IBM WebSphere Partner Gateway Enterprise Edition および Advanced Edition

E/A パートナー・ガイド

バージョン 6.1.1

IBM WebSphere Partner Gateway Enterprise Edition および Advanced Edition

E/A パートナー・ガイド

バージョン 6.1.1

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、 109 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(TM)® WebSphere(TM)® Partner Gateway Advanced Edition (5724-L68) および Enterprise Edition (5724-L69) バージョン 6.1.1、リリース 1、モディフィケーション 1、および新しいバージョン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。

IBM 発行のマニュアルに関する情報のページ

`http://www.ibm.com/jp/manuals/`

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

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： IBM WebSphere Partner Gateway Enterprise and Advanced Editions
Partner Guide
Version 6.1.1

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2008.3

目次

本書について

IBM WebSphere Partner Gateway は、企業間 (B2B) 取引コミュニティーの管理に使用される電子文書処理システムです。B2B はここ数年で大きな進歩を遂げており、さまざまなタイプの自動トランザクション (購入注文、送り状など) を時間をかけず、簡単で経済的に行うことに役立っています。

本書では、コミュニティー・パートナーを対象に、コンソールの設定と日常タスクの実行に必要な情報を詳細に説明します。

対象読者

IBM WebSphere Partner Gateway の取引コミュニティー、つまりハブ・コミュニティーは、内部パートナー、ハブ管理者、および外部パートナーから構成されます。それぞれには、さまざまなレベルの特権を持つ管理ユーザーが含まれています。また、管理ユーザーは特定のコンソール・アクセス権を持つ通常ユーザーを追加します。

表記上の規則

本書では、次のような表記上の規則を使用しています。

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、ユーザーが入力するテキスト、引数またはコマンド・オプションの値、例およびコード・サンプル、またはシステムが画面に表示する情報 (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、グラフィカル・ユーザー・インターフェース・コントロール (例えば、オンライン・ボタン名、メニュー名、またはメニュー・オプションなど)、および表やテキストの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、書籍名、新規用語および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。
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。
青のアウトラインのテキスト	(PDF ファイルのみ) テキストの周りの青のアウトラインは、相互参照を示します。アウトラインで囲まれた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、この表に記載されている「下線付きのカラー・テキスト」の規則の PDF ファイルの場合に相当します。
{INSTALL DIR}	製品のインストール先ディレクトリーを表します。

UNIX:/Windows:	このいずれかの文字で始まるパラグラフは、オペレーティング・システムによる差をリストしたメモであることを示します。
『 』 (かぎ括弧)	(PDF ファイルのみ) かぎ括弧により、本書の他のセクションへの相互参照を囲んでいます。
{ }	構文の記述行で、複数のオプションが中括弧で囲まれている場合、その中の 1 つのオプションのみを選択することが必要です。
[ ]	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。
...	構文の記述行の場合、省略符号 ... は直前のパラメーターが繰り返されることを示します。例えば、`option[,...]` は、複数のオプションをコンマで区切って指定できることを意味します。
< >	名前の変数要素は、不等号括弧で囲んで他の要素と区別しています。例えば、<*server_name*><*connector_name*>tmp.log のように表記されています。
\, /	円記号 (¥) は、Windows インストールでのディレクトリー・パスの中で、コンポーネントの分離文字として使用しています。UNIX をインストールしている場合は、スラッシュ (/) をバックスラッシュで置換します。

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。

文書は、次のサイトでダウンロードするか、オンライン上で直接読むことができます。

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

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。これらの情報は、WebSphere Partner Gateway Support 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。

このリリースの新機能

このセクションでは、 IBM WebSphere Partner Gateway の新規のフィーチャーを説明します。

リリース 6.1.1 の新機能

WebSphere Partner Gateway 6.1.1 は、以下の新機能をサポートします。

- 以前のリリースでは、基本認証サポートは Web サービスのメッセージに対してのみ有効でした。この機能はすべてのプロトコルに拡張されました。基本認証には、セキュア HTTP 接続を使用 (つまり HTTP の代わりに HTTPS を使用) することをお勧めします。
- 符号化と暗号化を除き、圧縮と解凍のサポートが RNIF メッセージに提供されます。
- SOAP 本体と SOAP エンベロープを検証するサポートが提供されます。さらに SOAP エンベロープ解除も可能です。
- すべての HTTP レシーバーに関して最大同期タイムアウトと最大同期接続をローカル側で制御できます。
- FTP サーバーは WebSphere Partner Gateway と統合され、AS3 プロトコル、FTP Scripting Destination、FTP Scripting レシーバー、および FTP / FTPS の受信局と宛先をサポートします。
- エラー文書は、開始パートナー、受信パートナー、または両方に送信できます。エラー文書フローは、WebSphere Partner Gateway コンソールで構成でき、WebSphere Partner Gateway 形式または Web サービス形式のいずれかで送信できます。
- アーカイバーのパフォーマンスが改善されました。
- 複数の社内パートナーにサポートが提供されます。
- 同時に複数のインバウンド文書またはアウトバウンド文書を再送できます。
- FIPS モードのサポートが提供されます。製品を FIPS モードまたはデフォルト・モードで稼働するように構成できます。
- 宛先、検証マップ、文書定義、対話、およびユーザーに関して、削除機能と使用場所機能が提供されます。
- AS2、および AS3 の文書に関して、大容量ファイル圧縮サポートが提供されます。
- 暗号化と署名にサポートが提供されます。
- マイグレーションの際に構成タイプに依存するものには、イベント・コードとアラート通知も含まれます。また、アラート可能イベントのインポート / エクスポートの定義のサポートを提供するため、パートナー・マイグレーション機能が拡張されました。
- 複数の証明書をアップロードするサポートが提供されます。証明書のアップロードと構成を行う新規ウィザードがコンソールに含まれます。

- この製品は現在、AIX 6.1、RHEL 5 (32 ビットと 64 ビット)、SLES 10 (64 ビット)、および Windows Server 2003 (64 ビット) をサポートします。

リリース 6.1 の新機能

WebSphere Partner Gateway V6.1 は、次の新機能をサポートします。

- 新規ビジネス・プロトコル: AS3、添付ファイルによる SOAP、CIDX、および ebXML メッセージ・サービス (ebMS) 2.0 サポート
- カスタム XML 文書サポートの向上 (構成の向上、XPath 式のフル・サポート、検索フィールドのサポート、ユーザー定義属性のサポート、同期サポートなど)
- 新しい IPv6 のサポートおよび AS3 をサポートするための拡張 FTP スクリプト記述
- 文書定義属性の再編成
- ユーザー出口と併用するための新しい文書定義属性
- 文書タイプ別および取引先レベル別の構成可能な否認防止
- 文書ビューアーに対するユーザー定義検索フィールドの増設
- MDN 戻り状況に基づく AS ビューアー・サポートの向上
- EDI 構成ウィザードおよび EIF インポート・ウィザード (以前は GA02 サポート・パックに同梱)
- すべての関係者 (ソース・パートナーおよびターゲット・パートナーまたはすべてのサブスクライブ済み連絡先) に通知を送信するための新しいアラート通知モード。これにより、アラート構成作業が削減されます。
- hubadmin 管理者以外のユーザーに対する再送信許可およびゲートウェイ許可の利用可能化
- 複数のユーザーをハブ管理者にすることができる新しいユーザー・グループ
- ログオン認証での LDAP サポート
- WebSphere Application Server ロギングの使用および WebSphere Partner Gateway コンポーネントのトレースの使用
- WebSphere Partner Gateway コンソールによるプロパティー・ファイル構成データの集中的な設置および一元管理
- WebSphere MQ は前提条件製品ではなくなりました。社内の通信には、WebSphere Platform Messaging サポートが使用されるようになりました。
- パートナーまたは文書タイプ (あるいはその両方) を基にした選択アーカイブ
- ある WebSphere Partner Gateway インスタンスから別のインスタンスに定義をエクスポートおよびインポートすることによる WebSphere Partner Gateway 構成のマイグレーション
- 簡略化された単一マシン (簡易モード) インストール・オプション
- 複数マシンのデプロイメントに WebSphere Application Server Network Deployment が使用されるようになったことによるクラスター化およびインフラストラクチャーの一元管理化
- WebSphere Process Server バージョン 6.1 をバックエンド統合システムとして使用するためのサポート

注:

1. XML ベースの管理 API は、バージョン 6.1 では推奨されません。
2. WebSphere Partner Gateway バージョン 6.1 は、RC5 アルゴリズムをサポートしません。

第 1 章 概要

ハブ・コミュニティー

IBM WebSphere Partner Gateway のハブ・コミュニティーは、ビジネス文書のリアルタイム交換用に中央のハブに接続された 3 つのエンティティー、つまりハブ管理者、内部パートナー、および外部パートナーから構成されます。

ハブ管理者

ハブ管理者とは、ハブ・コミュニティーの日常的な運用の管理を担当する会社です。ハブ管理者は、1 日 24 時間 週 7 日、ハブ・コミュニティーのハードウェアとソフトウェアのインフラストラクチャーを保守します。次のような作業を担当しています。

- トラブルシューティングと修復。
- すべての外部パートナーにハブ・コミュニティーが正しく構成されていることを確認する。
- ハブ・コミュニティーへの新しい外部パートナーの構成を援助する。
- ハブ・コミュニティーをできるだけ効率的に運用するため、将来の成長に向けた戦略的計画を立てる。

ハブ管理者の役割は、ハブ・コミュニティー内のサード・パーティーの会社に外部委託できます。また、 WebSphere Partner Gateway を購入した内部パートナーがハブ管理者の機能を実行することもできます。

内部パートナー

内部パートナーとは、ハブ・コミュニティー内で主要な役割を果たす会社です。この会社は、外部パートナーとの間で行われる電子ビジネス・プロセスの定義を含め、ハブ・コミュニティーの購入と構築を担当します。

内部パートナーはハブ管理者になることもできます。

外部パートナー

外部パートナーとは、ハブ・コミュニティー経由で内部パートナーとビジネスを行う会社です。外部パートナーがハブ・コミュニティーに接続するには、構成プロセスを完了する必要があります。接続すると、外部パートナーは内部パートナーと電子ビジネス文書を交換できます。

コミュニティー・コンソールのアイコン

次の表に示すアイコンは、WebSphere Partner Gateway コミュニティー・コンソールに固有のものです。

表 1. コミュニティー・コンソールのアイコン

アイコン	アイコン名
	縮小
	コピー
	役割を作成。役割はアクティブではありません
	データあり
	活動化
	削除
	ロー文書を表示
	進行中の文書
	文書処理に失敗
	文書処理に成功
	マップのダウンロード
	編集
	属性値の編集
	編集オフ
	RosettaNet 属性値の編集
	展開
	情報のエクスポート
	レポートのエクスポート
	宛先無効
	検索条件を非表示
	変更
	格納データなし
	カレンダーを開く

表 1. コミュニティー・コンソールのアイコン (続き)

アイコン	アイコン名
	文書の順序付けの有効化/無効化
	一時停止
	印刷
	必要入力
	開始
	処理の停止。文書の処理は進行中であるため、文書の処理を停止するようサーバーに要求するユーザー・オプションです。
	同期データ・フロー。非同期のトランザクションの場合、アイコンは表示されません。
	マップのアップロード
	詳細の表示
	文書定義の属性セットアップの表示
	ヘルプ・システムの表示
	メンバーの表示
	元文書の表示
	アクセス権の表示
	グループのメンバーシップの表示
	検証エラーの表示
	使用箇所

コミュニティー・コンソールの使用

WebSphere Partner Gateway を構成した後は、イベント・ビューアーと文書分析の 2 つのコンソール・ツールを定期的に使用します。

イベントを検索する場合、ビューアー・モジュールのイベント・ビューアーを使用します。大半の文書は何度も再送されるため、文書に障害が発生してアラートが生成された場合、このアラートは、それ以降同様な障害が発生しないよう調査して修正する必要があるという意味になります。

特定のイベントを検索して、そのイベントの発生原因を調査できます。イベント・ビューアーを使用すると、時刻、日付、イベント・タイプ、イベント名、およびイ

ベント・ロケーションごとにイベントを検索できます。ハブ管理者は、パートナー、ソース IP、およびイベント IP ごとに検索することもできます。

注: すべてのユーザーがデバッグ・イベントへのアクセス権を所有しているわけではありません。

イベント・ビューアーで生成されるデータは、イベントおよびイベントを作成した文書の確認に役立ちます。ロー文書も表示できます。これにより、フィールド、値、およびエラーの理由を確認できます。

2 番目によく使用されるツールは、ツール・モジュールの機能である文書分析です。文書分析を使用して、受信した文書数、処理が進行中の文書数、および処理が完了した文書のうちで失敗した数と成功した数を確認します。このツールを使用すると、処理が失敗した理由がわからなかった特定の文書を詳しく調べることができます。

コンソールのアカウント管理モジュールは、主に WebSphere Partner Gateway のセットアップとその後の保守で使用されます。

第 2 章 WebSphere Partner Gateway 環境のセットアップ

ここでは、外部パートナーのユーザーおよび環境に合うように WebSphere Partner Gateway の準備をするときに、外部パートナーが実行する必要のあるタスクについて説明します。

会社用に WebSphere Partner Gateway を構成するには、下記の順序でコミュニティー・コンソールから次の操作を実行する必要があります。

1. 『コミュニティー・コンソールへのログイン』
2. 6 ページの『パートナー・プロファイルの検査』
3. 7 ページの『宛先の作成』
4. 7 ページの『B2B 機能について』
5. 9 ページの『デジタル証明書のアップロード』
6. 30 ページの『コンソール・グループの作成』
7. 31 ページの『ユーザーの作成』
8. 32 ページの『FTP ユーザーの構成』
9. 33 ページの『連絡先情報の作成』
10. 34 ページの『アラートの作成と連絡先の追加』
11. 41 ページの『新規住所の作成』

コミュニティー・コンソールへのログイン

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 に個人情報は保管されません。また、Cookie はブラウザーを閉じ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 (非セキュア)

   https://<*hostname*>.<*domain*>:58443/console (セキュア)

   <*hostname*> と <*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と場所を示します。

   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. 「**保管**」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。

パートナー・プロファイルの検査

アカウント管理のパートナー機能を使用すると、会社をシステムに識別させる情報を表示し、編集できます。

パートナーは、会社ログイン名を除いて、自分のプロファイルの属性をすべて編集できます。「パートナー」は、「ビジネス ID」、すべての「ビジネス ID」に関連した「E メール ID」、および「IP アドレス」の追加と除去もできます。 IP アドレスまたはホスト名は、「実動」、「テスト」、「CPS マネージャー」、および「CPS パートナー」の動作モードに対して入力できます。

この機能には、すべてのユーザー・パスワードをリセットするオプションも含まれています。ユーザー・パスワードが漏えいした場合、この機能の使用が必要になることがあります。

パートナー・プロファイルの表示と編集

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. 「ユーザー・プロファイル」アイコンをクリックして編集します。「パートナーの詳細」画面が表示されます。
3. 必要に応じてプロファイルを編集します (一部の値は編集できません)。値の説明については、7 ページの表 2 を参照してください。

表 2. パートナー画面の値

値	説明
会社ログイン名	パートナーをシステムに示します。最大 15 文字です。特殊文字 , . ! # ; : ¥ / & ? は使用できません。パートナーはこの値を編集できません。
パートナー表示名	パートナーとしてハブ・コミュニティーに表示する名前。最大 30 文字です。
パートナー・タイプ	パートナー・タイプ - 外部パートナーまたは内部パートナー。パートナーは、プロパティー bcg.allow.partner.type.edit が「真」に設定されている場合にのみこの値を編集できます。デフォルトでは、この値は「偽」に設定されています。
状況	「使用可能」または「使用不可」です。使用不可にした場合、検索条件とドロップダウン・リストにパートナーは表示されません。
ベンダー・タイプ	契約製造メーカー、ディストリビューターなど、パートナーの役割を示します。
Web サイト	パートナーの Web サイトを示します。
ビジネス ID	システムが経路指定に使用する DUNS、DUNS+4、または Freeform の番号。ビジネス ID 番号を追加できます。 • DUNS 番号は 9 桁にする必要があります。 • DUNS+4 番号は 13 桁にする必要があります。 • Freeform ID 番号では 60 個までの英数字と特殊文字を使用できます。 **注:** EDI ビジネス ID は、EDI 文書で使用される任意の修飾子によってプレフィックスを付ける必要があります。書式は、EDI 修飾子の後に「-」および ID を続けた形です。例えば、DUNS を使用する EDI X12 は、01-123456789 のようになります。
E メール ID	各ビジネス ID の有効な E メール ID。各ビジネス ID に E メール ID を追加できます。ビジネス ID が存在しない場合、このフィールドは表示されません。
IP アドレスまたはホスト名	• 動作モード。例えば、CPS パートナー。 • パートナーの IP アドレスまたはホスト名。

4. 「**保管**」をクリックします。

宛先の作成

デフォルト宛先を作成し、保守する必要があります。さもないと、接続を作成できません。宛先の作成方法の詳細については、43 ページの『第 3 章 宛先の作成』を参照してください。

B2B 機能について

注: 小規模なインストール先では、このプロセスはハブ管理者によって実行されることがあります。

この機能を使用すると、ハブ全体の定義済み B2B 機能の表示と編集を行い、必要に応じてさらにローカル B2B 機能を使用可能に設定できます。

B2B 機能は、コミュニティー・メンバー間で交換できる特定タイプのビジネス・プロセスを示します。B2B 機能または文書処理機能は、文書タイプの定義を使用して定義されます。文書タイプの定義によって、コミュニティー・メンバー間での文書の受信、処理、および経路指定に必要なすべての情報がシステムに指定されます。

各機能は、最大 5 つの異なる文書タイプの定義から構成されます。

パッケージ。インターネット経由の文書伝送に使用される文書パッケージ化フォーマットを示す。例えば、RNIF、AS1、AS2 および AS3。

プロトコル。文書内の情報の構造と場所を識別します。システムが文書を処理し、経路を定めるには、この情報が必要です。

文書タイプ。内部パートナーとその外部パートナー間で処理されるビジネス・プロセスを示します。

アクティビティー。プロセスが行うビジネス機能。

アクション。1 つの完全なビジネス・プロセスを構成する個々の文書。文書は内部パートナーと外部パートナーの間で処理されます。

各文書タイプの定義には、定義の機能を定義する属性 (つまり、情報) が含まれています。属性は特定の文書タイプに関連付けられた情報です。システムでは、文書の検証、暗号化の検査など、さまざまな機能にこの情報を使用します。

B2B 機能の確認と編集

1. 「**アカウント管理**」 >「**プロファイル**」 > 「**B2B 機能**」をクリックします。「B2B 機能」画面が表示されます。
   - フォルダーがパッケージの横に表示され、「使用可能」列に「使用可能」が表示されている場合、ハブ管理者がこの機能を使用可能に設定している。
   - 「ソースの設定」または「ターゲットの設定」の下にチェック・マークがある場合、その役割で (つまり、ソースとして、ターゲットとして、またはその両方で) この機能が使用できることを示す。
   - 「ソースの設定」または「ターゲットの設定」の下にある「ロールの作成」アイコンは、その役割 (つまり、ソースとして、ターゲットとして、またはその両方) でこの機能が使用できないことを示す。
   - 「使用可能」列には、パッケージの状況が「使用可能」または「使用不可」として表示される。

   注: この機能を使用可能にするには、ターゲット、ソース、またはその両方の機能を設定する必要があります。
2. 文書タイプのコンテキストの開始 (「**ソースの設定**」)、受信 (「**ターゲットの設定**」)、つまり開始と受信を行う機能を設定します。双方向 PIP では、要求を出すパートナーと、対応する確認を行うパートナーが異なる場合でも、すべてのアクションに関して「ソースの設定」と「ターゲットの設定」は同一です。
3. 下位レベルの各文書タイプの定義について、開始 (「**ソースの設定**」)、受信 (「**ターゲットの設定**」)、または開始と受信を行う機能を設定する。
4. 「編集」アイコンをクリックして表示し、必要であれば下位レベルの文書タイプの定義 (例えば、「プロトコル」や「文書タイプ」など) を変更します。また、

文書タイプの定義の属性 (「実行のための時間」、「再試行カウント」など) を変更することもできます。この画面をはじめて使用する場合、属性はグローバル・レベルで設定されています。しかし、必要に応じて属性をローカル・レベルで再設定できます。ローカル・レベルで属性を設定すると、ユーザーの環境のグローバル設定はオーバーライドされますが、グローバル設定自体は変更されません。

- どのレベルで変更を行った場合でも、変更は下位のすべてのレベルに反映される。
- 必要に応じて、パッケージの下の個々のフォルダーを選択し、編集できる。このように行った変更は下位レベルには反映されません。
- 組み込みの「全選択」オプションは、下位レベルで選択解除することでオーバーライドできる。
- 受取確認通知などのシグナルは、RosettaNet に固有のものである。各アクションの下には、受取確認通知、一般例外、および受取確認通知例外という 3 つのシグナルがあります。シグナルの属性を設定できます。
- 否認防止が必要
- AS ビジネス ID

属性を変更した場合は、「**保管**」をクリックします。

デジタル証明書のアップロード

デジタル証明書とは、運転免許証やパスポートと同様の、オンラインの身分証明書のことです。デジタル証明書を使用して、個人または組織を識別することができます。

デジタル署名とは、公開鍵暗号方式を使用した電子文書に基づいた計算のことです。この処理によって、デジタル署名は署名される文書および署名者と結合されるため、複製することはできません。連邦政府のデジタル署名法案が通過したことにより、デジタル署名のある電子取引には、手書きで署名された取り引きと同等の法的効力があります。

WebSphere Partner Gateway はデジタル証明書を使用して、内部パートナーと外部パートナー間で行われるビジネス文書トランザクションが信頼できるものであるかどうかを検証します。また、暗号化と暗号化解除にも使用されます。

アウトバウンド文書の 1 次証明書と 2 次証明書を指定して、文書交換が中断されないようにすることができます。1 次証明書はすべてのトランザクションで使用します。2 次証明書は、1 次証明書が期限切れになったり失効したりした場合に使用します。

デジタル証明書は、構成処理時にアップロードされ、識別されます。

証明書の有効期限が切れていたり失効していたりすると、証明書は使用不可になり、コンソールにその状態が反映されます。1 次証明書が期限切れになったり失効したりすると、使用不可になり、2 次証明書が 1 次証明書として設定されます。証明書が期限切れになったり失効したりすると、イベントが生成されます。

選択した証明書タイプを基にした「証明書の使用」オプションを使用できます。ハブ・オペレーター・プロファイルでは、デジタル署名または SSL クライアント証明書に対して「証明書の使用」を設定できます。パートナー・プロファイルでは、暗号化証明書に対して「証明書の使用」を設定できます。例えばハブ・オペレーター・プロファイル内でのデジタル署名と暗号化のように、同じ証明書が異なる目的で使用されることになっている場合は、デジタル署名のために 1 度、暗号化証明書のために 1 度の、合わせて 2 度ロードする必要があります。ただし、証明書がデジタル署名と SSL クライアントに使用される場合は、同一の証明書項目内で対応するチェック・ボックスを設定できます。

このような証明書は、デジタル署名のために 1 度、SSL クライアントのために 1 度の、合わせて 2 度ロードすることもできます。その場合、2 次証明書用に、同一のパターンがロードされる必要があります。例えば、1 次証明書が、デジタル署名用と SSL クライアント用の異なる証明書としてロードされた場合、2 次証明書も (同一の証明書であっても) 異なる証明書項目としてロードする必要があります。

完全な certpath を構築して検証するには、証明書チェーン内の証明書すべてをアップロードする必要があります。例えば、証明書チェーンに A -> B -> C -> D (A -> B は、A が B の発行者という意味) という証明書がある場合は、証明書 A、B、および C はルート証明書としてアップロードしてください。証明書の 1 つが使用不可の場合は、certpath が構築されず、トランザクションは正常に行われません。CA 証明書は、認証局が保持する証明書リポジトリーから取得するか、証明書を供給したパートナーから取得することができます。ルート証明書および中間証明書は、ハブ・オペレーター・プロファイルでのみアップロードできます。

