
b. 「**プロトコル: X12V5R1**」の横にあるチェック・ボックスを選択し、フォルダーを展開します。
c. 「**文書タイプ: 850**」の横にあるチェック・ボックスを選択します。
d. 「**保存**」をクリックします。

これで、この機能確認通知 997 マップが X12 プロトコルに関連付けられました。

## インタラクションの作成

### このタスクについて

997 確認通知を表す対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」をクリックします。
3. 「**ソース**」の下で、「**パッケージ: N/A**」および「**プロトコル: &DT99724**」を展開し、「**文書タイプ: 997**」を選択します。
4. 「**ターゲット**」の下で、「**パッケージ: N/A**」および「**プロトコル: &DT99724**」を展開し、「**文書タイプ: 997**」を選択します。
5. 「アクション」リストから「**パススルー**」を選択します。
6. 「**保存**」をクリックします。

エンベロープを表す対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」をクリックします。
3. 「**パッケージ: N/A**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
4. 「**パッケージ: なし**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
5. 「アクション」リストから「**パススルー**」を選択します。
6. 「**保存**」をクリックします。

## B2B 機能の使用可能化

### このタスクについて

次に、新規に作成したインタラクションをパートナーの B2B 機能に追加します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. この例のソース・パートナー (**Manager**) に対して「**詳細の表示**」アイコンをクリックします。

   **注:** 機能確認通知のフローは、ROD 文書を受信するパートナーから、その文書を送信したパートナーへの流れです。この例では、Manager が機能確認通知のソースであり、パートナー TP1 がターゲットです。
3. 「**B2B 機能**」をクリックします。

4. ソース・パートナーに対して 2 組の機能を使用可能に設定します。
   a. 最初に、FA 用の機能を使用可能に設定します。
      1) 「**ソースの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ソースの設定**」の下で、「**プロトコル: &DT99724**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: &DT99724**」を展開します。
      5) 「**ソースの設定**」の下で、「**文書タイプ: 997 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
   b. 次に、エンベロープ用の機能を使用可能に設定します。
      1) 「**ソースの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ソースの設定**」の下で、「**プロトコル: EDI-X12**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。
      5) 「**ソースの設定**」の下で、「**文書タイプ: ISA (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
5. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
6. この例のターゲット・パートナー (**TP1**) に対して「**詳細の表示**」アイコンをクリックします。
7. 「**B2B 機能**」をクリックします。
8. ターゲット・パートナーに対して 2 組の機能を使用可能に設定します。
   a. 最初に、997 を表す文書定義を使用可能に設定します。
      1) 「**ターゲットの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ターゲットの設定**」の下で、「**プロトコル: &DT99724 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: &DT99724 (すべて)**」を展開します。
      5) 「**ターゲットの設定**」の下で、「**文書タイプ: 997 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
   b. 次に、EDI エンベロープを表す文書定義を使用可能に設定します。
      1) 「**ターゲットの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: なし**」を展開します。
      3) 「**ターゲットの設定**」の下で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。

5) 「**ターゲットの設定**」の下で、「**文書タイプ: ISA(すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

## エンベロープ・プロファイルの作成

### このタスクについて

次に、997 機能確認通知を包むエンベロープのプロファイルを作成します。機能確認通知は、トランザクションと同様に、エンベロープに包んで送信する必要があります。

1. 「**ハブ管理**」>「**ハブ構成**」>「**EDI**」>「**エンベロープ・プロファイル**」の順にクリックします。
2. 「**作成**」をクリックします。
3. プロファイルの名前として **EnvProf1** を入力します。
4. 「EDI 標準」リストから「**X12**」を選択します。
5. 「**一般**」ボタンがデフォルトで選択されています。エンベロープの一般属性として以下の値を入力します。
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. 「**交換**」ボタンをクリックし、交換の属性として以下の値を入力します。
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: **¥**
   - ISA12: **00501**
   - ISA15: **T**
7. 「**保存**」をクリックします。

## パートナー接続のアクティブ化

### このタスクについて

接続をアクティブ化するには、以下のステップを実行します。

1. 「**アカウント管理**」>「**接続**」をクリックします。
2. 「ソース」リストから「**Manager**」を選択します。
3. 「ターゲット」リストから「**TP1**」を選択します。
4. 「**検索**」をクリックします。

5. 997 機能確認通知を表す接続に対して「**アクティブ化**」をクリックします。

*表 38. 機能確認通知接続*

| ソース | ターゲット |
|---|---|
| パッケージ: N/A (N/A) プロトコル: &DT99724 (すべて) 文書タイプ: 997 (すべて) | パッケージ: N/A (N/A) プロトコル: &DT99724 (すべて) 文書タイプ: 997 (すべて) |

6. 交換の発信元に送り返される EDI エンベロープを表す接続に対して、「**アクティブ化**」をクリックします。

*表 39. エンベロープ接続*

| ソース | ターゲット |
|---|---|
| パッケージ: N/A (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) | パッケージ: なし (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) |

## 属性の構成

### このタスクについて

最初に、使用する FA マップを指定します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. リストから「**TP1**」を選択します。
3. 「**B2B 機能**」をクリックします。
4. 「**パッケージ: N/A**」の横にある「**展開 (Expand)**」アイコンをクリックします。
5. 「**プロトコル: X12V5R1 (すべて)**」の横にある「**編集**」アイコンをクリックします。
6. 「FA マップ (FA Map)」の行で、「**&DT_FA997V2R4**」を選択します。
7. 「**B2B 機能**」を再度クリックします。
8. 「**パッケージ: N/A**」の横にある「**展開 (Expand)**」アイコンをクリックします。
9. 「**プロトコル: &DT99724 (すべて)**」の横にある「**編集**」アイコンをクリックします。
10. 以下の属性を指定します。
    a. 「エンベロープ・プロファイル」の行で、リストから「**EnvProf1**」を選択します。
    b. 「交換修飾子」の行に **01** と入力します。
    c. 「交換 ID」の行に **000000001** と入力します。
    d. 「交換の使用標識」の行に **T** と入力します。
11. 「**保存**」をクリックします。

この一連のタスクで、EDI-X12 997 機能確認通知を交換に追加しました。これにより、内部パートナーが文書を受信すると、送信側 (TP1) に 997 を送り返します。

997 確認通知は、エンベロープ・プロファイル EnvProf1 に準拠したエンベロープに包まれて送信されます。

## EDI から XML への例

このセクションでは、EDI トランザクションを (エンベロープに包んで) ハブに送信する例を示します。EDI トランザクションはハブで XML 文書に変換され、内部パートナーに送信されます。

この例では、Data Interchange Services のマッピング担当者が変換マップを作成したと想定しています。その変換マップは、標準の EDI 879 トランザクション (X12 のバージョン 5010 に対応した X12V5R1 ディクショナリーを使用して定義されたもの) を受け取り、XML 文書に変換します。変換された文書は、内部パートナーのバックエンド・アプリケーションによって処理されます。この例のマップは S_DT_EDI_TO_XML.eif という名前です。

Data Interchange Services のマッピング担当者は、変換マップを WebSphere Partner Gateway データベースに直接エクスポートすることができます。あるいは、Data Interchange Services のマッピング担当者からユーザーにファイルを送信することもできます。その場合、ユーザーは bcgDISImport ユーティリティーを使用してファイルを WebSphere Partner Gateway にインポートします。この付録では、後者のシナリオを想定しています。

### 変換マップのインポート

#### このタスクについて

このセクションでは、EDI 入力を受け取って XML 形式に変換する変換マップのインポート手順について説明します。変換マップをインポートするプロセスで、マップに関連付けられた文書定義もインポートします。

変換マップをインポートする前に、Data Interchange Services のマッピング担当者から変換マップを受信する必要があります。この一連の手順では、S_DT_EDI_TO_XML.eif というファイルがシステムにあることを前提にしています。

1. コマンド・ウィンドウを開きます。
2. 以下のコマンドまたはスクリプトを入力します。
   - UNIX システムの場合:

     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
      <password> S_DT_EDI_TO_XML.eif
     ```

   - Windows システムの場合:

     ```
     <ProductDir>¥bin¥bcgDISImport.bat <database_user_ID>
      <password> S_DT_EDI_TO_XML.eif
     ```

     ここで、*<database_user_ID>* と *<password>* は、WebSphere Partner Gateway のインストール作業の一部としてデータベースをインストールしたときに使用した値です。

## 変換マップと文書定義の検証

### このタスクについて

インポートした変換マップと文書定義がコミュニティー・コンソールに表示されることを確認するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**変換マップ**」の順にクリックします。

   S_DT_EDI_TO_XML マップが表示されます。
2. マップの横にある「**詳細の表示**」アイコンをクリックします。

   このマップが関連付けられている文書定義を確認できます。

*表 40. マップに関連付けられた文書定義*

| ソース | ターゲット |
|---|---|
| パッケージ: N/A プロトコル: X12V5R1 文書タイプ: 879 (すべて) | パッケージ: なしプロトコル: FVT-XML-TEST (すべて) 文書タイプ: WWRE_ITEMCREATIONINTERNAL (すべて) |

S_DT_EDI_TO_XML マップは、X12 879 トランザクション (X12V5R1 規格に準拠) を読み込み、カスタム・プロトコルに変換するように定義されています。

## レシーバーの構成

### このタスクについて

このセクションでは、ハブ用のファイル・システム・ディレクトリー・レシーバーを作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックし、「**レシーバーの作成**」をクリックします。
2. 「レシーバー名」に **EDIFileTarget** と入力します。
3. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
4. 「ルート・パス (Root Path)」に **/Data/Manager/editarget** と入力します。
5. 「**保管**」をクリックします。

パートナーは、このレシーバーに EDI 交換を送信します。

## インタラクションの作成

### このタスクについて

2 つの対話を作成します。1 つは EDI エンベロープ用、もう 1 つは EDI エンベロープ内でのトランザクション用です。

EDI エンベロープを表す対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」 > 「**インタラクションの管理**」をクリックします。
2. 「**パッケージ: なし**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。

3. 「**パッケージ: N/A**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
4. 「アクション」リストから「**EDI エンベロープ解除**」を選択します。

   **注:** この対話では、変換は発生しません。EDI 交換のエンベロープ解除が行われ、個々のトランザクション (879) が取り出されます。そのため、この対話に変換マップは必要ありません。
5. 「**保存**」をクリックします。

879 トランザクションを表すソースと、変換された文書を表すターゲットを持つ対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」をクリックします。
3. 「**パッケージ: N/A**」および「**プロトコル: X12V5R1**」を展開し、「**文書タイプ: 879**」を選択します。
4. 「**パッケージ: なし**」および「**プロトコル: FVT-XML-TEST**」を展開し、「**文書タイプ: WWRE_ITEMCREATIONINTERNAL**」を選択します。
5. 「変換マップ」リストから「**S_DT_EDI_TO_XML**」を選択します。
6. 「アクション」リストから「**EDI 検証および EDI 変換**」を選択します。
7. 「**保存**」をクリックします。

この対話は、標準の EDI X12 879 トランザクションから別の形式への変換を表します。したがって、変換マップを選択する必要があります。

# パートナーの作成

## このタスクについて

この例のパートナーは、内部パートナー (Manager) と外部パートナー (TP1) の 2 つです。

内部パートナー・プロファイルを作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**作成**」をクリックします。
2. 「会社ログイン名」に **ComManager** と入力します。
3. 「パートナー表示名」に **Manager** と入力します。
4. 「パートナー・タイプ」に「**内部パートナー**」を選択してください。
5. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `000000000` を入力します。

   **注:** DUNS ではなく Freeform を必ず選択してください。
6. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `01-000000000` を入力します。
7. 「**保存**」をクリックします。

2 番目のパートナーを作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**作成**」をクリックします。
2. 「会社ログイン名」に **TP1** と入力します。
3. 「パートナー表示名」に **TP1** と入力します。
4. 「パートナー・タイプ」に「**外部パートナー**」を選択してください。
5. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `000000001` を入力します。

   **注:** DUNS ではなく Freeform を必ず選択してください。
6. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `01-000000001` を入力します。
7. 「**保存**」をクリックします。

## 宛先の作成

### このタスクについて

この例の両方のパートナー用にファイル・ディレクトリー宛先を作成します。最初に、Manager 用の宛先を作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. Manager プロファイルの横にある「**詳細の表示**」アイコンをクリックします。
3. 「**宛先**」をクリックし、次に「**作成**」をクリックします。
4. 宛先に関する以下の値を入力します。ファイル・ディレクトリー (パス全体) がファイル・システムに既に存在している必要があります。
   a. 「名前」に **ManagerFileDestination** と入力します。
   b. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
   c. 「アドレス」に **file://Data/Manager/filedestination** と入力します。
   d. 「**保存**」をクリックします。
5. 「**リスト**」をクリックし、内部パートナー用の宛先をすべてリストします。
6. 「**デフォルト宛先の表示**」をクリックします。
7. 「**実動**」リストから、ステップ 4 で作成した宛先を選択します。
8. 「**保存**」をクリックします。

次に、パートナー用の宛先を作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. 「**TP1**」の横にある「**詳細の表示**」アイコンをクリックして、この例で作成した別のパートナーを選択します。
3. 「**宛先**」をクリックし、次に「**作成**」をクリックします。
4. 宛先に関する以下の値を入力します。ファイル・ディレクトリー (パス全体) は、既存のディレクトリーである必要があります。
   a. 「名前」に **TP1FileDestination** と入力します。

b. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
c. 「アドレス」に **file://Data/TP1/filedestination** と入力します。
d. 「**保存**」をクリックします。

5. 「**リスト**」をクリックし、パートナー用の宛先をすべてリストします。
6. 「**デフォルト宛先の表示**」をクリックします。
7. 「**実動**」リストから、ステップ 4 (366 ページ) で作成した宛先を選択します。
8. 「**保存**」をクリックします。

## B2B 機能の設定

### このタスクについて

この交換処理での 2 つのパートナーの B2B 機能を使用可能に設定します。この例では、EDI 交換は外部パートナー (TP1) から発信され、内部パートナーに配信されます。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. この例のソース・パートナー (**TP1**) に対して「**詳細の表示**」アイコンをクリックします。
3. 「**B2B 機能**」をクリックします。
4. ソース・パートナーに対して 2 組の機能を使用可能に設定します。
   a. 最初に、EDI エンベロープを表す文書定義を使用可能に設定します。
      1) 「**ソースの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: なし**」を展開します。
      3) 「**ソースの設定**」の下で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。
      5) 「**ソースの設定**」の下で、「**文書タイプ: ISA (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
   b. 次に、トランザクションを表す文書定義を使用可能に設定します。
      1) 「**ソースの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ソースの設定**」の下で、「**プロトコル: X12V5R1 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: X12V5R1 (すべて)**」を展開します。
      5) 「**ソースの設定**」の下で、「**文書タイプ: 879**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
5. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
6. この例のターゲット・パートナー (**Manager**) に対して「**詳細の表示**」アイコンをクリックします。

7. 「**B2B 機能**」をクリックします。
8. ターゲット・パートナーに対して 2 組の機能を使用可能に設定します。
   a. 最初に、文書定義を使用可能に設定します。
      1) 「**ターゲットの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ターゲットの設定**」の下で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。
      5) 「**ターゲットの設定**」の下で、「**文書タイプ: ISA (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
   b. 次に、変換した文書を表す文書定義を使用可能に設定します。
      1) 「**ターゲットの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: なし**」を展開します。
      3) 「**ターゲットの設定**」の下で、「**プロトコル: FVT-XML-TEST (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: FVT-XML-TEST (すべて)**」を展開します。
      5) 「**ターゲットの設定**」の下で、**文書タイプ: WWRE_ITEMCREATIONINTERNAL(すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

## 接続のアクティブ化

### このタスクについて

接続をアクティブ化するには、以下のステップを実行します。

1. 「**アカウント管理**」>「**接続**」をクリックします。
2. 「ソース」リストから「**TP1**」を選択します。
3. 「ターゲット」リストから「**Manager**」を選択します。
4. 「**検索**」をクリックします。
5. エンベロープを表す接続に対して「**アクティブ化**」をクリックします。

*表 41. エンベロープ接続*

| ソース | ターゲット |
|---|---|
| パッケージ: なし (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) | パッケージ: N/A (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) |

6. 変換した文書に対する 879 トランザクションを表す接続の「**アクティブ化**」をクリックします。

*表 42. XML 文書接続に対する EDI トランザクション*

| ソース | ターゲット |
|---|---|
| パッケージ: N/A (N/A) プロトコル: X12V5R1 (すべて)文書タイプ: 879 (すべて) | パッケージ: なし (N/A) プロトコル: FVT-XML-TEST (すべて) 文書タイプ: WWRE_ITEMCREATIONINTERNAL (すべて) |

この時点で、TP1 が 879 トランザクションを含む EDI 交換を内部パートナーに送信すると、EDI 交換のエンベロープが解除されて 879 トランザクションが取り出されます。次に、879 トランザクションは変換され、変換された文書が内部パートナーの宛先に送信されます。

## XML から EDI への例

このセクションでは、内部パートナーからハブに XML 文書を送信する例を示します。XML 文書はハブで EDI トランザクションに変換され、EDI 交換内のエンベロープに包まれてパートナーに送信されます。

この例では、Data Interchange Services のマッピング担当者が変換マップを作成したと想定しています。その変換マップは、XML 文書を受け取り、標準の EDI 850 トランザクション (MX12V3R1 ディクショナリーを使用して定義されたもの) に変換します。変換されたトランザクションは、パートナーによって処理されます。この例のマップは S_DT_XML_TO_EDI.eif という名前です。

Data Interchange Services のマッピング担当者は、変換マップを WebSphere Partner Gateway データベースに直接エクスポートすることができます。あるいは、Data Interchange Services のマッピング担当者からユーザーにファイルを送信することもできます。その場合、ユーザーは bcgDISImport ユーティリティーを使用してファイルを WebSphere Partner Gateway にインポートします。この付録では、後者のシナリオを想定しています。

### 変換マップのインポート

#### このタスクについて

このセクションでは、XML 入力を受け取って EDI トランザクションに変換する変換マップのインポート手順について説明します。変換マップをインポートするプロセスで、マップに関連付けられた文書定義もインポートします。

変換マップをインポートする前に、Data Interchange Services のマッピング担当者から変換マップを受信する必要があります。この一連の手順では、S_DT_XML_TO_EDI.eif というファイルがシステムにあることを前提にしています。

1. コマンド・ウィンドウを開きます。
2. 以下のコマンドまたはスクリプトを入力します。
   - UNIX システムの場合:

     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
      <password> S_DT_XML_TO_EDI.eif
     ```

   - Windows システムの場合:

```
<ProductDir>¥bin¥bcgDISImport.bat <database_user_ID>
 <password> S_DT_XML_TO_EDI.eif
```

ここで、*<database_user_ID>* と *<password>* は、WebSphere Partner Gateway のインストール作業の一部としてデータベースをインストールしたときに使用した値です。

## 変換マップと文書定義の検証

### このタスクについて

インポートした変換マップと文書定義がコミュニティー・コンソールに表示されることを確認するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**変換マップ**」の順にクリックします。

   S_DT_XML_TO_EDI マップが表示されます。
2. マップの横にある「**詳細の表示**」アイコンをクリックします。

   このマップが関連付けられている文書定義を確認できます。

*表 43. マップに関連付けられた文書定義*

| ソース | ターゲット |
|---|---|
| パッケージ: なしプロトコル: FVT-XML-TEST (すべて) 文書タイプ: ICGCPO (すべて) | パッケージ: N/A プロトコル: MX12V3R1 (すべて) 文書タイプ: 850 (すべて) |

S_DT_XML_TO_EDI マップは、XML 文書を受け取って EDI トランザクションに変換するように定義されています。

## レシーバーの構成

### このタスクについて

このセクションでは、ハブ用のファイル・システム・ディレクトリー・レシーバーを作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックし、「**レシーバーの作成**」をクリックします。
2. 「レシーバー名」に **XMLFileTarget** と入力します。
3. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
4. 「ルート・パス (Root Path)」に **/Data/Manager/xmltarget** と入力します。
5. 「構成ポイント (Configuration Point)」リストから「**前処理**」を選択します。
6. 「使用可能リスト」から「**com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler**」を選択し、「**追加**」をクリックして「構成済みリスト」に移動します。
7. 「**保管**」をクリックします。

内部パートナーは、このレシーバーに XML 文書を送信します。

## インタラクションの作成

### このタスクについて

2 つの対話を作成します。1 つは XML から EDI への変換用、もう 1 つは EDI エンベロープ用です。

XML 文書を表すソースと、変換された 850 トランザクションを表すターゲットを持つ対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」をクリックします。
3. 「**パッケージ: なし**」および「**プロトコル: FVT-XML-TEST**」を展開し、「**文書タイプ: ICGCPO**」を選択します。
4. 「**パッケージ: N/A**」および「**プロトコル: MX12V3R1**」を展開し、「**文書タイプ: 850**」を選択します。
5. 「変換マップ」リストから「**S_DT_XML_TO_EDI**」を選択します。
6. 「アクション」リストから「**XML 変換および EDI 検証**」を選択します。
7. 「**保存**」をクリックします。

この対話は、XML 文書から EDI トランザクションへの変換を表します。したがって、変換マップを選択する必要があります。

EDI エンベロープを表す対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」をクリックします。
3. 「**パッケージ: N/A**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
4. 「**パッケージ: なし**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
5. 「アクション」リストから「**パススルー**」を選択します。

   **注:** この対話では、変換は発生しません。
6. 「**保存**」をクリックします。

## パートナーの作成

### このタスクについて

この例のパートナーは、内部パートナー (Manager) と外部パートナー (TP1) の 2 つです。

内部パートナー・プロファイルを作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**作成**」をクリックします。
2. 「会社ログイン名」に **ComManager** と入力します。
3. 「パートナー表示名」に **Manager** と入力します。
4. 「パートナー・タイプ」に「**内部パートナー**」を選択してください。

5. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として 000000000 を入力します。

   **注:** DUNS ではなく Freeform を必ず選択してください。
6. 「ビジネス ID」に対して「**新規**」をクリックし、FreeForm ID として 01-000000000 を入力します。
7. 「**保存**」をクリックします。

2 番目のパートナーを作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**作成**」をクリックします。
2. 「会社ログイン名」に **TP1** と入力します。
3. 「パートナー表示名」に **TP1** と入力します。
4. 「パートナー・タイプ」に「**外部パートナー**」を選択してください。
5. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として 000000001 を入力します。

   **注:** DUNS ではなく Freeform を必ず選択してください。
6. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として 01-000000001 を入力します。
7. 「**保存**」をクリックします。