注: 以下のセクションの手順を実行する場合は、先に証明書をシステムにロードしておく必要があります。証明書のロードの詳細については、「*ハブ構成ガイド*」を参照してください。

証明書の有効期限がもうすぐ切れることを通知する証明書有効期限アラートを作成できます。詳しくは、34 ページの『アラートの作成と連絡先の追加』を参照してください。有効期限が切れた証明書は IBM WebSphere Partner Gateway データベースに保管されます。システムから削除することはできません。

証明書の用語

認証局 (CA)。メッセージ暗号化用のセキュリティー信任状と公開鍵を発行し、管理する機関。個人または会社がデジタル証明書を要求すると、CA は登録局 (RA) に確認し、個人または会社から提出された情報を検査します。RA が処理依頼された情報を検証すると、CA は証明書を発行します。

CA には、VeriSign、Thawte などがあります。

デジタル証明書。デジタル証明書は、電子版の ID カードです。インターネットを介して B2B トランザクションを行うとき、デジタル証明書はユーザーの身元を保証します。デジタル証明書は認証局 (CA) から取得され、次の 3 つの部分から構成されます。

- 公開鍵と秘密鍵のペアの公開鍵部分。
- ユーザーを識別する情報。
- 証明書の妥当性を証明する信頼された機関 (CA) のデジタル署名。

デジタル署名。秘密鍵で作成されたデジタル・コード。デジタル署名により、ハブ・コミュニティーのメンバーは、シグニチャーを検証して伝送を認証できます。ファイルに署名すると、ファイルの内容と秘密鍵に固有のデジタル・コードが作成されます。シグニチャーの検証には公開鍵が使用されます。

暗号化。情報を加工し、意図された受信者以外には読めないようにする方法。受信者は読むために、情報の暗号化を解除する必要があります。

暗号化解除。暗号化された情報の加工を解除し、もう一度読めるようにする方法。暗号化解除には受信者の秘密鍵が使用されます。

鍵。ファイルの暗号化、署名、暗号化解除、および検証に使用されるデジタル・コード。鍵は秘密鍵と公開鍵の鍵ペアで使用されます。

否認防止。以前の関与またはアクションが否認されないようにすること。B2B 電子トランザクションでは、デジタル署名を使用して送信側を検証し、トランザクションのタイム・スタンプを設定します。否認防止により、関係者はトランザクションが許可されていない、または無効であると主張できないようになります。

秘密鍵。鍵ペアの秘密部分。この鍵は情報の署名と暗号化解除に使用されます。ユーザーの秘密鍵にはユーザーしかアクセスできません。文書の内容に基づく固有のデジタル署名生成にも、秘密鍵が使用されます。

公開鍵。鍵ペアの公開部分。この鍵は情報の暗号化とシグニチャーの検証に使用されます。公開鍵はハブ・コミュニティーのほかのメンバーに配布できます。他人の公開鍵を知っても、対応する秘密鍵を見つけることはできません。

自己署名鍵。所有権を証明するため、対応する秘密鍵で署名された公開鍵。

X.509 証明書。通信ネットワーク上で身元と公開鍵の所有権の証明に使用されるデジタル証明書。証明書には、発行者の名前 (つまり、CA)、ユーザーの識別情報、および発行者のデジタル署名が入っています。

証明書は組織、および証明書が有効である期間を識別します。

証明書のタイプとサポートされているフォーマット

すべての証明書は DER フォーマットまたは ASCII Privacy Enhanced Mail (PEM) フォーマットにする必要があります。証明書は、一方のフォーマットから他方のフォーマットに変換できます。

証明書にはいくつかのタイプがあります。

- **SSL クライアント証明書 (外部パートナーと内部パートナー)**。トランスポート証明書の 1 つ。アウトバウンド・トランスポートが HTTPS である場合、SSL クライアント証明書が必要です。ほとんどの場合、SSL クライアント証明書には CA の署名が必要です。証明書をテスト環境で使用する場合は、自己署名できます。

  コンソールを使用して WebSphere Partner Gateway に証明書をアップロードし、ハブ・オペレーターに証明書のコピーを送信する必要があります。

- **SSL サーバー証明書。**SSL サーバー認証を使用可能にします。CA の SSL サーバー証明書をパートナー間で交換する必要があります。
- **暗号化証明書 (外部パートナーと内部パートナー)。**ハブ・コミュニティー・メンバーがファイルを暗号化した場合は、暗号化証明書の公開鍵部分をハブ・コミュニティー・メンバーに送信する必要があります。それに対応する暗号化証明書の秘密鍵部分は、コンソールを使用してハブ・オペレーター・レベルにアップロードする必要があります。パートナーの証明書の公開部分はコンソールを使用して WebSphere Partner Gateway にアップロードし、証明書のコピーはハブ・オペレーターに送信する必要があります。
- **デジタル署名証明書 (外部パートナーと内部パートナー)。**ハブ・コミュニティー・メンバーが文書に署名した場合、署名された証明書の公開部分は、署名証明書としてパートナー・レベルでハブにアップロードする必要があります。ハブ・コミュニティー・メンバーに送信する文書にハブ・マネージャーが署名する必要がある場合は、ハブ・マネージャーの証明書の公開部分をハブ・コミュニティー・メンバーに送信する必要があります。ハブの署名証明書は、ハブ・オペレーターのコンソールを使用してアップロードする必要があります。
- **VTP 証明書 (内部パートナー)。**この証明書は、WebSphere Partner Gateway の文書マネージャーが外部パートナーのシミュレーター機能に使用します。この証明書はコンソールを使用してアップロードするのではなく、ファイル・システムにコピーされます。

  ファイル・システムにコピーされた VTP 証明書は、コンソールから作成されたすべてのパートナーに対してアクティブです。これらを使用して、外部パートナーのシミュレーターから受け取った署名済み文書の妥当性検査を行います。また、ファイル・システムにコピーされた証明書はコンソールでは表示できません。

SSL サーバーとクライアントの認証

クライアント認証が必要とされないのは、次の場合です。

- ハブ・コミュニティーの Web サーバーの証明書が自己署名証明書である場合、パートナーはその証明書のコピーを所有している必要がある。
- ハブ・コミュニティーの Web サーバーの証明書が認証局から発行された場合、パートナーは CA ルートおよび中間証明書のコピーを所有している必要がある。

クライアント認証が必要とされるのは、次の場合です。

- ハブ・コミュニティーの Web サーバーの証明書が自己署名証明書である場合、パートナーはその証明書のコピーを所有している必要がある。
- ハブ・コミュニティーの Web サーバーの証明書が認証局から発行された場合、パートナーは CA ルートおよび中間証明書のコピーを所有している必要がある。
- パートナーの証明書が自己署名され、トラスト鍵ストアにロードされた場合、ターゲット・サーバーはその証明書のコピーを所有している必要がある。
- 証明書が CA から認証され、トラスト鍵ストアにロードされた場合、ターゲット・サーバーは認証局証明書のコピーを所有している必要がある。

注: 前のバージョンの WebSphere Partner Gateway は、IPv6 アドレス・フォーマットをサポートしませんでした。WebSphere Partner Gateway 6.1 は、このフォーマットをサポートしています。ご使用のサーバーの少なくとも 1 つが、IPv6 ア

ドレス・フォーマットをサポートするように構成されていることを確認してください。IPv6 フォーマット構成は、そのサーバーでのみ必要とされます。

インバウンド SSL 証明書の構成

このセクションでは、パートナーからのインバウンド接続要求のサーバー認証およびクライアント認証の構成の方法について説明します。

インバウンド要求はパートナーが文書を WebSphere Partner Gateway に送信しているとき出されます。ユーザーのコミュニティーが SSL を使用していない場合、インバウンド SSL 証明書またはアウトバウンド SSL 証明書は必要ではありません。

注: インバウンド FTPS の場合、WebSphere Partner Gateway は顧客により提供される FTP サーバー使用し、すべてのインバウンド SSL 構成は顧客が使用している特定の FTP サーバー製品毎です。

ステップ 1: SSL 証明書の入手: WebSphere Application Server は、SSL を介してパートナーから接続要求を受信したとき、SSL 証明書を使用します。それはレシーバーがハブを識別するために、パートナーに提示する証明書です。このサーバー証明書は自己署名、または CA による署名が可能です。ほとんどの場合、セキュリティーを強化するため、CA 証明書を使用します。自己署名証明書はテスト環境で使用される場合があります。証明書および鍵ペアを生成するため、iKeyman または WebSphere Application Server 管理コンソールを使用してください。iKeyman または WebSphere Application Server 管理コンソールの使用について詳しくは、IBM から入手可能な資料を参照してください。

証明書と鍵ペアを生成した後、すべてのパートナーに対するインバウンド SSL トラフィック用の証明書を使用してください。ユーザーが複数のレシーバーまたはコンソールを持つ場合、これに伴う鍵ストアを各インスタンスにコピーしてください。証明書が WebSphere Application Server 管理コンソールを使用して生成された場合、鍵および証明書は WebSphere Application Server 管理コンソールを使用して、別のサーバー内の別の鍵ストアにインポートできます。証明書が自己署名である場合、この証明書をパートナーに提供してください。この証明書を入手するには、公開証明書をファイルに抽出するため、iKeyman を使用してください。

自己署名証明書の生成: 自己署名のサーバー証明書を使用しようとしている場合、次の手順を実行します。

1. /<*WAS_Installation_dir*>/bin に配置されている iKeyman ユーティリティーを開始します。これが iKeyman の初めての使用である場合、鍵ストアにある「ダミー」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鍵ストアを開き、iKeyman を使用して自己署名証明書およびレシーバーまたはコンソール鍵ストア用の鍵ペアを生成します。
3. iKeyman を使用してファイルをユーザーの公開鍵を組み込む証明書に抽出します。

   鍵ストアを JKS、PKCS12、または JCEKS ファイルに保存します。

4. 証明書をユーザーのパートナーに配布します。配布の好ましい方法は、証明書をパスワードで保護された zip ファイルで E メールで送信することです。ユーザーのパートナーは、ユーザーをコールし、 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、SSL 構成およびレシーバーとコンソール用の設定内に新規の証明書を設定してください。これは、各ノード用構成またはサーバー用構成内の鍵ストア内の新規証明書の別名を選択して行うことができます。

CA 生成の証明書の入手: CA により署名された証明書を使用しようとしている場合、次の手順を実行してください。

1. /<*WAS_Installation_dir*>/bin ディレクトリーに配置されている iKeyman ユーティリティーを開始します。
2. iKeyman を使用してレシーバーの証明書要求と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 から署名された証明書を受信したとき、iKeyman を使用して鍵ストアに署名された証明書を置きます。
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、SSL 構成およびレシーバーとコンソール用の設定内に新規の証明書を設定してください。これは、各ノード用構成またはサーバー用構成内の鍵ストア内の新規証明書の別名を選択して行うことができます。

   注: 以前のステップを実行するために、WebSphere Application Server 管理コンソールを使用することもできます。

ステップ 2: クライアントの認証: 文書を送信したパートナーを認証したい場合、このセクションのステップを実行します。

クライアントの証明書のインストール: クライアント認証の場合は、次の手順に従います。

1. パートナーの証明書を入手します。
2. 証明書が自己署名である場合、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証明書をインストールします。
3. 証明書が CA 発行である場合、iKeyman または WebSphere Application Server 管理コンソールを使用して関連した CA 証明書を関連したトラストストアに追加します。

注: ユーザーのハブ・コミュニティーにさらにパートナーを追加するとき、それらの証明書をトラストストアに追加するため、ユーザーは iKeyman または WebSphere Application Server 管理コンソールを使用できます。パートナーがコミュニティーから離れる場合、トラストストアからパートナーの証明書を除去するためユーザーは iKeyman または WebSphere Application Server 管理コンソールを使用できます。

クライアント認証の設定: 証明書 (複数可) をインストールした後、ユーティリティー・スクリプト bcgClientAuth.jacl の実行により、クライアント認証を使用するため WebSphere Application Server を構成します。

1. 次のディレクトリーにナビゲートします。 */<ProductDir>*/bin
2. クライアント認証をオンにするため、次のスクリプトをコールします。

```
./bcgwsadmin.sh -f /<ProductDir>/scripts/bcgClientAuth.jacl
   -conntype NONE set
```

注: クライアント認証をオフにするため、次のスクリプトをコールします。

```
./bcgwsadmin.sh -f /<ProductDir>/receiver/scripts/bcgClientAuth.jacl
  -conntype NONE clear
```

これらの変更を有効にするため、bcgreceiver サーバーを再始動する必要があります。クライアント認証は、WebSphere Application Server 管理コンソールを使用して使用可能にすることもできます。値「サポート (Supported)」は、サーバーがクライアント証明書を要求しますが、しかし、クライアント認証が使用不可である場合、SSL ハンドシェークはまだ確立されるかもしれません。値「必要」は、クライアントの証明書を送信する必要があることを意味します。そうでなければ、ハンドシェークは失敗します。

クライアントの証明書の妥当性検査: SSL クライアント認証で使用できる追加機能があります。この機能はコミュニティー・コンソールを介して使用可能です。HTTPS の場合、WebSphere Partner Gateway はインバウンド文書内のビジネス ID に対して証明書をチェックします。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、クライアントの証明書をインポートし、次にそれを SSL としてフラグを立てます。

1. クライアントの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、そ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、証明書を保管したディレクトリーにナビゲートします。
   e. 「**SSL クライアント**」を証明書のタイプとして選択します。
   f. 証明書の記述 (必須) をタイプします。
   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したい場合、リストから選択します。
   i. 「**終了**」をクリックします。
2. クライアントの宛先を更新します。
   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、そ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. 以前作成した HTTPS 宛先を選択します。HTTPS 宛先をまだ作成していない場合、45 ページの『HTTPS 宛先の設定』を参照してください。
   d. 「**編集**」アイコンをクリックして宛先を編集します。
   e. 「**SSL クライアント証明書の検証 (Validate SSL Client Certificate)**」用に「**はい**」を選択します。
   f. 「**保管**」をクリックします。

レシーバーおよびコンソール用の別個の鍵ストアおよびトラストストアの構成: デフォルトで、WebSphere Partner Gateway バージョン 6.1 はレシーバーおよびコンソール用に共通の鍵ストアおよびトラストストアを使用します。しかし、配布モードをインストールした環境で、レシーバーおよびコンソール用の別個の鍵ストアおよびトラストストアを構成できます。

鍵ストアおよびトラストストアを構成するには、レシーバーおよびコンソール用の別個の鍵ストアおよびトラストストアを作成し、設定します。また、別個の SSL 構成を作成します。 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できます。クラスター内のすべてのサーバーに適用でき、各サーバーを別個に構成する必要がないので、クラスター・レベルでの SSL 構成の設定はより容易です。

クラスター・レベルでの SSL 構成の設定: クラスター・レベルで新規鍵ストアおよびトラストストアで SSL 構成を設定しているとき、サーバー・レベルで SSL 構成をしてはなりません。サーバー・レベルで SSL 構成セットが存在する場合、クラスター・レベルの SSL 構成は使用されません。その代わりサーバー用の 1 つのセットが使用されます。

bcgconsoleCluster 用 SSL 構成を設定するためこれらのステップを実行します。

1. コンソール・クラスター用の鍵ストアを作成します。鍵ストアは、「**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**」にナビゲートすることにより、bcgconsole クラスター・スコープ内に作成する必要があります。
2. コンソール・クラスター用のトラストストアを作成します。トラストストアは、「**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**」にナビゲートすることにより、bcgconsole クラスター・スコープ内に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**」にナビゲートすることにより、コンソール・クラスター・スコープのコンソール・クラスター用 SSL 構成を作成します。以前のステップで作成された鍵ストアおよびトラストストアを設定します。「**証明書の別名の取得 (Get certificate aliases)**」をクリックすることにより、証明書の別名リスト内の証明書の別名を更新し、サーバー認証用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. 継承された SSL 構成の指定変更により、bcgconsoleCluster 内のこの SSL 構成を設定します。「**証明書の別名の更新 (Update the certificate aliases)**」をクリックすることにより、証明書の別名を更新し、サーバー認証用に使用される別名を設定します。
5. bcgconsoleCluster を再始動します。

bcgreceiverCluster 用 SSL 構成を設定するためこれらのステップを実行します。

1. レシーバー・クラスター用の鍵ストアを作成します。鍵ストアは、「**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**」にナビゲートすることにより、bcgreceiver クラスター・スコープ内に作成する必要があります。

2. レシーバー・クラスター用のトラストストアを作成します。トラストストアは、**「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」**にナビゲートすることにより、bcgconsole クラスター・スコープ内に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」**にナビゲートすることにより、レシーバー・クラスター・スコープのレシーバー・クラスター用 SSL 構成を作成し、以前のステップで作成された鍵ストアおよびトラストストアを設定します。**「証明書の別名の取得 (Get certificate aliases)」**をクリックすることにより証明書の別名を取得し、サーバー認証用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. 継承された SSL 構成の指定変更により、bcgreceiverCluster 内のこの SSL 構成を設定します。**「証明書の別名の更新 (Update the certificate aliases)」**をクリックすることにより、証明書の別名を更新し、サーバー認証用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との連携について詳しくは、セクション「*Securing applications and their environment of WebSphere Application Server Documentation.*」を参照してください。

注:

配布モードでの NodeDefaultSSLSetting 内の NodeDefaultTrustStore の設定: 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。しかし、共通鍵ストアおよびトラストストアをレシーバーおよびコンソールに対して使用する場合、これは完全配布モードに対しても適用されます。セル内でノードが連合される場合、そのノードからの署名者証明書は CellDefaultTrustStore に追加されます。デフォルトで、NodeDefaultSSLSetting は CellDefaultTrustStore をトラストストアとして参照します。 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の使用は望ましくない場合があります。WebSphere Partner Gateway がインストールされているノード用の専用トラストストアを使用するために、NodeDefaultTrustStore を NodeDefaultSSLSettings に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 証明書と鍵管理 (SSL certificate and key management)」 > 「エンドポイント・セキュリティー構成 (Manage endpoint security configurations)」 > <node_name> > 「SSL 構成 (SSL configurations)」 > 「NodeDefaultSSLSettings」**にナビゲートします。
2. トラストストア名のフィールドで、**NodeDefaultTrustStore** を選択します。

   注: NodeDefaultTrustStore が使用したいトラストストア (例えば、bcgSecurityTrust.jks) 用に構成されていることを確認してください。
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. そのノードでサーバーを再始動します。

注: 完全配布モードの場合、上記の変更は bcgreceiver サーバーおよび bcgconsole サーバーが組み込まれているすべてのノードに対して行う必要があります。シンプル配布モードの場合、これらの変更は bcgserver が組み込まれているすべてのノードに対して行う必要があります。

NodeDefaultTrustStore が、WebSphere Partner Gateway サーバーが組み込まれているノードに設定されている場合の署名者証明書の trust.p12 への追加: 現在は、NodeDefaultTrustStore は trust.p12 を参照します。NodeDefaultTrustStore が、WebSphere Partner Gateway サーバーが組み込まれているノードに対して設定される場合、bcgSecurityTrust.jks は使用されません。要求に応じ、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しているとき出されます。ユーザーのコミュニティーが SSL を使用していない場合、インバウンド SSL 証明書またはアウトバウンド SSL 証明書は必要ではありません。

ステップ 1: サーバーの認証: アウトバウンド文書をユーザーのパートナーに送信するために SSL が使用されているとき、WebSphere Partner Gateway はパートナーからのサーバー・サイド証明書を要求します。複数のパートナー用に同一の CA 証明書が使用できます。証明書は X.509 DER フォーマットでなければなりません。

注: iKeyman ユーティリティーでフォーマットを変換できます。フォーマットを変換するために iKeyman を使用するには、以下のステップを実行します。

1. iKeyman を開始します。
2. 新規のブランクの鍵ストアを作成するか、または既存の鍵ストアを開きます。
3. 鍵データベース・コンテンツで、「**署名者証明書**」を選択します。
4. 「**追加 (Add)**」オプションを使用して ARM 証明書を追加します。
5. **抽出 (Extract)** オプションを使用して、同一の証明書をバイナリー DER データとして抽出します。
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 CA により署名され、 CA ルート証明書および証明書チェーンの一部分である他の証明書がハブ・オペレーターにまだインストールされていない場合、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てください。

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。

   コミュニティー・コンソールにハブ・オペレーターまたは内部パートナーとしてログインしていることを確認してください。
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 ファイルは、ただ 1 つの秘密鍵および関連付けられる証明書を組み込む必要があります。証明書と PKCS#8 形式の秘密鍵を別個にアップロードすることもできます。
3. 「**SSL クライアント**」を証明書のタイプとして選択します。

4. 証明書の記述 (必須) をタイプします。
5. 状況を「**有効**」に変更します。
6. 「**参照**」をクリックし、証明書を保管したディレクトリーにナビゲートします。
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したい場合、リストから選択します。
10. 2 つの SSL 証明書を持っている場合、「**証明書の使用**」リストから「**1 次**」または「**2 次**」を選択することにより、これが 1 次証明書であるか、または 2 次証明書であるかを示します。
11. 「**アップロード**」をクリックし、次に「**保存**」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、前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: SSL クライアント認証が必要である場合、パートナーは、順々に、ハブから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ユーザーの証明書を WebSphere Partner Gateway にインポートします。iKeyman を使用して証明書を生成できます。証明書が自己署名証明書である場合、それをパートナーに配布する必要があります。CA 署名の証明書である場合、パートナーが CA ルート証明書を自身のトラステッド証明書に追加できるようにするため、CA ルート証明書をパートナーに与える必要があります。

複数の SSL 証明書を持つことができます。 1 つは、1 次証明書で、デフォルトでこれが使用されます。もう 1 つは、2 次証明書で、これは 1 次証明書の有効期限が切れる場合に使用されます。

自己署名証明書の使用: 自己署名証明書を使用しようとしている場合、次の手順を実行します。

1. iKeyman ユーティリティーを開始します。
2. iKeyman を使用して自己署名証明書と鍵ペアを生成します。
3. iKeyman を使用してファイルをユーザーの公開鍵を組み込む証明書に抽出します。
4. 証明書をユーザーのパートナーに配布します。配布の好ましい方法は、証明書をパスワードで保護された zip ファイルで E メールで送信することです。ユーザーのパートナーは、ユーザーをコールし、 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および秘密鍵ペアを PKCS12 ファイルの書式でエクスポートします。
6. コミュニティー・コンソールを介して自己署名証明書および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。

      「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ていることを確認してください。

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 ファイルは、ただ 1 つの秘密鍵および関連付けられる証明書を組み込む必要があります。証明書と PKCS#8 形式の秘密鍵を別個にアップロードすることもできます。

c. 「**SSL クライアント**」を証明書のタイプとして選択します。

d. 証明書の記述 (必須) をタイプします。

e. 状況を「**有効**」に変更します。

f. 「**参照**」をクリックし、証明書を保管したディレクトリーにナビゲートします。

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したい場合、リストから選択します。

j. 2 つの SSL 証明書を持っている場合、「**証明書の使用**」リストから「**1 次**」または「**2 次**」を選択することにより、これが 1 次証明書であるか、または 2 次証明書であるかを示します。

k. 「**アップロード**」をクリックし、次に「**保存**」クリックします。

SSL クライアント認証およびデジタル署名の両方の 1 次証明書および 2 次証明書をアップロードし、1 次証明書を 2 つの別個の項目としてアップロードする場合、対応する 2 次証明書が 2 つの異なる項目としてアップロードされていることを確認してください。

CA 署名の証明書の使用: CA により署名された証明書を使用しようとしている場合、次の手順を実行してください。

1. iKeyman を使用してレシーバーの証明書要求と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 から署名された証明書を受信したとき、iKeyman を使用して鍵ストアに署名された証明書を置きます。
4. すべてのパートナーに署名 CA 証明書を配布します。

暗号化を使用可能にするための証明書の使用

このセクションでは暗号化証明書を説明します。

インバウンド暗号化証明書の作成とインストール

この証明書は、パートナーから受信した暗号化ファイルを暗号化解除するため、ハブにより使用されます。ハブは文書を暗号化解除するためにユーザーの秘密鍵を使用します。暗号化は、送信者と意図された受信者以外の誰も転送中の文書を見ることを避けるために使用されます。

パートナーからの暗号化された AS2 メッセージの受信についての次の重要な制約事項について注意してください。パートナーが暗号化された AS2 メッセージを送信するが間違った証明書を使用する場合、暗号化解除は失敗します。しかし、失敗を示すための MDN はパートナーに返されません。この状況で、ユーザーのパートナーが MDN を受信するため、次の文書定義を持つパートナーへの接続を作成します。

- パッケージ: **AS** to Package: **None**
- プロトコル: **Binary**to Protocol: **Binary**
- 文書タイプ: **Binary**to Document Type: **Binary**

None 接続に対して作成される接続は AS 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、他方のパートナーで None B2B 機能をアクティブ化することにより接続を作成します。AS 側のソース・ゲートウェイは、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) であり、MDN アドレスに構成されていることを確認してください。このようにして、暗号化解除の失敗した MDN はこの AS から None Binary 接続に送り返されます。

ステップ 1: 証明書の入手:

自己署名証明書の生成: 自己署名証明書を使用しようとしている場合、次の手順を実行します。

1. iKeyman ユーティリティーを開始します。
2. iKeyman を使用して自己署名証明書と鍵ペアを生成します。
3. iKeyman を使用してファイルをユーザーの公開鍵を組み込む証明書に抽出します。
4. 証明書をユーザーのパートナーに配布します。それらは暗号化証明書としての使用のために、ファイルを B2B 製品にインポートする場合に必要です。暗号化ファイルを内部パートナーに送信したいとき、それを使用するようにアドバイスします。ユーザーの証明書が CA 署名である場合、CA 証明書も同様に提供してください。
5. iKeyman を使用して自己署名証明書および秘密鍵ペアを PKCS12 ファイルの書式で保管します。
6. 「**プロファイル**」> 「**{ハブ・オペレーター/内部パートナー}**」> 「**証明書**」> 「**新規証明書の作成 (create new certificate)**」にナビゲートします。
7. 「**この証明書が属するパートナー**」 ドロップダウンで、新規にアップロードされた証明書に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」をアップロードするため、「**証明書のロケーション**」の隣の「**参照**」をクリックします。
10. 「**次へ**」をクリックします。
11. 「証明書の詳細の指定」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**」 または 「**中間 CA 証明書 (intermediate CA certificate)**」。
12. この証明書を「**暗号化**」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、証明書を使用可能または使用不可にするかにより、「**状況**」内の「**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 署名の証明書の使用: CA により署名された証明書を使用しようとしている場合、次の手順を実行してください。

1. iKeyman ユーティリティーを開始します。
2. iKeyman を使用してレシーバーの証明書要求と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 から署名された証明書を受信したとき、iKeyman を使用して鍵ストアに署名された証明書を置きます。

ステップ 2: 証明書の配布: 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暗号化文書をパートナーに送信するとき使用されます。WebSphere Partner Gateway は文書をパートナーの公開鍵で暗号化し、パートナーは文書を秘密鍵で暗号化解除します。

パートナーは複数の暗号化証明書を持つことができます。1 つは、1 次証明書で、デフォルトでこれが使用されます。もう 1 つは、2 次証明書で、これは 1 次証明書の有効期限が切れる場合に使用されます。

ステップ 1: パートナーの証明書の入手: パートナーの暗号化証明書を入手します。証明書は X.509 DER フォーマットでなければなりません。WebSphere Partner Gateway は X5.09 証明書のみをサポートす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: 次の手順を完了することにより、パートナーのプロファイルの下でコミュニティー・コンソールを介して証明書をインストールします。

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「**パートナーの選択**」、「**ファイル・ロケーション**」、「**パスワード**」ページで次の値を入力します。
   - 「**この証明書が属するパートナー**」: 新規にアップロードされた証明書に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」である場合、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 (または)「トラストストアまたは鍵ストアをパスワードに指定してください」。「外部パートナー」の場合、証明書のロケーションを入力します (または) 証明書チェーンを含むトラストストアのロケーションを指定してください。
   - **証明書のロケーション**: 「**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、証明書の以下の詳細を入力します。
   - 「**リーフ証明書名**」 - リーフ証明書の名前。フィールド名は、証明書がリーフ証明書、ルート CA 証明書または中間 CA 証明書であるかによって決まります。
   - 「**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に関連付けます。

- 「**証明書の使用**」 - 証明書の使用に関連付けます。値は「1 次」および「2 次」です。
- 「**動作モード**」 - 操作のモードを入力します。
- 「**状況**」- アップロード後、証明書を使用可能または使用不可にするかにより、「使用可能」または「使用不可」を選択します。「次へ」ボタンは、証明書が使用可能である場合にのみ使用可能です。
- 「**セットの管理**」- ユーザーは証明書を既存のセットに関連付けるか、または新規セットを作成するかのいずれかができます。証明書が 2 次証明書である場合、それは既存のセットにのみ関連付けることができます。ユーザーは、暗号化のタイプを持つ内部パートナー、または SSL タイプ (着信クライアント認証) または「署名 (検証)」を持つ外部パートナーの任意のセットに証明書を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 次である場合、ユーザーはセットの作成、証明書のセットおよびパートナー接続への関連付けを行う必要はありません。「**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、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。さもなければ、ウィザードの「**既存への追加 (Add to Existing)**ページがオープンします。ファイルが内部パートナーの秘密鍵、または SSL / デジタル署名用に使用された外部パートナーの公開証明書を持つ場合、「**終了**」をクリックできます。
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を入力します。1 次証明書の場合、セットの作成と証明書のセットへの関連付けは必要ありません。以下の値を入力します。
   - 「**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」を選択します。「無効」の場合、「**次へ**」ボタンは使用可能ではありません。
   - 「**デフォルトに設定**」 - このセットをデフォルトに設定する場合、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 (Add to Existing Set)**」ページで、証明書に追加するセット (複数可) を選択します。以下の値を入力します。
   - 「**選択した証明書タイプに使用可能なセットのリストから選択してください**」 - リストから、証明書に追加するセット (複数可) を選択します。
   - 「**デフォルトに設定**」 - このセットをデフォルトに設定する場合、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「**既存のセットに追加 (Add to Existing Set)**」から、ウィザードの「**デフォルトの設定値 (Default Settings)**」ページに進むため、「**次へ**」をクリックします。セットの状況が「有効」の場合にのみ「**次へ**」ボタンは使用可能です。
9. アップロード後、証明書を使用可能または使用不可にするかにより、「**状況**」内の「**有効**」または「**無効**」を選択します。

   注: 以前のページ (「新規セットの作成」または「既存のセットへの追加」) 内の「**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、セットを動作モードに関連付ける必要があります。これに

より、動作モードに対する証明書の使用が表示されます。内部パートナーの暗号化は無効です。外部パートナーの SSL クライアントおよびデジタル署名は無効です。

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、欠落ルートまたは中間 CA 証明書が存在する場合に備えて、アップロードするようにプロンプトが出されます。プロンプト・ウィンドウで「はい」をクリックする場合、ウィザードの最初のページが開きます。後ろの段階でアップロードする場合は「**キャンセル**」をクリックします。
11. ウィザードの「構成」ページで、以下の値を入力します。

    注: 「構成」ページに動作モードに対する証明書 (セット) の使用のリストが表示されます。現行のセット名は定義済みですが、リセットできます。

    - 「**送信側パートナー**」 - このフィールドは内部パートナーの値で定義済みです。
    - 「**受信側パートナー**」 - このドロップダウンはすべての外部パートナーのリストで定義済みです。すべての外部パートナーを組み込むために値「すべて」を選択することもできます。
    - 「**送信側パッケージ**」 - ドロップダウンから、内部パートナーのパッケージ「文書フローの定義 (Document Flow Definitions)」オブジェクトを選択します。
    - 「**受信側パッケージ**」 - リストから、外部パートナーのパッケージ「文書フローの定義 (Document Flow Definitions)」オブジェクトを選択します。
12. セットを他のパートナー接続に関連付ける場合、「**更に接続を追加 (Add more connections)**」をクリックします。
13. 「**2 次証明書を追加 (Add Secondary Certificate)**」をクリックして現行のセットに 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。欠落ルートまたは中間 CA 証明書が存在する場合に備えて、アップロードするようにプロンプトが出されます。プロンプト・ウィンドウで「はい」をクリックする場合、ウィザードの最初のページが開きます。後ろの段階でアップロードする場合はプロンプト・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 次の暗号化証明書を持つ場合この手順を繰り返します。

ステップ 3: CA 発行の証明書のインストール: 証明書が CA により署名され、CA ルート証明書および証明書チェーンの一部分である他の証明書がハブ・オペレーター・プロファイルにまだインストールされていない場合、証明書をこの手順に従って今インストールしてください。

注: CA 発行の証明書がすでにインストールされている場合、このステップを実行する必要はありません。

1. 「**プロファイル**」> 「**ハブ・オペレーター**」> 「**証明書**」 > 「**新規証明書の作成 (create new certificate)**」にナビゲートします。
2. 「**この証明書が属するパートナー**」 ドロップダウンで、新規にアップロードされた証明書に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**」の隣の「**参照**」をクリックします。
5. 「証明書」および「トラストストア」の両方に対して、「**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**」を入力し、「**次へ**」をクリックします。
7. ウィザードの 「**アップロードするためのエンド・エンティティー 証明書の選択 (Select end entity certificate to upload)**」ページで、ロードするための証明書を選択します。

   注: 複数の証明書を持つトラストストア使用して証明書をロードするとき、「**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してください**」はすべての証明書でデータが設定されています。複数の証明書をアップロードできます。
8. 「**終了**」をクリックします。

ステップ 4: 暗号化を使用可能にする: パッケージ (最高レベル)、パートナー、または接続レベル (最低レベル) で暗号化を使用可能にします。設定は、接続レベルで他の設定値に優先します。必須の属性が欠落している場合、接続の要約により通知されます。

例えば、パートナー接続の属性を変更する場合、「**アカウント管理**」 > 「**接続**」をクリックし、次にパートナーを選択します。「**属性**」をクリックし、次に属性 (例えば、「**AS 暗号化**」)を編集します。

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、1 次証明書および 2 次証明書の両方とも無効です。証明書の有効期限が切れたか、失効した可能性があります。証明書の有効期限が切れたか、失効した場合、該当するイベント (「証明書が取り消されたか有効期限切れです (Certificate revoked or expired)」) がイベント・ビューアーに表示されます。これら 2 つのイベントは他のイベントにより分離される場合があることに注意してください。

イベント・ビューアーを表示するには以下の手順を実行します。

1. 「**ビューアー**」> 「**イベント・ビューアー**」の順にクリックします。
2. 適切な検索条件を選択します。
3. 「**検索**」をクリックします。

イベント・ビューアーの使用のついての情報は「*WebSphere Partner Gateway Administrator Guide*」を参照してください。

デジタル署名を使用可能にするための証明書の使用

アウトバウンド・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文書、署名した文書を送信するとき、この証明書を使用します。すべてのポートとプロトコルに対して同一の証明書および鍵が使用されます。

複数のデジタル署名証明書を持つことができます。1 つは、1 次証明書で、デフォルトでこれが使用されます。もう 1 つは、2 次証明書で、これは 1 次証明書の有効期限が切れる場合に使用されます。

自己署名証明書の生成: 自己署名証明書を使用しようとしている場合、次の手順を実行します。

1. iKeyman ユーティリティーを開始します。
2. iKeyman を使用して自己署名証明書と鍵ペアを生成します。
3. iKeyman を使用してファイルをユーザーの公開鍵を組み込む証明書に抽出します。
4. 証明書をユーザーのパートナーに配布します。配布の好ましい方法は、証明書をパスワードで保護された zip ファイルで E メールで送信することです。ユーザーのパートナーは、ユーザーをコールし、 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および秘密鍵ペアを PKCS12 ファイルの書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:

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**「パートナーの選択」**、**「ファイル・ロケーション」**、**「パスワード」**ページで次の値を入力します。
   - **「この証明書が属するパートナー」**: 新規にアップロードされた証明書に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」である場合、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 (または)「トラストストアまたは鍵ストアをパスワードに指定してください」。「外部パートナー」の場合、証明書のロケーションを入力します (または) 証明書チェーンを含むトラストストアのロケーションを指定してください。
   - **「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」:** 証明書がパスワードを持つ場合、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」: 「参照」**をクリックして「鍵ストアロケーション」を選択します。鍵ストアはトラステッド・ルートおよび CA 証明書と同様に秘密鍵および CA 証明書のコレクションです。
   - **「パスワード」:** 「鍵ストア・ロケーション」用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。ドロップダウン内の選択可能な値は、JKS、JCEKS、および PKCS12 です。
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。複数の証明書を持つトラストストア経由で証明書をロードするとき、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」** ページが開きます。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・エンティティーおよび CA 証明書の選択**」 ページで、次の値を入力します。
   - **鍵ストアは複数のエンド・エンティティー証明書を含みます。アップロードする証明書を選択してください。**- ドロップダウンはすべてのエンド・エンティティー証明書のリストを持ちます。アップロードするための証明書を選択してください。
   - 「**パスワード**」- 鍵ストアがパスワードを持つ場合、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 証明書のリストを選択してください」**- 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 証明書のリストを選択してください。
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、証明書の以下の詳細を入力します。
   - 「**リーフ証明書名**」 - リーフ証明書の名前。フィールド名は、証明書がリーフ証明書、ルート CA 証明書または中間 CA 証明書であるかによって決まります。
   - 「**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に関連付けます。
   - 「**証明書の使用**」 - 証明書の使用に関連付けます。値は「1 次」および「2 次」です。
   - 「**動作モード**」 - 操作のモードを入力します。
   - 「**状況**」- アップロード後、証明書を使用可能または使用不可にするかにより、「使用可能」または「使用不可」を選択します。「次へ」ボタンは、証明書が使用可能である場合にのみ使用可能です。
   - 「**セットの管理**」- ユーザーは証明書を既存のセットに関連付けるか、または新規セットを作成するかのいずれかができます。証明書が 2 次証明書である場合、それは既存のセットにのみ関連付けることができます。ユーザーは、暗号化のタイプを持つ内部パートナー、または SSL タイプ (着信クライアント認証) または「署名 (検証)」を持つ外部パートナーの任意のセットに証明書を関連付けることができます。

     注: ハブ・オペレーターの場合、セットの管理は存在しません。証明書は、作成されるデフォルトのセット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 次である場合、ユーザーはセットの作成、証明書のセットおよびパートナー接続への関連付けを行う必要はありません。「**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、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。さもなければ、ウィザードの「**既存への追加 (Add to Existing)**ページがオープンします。ファイルが内部パートナーの秘密鍵、またはSSL / デジタル署名用に使用された外部パートナーの公開証明書を持つ場合、「**終了**」をクリックできます。
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を入力します。1 次証明書の場合、セットの作成と証明書のセットへの関連付けは必要ありません。以下の値を入力します。
   - 「**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」を選択します。「無効」の場合、「**次へ**」ボタンは使用可能ではありません。
- 「**デフォルトに設定**」 - このセットをデフォルトに設定する場合、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 (Add to Existing Set)**」ページで、証明書に追加するセット (複数可) を選択します。以下の値を入力します。
   - 「**選択した証明書タイプに使用可能なセットのリストから選択してください**」 - リストから、証明書に追加するセット (複数可) を選択します。
   - 「**デフォルトに設定**」 - このセットをデフォルトに設定する場合、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「**既存のセットに追加 (Add to Existing Set)**」から、ウィザードの「**デフォルトの設定値 (Default Settings)**」ページに進むため、「**次へ**」をクリックします。セットの状況が「有効」の場合にのみ「**次へ**」ボタンは使用可能です。
11. アップロード後、証明書を使用可能または使用不可にするかにより、「**状況**」内の「**有効**」または「**無効**」を選択します。

    注: 以前のページ (「新規セットの作成」または「既存のセットへの追加」) 内の「**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、セットを動作モードに関連付ける必要があります。これにより、動作モードに対する証明書の使用が表示されます。内部パートナーの暗号化は無効です。外部パートナーの SSL クライアントおよびデジタル署名は無効です。
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、欠落ルートまたは中間 CA 証明書が存在する場合に備えて、アップロードするようにプロンプトが出されます。プロンプト・ウィンドウで「はい」をクリックする場合、ウィザードの最初のページが開きます。後ろの段階でアップロードする場合は「**キャンセル**」をクリックします。
13. ウィザードの「構成」ページで、以下の値を入力します。

    注: 「構成」ページに動作モードに対する証明書 (セット) の使用のリストが表示されます。現行のセット名は定義済みですが、リセットできます。
    - 「**送信側パートナー**」 - このフィールドは内部パートナーの値で定義済みです。
    - 「**受信側パートナー**」 - このドロップダウンはすべての外部パートナーのリストで定義済みです。すべての外部パートナーを組み込むために値「すべて」を選択することもできます。
    - 「**送信側パッケージ**」 - ドロップダウンから、内部パートナーのパッケージ「文書フローの定義 (Document Flow Definitions)」オブジェクトを選択します。
    - 「**受信側パッケージ**」 - リストから、外部パートナーのパッケージ「文書フローの定義 (Document Flow Definitions)」オブジェクトを選択します。
14. セットを他のパートナー接続に関連付ける場合、「**更に接続を追加 (Add more connections)**」をクリックします。

15. 「**2 次証明書を追加(Add Secondary Certificate)**」をクリックして現行のセットに 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。欠落ルートまたは中間 CA 証明書が存在する場合に備えて、アップロードするようにプロンプトが出されます。プロンプト・ウィンドウで「はい」をクリックする場合、ウィザードの最初のページが開きます。後ろの段階でアップロードする場合はプロンプト・ウィンドウで「**キャンセル**」をクリックします。

SSL クライアント認証およびデジタル署名の両方の 1 次証明書および 2 次証明書をアップロードし、1 次証明書を 2 つの別個の項目としてアップロードする場合、対応する 2 次証明書が 2 つの異なる項目としてアップロードされていることを確認してください。

CA 署名の証明書の入手: CA により署名された証明書を使用しようとしている場合、次の手順を実行してください。

1. iKeyman ユーティリティーを開始します。
2. iKeyman を使用してレシーバーの証明書要求と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 から署名された証明書を受信したとき、iKeyman を使用して鍵ストアに署名された証明書を置きます。
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・シグニチャー証明書のインストール

ユーザーが文書を受信したとき、「文書マネージャー」は送信者のシグニチャーを検査するため、パートナーの署名した証明書を使用します。パートナーはユーザーに X.509 DER フォーマットで、自身の自己署名のシグニチャー証明書を送信します。ユーザーは、順に、個別のパートナーのプロファイルの下でコミュニティー・コンソールを介してパートナーの証明書を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 フォーマットで受信します。
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」をアップロードするため、「**証明書のロケーション**」の隣の「**参照**」をクリックします。
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**」に関連付けます。
7. アップロード後、証明書を使用可能または使用不可にするかにより、「**状況**」内の「**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、「**動作モード**」を選択するオプションは存在しません。
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 CA により署名され、 CA ルート証明書および証明書チェーンの一部分である他の証明書がハブ・オペレーター・プロファイルにまだインストール

されていない場合、証明書を今インストールしてください。これのみがトラストストア/鍵ストアに対して適用可能です。

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。

「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、自身のプロファイルに証明書をインストールしていることを確認してください。

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. 証明書の記述 (必須) をタイプします。

e. 状況を「**有効**」に変更します。

f. 「**参照**」をクリックし、証明書を保管したディレクトリーにナビゲートします。

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**」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、前のステップを実行する必要はありません。

11. パッケージ (最高レベル)、パートナー、または接続レベル (最低レベル) で署名を使用可能にします。設定は、接続レベルで他の設定値に優先します。必須の属性が欠落している場合、接続の要約により通知されます。

例えば、パートナー接続の属性を変更する場合、「**アカウント管理**」 > 「**接続**」をクリックし、次にパートナーを選択します。「**属性**」をクリックし、次に属性 (例えば、「**AS 署名済み**」)を編集します。

コンソール・グループの作成

グループ機能を使用すると、特定のコンソール特権を持つ特定タイプのユーザーのグループを作成できます。例えば、テスト・サイクル中の接続テストが割り当てられるユーザー用にテスター・グループを作成するとします。テスター・グループを作成した後、テスト・サイクル中にグループのユーザーがアクセスする必要があるコンソール機能に基づいて、グループにアクセス権を割り当てます。

管理者グループとデフォルト・グループは、デフォルトのアクセス権設定で自動的に作成されます。パートナーのハブ管理者グループまたは管理者グループに属するどのユーザーであっても、デフォルトのアクセス権設定を変更することができます。

警告: 管理者グループとデフォルト・グループはシステムで生成されます。編集や削除はできません。ハブ管理者グループには、その他に「ハブ管理」というグループがあります。

グループの作成方法

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**グループ**」をクリックします。「グループ・リスト」画面が表示されます。

2. 画面の右上隅にある「**作成**」をクリックします。「グループの詳細」画面が表示されます。
3. 新規グループの「**名前**」と「**説明**」を入力します。
4. 「**保管**」をクリックします。さらにグループを追加する場合は、以上のステップを繰り返します。

ユーザーの作成

この機能を使用すると、ユーザー・プロファイルを作成できます。システムでは、パートナー・プロファイルを使用して、コンソール・アクセス、アラート配信、およびユーザーの可視性を制御します。

ユーザー・プロファイルには、ユーザーの名前と連絡先情報 (E メール・アドレスと電話番号)、ログイン状況 (使用可能または使用不可)、ユーザーのアラート状況 (使用可能または使用不可)、および可視性 (ローカルまたはグローバル) が設定されています。ユーザー名は固有です。

- ユーザー・ログイン状況が「使用可能」である場合、ユーザーはコミュニティー・コンソールにログインできます。ユーザー・ログイン状況が「使用不可」である場合、ユーザーはコミュニティー・コンソールにログインできません。
- ユーザーのアラート状況が「使用可能」である場合、ユーザーはアラート通知を受信できます。ユーザーのアラート状況が「使用不可」である場合、ユーザーはアラート通知を受信できません。
- ユーザーの可視性が「ローカル」である場合、ユーザーは自分の組織にしか表示されません。ユーザーの可視性が「グローバル」である場合、ユーザーはハブ・コミュニティー全体に表示されます。

ユーザーのパスワードを自動生成することもできます。

新規ユーザーの作成

この機能を使用すると、新規ユーザーを追加できます。ユーザーとグループを定義した後は、グループにユーザーを追加できます。

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**ユーザー**」をクリックします。「ユーザー・リスト」画面が表示されます。
2. 画面の右上隅にある「**作成**」をクリックします。「ユーザーの詳細」画面が表示されます。
3. **ユーザー名** (ユーザーのログイン名) を入力します。
4. このユーザーのコンソール・アクセスを使用可能にするか使用不可にするかに関して、「**状況**」を選択します。
5. ユーザー名 (「**名**」と「**姓**」) を入力します。
6. システムがユーザーへのアラート通知の送信に使用する **E メール**・アドレスを入力します。
7. ユーザーの「**電話番号**」と「**FAX 番号**」を入力します。
8. 「**言語ロケール**」、「**書式ロケール**」、および「**時間帯**」を選択します。

9. このユーザーへのアラート通知を使用可能にするか使用不可にするかに関して、「**アラート状況**」を選択します。使用可能にした場合、ユーザーはサブスクライブしたすべてのアラートを受信します。使用不可にした場合、ユーザーはアラートを受信しません。