## 宛先の作成

### このタスクについて

この例の両方のパートナー用にファイル・ディレクトリー宛先を作成します。最初に、Manager 用の宛先を作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. Manager プロファイルの横にある「**詳細の表示**」アイコンをクリックします。
3. 「**宛先**」をクリックし、次に「**作成**」をクリックします。
4. 宛先に関する以下の値を入力します。ファイル・ディレクトリー (パス全体) がファイル・システムに既に存在している必要があります。
   a. 「名前」に **ManagerFileDestination** と入力します。
   b. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
   c. 「アドレス」に **file://Data/Manager/filedestination** と入力します。
   d. 「**保存**」をクリックします。
5. 「**リスト**」をクリックし、内部パートナー用の宛先をすべてリストします。
6. 「**デフォルト宛先の表示**」をクリックします。
7. 「**実動**」リストから、ステップ 4 で作成した宛先を選択します。
8. 「**保存**」をクリックします。

次に、パートナー用の宛先を作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. 「**TP1**」の横にある「**詳細の表示**」アイコンをクリックして、この例で作成した別のパートナーを選択します。
3. 「**宛先**」をクリックし、次に「**作成**」をクリックします。
4. 宛先に関する以下の値を入力します。ファイル・ディレクトリー (パス全体) は、既存のディレクトリーである必要があります。
   a. 「名前」に **TP1FileDestination** と入力します。
   b. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
   c. 「アドレス」に **file://Data/TP1/filedestination** と入力します。
   d. 「**保存**」をクリックします。
5. 「**リスト**」をクリックし、パートナー用の宛先をすべてリストします。
6. 「**デフォルト宛先の表示**」をクリックします。
7. 「**実動**」リストから、ステップ 4 で作成した宛先を選択します。
8. 「**保存**」をクリックします。

## B2B 機能の設定

### このタスクについて

この交換処理での 2 つのパートナーの B2B 機能を使用可能に設定します。この例では、XML 文書は内部パートナーから発信され、外部パートナーに配信されます。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. この例のソース・パートナー (**ComMan**) に対して「**詳細の表示**」アイコンをクリックします。
3. 「**B2B 機能**」をクリックします。
4. ソース・パートナーに対して 3 組の機能を使用可能に設定します。
   a. XML 文書を表す文書定義を使用可能に設定します。
      1) 「**ソースの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: なし**」を展開します。
      3) 「**ソースの設定**」の下で、「**プロトコル: FVT-XML-TEST (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: FVT-XML-TEST (すべて)**」を展開します。
      5) 「**ソースの設定**」の下で、「**文書タイプ: ICGCPO (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
   b. 次に、変換した文書を表す文書定義を使用可能に設定します。
      1) 「**ソースの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ソースの設定**」の下で、「**プロトコル: MX12V3R1 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

4) 「**プロトコル: MX12V3R1 (すべて)**」を展開します。

5) 「**ソースの設定**」の下で、「**文書タイプ: 850**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

c. 次に、EDI エンベロープを表す文書定義を使用可能に設定します。

1) 「**ソースの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。

2) 「**パッケージ: N/A**」を展開します。

3) 「**ソースの設定**」の下で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。

5) 「**ソースの設定**」の下で、「**文書タイプ: ISA (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

5. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。

6. この例のターゲット・パートナー (**TP1**) に対して「**詳細の表示**」アイコンをクリックします。

7. 「**B2B 機能**」をクリックします。

8. ターゲット・パートナーに対して 2 組の機能を使用可能に設定します。

a. 最初に、EDI 850 トランザクションを表す文書定義を使用可能に設定します。

1) 「**ターゲットの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。

2) 「**パッケージ: N/A**」を展開します。

3) 「**ターゲットの設定**」の下で、「**プロトコル: MX12V3R1 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

4) 「**プロトコル: MX12V3R1 (すべて)**」を展開します。

5) 「**ターゲットの設定**」の下で、「**文書タイプ: 850 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

b. 次に、文書定義を使用可能に設定します。

1) 「**ターゲットの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。

2) 「**パッケージ: なし**」を展開します。

3) 「**ターゲットの設定**」の下で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。

5) 「**ターゲットの設定**」の下で、「**文書タイプ: ISA(すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

## エンベロープ・プロファイルの作成

### このタスクについて

次に、変換された 850 トランザクションを包むエンベロープのプロファイルを作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**EDI**」>「**エンベロープ・プロファイル**」の順にクリックします。
2. 「**作成**」をクリックします。
3. プロファイルの名前として **EnvProf1** を入力します。
4. 「EDI 標準」リストから「**X12**」を選択します。
5. 「**一般**」ボタンがデフォルトで選択されています。エンベロープの一般属性として以下の値を入力します。
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. 「**交換**」をクリックし、交換の属性として以下の値を入力します。
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: **U**
   - ISA12: **00301**
   - ISA15: **T**
7. 「**保存**」をクリックします。

## XML 形式の作成

### このタスクについて

このセクションでは、カスタム XML 形式を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**XML 形式**」をクリックします。
2. 「**XML 形式の作成**」をクリックします。
3. 「ルーティング形式」で「**FVT-XML-TEST ALL**」を選択します。
4. 「ファイル・タイプ」で「**XML**」を選択します。
5. 「ID タイプ」で「**ルート・タグ**」を選択し、**MMDoc** と入力します。
6. 「ソース・ビジネス ID」で「**定数**」を選択し、**000000000** と入力します。
7. 「ターゲット・ビジネス ID」で「**定数**」を選択し、**000000001** と入力します。
8. 「ソース・ドキュメント・タイプ」で「**定数**」を選択し、**ICGCPO** と入力します。
9. 「ソース・ドキュメント・タイプ・バージョン」で「**定数**」を選択し、**ALL** と入力します。
10. 「**保存**」をクリックします。

## 接続のアクティブ化

### このタスクについて

パートナー接続をアクティブ化します。

1. 「**アカウント管理**」>「**接続**」をクリックします。
2. 「ソース」リストから「**Manager**」を選択します。
3. 「ターゲット」リストから「**TP1**」を選択します。
4. 「**検索**」をクリックします。
5. 以下の接続に対して「**アクティブ化**」をクリックします。

*表 44. XML 文書から EDI へのトランザクション接続*

| ソース | ターゲット |
|---|---|
| パッケージ: なし (N/A) プロトコル: FVT-XML-TEST (すべて) 文書タイプ: ICGCPO (すべて) | パッケージ: N/A (N/A) プロトコル: MX12V3R1 (すべて) 文書タイプ: 850 (すべて) |

6. EDI エンベロープを表す接続に対して「**アクティブ化**」をクリックします。

*表 45. EDI エンベロープ接続*

| ソース | ターゲット |
|---|---|
| パッケージ: N/A (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) | パッケージ: なし (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) |

## 属性の構成

### このタスクについて

ターゲット・パートナー (TP1) およびソース・パートナー (Manager) の B2B 機能の属性を構成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. 「**TPI**」の横にある「**詳細の表示**」アイコンをクリックして選択します。
3. 「**B2B 機能**」をクリックします。
4. 「**パッケージ: N/A**」の横にある「**展開 (Expand)**」アイコンをクリックします。
5. 「**プロトコル: MX12V3R1**」の横にある「**編集**」アイコンをクリックします。
6. 以下の属性を指定します。
   a. 「エンベロープ・プロファイル」の行で、リストから「**EnvProf1**」を選択します。
   b. 「交換修飾子」の行に **01** と入力します。
   c. 「交換 ID」の行に **000000001** と入力します。
   d. 「交換の使用標識」の行に **T** と入力します。
7. 「**保存**」をクリックします。

8. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
9. 「**Manager**」の横にある「詳細の表示」をクリックして選択します。
10. 「**B2B 機能**」をクリックします。
11. 「**パッケージ: N/A**」の横にある「**展開 (Expand)**」アイコンをクリックします。
12. 「**プロトコル: MX12V3R1 (すべて)**」の横にある「**編集**」アイコンをクリックします。
13. 以下の属性を指定します。
    a. 「交換修飾子」の行に **01** と入力します。
    b. 「交換 ID」の行に **000000000** と入力します。
    c. 「交換の使用標識」の行に **T** と入力します。
14. 「**保存**」をクリックします。

この時点で、ソース・パートナー (内部パートナー) がパートナーに XML 文書を送信すると、その文書は (ハブで) EDI トランザクションに変換され、エンベロープに包まれた後、パートナーの宛先に送信されます。

## ROD から EDI への例

このセクションでは、内部パートナーからハブに ROD 文書を送信する例を示します。ROD 文書はハブで EDI トランザクションに変換され、EDI 交換内のエンベロープに包まれてパートナーに送信されます。

この例では、Data Interchange Services のマッピング担当者が変換マップを作成したと想定しています。その変換マップは、レコード指向文書 (ROD) を受け取り、標準の EDI 850 トランザクション (X12 のバージョン 5010 に対応した X12V5R1 ディクショナリーを使用して定義されたもの) に変換します。変換されたトランザクションは、パートナーによって処理されます。この例のマップは S_DT_ROD_TO_EDI.eif という名前です。

Data Interchange Services のマッピング担当者は、変換マップを WebSphere Partner Gateway データベースに直接エクスポートすることができます。あるいは、Data Interchange Services のマッピング担当者からユーザーにファイルを送信することもできます。その場合、ユーザーは bcgDISImport ユーティリティーを使用してファイルを WebSphere Partner Gateway にインポートします。この付録では、後者のシナリオを想定しています。

### 変換マップのインポート

#### このタスクについて

このセクションでは、ROD 入力を受け取って X12 トランザクションに変換する変換マップのインポート手順について説明します。変換マップをインポートするプロセスで、マップに関連付けられた文書定義もインポートします。

変換マップをインポートする前に、Data Interchange Services のマッピング担当者から変換マップを受信する必要があります。この一連の手順では、S_DT_ROD_TO_EDI.eif というファイルがシステムにあることを前提にしています。

1. コマンド・ウィンドウを開きます。
2. 以下のコマンドまたはスクリプトを入力します。
   - UNIX システムの場合:

     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
      <password> S_DT_ROD_TO_EDI.eif
     ```

   - Windows システムの場合:

     ```
     <ProductDir>¥bin¥bcgDISImport.bat <database_user_ID>
      <password> S_DT_ROD_TO_EDI.eif
     ```

     ここで、*<database_user_ID>* と *<password>* は、WebSphere Partner Gateway のインストール作業の一部としてデータベースをインストールしたときに使用した値です。

## 変換マップと文書定義の検証

### このタスクについて

インポートした変換マップと文書定義がコミュニティー・コンソールに表示されることを確認するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**マップ**」>「**変換マップ**」の順にクリックします。

   S_DT_ROD_TO_EDI マップが表示されます。
2. マップの横にある「**詳細の表示**」アイコンをクリックします。

   このマップが関連付けられている文書定義を確認できます。

*表 46. マップに関連付けられた文書定義*

| ソース | ターゲット |
|---|---|
| パッケージ: なしプロトコル: ROD-TO-EDI_DICT (すべて) 文書タイプ: DTROD-TO-EDI_ROD (すべて) | パッケージ: N/A プロトコル: X12V5R1 (すべて) 文書タイプ: 850 (すべて) |

S_DT_ROD_TO_EDI マップは、ROD-TO-EDI_DICT ディクショナリーに関連付けられた ROD 文書を受け取り、X12V5R1 規格に準拠した X12 850 トランザクションに変換するように定義されています。

## レシーバーの構成

### このタスクについて

このセクションでは、ハブ用のファイル・システム・ディレクトリー・レシーバーを作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**レシーバー**」をクリックし、「**レシーバーの作成**」をクリックします。

2. 「レシーバー名」に **RODFileTarget** と入力します。
3. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
4. 「ルート・パス (Root Path)」に **/Data/Manager/rodtarget** と入力します。
5. 「構成ポイント (Configuration Point)」リストから「**前処理**」を選択します。
6. 「使用可能リスト」から「**com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler**」を選択し、「**追加**」をクリックして「構成済みリスト」に移動します。
7. 「構成済みリスト」から「**com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler**」を選択し、「**構成**」をクリックします。
8. 次の表に示す値を追加します。

*表 47. ROD スプリッター・ハンドラーの属性*

| フィールド | 値 |
|---|---|
| 送信元パッケージ名 (From Packaging Name) | なし |
| 送信元パッケージ・バージョン (From Packaging Version) | なし |
| 送信元プロトコル名 (From Protocol Name) | ROD-TO-EDI_DICT |
| 送信元プロトコル・バージョン (From Protocol Version) | ALL |
| 送信元プロセス・コード (From Process Code) | DTROD-TO-EDI_ROD |
| 送信元プロセス・バージョン (From Process Version) | ALL |
| METADICTIONARY | ROD-TO-EDI_DICT |
| METADOCUMENT | DTROD-TO-EDI_ROD |
| METASYNTAX | rod |
| ENCODING | ascii |
| BCG_BATCHDOCS | ON |

9. 「**値の設定 (Set Values)**」をクリックします。
10. 「**保管**」をクリックします。

内部パートナーは、このターゲットに ROD 文書を送信します。

## インタラクションの作成

### このタスクについて

2 つの対話を作成します。1 つはハブから送信される EDI エンベロープ用、もう 1 つは ROD 文書から EDI への変換用です。

ROD 文書を表すソースと、X12 文書をあらわすターゲットを持つ対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」をクリックします。

3. 「**パッケージ: なし**」および「**プロトコル: ROD-TO-EDI_DICT**」を展開し、「**DTROD-TO-EDI_ROD**」を選択します。
4. 「**パッケージ: N/A**」および「**プロトコル: X12V5R1**」を展開し、「**文書タイプ: 850**」を選択します。
5. 「変換マップ」リストから「**S_DT_ROD_TO_EDI**」を選択します。
6. 「アクション」リストから「**ROD 変換および EDI 検証**」を選択します。
7. 「**保存**」をクリックします。

この対話は、ROD 文書から標準の X12 トランザクションへの変換を表します。したがって、変換マップを選択する必要があります。

EDI エンベロープを表す対話を作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**インタラクションの管理**」をクリックします。
3. 「**パッケージ: N/A**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
4. 「**パッケージ: なし**」および「**プロトコル: EDI-X12**」を展開し、「**文書タイプ: ISA**」を選択します。
5. 「アクション」リストから「**パススルー**」を選択します。

   **注:** この対話では、変換は発生しません。この対話では、EDI 交換をエンベロープに包みます。
6. 「**保存**」をクリックします。

## パートナーの作成

### このタスクについて

この例のパートナーは、内部パートナー (Manager) と外部パートナー (TP1) の 2 つです。

内部パートナー・プロファイルを作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**作成**」をクリックします。
2. 「会社ログイン名」に **ComManager** と入力します。
3. 「パートナー表示名」に **Manager** と入力します。
4. 「パートナー・タイプ」に「**内部パートナー**」を選択してください。
5. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `000000000` を入力します。

   **注:** DUNS ではなく Freeform を必ず選択してください。
6. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `01-000000000` を入力します。
7. 「**保存**」をクリックします。

2 番目のパートナーを作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**作成**」をクリックします。
2. 「会社ログイン名」に **TP1** と入力します。
3. 「パートナー表示名」に **TP1** と入力します。
4. 「パートナー・タイプ」に「**外部パートナー**」を選択してください。
5. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `000000001` を入力します。

   **注:** DUNS ではなく Freeform を必ず選択してください。
6. 「ビジネス ID」に対して「**新規**」をクリックし、Freeform ID として `01-000000001` を入力します。
7. 「**保存**」をクリックします。

## 宛先の作成

### このタスクについて

この例の両方のパートナー用にファイル・ディレクトリー宛先を作成します。最初に、Manager 用の宛先を作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. Manager プロファイルの横にある「**詳細の表示**」アイコンをクリックします。
3. 「**宛先**」をクリックし、次に「**作成**」をクリックします。
4. 宛先に関する以下の値を入力します。ファイル・ディレクトリー (パス全体) がファイル・システムに既に存在している必要があります。
   a. 「名前」に **ManagerFileDestination** と入力します。
   b. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。
   c. 「アドレス」に **file://Data/Manager/filedestination** と入力します。
   d. 「**保存**」をクリックします。
5. 「**リスト**」をクリックし、内部パートナー用の宛先をすべてリストします。
6. 「**デフォルト宛先の表示**」をクリックします。
7. 「**実動**」リストから、ステップ 4 で作成した宛先を選択します。
8. 「**保存**」をクリックします。

次に、パートナー用の宛先を作成します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. 「**TP1**」の横にある「**詳細の表示**」アイコンをクリックして、この例で作成した別のパートナーを選択します。
3. 「**宛先**」をクリックし、次に「**作成**」をクリックします。
4. 宛先に関する以下の値を入力します。ファイル・ディレクトリー (パス全体) は、既存のディレクトリーである必要があります。
   a. 「名前」に **TP1FileDestination** と入力します。

b. 「トランスポート」リストから「**ファイル・ディレクトリー**」を選択します。

c. 「アドレス」に **file://Data/TP1/filedestination** と入力します。

d. 「**保存**」をクリックします。

5. 「**リスト**」をクリックし、パートナー用の宛先をすべてリストします。
6. 「**デフォルト宛先の表示**」をクリックします。
7. 「**実動**」リストから、ステップ 4 (381 ページ) で作成した宛先を選択します。
8. 「**保存**」をクリックします。

## B2B 機能の設定

### このタスクについて

この交換処理での 2 つのパートナーの B2B 機能を使用可能に設定します。この例では、ROD 文書は内部パートナーから発信され、外部パートナー (TP1) に配信されます。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. この例のソース・パートナー (**Manager**) に対して「**詳細の表示**」アイコンをクリックします。
3. 「**B2B 機能**」をクリックします。
4. ソース・パートナーに対して 2 組の機能を使用可能に設定します。
   a. 最初に、ROD 文書を表す文書定義を使用可能に設定します。
      1) 「**ソースの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: なし**」を展開します。
      3) 「**ソースの設定**」の下で、「**プロトコル: ROD-TO-EDI_DICT (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: ROD-TO-EDI_DICT (すべて)**」を展開します。
      5) 「**ソースの設定**」の下で、「**文書タイプ: DTROD-TO-EDI_ROD (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
   b. 次に、EDI エンベロープを表す文書定義を使用可能に設定します。
      1) 「**ソースの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ソースの設定**」の下で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。
      5) 「**ソースの設定**」の下で、「**文書タイプ: ISA (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
5. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。

6. この例のターゲット・パートナー (**TP1**) に対して「**詳細の表示**」アイコンをクリックします。
7. 「**B2B 機能**」をクリックします。
8. ターゲット・パートナーに対して 2 組の機能を使用可能に設定します。
   a. 最初に、EDI 850 トランザクションを表す文書定義を使用可能に設定します。
      1) 「**ターゲットの設定**」の下で、「**パッケージ: N/A**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: N/A**」を展開します。
      3) 「**ターゲットの設定**」の下で、「**プロトコル: X12V5R1 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: X12V5R1 (すべて)**」を展開します。
      5) 「**ターゲットの設定**」の下で、「**文書タイプ: 850 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
   b. 次に、エンベロープを表す文書定義を使用可能に設定します。
      1) 「**ターゲットの設定**」の下で、「**パッケージ: なし**」に対して「**役割はアクティブではありません**」アイコンをクリックし、有効にします。
      2) 「**パッケージ: なし**」を展開します。
      3) 「**ターゲットの設定**」の下で、「**プロトコル: EDI-X12 (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。
      4) 「**プロトコル: EDI-X12 (すべて)**」を展開します。
      5) 「**ターゲットの設定**」の下で、「**文書タイプ: ISA (すべて)**」に対して「**役割はアクティブではありません**」アイコンをクリックします。

## エンベロープ・プロファイルの作成

### このタスクについて

次に、変換された 850 トランザクションを包むエンベロープのプロファイルを作成します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**EDI**」>「**エンベロープ・プロファイル**」の順にクリックします。
2. 「**作成**」をクリックします。
3. プロファイルの名前として **EnvProf1** を入力します。
4. 「EDI 標準」リストから「**X12**」を選択します。
5. 「**一般**」ボタンがデフォルトで選択されています。エンベロープの一般属性として以下の値を入力します。
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. 「**交換**」ボタンをクリックし、交換の属性として以下の値を入力します。
   - ISA01: **01**

- ISA02: **ISA0000002**
- ISA03: **02**
- ISA04: **ISA0000004**
- ISA11: **¥**
- ISA12: **00501**
- ISA15: **T**

7. 「**保存**」をクリックします。

## 接続のアクティブ化

### このタスクについて

接続をアクティブ化するには、以下のステップを実行します。

1. 「**アカウント管理**」>「**接続**」をクリックします。
2. 「ソース」リストから「**Manager**」を選択します。
3. 「ターゲット」リストから「**TP1**」を選択します。
4. 「**検索**」をクリックします。
5. ROD 文書から EDI トランザクションへのフローを表す接続に対して「**アクティブ化**」をクリックします。

*表 48. ROD から EDI への接続*

| ソース | ターゲット |
|---|---|
| パッケージ: N/A (N/A) プロトコル: ROD-TO-EDI_DICT (すべて) 文書タイプ: DTROD-TO-EDI_ROD (すべて) | パッケージ: なし (N/A) プロトコル: X12V5R1 (すべて) 文書タイプ: 850 |

6. エンベロープを表す接続に対して「**アクティブ化**」をクリックします。

*表 49. エンベロープ接続*

| ソース | ターゲット |
|---|---|
| パッケージ: なし (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) | パッケージ: N/A (N/A) プロトコル: EDI-X12 (すべて) 文書タイプ: ISA (すべて) |

## 属性の構成

### このタスクについて

エンベロープ・プロファイルの属性を指定するには、以下のステップを実行します。

1. 「**アカウント管理**」>「**プロファイル**」>「**パートナー**」をクリックし、「**検索**」をクリックします。
2. リストから「**TP1**」を選択します。
3. 「**B2B 機能**」をクリックします。
4. 「**パッケージ: N/A**」の横にある「**展開 (Expand)**」アイコンをクリックします。
5. 「**プロトコル: X12V5R1**」の横にある「**編集**」アイコンをクリックします。

6. 以下の属性を指定します。
   a. 「エンベロープ・プロファイル」の行で、リストから「**EnvProf1**」を選択します。
   b. 「交換修飾子」の行に **01** と入力します。
   c. 「交換 ID」の行に **000000001** と入力します。
   d. 「交換の使用標識」の行に **T** と入力します。
7. 「**保存**」をクリックします。