   注: 「サブスクライブ済み」の値はシステムによって入力されます。
10. ユーザーが組織内でのみ表示されるようにするか (「ローカル」)、ハブ・コミュニティー全体に表示されるようにするか (「グローバル」) に関して、ユーザーの「**サブスクライブした可視性 (Subscribed Visibility)**」を選択します。
11. 「**パスワードの自動生成**」 をクリックしてパスワードを自動的に生成します。このユーザーのパスワードを選択する場合は、「パスワード」と「パスワードの再入力」テキスト・ボックスにパスワードを入力します。
12. 「**保管**」をクリックします。さらにユーザーを追加する場合は、上記のステップを繰り返します。

FTP ユーザーの構成

現行ユーザーを FTP ユーザーとして使用可能にするには、以下を実行します。

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**ユーザー**」をクリックします。「ユーザー・リスト」画面が表示されます。
2. 必要なユーザーを選択し、「**編集**」 アイコンをクリックします。
3. 「**FTP 構成**」をクリックします。
4. 「**ホーム・ディレクトリー**」を入力します。これは、bcg.ftp.config.rootdirectory に対して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。
5. 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。
6. 「**ディレクトリーの作成/除去**」へのアクセス権を使用可能または使用不可にします。.
7. 許可されている、最大同時ログインである「**最大ログイン回数**」を選択します。「カスタム制限」を選択した場合、テキスト・ボックスにカスタマイズされた値を入力します。
8. 同一の IP アドレスから許可されている最大同時ログインである、「**同一 IP からの最大ログイン回数**」を選択します。リストから「カスタム制限」を選択した場合、テキスト・ボックスにカスタマイズされた値を入力します。
9. 「**最大アイドル時間 (Max Idle Time)**」を選択します。これは、経過後、ユーザー接続が廃棄される最大アイドル時間 (秒単位) です。リストから「カスタム制限」を選択した場合、テキスト・ボックスにカスタマイズされた値を入力します。
10. 「**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、テキスト・ボックスにカスタマイズされた値を入力します。
11. 「**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、テキスト・ボックスにカスタマイズされた値を入力します。
12. 「**保管**」をクリックします。

グループへのユーザーの追加

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**ユーザー**」をクリックします。「ユーザー・リスト」画面が表示されます。
2. 「詳細の表示」アイコンをクリックして、ターゲット・ユーザーのグループ・メンバーシップの詳細を表示します。
3. 「編集」アイコンをクリックして、ユーザーのグループ・メンバーシップを編集します。
4. グループを選択し、「**グループへの追加**」または「**グループからの除去**」をクリックして、ユーザーをグループに対して追加または除去します。
5. 編集が終了したら「編集オフ (Edit off)」アイコンをクリックします。

連絡先情報の作成

連絡先機能を使用すると、主要担当者の連絡先情報を作成できます。イベントが発生し、アラート通知が生成されたときは、この連絡先情報を使用して通知の送信先を確認します。

組織のサイズによっては、発生したイベントのタイプによって異なる連絡先への通知が必要になることがあります。例えば、文書の検証が失敗した場合、問題を評価するため、セキュリティー担当者に通知する必要があります。内部パートナーの送信が通常の範囲を超える場合、ネットワーク管理者に通知し、送信量の増加が効率的に処理されるようにします。

連絡先を作成した後、アラート機能に戻り、作成した各アラートに適切な連絡先をリンクします。

新規連絡先の作成方法

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**連絡先**」をクリックします。現在の連絡先のリストが表示されます。
2. 画面の右上隅にある「**作成**」をクリックします。「連絡先の詳細」画面が表示されます。
3. 連絡先の「**名**」と「**姓**」を入力します。
4. 連絡先の「**住所**」を入力します。
5. ドロップダウン・リストから「**連絡先タイプ**」を選択します (例えば、「B2B担当」や「ビジネス担当」など)。
6. 連絡先の **E メール**・アドレスを入力します。
7. 連絡先の「**電話番号**」と「**FAX 番号**」を入力します。
8. 「**言語ロケール**」、「**書式ロケール**」、および「**時間帯**」を選択します。
9. この連絡先へのアラート通知を使用可能にするか使用不可にするかに関して、「**アラート状況**」を選択します。使用可能にした場合、この連絡先はサブスクライブしたすべてのアラートを受信します。使用不可にした場合、この連絡先はアラートを受信しません。

   注: 「サブスクライブ済み」の値はシステムによって入力されます。
10. 連絡先の「**サブスクライブした可視性 (Subscribed Visibility)**」を選択します。「ローカル」を選択した場合、連絡先はユーザーの組織にしか表示されませ

ん。「グローバル」を選択した場合、連絡先はハブ管理者と内部パートナーに表示されます。両者とも連絡先をアラートにサブスクライブできます。

11. 「**保管**」をクリックします。連絡先をアラートに追加するには、いくつかの方法があります。

    既存のアラートに連絡先を追加するには、40 ページの『既存のアラートへの新規連絡先の追加』を参照してください。

    ボリューム・ベースのアラートを作成し、そのアラートに連絡先を追加するには、35 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。

    イベント・ベースのアラートを作成し、そのアラートに連絡先を追加するには、38 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。

アラートの作成と連絡先の追加

問題の早期解決には、適切なときに適切な人にシステムの問題に関する情報を送ることが重要です。

WebSphere Partner Gateway のアラートを使用すると、受信した伝送量に異常な変動があったり、ビジネス文書処理エラーが発生したときに、主要な担当者に通知できます。

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、さらに処理エラーの識別、トラブルシューティング、および解決に役立ちます。

アラートは、テキスト・ベースの E メール・メッセージから構成され、サブスクライブされた連絡先または主要担当者の配布リストに送信されます。アラートは、システム・イベントの発生 (イベント・ベースのアラート) または予想される文書フローのボリューム (ボリューム・ベースのアラート) に基づいて送信されます。

- 伝送量の増減の通知を受け取るには、ボリューム・ベースのアラートを使用します。

  例えば、外部パートナーは、営業日に内部パートナーからの伝送をまったく受信しない場合に通知するボリューム・ベースのアラートを作成できます (「ボリューム」を 「ゼロ・ボリューム」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」を選択します)。このアラートでは、内部パートナーのネットワーク伝送の障害が強調表示されます。

  外部パートナーは、内部パートナーからの伝送回数が通常の比率を超えている場合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、通常は毎日約 1000 回の伝送を受信している場合、「予期ボリューム (Expected Volume)」を 1000 に設定し、「逸脱率 (%)」を 25% に設定します。この場合、一日の伝送数が 1250 回を超えると、アラートが通知されます (伝送数が 750 回を下回る場合も通知されます)。このアラートは、内部パートナー側での要求の増加を示すことがあります。そのため、やがて、ユーザーの環境でサーバーの追加が必要になることがあります。

ボリューム・ベースのアラートでは、アラート作成時に選択した文書タイプに関連してボリュームをモニターすることに注意してください。WebSphere Partner Gateway では、アラートに選択された文書タイプが入った文書しか検索せず、アラートのすべての判定条件が満たされた場合にのみアラートを生成します。

- 文書処理エラーが発生したときに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、検証エラーまたは重複文書の受信のため、文書の処理が失敗した場合に通知するアラートを作成します。また、証明書の有効期限が切れそうな場合に通知するアラートを作成することもできます。

  イベント・ベースのアラートを作成するには、WebSphere Partner Gateway の定義済みイベント・コードを使用します。イベントには、デバッグ、情報、警告、エラー、重大の 5 つのタイプがあります。各イベント・タイプには、多くのイベントが属します。定義済みイベントは、「アラート: イベント」画面で表示し、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」などがあります。

注: 外部パートナーは、内部パートナーに送信された文書のボリュームに関するボリューム・ベースのアラートしか作成できません。外部パートナーは、内部パートナーから外部パートナーに送信された文書のボリュームにボリューム・ベースのアラートを設定する場合、ハブ管理者に対し、外部パートナーをアラート所有者として指定して外部パートナーのためにボリューム・ベースのアラートを設定するよう依頼します。

ヒント:

- 外部パートナーまたは内部パートナーの予想伝送量が運用上の限界を下回る場合
- に通知を受け取るようにするには、ボリューム・ベースのアラートを使用します。このアラートでは、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が強調表示されます。
- 文書処理エラーの通知を受け取るには、イベント・ベースのアラートを使用する。例えば、検証エラーのために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。

ボリューム・ベースのアラートの作成

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」画面が表示されます。
2. 画面の右上隅にある「**作成**」をクリックします。「アラート定義 (Alert Define)」タブが表示されます。
3. 「**アラート・タイプ**」に「**ボリューム・アラート**」を選択します (デフォルト設定です)。ボリューム・アラートに適したテキスト・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. 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**」を選択します (内部パートナーとハブ管理者のみ)。
6. 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。

選択されたパッケージ、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する必要があります。

7. 3 つのボリューム・オプション (「予期」、「範囲」、「ゼロ・ボリューム」) のいずれか 1 つを選択し、8 (36 ページ) に進みます。
   - **「予期」**。文書タイプのボリュームが正確な数量値から離れた場合にアラートを生成するには、「予期」を選択します。予期される文書タイプのボリュームに関するアラートを作成するには、次のステップに従います。
     a. 「ボリューム」テキスト・ボックスに、8 で選択する時間フレーム内に受信が予想される文書タイプの数を入力します。正数のみを入力します。負の数値を入力すると、アラートは機能しません。
     b. 「逸脱率 (%)」テキスト・ボックスに数値を入力します。文書フローのボリュームがこの値から逸脱するとアラートがアクティブになります。例を次に示します。
        – ボリューム = 20 で逸脱率 = 10% である場合、文書フローのボリュームが 18 より小さいか、22 より大きい場合、アラートが生成される。
        – ボリューム = 20 で逸脱率 = 0% である場合、20 以外のすべての文書フローのボリュームでアラートが生成される。
   - **「範囲」**。文書フローのボリュームが最大/最小範囲の外側になった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、次のステップに従います。
     a. 「最小」テキスト・ボックスに、8 で選択する時間フレーム内に受信が予想される文書タイプの最小数を入力します。文書フローのボリュームがこの数を下回った場合にのみ、アラートが生成されます。
     b. 「最大」テキスト・ボックスに、8 で選択する時間フレーム内に受信が予想される文書タイプ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、「最小」と「最大」の両テキスト・ボックスに入力する必要があります。
   - **「ゼロ・ボリューム」**。8 で選択する時間フレーム内に文書タイプが発生しない場合にアラートを生成するには、「ゼロ・ボリューム」を選択します。
8. アラート生成のため、文書フローのボリュームのモニターに使用される時間フレーム (頻度) として「毎日」または「範囲」を選択します。
   - **「毎日」**。毎週または毎月 1 日以上を指定して文書フローの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、または月曜日と木曜日など) または毎月の決まった日 (1 日と 15 日など) にのみ文書フローの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」**。毎週または毎月の 2 つの日で指定した間、文書フローの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、月曜日から金曜日までの毎日、または毎月 5 日から 20 日までの毎日、文書フローのボリュームをモニターするには、「範囲」を選択します。
9. 次のステップで選択される日に文書フローのボリュームをモニターする場合の開始時刻と終了時刻 (24 時間制) を選択します。範囲の頻度を選択した場合、

文書フローのボリュームのモニターは範囲内の最初の日の開始時刻から範囲内の最後の日の終了時刻まで行われることに注意してください。

10. アラート・モニターを行う毎週または毎月の特定の日を選択します。頻度として「毎日」を選択した場合、アラート・モニター用の曜日または毎月の日を選択します。頻度として「範囲」を選択した場合、アラート・モニターを行う期間を示す 2 つの曜日または月の 2 つの日を選択します。
11. このアラートの「**アラート状況**」として、「使用可能」または「使用不可」を選択します。
12. 「**保管**」をクリックします。
13. 「**通知**」タブをクリックします。
14. 「編集」アイコンをクリックします。
15. パートナーを選択します (内部パートナーとハブ管理者のみ)。
16. 追加する連絡先が「連絡先」テキスト・ボックスに表示されている場合、その連絡先を選択し、「**サブスクライブ**」をクリックします。21 に進みます。

    追加する連絡先が「連絡先」テキスト・ボックスに表示されていない場合、「**連絡先に新規記入項目を追加 (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。

    アラート所有者に表示される「連絡先に新規記入項目を追加 (Add New Entry to Contacts)」オプションでは、アラート所有者に関連付けられた連絡先しか作成できません。アラート所有者はこの機能を使用して、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。
17. 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。
18. 連絡先のアラート状況を選択します。
    - このアラートが生成されたときにこの連絡先に E メール・メッセージを送信するには、「**使用可能**」を選択する。
    - このアラートが生成されたときにこの連絡先に E メール・メッセージを送信しない場合は、「**使用不可**」を選択する。
19. 連絡先の可視性を選択します。
    - 連絡先をユーザーの組織にのみ表示する場合は、「**ローカル**」を選択する。
    - ハブ管理者と内部パートナーに連絡先を表示するには、「**グローバル**」を選択する。両者とも連絡先をアラートにサブスクライブできます。
20. 連絡先を保管するには、「**保管**」をクリックします。このアラートの連絡先リストに連絡先を追加するには、「**保管してサブスクライブ**」をクリックします。
21. 「**保管**」をクリックします。

注: 元のモニター期間が過ぎた後に、ボリューム・ベースのアラートに変更を行うと、次のモニター期間の日に有効になります。例えば、水曜日と木曜日の午後 1 時から 3 時にアラートをモニターしています。ここで、水曜日の午後 4 時に、午後 5 時から 7 時までアラートをモニターするように変更します。この場合、水曜日にアラートが 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

注: アラート E メール・サーバーを構成する必要があります。アラート E メール・サーバーの構成について詳しくは、「*管理ガイド*」を参照してください。

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」画面が表示されます。
2. 画面の右上隅にある「**作成**」をクリックします。「アラート定義 (Alert Define)」タブが表示されます。
3. **アラート・タイプ**に「**イベント・アラート**」を選択します。イベント・ベースのアラートに適したテキスト・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。この名前は、このアラートの ID になります。
5. アラートを発生させる「**パートナー**」を選択します (このオプションは内部パートナーとハブ管理者のみ使用できます)。

   「すべてのパートナー」オプションを選択し、システムのすべてのパートナーにアラートを関連付けます。アラート検索を実行し、「パートナーのアラート」として「すべてのパートナー」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。
6. 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。
7. イベント・タイプとして、「デバッグ」、「情報」、「警告」、「エラー」、「重大」、または「すべて」を選択します。これは、「イベント名」リストに表示されるイベントを制限するフィルターとして働きます。
8. 「BCG240601 AS 再試行の失敗」や「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を選択します。証明書の有効期限がもうすぐ切れるときに通知するアラートを作成するには、次のいずれか 1 つを選択します。
   - 「BCG108005 証明書の有効期限は 60 日です」
   - 「BCG108006 証明書の有効期限は 30 日です」
   - 「BCG108007 証明書の有効期限は 15 日です」
   - 「BCG108008 証明書の有効期限は 7 日です」
   - 「BCG108009 証明書の有効期限は 2 日です」
9. このアラートの状況として「使用可能」または「使用不可」を選択します。
10. 「**保管**」をクリックします。
11. 「**通知**」タブをクリックします。
12. 「編集」アイコンをクリックします。
13. パートナーを選択します (内部パートナーとハブ管理者のみ)。
14. 追加する連絡先が「連絡先」テキスト・ボックスに表示されている場合、その連絡先を選択し、「**サブスクライブ**」をクリックします。19 に進みます。

    追加する連絡先が「連絡先」テキスト・ボックスに表示されていない場合、「**連絡先に新規記入項目を追加 (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。

アラート所有者に表示される「連絡先に新規記入項目を追加 (Add New Entry to Contacts)」オプションでは、アラート所有者に関連付けられた連絡先しか作成できません。アラート所有者はこの機能を使用して、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。

15. 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。アラートの送出には E メール・アドレスのみが使用されます。エントリーの残りは、追加情報として使用されます。
16. 連絡先のアラート状況を選択します。
    - このアラートが生成されたときにこの連絡先に E メール・メッセージを送信するには、「**使用可能**」を選択する。
    - このアラートが生成されたときにこの連絡先に E メール・メッセージを送信しない場合は、「**使用不可**」を選択する。
17. 連絡先の可視性を選択します。
    - 連絡先をユーザーの組織にのみ表示する場合は、「**ローカル**」を選択する。
    - ハブ管理者と内部パートナーに連絡先を表示するには、「**グローバル**」を選択する。両者とも連絡先をアラートにサブスクライブできます。
18. 連絡先を保管するには、「**保管**」をクリックします。連絡先を保管し、このアラートの連絡先リストに連絡先を追加するには、「**保管してサブスクライブ**」をクリックします。
19. 配信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、アラートが発生したとき、連絡先にアラート通知が送信されます。重大なアラートに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信する時期を指定できます。重大ではないアラートにはこのオプションを使用します。

      ここでの 2 つのオプション「カウント」と「時間」は、相互に排他的ではありません。

      「カウント」オプションを選択する場合は、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 (「カウント」) に達した場合、アラート通知が生成されます。
      - アラートは発生したが、選択した制限時間 (「時間」) 内にアラート数 (「カウント」) に達していない場合、制限時間に達したときにアラート通知が生成されます。

      「時間」オプションは「カウント」オプションなしで使用できますが、「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ときは、「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。この数のアラートが選択した時間 (「時間」) 内に発生すると、アラート通知がアラートの連絡先に送信されます。

2 つのオプションを一緒に使用する例を次に示します。

この例で、「バッチ・アラート元:」オプションは「カウント」が 10 (10 回のアラート)、「時間」が 2 (2 時間) に設定されています。システムでは、2 時間以内に 10 回のアラートが発生するか、制限時間に達するまで、このアラートの通知をすべて保持します。

アラート・カウントが 2 時間以内に 10 回に達すると、このアラートに対するすべてのアラート通知が連絡先に送信されます。

アラートは発生したが、制限時間 (2 時間) 内に 10 回は発生しなかった場合、制限時間に達したときにアラート通知がアラートの連絡先に送信されます。

– **「時間」**。時間数 (n) を選択します。n 時間の間、システムはアラート通知を保持します。n 時間ごとに、保持されたアラート通知はすべて連絡先に送信されます。

例えば、2 を入力した場合、システムは発生したアラートのすべての通知を 2 時間の間隔で保持します。2 時間の期限が切れると、このアラートのすべてのアラート通知は連絡先に送信されます。

20. **「保管」**をクリックします。

既存のアラートへの新規連絡先の追加

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」画面が表示されます。
2. ドロップダウン・リストから検索条件を入力します。アラート名を入力します。
3. **「検索」**をクリックします。検索条件に合致するアラートのリストが表示されます (存在する場合)。
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. パートナーを選択します (内部パートナーとハブ管理者のみ)。
8. 追加する連絡先が「連絡先」テキスト・ボックスに表示されている場合、その連絡先を選択し、**「サブスクライブ」**をクリックします。13 に進みます。

   追加する連絡先が「連絡先」テキスト・ボックスに表示されていない場合、**「連絡先に新規記入項目を追加 (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。

   アラート所有者に表示される「連絡先に新規記入項目を追加 (Add New Entry to Contacts)」オプションでは、アラート所有者に関連付けられた連絡先しか作成できません。アラート所有者はこの機能を使用して、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。
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。

- このアラートが生成されたときにこの連絡先に E メール・メッセージを送信するには、「**使用可能**」を選択する。
- このアラートが生成されたときにこの連絡先に E メール・メッセージを送信しない場合は、「**使用不可**」を選択する。

11. 連絡先の可視性を選択します。
    - 連絡先をユーザーの組織にのみ表示する場合は、「**ローカル**」を選択する。
    - ハブ管理者と内部パートナーに連絡先を表示するには、「**グローバル**」を選択する。両者とも連絡先をアラートにサブスクライブできます。
12. 連絡先を保管するには、「**保管**」をクリックします。連絡先を保管し、このアラートの連絡先リストに連絡先を追加するには、「**保管してサブスクライブ**」をクリックします。
13. 「**保管**」をクリックします。

新規住所の作成

この機能を使用すると、パートナー・プロファイルに住所を作成できます。システムは、企業、広告、および技術担当の場所について、複数の住所タイプをサポートするように構成されています。

新規住所の作成方法

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**住所**」をクリックします。「住所」画面が表示されます。
2. 画面の右上隅にある「**新規住所の作成**」をクリックします。「住所」画面が表示されます。
3. ドロップダウン・リストから住所タイプを選択します (「広告」、「会社」、「技術」)。
4. 該当するテキスト・ボックスに住所を入力します。
5. 「**保管**」をクリックします。

第 3 章 宛先の作成

宛先は、エントリー・ポイントをシステム内に定義します。本章では、宛先の作成手順について説明します。含まれるトピックは以下のとおりです。

概要

WebSphere Partner Gateway は、宛先を使用して、文書を適切な宛先に送付します。受信者は、外部パートナーまたは内部パートナーです。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。

パートナー宛先で (デフォルトで) サポートされているトランスポートは、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)。
- 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。

HTTP 宛先の設定

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**」 > 「**宛先**」をクリックします。
2. 「**作成**」をクリックします。

宛先の詳細

「**宛先リスト**」ページから、以下のステップを実行します。

1. 宛先を示す名前を入力します。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「**使用可能**」です。使用可能状態の宛先は、文書を送信することができます。使用不可状態の宛先は、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. オプションで、使用されるプロキシー・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・サーバーを含む、ユーザーが作成したすべてのプロキシー・サーバーが含まれます。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を使用する**」 です。異なるプロキシー・サーバーを使用するため、選択したパートナーを使用したい場合、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対してこの機能を使用したくない場合、 select 「**順方向プロキシーを使用しない**」を選択します。
2. 「**トランスポート**」リストから、「**HTTP/1.1**」を選択します。
3. 「**住所**」フィールドには、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。

   この形式の一例を以下に示します。

   ```
   http://anotherserver.ibm.com:57080/bcgreceiver/Receiver
   ```

   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。
4. (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。

5. 「**再試行カウント**」フィールドには、失敗するまでに宛先が行う文書の送信試行回数を入力します。デフォルトは 3 です。
6. 「**再試行間隔**」フィールドには、宛先で文書の再送付を行うまで待機する時間を入力します。デフォルトは 300 秒です。
7. 「**スレッド数**」フィールドには、同時に処理する文書数を入力します。デフォルトは 3 です。
8. 「**クライアント IP の検証**」フィールドでは、文書が処理される前に送信側の IP アドレスを検証する場合には、「**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。
9. 「**自動キュー**」フィールドでは、残りの再試行回数がなくなって配信障害が発生しそうなときに宛先を (自動的に) オフラインにする場合には、「**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**」フィールドには、トラフィックなしでもソケットが開いたままの状態を続ける秒数を入力します。デフォルトは 120 秒です。
11. 宛先のプリプロセスまたはポストプロセス・ステップを構成する場合は、56 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。

HTTPS 宛先の設定

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**」 > 「**宛先**」をクリックします。
2. 「**作成**」をクリックします。

宛先の詳細

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を示す名前を入力します。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「**使用可能**」です。使用可能状態の宛先は、文書を送信することができます。使用不可状態の宛先は、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. 「**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。HTTP/S 宛先構成に順方向プロキシー構成は含まれません。
2. 「**住所**」フィールドには、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。

   例を次に示します。

   ```
   https://anotherserver.ibm.com:57443/bcgreceiver/Receiver
   ```
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**」フィールドには、失敗するまでに宛先が行う文書の送信試行回数を入力します。デフォルトは 3 です。
5. 「**再試行間隔**」フィールドには、宛先で文書の再送付を行うまで待機する時間を入力します。デフォルトは 300 秒です。
6. 「**スレッド数**」フィールドには、同時に処理する文書数を入力します。デフォルトは 3 です。
7. 「**クライアント IP の検証**」フィールドでは、文書が処理される前に送信側の IP アドレスを検証する場合には、「**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. 「**クライアント SSL 証明書の検証**」フィールドで、送信側パートナーのデジタル証明書を文書に関連付けられているビジネス ID に対して検証する場合は、「**はい**」をクリックします。デフォルトは「**いいえ**」です。
9. 「**自動キュー**」フィールドでは、残りの再試行回数がなくなって配信障害が発生しそうなときに宛先を (自動的に) オフラインにする場合には、「**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**」フィールドには、トラフィックなしでもソケットが開いたままの状態を続ける秒数を入力します。デフォルトは 120 秒です。
11. 宛先のプリプロセスまたはポストプロセス・ステップを構成する場合は、56 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。

FTP 宛先のセットアップ

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**」 > 「**宛先**」をクリックします。
2. 「**作成**」をクリックします。

宛先の詳細

「宛先の詳細」ページから、以下のステップを実行します。

1. 宛先を示す名前を入力します。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「**使用可能**」です。使用可能状態の宛先は、文書を送信することができます。使用不可状態の宛先は、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. 「**トランスポート**」リストから、「**FTP**」を選択します。
2. 「**住所**」フィールドには、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。

   例を次に示します。

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   ポート番号を入力しない場合は、標準の FTP ポートが使用されます。
3. (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。
4. 「**再試行カウント**」フィールドには、失敗するまでに宛先が行う文書の送信試行回数を入力します。デフォルトは 3 です。
5. 「**再試行間隔**」フィールドには、宛先で文書の再送付を行うまで待機する時間を入力します。デフォルトは 300 秒です。
6. 「**スレッド数**」フィールドには、同時に処理する文書数を入力します。デフォルトは 3 です。
7. 「**クライアント IP の検証**」フィールドでは、文書が処理される前に送信側の IP アドレスを検証する場合には、「**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. 「**自動キュー**」フィールドでは、残りの再試行回数がなくなって配信障害が発生しそうなときに宛先を (自動的に) オフラインにする場合には、「**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**」フィールドには、トラフィックなしでもソケットが開いたままの状態を続ける秒数を入力します。デフォルトは 120 秒です。
10. 必要に応じて、「**固有ファイル名の使用**」フィールドで、ボックスにチェック・マークを付けたままにしておきます。それ以外の場合は、ボックスをクリックしてチェック・マークを外します。「**固有ファイル名の使用**」を選択する場合、元のファイル名はデータベースに保管されます。
11. 宛先のプリプロセスまたはポストプロセス・ステップを構成する場合は、56 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。

SMTP 宛先のセットアップ

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**」 > 「**宛先**」をクリックします。
2. 「**作成**」をクリックします。

宛先の詳細

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を示す名前を入力します。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「**使用可能**」です。使用可能状態の宛先は、文書を送信することができます。使用不可状態の宛先は、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. 「**トランスポート**」リストから、「**SMTP**」を選択します。
2. 「**住所**」フィールドには、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。

   例を次に示します。

   ```
   mailto:admin@anotherserver.ibm.com
   ```

3. (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。
4. 「**再試行カウント**」フィールドには、失敗するまでに宛先が行う文書の送信試行回数を入力します。デフォルトは 3 です。
5. 「**再試行間隔**」フィールドには、宛先で文書の再送付を行うまで待機する時間を入力します。デフォルトは 300 秒です。
6. 「**スレッド数**」フィールドには、同時に処理する文書数を入力します。デフォルトは 3 です。
7. 「**クライアント IP の検証**」フィールドでは、文書が処理される前に送信側の IP アドレスを検証する場合には、「**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. 「**自動キュー**」フィールドでは、残りの再試行回数がなくなって配信障害が発生しそうなときに宛先を (自動的に) オフラインにする場合には、「**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. 「**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。
10. 宛先のプリプロセスまたはポストプロセス・ステップを構成する場合は、56 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。

JMS 宛先のセットアップ

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**」 > 「**宛先**」をクリックします。
2. 「**作成**」をクリックします。

宛先の詳細

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を示す名前を入力します。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「**使用可能**」です。使用可能状態の宛先は、文書を送信することができます。使用不可状態の宛先は、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. 「**トランスポート**」リストから、「**JMS**」を選択します。
2. 「**住所**」フィールドには、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 MQ JMS の場合、ターゲット URI のフォーマットは次のようになります。

   ```
   file:///<user_defined_MQ_JNDI_bindings_path>
   ```

   例を次に示します。

   ```
   file:///opt/JNDI-Directory
   ```

   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。このフィールドは必須です。
3. (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、JMS 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**」フィールドには、失敗するまでに宛先が行う文書の送信試行回数を入力します。デフォルトは 3 です。
5. 「**再試行間隔**」フィールドには、宛先で文書の再送付を行うまで待機する時間を入力します。デフォルトは 300 秒です。

6. 「**スレッド数**」フィールドには、同時に処理する文書数を入力します。デフォルトは 3 です。
7. 「**クライアント IP の検証**」フィールドでは、文書が処理される前に送信側の IP アドレスを検証する場合には、「**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. 「**自動キュー**」フィールドでは、残りの再試行回数がなくなって配信障害が発生しそうなときに宛先を (自動的に) オフラインにする場合には、「**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. 「**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。
10. 「**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。
11. 「**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。
12. 「**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。
13. 「**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。値を指定しない場合は、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。
14. 「**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。
15. 「**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。
16. 宛先のプリプロセスまたはポストプロセス・ステップを構成する場合は、56 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セットアップ

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**」 > 「**宛先**」をクリックします。
2. 「**作成**」をクリックします。

宛先の詳細

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を示す名前を入力します。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「**使用可能**」です。使用可能状態の宛先は、文書を送信することができます。使用不可状態の宛先は、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. 「**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。
2. 「**住所**」フィールドには、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 システムおよび Windows システムの場合、形式は、file:///<path to target directory> になります。