この時点で、内部パートナーが ROD 文書をハブに送信すると、文書は 850 トランザクションに変換され、エンベロープに包まれた後、パートナーの宛先に送信されます。

# 第 20 章 RosettaNet に関する追加情報

この付録では、RosettaNet のサポートに関する追加情報を示します。以下のトピックを扱います。

- 『PIP の非アクティブ化』
- 『 障害通知機能』
- 389 ページの『PIP 文書定義パッケージの作成』
- 401 ページの『PIP 文書定義パッケージ』

## PIP の非アクティブ化

### このタスクについて

PIP パッケージは、WebSphere Partner Gateway にアップロードされた後は、削除できません。ただし、使用できないように PIP を非アクティブにすることはできます。

パートナーとのすべての通信に対して PIP を非アクティブにするには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 文書定義を展開して、使用不可にする PIP の文書タイプを表示します。
3. パッケージの「状況」列で、「**有効**」をクリックします。「状況」列に「**無効**」と表示され、WebSphere Partner Gateway は PIP の文書定義を使用できなくなります。

特定のパートナーとの PIP 通信を非アクティブにするには、PIP 用に定義されたパートナーとの接続を非アクティブにします。

## 障害通知機能

### 0A1 PIP

PIP メッセージの処理中に障害が発生した場合、WebSphere Partner Gateway は、メッセージの送信元であるパートナーまたはバックエンド・システムに障害をブロードキャストするメカニズムとして、0A1 PIP を使用します。例えば、バックエンド・システムが 3A4 PIP を開始するとします。WebSphere Partner Gateway は RNSC メッセージを処理して、パートナーに RosettaNet メッセージを送信します。WebSphere Partner Gateway は待ち時間がタイムアウト制限に達するまで、RosettaNet メッセージへの応答を待機します。この処理が発生すると、WebSphere Partner Gateway は 0A1 PIP を作成し、パートナーに送信します。0A1 PIP により例外条件が識別されるため、パートナーは 3A4 PIP 障害を補正することができます。

障害通知を行うには、0A1 パッケージをアップロードし、このパッケージを使用してパートナーとの PIP 接続を作成します。

### 連絡先情報の更新

0A1 PIP の RosettaNet 連絡先情報を変更するには、*<ProductDir>*/router/lib/config ディレクトリー内の BCG.Properties ファイルを編集する必要があります。

これらのフィールドには、0A1 PIP 内の連絡先情報が取り込まれます。FAX はオプションです (値を空にすることができます) が、それ以外の情報は必須です。

- **bcg.0A1.fromContactName**
- **bcg.0A1.fromEMailAddr**
- **bcg.0A1.fromPhoneNbr**
- **bcg.0A1.fromFaxNbr**

電話番号の長さは、最大で 30 バイトです。それ以外のフィールドの長さには、制限がありません。値を変更した場合は、文書マネージャーを再始動する必要があります。

## RosettaNet 属性値の編集

### このタスクについて

RosettaNet をサポートするために、アクション・タイプの文書定義に特定の属性セットが設定されています。これらの属性は、PIP メッセージの検証、PIP で使用される役割やサービスの定義、およびアクションに対する応答の定義に使用される情報を提供します。これらの属性値は、WebSphere Partner Gateway が提供する PIP パッケージによって自動的に定義されるため、通常は変更の必要がありません。

アクション文書定義の RosettaNet 属性を編集するには、以下のステップを実行します。

1. 「**ハブ管理**」>「**ハブ構成**」>「**文書定義**」をクリックします。
2. 「**展開 (Expand)**」アイコンをクリックして個々にノードを適切な文書定義レベルまで展開するか、「**すべて**」を選択してツリー全体を展開します。
3. 各アクションの「アクション」列には、「**RosettaNet 属性値の編集**」アイコンが配置されています。このアイコンをクリックして、アクションの RosettaNet 属性を編集します。コミュニティー・コンソールの RosettaNet 属性の下に、定義済み属性のリストが表示されます。
4. RosettaNet 属性の下に次のパラメーターを入力します。(これらの属性は、PIP をシステムにアップロードしたときに自動的に定義されます。)

*表 50. RosettaNet 属性*

| RosettaNet 属性 | 説明 |
|---|---|
| DTD 名 | RosettaNet が提供する DTD 内の PIP アクション名を識別します。 |
| 元サービス | メッセージの送信元であるパートナーまたはバックエンド・システムのネットワーク・コンポーネント・サービス名を格納します。 |
| 宛先サービス | メッセージの受信先であるパートナーまたはバックエンド・システムのネットワーク・コンポーネント・サービス名を格納します。 |

*表 50. RosettaNet 属性 (続き)*

| RosettaNet 属性 | 説明 |
|---|---|
| 送信側役割 | メッセージの送信元であるパートナーまたはバックエンド・システムの役割名を格納します。 |
| 受信側役割 | メッセージの受信先であるパートナーまたはバックエンド・システムの役割名を格納します。 |
| ルート・タグ | PIP に関連付けられた XML 文書のルート・エレメントの名前を格納します。 |
| アクション名からの応答 | PIP で次に実行するアクションを識別します。 |

**注:** コンソールに「属性が見つかりませんでした」というメッセージが表示される場合は、属性が定義されていません。

5. コンソールに表示されたこのメッセージの定義レベルが下位レベルの場合でも、より高いレベルの定義から属性が継承されるため、定義が機能することがあります。属性および値を追加すると、継承された属性がオーバーライドされ、文書定義の機能が変更されます。
6. 「**保存**」をクリックします。

## PIP 文書定義パッケージの作成

### このタスクについて

RosettaNet では PIP を随時追加しているため、これらの新しい PIP をサポートできるように、または PIP のアップグレードをサポートできるように、独自の PIP パッケージを作成しなければならない場合があります。特に明記されていない限り、このセクションでは、PIP 5C4 V01.03.00 の PIP 文書定義パッケージの作成方法について説明します。WebSphere Partner Gateway が提供しているのは PIP 5C4 V01.02.00 の PIP 文書定義パッケージです。したがって、手順で実際に説明しているのはアップグレードの実行方法です。ただし、PIP 文書定義パッケージの作成手順は類似しており、追加ステップについては手順内で示しています。

始める前に、www.rosettanet.org から新しいバージョンの PIP 仕様をダウンロードします。アップグレードを実行する場合は、古いバージョンもダウンロードします。例えば、この手順に記載されたアップグレードを実行する場合は、5C4_DistributeRegistrationStatus_V01_03_00.zip および 5C4_DistributeRegistrationStatus_V01_02_00.zip をダウンロードします。仕様には次のファイル・タイプが含まれます。

- RosettaNet XML メッセージ・ガイドライン - PIP のカーディナリティー、語彙、構造、および許容データ・エレメント値や値タイプを定義する 5C4_MG_V01_03_00_RegistrationStatusNotification.htm などの HTML ファイル
- RosettaNet XML メッセージ・スキーマ - PIP の順序またはシーケンス、エレメントの命名、構成、および属性を定義する 5C4_MS_V01_03_RegistrationStatusNotification.dtd などの DTD ファイル
- PIP 仕様 - PIP の業務パフォーマンスを規定する 5C4_Spec_V01_03_00.doc などの DOC ファイル

- PIP リリース・ノート - このバージョンと以前のバージョンの違いを示す 5C4_V01_03_00_ReleaseNotes.doc などの DOC ファイル

PIP 文書定義パッケージを作成またはアップグレードする手順では、以下の作業を行います。

- XSD ファイルの作成
- XML ファイルの作成
- パッケージの作成

## XSD ファイルの作成

### このタスクについて

PIP 文書定義パッケージには、メッセージ・フォーマットおよびエレメントの許容値を定義する XML スキーマ・ファイルが含まれます。次の手順では、PIP 仕様ファイルの内容に基づいてこれらのファイルを作成する方法について説明します。

PIP 仕様ファイル内の DTD ファイルごとに、XSD ファイルを少なくとも 1 つ作成します。PIP 5C4 V01.03.00 ではメッセージ・フォーマットが変更されているため、このバージョンにアップグレードする例では、BCG_5C4RegistrationStatusNotification_V01.03.xsd ファイルの作成方法を例として示します。XSD ファイルについては、 400 ページの『検証の概要』を参照してください。

PIP 文書定義パッケージの XSD ファイルを作成するには、以下のステップを実行します。

1. DTD ファイルを WebSphere Studio Application Developer などの XML エディターにインポートまたはロードします。例えば、5C4_MS_V01_03_RegistrationStatusNotification.dtd ファイルをロードします。
2. XML エディターを使用して、DTD を XML スキーマに変換します。ここでは、Application Developer を使用した変換方法について説明します。
   a. XML パースペクティブの「ナビゲーション」ペインで、インポートされた DTD ファイルを含むプロジェクトを開きます。
   b. DTD ファイルを右クリックし、「**生成**」>「**XML スキーマ**」を選択します。
   c. 「生成」パネルで、新しい XSD ファイルを保存する場所を入力するか、または選択します。「ファイル名」フィールドに新しい XSD ファイルの名前を入力します。この例の場合は、BCG_5C4RegistrationStatusNotification_V01.03.xsd のような名前を入力します。
   d. 「**終了**」をクリックします。
3. 新しい XSD ファイルに仕様を追加して、RosettaNet XML ガイドライン内で複数のカーディナリティー値を持つエレメントを補正します。ガイドラインでは、メッセージ内のエレメントはツリー形式で示され、エレメントの左側に各エレメントのカーディナリティーが表示されます。

   一般に、ガイドライン内のエレメントは、DTD ファイル内のエレメントの定義と一致します。ただし、ガイドラインには、名前が同じであってもカーディナリ

ティーが異なるエレメントが含まれる場合があります。この場合、DTD はカーディナリティーを提供できないため、XSD を変更する必要があります。例えば、5C4_MG_V01_03_00_RegistrationStatusNotification.htm ガイドライン・ファイルでは、次のカーディナリティーを持つ 5 つの子エレメントを含む ContactInformation が 15 行目で定義されています。

1 contactName

0..1 EmailAddress

0..1 facsimileNumber

0..1 PhysicalLocation

0..1 telephoneNumber

150 行目の ContactInformation 定義には、次のカーディナリティーを持つ 4 つの子エレメントが含まれます。

1 contactName

1 EmailAddress

0..1 facsimileNumber

1 telephoneNumber

ただし、XSD ファイルの ContactInformation のそれぞれの子には、両方の定義に適合するカーディナリティーが 1 つ含まれます。

```
<xsd:element name="ContactInformation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref="contactName"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="EmailAddress"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="facsimileNumber"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="PhysicalLocation"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="telephoneNumber"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

別のバージョンのパッケージに基づいて PIP 文書定義パッケージを更新し、別のバージョンの定義を再利用する場合は、これらの定義のそれぞれに対して以下のステップを実行します。

a. エレメントの定義を削除します。例えば、ContactInformation エレメントを削除します。

b. 置き換えられるバージョンの PIP 文書定義パッケージを開きます。例えば、BCG_Package_RNIFV02.00_5C4V01.02.zip ファイルを開きます。

c. 再利用する定義を検索します。例えば、BCG_ContactInformation_Types.xsd ファイル内の ContactInformation_type7 定義は、ガイドラインの 15 行目に必要な定義と一致します。

```
<xsd:complexType name="ContactInformation_type7">
  <xsd:sequence>
    <xsd:element name="contactName" type="common_FreeFormText_R"/>
    <xsd:element name="EmailAddress" type="common_EmailAddres_R"
        minOccurs="0"/>
    <xsd:element name="facsimileNumber"
        type="common_CommunicationsNumber_R" minOccurs="0"/>
    <xsd:element name="PhysicalLocation"
        type="PhysicalLocation_type1" minOccurs="0" />
```

```
    <xsd:element name="telephoneNumber"
        type="common_CommunicationsNumber_R minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>
```

d. 更新された PIP 文書定義パッケージ用に作成している新しい XSD ファイル内に、再利用する定義を含む XSD ファイルへの参照を作成します。例えば、次のように、BCG_5C4RegistrationStatusNotification_V01.03.xsd ファイル内に BCG_ContactInformation_Types.xsd への参照を作成します。

```
<xsd:include schemaLocation="BCG_ContactInformation_Types.xsd"/>
```

e. 新しい XSD ファイル内で、削除したエレメントを参照するすべてのエレメントの ref 属性を削除します。再利用する定義を参照する type 属性を追加します。例えば、productProviderFieldApplicationEngineer エレメント内で *ref="Contact Information"* を削除し、以下の情報を追加します。

```
name="ContactInformation"
 type="ContactInformation_type7"
```

PIP 文書定義パッケージを作成する場合、または PIP 文書定義パッケージをアップグレードする際に、必要な定義が別のバージョン内に存在しない場合は、ガイドライン内のエレメントのインスタンスごとに以下のステップを実行します。

a. エレメントの定義を削除します。例えば、ContactInformation エレメントを削除します。

b. 置き換える定義を作成します。例えば、ガイドラインの 15 行目の定義と一致する ContactInformation_localType1 定義を作成します。

```
<xsd:complexType name="ContactInformation_localType1">
  <xsd:sequence>
    <xsd:element ref="contactName"/>
    <xsd:element maxOccurs="1" minOccurs="0" ref="EmailAddress"/>
    <xsd:element maxOccurs="1" minOccurs="0"
        ref="facsimileNumber"/>
    <xsd:element maxOccurs="1" minOccurs="0"
        ref="PhysicalLocation"/>
    <xsd:element maxOccurs="1" minOccurs="0"
        ref="telephoneNumber"/>
  </xsd:sequence>
</xsd:complexType>
```

c. 削除されたエレメントを参照するすべてのエレメントについて、ref 属性を削除し、上記ステップで定義した適切な複合タイプを参照する type 属性を追加します。例えば、productProviderFieldApplicationEngineer エレメント内で *ref="Contact Information"* を削除し、以下の情報を追加します。

```
name="ContactInformation"
type="ContactInformation_localType1"
```

393 ページの図 35 は、変更前の productProviderFieldApplicationEngineer エレメントを示しています。

```
<xsd:element name="productProviderFieldApplicationEngineer">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref="ContactInformation"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

*図 35. 変更前の productProviderFieldApplicationEngineer エレメント:*

図 36 は、変更後の productProviderFieldApplicationEngineer エレメントを示しています。

```
<xsd:element name="productProviderFieldApplicationEngineer">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="ContactInformation"
          type="ContactInformation_localType1"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

*図 36. 変更後の productProviderFieldApplicationEngineer エレメント:*

4. 特定の値のみを設定できるエレメントの列挙値を指定します。列挙値は、ガイドラインの『ガイドライン情報 (Guideline Information)』セクションの表に記載されています。

   例えば、PIP 5C4 V01.03.00 メッセージの GlobalRegistrationComplexityLevelCode では、「Above average」、「Average」、「Maximum」、「Minimum」、「None」、および「Some」の値のみが有効です。

   別のバージョンのパッケージに基づいて PIP 文書定義パッケージを更新し、別のバージョンの列挙値セットを再利用する場合は、セットごとに以下のステップを実行します。

   a. エレメントの定義を削除します。例えば、GlobalRegistrationComplexityLevelCode エレメントを削除します。
   b. 置き換えられるバージョンの PIP 文書定義パッケージを開きます。例えば、BCG_Package_RNIFV02.00_5C4V01.02.zip ファイルを開きます。
   c. 再利用する列挙値を含む定義を検索します。例えば、BCG_GlobalRegistrationComplexityLevelCode.xsd ファイル内の GlobalRegistrationComplexityLevelCode 定義には、Entity Instance テーブルで定義された列挙値の定義が含まれています。

      ```
      <xsd:simpleType name="_GlobalRegistrationComplexityLevelCode">
        <xsd:restriction base="xsd:string">
          <xsd:enumeration value="Above average"/>
          <xsd:enumeration value="Average"/>
          <xsd:enumeration value="Maximum"/>
          <xsd:enumeration value="Minimum"/>
          <xsd:enumeration value="None"/>
          <xsd:enumeration value="Some"/>
        </xsd:restriction>
      </xsd:simpleType>
      ```

   d. 更新された PIP 文書定義パッケージ用に作成している新しい XSD ファイル内に、再利用する定義を含む XSD ファイルへの参照を作成します。例え

ば、次のように、BCG_5C4RegistrationStatusNotification_V01.03.xsd ファイル内に BCG_GlobalRegistrationComplexityLevelCode.xsd への参照を作成します。

```
<xsd:include schemaLocation=
    "BCG_GlobalRegistrationComplexityLevelCode_Types.xsd" />
```

e. 新しい XSD ファイル内で、削除したエレメントを参照するすべてのエレメントの ref 属性を削除します。再利用する定義を参照する type 属性を追加します。例えば、DesignAssemblyInformation エレメント内で *ref=″*GlobalRegistrationComplexityLevelCode*″* を削除し、以下の情報を追加します。

```
name="GlobalRegistrationComplexityLevelCode"
type="_GlobalRegistrationComplexityLevelCode"
```

PIP 文書定義パッケージを作成する場合、または PIP 文書定義パッケージをアップグレードする際に、必要な列挙値の定義が別のバージョンに存在しない場合は、ガイドライン内の列挙値を持つすべてのエレメントに対して以下のステップを実行します。

a. エレメントの定義を削除します。例えば、GlobalRegistrationComplexityLevelCode エレメントを削除します。

b. 置き換える定義を作成します。例えば、GlobalRegistrationComplexityLevelCode_localType 定義を作成し、テーブルに記載されている列挙値の定義を含めます。

```
<xsd:simpleType
    name="GlobalRegistrationComplexityLevelCode_localType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Above average"/>
    <xsd:enumeration value="Average"/>
    <xsd:enumeration value="Maximum"/>
    <xsd:enumeration value="Minimum"/>
    <xsd:enumeration value="None"/>
    <xsd:enumeration value="Some"/>
  </xsd:restriction>
</xsd:simpleType>
```

c. 削除されたエレメントを参照するすべてのエレメントについて、ref 属性を削除し、上記ステップで定義した適切な複合タイプを参照する type 属性を追加します。例えば、*ref="GlobalRegistrationComplexityLevelCode"* を削除し、以下の情報を追加します。

```
name="GlobalRegistrationComplexityLevelCode"
type="GlobalRegistrationComplexityLevelCode_localType"
```

395 ページの図 37 は、変更前の DesignAssemblyInformation エレメントを示しています。

```
<xsd:element name="DesignAssemblyInformation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="assemblyComments"/>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="demandCreatorTrackingIdentifier"/>
      <xsd:element maxOccurs="unbounded" minOccurs="0"
          ref="DesignPartInformation"/>
      <xsd:element ref="DesignRegistrationIdentification"/>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="GeographicRegion"/>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="GlobalRegistrationComplexityLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="GlobalRegistrationInvolvementLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="RegistrationStatus"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

*図 37. 変更前の DesignAssemblyInformation エレメント:*

図 38 は、変更後の DesignAssemblyInformation エレメントを示しています。

```
<xsd:element name="DesignAssemblyInformation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element maxOccurs="1" minOccurs="0"
         ref="assemblyComments"/>
      <xsd:element maxOccurs="1" minOccurs="0"
         ref="demandCreatorTrackingIdentifier"/>
      <xsd:element maxOccurs="unbounded" minOccurs="0"
         ref="DesignPartInformation"/>
      <xsd:element ref="DesignRegistrationIdentification"/>
      <xsd:element maxOccurs="1" minOccurs="0"
         ref="GeographicRegion"/>
      <xsd:element maxOccurs="1" minOccurs="0"
         name="GlobalRegistrationComplexityLevelCode"
           type="GlobalRegistrationComplexityLevelCode_localType"/>

      <xsd:element maxOccurs="1" minOccurs="0"
         ref="GlobalRegistrationInvolvementLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
         ref="RegistrationStatus"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

*図 38. 変更後の DesignAssemblyInformation エレメント:*

5. データ・エンティティーのデータ型、最小長、最大長、および表現を設定します。RosettaNet XML メッセージ・ガイドラインでは、Fundamental Business Data Entities テーブルにこの情報が記載されています。

   別のバージョンのパッケージに基づいて PIP 文書定義パッケージを更新し、別のバージョンのデータ・エンティティー定義を再利用する場合は、セットごとに以下のステップを実行します。

   a. データ・エンティティー・エレメントの定義を削除します。例えば、DateStamp エレメントを削除します。

b. 置き換えるバージョンの PIP 文書定義パッケージを開きます。例えば、BCG_Package_RNIFV02.00_5C4V01.02.zip ファイルを開きます。

c. 再利用する定義を検索します。例えば、BCG_common.xsd ファイル内の _common_DateStamp_R 定義には、ガイドラインで指定された情報に適合する次の定義が含まれます。

```
<xsd:simpleType name="_common_DateStamp_R">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{8}Z" />
  </xsd:restriction>
</xsd:simpleType>
```

d. 更新された PIP 文書定義パッケージ用に作成している新しい XSD ファイル内に、再利用する定義を含む XSD ファイルへの参照を作成します。例えば、次のように、BCG_5C4RegistrationStatusNotification_V01.03.xsd ファイル内で BCG_common.xsd への参照を作成します。

```
<xsd:include schemaLocation="BCG_common.xsd" />
```

e. 新しい XSD ファイル内で、削除したエレメントを参照するすべてのエレメントの ref 属性を削除します。再利用する定義を参照する type 属性を追加します。例えば、DesignAssemblyInformation エレメント内で *ref*=″DateStamp″ を削除し、以下の情報を追加します。

```
name="DateStamp" type="_common_DateStamp_R"
```

PIP 文書定義パッケージを作成する場合、または PIP 文書定義パッケージをアップグレードする際に、必要なデータ・エンティティー定義が別のバージョン内に存在しない場合は、データ・エンティティー・エレメントごとに以下のステップを実行します。

a. エレメントの定義を削除します。例えば、DateStamp エレメントを削除します。

b. 置き換える定義を作成します。例えば、データ型、最小長、最大長、および表現情報を使用して、DateStamp_localType 定義を作成します。

```
<xsd:simpleType name="DateStamp_localType">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{8}Z" />
  </xsd:restriction>
</xsd:simpleType>
```

c. 削除されたエレメントを参照するすべてのエレメントについて、ref 属性を削除し、上記ステップで定義した適切な複合タイプを参照する type 属性を追加します。例えば、*ref=″DateStamp″* を削除し、以下の情報を追加します。

```
name="DateStamp" type="DateStamp_localType"
```

図 39 は、変更前の beginDate エレメントを示しています。

```
<xsd:element name="beginDate">
  <xsd:complexType">
    <xsd:sequence>
      <xsd:element ref="DateStamp"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

*図 39. 変更前の beginDate エレメント:*

図 40 は、変更後の beginDate エレメントを示しています。

```
<xsd:element name="beginDate">
  <xsd:complexType">
    <xsd:sequence>
      <xsd:element name="DateStamp" type="DateStamp_localType"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

*図 40. 変更後の beginDate エレメント:*

# XML ファイルの作成

## このタスクについて

PIP 文書定義パッケージ用の XSD ファイルを作成すると、RNIF パッケージ用の XML ファイル、およびバックエンド統合パッケージ用の XML ファイルを作成できるようになります。例えば、これらは BCG_Package_RNIFV02.00_5C4V01.03.zip および BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.03.zip というパッケージです。以下に、RNIF パッケージ用の XML ファイルを作成する手順を示します。

1. RNIF PIP 文書定義パッケージ・ファイルから XML ファイルを抽出します。アップグレードする場合は、前のバージョンのパッケージ (例えば BCG_Package_RNIFV02.00_5C4V01.02.zip) からファイルを抽出します。新しいパッケージを作成する場合は、作成しようとしているパッケージと類似した PIP 文書定義パッケージからファイルを抽出します。例えば、2 アクション PIP をサポートするパッケージを作成する場合は、別の 2 アクション PIP パッケージから XML ファイルをコピーします。
2. ファイルをコピーし、適切な名前に変更します (例えば BCG_RNIFV02.00_5C4V01.03.xml)。
3. 新しいファイル内で、PIP に関する情報を含むエレメントを更新します。次の表に、5C4 PIP での更新に必要な情報の例を示します。この情報はファイル内に複数存在することがあることに注意してください。必ずすべてのインスタンスを更新してください。

*表 51. 5C4 PIP 更新情報*

| 変更する情報 | 古い値 | 新しい値 |
|---|---|---|
| PIP ID | 5C4 | 5C4 |
| PIP のバージョン | V01.02 | V01.03 |
| ファイル拡張子を含まない要求メッセージ DTD ファイルの名前 | 5C4_MS_V01_02_ RegistrationStatusNotification | 5C4_MS_V01_03_ RegistrationStatusNotification |
| ファイル拡張子を含まない確認メッセージ DTD ファイルの名前 (2 アクション PIP の場合のみ) | なし | なし |
| ファイル拡張子を含まない要求メッセージ XSD ファイルの名前 | BCG_5C4RegistrationStatus Notification_V01.02 | BCG_5C4RegistrationStatus Notification_V01.03 |

*表 51. 5C4 PIP 更新情報 (続き)*

| 変更する情報 | 古い値 | 新しい値 |
|---|---|---|
| ファイル拡張子を含まない確認メッセージ XSD ファイルの名前 (2 アクション PIP の場合のみ) | なし | なし |
| 要求メッセージに対する XSD ファイルのルート・エレメント名 | Pip5C4RegistrationStatus Notification | Pip5C4RegistrationStatus Notification |
| 確認メッセージに対する XSD ファイルのルート・エレメント名 (2 アクション PIP の場合のみ) | なし | なし |

4. PIP 仕様文書を開き、これを使用して次の表に記載された情報を更新します。これらの値は更新しなくてもよい場合があるため、更新する場合は各バージョンの仕様を比較してください。

*表 52. PIP 仕様の 5C4 PIP 更新情報*

| 更新する情報 | 説明 | 5C4 パッケージの値 |
|---|---|---|
| アクティビティー名 | 表 3-2 で指定 | 配布登録状況 |
| イニシエーターの役割名 | 表 3-1 で指定 | 製品プロバイダー |
| 応答者の役割名 | 表 3-1 で指定 | 要求作成者 |
| 要求アクション名 | 表 4-2 で指定 | 登録状況通知 |
| 確認アクション名 | 表 4-2 で指定 (2 アクション PIP の場合のみ) | なし |

5. パッケージ属性値を更新します。これらの値は更新しなくてもよい場合があるため、更新する場合は各バージョンの仕様を比較してください。

   **注:** バックエンド統合パッケージを作成する場合は、このステップを省略してステップ 6 (399 ページ) に進んでください。

*表 53. 5C4 PIP 属性の更新*

| 更新する情報 | 説明 | 5C4 パッケージの値 | XML ファイルのエレメント・パス |
|---|---|---|---|
| NonRepudiation Required | 表 3-3 で指定 | N | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (ATTRIBUTEKEY は NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY |
| NonRepudiationOf Receipt | 表 3-3 で指定 | N | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (ATTRIBUTEKEY は NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY |

*表 53. 5C4 PIP 属性の更新 (続き)*

| 更新する情報 | 説明 | 5C4 パッケージの値 | XML ファイルのエレメント・パス |
|---|---|---|---|
| DigitalSignature Required | 表 5-1 で指定 | Y | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (ATTRIBUTEKEY は DigitalSignatureRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY |
| TimeToAcknowledge | 表 3-3 で指定 | 2 (120 分) | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (ATTRIBUTEKEY は TimeToAcknowledge) ns1:AttributeValue ATTRVALUE |
| TimeToPerform | 表 3-3 で指定 | 2 (120 分) | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (ATTRIBUTEKEY は TimeToPerform) ns1:AttributeValue ATTRVALUE |
| RetryCount | 表 3-3 で指定 | 3 | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (ATTRIBUTEKEY は RetryCount) ns1:AttributeValue ATTRVALUE |

6. ns1:Package/ns1:Protocol/GuidelineMap エレメントを更新して、未使用の XSD ファイルを削除し、作成または参照したすべての XSD ファイルを追加します。

バックエンド統合パッケージを作成するには、次の手順を除いて、ステップ 1 (397 ページ) から 6 までを繰り返します。

- ステップ 1 (397 ページ) で、バックエンド統合パッケージ (例えば BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip) から XML ファイルを抽出します。
- ステップ 5 (398 ページ) を実行しないでください。

XML および XSD ファイルを作成すると、PIP 文書フロー・パッケージを作成できるようになります。

## パッケージの作成

### このタスクについて

RNIF パッケージを作成するには、以下のステップを実行します。

1. GuidelineMaps ディレクトリーを作成し、このディレクトリーにパッケージの XSD ファイルをコピーします。
2. Packages ディレクトリーを作成し、このディレクトリーに RNIF XML ファイルをコピーします。
3. 親ディレクトリーに移動して、GuidelineMaps および Packages ディレクトリーを含む PIP 文書定義パッケージ (ZIP ファイル) を作成します。ZIP ファイル内ではディレクトリー構造を保持する必要があります。

バックエンド統合パッケージを作成するには、RNIF ファイルの代わりにバックエンド統合 XML ファイルを使用して、ステップ 1 から 3 までを繰り返します。

PIP パッケージを作成すると、 116 ページの『RNIF および PIP の文書タイプ・パッケージ』の手順を使用して、PIP パッケージをアップロードできるようになります。

## 検証の概要

WebSphere Partner Gateway は検証マップを使用して RosettaNet メッセージのサービス内容を検証します。これらの検証マップは、有効メッセージの構造、およびメッセージ内のエレメントのカーディナリティー、フォーマット、有効値 (列挙) を定義します。各 PIP 文書定義パッケージ内で、WebSphere Partner Gateway は検証マップを GuidelineMaps ディレクトリー内の XSD ファイルとして提供します。

PIP メッセージのフォーマットは RosettaNet で指定されるため、通常は検証マップをカスタマイズする必要がありません。ただし、カスタマイズする場合は、 389 ページの『PIP 文書定義パッケージの作成』を参照して、メッセージの検証に使用する XSD ファイルのアップグレードに必要な手順、およびカスタム PIP 文書定義パッケージの作成手順を確認してください。

### カーディナリティー

カーディナリティーは、特定のエレメントがメッセージ内に出現できる回数、または出現しなければならない回数を決定します。検証マップでは、属性のカーディナリティーは minOccurs および maxOccurs 属性によって決まります。BCG_5C4RegistrationStatusNotification_V01.02.xsd に関する次の例を参照してください。

```
<xsd:element name="GeographicRegion" type="GeographicRegionType"
    minOccurs="0"/>
```

WebSphere Partner Gateway でエレメントのカーディナリティーを検査する必要がない場合、検証マップ内のエレメントの minOccurs および maxOccurs 属性値は、次の例のように「0」および「unbounded」になります。

```
<xsd:element name="DesignRegistrationIdentification"
    type="DesignRegistrationIdentificationType2"
    minOccurs="0" maxOccurs="unbounded"/>
```

### フォーマット

フォーマットは、エレメント・タイプに関するデータの配置またはレイアウトを決定します。検証マップでは、次の例のように、タイプに 1 つ以上の制限が適用されます。

#### 例 1

```
<xsd:simpleType name="_common_LineNumber_R">
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1" />
    <xsd:maxLength value="6" />
  </xsd:restriction>
</xsd:simpleType>
```

メッセージ内のすべての _common_LineNumber_R タイプ・エレメントには、1 から 6 文字のストリングを設定する必要があります。

### 例 2

```
<xsd:simpleType name="_GlobalLocationIdentifier">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{9}.{1,4}" />
  </xsd:restriction>
</xsd:simpleType>
```

メッセージ内のすべての _GlobalLocationIdentifier タイプ・エレメントには、9 文字の数値データのあとに 1 から 4 文字の英数字データが続くストリングを設定する必要があります。したがって、最小長は 10 文字、最大長は 13 文字です。

### 例 3

```
<xsd:element name="DayOfMonth">
  <xsd:simpleType>
    <xsd:restriction base="xsd:positiveInteger">
      <xsd:totalDigits value="2" />
      <xsd:minInclusive value="1" />
      <xsd:maxInclusive value="31" />
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
```

メッセージ内のすべての _DayofMonth タイプ・エレメントには、1 または 2 文字で、かつ 1 から 31 (両端を含む) の PositiveInteger の値を設定する必要があります。

## 列挙

列挙はエレメントの有効値を決定します。検証マップでは、次の例のように、エレメントのタイプに 1 つ以上の列挙制限が適用されます。