   例を次に示します。

   ```
   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。

   WebSphere Partner Gateway とは別のドライブにファイル・ディレクトリーがある Windows システムの場合、形式は、file:///<drive letter>:/<path> になります。
3. 「**再試行カウント**」フィールドには、失敗するまでに宛先が行う文書の送信試行回数を入力します。デフォルトは 3 です。
4. 「**再試行間隔**」フィールドには、宛先で文書の再送付を行うまで待機する時間を入力します。デフォルトは 300 秒です。
5. 「**スレッド数**」フィールドには、同時に処理する文書数を入力します。デフォルトは 3 です。
6. 「**クライアント IP の検証**」フィールドでは、文書が処理される前に送信側の IP アドレスを検証する場合には、「**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. 「**自動キュー**」フィールドでは、残りの再試行回数がなくなって配信障害が発生しそうなときに宛先を (自動的に) オフラインにする場合には、「**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. 必要に応じて、「**固有ファイル名の使用**」フィールドで、ボックスにチェック・マークを付けたままにしておきます。それ以外の場合は、ボックスをクリックしてチェック・マークを外します。「**固有ファイル名の使用**」を選択する場合、元のファイル名はデータベースに保管されます。
9. 宛先のプリプロセスまたはポストプロセス・ステップを構成する場合は、56 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。

FTPS 宛先のセットアップ

FTPS 宛先の作成は、次の手順で行います。

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**宛先**」をクリックします。
2. 「**作成**」をクリックします。

宛先の詳細

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を示す名前を入力します。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「**使用可能**」です。使用可能状態の宛先は、文書を送信することができます。使用不可状態の宛先は、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. 「**トランスポート**」リストから、「**FTPS**」を選択します。
2. 「**住所**」フィールドには、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。

   例を次に示します。

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   ポート番号を入力しない場合は、標準の FTP ポートが使用されます。
3. (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。
4. 「**再試行カウント**」フィールドには、失敗するまでに宛先が行う文書の送信試行回数を入力します。デフォルトは 3 です。
5. 「**再試行間隔**」フィールドには、宛先で文書の再送付を行うまで待機する時間を入力します。デフォルトは 300 秒です。
6. 「**スレッド数**」フィールドには、同時に処理する文書数を入力します。デフォルトは 3 です。
7. 「**クライアント IP の検証**」フィールドでは、文書が処理される前に送信側の IP アドレスを検証する場合には、「**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. 「**自動キュー**」フィールドでは、残りの再試行回数がなくなって配信障害が発生しそうなときに宛先を (自動的に) オフラインにする場合には、「**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**」フィールドには、トラフィックなしでもソケットが開いたままの状態を続ける秒数を入力します。デフォルトは 120 秒です。
10. 必要に応じて、「**固有ファイル名の使用**」フィールドで、ボックスにチェック・マークを付けたままにしておきます。それ以外の場合は、ボックスをクリックしてチェック・マークを外します。「**固有ファイル名の使用**」を選択する場合、元のファイル名はデータベースに保管されます。
11. 宛先のプリプロセスまたはポストプロセス・ステップを構成する場合は、56 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。

FTP スクリプト記述宛先のセットアップ

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・スクリプトで制御します。

FTP スクリプトの作成

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。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 3. スクリプト・パラメーターの FTP スクリプト記述宛先のフィールド記入項目へのマップ

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

これらのコマンドは FTP サーバーに送信されません。各コマンドは、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) を変更します。

- cd

  このコマンドは、指定されたディレクトリーに移動します。

- delete

  このコマンドは、FTP サーバーからファイルを削除します。

- mkdir

  このコマンドは、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もできます。

- open

  このコマンドは、FTP サーバーの 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。これらは、%BCGSERVERIP%、%BCGUSERID%、%BCGPASSWORD% 変数にそれぞれマップされます。FTP スクリプト記述ターゲットのスクリプトの最初の行は `open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%` である必要があります。

- quit、bye

  このコマンドは、FTP サーバーへの既存の接続を終了します。

- quote

  このコマンドは、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

  このコマンドは、FTP サーバー上からディレクトリーを除去します。

- 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

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」 > 「宛先」**をクリックします。
2. **「作成」**をクリックします。

宛先の詳細

「宛先リスト」ページから、以下のステップを実行します。

1. 宛先を示す名前を入力します。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「**使用可能**」です。使用可能状態の宛先は、文書を送信することができます。使用不可状態の宛先は、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. 「**トランスポート**」リストから、「**FTP Scripting**」を選択します。
2. 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。
3. 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。
4. ターゲットがセキュア・モードの場合は、「**FTPS モード**」に対してデフォルトの「**はい**」を使用してください。それ以外は、「**いいえ**」をクリックします。
5. 以下の手順に従い、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. 文書を処理するためのスクリプトを含む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にナビゲートします。
   c. 「**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。
   d. このスクリプト・ファイルが使用したいスクリプト・ファイルである場合は、「**保管**」をクリックします。
   e. 「**ウィンドウを閉じる**」をクリックします。
6. 「**再試行カウント**」フィールドには、失敗するまでに宛先が行う文書の送信試行回数を入力します。デフォルトは 3 です。
7. 「**再試行間隔**」フィールドには、宛先で文書の再送付を行うまで待機する時間を入力します。デフォルトは 300 秒です。
8. 「**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。
9. 「**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。

ユーザー定義属性

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、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. 宛先のプリプロセスまたはポストプロセス・ステップを構成する場合は、『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

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。

プリプロセスまたはポストプロセスの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「**使用可能なリスト**」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。

ユーザー作成ハンドラーをこれらの構成ポイントに適用するには、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、「*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、「**preprocess**」または「**postprocess**」を選択します。
2. 「**使用可能なリスト**」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. 「**保管**」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、「**削除**」をクリックして、ハンドラーを削除します。ハンドラーが「**使用可能なリスト**」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。

デフォルト宛先の指定

内部パートナーまたは外部パートナーの宛先を作成したら、デフォルト宛先として宛先の 1 つを選択します。

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**宛先**」をクリックします。
2. 「**作成**」をクリックします。
3. 「**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。
4. 「**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**」などの他のタイプの宛先に対しても設定できます。
5. 「**保管**」をクリックします。

第 4 章 コミュニティー接続とユーザーの管理: アカウント管理

アカウント管理モジュールの機能により、WebSphere Partner Gateway の使用方法と使用者を制御します。

例えば、コミュニティー・コンソールとその各機能へのアクセスを制御できます。重要なイベントが発生したときのアラートの受信者を制御できます。イベントの例としては、「パートナー接続が見つかりません (Partner Connection Not Found)」、「RosettaNet 検証エラー」、「文書の送達に失敗しました」などがあります。

また、このモジュールを使用して、パートナー・プロファイル、証明書、宛先、ユーザー、グループ、連絡先、住所、アラート、および B2B 機能も保守します。(B2B 機能では、システムが送受信できるビジネス・プロセスのタイプを定義します。) 構成プロセスを行ったことがあれば、既にこれらの機能を利用しています。

表 4. アカウント管理機能

使用する機能
『宛先の管理』 61 ページの『証明書の管理』 61 ページの『グループの管理』 63 ページの『ユーザーの管理』 65 ページの『連絡先の管理』 66 ページの『アラートの管理』 68 ページの『住所の管理』

宛先の管理

宛先機能を使用すると、文書を適切な宛先に送付するときに使用される宛先情報を表示できます。この機能では、ターゲット URI、トランスポート・プロトコル、および宛先の状況を表示できます。

重要: 一部の宛先の値は、選択されたトランスポート・プロトコルによって異なります。制限は、値テーブルと手順に記述されています。

宛先のリストの表示

システムの宛先リストを表示するには、**「アカウント管理」** > **「プロファイル」** > **「宛先」**をクリックします。

宛先詳細の表示または編集

重要: 宛先を使用不可に設定する場合、その宛先と関連したパートナー接続も使用不可になります。宛先は機能しません。宛先をオフラインに設定すると、宛先をオンラインに戻すまで文書はキューに入ります。

1. **「アカウント管理」** > **「プロファイル」** > **「宛先」**をクリックします。「宛先リスト」画面が表示されます。

2. 「詳細の表示」アイコンをクリックして、宛先の詳細を表示します。
3. 「編集」アイコンをクリックして、宛先の詳細を編集します。
4. 必要に応じて情報を編集します。次の表に、宛先の値を示します。

表 5. 宛先画面の値

値	説明
宛先名	宛先の名前。 注: 「宛先名」はユーザー定義のフリー・フォーマット・フィールドです。混乱の可能性を避けるため、個々の宛先には異なる名前を使用することをお勧めします。
トランスポート	文書を送付するために使用されるプロトコル。
ターゲット URI	宛先の URI。
「オンライン」または「オフライン」	オフラインにした場合、宛先がオンラインになるまで、文書はキューに入れられます。
状況	「使用可能」または「使用不可」です。状況が使用不可に設定された宛先による文書経路指定の処理は失敗します。
デフォルト	デフォルト宛先を示します。

5. **「保管」**をクリックします。

デフォルト宛先の表示、選択、または編集

1. **「アカウント管理」** > **「プロファイル」** > **「宛先」**をクリックします。「宛先リスト」画面が表示されます。
2. 画面の右上隅にある**「デフォルト宛先の表示」**をクリックします。「デフォルト宛先リスト」画面が表示されます。
3. ドロップダウン・リストを使用して、1 つ以上のデフォルト宛先を選択するか変更します。
4. **「保管」**をクリックします。

宛先の使用場所の表示

個々の宛先全体が使用されている場所の詳細を表示するには、次の手順を使用します。

1. **「アカウント管理」** > **「プロファイル」** > **「宛先」**をクリックします。
2. 宛先リストから適切な宛先を選び、その宛先に対する**「使用場所 (Whereused)」**アイコンをクリックします。選択した宛先全体が使用されている場所のリストが表示されます。

   注: 選択した宛先を使用するチャネルが多数あるかもしれないため、この画面はページング情報と共に提供されます。各ページには、最大で 10 接続が表示されます。

宛先の削除

宛先の削除機能は、デフォルト宛先を除くすべての宛先に使用できます。宛先を削除するには、次の手順を使用します。

1. **「アカウント管理」** > **「プロファイル」** > **「宛先」**をクリックします。

2. 宛先リストから削除する宛先を選び、その宛先に対する「**削除**」アイコンをクリックします。

   注: 「**削除**」アイコンはデフォルト宛先には使用できません。また、削除操作が許可されるのは、選択した宛先が接続で使用されていない場合のみです。宛先の使用法についての情報が必要な場合は、 60 ページの『宛先の使用場所の表示』を参照してください。

3. 削除確認用の警告ウィンドウで、「**OK**」をクリックします。

証明書の管理

ここでは、コミュニティー・コンソールを使用して、デジタル証明書の表示、編集、および削除を行う手順について説明します。

デジタル証明書の詳細の表示と編集

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**証明書**」をクリックします。既存のデジタル証明書のリストが表示されます。
2. 「詳細の表示」アイコンをクリックして、証明書の詳細を表示します。「証明書の詳細」画面が表示されます。
3. 「編集」アイコンをクリックして、証明書を編集します。
4. 必要に応じて編集します。
5. 「**保管**」をクリックします。

デジタル証明書の使用不可化

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**証明書**」をクリックします。「証明書リスト」画面が表示されます。
2. 「詳細の表示」アイコンをクリックして、証明書の詳細を表示します。「証明書の詳細」画面が表示されます。
3. 「編集」アイコンをクリックして、証明書を編集します。
4. 「**使用不可**」をクリックします。
5. 「**保管**」をクリックします。

グループの管理

コミュニティー・コンソールを使用して、グループの表示、編集、および削除を行うことができます。この機能は、社内/社外パートナーの管理者グループ・ユーザーにのみ使用できます。

グループ・メンバーシップの表示とグループへのユーザーの割り当て

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**グループ**」をクリックします。「グループ・リスト」画面が表示されます。

表 6. 「グループ・リスト」画面の値

値	説明
名前	グループ名。
説明	グループの説明。
グループ・タイプ	「システム」などのタイプ。

2. 「メンバーの表示」アイコンをクリックして、グループ内のメンバーのリストを表示します。このアイコンが表示されない場合、グループにメンバーはありません。サブメニューの「メンバーシップ」をクリックします。
3. 「編集」アイコンをクリックして、グループ内のユーザーを編集します。
4. 「**グループへの追加**」をクリックして、ユーザーをグループに割り当てます。
5. 「編集オフ (Edit off)」アイコンをクリックして保管し、終了します。

グループ・アクセス権の表示、編集、または割り当て

管理者グループ・ユーザーであっても、ユーザーとグループのグループ・アクセス権を設定することはできません。ほかのグループのアクセス権は、常に管理者アクセス権より低いか同等となります。例えば管理者にアドレスへの読み取り専用アクセス権があった場合、ほかのグループのアクセス権は「権限なし」または「読み取り専用」となります。

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**グループ**」をクリックします。「グループ・リスト」画面が表示されます。
2. 「アクセス権の表示」アイコンをクリックして、グループのアクセス権を表示します。選択したグループのアクセス権のリストが表示されます。
3. 機能ごとに「**アクセスなし**」、「**読み取り専用**」、または「**読み取り/書き込み**」を選択します。
4. 「**保管**」をクリックします。

グループの詳細の表示または編集

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**グループ**」をクリックします。「グループ・リスト」画面が表示されます。
2. 「詳細の表示」アイコンをクリックして、グループの詳細 (名前および説明) を表示します。「グループの詳細」画面が表示されます。
3. 「編集」アイコンをクリックして、グループの詳細を編集します (システム生成のグループは編集できません)。
4. 必要に応じて編集します。
5. 「**保管**」をクリックします。

制約事項: 管理者グループとデフォルト・グループはシステムで生成されます。編集や削除はできません。ハブ管理者にはさらにハブ管理者グループがあります。

グループの削除

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**グループ**」をクリックします。「グループ・リスト」画面が表示されます。

2. 「詳細の表示」アイコンをクリックして、グループの詳細を表示します。「グループの詳細」画面が表示されます。
3. 「編集」アイコンをクリックして、グループの詳細を編集します。
4. 「**削除**」をクリックします。削除を確認します。

警告: 管理者グループとデフォルト・グループはシステムで生成されます。編集や削除はできません。

ユーザーの管理

この機能を使用すると、パートナー・プロファイルを表示し、編集できます。この機能は、社内/社外パートナーの管理者グループ・ユーザーにのみ使用できます。

注: この機能を使用して、ユーザーの新規パスワードを割り当てたり、自動生成したりできます。

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**ユーザー**」をクリックします。「ユーザー・リスト」画面が表示されます。

次の表に、「ユーザー・リスト」画面の値を示します。

表 7. 「ユーザー・リスト」画面の値

値	説明
ユーザー名	コンソール・ログイン名。
氏名	ユーザーの氏名。
E メール	アラート通知に使用される E メール・アドレス。
サブスクライブ済み	このオプションにチェックマークを付けると、1 つ以上のアラートがユーザーに割り当てられます。ユーザーがシステムから除去されると、このユーザーへのすべてのアラート・サブスクリプションも除去されます。
ログイン状況	状況を使用可能にすると、ユーザーはコンソールにログインできます。

2. 「詳細の表示」アイコンをクリックして、ユーザーの詳細を表示します。
3. 「編集」アイコンをクリックして、ユーザーの詳細を編集します。
4. 必要に応じて情報を編集します。次の表に、「ユーザーの詳細」画面の値を示します。

表 8. 「ユーザーの詳細」

値	説明
ユーザー名	コンソール・ユーザーのログイン名。
使用可能	コンソールへのアクセスを使用可能または使用不可にします。
名	ユーザーの名。
姓	ユーザーの姓。
E メール	アラート通知に使用される E メール・アドレス。
電話番号	ユーザーの電話番号。
FAX 番号	ユーザーの FAX 番号。
言語ロケール	ユーザーの地域を選択します。デフォルト値は、ハブ管理者によって設定されたロケールです。
書式ロケール	ユーザーの国を選択します。デフォルト値は、ハブ管理者によって設定されたロケールです。
時間帯	ユーザーの時間帯を選択します。デフォルト値は、ハブ管理者によって設定された時間帯です。
アラート状況	使用可能にすると、このユーザーはサブスクライブしたすべてのアラートを受信します。このユーザーがアラートをまったく受信しないようにするには、「使用不可」を選択します。
サブスクライブ済み	この値はシステムによって入力されます。
可視	ユーザーの組織内でのみユーザーを表示できるようにするには、「ローカル」を選択します。ユーザーを組織とマネージャーに表示できるようにするには、「グローバル」を選択します。

注: インストールと始動後のデフォルトのシステム・ロケールと時間帯は、「英語 (米国) (English (United States))」と「UTC」です。システムでは、時間帯計算に UTC を使用します。デフォルトの UTC はシステム・レベルでは変更できません。しかし、すべてのユーザーはコミュニティー・コンソール内に表示される時間帯を変更できます。

Hubadmin ユーザーは、はじめてシステムにログインすると、システム・ロケールと時間帯を選択します (英語、UTC)。Hubadmin ユーザーはシステム構成を担当するスーパーユーザーであるため、Hubadmin ユーザーが選択したコミュニティー・コンソール・ロケールと時間帯はすべてのコミュニティー・コンソール・ユーザーの新しいデフォルト値になります。個々のユーザーも、必要に応じて自分のロケールと時間帯を変更できます。

5. 「**保管**」をクリックします。

ユーザーの削除

ユーザーの削除に適したアクセス権を持つ必要があります。この機能を使用すると、HUBADMIN を除くすべてのユーザーを削除することができます。

この機能を使用して、次のようにユーザーを削除します。

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**ユーザー**」をクリックします。
2. 削除したいユーザーに対する「**削除**」アイコンをクリックします。
3. 警告ウィンドウで「**OK**」をクリックして、削除を確認します。「**キャンセル**」をクリックすると、削除操作は打ち切られます。

連絡先の管理

連絡先機能を使用すると、主要担当者の連絡先情報を表示し、編集できます。

組織のサイズによっては、発生したイベントのタイプによって異なる連絡先への通知が必要になることがあります。例えば、文書の検証が失敗した場合、問題を評価するため、セキュリティー担当者に通知する必要があります。内部パートナーの送信が通常の範囲を超える場合、ネットワーク管理者に通知し、送信量の増加が効率的に処理されるようにします。

連絡先の詳細の表示と編集

1. **「アカウント管理」** > **「プロファイル」** > **「連絡先」**をクリックします。現在の連絡先のリストが表示されます。

   次の表に、「連絡先」画面に表示される値を示します。

表 9. 「連絡先リスト」画面の値

値	説明
氏名	連絡先の氏名。
連絡先タイプ	連絡先の役割を記述します (「B2B リード」、「ビジネス・リード」など)。
E メール	アラート通知に使用される E メール・アドレス。
可視	• 「ローカル」 - 連絡先はユーザーの組織にしか表示されない。 • 「グローバル」 - 連絡先はハブ管理者と内部パートナーに表示される。両者とも連絡先をアラートにサブスクライブできます。
サブスクライブ済み	このオプションを選択すると、1 つ以上のアラートがこの連絡先に割り当てられます。連絡先がシステムから除去されると、この連絡先へのすべてのアラート・サブスクリプションも除去されます。
アラート状況	「アラート状況」を使用可能にした場合、この連絡先はサブスクライブしたすべてのアラートを受信します。

2. 「詳細の表示」アイコンをクリックして、連絡先の詳細を表示します。「連絡先の詳細」画面が表示されます。
3. 「編集」アイコンをクリックして、連絡先の詳細を編集します。

4. 必要に応じて情報を編集します。次の表に、連絡先の値を示します。

表 10. 連絡先の詳細

値	説明
名	連絡先の名。
姓	連絡先の姓。
住所	郵便番号、都道府県名、市区町村名、番地を含む連絡先の住所。
連絡先タイプ	連絡先の役割を記述します (「B2B リード」、「ビジネス・リード」など)。
E メール	アラート通知用の連絡先の E メール・アドレス。
電話番号	連絡先の電話番号。
FAX 番号	連絡先の FAX 番号。
アラート状況	このオプションを使用可能にした場合、この連絡先はサブスクライブしたすべてのアラートを受信します。この連絡先がアラートをまったく受信しないようにするには、「使用不可」を選択します。
サブスクライブ済み	この値はシステムによって入力されます。
可視	• 「ローカル」 - 連絡先はユーザーの組織にしか表示されない。 • 「グローバル」 - 連絡先はハブ管理者と内部パートナーに表示される。両者とも連絡先をアラートにサブスクライブできます。

5. 「**保管**」をクリックします。

連絡先の除去

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**連絡先**」をクリックします。現在の連絡先のリストが表示されます。
2. 「削除」アイコンをクリックして、該当する連絡先を削除します。

アラートの管理

WebSphere Partner Gateway のアラートを使用すると、受信した伝送量に異常な変動があったり、ビジネス文書処理エラーが発生したときに、主要な担当者に通知できます。

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。

アラート詳細と連絡先の表示または編集

内部パートナーは、アラート所有者 (アラートの作成者) とは関係なく、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」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。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」画面が表示されます。
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. パートナーを選択します (内部パートナーまたはハブ管理者のみ)。内部パートナーは、アラート所有者とは関係なく、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. 「**保管**」をクリックします。

アラートの検索

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」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。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 11. 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	使用可能、使用不可、またはすべてのアラート。
サブスクライブした連絡先	アラートの割り当てられた連絡先。「サブスクライバーあり」、「サブスクライバーなし」、または「すべて」を選択します。
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 12. 内部パートナーと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	アラートの適用先のパートナー。
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	使用可能、使用不可、またはすべてのアラート。
サブスクライブした連絡先	アラートの割り当てられた連絡先。「サブスクライバーあり」、「サブスクライバーなし」、または「すべて」を選択します。
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。検索条件に合致するアラートのリストが表示されます (存在する場合)。

アラートの使用不可化または使用可能化

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」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。アラート名を入力します。

3. 「**検索**」をクリックします。検索条件に合致するアラートのリストが表示されます (存在する場合)。
4. アラートを見つけ、「状況」の下にある「**使用不可**」または「**使用可能**」をクリックします。ハブ管理者とアラート所有者 (アラートの作成者) にのみ、アラート状況を編集する権限があります。

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」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。アラート名を入力します。
3. 「**検索**」をクリックします。検索条件に合致するアラートのリストが表示されます (存在する場合)。
4. アラートを見つけ、「削除」アイコンをクリックして削除します。ハブ管理者とアラート所有者 (アラートの作成者) のみが、アラートを除去できます。

イベント通知

WebSphere Partner Gateway でイベント・アラートを構成できます。イベント・アラートを構成した場合、イベントが発生すると、イベントのソース・パートナーとターゲット・パートナーの両方に通知されます。アラート通知では 2 つのオプションを選択できます。次のとおりです。

- すべての関係者に通知
- サブスクライブ済み連絡先にのみ通知

「すべての関係者に通知」オプションを選択すると、アラート機能により、イベントのソース・パートナーの連絡先とターゲット・パートナーの連絡先のほか、アラート所有者の連絡先にも自動的に通知されます。ユーザーは、このモードが選択されている場合、「サブスクライブ済み連絡先」を指定する必要はありません (また、指定することもできません)。「サブスクライブ済み連絡先にのみ通知」モードを選択すると、アラート機能によりサブスクライブ済み連絡先にのみアラートが送信されます。

通知先の関係者を決定した後は、次の機能を選択することができます。

- アラートの即時送信
- アラートのバッチ処理 (カウントまたは時間ごと)

注: この追加機能を使用するには、アラート E メール・サーバーを構成する必要があります。このサーバーの構成について詳しくは、「*System Administrator Guide*」を参照してください。

住所の管理

この機能を使用すると、パートナー・プロファイルの住所を管理できます。

住所の編集

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**住所**」をクリックします。「住所」画面が表示されます。

2. 編集する住所を見つけ、「編集」アイコンをクリックします。
3. 必要な変更を行います。次の表に、住所の値を示します。

表 13. 住所の値

値	**説明**
住所のタイプ	「会社」、「広告」、および「技術」。
住所	郵便番号、都道府県名、市区町村名、および番地を含む住所。

4. 「**保管**」をクリックします。

住所の削除

1. 「**アカウント管理**」 > 「**プロファイル**」 > 「**住所**」をクリックします。「住所」画面が表示されます。
2. 削除する住所を見つけ、「削除」アイコンをクリックします。
3. 住所の削除を確認します。

第 5 章 イベントおよび文書の表示: ビューアー

ビューアーにより、システム全体の正常性を表示できます。イベント解決のためのトラブルシューティング・ツールにもなります。

ビューアー・モジュールには、次の機能が組み込まれています。

- 『イベント・ビューアー』
- 74 ページの『AS ビューアー』
- 77 ページの『ebMS ビューアー』
- 79 ページの『RosettaNet ビューアー』
- 81 ページの『文書ビューアー』
- 86 ページの『宛先キュー』

RosettaNet ビューアーおよび AS ビューアーには、ハブ管理者用の検索条件が追加されています。詳しくは、「*管理者ガイド*」を参照してください。