```
<xsd:simpleType name="_local_GlobalDesignRegistrationNotificationCode">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Initial" />
    <xsd:enumeration value="Update" />
  </xsd:restriction>
</xsd:simpleType>
```

メッセージ内のすべての _local_GlobalDesignRegistrationNotificationCode タイプ・エレメントの有効値は、「Initial」または「Update」のみです。

# PIP 文書定義パッケージ

以降のセクションに、各 PIP に対して WebSphere Partner Gateway が提供する PIP 文書定義パッケージを示します。各パッケージ内の Packages ディレクトリーには XML ファイルが 1 つ、GuidelineMaps ディレクトリーには XSD ファイルが複数格納されています。これらの構造は、PIP のすべての PIP 文書定義パッケージで共通です。

## 0A1 Notification of Failure V1.0

ここでは、0A1 Notification of Failure V1.0 PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、0A1 Notification of Failure V1.0 PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 54. 0A1 Notification of Failure V1.0 PIP の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_0A11.0.zip | BCG_RNIF1.1_0A11.0.xml |
| BCG_Package_RNSC1.0_RNIF1.1_0A11.0.zip | BCG_RNSC1.0_RNIF1.1_0A11.0.xml |

### ガイドライン・マップの内容

このセクションでは、0A1 Notification of Failure V1.0 のガイドライン・マップの内容を示します。

- 0A1FailureNotification_1.0.xml
- BCG_0A1FailureNotification_1.0.xsd
- BCG_common.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 0A1 Notification of Failure V02.00

ここでは、0A1 Notification of Failure V02.00 PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、0A1 Notification of Failure V02.00 PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 55. 0A1 Notification of Failure V02.00 PIP の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIFV02.00_0A1V02.00.zip | BCG_RNIFV02.00_0A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_0A1V02.00.zip | BCG_RNSC1.0_RNIFV02.00_0A1V02.00.xml |

### ガイドライン・マップの内容

このセクションでは、0A1 Notification of Failure V02.00 のガイドライン・マップの内容を示します。

- 0A1FailureNotification_V02.00.xml
- BCG_0A1FailureNotification_V02.00.xsd
- BCG_common.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd

- BCG_string_len_0.xsd
- BCG_xml.xsd

## 2A1 Distribute New Product Information

ここでは、2A1 Distribute New Product Information PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、2A1 Distribute New Product Information PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 56. 2A1 Distribute New Product Information の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_2A1V02.00.zip | BCG_RNIF1.1_2A1V02.00.xml |
| BCG_Package_RNIFV02.00_2A1V02.00.zip | BCG_RNIFV02.00_2A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_2A1V02.00.zip | BCG_RNSC1.0_RNIF1.1_2A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_2A1V02.00.zip | BCG_RNSC1.0_RNIFV02.00_2A1V02.00.xml |

### ガイドライン・マップの内容

このセクションでは、2A1 Distribute New Product Information のガイドライン・マップの内容を示します。

- BCG_2A1ProductCatalogInformationNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalLeadTimeClassificationCode_V43.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPackageTypeCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd

- BCG_GlobalPriceTypeCode_V43.xsd
- BCG_GlobalProductAssociationCode_V43.xsd
- BCG_GlobalProductLifeCycleStatusCode.xsd
- BCG_GlobalProductProcurementTypeCode_V43.xsd
- BCG_GlobalProductTypeCode_V43.xsd
- BCG_GlobalProductUnitofMeasureCode_V43.xsd
- BCG_GlobalProprietaryProductIdentificationTypeCode_V43.xsd
- BCG_GlobalStandardClassificationSchemeCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 2A12 Distribute Product Master

ここでは、2A12 Distribute Product Master PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、2A12 Distribute Product Master PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 57. 2A12 Distribute Product Master の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_2A12V01.03.zip | BCG_RNIF1.1_2A12V01.03.xml |
| BCG_Package_RNIFV02.00_2A12V01.03.zip | BCG_RNIFV02.00_2A12V01.03.xml |
| BCG_Package_RNSC1.0_RNIF1.1_2A12V01.03.zip | BCG_RNSC1.0_RNIF1.1_2A12V01.03.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_2A12V01.03.zip | BCG_RNSC1.0_RNIFV02.00_2A12V01.03.xml |

### ガイドライン・マップの内容

このセクションでは、2A12 Distribute Product Master のガイドライン・マップの内容を示します。

- BCG_2A12ProductMasterNotification_V01.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAssemblyLevelCode.xsd

- BCG_GlobalCountryCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalLeadTimeClassificationCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductLifeCycleStatusCode.xsd
- BCG_GlobalProductProcurementTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A1 Request Quote

ここでは、3A1 Request Quote PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3A1 Request Quote PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 58. 3A1 Request Quote PIP の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3A1V02.00.zip | BCG_RNIF1.1_3A1V02.00.xml |
| BCG_Package_RNIFV02.00_3A1V02.00.zip | BCG_RNIFV02.00_3A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A1V02.00.zip | BCG_RNSC1.0_RNIF1.1_3A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A1V02.00.zip | BCG_RNSC1.0_RNIFV02.00_3A1V02.00.xml |

### ガイドライン・マップの内容

このセクションでは、3A1 Request Quote のガイドライン・マップの内容を示します。

- BCG_3A1QuoteConfirmation_V02.00.xsd
- BCG_3A1QuoteRequest_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd

- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalQuoteLineItemStatusCode.xsd
- BCG_GlobalQuoteTypeCode.xsd
- BCG_GlobalStockIndicatorCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A2 Request Price and Availability

ここでは、3A2 Request Price and Availability PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3A2 Request Price and Availability PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 59. 3A2 Request Price and Availability の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3A2R02.01.zip | BCG_RNIF1.1_3A2R02.01.xml |
| BCG_Package_RNIFV02.00_3A2R02.01.zip | BCG_RNIFV02.00_3A2R02.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A2R02.01.zip | BCG_RNSC1.0_RNIF1.1_3A2R02.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A2R02.01.zip | BCG_RNSC1.0_RNIFV02.00_3A2R02.01.xml |

### ガイドライン・マップの内容

このセクションでは、3A2 Request Price and Availability のガイドライン・マップの内容を示します。

- BCG_3A2PriceAndAvailabilityRequest_R02.01.xsd
- BCG_3A2PriceAndAvailabilityResponse_R02.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalCustomerAuthorizationCode.xsd

- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPricingTypeCode.xsd
- BCG_GlobalProductAvailabilityCode.xsd
- BCG_GlobalProductStatusCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A4 Request Purchase Order V02.00

ここでは、3A4 Request Purchase Order V02.00 PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3A4 Request Purchase Order PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 60. 3A4 Request Purchase Order の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3A4V02.00.zip | BCG_RNIF1.1_3A4V02.00.xml |
| BCG_Package_RNIFV02.00_3A4V02.00.zip | BCG_RNIFV02.00_3A4V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A4V02.00.zip | BCG_RNSC1.0_RNIF1.1_3A4V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.00.zip | BCG_RNSC1.0_RNIFV02.00_3A4V02.00.xml |

### ガイドライン・マップの内容

このセクションでは、3A4 Request Purchase Order のガイドライン・マップの内容を示します。

- BCG_3A4PurchaseOrderConfirmation_V02.00.xsd
- BCG_3A4PurchaseOrderRequest_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd

- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V422.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShipmentTermsCode_V422.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode_V422.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTaxExemptionCode_V422.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A4 Request Purchase Order V02.02

ここでは、3A4 Request Purchase OrderV02.02 PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3A4 Request Purchase Order PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 61. 3A4 Request Purchase Order の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3A4V02.02.zip | BCG_RNIF1.1_3A4V02.02.xml |

表 61. 3A4 Request Purchase Order の ZIP および XML ファイル (続き)

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIFV02.00_3A4V02.02.zip | BCG_RNIFV02.00_3A4V02.02.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A4V02.02.zip | BCG_RNSC1.0_RNIF1.1_3A4V02.02.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip | BCG_RNSC1.0_RNIFV02.00_3A4V02.02.xml |

## ガイドライン・マップの内容

このセクションでは、3A4 Request Purchase Order のガイドライン・マップの内容を示します。

- BCG_3A4PurchaseOrderConfirmation_V02.02.xsd
- BCG_3A4PurchaseOrderRequest_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd

- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A5 Query Order Status

ここでは、3A5 Query Order Status PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3A5 Query Order Status PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 62. 3A5 Query Order Status の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3A5R02.00.zip | BCG_RNIF1.1_3A5R02.00.xml |
| BCG_Package_RNIFV02.00_3A5R02.00.zip | BCG_RNIFV02.00_3A5R02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A5R02.00.zip | BCG_RNSC1.0_RNIF1.1_3A5R02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A5R02.00.zip | BCG_RNSC1.0_RNIFV02.00_3A5R02.00.xml |

### ガイドライン・マップの内容

このセクションでは、3A5 Query Order Status のガイドライン・マップの内容を示します。

- BCG_3A5PurchaseOrderStatusQuery_R02.00.xsd
- BCG_3A5PurchaseOrderStatusResponse_R02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalCustomerTypeCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalFreeOnBoardCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalOrderQuantityTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd

- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriority
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A6 Distribute Order Status

ここでは、3A6 Distribute Order Status PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3A6 Distribute Order Status PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 63. 3A6 Distribute Order Status の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3A6V02.02.zip | BCG_RNIF1.1_3A6V02.02.xml |
| BCG_Package_RNIFV02.00_3A6V02.02.zip | BCG_RNIFV02.00_3A6V02.02.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A6V02.02.zip | BCG_RNSC1.0_RNIF1.1_3A6V02.02.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A6V02.02.zip | BCG_RNSC1.0_RNIFV02.00_3A6V02.02.xml |

### ガイドライン・マップの内容

このセクションでは、3A6 Distribute Order Status のガイドライン・マップの内容を示します。

- BCG_3A6PurchaseOrderStatusNotification_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd

- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalNotificationReasonCode.xsd
- BCG_GlobalOrderQuantityTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A7 Notify of Purchase Order Update

ここでは、3A7 Notify of Purchase Order Update PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3A7 Notify of Purchase Order Update PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 64. 3A7 Notify of Purchase Order Update の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3A7V02.02.zip | BCG_RNIF1.1_3A7V02.02.xml |
| BCG_Package_RNIFV02.00_3A7V02.02.zip | BCG_RNIFV02.00_3A7V02.02.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A7V02.02.zip | BCG_RNSC1.0_RNIF1.1_3A7V02.02.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A7V02.02.zip | BCG_RNSC1.0_RNIFV02.00_3A7V02.02.xml |

## ガイドライン・マップの内容

このセクションでは、3A7 Notify of Purchase Order Update のガイドライン・マップの内容を示します。

- BCG_3A7PurchaseOrderUpdateNotification_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd

- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A8 Request Purchase Order Change V01.02

ここでは、3A8 Request Purchase Order Change V01.02 PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3A8 Request Purchase Order Change PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 65. 3A8 Request Purchase Order Change の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3A8V01.02.zip | BCG_RNIF1.1_3A8V01.02.xml |
| BCG_Package_RNIFV02.00_3A8V01.02.zip | BCG_RNIFV02.00_3A8V01.02.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A8V01.02.zip | BCG_RNSC1.0_RNIF1.1_3A8V01.02.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.02.zip | BCG_RNSC1.0_RNIFV02.00_3A8V01.02.xml |

### ガイドライン・マップの内容

このセクションでは、3A8 Request Purchase Order Change のガイドライン・マップの内容を示します。

- BCG_3A8PurchaseOrderChangeConfirmation_V01.02.xsd
- BCG_3A8PurchaseOrderChangeRequest_V01.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd

- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A8 Request Purchase Order Change V01.03

ここでは、3A8 Request Purchase Order Change V01.03 PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3A8 Request Purchase Order Change PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 66. 3A8 Request Purchase Order Change の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3A8V01.03.zip | BCG_RNIF1.1_3A8V01.03.xml |
| BCG_Package_RNIFV02.00_3A8V01.03.zip | BCG_RNIFV02.00_3A8V01.03.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A8V01.03.zip | BCG_RNSC1.0_RNIF1.1_3A8V01.03.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.03.zip | BCG_RNSC1.0_RNIFV02.00_3A8V01.03.xml |

### ガイドライン・マップの内容

このセクションでは、3A8 Request Purchase Order Change のガイドライン・マップの内容を示します。

- BCG_3A8PurchaseOrderChangeConfirmation_V01.03.xsd
- BCG_3A8PurchaseOrderChangeRequest_V01.03.xsd
- BCG_BusinessDescription_Types.xsd

- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalFreeOnBoardCode_V422.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode_V43.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode_V43.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A9 Request Purchase Order Cancellation

ここでは、3A9 Request Purchase Order Cancellation PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3A9 Request Purchase Order Cancellation PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 67. 3A9 Request Purchase Order Cancellation の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3A9V01.01.zip | BCG_RNIF1.1_3A9V01.01.xml |
| BCG_Package_RNIFV02.00_3A9V01.01.zip | BCG_RNIFV02.00_3A9V01.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A9V01.01.zip | BCG_RNSC1.0_RNIF1.1_3A9V01.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A9V01.01.zip | BCG_RNSC1.0_RNIFV02.00_3A9V01.01.xml |

### ガイドライン・マップの内容

このセクションでは、3A9 Request Purchase Order Cancellation のガイドライン・マップの内容を示します。

- BCG_3A9PurchaseOrderCancellationConfirmation_V01.01.xsd
- BCG_3A9PurchaseOrderCancellationRequest_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPurchaseOrderCancellationCode.xsd
- BCG_GlobalPurchaseOrderCancellationResponseCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3B2 Notify of Advance Shipment

ここでは、3B2 Notify of Advance Shipment PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3B2 Notify of Advance Shipment PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 68. 3B2 Notify of Advance Shipment の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3B2V01.01.zip | BCG_RNIF1.1_3B2V01.01.xml |
| BCG_Package_RNIFV02.00_3B2V01.01.zip | BCG_RNIFV02.00_3B2V01.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B2V01.01.zip | BCG_RNSC1.0_RNIF1.1_3B2V01.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B2V01.01.zip | BCG_RNSC1.0_RNIFV02.00_3B2V01.01.xml |

### ガイドライン・マップの内容

このセクションでは、3B2 Notify of Advance Shipment のガイドライン・マップの内容を示します。

- BCG_3B2AdvanceShipmentNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentChangeDispositionCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3B3 Distribute Shipment Status

ここでは、3B3 Distribute Shipment Status PIP の内容を説明します。

## パッケージ・ファイルの内容

次の表は、3B3 Distribute Shipment Status PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 69. 3B3 Distribute Shipment Status の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3B3R01.00.zip | BCG_RNIF1.1_3B3R01.00.xml |
| BCG_Package_RNIFV02.00_3B3R01.00.zip | BCG_RNIFV02.00_3B3R01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B3R01.00.zip | BCG_RNSC1.0_RNIF1.1_3B3R01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B3R01.00.zip | BCG_RNSC1.0_RNIFV02.00_3B3R01.00.xml |

## ガイドライン・マップの内容

このセクションでは、3B3 Distribute Shipment Status のガイドライン・マップの内容を示します。

- 3B3 Distribute Shipment Status_R01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalShipmentDispositionCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShipmentStatusCode_V43.xsd
- BCG_GlobalShipmentStatusReportingLevelCode_V43.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_PhysicalAddress_Types_V423.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 3B11 Notify of Shipping Order

ここでは、3B11 Notify of Shipping Order PIP の内容を説明します。

## パッケージ・ファイルの内容

次の表は、3B11 Notify of Shipping Order PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 70. 3B11 Notify of Shipping Order の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3B11R01.00A.zip | BCG_RNIF1.1_3B11R01.00A.xml |
| BCG_Package_RNIFV02.00_3B11R01.00A.zip | BCG_RNIFV02.00_3B11R01.00A.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B11R01.00A.zip | BCG_RNSC1.0_RNIF1.1_3B11R01.00A.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B11R01.00A.zip | BCG_RNSC1.0_RNIFV02.00_3B11R01.00A.xml |

## ガイドライン・マップの内容

このセクションでは、3B11 Notify of Shipping Order のガイドライン・マップの内容を示します。

- 3B11 ShippingOrderNotification_R01.00A.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V422.xsd
- BCG_GlobalFreightPaymentTermsCode_V422.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalOrderAdminCode_V422.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V422.xsd

- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3B12 Request Shipping Order

ここでは、3B12 Request Shipping Order PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3B12 Request Shipping Order PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 71. 3B12 Request Shipping Order の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3B12V01.01.zip | BCG_RNIF1.1_3B12V01.01.xml |
| BCG_Package_RNIFV02.00_3B12V01.01.zip | BCG_RNIFV02.00_3B12V01.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B12V01.01.zip | BCG_RNSC1.0_RNIF1.1_3B12V01.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B12V01.01.zip | BCG_RNSC1.0_RNIFV02.00_3B12V01.01.xml |

### ガイドライン・マップの内容

このセクションでは、3B12 Request Shipping Order のガイドライン・マップの内容を示します。

- BCG_3B12ShippingOrderConfirmation_V01.01.xsd
- BCG_3B12ShippingOrderRequest_V01.01.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd

- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V422.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3B13 Notify of Shipping Order Confirmation

ここでは、3B13 Notify of Shipping Order Confirmation PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3B13 Notify of Shipping Order Confirmation PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 72. 3B13 Notify of Shipping Order Confirmation の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3B13V01.01.zip | BCG_RNIF1.1_3B13V01.01.xml |
| BCG_Package_RNIFV02.00_3B13V01.01.zip | BCG_RNIFV02.00_3B13V01.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B13V01.01.zip | BCG_RNSC1.0_RNIF1.1_3B13V01.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B13V01.01.zip | BCG_RNSC1.0_RNIFV02.00_3B13V01.01.xml |

### ガイドライン・マップの内容

このセクションでは、3B13 Notify of Shipping Order Confirmation のガイドライン・マップの内容を示します。

- BCG_3B13ShippingOrderConfirmationNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd

- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3B14 Request Shipping Order Cancellation

ここでは、3B14 Request Shipping Order Cancellation PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3B14 Request Shipping Order Cancellation PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 73. 3B14 Request Shipping Order Cancellation の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3B14V01.00.zip | BCG_RNIF1.1_3B14V01.00.xml |
| BCG_Package_RNIFV02.00_3B14V01.00.zip | BCG_RNIFV02.00_3B14V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B14V01.00.zip | BCG_RNSC1.0_RNIF1.1_3B14V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B14V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3B14V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、3B14 Request Shipping Order Cancellation のガイドライン・マップの内容を示します。

- 3B14_ShippingOrderCancellationConfirmation_V01.00.xsd
- 3B14_ShippingOrderCancellationRequest_V01.00.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalOrderAdminCode_V22.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalShippingOrderCancellationStatusReasonCode_V43.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3B18 Notify of Shipping Documentation

ここでは、3B18 Notify of Shipping Documentation PIP の内容を説明します。

## パッケージ・ファイルの内容

次の表は、3B18 Notify of Shipping Documentation PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 74. 3B18 Notify of Shipping Documentation の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3B18V01.00.zip | BCG_RNIF1.1_3B18V01.00.xml |
| BCG_Package_RNIFV02.00_3B18V01.00.zip | BCG_RNIFV02.00_3B18V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B18V01.00.zip | BCG_RNSC1.0_RNIF1.1_3B18V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B18V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3B18V01.00.xml |

## ガイドライン・マップの内容

このセクションでは、3B18 Notify of Shipping Documentation のガイドライン・マップの内容を示します。

- BCG_3B18ShippingDocumentationNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFreeOnBoardCode_V422.xsd
- BCG_GlobalFreightPaymentTermsCode_V422.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalOrderAdminCode_V422.xsd
- BCG_GlobalPackageTypeCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V422.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode_V422.xsd
- BCG_GlobalPortIdentifierAuthorityCode_V422.xsd
- BCG_GlobalPortTypeCode_V422.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingDocumentCode_V422.xsd
- BCG_GlobalShippingServiceLevelCode.xsd

- BCG_GlobalSpecialHandlingCode_V422.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3C1 Return Product

ここでは、3C1 Return Product PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3C1 Return Product PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 75. 3C1 Return Product の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3C1V01.00.zip | BCG_RNIF1.1_3C1V01.00.xml |
| BCG_Package_RNIFV02.00_3C1V01.00.zip | BCG_RNIFV02.00_3C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3C1V01.00.zip | BCG_RNSC1.0_RNIF1.1_3C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3C1V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3C1V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、3C1 Return Product のガイドライン・マップの内容を示します。

- BCG_3C1ReturnProductConfirmation_V01.00.xsd
- BCG_3C1ReturnProductRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFailureTypeCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalProductUnitOfMeasureCode_V43.xsd
- BCG_GlobalShippingServiceLevelCode.xsd

- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3C3 Notify of Invoice

ここでは、3C3 Notify of Invoice PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3C3 Notify of Invoice PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 76. 3C3 Notify of Invoice の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3C3V01.01.zip | BCG_RNIF1.1_3C3V01.01.xml |
| BCG_Package_RNIFV02.00_3C3V01.01.zip | BCG_RNIFV02.00_3C3V01.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3C3V01.01.zip | BCG_RNSC1.0_RNIF1.1_3C3V01.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3C3V01.01.zip | BCG_RNSC1.0_RNIFV02.00_3C3V01.01.xml |

### ガイドライン・マップの内容

このセクションでは、3C3 Notify of Invoice のガイドライン・マップの内容を示します。

- BCG_3C3InvoiceNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalSaleTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd

- BCG_InvoiceChargeTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3C4 Notify of Invoice Reject

ここでは、3C4 Notify of Invoice Reject PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3C4 Notify of Invoice Reject PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 77. 3C4 Notify of Invoice Reject の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3C4V01.00.zip | BCG_RNIF1.1_3C4V01.00.xml |
| BCG_Package_RNIFV02.00_3C4V01.00.zip | BCG_RNIFV02.00_3C4V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3C4V01.00.zip | BCG_RNSC1.0_RNIF1.1_3C4V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3C4V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3C4V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、3C4 Notify of Invoice Reject のガイドライン・マップの内容を示します。

- BCG_3C4InvoiceRejectNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalInvoiceRejectionCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3C6 Notify of Remittance Advice

ここでは、3C6 Notify of Remittance Advice PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3C6 Notify of Remittance Advice PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 78. 3C6 Notify of Remittance Advice の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3C6V01.00.zip | BCG_RNIF1.1_3C6V01.00.xml |
| BCG_Package_RNIFV02.00_3C6V01.00.zip | BCG_RNIFV02.00_3C6V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3C6V01.00.zip | BCG_RNSC1.0_RNIF1.1_3C6V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3C6V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3C6V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、3C6 Notify of Remittance Advice のガイドライン・マップの内容を示します。

- BCG_3C6RemittanceAdviceNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalFinancialAdjustmentReasonCode.xsd
- BCG_GlobalInvoiceRejectionCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPaymentMethodCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3C7 Notify of Self-Billing Invoice

ここでは、3C7 Notify of Self-Billing Invoice PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3C7 Notify of Self-Billing Invoice PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 79. 3C7 Notify of Self-Billing Invoice の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3C7V01.00.zip | BCG_RNIF1.1_3C7V01.00.xml |
| BCG_Package_RNIFV02.00_3C7V01.00.zip | BCG_RNIFV02.00_3C7V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3C7V01.00.zip | BCG_RNSC1.0_RNIF1.1_3C7V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3C7V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3C7V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、3C7 Notify of Self-Billing Invoice のガイドライン・マップの内容を示します。