注: パートナーという用語は、内部パートナーなどのハブ・コミュニティー・メンバーを識別するときに、ビューアー画面で使用します。

イベント・ビューアー

イベント・ビューアーを使用すると、時刻、日付、イベント・タイプ、イベント名、およびイベント・ロケーションごとにイベントを検索できます。ハブ管理者は、パートナー、ソース IP、およびイベント ID ごとに検索することもできます。

イベント・ビューアーが生成するデータにより、特にイベント名、タイム・スタンプ、ソース IP を識別し、イベントや文書の詳細を表示して問題を診断できます。ロー文書も表示できます。これにより、フィールド、値、およびエラーの理由を確認できます。

イベントは、システムに何らかの異常が発生したことを通知する役割を果たします。イベントにより、システムの動作または機能が正常であったかどうか (例えば、パートナーがシステムに正常に追加されたか、パートナーの接続は内部パートナーと外部パートナーとの間に正常に作成されたか) がわかります。イベントによって問題を確認することもできます (例えば、システムが文書を処理できなかった、またはシステムが文書内で重要ではないエラーを検出したなど)。大半の文書は何度も再送されるため、文書に障害が発生してアラートが生成された場合、このアラートは、それ以降同様な障害が発生しないよう調査して修正する必要があるという意味になります。

WebSphere Partner Gateway には、事前定義イベントが用意されています。イベント・ベースのアラートを作成するには、この製品のアカウント管理モジュールに組み込まれているアラート機能を使用します。この処理では、気がかりなイベントを指定します。次に、同じアカウント管理モジュールに用意されている連絡先機能を使用して、これらのイベントが発生した場合にシステムから通知されるスタッフのメンバーを指定します。

イベント・ビューアーは、具体的な検索条件に基づいてイベントを表示します。特定のイベントを検索して、そのイベントの発生原因を調査できます。イベント・ビューアーを使用すると、時刻、日付、イベント・タイプ (デバッグ、通知、警告、エラー、重大)、イベント名 (210031 など)、およびイベント・ロケーションごとにイベントを検索できます。

イベント・ビューアーを介して使用できるデータには、イベント名、タイム・スタンプ、ユーザー、およびパートナーの情報があります。これらのデータは、イベントの発生元となる文書またはプロセスを特定するのに役立ちます。イベントが文書に関連している場合は、ロー文書も表示できます。これにより、フィールド、値、およびエラーの理由を確認できます。

イベント・タイプ

WebSphere Partner Gateway には、次のイベント・タイプがあります。

表 14. イベント・タイプ

イベント・タイプ	説明
デバッグ	デバッグ・イベントは、下位のシステム動作およびサポートのために使用されます。このイベントの可視性および用途は、ユーザーのアクセス権レベルによって変わります。すべてのユーザーがデバッグ・イベントへのアクセス権を所有しているわけではありません。
通知	通知イベントは、システム動作が正常に終了すると生成されます。これらのイベントは、現在処理中の文書の状況を示すときにも使用されます。通知イベントでは、ユーザー処置は必要ありません。
警告	警告イベントが発生するのは、文書の処理またはシステムの機能において、動作を継続できる重大ではない異常が発生した場合です。
エラー	エラー・イベントが発生するのは、文書の処理において、プロセスの終了を引き起こす異常が発生した場合です。
重大	重大イベントは、システム障害によってサービスが終了すると生成されます。重大イベントが生成されると、サポート要員による操作が必要になります。

イベント・ビューアー・タスクの実行

表 15. イベント・ビューアーのタスク

実行する作業	参照先
イベントを検索する。	72 ページ
イベントの詳細を表示する。	73 ページ

イベントの検索

1. **「ビューアー」** > **「イベント・ビューアー」**の順にクリックします。

   イベントは、「イベント・ビューアー検索」画面の左から右へ重大度の順に列記されます。左側に表示されている「通知」は、最も重大度の低いイベント・タイプです。逆に、右側に表示されている「重大」は、重大度が最も高いイベント・タイプです。(デバッグ・イベントは必ずしもすべてのユーザーに表示されるわけではありません。) イベントを選択すると、そのイベントと、それより重大度の高いすべてのイベントがイベント・ビューアーに表示されます。例えば、検索

条件に警告イベント・タイプを選択すると、警告、エラー、重大のイベントが表示されます。通知イベントを選択すると、すべてのイベント・タイプが表示されます。

2. ドロップダウン・リストから検索条件を選択します。

表 16. イベントの検索条件

値	説明
開始日および開始時刻 (Start date and time)	最初のイベントが発生した日時。デフォルト値は 10 分前です。
終了日および終了時刻 (End date and time)	最後のイベントが発生した日時。
パートナー	すべてのパートナーまたは特定のパートナー (内部パートナーのみ) を選択します。
イベント・タイプ	イベントの種類。デバッグ、通知、警告、エラー、重大のいずれかです。
イベント名	選択されたイベント・タイプに基づいて使用可能なイベント名を検索します。
イベント・ロケーション	イベントが生成された場所。すべて、不明、生成元、生成先があります。
ソート順	結果をソートするときに使用する値。
「昇順」または「降順」	昇順または降順でソートします。
ページごとの結果件数	1 ページに表示されるレコードの数。
最新表示	デフォルト設定はオフです。「最新表示」をオンにすると、イベント・ビューアーは最初に新規照会を実行し、それ以降は最新表示モードを維持します。
最新表示頻度	検索結果の更新頻度を制御します (内部パートナーのみ)。

3. 「**検索**」をクリックします。イベントのリストが表示されます。

ヒント: イベント・リストは、イベント・ビューアー画面の上部で選択したイベント・タイプに基づいて、再度フィルター処理できます。次の画面の最新表示を実行すると、新たに選択されたイベント・タイプが反映されます。

イベント詳細の表示

1. 「**ビューアー**」 > 「**イベント・ビューアー**」の順にクリックします。
2. ドロップダウン・リストから検索条件を選択します。
3. 「**検索**」をクリックします。イベントのリストが表示されます。
4. 表示するイベントの横にある「詳細の表示」アイコンをクリックします。イベントの詳細と関連文書が表示されます。
5. 表示する文書がある場合は、その文書の横にある「詳細の表示」アイコンをクリックします。
6. ロー文書がある場合、それを表示するには、「ロー文書の表示 (Display raw document)」アイコンをクリックします。
7. 検証エラーを表示するには、「検証エラーの表示」アイコンをクリックします。

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、1 次証明書および 2 次証明書の両方とも無効です。証明書の有効期限が切れたか、失

効した可能性があります。証明書の有効期限が切れたか、失効した場合、該当するイベント (有効な暗号化証明書が見つかりません) がイベント・ビューアーに表示されます。

ヒント: 「イベント・ビューアー詳細 (Event Viewer Detail)」に重複文書イベントが表示された場合は、「文書の詳細」の 「元文書の表示 (View original document)」アイコンをクリックして以前に送信された元文書を表示します。

AS ビューアー

AS1、AS2 または AS3 通信プロトコルを使用して、文書のトランスポート情報を検索および表示するには、AS ビューアーを使用します。メッセージ ID、Message Disposition Notification (MDN) の宛先 URI および状況、および文書の詳細 (文書およびラッパー) を表示できます。

AS ビューアーを使用して、AS1、AS2 または AS3 (Applicability Statement 1 または 2) 通信プロトコルを使用する、パッケージ化された B2B トランザクションおよび B2B プロセスの詳細を表示することもできます。B2B プロセスのコレオグラフィーと、関連のビジネス文書、確認通知シグナル、プロセス状態、HTTP ヘッダー、および送信された文書の内容を表示できます。

SMTP を使用するデータ伝送の標準を定義する先行版の AS1 と同様に、AS2 は、HTTP を使用するデータ伝送の標準を定義します。

AS2 では、データの接続方法、配信方法、検証方法、およびデータへの応答方法が定められています。AS2 は、文書の内容とは関係なく、文書の転送にのみ関係があります。AS2 では、HTTP または HTTPS を使用し、インターネットを介して文書を転送できるよう、文書にラッパーが作成されます。文書とラッパーをまとめてメッセージと呼びます。AS2 には、HTTP パケットのセキュリティーを確保し、暗号化を行う機能があります。AS2 は、配信が保証されている暗号化の基本機能を備えています。AS3 は、FTP または FTPS を介して文書を安全に伝送するための新しい標準です。

AS2 の重要なコンポーネントは、MDN (Message Disposition Notification) と呼ばれる受信機構です。この仕組みにより、文書の送信側は、受信側が文書を正常に受信することを保証されます。送信側は、MDN の返送方法 (同期または非同期、符号ありまたは符号なし) を指定します。

AS ビューアーにより、「メッセージ ID」、「タイム・スタンプ」、「文書タイプ」、「宛先タイプ」、「同期の状況 (Synchronous status)」、ならびに文書の詳細を表示できます。文書の詳細を表示すると、追加の文書処理情報が表示されます。

AS ビューアー・タスクの実行

表 17. AS1/AS2 ビューアーのタスク

実行する作業	参照先
AS メッセージの検索	『メッセージの検索』 ページ 76 ページの『メッセージの詳細の表示』 ページ
ロー文書の表示	

メッセージの検索

1. 「**ビューアー**」 > 「**AS ビューアー**」の順にクリックします。「AS ビューアー」画面が表示されます。

2. ドロップダウン・リストから検索条件を選択します。

表 18. AS ビューアーの検索条件

値	説明
開始日および開始時刻 (Start Date and Time)	処理が開始された日時。
終了日および終了時刻 (End Date and Time)	処理が完了した日時。
ソース・パートナー	伝送パートナーを示します (内部パートナーのみ)。
ターゲット・パートナー	受信側パートナーを示します。
検索場所:	検索対象の文書が、ソースまたはターゲットの文書タイプかどうかを指定します。
AS ソース・ビジネス ID	ソースのパートナーのビジネス識別番号 (例: Duns)。
ペイロード・ソース・ビジネス ID	ペイロード・ソースの識別番号。
動作モード	実動、テスト、RN シミュレーター外部パートナー、または RN シミュレーター内部パートナー。テストが使用できるのは、テスト宛先タイプをサポートするシステムのみです。
パッケージ	文書フォーマット、パッケージ化、暗号化、およびコンテンツ・タイプ識別番号について説明します。
プロトコル	パートナーに対して使用できる文書フォーマット (例: XML の RosettaNet)。
文書タイプ	特定のビジネス・プロセス。
メッセージ ID	AS1、AS2 または AS3 でパッケージ化された文書に割り当てられた ID 番号。検索条件には、アスタリスク (*) のワイルドカードを使用できます。最大長は 255 文字です。
文書 ID	文書に割り当てられた固有の識別番号。
同期/非同期	同期または非同期モードで受信した文書を検索します。同期モードでは、イニシエーターと文書マネージャーとの接続は、要求と Message Disposition Notification (MDN) を含むトランザクションが完了するまで、開通状態を維持します。
MDN 状況	このフィールドでは、このメッセージについての MDN の状況を選択できます。
ソート順	この値によって結果をソートします。
「降順」または「昇順」	「昇順」 - 最も古いタイム・スタンプまたはアルファベットの最後を最初に表示します。 「降順」 - 最新のタイム・スタンプまたはアルファベットの先頭を最初に表示します。
ページごとの結果件数	1 ページに表示されるレコードの数を選択するときに使用します。

3. 「**検索**」をクリックします。メッセージのリストが表示されます。

メッセージの詳細の表示

1. 「**ビューアー**」 > 「**AS ビューアー**」の順にクリックします。「AS ビューアー」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。
3. 「**検索**」をクリックします。メッセージのリストが表示されます。
4. 表示するメッセージの横にある「詳細の表示」アイコンをクリックします。メッセージとその関連文書の詳細が表示されます。

表 19. AS ビューアー: パッケージの詳細

値	説明
メッセージ ID	AS1、AS2 または AS3 でパッケージ化された文書に割り当てられた ID 番号。この番号で識別できるのは、パッケージのみです。文書自体には、文書の詳細を表示すると表示される文書 ID 番号が別個に存在します。最大長は 255 文字です。
ソース・パートナー	ビジネス・プロセスを開始するパートナー。
ターゲット・パートナー	ビジネス・プロセスを受け取るパートナー。
開始時のタイム・スタンプ (Initiating Time Stamp)	文書の処理が開始された日時。
宛先タイプ	実動またはテスト。テストが使用できるのは、テスト宛先タイプをサポートするシステムのみです。
MDN URI	MDN の宛先アドレス。このアドレスは、HTTP URI または E メール・アドレスとして指定できます。
MDN 処理テキスト	このテキストは、発信メッセージの受信状況 (正常または失敗) を示します。例を次に示します。 • Automatic-=action/MDN-sent-automatically; processed. • Automatic-action/MDN-sent- automatically;processed/ Warning;duplicate-document. • Automatic-action/MDN-sent- automatically;processed/ Error;description-failed. • Automatic-action/MDN-sent- automatically;failed:unsupported MIC-algorithms.

5. (オプション) ロー文書を表示するには、「ロー文書の表示 (Display raw document)」アイコンをクリックします。

ebMS ビューアー

ebXML Message Service (ebMS) 機能は、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。 この機能により、独自開発の技術やソリューションに依存することなく、ビジネス・メッセージを交換するための確実な手段を得ることができます。 ebXML メッセージには、メッセージ・ヘッダー (ルーティングや配信に必要) およびペイロード・セクションの構造が記述されています。 ebMS は、ebXML 取引先間でビジネス・メッセージを交換するための標準的な方法を提供します。 ebXML メッセージは、MIME/Multipart メッセージ・エンベロープに依存しない通信プロトコルです。

ebMS ビューアー・タスクの実行

表 20. ebMS ビューアーのタスク

実行する作業	参照先
ebMS プロセスを検索する。	78 ページの『ebMS プロセスの検索』
ebMS プロセスを表示する	78 ページの『ebMS プロセスの詳細の表示』
ロー文書を表示する	79 ページの『ロー文書の表示』
文書状況を表示する	79 ページの『文書状況の表示』

ebMS プロセスの検索

1. 「**ビューアー**」 > 「**ebMS ビューアー**」の順にクリックします。「ebMS ビューアー検索」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。

値	説明
開始日および開始時刻 (Start Date and Time)	処理が開始された日時。
終了日および終了時刻 (End Date and Time)	処理が完了した日時。
ソース・パートナー	送信側パートナーを示します。
ターゲット・パートナー	受信側パートナーを示します。
ソース・ビジネス ID	開始側のパートナーのビジネス識別番号 (例: DUNS)。
動作モード	実動、テスト、RN シミュレーター外部パートナー、または RN シミュレーター内部パートナー。テストが使用できるのは、テスト宛先タイプをサポートするシステムのみです。
プロトコル	パートナーに対して使用できるプロトコル。
文書タイプ	処理される文書タイプ。
会話 ID	プロセスに割り当てられた固有の識別情報。検索条件には、アスタリスク (*) のワイルドカードを使用できます。
ソート順	「受信時刻のタイム・スタンプ (Received Time Stamp)」などによって結果をソートします。
「降順」または「昇順」	「昇順」 - 最も古いタイム・スタンプまたはアルファベットの最後を最初に表示します。 「降順」 - 最新のタイム・スタンプまたはアルファベットの先頭を最初に表示します。
ページごとの結果件数	1 ページ当たりの結果の数を表示します。

3. 「**検索**」をクリックします。検索条件に合致した ebMS プロセスが表示されます。

ebMS プロセスの詳細の表示

1. 「**ビューアー**」 > 「**ebMS ビューアー**」の順にクリックします。「ebMS ビューアー」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。
3. 「**検索**」をクリックします。検索結果が表示されます。

表 21. ebMS ビューアーの検索条件の値

値	説明
パートナー	ビジネス・プロセスに関与しているパートナー。
ソース・タイム・スタンプ	最初の文書の処理が開始された日時。
文書タイプ	特定のビジネス・プロセス (例: ebMS 2.0 : ALMService Production)
動作モード	動作のモード (例: 実動)
会話 ID	このイベントに割り当てられた固有の識別番号

ロー文書の表示

ロー文書を表示するには、以下の手順に従います。

1. 「**ビューアー**」 > 「**ebMS ビューアー**」の順にクリックします。
2. ドロップダウン・リストから検索条件を選択します。 78 ページの『ebMS プロセスの検索』を参照してください。
3. 「**検索**」をクリックします。
4. 「**凡例**」セクションの下にある「**ロー文書を参照するにはここをクリックしてください**」のアイコンをクリックします。

- 処理できなかった文書のトラブルシューティングを行うには、85 ページの『データ検証エラーの表示』を参照してください。
- ロー文書のビューアーには、ロー文書に HTTP ヘッダーが付いた状態で表示されます。

文書状況の表示

1. 「**ビューアー**」 > 「**ebMS ビューアー**」の順にクリックします。
2. ドロップダウン・リストから検索条件を選択します。 78 ページの『ebMS プロセスの検索』を参照してください。
3. 「**検索**」をクリックします。
4. 「**状況の要求**」をクリックします。
5. 「**状況の表示**」をクリックします。

RosettaNet ビューアー

イベントを生成した特定のプロセスを検索するには、RosettaNet ビューアーを使用します。目的のプロセスを特定したら、プロセスの詳細とロー文書を表示できます。

RosettaNet は、e-ビジネス取引の業界標準を作成した企業グループです。Partner Interface Processes (PIP) では、ハブ・コミュニティーのメンバー間でのビジネス・プロセスを定義します。各 PIP では、特定のビジネス文書と、内部パートナーと外部パートナーとの間でこの文書がどのように処理されるかが定められます。

RosettaNet ビューアーは、ビジネス・プロセスを構成する文書のコレオグラフィーを表示します。RosettaNet ビューアーを使用して表示できる値には、プロセスの状況、詳細、ロー文書、関連のプロセス・イベントなどがあります。

RosettaNet ビューアーは、特定の検索条件に基づいてプロセスを表示します。

RosettaNet ビューアー・タスクの実行

表 22. RosettaNet ビューアーのタスク

実行する作業	参照先
RosettaNet プロセスを検索する。	80 ページ
RosettaNet プロセスの詳細を表示する。	80 ページ
ロー文書を表示する。	81 ページ

RosettaNet プロセスの検索

1. 「**ビューアー**」 > 「**RosettaNet ビューアー**」の順にクリックします。「RosettaNet ビューアー検索」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。検索条件は以下のとおりです。

表 23. RosettaNet の検索条件

値	説明
開始日および開始時刻 (Start Date and Time)	処理が開始された日時。
終了日および終了時刻 (End Date and Time)	処理が完了した日時。
ソース・パートナー	送信側パートナーを示します。
ターゲット・パートナー	受信側パートナーを示します。
ソース・ビジネス ID	開始側のパートナーのビジネス識別番号 (例: DUNS)。
動作モード	実動、テスト、RN シミュレーター外部パートナー、または RN シミュレーター内部パートナー。テストが使用できるのは、テスト宛先タイプをサポートするシステムのみです。
プロトコル	パートナーに対して使用できるプロトコル。
文書タイプ	処理される文書タイプ。
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。検索条件には、アスタリスク (*) のワイルドカードを使用できます。
ソート順	「受信時刻のタイム・スタンプ (Received Time Stamp)」などによって結果をソートします。
「降順」または「昇順」	「昇順」 - 最も古いタイム・スタンプまたはアルファベットの最後を最初に表示します。 「降順」 - 最新のタイム・スタンプまたはアルファベットの先頭を最初に表示します。
ページごとの結果件数	1 ページ当たりの結果の数を表示します。

3. 「**検索**」をクリックします。検索条件に合致した RosettaNet プロセスが表示されます。
4. 表示する ebMS プロセスの横にある「詳細の表示」アイコンをクリックします。選択したプロセスの詳細と関連文書が表示されます。
5. 表示する文書の横にある「詳細の表示」アイコンをクリックします。文書とその関連イベントの詳細が表示されます。

RosettaNet プロセスの詳細の表示

1. 「**ビューアー**」 > 「**RosettaNet ビューアー**」の順にクリックします。「RosettaNet ビューアー検索」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。

3. 「**検索**」をクリックします。検索結果が表示されます。

表 24. 文書処理の詳細

値	説明
パートナー	ビジネス・プロセスに関与しているパートナー。
タイム・スタンプ	最初の文書の処理が開始された日時。
文書タイプ	特定のビジネス・プロセス (例: RosettaNet (1.1): 3A7)。
宛先タイプ	例えば、実動。
プロセス・インスタンス ID	コミュニティーのメンバーを加入させることによってプロセスに割り当てられる固有の番号。
文書 ID	送信側のパートナーによって割り当てられる専有文書 ID。このフィールドの場所は固定されておらず、文書タイプによって変動します。
ソース・パートナー	開始する側のパートナー。
ターゲット・パートナー	受信する側のパートナー。

4. 表示する RosettaNet プロセスの横にある「詳細の表示」アイコンをクリックします。選択したプロセスの詳細と関連文書が表示されます。
5. 表示する文書の横にある「詳細の表示」アイコンをクリックします。文書とその関連イベントの詳細が表示されます。

ロー文書の表示

1. 「**ビューアー**」 > 「**RosettaNet ビューアー**」の順にクリックします。「RosettaNet ビューアー検索」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。
3. 「**検索**」をクリックします。プロセスのリストが表示されます。
4. 表示するプロセスの横にある「詳細の表示」アイコンをクリックします。選択したプロセスの詳細と関連文書が表示されます。
5. 「文書タイプ」の横にある「ロー文書の表示 (Display raw document)」アイコンをクリックして、ロー文書を表示します。

制約事項: ロー文書のうち、100K を超える部分は切り捨てられます。

ヒント:

- 処理できなかった文書のトラブルシューティングを行うには、85 ページの『データ検証エラーの表示』を参照してください。
- ロー文書のビューアーには、ロー文書に HTTP ヘッダーが付いた状態で表示されます。

文書ビューアー

文書ビューアーは、調査する特定の文書を検索して表示するときに使用します。文書は、日付、時刻、プロセスの種類 (「開始プロセス (From Process)」または「終了プロセス (To Process)」)、パートナーの接続、宛先タイプ、文書の状況、プロトコル、文書タイプ、およびプロセスのバージョンに基づいて検索できます。

XML 形式を使用するカスタム Extensible Markup Language (XML) プロトコルなどの一部のプロトコルでは、文書から情報を抽出して保存し、文書ビューアーを使用

してその情報を検索することができます。XML 形式定義のユーザー検索フィールドの属性は、この目的で使用します。検索フィールドを含む XML 形式を使用して経路指定された文書の場合、検索フィールドを使用して取得された文書の情報を検索のターゲットにすることができます。例としては、購入注文のカスタム XML 文書があります。文書構造についての知識に基づいて、購入注文番号を抽出する検索フィールド付きの XML 形式を定義できます。この XML 形式を使用して文書の経路指定を行う場合には、文書ビューアー検索画面の適切なユーザー定義検索フィールドに購入注文番号を入力することにより、その番号を使用して文書を検索できます。

文書から情報を抽出する Electronic Data Interchange (EDI) 文書の経路指定も定義することができます。これには、ユーザー定義検索フィールドに値が入力されるように、DIS マップを符号化します。

また、文書から情報を抽出するユーザー出口も作成し、検索のターゲットにすることもできます。ユーザー出口メソッド BusinessDocumentInterface.setAttribute() を使用して、ユーザー定義検索フィールドに値を入力します。

検索結果には、検索条件に合致するすべての文書が表示されるため、タイム・スタンプ、プロセス、パートナーの接続、および宛先の種類を特定できます。ロー文書を表示するには、目的の文書を検索して、ビューアーの機能を使用します。また、文書ビューアーを使用して、処理に失敗した文書、または正常に処理された文書を再送することもできます。

文書の検索

1. 「**ビューアー**」 > 「**文書ビューアー**」の順にクリックします。「文書ビューアー検索」画面が表示されます。

2. ドロップダウン・リストから検索条件を選択します。

表 25. 文書ビューアーの検索条件

値	説明
開始日および開始時刻 (Start date and time)	処理が開始された日時。
終了日および終了時刻 (End date and time)	処理が完了した日時。
ソース・パートナー	送信側パートナーを示します。
ターゲット・パートナー	受信側パートナーを示します。.
検索場所:	文書タイプの「元 (From)」または「宛先 (To)」を検索します。
動作モード	実動、テスト、RN シミュレーター外部パートナー、または RN シミュレーター内部パートナー。テストが使用できるのは、テスト宛先タイプをサポートするシステムのみです。
文書の状況	システム内での現在の文書の状況。「進行中」、「成功」、または「失敗」を選択できます。デフォルトは「すべて」です。
パッケージ	文書フォーマット、パッケージ化、暗号化、およびコンテンツ・タイプ識別番号について説明します。
プロトコル	パートナーに対して使用できるプロセス・プロトコルの種類。
文書タイプ	特定のビジネス・プロセス。
文書 ID	ソースのパートナーによって作成されます。検索条件には、アスタリスク (*) のワイルドカードを使用できます。
参照 ID	文書状況の追跡のためにシステムで作成される ID 番号。
ソース IP アドレス	ソースのパートナーの IP アドレス。
フィルター	同期モードで受信した文書を検索します。これは、イニシエーターと文書マネージャーとの接続は、要求と確認通知または要求と応答などのトランザクションが完了するまで開通状態を維持するという意味です。
ソート順	結果をソートするときに使用する値。
ページごとの結果件数	1 ページに表示されるレコードの数。
降順	降順または昇順で結果をソートします。
ユーザー定義の検索フィールド	ユーザー定義の基準に基づく検索を実行します。

注: 警告イベントはデフォルトで表示されます。すべてのイベントを参照するには、「デバッグ」を選択します。

3. 「**検索**」をクリックします。検索条件に合致する文書のリストが表示されます。

表 26. 文書ビューアーによって使用可能な文書情報

値	説明
パートナー	ビジネス・プロセスに関与するソース (「元 (From)」) のパートナーとターゲット (「宛先 (To)」) のパートナー。
タイム・スタンプ	文書の処理が開始された日時および終了した日時。
文書タイプ	トランザクションが実行されているビジネス・プロセス。
宛先タイプ	実動またはテスト。テストが使用できるのは、テスト宛先タイプをサポートするシステムのみです。
同期	同期モードで受信した文書を識別します。これは、イニシエーターと文書マネージャーとの接続は、要求と確認通知または要求と応答などのトランザクションが完了するまで開通状態を維持するという意味です。

文書の詳細、イベント、およびロー文書の表示

1. 「**ビューアー**」 > 「**文書ビューアー**」の順にクリックします。「文書ビューアー検索」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。
3. 「**検索**」をクリックします。文書のリストが表示されます。
   - 文書の詳細とイベントを表示するには、「関連した文書」ヘッダーに表示される文書の横にある「フォルダーのオープン」アイコンをクリックします。選択した文書についてプロセスの詳細とイベントが表示されます。EDI 交換文書で、エンベロープ解除またはエンベロープのいずれかからの、子 EDI トランザクションがある場合、「**文書の子**」ソース・ラジオ・ボタンまたはターゲット・ラジオ・ボタンを選択すると、それらのトランザクションを表示できます。EDI 文書の表示の詳細については、「*管理者ガイド*」を参照してください。
   - HTTP ヘッダー付きのロー文書を表示するには、その文書の横にある「ロー文書の表示 (Display raw document)」アイコンをクリックします。ロー文書の内容が表示されます。

文書の詳細を表示すると、次に示す文書処理情報が表示されます。

表 27. 文書ビューアーによって使用可能な文書処理の値

値	説明
参照 ID	システムによって文書に割り当てられた固有の識別番号。
文書 ID	ソースのパートナーによって文書に割り当てられた固有の識別番号。
文書のタイム・スタンプ	パートナーによって文書が作成された日時。
宛先	文書が通過する宛先。
接続文書タイプ	パートナー間のビジネス要件との文書の互換性を確保するために、システムによって文書に実行されるアクション。
ソースとターゲット (Source and Target)	ビジネス・プロセスに関与しているソースとターゲットのパートナー。
入力タイム・スタンプ	システムがパートナーから文書を受信した日時。
終了状態タイム・スタンプ	システムがターゲットのパートナーへ文書を正常に転送した日時。
ソースとターゲットのビジネス ID (Source and Target Business ID)	ソースとターゲットのパートナーのビジネス識別番号 (例: DUNS)。
ソースおよびターゲットの文書タイプ	ソースとターゲットのパートナーとの間でトランザクションが行われる特定のビジネス・プロセス。

制約事項: ロー文書のうち、100K を超える部分は切り捨てられます。

ヒント: システムに「文書が重複しています」イベントが表示されている場合は、「文書が重複しています」イベントの横にある青色の矢印アイコンを選択して、以前送信された元文書を表示し、次に「元文書の表示 (View original document)」アイコンをクリックします。

ヒント: 処理できなかった文書のトラブルシューティングを行うには、85 ページの『データ検証エラーの表示』を参照してください。

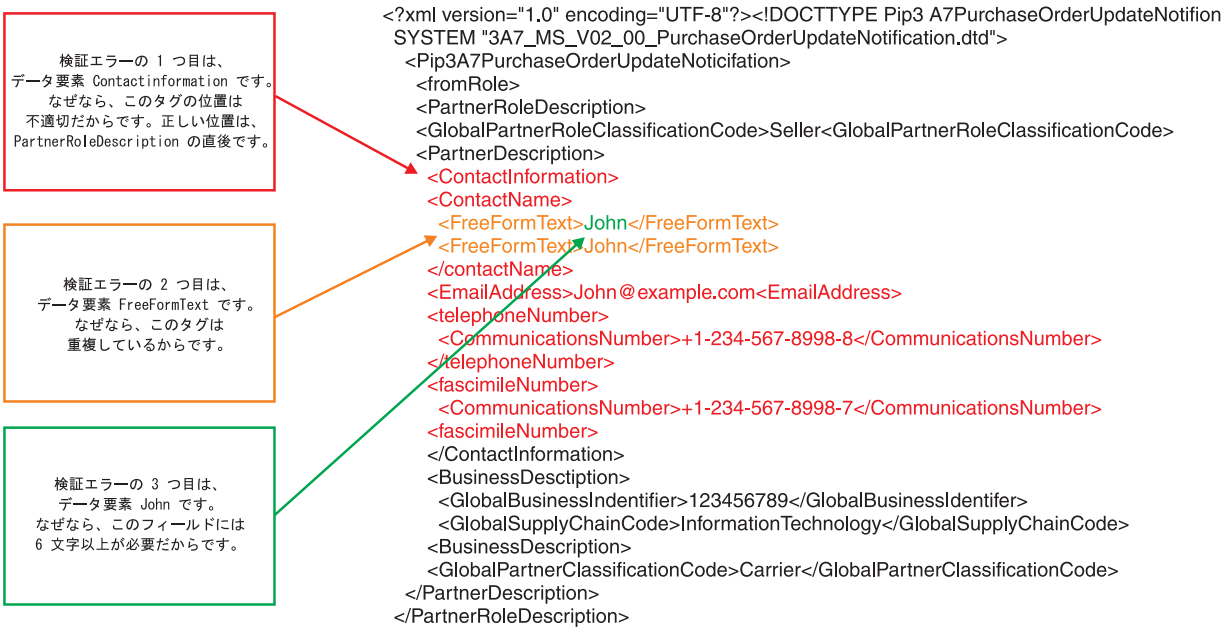
データ検証エラーの表示

検証エラーが含まれている XML フィールドで、色分けされたテキストを使用すると、処理できなかった文書を素早く検索できます。検証エラーが含まれるフィールドは、赤色で表示されます。ネストされた XML フィールド内で、異なる検証エラーが最大 3 種類発生した場合、エラー・フィールドを区別するために次の色が使用されます。

表 28. 色分けされた文書検証エラー

値	説明
赤色	第 1 の検証エラー
オレンジ色	第 2 の検証エラー
緑色	第 3 の検証エラー

ネストされた XML 検証エラーの例を次に示します。



ネストされていない XML 検証エラーの例は次のとおりです。

ロー文書の検証エラーを表示するには、81 ページの『ロー文書の表示』を参照してください。

制約事項: コンソールに表示される内容は、ロー文書の先頭の 100KB のみです。100KB を超える検証エラーは表示できません。

「プロセスの停止」機能の使用

現在進行中の文書の処理を途中で停止させるには、「**プロセスの停止**」をクリックします。この機能はハブ管理者ユーザーに限定されません。この機能を利用するには、グループのアクセス権を構成する必要があります。

注: 文書の処理を途中で停止させるには、最大で 1 時間かかります。この間、文書ビューアーは文書の状況を進行中として表示し続けます。

宛先キュー

宛先キューを使用すると、システムの宛先の配信キューに入っている文書を表示できます。配信キューに入っている文書を持つすべての宛先の表示、キュー内の文書の表示および削除、および宛先の使用可能化または使用不可化も可能です。

宛先キューは、時間依存の文書をキュー内に滞留させておかないために使用できます。また、キューに入れられる文書の数が最大数を超えないようにするためにも使用できます。宛先キューを使用すると、次の作業が可能になります。

- 配信キューに入っている文書を持つすべての宛先のリストを表示する。
- 長時間 (30 秒以上) 宛先キューに置かれている文書を表示する。こうすると、文書自体の問題が示される場合があります。さらに、文書の詳細を表示して、キュー内の文書のトラブルシューティングを行うこともできます。

  注: FTP スクリプトの宛先をインターバル・スケジュールまたはカレンダー・スケジュールでインプリメントしている場合、そのインターバルまたは日時に