- BCG_3C7SelfBillingInvoiceNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalDocumentTypeCode_V422.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalSaleTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3D8 Distribute Work in Process

ここでは、3D8 Distribute Work in Process PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、3D8 Distribute Work in Process PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 80. 3D8 Distribute Work in Process の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_3D8V01.00.zip | BCG_RNIF1.1_3D8V01.00.xml |
| BCG_Package_RNIFV02.00_3D8V01.00.zip | BCG_RNIFV02.00_3D8V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3D8V01.00.zip | BCG_RNSC1.0_RNIF1.1_3D8V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3D8V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3D8V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、3D8 Distribute Work in Process のガイドライン・マップの内容を示します。

- BCG_3D8WorkInProcessNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalLotStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_GlobalWorkInProcessPartTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4A1 Notify of Strategic Forecast

ここでは、4A1 Notify of Strategic Forecast PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、4A1 Notify of Strategic Forecast PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 81. 4A1 Notify of Strategic Forecast の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_4A1V02.00.zip | BCG_RNIF1.1_4A1V02.00.xml |
| BCG_Package_RNIFV02.00_4A1V02.00.zip | BCG_RNIFV02.00_4A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4A1V02.00.zip | BCG_RNSC1.0_RNIF1.1_4A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4A1V02.00.zip | BCG_RNSC1.0_RNIFV02.00_4A1V02.00.xml |

### ガイドライン・マップの内容

このセクションでは、4A1 Notify of Strategic Forecast のガイドライン・マップの内容を示します。

- BCG_4A1StrategicForecastNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_StrategicForecastQuantityTypeCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4A3 Notify of Threshold Release Forecast

ここでは、4A3 Notify of Threshold Release Forecast PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、4A3 Notify of Threshold Release Forecast PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 82. 4A3 Notify of Threshold Release Forecast の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_4A3V02.00.zip | BCG_RNIF1.1_4A3V02.00.xml |
| BCG_Package_RNIFV02.00_4A3V02.00.zip | BCG_RNIFV02.00_4A3V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4A3V02.00.zip | BCG_RNSC1.0_RNIF1.1_4A3V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4A3V02.00.zip | BCG_RNSC1.0_RNIFV02.00_4A3V02.00.xml |

### ガイドライン・マップの内容

このセクションでは、4A3 Notify of Threshold Release Forecast のガイドライン・マップの内容を示します。

- BCG_4A3ThresholdReleaseForecastNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_OrderForecastQuantityTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4A4 Notify of Planning Release Forecast

ここでは、4A4 Notify of Planning Release Forecast PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、4A4 Notify of Planning Release Forecast PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 83. 4A4 Notify of Planning Release Forecast の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_4A4R02.00A.zip | BCG_RNIF1.1_4A4R02.00A.xml |

表 83. 4A4 Notify of Planning Release Forecast の ZIP および XML ファイル (続き)

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIFV02.00_4A4R02.00A.zip | BCG_RNIFV02.00_4A4R02.00A.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4A4R02.00A.zip | BCG_RNSC1.0_RNIF1.1_4A4R02.00A.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4A4R02.00A.zip | BCG_RNSC1.0_RNIFV02.00_4A4R02.00A.xml |

### ガイドライン・マップの内容

このセクションでは、4A4 Notify of Planning Release Forecast のガイドライン・マップの内容を示します。

- BCG_4A4PlanningReleaseForecastNotification_R02.00A.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastQuantityTypeCode_V422.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4A5 Notify of Forecast Reply

ここでは、4A5 Notify of Forecast Reply PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、4A5 Notify of Forecast Reply PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 84. 4A5 Notify of Forecast Reply の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_4A5V02.00.zip | BCG_RNIF1.1_4A5V02.00.xml |

表 84. 4A5 Notify of Forecast Reply の ZIP および XML ファイル (続き)

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIFV02.00_4A5V02.00.zip | BCG_RNIFV02.00_4A5V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_34A5V02.00.zip | BCG_RNSC1.0_RNIF1.1_34A5V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4A5V02.00.zip | BCG_RNSC1.0_RNIFV02.00_4A5V02.00.xml |

### ガイドライン・マップの内容

このセクションでは、4A5 Notify of Forecast Reply のガイドライン・マップの内容を示します。

- BCG_4A5ForecastReplyNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ForecastReplyQuantityTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalForecastResponseCode.xsd
- BCG_GlobalForecastRevisionReasonCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4B2 Notify of Shipment Receipt

ここでは、4B2 Notify of Shipment Receipt PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、4B2 Notify of Shipment Receipt PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 85. 4B2 Notify of Shipment Receipt の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_4B2V01.00.zip | BCG_RNIF1.1_4B2V01.00.xml |
| BCG_Package_RNIFV02.00_4B2V01.00.zip | BCG_RNIFV02.00_4B2V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4B2V01.00.zip | BCG_RNSC1.0_RNIF1.1_4B2V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4B2V01.00.zip | BCG_RNSC1.0_RNIFV02.00_4B2V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、4B2 Notify of Shipment Receipt のガイドライン・マップの内容を示します。

- BCG_4B2ShipmentReceiptNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLotDiscrepancyReasonCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalReceivingDiscrepancyCode.xsd
- BCG_GlobalReceivingDiscrepancyReasonCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4B3 Notify of Consumption

ここでは、4B3 Notify of Consumption PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、4B3 Notify of Consumption PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 86. 4B3 Notify of Consumption の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_4B3V01.00.zip | BCG_RNIF1.1_4B3V01.00.xml |
| BCG_Package_RNIFV02.00_4B3V01.00.zip | BCG_RNIFV02.00_4B3V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4B3V01.00.zip | BCG_RNSC1.0_RNIF1.1_4B3V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4B3V01.00.zip | BCG_RNSC1.0_RNIFV02.00_4B3V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、4B3 Notify of Consumption のガイドライン・マップの内容を示します。

- BCG_4B3ConsumptionNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V43.xsd
- BCG_GlobalInventoryCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4C1 Distribute Inventory Report V02.01

ここでは、4C1 Distribute Inventory Report V02.01PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、4C1 Distribute Inventory Report PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 87. 4C1 Distribute Inventory Report の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_4C1V02.01.zip | BCG_RNIF1.1_4C1V02.01.xml |
| BCG_Package_RNIFV02.00_4C1V02.01.zip | BCG_RNIFV02.00_4C1V02.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4C1V02.01.zip | BCG_RNSC1.0_RNIF1.1_4C1V02.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.01.zip | BCG_RNSC1.0_RNIFV02.00_4C1V02.01.xml |

### ガイドライン・マップの内容

このセクションでは、4C1 Distribute Inventory Report のガイドライン・マップの内容を示します。

- BCG_4C1InventoryReportNotification_V02.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalInventoryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4C1 Distribute Inventory Report V02.03

ここでは、4C1 Distribute Inventory Report V02.03 PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、4C1 Distribute Inventory Report PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 88. 4C1 Distribute Inventory Report の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_4C1V02.03.zip | BCG_RNIF1.1_4C1V02.03.xml |
| BCG_Package_RNIFV02.00_4C1V02.03.zip | BCG_RNIFV02.00_4C1V02.03.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4C1V02.03.zip | BCG_RNSC1.0_RNIF1.1_4C1V02.03.xml |

表 88. 4C1 Distribute Inventory Report の ZIP および XML ファイル (続き)

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.03.zip | BCG_RNSC1.0_RNIFV02.00_4C1V02.03.xml |

### ガイドライン・マップの内容

このセクションでは、4C1 Distribute Inventory Report のガイドライン・マップの内容を示します。

- BCG_4C1InventoryReportNotification_V02.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalInventoryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 5C1 Distribute Product List

ここでは、5C1 Distribute Product List PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、5C1 Distribute Product List PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 89. 5C1 Distribute Product List の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_5C1V01.00.zip | BCG_RNIF1.1_5C1V01.00.xml |
| BCG_Package_RNIFV02.00_5C1V01.00.zip | BCG_RNIFV02.00_5C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_5C1V01.00.zip | BCG_RNSC1.0_RNIF1.1_5C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_5C1V01.00.zip | BCG_RNSC1.0_RNIFV02.00_5C1V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、5C1 Distribute Product List のガイドライン・マップの内容を示します。

- BCG_5C1ProductListNotification_V01.00.xsd

- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 5C2 Request Design Registration

ここでは、5C2 Request Design Registration PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、5C2 Request Design Registration PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 90. 5C2 Request Design Registration の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_5C2V01.00.zip | BCG_RNIF1.1_5C2V01.00.xml |
| BCG_Package_RNIFV02.00_5C2V01.00.zip | BCG_RNIFV02.00_5C2V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_5C2V01.00.zip | BCG_RNSC1.0_RNIF1.1_5C2V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_5C2V01.00.zip | BCG_RNSC1.0_RNIFV02.00_5C2V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、5C2 Request Design Registration のガイドライン・マップの内容を示します。

- BCG_5C2DesignRegistrationConfirmation_V01.00.xsd
- BCG_5C2DesignRegistrationRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_DesignWinStatusReasonCode_V43.xsd
- BCG_GlobalAttachmentDescriptionCode_V422.xsd

- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalMimeTypeQualifierCode_V43.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPriceTypeCode_V43.xsd
- BCG_GlobalRegistrationComplexityLevelCode.xsd
- BCG_GlobalRegistrationInvolvementLevelCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 5C4 Distribute Registration Status

ここでは、5C4 Distribute Registration Status PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、5C4 Distribute Registration Status PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 91. 5C4 Distribute Registration Status の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_5C4V01.02.zip | BCG_RNIF1.1_5C4V01.02.xml |
| BCG_Package_RNIFV02.00_5C4V01.02.zip | BCG_RNIFV02.00_5C4V01.02.xml |
| BCG_Package_RNSC1.0_RNIF1.1_5C4V01.023.zip | BCG_RNSC1.0_RNIF1.1_5C4V01.023.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip | BCG_RNSC1.0_RNIFV02.00_5C4V01.02.xml |

### ガイドライン・マップの内容

このセクションでは、5C4 Distribute Registration Status のガイドライン・マップの内容を示します。

- BCG_5C4RegistrationStatusNotification_V01.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd

- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalRegistrationComplexityLevelCode.xsd
- BCG_GlobalRegistrationInvolvementLevelCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 5D1 Request Ship From Stock And Debit Authorization

ここでは、5D1 Request Ship From Stock And Debit Authorization PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、5D1 Request Ship From Stock And Debit Authorization PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 92. 5D1 Request Ship from Stock and Debit Authorization の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_5D1V01.00.zip | BCG_RNIF1.1_5D1V01.00.xml |
| BCG_Package_RNIFV02.00_5D1V01.00.zip | BCG_RNIFV02.00_5D1V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_5D1V01.00.zip | BCG_RNSC1.0_RNIF1.1_5D1V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_5D1V01.00.zip | BCG_RNSC1.0_RNIFV02.00_5D1V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、5D1 Request Ship From Stock And Debit Authorization のガイドライン・マップの内容を示します。

- BCG_5D1ShipFromStockAndDebitAuthorizationConfirmation_V01.00.xsd
- BCG_5D1ShipFromStockAndDebitAuthorizationRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd

- BCG_GlobalShipFromStockAndDebitAuthorizationRejectionCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 6C1 Query Service Entitlement

ここでは、6C1 Query Service Entitlement PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、6C1 Query Service Entitlement PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 93. 6C1 Query Service Entitlement の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_6C1V01.00.zip | BCG_RNIF1.1_6C1V01.00.xml |
| BCG_Package_RNIFV02.00_6C1V01.00.zip | BCG_RNIFV02.00_6C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_6C1V01.00.zip | BCG_RNSC1.0_RNIF1.1_6C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_6C1V01.00.zip | BCG_RNSC1.0_RNIFV02.00_6C1V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、6C1 Query Service Entitlement のガイドライン・マップの内容を示します。

- BCG_6C1ServiceEntitlementQuery_V01.00.xsd
- BCG_6C1ServiceEntitlementStatusResponse_V01.00.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalNotificationCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPaymentTypeCode_V43.xsd
- BCG_GlobalServiceDeliveryMethodCode_V43.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalWarrantyMethodCode_V43.xsd
- BCG_GlobalWarrantyProgramCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 6C2 Request Warranty Claim

ここでは、6C2 Request Warranty Claim PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、6C2 Request Warranty Claim PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 94. 6C2 Request Warranty Claim の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_6C2V01.00.zip | BCG_RNIF1.1_6C2V01.00.xml |
| BCG_Package_RNIFV02.00_6C2V01.00.zip | BCG_RNIFV02.00_6C2V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_6C2V01.00.zip | BCG_RNSC1.0_RNIF1.1_6C2V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_6C2V01.00.zip | BCG_RNSC1.0_RNIFV02.00_6C2V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、6C2 Request Warranty Claim のガイドライン・マップの内容を示します。

- BCG_6C2WarrantyClaimConfirmation_V01.00.xsd
- BCG_6CWarrantyClaimRequest_V01.00.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFailureTypeCode_V43.xsd
- BCG_GlobalOperatingSystemCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPaymentTypeCode_V43.xsd
- BCG_GlobalServiceDeliveryMethodCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 7B1 Distribute Work in Process

ここでは、7B1 Distribute Work in Process PIP の内容を説明します。

### パッケージ・ファイルの内容

次の表は、7B1 Distribute Work in Process PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

表 95. 7B1 Distribute Work in Process の ZIP および XML ファイル

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_7B1V01.00.zip | BCG_RNIF1.1_7B1V01.00.xml |
| BCG_Package_RNIFV02.00_37B1V01.00.zip | BCG_RNIFV02.00_37B1V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_7B1V01.00.zip | BCG_RNSC1.0_RNIF1.1_7B1V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_7B1V01.00.zip | BCG_RNSC1.0_RNIFV02.00_7B1V01.00.xml |

### ガイドライン・マップの内容

このセクションでは、7B1 Distribute Work in Process のガイドライン・マップの内容を示します。

- BCG_7B1WorkInProcessNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalEquipmentTypeCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalLotStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_GlobalWorkInProcessPartTypeCode.xsd
- BCG_GlobalWorkInProcessQuantityChangeCode.xsd
- BCG_GlobalWorkInProcessTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 7B5 Notify Of Manufacturing Work Order

ここでは、7B5 Notify Of Manufacturing Work Order PIP の内容を説明します。

## パッケージ・ファイルの内容

次の表は、7B5 Notify Of Manufacturing Work Order PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 96. 7B5 Notify of Manufacturing Work Order の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_7B5V01.00.zip | BCG_RNIF1.1_7B5V01.00.xml |
| BCG_Package_RNIFV02.00_7B5V01.00.zip | BCG_RNIFV02.00_7B5V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_7B5V01.00.zip | BCG_RNSC1.0_RNIF1.1_7B5V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_7B5V01.00.zip | BCG_RNSC1.0_RNIFV02.00_7B5V01.00.xml |

## ガイドライン・マップの内容

このセクションでは、7B5 Notify Of Manufacturing Work Order のガイドライン・マップの内容を示します。

- BCG_7B5NotifyOfManufacturingWorkOrder_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAttachmentDescriptionCode_V422.xsd
- BCG_GlobalBusinessActionCode_V422.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDevicePackageTypeCode_V422.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalMimeTypeQualifierCode_V422.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 7B6 Notify Of Manufacturing Work Order Reply

ここでは、7B6 Notify Of Manufacturing Work Order Reply PIP の内容を説明します。

## パッケージ・ファイルの内容

次の表は、7B6 Notify Of Manufacturing Work Order Reply PIP の ZIP ファイルおよび対応する XML ファイルを示しています。すべてのバージョンに共通のガイドライン・マップをその後のセクションに示します。

*表 97. 7B6 Notify of Manufacturing Work Order Reply の ZIP および XML ファイル*

| ZIP ファイル名 | XML ファイル名 |
|---|---|
| BCG_Package_RNIF1.1_7B6V01.00.zip | BCG_RNIF1.1_7B6V01.00.xml |
| BCG_Package_RNIFV02.00_7B6V01.00.zip | BCG_RNIFV02.00_7B6V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_7B6V01.00.zip | BCG_RNSC1.0_RNIF1.1_7B6V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_7B6V01.00.zip | BCG_RNSC1.0_RNIFV02.00_7B6V01.00.xml |

## ガイドライン・マップの内容

このセクションでは、7B6 Notify Of Manufacturing Work Order Reply のガイドライン・マップの内容を示します。

- BCG_7B6NotifyOfManufacturingWorkOrderReply_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 第 21 章 CIDX に関する追加情報

この付録では、CIDX のサポートに関する追加情報を示します。以下のトピックを扱います。

- 『CIDX プロセス有効化サポート』
- 『CIDX 文書定義パッケージの作成』

## CIDX プロセス有効化サポート

CIDX では、プロセス有効化のために、以下の 2 つの手段をサポートします。

- **メッセージ・ベースの有効化:** 文書の結合は、<RequestingDocumentIdentifier> および <ThisDocumentIdentifier>に基づきます。
- **フレームワーク・ベースの有効化:** 文書の結合は、RNIF 1.1 サービス・ヘッダー・セマンティクスに基づきます。

メッセージ・ベースの有効化の場合、ChemXML トランザクション用の 1 アクション PIP パッケージが必要です。フレームワーク・ベースの有効化の場合、ChemXML トランザクション用の 2 アクション PIP パッケージが必要です。WebSphere Partner Gateway では、両方の形態のプロセス有効化がサポートされています。WebSphere Partner Gateway では、「E41 Order Create」および「E42 Order Response」用の 1 アクション PIP パッケージを提供します。

## CIDX 文書定義パッケージの作成

その他の CIDX メッセージをサポートするには、独自の CIDX パッケージを作成する必要があります。新規の CIDX 文書定義パッケージを作成する手順は、RosettaNet の場合と同じです。

RosettaNet の追加情報については、 387 ページの『第 20 章 RosettaNet に関する追加情報』

# 第 22 章 属性

この付録では、コミュニティー・コンソールから設定できる属性について説明します。次の属性について説明します。

- 『EDI 属性』
- 462 ページの『AS 属性』
- 466 ページの『RosettaNet 属性』
- 469 ページの『「バックエンド統合」属性』
- 470 ページの『ebMS 属性』
- 476 ページの『一般属性』

## EDI 属性

このセクションでは、EDI 交換の設定時に使用できる EDI 属性について説明します。これらの属性の一部は、EDI 文書に関連付けられた変換マップを表す制御ストリングで事前定義されています。制御ストリング (Data Interchange Services クライアント) で設定される値は、コミュニティー・コンソールで入力する値をオーバーライドします。

### エンベロープ・プロファイル属性

EDI エンベロープ・プロファイルのさまざまな属性を設定できます。使用可能な属性は、EDI タイプによって異なります。一般に、属性は EDI 標準に対応しており、許容値はエンベロープ・プロファイルが表す EDI 標準によって異なります。

いずれの属性にも値を指定する必要はありません。一部の属性では、値を入力しない場合にデフォルト値が使用されます。このセクションの表に、デフォルトが関連付けられている属性およびそのデフォルト値をリストします。

**注:** リストされていないエンベロープ・プロファイル・プロパティーには、デフォルト値がありません。マップまたは接続で設定される汎用または特定のエンベロープ・プロパティーによってオーバーライドされない場合は、指定するテキスト値が使用されます。

#### X12 属性

このセクションの表に、デフォルト値が提供されている X12 属性をリストします。

#### 一般属性

450 ページの表 98 は、デフォルト値が提供されている一般属性をリストしています。

*表 98. 一般属性*

| フィールド名 | 必須 | 説明 | デフォルト |
|---|---|---|---|
| INTCTLLEN (交換制御番号の長さ) | いいえ | 交換制御番号の特定の長さを定義します。値を入力する場合、整数を入力する必要があります。<br><br>値を入力しない場合、デフォルトの長さが使用されます。 | 9 |
| GRPCTLLEN (グループ制御番号の長さ) | いいえ | グループ制御番号の特定の長さを定義します。値を入力する場合、整数を入力する必要があります。<br><br>値を入力しない場合、デフォルトの長さが使用されます。 | 9 |
| TRXCTLLEN (トランザクション制御番号の長さ) | いいえ | トランザクション制御番号の特定の長さを定義します。値を入力する場合、整数を入力する必要があります。<br><br>値を入力しない場合、デフォルトの長さが使用されます。 | 9 |
| ENVTYPE (エンベロープ・タイプ) | いいえ | この属性は、ユーザーによって設定されるのではなく、作成されるエンベロープ・プロファイルのタイプから派生します。 | X12 |
| MAXDOCS (最大トランザクション番号) | いいえ | エンベロープ内のトランザクションの最大数です。値を入力する場合、整数を入力する必要があります。 | 最大数はありません。 |
| CTLNUMFLAG (トランザクション ID 別制御番号) | いいえ | 「はい」は、EDI トランザクション・タイプを基にした別々の制御番号のセットが使用されることを示します。<br><br>「いいえ」は、すべての EDI トランザクション・タイプに共通の制御番号のセットが使用されることを示します。 | いいえ |

### 交換属性

X12 交換属性は必須ではなく、この属性にデフォルト値はありません。

*表 99. グループ属性*

| フィールド名 | 必須 | 説明 | デフォルト |
|---|---|---|---|
| GS01 (機能グループ ID) | いいえ | グループ ID。 | デフォルト値は、制御ストリング・ヘッダーに由来します。この値は、Data Interchange Services クライアントの「EDI 文書定義」ページの「機能グループ」列で確認できます。 |
| GS08 (グループ・バージョン) | いいえ | グループ・バージョン。 | デフォルト値は、標準ごとに異なります。 |

### グループ属性

表 99 は、デフォルト値が提供されているグループ属性をリストしています。

### トランザクション属性

トランザクション属性は必須ではありません。この属性にはデフォルト値がありません。

## UCS 属性

ここでは、UCS 交換、グループ、およびトランザクションにデフォルト値が適用されるかどうかをリストします。

### 一般属性

表 100 は、デフォルト値が提供されている一般属性をリストしています。

*表 100. 一般属性*

| フィールド名 | 必須 | 説明 | デフォルト |
|---|---|---|---|
| INTCTLLEN (交換制御番号の長さ) | いいえ | 交換制御番号の特定の長さを定義します。値を入力する場合、整数を入力する必要があります。<br><br>値を入力しない場合、デフォルトの長さが使用されます。 | 5 |
| GRPCTLLEN (グループ制御番号の長さ) | いいえ | グループ制御番号の特定の長さを定義します。値を入力する場合、整数を入力する必要があります。<br><br>値を入力しない場合、デフォルトの長さが使用されます。 | 9 |
| TRXCTLLEN (トランザクション制御番号の長さ) | いいえ | トランザクション制御番号の特定の長さを定義します。値を入力する場合、整数を入力する必要があります。<br><br>値を入力しない場合、デフォルトの長さが使用されます。 | 9 |
| ENVTYPE (エンベロープ・タイプ) | いいえ | この属性は、ハブ管理者によって設定されるのではなく、作成されるエンベロープ・プロファイルのタイプから派生します。 | UCS |
| MAXDOCS (最大トランザクション番号) | いいえ | エンベロープ内のトランザクションの最大数です。値を入力する場合、整数を入力する必要があります。 | 最大数はありません。 |
| CTLNUMFLAG (トランザクション ID 別制御番号) | いいえ | 「はい」は、EDI トランザクション・タイプを基にした別々の制御番号のセットが使用されることを示します。<br><br>「いいえ」は、すべての EDI トランザクション・タイプに共通の制御番号のセットが使用されることを示します。 | いいえ |

### 交換属性

交換属性は必須ではありません。この属性にはデフォルト値がありません。

### グループ属性

表 101 は、デフォルト値が提供されているグループ属性をリストしています。

*表 101. グループ属性*

| フィールド名 | 必須 | 説明 | デフォルト |
|---|---|---|---|
| GS01 (機能グループ ID) | いいえ | グループ ID。 | デフォルト値は、制御ストリング・ヘッダーに由来します。この値は、Data Interchange Services クライアントの「EDI 文書定義」ページの「機能グループ」列で確認できます。 |
| GS08 (グループ・バージョン) | いいえ | グループ・バージョン。 | デフォルト値は、標準ごとに異なります。 |

### トランザクション属性

トランザクション属性は必須ではありません。この属性にはデフォルト値がありません。

## EDIFACT 属性

ここでは、EDIFACT 交換、グループ、およびメッセージにデフォルト値が適用されるかどうかをリストします。

### 一般属性

表 102 は、デフォルト値が提供されている一般属性をリストしています。

*表 102. 一般属性*

| フィールド名 | 必須 | 説明 | デフォルト |
|---|---|---|---|
| INTCTLLEN (交換制御番号の長さ) | いいえ | 交換制御番号の特定の長さを定義します。値を入力する場合、整数を入力する必要があります。<br><br>値を入力しない場合、デフォルトの長さが使用されます。 | 9 |
| GRPCTLLEN (グループ制御番号の長さ) | いいえ | グループ制御番号の特定の長さを定義します。値を入力する場合、整数を入力する必要があります。<br><br>値を入力しない場合、デフォルトの長さが使用されます。 | 9 |
| TRXCTLLEN (トランザクション制御番号の長さ) | いいえ | トランザクション制御番号の特定の長さを定義します。値を入力する場合、整数を入力する必要があります。<br><br>値を入力しない場合、デフォルトの長さが使用されます。 | 9 |
| ENVTYPE (エンベロープ・タイプ) | いいえ | この属性は、ハブ管理者によって設定されるのではなく、作成されるエンベロープ・プロファイルのタイプから派生します。 | EDIFACT |

*表 102. 一般属性 (続き)*

| フィールド名 | 必須 | 説明 | デフォルト |
|---|---|---|---|
| EDIFACTGRP (EDI 用のグループの作成) | いいえ | この値は EDIFACT エンベロープ・タイプ専用です。(EDIFACT では、グループ・レベルを使用すべきではありません。)<br><br>「はい」は、EDIFACT DATA 用の機能グループ (UNG/UNE セグメント) を作成することを示します。<br><br>「いいえ」は、作成しないことを示します。 | いいえ |
| MAXDOCS (最大トランザクション番号) | いいえ | エンベロープ内のトランザクションの最大数です。値を入力する場合、整数を入力する必要があります。 | 最大数はありません。 |
| CTLNUMFLAG (トランザクション ID 別制御番号) | いいえ | 「はい」は、EDI トランザクション・タイプを基にした別々の制御番号のセットが使用されることを示します。<br><br>「いいえ」は、すべての EDI トランザクション・タイプに共通の制御番号のセットが使用されることを示します。 | いいえ |

## 交換属性

交換属性は必須ではありません。この属性にはデフォルト値がありません。

## グループ属性

表 103 は、デフォルト値が提供されているグループ属性をリストしています。

*表 103. グループ属性*

| フィールド名 | 必須 | 説明 | デフォルト |
|---|---|---|---|
| UNG01 (機能グループ ID) | いいえ | グループ ID。 | デフォルト値は、制御ストリング・ヘッダーに由来します。この値は、Data Interchange Services クライアントの「EDI 文書定義」ページの「機能グループ」列で確認できます。 |

## メッセージ属性

表 104 は、デフォルト値が提供されているメッセージ属性をリストしています。

*表 104. メッセージ属性*

| フィールド名 | 必須 | 説明 | デフォルト |
|---|---|---|---|
| UNH0201 (メッセージ・タイプ) | いいえ | メッセージのタイプ。 | デフォルト値は、制御ストリング・ヘッダーに由来します。この値は、Data Interchange Services クライアントの「EDI 文書定義」ページで確認できます。 |
| UNH0202 (メッセージ・バージョン) | いいえ | メッセージのバージョン。 | D |
| UNH0203 (メッセージ・リリース) | いいえ | メッセージのリリース。 | 標準ごとに異なります。 |
| UNH0204 (制御機関) | いいえ | 制御機関を識別するコード。 | UN |

## 文書定義および接続属性

ここでは、エンベロープ用の文書の定義属性をリストします。これらの属性の一部は、以下に示すとおり、プロトコルまたは接続レベルでのみ設定可能です。

### 分離文字および区切り文字属性

ここでは、EDI 交換内で分離文字または区切り文字として使用される文字をリストします。表 105 は、コミュニティー・コンソールに表示される属性、X12 および EDIFACT (ISO 9735 バージョン 4、リリース 1) での対応する用語、属性が必須かどうか、および属性の説明を示しています。表に続けて、EDI 文書内でのこれらの文字の使用例を示します。

### 属性の説明

表 105 に分離文字および区切り文字属性をリストします。

**注:** 一部の文字には 16 進値を使用できます (記載されているとおり)。これらは、Unicode 値または別のエンコード・タイプの値の場合があります。Unicode の場合、¥unnnn という形式を使用します。その他のエンコードの場合、0xnn という形式を使用します。

*表 105. エンベロープ・プロファイル属性*

| 属性 | X12 での用語 | EDIFACT での用語 | 説明 |
|---|---|---|---|
| セグメント区切り文字 | セグメント終了記号 | セグメント終了記号 | これは、セグメントの最後の文字として現れる単一文字です。この文字には 16 進値を使用できます。<br><br>デフォルト値は、EDI タイプに基づきます。<br><br>**X12** ～ (波形記号)<br><br>**EDIFACT**<br>‘ (単一引用符)<br><br>**UCS** ～ (波形記号) |
| データ・エレメント区切り文字 | データ・エレメント分離記号 | データ・エレメント分離記号 | これは、セグメントのデータ・エレメントを分離する単一文字です。この文字には 16 進値を使用できます。<br><br>デフォルト値は、EDI タイプに基づきます。<br><br>**X12** * (アスタリスク)<br><br>**EDIFACT**<br>+ (正符号)<br><br>**UCS** * (アスタリスク) |

*表 105. エンベロープ・プロファイル属性 (続き)*

| 属性 | X12 での用語 | EDIFACT での用語 | 説明 |
|---|---|---|---|
| サブエレメント区切り文字 | コンポーネント・エレメント分離記号 | コンポーネント・データ・エレメント分離記号 | これは、複合データ・エレメントのコンポーネント・エレメントを分離する単一文字です。この文字には 16 進値を使用できます。<br><br>デフォルト値は、EDI タイプに基づきます。<br><br>**X12** ¥ (円記号)<br><br>**EDIFACT**<br>: (コロン)<br><br>**UCS** ¥ (円記号) |
| リリース文字 | | リリース文字 | これは、次の文字の意味をオーバーライドする単一文字で、データ・エレメント内に分離文字が出現することを許可します。この文字には 16 進値を使用できます。これは、EDIFACT のみに適用されます。<br><br>**EDIFACT**<br>? (疑問符) |
| 反復データ・エレメント分離記号 | 反復分離記号 | 反復分離記号 | これは、反復データ・エレメントのインスタンスを分離する単一文字です。この文字には 16 進値を使用できます。<br><br>デフォルト値は、X12 または EDIFACT の EDI タイプに基づきます。<br><br>**X12** ^ (ハット記号、曲折アクセント記号)<br><br>**EDIFACT**<br>* (アスタリスク) |
| 10 進表記 | | 10 進表記 (使用すべきでない) | この属性は 10 進フォーマットまたは構文解析で使用されていましたが、今は使用すべきではありません。これには、単にピリオドまたはコンマを使用できます。<br><br>デフォルト値はピリオドです。 |

## EDI 構造の例

ここでは、単純な EDI 交換、および 454 ページの表 105 の属性の交換での使用方法について示します。

EDI メッセージは、特定の順序に並んだ一連のセグメントで構成されます。セグメントは、一連のエレメントで構成されます。セグメント内のエレメントは、1 つの情報のみが含まれる単純データ・エレメントである場合があります。エレメントは、2 つ以上の単純データ・エレメントを含む複合データ・エレメントである場合があります。複合エレメントを構成する単純エレメントは、コンポーネント・データ・エレメントと呼ばれます。

複合データ・エレメントはネストできません。複合エレメントに含めることができるのは、単純データ・エレメントのみで、他の複合データ・エレメントを含めるこ

とはできません。ここでは説明しませんが、コンポーネント・データ・エレメントを反復データ・エレメントとして定義することもできます。

以下の例を考えてみましょう。

```
ABC*123*AA¥BB¥CC*001^002^003*star?*power~
```

この例では、以下のようになります。

- 「ABC」はセグメント名で (EDIFACT では「セグメント・タグ」といいます)、これは「ABC セグメント」と呼ばれます。
- 「*」(アスタリスク) はデータ・エレメント分離記号です。

  コミュニティー・コンソールでの対応する属性名は、セグメント区切り文字です。
- 「123」は最初のデータ・エレメントで、単純データ・エレメントです (コンテキストによっては ABC01 と呼ばれます)。
- 「AA¥BB¥CC」は 2 番目のデータ・エレメント (ABC02) で、コンポーネント・データ・エレメントで構成される複合エレメントです。
  - 「¥」(円記号) は、コンポーネント・データ・エレメント分離記号です。

    コミュニティー・コンソールでの対応する属性名は、データ・エレメント区切り文字です。
  - 「AA」は、ABC02 の最初のコンポーネント・データ・エレメントです (ABC0201 と指定される場合もあります)。
  - 「BB」は、ABC02 の 2 番目のコンポーネント・データ・エレメントです (ABC0202)。
  - 「CC」は、ABC02 の 3 番目のコンポーネント・データ・エレメントです (ABC0203)。
- 「001^002^003」は、3 番目のデータ・エレメント (ABC03) で、反復データ・エレメントです。
  - 「^」 (ハット記号) は、反復分離記号です。

    コミュニティー・コンソールでの対応する属性名は、データ・エレメント区切り文字です。反復データ・エレメント文字です。
  - 「001」、「002」、「003」は、反復です (すべてが ABC03 として指定されます)。
- 「star?*power」は、4 番目のデータ・エレメント (ABC04) です。
  - ″?″ (疑問符) はリリース文字で、この後に続く次のアスタリスクをデータ・エレメントの分離文字として扱わないことを意味します。
  - 「star*power」は、ABC04 の結果値です。
- 「~」(波形記号) は、セグメント終了記号です。

  コミュニティー・コンソールでの対応する属性名は、セグメント区切り文字です。

## 追加の EDI 属性

ここでは、文書定義レベルまたは接続レベルで設定できる追加の EDI 属性をリストします。

*表 106. 追加の EDI 属性*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| セグメント出力 | いいえ | EDI/XML 変換で使用され、各 EDI セグメントまたは XML エレメントの後ろで改行するかどうかを示します。 | プロトコルまたは接続に限定されます。 | はい |
| 重複する文書 ID を持つ文書を許可します。 | いいえ | 「はい」は、文書 ID (交換制御番号) の重複が許可されることを示します。<br><br>「いいえ」は、交換制御番号の重複をエラーとして扱うことを示します。 | プロトコルまたは接続に限定されます。 | いいえ |
| 変換時の最大エラー・レベル | いいえ | 変換中に許容されるエラー発生の最大数を示します。これ以上エラーが発生すると、変換は失敗します。<br><br>有効な値は、0、1、または 2 です。<br><br>ユーザー指定エラーを示すためのエラー・コマンドが変換マップに含まれている場合で、エラー・コマンドのレベル・パラメーターがこの値より大きい場合、変換は失敗します。 | プロトコルまたは接続に限定されます。 | 0 |
| FA マップ | いいえ | 内部汎用 FA を特定の FA に変換するために使用するマップを提供します。<br>**注:** この属性は、FA マップとして識別されるマップ (マップ・タイプは「K」) のリストから選択します。 | プロトコルまたは接続に限定されます。 | |
| エンベロープ・プロファイル | はい | エンベロープに使用する EDI エンベロープ・プロファイル名。定義したすべてのエンベロープ・プロファイルをリストから選択できます。 | | |
| XMLNS アクティブ | いいえ | 入力 XML 文書のネーム・スペース処理を実行します。この属性は、XML 変換ステップで使用されます。<br><br>有効な値は「はい」または「いいえ」です。 | | スキーマ: はい<br>DTD: いいえ |
| 最大検証エラー・レベル | いいえ | 最大許容検証エラー・レベルです (許容されるエラーの重大度で、これを超えると、トランザクションは失敗したと見なされます)。<br><br>有効な値は、0、1、または 2 です。<br><br>**0** エラーのない検証だけを許可します。<br><br>**1** 単純な要素検証エラーだけを持つ文書を許可します。<br><br>**2** 要素またはセグメントの検証エラーを持つ文書を許可します。 | | 0 |

*表 106. 追加の EDI 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 検証レベル | いいえ | トランザクション・レベルで実行する検査のレベルを示します。値が 2 の場合、英数字検証テーブル属性および文字セット検証テーブル属性に設定されている値を使用することを意味します。この属性は、セグメントの詳細な検証属性が「はい」に設定されている場合、その属性にも適用されます。<br><br>有効な値は、0、1、または 2 です。<br><br>**0** 基本的な検証 (必須エレメントの欠落、セグメント、および最小長/最大長の検査など) のみを実行します。トランザクション定義に指定されているデータ・タイプまたはコード・リストに対してエレメント値を検証しません。<br><br>**1** レベル 0 検証に加えて、データ・エレメントに指定されているコード・リストに対してエレメント値を検証します。<br><br>**2** レベル 1 検証に加えて、エレメントのデータ・タイプについてエレメント値が正しいことを検証します。 | | 0 |
| 文字セット検証テーブル | いいえ | 文字セット検証に使用するテーブルを示します。このテーブルは、検証レベル属性が 2 の場合にのみ使用されます。<br><br>この属性は、仮想コード・リスト・テーブルを参照します。ユーザーは、Data Interchange Services クライアントのマッピング領域の「コード・リスト」タブで、コード・リストを新規作成できます。この領域には、他の目的 (特定の EDI エレメントの検証など) で使用されるコード・リストも含まれています。 | | CHARSET |
| 英数字検証テーブル | いいえ | 英数字検証に使用するテーブルを示します。このテーブルは、検証レベル属性が 2 の場合にのみ使用されます。<br><br>この属性は、仮想コード・リスト・テーブルを参照します。ユーザーは、Data Interchange Services クライアントのマッピング領域の「コード・リスト」タブで、コード・リストを新規作成できます。この領域には、他の目的 (特定の EDI エレメントの検証など) で使用されるコード・リストも含まれています。 | | ALPHANUM |

*表 106. 追加の EDI 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 機能確認通知のみでのグループ・レベル情報の生成 | いいえ | この属性は EDI-X12 に適用されます。値は、「はい」または「いいえ」です。<br>**はい** 機能確認通知のグループ・レベル情報のみを生成します。<br>**いいえ** 機能確認通知の全詳細を生成します (個々のトランザクション、およびトランザクション内のセグメントおよびエレメントごとに生成)。 | プロトコルまたは接続に限定されます。 | いいえ |
| 世紀制御年 | いいえ | 日付が 2 桁の年から 4 桁の年に変換される場合、この値より大きい 2 桁の年の世紀値が「19」であると見なされます。この値と等しいか、この値より小さい 2 桁の年は、世紀値が「20」であると見なされます。<br>有効な範囲は、0 から 99 です。 | プロトコルまたは接続に限定されます。 | 10 |
| セグメントの詳細な検証 | いいえ | この属性は、以下のセグメント・ヘッダーおよびトレーラーに適用されます。<br>• X12<br>– ISA、IEA<br>– GS、GE<br>– ST、SE<br>• EDIFACT<br>– UNA<br>– UNB、UNZ<br>– UNG、UNE<br>– UNH、UNT<br>• UNTUCS<br>– BG、EG<br>– GS、GE<br>– ST、SE<br>有効な値は「はい」または「いいえ」です。<br>**はい** 詳細なエンベロープ・セグメント検証を実行します。検査の深さは、検証レベル属性によって制御されます。<br>**いいえ** 詳細なエンベロープ・セグメント検証を実行しません。 | プロトコルまたは接続に限定されます。 | いいえ |

*表 106. 追加の EDI 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| TA1 オーバーライド | いいえ | 交換エンベロープ・セグメントに指定されている場合、TA1 要求の生成を許可します。EDI-X12 のみに適用されます。<br><br>「はい」に設定すると、TA1 が交換エンベロープ・セグメントに指定されている場合、TA1 が生成されます。<br><br>「いいえ」に設定すると、TA1 が交換エンベロープ・セグメントに指定されている場合でも、TA1 は生成されません。 | プロトコルまたは接続に限定されます。 | はい |
| エラー時に廃棄 (Discard on error) | いいえ | この属性は、ポリモアフィック処理で使用されます。<br><br>エンベロープ解除に起因するバッチの場合、この属性は、いずれかのトランザクションが失敗した場合にバッチ全体を廃棄するかどうかを示します。<br><br>有効な値は「はい」および「いいえ」です。 | プロトコルまたは接続に限定されます。 | いいえ |
| 接続プロファイル修飾子 1 | いいえ | この属性は、交換接続に使用するプロファイルを判別するためにエンベローパーで使用されます。この属性の値が異なるトランザクションは、別々の交換に入れられます。 | | |
| 交換修飾子 | いいえ | 交換の送信側と受信側の ID の形式を識別するためのコード。 | | |
| 交換 ID | いいえ | 文書の特定の送信側または受信側を示します。入力されたデータの型は、交換修飾子属性によって決定されます。 | | |
| 交換の使用標識 | いいえ | 変換中のソース・ドキュメントを実動、テスト、または情報のいずれの文書として分類するかを示します。<br><br>有効な値は P、T、および I です。 | | |
| グループ・アプリケーション送信側 ID | いいえ | トランザクションの特定の送信側を示します。この属性は、取引先から合意を得たときに、会社内でアドレッシングを促進します。 | | |
| グループ・アプリケーション受信側 ID | いいえ | トランザクションの特定の受信側またはアプリケーションを示します。この属性は、取引先から合意を得たときに、会社内でアドレッシングを促進します。 | | |
| 交換の逆ルーティング | いいえ | 受信側が応答を送信する宛先を示します。 | | |
| 交換のルーティング・アドレス | いいえ | 前方ルーティング用のサブアドレス・コード | | |
| グループ・アプリケーション送信側修飾子 | いいえ | グループ・アプリケーション送信側 ID の形式を識別するためのコード。 | | |

*表 106. 追加の EDI 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| グループ・アプリケーション受取先修飾子 | いいえ | グループ・アプリケーション受信側 ID の形式を識別するためのコード。 | | |
| グループ・アプリケーション・パスワード | いいえ | この属性は、セキュリティー情報を定義します。 | | |
| FA 必要制限時間 | | FA を戻す必要があるトランザクションが送信されてから経過した分数。値がブランクの場合、FA は必要ありません。 | | |

## Data Interchange Services クライアント・プロパティー

ここでは、Data Interchange Services クライアントの変換マップの一部として設定できるプロパティー、および対応する WebSphere Partner Gateway 属性をリストします。

*表 107. マップ・プロパティーおよび対応する属性*

| Data Interchange Services クライアント・プロパティー | オーバーライドされる WebSphere Partner Gateway 属性 |
|---|---|
| AckReq | 応答要求済み |
| Alphanum | 英数字検証テーブル |
| Charset | 文字セット検証テーブル |
| CtlNumFlag | トランザクション ID 別制御番号 |
| EdiDecNot (10 進表記) | 10 進表記 |
| EdiDeDlm (データ・エレメント分離文字) | データ・エレメント区切り文字 |
| EdiDeSep (反復データ・エレメント分離記号) | 反復データ・エレメント分離記号 |
| EdifactGrp | EDI 用のグループの作成 |
| EdiRlsChar (リリース文字) | リリース文字 |
| EdiSeDlm (コンポーネント・データ・エレメント分離記号) | サブエレメント区切り文字 |
| EdiSegDlm (セグメント終了記号) | セグメント区切り文字 |
| EnvProfName | エンベロープ・プロファイル |
| EnvType | エンベロープ・タイプ |
| MaxDocs | 最大トランザクション番号 |
| Reroute | 交換の逆ルーティング |
| SegOutput | セグメント出力 |
| ValLevel | 検証レベル |
| ValErrLevel | 最大検証エラー・レベル |
| ValMap | 検証マップ |

462 ページの表 108 は、追加の Data Interchange Services クライアント・プロパティーおよび関連する WebSphere Partner Gateway 属性をリストしています。

表 108. Data Interchange Services クライアント・プロパティーおよび関連する属性

| Data Interchange Services クライアント・プロパティー | オーバーライドされる WebSphere Partner Gateway 属性 |
|---|---|
| IchgCtlNum | 交換制御番号 |
| IchgSndrQl | 交換送信側修飾子 |
| IchgSndrId | 交換送信側 ID |
| IchgRcvrQl | 交換受信側修飾子 |
| IchgRcvrId | 交換受信側 ID |
| IchgDate | 交換日付 |
| IchgTime | 交換時間 |
| IchgPswd | 交換パスワード |
| IchgUsgInd | 交換の使用標識 |
| IchgAppRef | 交換のアプリケーション参照 |
| IchgVerRel | 交換のバージョンとリリース番号 |
| IchgGrpCnt | 交換内のグループ数 |
| IchgCtlTotal | 交換トレーラー・セグメントからの照査合計 |
| IchgTrxCnt | 交換内の文書数 |
| GrpCtlNum | グループ制御番号 |
| GrpFuncGrpId | 機能グループ ID |
| GrpAppSndrId | グループ・アプリケーションの送信側 ID |
| GrpAppRcvrId | グループ・アプリケーションの受信側 ID |
| GrpDate | グループの日付 |
| GrpTime | グループの時刻 |
| GrpPswd | グループ・パスワード |
| GrpVer グループ・バージョン | グループ・バージョン |
| GrpRel グループのリリース | グループ・リリース |
| GrpTrxCnt | グループ内の文書数 |
| TrxCtlNum | トランザクション制御番号 |
| TrxCode | トランザクション・コード |
| TrxVer | トランザクション・バージョン |
| TrxRel | トランザクション・リリース |
| TrxSegCnt | 文書内の EDI セグメント数 |

## AS 属性

このセクションでは、AS 属性について説明します。

表 109. AS 属性

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 応答のための時間 (分単位) | いいえ | 元の要求を再送する前に MDN 確認通知を待つ時間。この属性は、「再試行カウント」と連動します。単位は分です。 | パッケージまたは接続に限定されます。 | 30 |

*表 109. AS 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 再試行カウント | いいえ | MDN が受信されない場合に要求を送信する回数。この属性は、「応答のための時間」と連動します。<br><br>例えば、この属性が 3 に設定されている場合、要求は 4 回まで送信できます (最初と 3 回の再試行)。 | パッケージまたは接続に限定されます。 | 3 |
| AS 圧縮後に署名 | いいえ | AS 圧縮をペイロードと署名の両方に適用するか、あるいはペイロードだけに適用するかを示します。<br><br>「はい」を選択すると、ペイロードはメッセージの署名前に圧縮されます。この属性は、「AS 圧縮」属性と連動します。 | パッケージまたは接続に限定されます。 | はい |
| AS 圧縮 | いいえ | データを圧縮します。この属性は、「AS 圧縮後に署名」属性と連動します。 | パッケージまたは接続に限定されます。 | いいえ |
| AS 暗号化 | いいえ | この属性は AS2 に適用され、パートナーが非同期 MDN を送信する URL を指定するために使用されます。この属性は、「AS MDN 非同期」属性と連動しますが、同期 MDN の場合でも値は必要です。 | パッケージまたは接続に限定されます。 | いいえ |
| AS MDN Http Url | 「AS MDN 非同期」属性が「はい」で、AS2 を使用している場合は「はい」 | この属性は AS2 に適用され、パートナーが非同期 MDN を送信する URL を指定するために使用されます。この属性は、「AS MDN 非同期」属性と連動しますが、同期 MDN の場合でも値は必要です。 | パッケージまたは接続に限定されます。 | |
| AS MDN E メール・アドレス | 「AS MDN 非同期」属性が「はい」で、AS1 を使用している場合は「はい」 | 非同期 MDN の送信時に使用するパートナーの E メール・アドレスを指定します。この属性は、「AS MDN 要求済み」属性と連動して使用します。AS MDN E メール・アドレスの値は、「Disposition-notification-to」フィールドで使用されます。<br><br>AS1 の場合、この属性は、mailto:xxx@company.com の形式の「AS MDN 非同期」属性と連動します。<br><br>AS2 の場合、E メール・アドレス自体が使用されませんが、この属性にはやはり値が必要です。 | パッケージまたは接続に限定されます。 | |

*表 109. AS 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| AS MDN 非同期 | いいえ | MDN が同期または非同期のどちらで戻されるかを指定します。この属性の値は、「AS MDN HTTP URL」属性または「AS MDN E メール・アドレス」属性のどちらが使用されるかに影響します。<br><br>有効な値は「はい」および「いいえ」です。<br><br>**はい** 非同期<br><br>**いいえ** 同期<br><br>この属性が「はい」である場合、「receipt-delivery-option」フィールドは「AS MDN HTTP URL」属性 (AS2 の場合) または「AS MDN E メール・アドレス」属性 (AS1 の場合) に基づいて入力されます。 | パッケージまたは接続に限定されます。 | はい |
| AS MDN 要求済み | いいえ | MDN 応答が必要かどうかを指定します。この属性が「はい」に設定されている場合、「transport Disposition-notification-to」ヘッダーは「AS MDN E メール・アドレス」属性からの値で埋められます。<br><br>有効な値は「はい」および「いいえ」です。<br><br>**はい** MDN を要求します。<br><br>**いいえ** MDN は要求しません。 | パッケージまたは接続に限定されます。 | はい |
| AS Message Digest アルゴリズム | いいえ | 署名時に使用するメッセージ・ダイジェスト・アルゴリズム。この属性は、「AS 署名済み」属性および「AS MDN 署名済み」属性と連動します。<br><br>署名済み MDN では、「Disposition-notification-options: signed-receipt-micalg」ヘッダーに入力するためにこの値が使用されます。 | パッケージまたは接続に限定されます。 | sha1 |

*表 109. AS 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| AS MDN 署名済み | いいえ | 署名済み MDN を戻すことを要求するかどうかを示します。この属性は、「AS MDN 要求済み」と連動します。<br><br>値が「はい」である場合は、「Disposition-notification-options: signed-receipt-protocol」に入力されます。<br><br>有効な値は「はい」および「いいえ」です。<br><br>**はい** 署名済み MDN が要求されます。<br><br>**いいえ** 署名済み MDN は要求されません。<br><br>この属性が「はい」に設定されている場合、パートナーによって送信される MDN は署名されている必要があります。<br><br>この属性が「いいえ」に設定されている場合、MDN は署名付きまたは未署名にすることができます。 | パッケージまたは接続に限定されます。 | いいえ |
| AS 署名済み | いいえ | 文書に署名するかどうかを指定します。<br><br>交換の TO 側では (文書をパートナーに送信する場合)、これは文書に署名するかどうかを指定します。<br><br>交換の FROM 側では (パートナーから受信する場合)、属性が「はい」に設定されている場合、パートナーから送信された AS 要求に署名する必要があります。属性が「いいえ」に設定されている場合、パートナーからの文書は署名付きまたは未署名にすることができます。<br><br>**はい** 文書に署名します。<br><br>**いいえ** 署名付きの文書は不要です。 | パッケージまたは接続に限定されます。 | いいえ |
| 否認防止が必要 | いいえ | この文書を否認防止ストアに保管する必要があるかどうかを示します。文書がソースであってもターゲットであっても適用されます。<br><br>はい – 文書を否認防止ストアに保管します。<br><br>いいえ – 文書を否認防止ストアに保管しません。 | パッケージまたは接続に限定されます。 | はい |

表 109. AS 属性 (続き)

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| メッセージ・ストアが必要 | いいえ | この文書をメッセージ・ストアに保管する必要があるかどうかを示します。ソース文書とターゲット文書の両方に適用されます。<br><br>はい – 文書をメッセージ・ストアに保管します。<br><br>いいえ – 文書をメッセージ・ストアに保管しません。 | パッケージまたは接続に限定されます。 | はい |
| AS ビジネス ID | いいえ | 「AS2-To」または「AS3-To」ヘッダーに使用する AS ビジネス ID。値が指定されない場合、WebSphere Partner Gateway はソース・ドキュメントで使用される受信側のビジネス ID を使用します。<br>**注:** 「AS2-From」ヘッダーまたは「AS3-From」ヘッダーは、ソース文書定義の「AS ビジネス ID」属性から設定されます。ソース文書が定義されていない場合は、WebSphere Partner Gateway に入り、AS として送信される元のソース文書から設定されます。 | パッケージまたは接続に限定されます。 | |
| AS MDN FTP アドレス | 「AS MDN 要求」属性が「はい」の場合は、AS3 では「はい」 | MDN の要求時に使用する AS MDN FTP アドレス。この属性は、「AS MDN 要求済み」属性と連動します。AS MDN FTP アドレスの値は、「Disposition-notification-to」フィールドで使用されます。次の形式にする必要があります。`ftp://username:pwd@host.com:port/folder-name` | パッケージまたは接続に限定されます。 | いいえ |

## RosettaNet 属性

このセクションでは、RosettaNet 属性について説明します。

表 110. RosettaNet 属性

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 応答のための時間 | はい | 元の要求を再送する前に受信確認通知を待つ時間。この属性は、「再試行カウント」と連動します。単位は分です。<br><br>デフォルト値は RosettaNet PIP 仕様文書から取得されます。 | パッケージまたは接続に限定されます。 | 120 |
| 実行のための時間 | はい | 障害通知メッセージを送信する前に要求アクションへの応答を待つ時間。 | パッケージまたは接続に限定されます。 | |

*表 110. RosettaNet 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 再試行カウント | はい | 受信確認通知が受信されなかった場合に要求を送信する回数。この属性は、「応答のための時間」と連動します。<br><br>例えば、3 が設定されている場合、要求は 4 回まで送信できます (最初と 3 回の再試行)。<br><br>デフォルト値は RosettaNet PIP 仕様文書から取得されます。 | パッケージまたは接続に限定されます。 | 3 |
| デジタル署名が必要 | いいえ | PIP メッセージにデジタル署名が必要かどうかを示します。<br><br>デフォルト値は RosettaNet PIP 仕様文書から取得されます。 | パッケージまたは接続に限定されます。 | はい |
| 否認防止が必要 | いいえ | この文書を否認防止ストアに保管する必要があるかどうかを示します。文書がソースであってもターゲットであっても適用されます。<br><br>はい – 文書を否認防止ストアに保管します。<br><br>いいえ – 文書を否認防止ストアに保管しません。 | パッケージまたは接続に限定されます。 | はい |
| メッセージ・ストアが必要 | いいえ | この文書をメッセージ・ストアに保管する必要があるかどうかを示します。ソース文書とターゲット文書の両方に適用されます。<br><br>はい – 文書をメッセージ・ストアに保管します。<br><br>いいえ – 文書をメッセージ・ストアに保管しません。 | パッケージまたは接続に限定されます。 | はい |
| 受信の否認防止が必要 (Non-Repudiation of Receipt Required) | いいえ | 否認防止ストアに受信確認通知文書を保管するかどうかを示します。<br><br>デフォルト値は RosettaNet PIP 仕様文書から取得されます。 | パッケージまたは接続に限定されます。 | はい |
| 同期サポートあり | | PIP が同期通信をサポートするかどうかを示します。<br><br>デフォルト値は PIP 仕様に基づいて提供されます。 | パッケージまたは接続に限定されます。<br><br>この属性は、RNIF 2.0 にのみ使用されます。 | |

*表 110. RosettaNet 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 同期応答が必要 | | PIP に同期受信確認通知が必要かどうかを示します。<br><br>デフォルト値は PIP 仕様に基づいて提供されます。 | パッケージまたは接続に限定されます。<br><br>この属性は、RNIF 2.0 にのみ使用されます。 | |
| グローバル・サプライ・チェーン・コード | RNIF 1.1 に必要 | パートナーの機能用のサプライ・チェーンを識別するコード。<br><br>有効な値は、以下のとおりです。<br>• 電子部品<br>• 情報技術<br>• 半導体テクノロジー | パッケージまたは接続に限定されます。 | |
| 暗号化 | | この属性は、暗号化を実行するかどうかを示します。<br>**注:** これは SSL 暗号化とは異なります。<br><br>交換の TO 側では (文書をパートナーに送信する場合)、これは文書を暗号化するかどうかを指定します。<br><br>交換の FROM 側では (パートナーから文書を受け取る場合)、属性が「はい」に設定されている場合、パートナーから送信された RNIF 要求を暗号化する必要があります。属性が「いいえ」に設定されている場合、パートナーからの文書は暗号化することもでき、暗号化しないこともできます。<br><br>有効な値は、以下のとおりです。<br>**なし** 暗号化は必要ありません。<br>**ペイロード** RosettaNet サービス・コンテンツのみを暗号化します。<br>**ペイロードおよびコンテナー** RosettaNet サービス・コンテンツとサービス・ヘッダーをともに暗号化します。 | パッケージまたは接続に限定されます。<br><br>この属性は、RNIF 2.0 にのみ使用されます。 | なし |
| メッセージ標準テキスト | いいえ | サービス・コンテンツが準拠しなければならない標準。これは、非 RosettaNet 指定のサービス・コンテンツ・メッセージの場合にのみ指定してください。 | | デフォルト値はありません。 |

表 110. RosettaNet 属性 (続き)

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| メッセージ標準バージョン | いいえ | サービス・コンテンツが準拠しなければならない標準のバージョン。これは、非 RosettaNet 指定のサービス・コンテンツ・メッセージの場合にのみ指定してください。 | | デフォルト値はありません。 |
| PIP ペイロード・バインディング ID | いいえ | これはパートナーが定義する PIP バインディング ID で、取引パートナー間で固有です。この属性は、非 RosettaNet サービス・コンテンツの場合にのみ設定されます。 | | デフォルト値はありません。 |
| FromGlobalPartner ClassificationCode | RNIF 1.1 スキーマの場合は「はい」 | サプライ・チェーン内のパートナーの機能を識別するコード。スキーマ・ベースの PIP に RNIF 1.1 を使用する場合にのみ必須です。スキーマ・ベースの PIP が使用されている場合には、この値を 0A1 PIP に対しても指定する必要があります。 | | デフォルト値はありません。 |
| ToGlobalPartner ClassificationCode | RNIF 1.1 スキーマの場合は「はい」 | サプライ・チェーン内のパートナーの機能を識別するコード。スキーマ・ベースの PIP に RNIF 1.1 を使用する場合にのみ必須です。スキーマ・ベースの PIP が使用されている場合には、この値を 0A1 PIP に対しても指定する必要があります。 | | デフォルト値はありません。 |
| RN Message Digest アルゴリズム | いいえ | この属性は、「デジタル署名が必要」属性が「はい」に設定されている場合にのみ使用されます。デジタル署名に使用するダイジェスト・アルゴリズムを決定します。指定可能な値は「SHA1」および「MD5」です。 | | SHA1 |
| RN 暗号化アルゴリズム | いいえ | この属性は、「暗号化」属性が「ペイロード」または「ペイロードおよびコンテナー」に設定されている場合にのみ使用されます。指定可能な値は「Triple-DES」および「RC2-40」です。 | | Triple-DES |

## 「バックエンド統合」属性

このセクションでは、バックエンド統合パッケージ化に関連する属性について説明します。

表 111. 「バックエンド統合」属性

| 属性 | 説明 | デフォルト |
|---|---|---|
| エンベロープ・フラグ | この属性は、文書を XML エンベロープでラップするかどうかを示します。<br><br>有効な値は「はい」および「いいえ」です。 | いいえ |

## ebMS 属性

このセクションでは、ebMS 属性について説明します。

*表 112. ebMS 属性*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 応答のための時間 (分単位) | いいえ | 元の要求を再送する前に確認通知を待つ時間。この属性は、「再試行カウント」と連動します。単位は分です。 | パッケージまたは接続に限定されます。 | 30 |
| 再試行カウント | いいえ | 確認通知が受信されない場合に要求を送信する回数。この属性は、「応答のための時間」と連動します。<br><br>例えば、この属性が 3 に設定されている場合、要求は 4 回まで送信できます (最初と 3 回の再試行)。 | パッケージまたは接続に限定されます。 | 3 |
| 否認防止が必要 | いいえ | この文書を否認防止ストアに保管する必要があるかどうかを示します。文書がソースであってもターゲットであっても適用されます。<br><br>はい – 文書を否認防止ストアに保管します。<br><br>いいえ – 文書を否認防止ストアに保管しません。 | パッケージまたは接続に限定されます。 | はい |
| メッセージ・ストアが必要 | いいえ | この文書をメッセージ・ストアに保管する必要があるかどうかを示します。ソース文書とターゲット文書の両方に適用されます。<br><br>はい – 文書をメッセージ・ストアに保管します。<br><br>いいえ – 文書をメッセージ・ストアに保管しません。 | パッケージまたは接続に限定されます。 | はい |
| 受信の否認防止が必要 (Non-Repudiation of Receipt Required) | いいえ | 否認防止ストアに受信確認通知文書を保管するかどうかを示します。 | パッケージまたは接続に限定されます。 | はい |

*表 112. ebMS 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 確認通知要求済み | いいえ | 指定可能な値は「always」、「perMessage」、および「never」です。<br><br>「always」に設定した場合、ebMS 文書を送信すると、ebMS SOAP 文書に acknowledgmentRequested エレメントを入れることにより、確認通知の要求が作成されます。<br><br>送信側にとって、「perMessage」と「never」は「いいえ」と同じ意味です。受信した ebMS 文書でこの値が「always」として設定されていた場合には、その文書は確認通知を要求します。要求しない場合、文書は許可されません。<br><br>値が受信側のハブで「perMessage」に設定されている場合は、文書が確認通知を要求してもしなくても許可されます。値が「never」に設定されている場合は、着信した ebMS 文書は確認通知を要求しません。 | | never |
| 確認通知署名要求済み | いいえ | 指定可能な値は「always」、「perMessage」、および「never」です。<br><br>「always」は署名付き確認通知を要求します。「perMessage」および「never」の場合は、未署名確認通知の要求があるかもしれません。これは、「AcknowledgementRequested」属性と連動します。<br><br>「AcknowledgmentRequested」属性の値が「perMessage」または「never」に設定されている場合は、この属性は考慮されません。<br><br>値が指定されていない場合は「never」が使用されます。この属性は、文書の送信時にのみ使用されます。受信文書には使用されません。 | | never |
| アクター | いいえ | この属性は、ebMS 2.0 インプリメンテーションでは設定する必要はありません。「アクター」属性が必要なのは、同期確認通知が要求される場合です。この属性は、ebMS SOAP 文書に入っています。<br><br>ebMS 2.0 仕様では、この属性の定数値はデフォルトで http://schemas.xmlsoap.org/soap/actor/next です。このように処理されるので、ユーザーはどんな場合もこの属性値を設定する必要はありません。これは、将来のインプリメンテーションで使用するように残されています。 | | http://schemas.xmlsoap.org/soap/actor/next |

表 112. ebMS 属性 (続き)

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 圧縮が必要 | いいえ | 指定可能な値は「はい」と「いいえ」です。ebMS ペイロードを圧縮する場合は値を「はい」に設定します。圧縮が不要なら、何も設定しないか「いいえ」に設定します。 | | いいえ |
| 重複の除去 | いいえ | ebMS メッセージの送信でこの属性の値が「always」に設定されていると、ebMS SOAP 文書に DuplicateElimination エレメントが組み込まれます。ebMS SOAP 文書にこのエレメントが存在すると、ebMS 文書が重複する場合、受信ハブは ebMS ペイロードをバックエンドに送信しません。値が「perMessage」と「never」の場合は、DuplicateElimination エレメントは SOAP 文書に組み込まれません。<br><br>ebMS 文書の受信で値が「always」に設定されている場合は、DuplicateElimination エレメントが ebMS SOAP 文書に存在する必要があります。存在しない場合、文書は許可されません。値が「perMessage」の場合は、DuplicateElimination エレメントが SOAP 文書内にあってもなくても、文書は許可されます。<br><br>値が「never」の場合は、DuplicateElimination エレメントが SOAP 文書に存在していてはいけません。存在する場合、文書は許可されません。値が指定されていない場合は「never」が使用されます。<br><br>受信した ebMS 文書で属性値が「always」であり、DuplicateElimination エレメントが存在する場合、その文書を調べて重複しているかどうかを確認します。重複している文書は許可されません。 | | never |
| 暗号化構成要素 | いいえ | この属性の値は、ペイロードのセミコロンで区切られたコンテンツ・タイプのリストです。例えば、application/xml;text/xml;application/binary:application/edi の場合、これらのコンテンツ・タイプのペイロードが暗号化されます。<br><br>この属性は、「暗号化が必要」属性が「はい」に設定されている場合にのみ使用されます。<br>**注:** 「暗号化が必要」が「はい」に設定されていて、コンテンツ・タイプが「暗号化構成要素」で構成されていない場合は、何も暗号化されません。 | | application/xml;text/xml;application/EDI-X12;application/EDI-CONSENT;application/EDIFACT;application/binary;application/octet-stream |

表 112. ebMS 属性 (続き)

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 暗号化 Mime パラメーター | いいえ | 追加パラメーターを MimeMultipart ヘッダーとして暗号化された文書に組み込む場合に使用されるオプション属性。個々の暗号化されたペイロードに適用されます。例えば、値を「smime-type=”enveloped-data”」や「type=”text/xml” version=”1.0.”」とします。<br><br>この属性は、「暗号化が必要」属性が「はい」に設定されている場合にのみ使用されます。 | | デフォルト値はありません。 |
| 暗号化 Mime タイプ | いいえ | 現行のインプリメンテーションでは使用されません。 | | デフォルト値はありません。 |
| 暗号化が必要 | いいえ | 指定可能な値は「はい」と「いいえ」です。「はい」に設定すると、ペイロードが暗号化されます。この属性は、「暗号化構成要素」と連動します。<br>**注:** 「暗号化が必要」が「はい」に設定されていて、コンテンツ・タイプが「暗号化構成要素」で構成されていない場合は、何も暗号化されません。 | | |
| 暗号化変換 | いいえ | 現行のインプリメンテーションでは使用されません。 | | デフォルト値はありません。 |
| 署名から除外 | いいえ | この属性の値は、セミコロンで区切られたコンテンツ・タイプのリストです (例: `application/binary;application/octet-stream`)。このコンテンツ・タイプのペイロードは署名には組み込まれません。<br><br>この属性は、「デジタル署名が必要」属性の値が「はい」である場合にのみ使用されます。 | | エントリーなし。すべてのペイロードに署名が適用されます。 |
| ハッシュ関数 | いいえ | 署名中にペイロードをハッシュする場合に XML Signature で使用されるハッシュ・アルゴリズム。<br><br>この属性は、「デジタル署名が必要」属性の値が「はい」である場合にのみ使用されます。 | | SHA1 |
| メッセージ順序セマンティクス | いいえ | 指定可能な値は「保証済み」および「未保証」です。文書の送信時に値が「保証済み」に設定されている場合、「メッセージ順序」エレメントが SOAP 文書に組み込まれます。SOAP 文書でこのエレメントを識別する受信ハブでは、ペイロードが必ず連続してバックエンドに送信されます。<br><br>受信文書では、この属性が「保証済み」に設定されていると、着信する ebMS 文書内に MessageOrder エレメントが存在します。このエレメントが欠落していると、文書は許可されず、エラー・コード「Inconsistent」のエラー・メッセージがパートナーに送信されます。 | | 未保証 |

表 112. ebMS 属性 (続き)

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 役割 | いいえ | ebMS 文書を送信する場合、この属性値は ebMS SOAP 文書の役割エレメント値に相当します。<br><br>ebMS を受信する場合、この属性値は ebMS SOAP 文書の役割エレメント値と比較され、値が一致しない場合 (属性値が空の場合も含む) は文書が許可されず、エラー・コード「Inconsistent」のエラー・メッセージがパートナーに送信されます。 | | デフォルト値はありません。 |
| 持続期間 | いいえ | 文書が持続する時間 (分単位)。例えば、24 時間の場合は 1440。<br><br>文書を送信する場合、公式を使用して TimeToLive を計算するのに「持続期間」が使用されます。つまり、TimeToLive = 持続時間 + (再試行の回数 * 再試行間隔) です。<br><br>文書を受信する場合は、重複の除去に「持続時間」が使用されます。messageID が重複する文書を受信すると、先に受信した文書の「持続時間」が経過したかどうかが検査されます。持続時間が経過していない場合は、文書に重複のマークが付けられます。経過した場合は、重複のマークは付けられません。<br><br>エントリーがない場合は、値はデフォルトの 0 になります。 | | 0 |
| パッケージ化構成要素 | いいえ | 現行のインプリメンテーションでは使用されません。 | | デフォルト値はありません。 |
| パッケージ Mime パラメーター | いいえ | 現行のインプリメンテーションでは使用されません。 | | デフォルト値はありません。 |
| 暗号化アルゴリズム | 「暗号化が必要」属性の値が「はい」に設定されている場合は「はい」 | ebMS ペイロードを暗号化するために使用するアルゴリズム。この値は、「暗号化プロトコル」属性と連動します。<br><br>この属性は、「暗号化が必要」属性が「はい」に設定されている場合にのみ使用されます。 | | AES-128 |
| 暗号化プロトコル | いいえ | ebMS ペイロードを暗号化するために使用するプロトコル。指定可能な値は「XMLEncryption」および「SMIME」です。<br><br>この属性は、「暗号化が必要」属性が「はい」に設定されている場合にのみ使用されます。「暗号化が必要」が「はい」に設定されていてこの属性に値が指定されていない場合は、文書は許可されません。 | | XMLEncryption |

*表 112. ebMS 属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 再試行間隔 | いいえ | 送信文書で、ebMS 文書を再送するまでの確認通知の待機時間 (分)。ebMS 文書が再送されるのは、確認通知が要求されているのに再試行間隔内にパートナーからの確認通知が受信されない場合のみです。<br><br>値 0 は、再試行を行わないことを意味します。この属性は、「再試行カウント」属性と連動します。 | | 270 |
| 署名アルゴリズム | 「デジタル署名が必要」が「はい」の場合は「はい」 | ebMS 文書に署名するために使用するアルゴリズム。この属性は、「デジタル署名が必要」属性の値が「はい」である場合にのみ使用されます。 | | dsa-sha1 |
| 署名変換 | いいえ | XML Signature を作成する前にペイロードを変換するために使用される変換アルゴリズム。この属性は、「デジタル署名が必要」属性の値が「はい」である場合にのみ使用されます。 | | デフォルト値はありません。 |
| 同期応答モード | いいえ | 送信される文書に必要な同期応答のタイプ。<br><br>指定可能な値は次のとおりです。<br>• **MSHSignalsOnly** - MSH 確認通知/エラー文書のみが同期接続で送信されます。ビジネス応答とビジネス・シグナル文書は非同期に戻されます。<br>• **signalsOnly** – ビジネス・シグナル文書と MSH 文書だけが同期接続で送信されます。ビジネス応答は非同期に戻されます。<br>• **responseOnly** – ビジネス応答と MSH 文書だけが同期接続で送信されます。ビジネス・シグナル文書は戻されません。<br>• **signalsAndResponse** - ビジネス応答とビジネス・シグナル文書が同期接続で送信されます。<br>• **なし** – 受信側からの同期応答文書はありません。 | | なし |
| 明りょう検査が必要 | いいえ | この属性の値は、ヘッダー「x-aux-IntelligibleCheckRequired」の値としてバックエンドに送信されます。指定可能な値は「はい」と「いいえ」です。目的は、ペイロードを持つ ebXML 文書にエラーが含まれていない場合にのみ ReceiptAcknowledgement を送信するように、バックエンドに指示することです。この値の解釈は、バックエンドに任されます。 | | いいえ |

表 112. ebMS 属性 (続き)

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 正規化方式 | いいえ | XML Signature を行う前に使用される正規化アルゴリズム。この属性は、「デジタル署名が必要」属性の値が「はい」である場合にのみ使用されます。 | | INCLUSIVE_WITH_COMMENTS |
| 圧縮構成要素 | いいえ | セミコロンで区切られた、ペイロードのコンテンツ・タイプのリスト。これは圧縮されます。例えば、コンテンツ・タイプが「text/xml」および「application/edi」のペイロードを圧縮する必要がある場合、この属性の値は「text/xml;application/edi」になります。エントリーがない場合は、「圧縮が必要」が「はい」に設定されていても、ペイロードは圧縮されません。<br><br>この属性は、「圧縮が必要」属性の値が「はい」である場合にのみ使用されます。 | | application/xml; text/xml; application/EDI-X12; application/EDI-CONSENT; application/EDIFACT |
| サービス・タイプ | サービス・エレメント (文書タイプ) の値が URI でない場合は「はい」 | ebMS 文書を送信する場合、ebMS SOAP メッセージ内の ebMSService エレメントの値が URI または一定のストリングのどちらかでなければなりません。ストリングの場合にはこのタイプの属性が必須です。サービス (文書タイプ) の値が URI でない場合、この「サービス・タイプ」属性の値は、ebMS 文書の type 属性値として使用されます。 | | デフォルト値はありません。 |

## 一般属性

このセクションでは、一般属性について説明します。

表 113. 一般属性

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| 検証マップ | いいえ | この文書の検証に使用する検証マップ。実行時に使用されるアクションには、この属性を利用する検証ステップが必要です。アップロードされ、この文書タイプに関連付けられている検証マップだけが選択できます。 | パッケージまたは接続に限定されます。 | デフォルト値はありません。 |
| ユーザー属性 1 | いいえ | ユーザー定義出口で使用されます。値は、ユーザー定義出口の作成者によって決定されます。これらは、属性が bcg.ro.user.User01 のビジネス文書オブジェクトで From (ソース文書) 接頭部または To (ターゲット文書) 接頭部として設定されます。 | | デフォルト値はありません。 |

*表 113. 一般属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| ユーザー属性 2 | いいえ | ユーザー定義出口で使用されます。値は、ユーザー定義出口の作成者によって決定されます。これらは、属性が bcg.ro.user.User02 のビジネス文書オブジェクトで From (ソース文書) 接頭部または To (ターゲット文書) 接頭部として設定されます。 | | デフォルト値はありません。 |
| ユーザー属性 3 | いいえ | ユーザー定義出口で使用されます。値は、ユーザー定義出口の作成者によって決定されます。これらは、属性が bcg.ro.user.User03 のビジネス文書オブジェクトで From (ソース文書) 接頭部または To (ターゲット文書) 接頭部として設定されます。 | | デフォルト値はありません。 |
| ユーザー属性 4 | いいえ | ユーザー定義出口で使用されます。値は、ユーザー定義出口の作成者によって決定されます。これらは、属性が bcg.ro.user.User04 のビジネス文書オブジェクトで From (ソース文書) 接頭部または To (ターゲット文書) 接頭部として設定されます。 | | デフォルト値はありません。 |
| ユーザー属性 5 | いいえ | ユーザー定義出口で使用されます。値は、ユーザー定義出口の作成者によって決定されます。これらは、属性が bcg.ro.user.User05 のビジネス文書オブジェクトで From (ソース文書) 接頭部または To (ターゲット文書) 接頭部として設定されます。 | | デフォルト値はありません。 |
| ユーザー属性 6 | いいえ | ユーザー定義出口で使用されます。値は、ユーザー定義出口の作成者によって決定されます。これらは、属性が bcg.ro.user.User06 のビジネス文書オブジェクトで From (ソース文書) 接頭部または To (ターゲット文書) 接頭部として設定されます。 | | デフォルト値はありません。 |
| ユーザー属性 7 | いいえ | ユーザー定義出口で使用されます。値は、ユーザー定義出口の作成者によって決定されます。これらは、属性が bcg.ro.user.User07 のビジネス文書オブジェクトで From (ソース文書) 接頭部または To (ターゲット文書) 接頭部として設定されます。 | | デフォルト値はありません。 |

*表 113. 一般属性 (続き)*

| 属性 | 必須 | 説明 | 制約事項 | デフォルト |
|---|---|---|---|---|
| ユーザー属性 8 | いいえ | ユーザー定義出口で使用されます。値は、ユーザー定義出口の作成者によって決定されます。これらは、属性が bcg.ro.user.User08 のビジネス文書オブジェクトで From (ソース文書) 接頭部または To (ターゲット文書) 接頭部として設定されます。 | | デフォルト値はありません。 |
| ユーザー属性 9 | いいえ | ユーザー定義出口で使用されます。値は、ユーザー定義出口の作成者によって決定されます。これらは、属性が bcg.ro.user.User09 のビジネス文書オブジェクトで From (ソース文書) 接頭部または To (ターゲット文書) 接頭部として設定されます。 | | デフォルト値はありません。 |
| ユーザー属性 10 | いいえ | ユーザー定義出口で使用されます。値は、ユーザー定義出口の作成者によって決定されます。これらは、属性が bcg.ro.user.User10 のビジネス文書オブジェクトで From (ソース文書) 接頭部または To (ターゲット文書) 接頭部として設定されます。 | | デフォルト値はありません。 |

# 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

*〒242-8502*
*神奈川県大和市下鶴間1623番14号*
*日本アイ・ビー・エム株式会社*
*法務・知的財産*
*知的財産権ライセンス渉外*

**以下の保証は、国または地域の法律に沿わない場合は、適用されません。** IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Burlingame Laboratory Director
IBM Burlingame Laboratory
577 Airport Blvd., Suite 800
Burlingame, CA 94010
U.S.A

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されていま

す。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。



この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

## プログラミング・インターフェース情報

プログラミング・インターフェース情報は、プログラムを使用してアプリケーション・ソフトウェアを作成する際に役立ちます。一般使用プログラミング・インターフェースにより、お客様はこのプログラム・ツール・サービスを含むアプリケーション・ソフトウェアを書くことができます。ただし、この情報には、診断、修正、および調整情報が含まれている場合があります。診断、修正、調整情報は、お客様のアプリケーション・ソフトウェアのデバッグ支援のために提供されています。

**重要:** 診断、修正、調整情報は、変更される場合がありますので、プログラミング・インターフェースとしては使用しないでください。

## 商標

以下は、世界の多くの国で登録された International Business Machines Corp. の商標です。

| | | | | |
|---|---|---|---|---|
| IBM | DB2 | IMS | MQIntegrator | Tivoli |
| IBM ロゴ | DB2 Universal Database | Informix | MVS | WebSphere |
| AIX | iSeries | OS/400 | z/OS | |
| CICS | IBMLink | Lotus | Passport Advantage | |
| CrossWorlds | i5/OS | Lotus Notes | SupportPac | |

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Pentium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

WebSphere Partner Gateway Enterprise および Advanced Editions には、Eclipse Project (www.eclipse.org) により開発されたソフトウェアが含まれています。

# 索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

## [ア行]



## [カ行]

## [サ行]

# [タ行]

## [ナ行]



## [ハ行]

## [マ行]



## [ヤ行]



## [ラ行]



## [ワ行]



## [数字]

## A



## B



## C



## D



## E

## F



## G



## H



## I



## J



## M



## N



## O



## P

# Q



# R

## S



## T



## U



## W



## X



## Z



## [特殊文字]

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21