達するまで期間を延長して、文書がこのキューに留まる場合があります。これは予想される操作であるため、キューから文書を除去しないことをお勧めします。

- 宛先の詳細を表示して正常な動作を確認する。宛先キューに留まっている文書が、送達マネージャーまたは宛先における障害を示している可能性があります。
- 宛先の状況を確認する。宛先がオフラインの場合、文書は宛先がオンラインになるまでキューに集められます。宛先の状況は接続の機能に影響を与えないため、文書は継続して処理され、配信キューに置かれます。
- 「**パートナー名 (Partner Name)**」フィールドと「**宛先**」フィールドを使用して宛先キュー・リストのサイズを制限する。

宛先リストの表示

宛先に存在する文書のリストを表示するには、次の手順に従います。

1. 「**ビューアー**」 > 「**宛先キュー**」を選択します。「宛先キュー」ウィンドウがコンソールにより表示されます。

2. 表 29 に示されているパラメーターを入力します。

表 29. 「宛先キュー」ウィンドウ

基準	説明
パートナー名 (Partner Name)	このフィールドを入力するには、以下のような方法があります。 1. パートナー名を指定する。 2. このフィールドにパートナー名の一部を指定し、「**パートナーの表示 (Show Partners)**」をクリックする。パートナー・リストからパートナーを選択する。 3. ワイルドカードである「*」を指定し、「**パートナーの表示 (Show Partners)**」をクリックする。パートナー・リストからパートナーを選択する。 「**パートナーの表示 (Show Partners)**」をクリックすると、同じページに「パートナー」フィールドが表示されます。「**パートナー**」フィールドには、選択可能なすべてのパートナーがアルファベット順にリストされます。
宛先	このリストの最初の項目は「すべて」であり、これはデフォルトで選択されています。リストの残りは宛先トランスポートの番号付きリストです。このリストでは、1 つの宛先のみ選択できます。デフォルトは「すべて」です。 **注:** 宛先リストには選択したパートナーの宛先が自動的に表示され、リストはアルファベット順に並べられます。
キューに入っている最小時間	文書が宛先キューで待機する最小分数。例えば、6 分を選択すると、6 分以上配信待機している文書を持つすべての宛先が表示されます。デフォルトは 0 です。
ソート順	パートナー (デフォルト) または宛先名の順に検索結果をソートします。
最新表示	最新表示機能をオンまたはオフ (デフォルト) にします。
キュー内最小項目数	宛先キュー内にある文書の最小数。デフォルトは 1 です。
方向	「**昇順**」をクリックすると、最も古いタイム・スタンプまたはアルファベットの最後から始まる文書から表示され、「**降順**」をクリックすると、最新のタイム・スタンプまたはアルファベットの先頭から始まる文書から表示されます。
最新表示頻度	表示されているデータが更新されるまでコンソールが待機する秒数。

3. 「**検索**」をクリックします。システムは、宛先の中で検索条件に一致する文書をすべて見つけます。**表 30** に、検索によって返される情報を示します。

表 30. 宛先キューの検索結果

基準	説明
パートナー	宛先に関連した取引先
宛先	宛先の名前
待機	宛先キューで配信を待つ文書の数。宛先詳細にリンクします。
状態	宛先の状態がオンラインかオフラインかを示します。
最終送信時	文書が宛先に正常に送信された最後の日時

注: コンソールで宛先を表示するには、宛先が AND 論理を使用する検索条件の要件すべてを満たしている必要があります。

キュー内の文書の表示

特定のパートナーのキューに入れられた文書を表示するには、次の手順を行います。

1. 「**ビューアー**」 > 「**宛先キュー**」をクリックします。
2. 「宛先キュー検索」ウィンドウで、「**文書検索**」をクリックします。
3. 「キュー文書検索 (Queue Documents Search)」ウィンドウで、検索条件を指定します (89 ページの表 31 を参照)。

表 31. 「キュー文書検索 (Queue Documents Search)」ウィンドウ

基準	説明
パートナー名 (Partner Name)	このフィールドを入力するには、以下のような方法があります。 1. このフィールドにパートナー名を指定する。 2. このフィールドにパートナー名の一部を指定し、「**パートナーの表示 (Show Partners)**」をクリックする。リストからパートナーを選択する。 3. ワイルドカードである「*」を指定し、「**パートナーの表示 (Show Partners)**」をクリックする。パートナー・リストからパートナーを選択する。 **注:** 「**パートナーの表示 (Show Partners)**」をクリックすると、同じページに「パートナー」フィールドが表示されます。「**パートナー**」フィールドには、選択可能なすべてのパートナーがアルファベット順にリストされます。
宛先	このリストの最初の項目は「すべて」であり、これはデフォルトで選択されています。リストの残りは宛先トランスポートの番号付きリストです。このリストでは、1 つの宛先のみ選択できます。デフォルトは「すべて」です。 **注:** 宛先リストには選択したパートナーの宛先が自動的に表示され、アルファベット順リストとして表示されます。
ソート順	リストをどの順でソートすべきかを、パートナー (デフォルト)、宛先、参照 ID、またはキューに入れられた際のタイム・スタンプ (文書の最新送信時間) の中から選択します。
参照 ID	システムによって文書に割り当てられた固有の識別番号を入力します。
方向	「**昇順**」をクリックすると、最も古いタイム・スタンプまたはアルファベットの最後から始まる文書から表示され、「**降順**」をクリックすると、最新のタイム・スタンプまたはアルファベットの先頭から始まる文書から表示されます。
文書 ID	ソース・パートナーによって文書に割り当てられた固有の識別番号を入力します。
ページごとの結果件数	1 ページに表示される文書の数を指定します。
表示できる文書の最大数 (Maximum Documents Allowed)	表示するレコードの数を指定します。

4. 「**検索**」をクリックします。キュー検索の結果が表示されます。

配信キューからの文書の削除

次の手順では、配信キューから文書を削除する方法について説明します。キューから文書を削除するには、ハブ管理者としてログインする必要があります。

1. 「**ビューアー**」 > 「**宛先キュー**」の順にクリックします。
2. 「宛先キュー」ウィンドウで、「**検索**」をクリックします。
3. ウィンドウに表示されたパラメーターをすべて入力します (88 ページの表 30 を参照)。
4. 「削除」アイコンをクリックして、文書を削除します。

宛先の詳細の表示

キュー内にある文書のリストなど、特定の宛先の情報を表示するには、次の手順に従います。

1. 「**ビューアー**」 > 「**宛先キュー**」の順にクリックします。
2. 「宛先キュー」ウィンドウで、検索条件を入力します (88 ページの表 29 を参照)。
3. 「**検索**」をクリックします。
4. 宛先のリストから、「**キュー内**」列にある文書数リンクをクリックします。宛先の詳細とキュー内にある文書のリストが表示されます。

宛先状況の変更

宛先をオンラインまたはオフラインにするには、次の手順に従います。

1. 「**ビューアー**」 > 「**宛先キュー**」の順にクリックします。
2. 「宛先キュー」ウィンドウで、検索条件を入力します (88 ページの表 29 を参照)。
3. 「**検索**」をクリックします。
4. 宛先のリストから、「**キュー内**」列にある文書数リンクをクリックします。宛先の詳細とキュー内にある文書のリストが表示されます。
5. 「**宛先情報**」の「**オンライン**」をクリックして宛先をオフラインにするか、「**オフライン**」をクリックして宛先をオンラインにします (宛先の状況を変更するには、ハブ管理者としてログインする必要があります)。

第 6 章 文書タイプの分析: ツール

文書分析ツールを使用すると、状態別 (「受信」、「進行中」、「失敗」、「成功」) にシステム内の文書数の詳細な概要が取得できます。検索条件には、日付、時刻、プロセスの種類 (「宛先 (To)」または「元 (From)」)、宛先タイプ、プロトコル、文書タイプ、およびプロセスのバージョンがあります。検索結果を使用して処理に失敗した文書を見つけて表示し、失敗の理由を調べます。

文書ボリューム・レポートは、ビジネス文書フローの管理、追跡、およびトラブルシューティングに使用する便利なツールです。レポートには、特定の期間内にシステムによって処理された文書のボリュームが表示されます。このレポートは表示と印刷ができ、また保管 (エクスポート) してほかのスタッフ・メンバーに送信することもできます。特定の検索条件に基づいて情報を表示するように、このレポートはカスタマイズできます。

宛先または Web サーバーをテストするには、パートナー接続のテスト・ツールを使用します。

表 32. ツール

使用する機能	参照先
文書分析	91 ページ
文書ボリューム・レポート	94 ページ
パートナー接続のテスト	96 ページ
EDI レポート	98 ページ
FTP レポート	102 ページ

文書分析

文書分析ツールを使用すると、特定の期間内に状態別にシステムの文書数の詳細な概要が取得できます。

処理が失敗した文書を探し出し、失敗の理由を調べるには、検索条件を使用します。

「文書分析」画面には、アラームが付いています。プロセスが失敗すると、失敗したプロセスが入った行が赤色に明滅します。

文書の状態

次の表に、文書のさまざまな状態を示します。

表 33. 文書の状態

状態	説明
受信	文書はシステムによって受信され、処理を待っています。
進行中	現在、文書は次のいずれかの処理ステップにあります。 • **未完了**。例えば、システムはほかの文書を待っています。 • **データ妥当性検査**。例えば、システムは文書内容をチェックしています。 • **変換**。例えば、システムは文書を別のプロトコルに変換しています。 • **キュー**。例えば、文書は外部パートナーまたは内部パートナーへの経路指定を待っています。
失敗	文書処理はシステムのエラー、データ妥当性検査、または重複によって中断されました。
正常終了	文書処理を完了する最終メッセージが、システムからターゲット・パートナーに送信されました。

システムの文書の表示

1. 「**ツール**」 > 「**文書分析**」をクリックします。「文書分析の検索」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。

表 34. 文書の検索条件

値	説明
開始日および開始時刻 (Start Date & Time)	処理が開始された日時。
終了日および終了時刻 (End Date & Time)	処理が完了した日時。
ソース・パートナー	ビジネス・プロセスを開始したパートナー (内部パートナーのみ)。
ターゲット・パートナー	ビジネス・プロセスを受信したパートナー (内部パートナーのみ)。
検索場所:	文書タイプの「元 (From)」または「宛先 (To)」を検索します。
宛先タイプ	例えば、実働またはテスト。テストが使用できるのは、テスト宛先タイプをサポートするシステムのみです。
パッケージ	文書フォーマット、パッケージ化、暗号化、およびコンテンツ・タイプ識別番号について説明します。
プロトコル	パートナーが使用可能な文書プロトコル。
文書タイプ	特定のビジネス・プロセス。
ソート順	ソース・パートナー名またはターゲット・パートナー名別に結果をソートします。
最新表示	検索結果を定期的に更新するかどうかを制御します (内部パートナーのみ)。
最新表示頻度	検索結果の更新頻度を制御します (内部パートナーのみ)。

3. 「**検索**」をクリックします。「文書分析の要約」が表示されます。

プロセスとイベントの詳細の表示

1. 「**ツール**」 > 「**文書分析**」をクリックします。「文書分析の検索」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。
3. 「**検索**」をクリックします。「文書分析の要約」が表示されます。
4. 表示するソース・パートナーとターゲット・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。選択したパートナーのすべての文書のリストが表示されます。文書の数量は文書処理状態別に列に並べられます。
5. 「受信」、「進行中」、「失敗」、「成功」のいずれかの列で数量リンクを選択します。文書分析レポートには、文書処理の詳細が記載されます。「失敗」を選択した場合、レポートには文書イベント要約も記載されます。

カスタム XML ファイルの処理

WebSphere Partner Gateway V6.0 以前のバージョンでは、XML 形式を使用することにより、Extensible Markup Language (XML) のカスタム処理サポートを提供していました。WebSphere Partner Gateway V6.0 以前の XML 形式では、文書から処理情報を抽出するときに、XPath 式言語を全面的に活用できませんでした。このため、WebSphere Partner Gateway V6.1 では、XML 形式の動作方法を再設計しました。WebSphere Partner Gateway V6.1 では、XML 形式に XPath バージョン 1.0 の式を使用できます。 XPath の全面サポートという処理能力の増強により、完全な XPath XML 形式で使用できるファイルのサイズは制限されます。大サイズのファイルを処理できるようにするため、文書ファミリーを定義するときに設定するオプションが用意されています。ラージ・ファイル・オプションを指定したファミリーの形式が備えている XPath 処理能力は、WebSphere Partner Gateway V6.0 以前のバージョンで提供されていた処理能力と同じで制限されていますが、大サイズのファイルを処理できます。文書ファミリーにラージ・ファイル処理オプションを使用した場合、これらの制限事項は、このファミリーに格納されている XML 形式で使用される式に以下のように適用されます。

1. 使用できるのは、文書のルートで始まる単純なエレメント・パスのみです。
2. エレメント・パスにはネーム・スペース・プレフィックスを使用できません。ただし、文書にはネーム・スペース・プレフィックスが出現することがあります。

「XML 形式の管理」ウィンドウには、「ラージ・ファイル・オプション」というラベルが付いたドロップダウン・リストがあります。このリストの選択項目は、「なし」、「*ラージ・ファイル・プロセッサーの使用*」、および「*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*」です。 ユーザーは、フル装備の XPath プロセッサーでは処理できない大規模な文書に適した XML 形式を記述する場合にラージ・ファイル・オプションを選択します。 ネーム・スペース認識オプションとは、文書内にエレメント・パスが出現する場合、エレメント・パスにネーム・スペース・プレフィックスが含まれることを意味します。

注: このオプションは、ファミリーの作成後に変更することはできません。これは、文書ファミリーには、ファミリー・タイプを変更した場合に無効になる XML 形式が既に含まれている場合があるためです。 パートナーにはカスタム XML ファイル処理を使用できません。

文書ボリューム・レポート

文書ボリューム・レポートは、ビジネス文書フローの管理、追跡、およびトラブルシューティングに使用する便利なツールです。レポートには、特定の期間内にシステムによって処理された文書のボリュームが表示されます。このレポートは表示と印刷ができ、また保管 (エクスポート) してほかのスタッフ・メンバーに送信することもできます。

特定の検索条件に基づいて情報を表示するように、このレポートはカスタマイズできます。

文書ボリューム・レポートでは、現在処理中の文書の数を状態別に示します。

表 35. 文書の状態

値	説明
受信合計	システムで受信した文書の総数。
進行中	進行中の文書では、テストと妥当性検査が行われています。エラーは検出されていませんが、プロセスはまだ完了していません。
失敗	文書処理はエラーのため中断されました。
正常終了	文書処理を完了する最終メッセージが、システムからターゲット・パートナーに送信されました。

次の作業を実行するには、このレポートを使用します。

- 主要ビジネス・プロセスが完了したかどうかを判断する。
- コスト管理のため、プロセスのボリュームの傾向を追跡する。
- プロセスの質 (成功と失敗) を管理する。
- 内部パートナーである場合、パートナーが効率的にプロセスを追跡できるように援助する。

文書ボリューム・レポートの作成

1. 「**ツール**」 > 「**文書ボリューム・レポート**」をクリックします。「文書ボリューム・レポートの検索」画面が表示されます。

2. ドロップダウン・リストから検索条件を選択します。

表 36. 文書ボリューム・レポートの検索条件

値	説明
開始日および開始時刻 (Start date & time)	処理が開始された日時。
終了日および終了時刻 (End date & time)	処理が完了した日時。
ソース・パートナー	ビジネス・プロセスを開始したパートナー (内部パートナーのみ)。
ターゲット・パートナー	ビジネス・プロセスを受信したパートナー (内部パートナーのみ)。
検索場所:	文書タイプの「元 (From)」または「宛先 (To)」を検索します。
宛先タイプ	実動またはテスト。テストが使用できるのは、テスト宛先タイプをサポートするシステムのみです。
パッケージ	文書フォーマット、パッケージ化、暗号化、およびコンテンツ・タイプ識別番号について説明します。
プロトコル	XML、EDI、フラット・ファイルなど、プロセス・プロトコルのタイプ。
文書タイプ	特定のビジネス・プロセス。
ソート順	この基準に従って結果をソートします (「文書タイプ」または「ターゲット文書タイプ」)。
ページごとの結果件数	1 ページに表示されるレコードの数。

3. 「**検索**」をクリックします。レポートが表示されます。

文書ボリューム・レポートのエクスポート

1. 「**ツール**」 > 「**文書ボリューム・レポート**」をクリックします。「文書ボリューム・レポートの検索」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。
3. 「**検索**」をクリックします。レポートが表示されます。
4. 「レポートのエクスポート」アイコンをクリックして、レポートをエクスポートします。希望する場所に移動して、ファイルを保管します。

注: レポートはコンマで区切られた値 (.CSV) ファイルとして保管されます。ファイル名には、「.csv」サフィックスが付きます。

レポートの印刷

1. 「**ツール**」 > 「**文書ボリューム・レポート**」をクリックします。「文書ボリューム・レポートの検索」画面が表示されます。
2. ドロップダウン・リストから検索条件を選択します。
3. 「**検索**」をクリックします。レポートが表示されます。
4. 「印刷」アイコンをクリックして、レポートを印刷します。

パートナー接続のテスト

パートナー接続のテスト機能を使用すると、宛先または Web サーバーをテストできます。内部パートナーは、特定のパートナーを選択することもできます。テストでは、空の POST 要求を宛先または URL に送信します。この要求は、ブラウザーのアドレス・フィールドに Yahoo の URL (www.yahoo.com) を入力することに似ています。これは空の要求であり、何も送信されません。宛先または Web サーバーから受信する応答がその状況を示します。

- 応答が返された場合、サーバーは稼働している。
- 応答がない場合、サーバーは停止している。

重要: パートナー接続のテスト機能は HTTP で作動します。接続パラメーターは必要ありません。

パートナー接続のテスト方法

1. 「**ツール**」 > 「**パートナー接続のテスト**」をクリックします。「パートナー接続のテスト」画面が表示されます。
2. ドロップダウン・リストからテスト基準を選択します。

表 37. パートナー接続のテストの値

値	説明
パートナー	テスト対象のパートナー (内部パートナーのみ)。
宛先	上で選択したパートナーに基づき使用可能な宛先を表示します。
URL	上で選択した宛先に基づき、動的に入力されます。
コマンド	Post または Get。

3. 「**URL のテスト**」をクリックします。テスト結果が表示されます。返される状況コードの詳細については、以下のセクションを参照してください。

Web サーバーの結果コード

200 番台

- 200 - OK - 送信成功。これはエラーではありません。要求したファイルが送信されました。
- 201 - 作成 - 要求は満たされ、新規リソースが作成されました。新規作成されたリソースは、応答の URL ヘッダー・フィールドに返された URL によって参照できます。リソースの最も詳しい URL は Location ヘッダー・フィールドにあります。
- 202 - 受領 - 要求は処理のために受領されましたが、処理はまだ完了していません。
- 203 - 不確実な情報 - Entity ヘッダーに返された META 情報はローカル・コピーまたはサード・パーティーのコピーから収集されており、元のサーバーから入手できる情報ほど信頼性が高くありません。
- 204 - 内容なし - サーバーは要求を満たしましたが、送り返す新しい情報はありません。
- 206 - 一部の内容 - ファイルの一定範囲のバイトを要求され、その内容を送信しました。これは HTTP 1.1 の新規機能です。

300 番台

- 301 - 永続的に移動 - 要求されたリソースには新規の永続的な URL が割り当てられられたため、将来このリソースを参照するときは、返された URL の 1 つを使用してください。
- 302 - 一時的に移動 - 要求されたリソースは、新規 URL に一時的に置かれています。新規 URL にリダイレクトされます。元のページは移動されています。これはエラーではありません。ほとんどのブラウザーでは、この結果を認識すると、自動的に新規ページを取り出します。

400 番台

- 400 - 不正な要求 - 構文が間違っているため、サーバーでは要求を理解できませんでした。不正な要求はクライアントによって行われました。
- 401 - 無許可 - 要求にはユーザー認証が必要です。応答には、要求されたソースに適用できる、ユーザー確認のための質問が入った WWW-Authenticate ヘッダー・フィールドが必要です。ユーザーは文書を要求したが、有効なユーザー名またはパスワードを指定しませんでした。
- 402 - 支払いが必要 - このコードは現在サポートされていませんが、将来の利用のために予約されています。
- 403 - 禁止 - サーバーは要求を理解しましたが、不特定の理由のため、要求の実行は拒否されました。この文書へのアクセスは明示的に拒否されました。(これは、要求されているファイルへの読み取りアクセス権が Web サーバーにないためかもしれません。) サーバーはこのファイルの送信を拒否しています。アクセス権が明示的に無効になっている可能性があります。
- 404 - 検出なし - 要求された URL に一致するリソースが見つかりませんでした。このファイルは存在しません。ブラウザーに不正な URL が指定されました。また、文書を保護するため、許可されていないユーザーにはファイルが存在しないと知らせるようにサーバーが指定されている場合にも、このコードが送信されます。404 エラーは、存在しないページへの要求の結果であり、その原因としては間違って入力された URL、もう存在しないファイルを指すブックマーク、robots.txt (検索エンジンで索引付けをしないページのマークに使用されます) を検索する検索エンジン、ファイル名を推測するほかのユーザー、ユーザーのサイトまたはほかのサイトからの間違ったリンクなどがあります。
- 405 - 許可されていないメソッド - 要求行に指定されたメソッドは要求 URL で指定されたリソースでは許可されていません。
- 406 - 許容対象なし - サーバーは要求 URL に一致するリソースを検出したが、Accept と Accept-Encoding 要求ヘッダーで指定された条件を満たすリソースはありません。
- 407 - プロキシー認証が必要 - このコードは将来の利用に備えて予約されています。401 (無許可) に似ていますが、クライアントには最初にプロキシーでの認証が必要であることを示しています。HTTP 1.0 にはプロキシー認証の方法が用意されていません。
- 408 - 要求タイムアウト - サーバーが準備していた待機時間内にクライアントは要求を作成しませんでした。
- 409 - 競合 - 要求は、リソースの現在の状態と競合するため、完了できませんでした。

- 410 - 喪失 - 要求されたリソースは現在サーバーでは使用できず、転送先アドレスはわかりません。
- 411 - 許可の拒否 - クライアントが提供した要求の証明書はサーバーで拒否されたか、リソースにアクセスするには権限が不足しています。
- 412 - 前提条件に問題がある
- 413 - 要求エンティティーが大きすぎる
- 414 - 要求 URI が大きすぎる
- 415 - メディア・タイプがサポートされない

500 番台

- 500 - 内部サーバー・エラー - サーバーに予期しない状態が発生し、要求を満たすことができませんでした。Web サーバーに何か問題があり、意味のある応答ができませんでした。通常、ブラウザー側からの操作でこのエラーを修正することはできません。このため、サーバー管理者は、サーバーのエラー・ログを調べて何が起こったかを確認することが必要になります。多くの場合、CGI スクリプトが正しくコード化されていないため、このエラー・メッセージが生成されます。
- 501 - メソッドがインプリメントされていない - サーバーは要求を満たすために必要な機能をサポートしていません。アプリケーション・メソッド (GET または POST) はインプリメントされていません。
- 502 - 不正な宛先 - サーバーは要求を満たすためにアクセスした宛先またはアップストリーム・サーバーから無効な応答を受信しました。
- 503 - サービスが一時的に利用できない - サーバーは、一時的な過負荷またはサーバーの保守のため、現在要求を処理できません。サーバーはリソース不足です。
- 504 - 宛先タイムアウト - サーバーは要求を完了するためにアクセスした宛先またはアップストリーム・サーバーから時間内に応答を受信しませんでした。
- 505 - HTTP バージョンがサポートされていない

EDI レポート

期限経過の電子データ交換 (EDI) 機能肯定応答 (FA) を検索するには EDI レポートを使用します。拒否電子データ交換 (EDI) トランザクションを検索することもできます。以下のセクションで EDI レポートを使用の詳細な手順を説明します。

EDI FA 期限経過の検索

「EDI FA 期限経過の検索」ページは、期限経過の電子データ交換 (EDI) 機能肯定応答 (FA) の検索の実行の検索基準を提供します。

注: 結果レポートから削除された、以前の EDI EDI FA 期限経過の検索で返された、すべてのレコードは後の検索で無視されます。そのために、削除されたレコードは後のレポートで表示されません。レコードは、「EDI FA 期限経過レポート」ページの「**選択されたレコードを無視**」の選択によりレポートできます。ハブ管理者のみがレポートからレコードを削除できます。

EDI FA 期限経過レコードを検索するには、以下を実行します。

1. 「**ツール**」 > 「**EDI レポート**」をクリックします。「EDI FA 期限経過の検索」画面が表示されます。
2. ドロップダウン・リストから 1 つ以上の検索条件を選択します。

表 38. EDI FA 期限経過の検索の基準

値	説明
開始日および開始時刻 (Start date & time)	トランザクションが開始された日時。
終了日および終了時刻 (End date & time)	トランザクションが完了した日時。
ソース・パートナー	トランザクションを開始したパートナー。
ターゲット・パートナー	トランザクションを受信したパートナー。
検索場所:	ソース文書タイプまたはターゲット文書タイプを検索します。
パッケージ	文書フォーマット、パッケージ化、暗号化、およびコンテンツ・タイプ識別番号について説明します。
プロトコル	XML、EDI、フラット・ファイルなど、プロセス・プロトコルのタイプ。表示されるプロトコルは、「パッケージ」フィールドで選択した値に応じて変わります。
文書タイプ	特定の文書タイプ。表示されるタイプは、「プロトコル」フィールドで選択した値に応じて変わります。
参照 ID	トランザクション ID を指定します。
ソート順	検索結果のソートの基準を指定します。デフォルトは、期限経過時間および降順。最大の期限経過の FA を最初に表示するには「降順」を使用します。最小の期限経過の FA を最初に表示するには「昇順」を選択します。
ページごとの結果件数	各ページに表示するトランザクションの検索結果の数を指定します。

3. 「**検索**」をクリックして「EDI FA 期限経過の検索」レポートを表示します。

EDI FA 期限経過レポートの表示

「EDI FA 期限経過の検索」ページで選択された検索条件に応じて、検索結果は「EDI FA 期限経過レポート」ページに表示されます。

当てはまる場合、次のデータは、「EDI FA 期限経過レポート」に表示されます。

表 39. EDI FA 期限経過レポート

値	説明
日付	ソース・パートナーからターゲット・パートナーに EDI が送信された日付。
時刻	ソース・パートナーからターゲット・パートナーに EDI が送信された時刻 (GMT)。
ActivityID	トランザクションの事実上固有の ID (VUID)。
ソース取引パートナー	トランザクションを送信したパートナー。
ソース・パッケージ	トランザクションのソース・パッケージ。
ソース・プロトコル	トランザクションのソース・プロトコル。
ソース文書タイプ	トランザクションのソース文書タイプ。
ターゲット取引パートナー	トランザクションを送信したパートナー。
ターゲット・パッケージ	トランザクションのターゲット・パッケージ。
ターゲット・プロトコル	トランザクションのターゲット・プロトコル。
ターゲット文書タイプ	トランザクションのターゲット文書タイプ。
交換番号 (Interchange Number)	トランザクションの交換番号
グループ番号 (Group Number)	トランザクションのグループ番号。
トランザクション番号 (Transaction Number)	トランザクションの識別番号。
FA 期限	トランザクションの FA の期限の日
期限経過	FA の期限経過の時間の量。
選択されたレコードを無視	レコードにこのオプションを選択した場合、その特定のレコードはレポートから削除されます。レコードが一度レポートから削除された場合、そのレコードは後の EDI FA 期限経過の検索により無視され、その結果、結果レポートに表示されません。ハブ管理者のみがレポートからレコードを削除できます。

EDI 拒否トランザクションの検索

「EDI 拒否トランザクションの検索」ページに、エラー・コードを含む機能肯定応答 (FA) を持つ、電子データ交換 (EDI) トランザクションの検索の実行の基準が含まれています。FA を持たないトランザクション・レコードは、「EDI 拒否トランザクションの検索」で返されません。

EDI 拒否レコードを検索するには、以下を実行します。

1. **「ツール」 > 「EDI レポート」> 「EDI 拒否レポート」**をクリックします。

2. ドロップダウン・リストから 1 つ以上の検索条件を選択します。

表 40. EDI 拒否トランザクションの検索の基準

値	説明
開始日および開始時刻 (Start date & time)	トランザクションが開始された日時。
終了日および終了時刻 (End date & time)	トランザクションが完了した日時。
ソース・パートナー	トランザクションを開始したパートナー。
ターゲット・パートナー	トランザクションを受信したパートナー。
検索場所:	ソース文書タイプまたはターゲット文書タイプを検索します。
パッケージ	文書フォーマット、パッケージ化、暗号化、およびコンテンツ・タイプ識別番号について説明します。
プロトコル	XML、EDI、フラット・ファイルなど、プロセス・プロトコルのタイプ。表示されるプロトコルは、「パッケージ」フィールドで選択した値に応じて変わります。
文書タイプ	特定の文書タイプ。表示されるタイプは、「プロトコル」フィールドで選択した値に応じて変わります。
参照 ID	トランザクション ID を指定します。
ソート順	検索結果のソートの基準を指定します。デフォルトは、期限経過時間および降順。最大の期限経過の FA を最初に表示するには「降順」を使用します。最小の期限経過の FA を最初に表示するには「昇順」を選択します。
ページごとの結果件数	各ページに表示するトランザクションの検索結果の数を指定します。

3. 「**検索**」をクリックして「EDI 拒否トランザクション・レポート」を表示します。

EDI 拒否トランザクション・レポートの表示

「EDI 拒否トランザクションの検索」ページで選択された検索条件に応じて、検索結果は「EDI 拒否トランザクション・レポート」ページに表示されます。

当てはまる場合、次のデータは、「EDI 拒否トランザクション・レポート」に表示されます。

表 41. EDI 拒否トランザクション・レポート

値	説明
日付	EDI が受信された日付。
時刻 (Time)	EDI トランザクションがソース・パートナーからターゲット・パートナーに送信された時刻 (GMT)。
ActivityID	トランザクションの事実上固有の ID (VUID)。
ソース取引パートナー	トランザクションを送信したパートナー。
ソース・パッケージ	トランザクションのソース・パッケージ。
ソース・プロトコル	トランザクションのソース・プロトコル。
ソース文書タイプ	トランザクションのソース文書タイプ。
ターゲット取引パートナー	トランザクションを受信したパートナー。
ターゲット・パッケージ	トランザクションのターゲット・パッケージ。
ターゲット・プロトコル	トランザクションのターゲット・プロトコル。
ターゲット文書タイプ	トランザクションのターゲット文書タイプ。
交換番号 (Interchange Number)	トランザクションの交換番号。
グループ番号 (Group Number)	トランザクションのグループ番号。
トランザクション番号 (Transaction Number)	トランザクションの識別番号。
状況コード	FA の状況コード。
状況テキスト	FA の状況テキスト。

FTP レポート

FTP レポートは FTP 統計および FTP 接続についての詳細を提供します。

FTP 統計

「FTP 統計」ページは「読み取り専用」モードで FTP サーバー状況を表示します。

注: FTP サーバーまたは FTP 管理サーバーが使用不可の場合、統計は表示されません。

FTP サーバー状況を表示するには、以下を行います。

1. 「**ツール**」 > 「**FTP レポート**」をクリックします。「FTP 統計」ページが表示されます。

2. 次のサーバー状況情報が表示されます。

表 42. FTP 統計

値	説明
サーバー開始時刻	FTP サーバーの開始時刻。
作成されたディレクトリー数	mkdir を使用して、ユーザーにより作成されたディレクトリー数。
除去されたディレクトリー数	rmdir を使用して、ユーザーにより除去されたディレクトリー数。
アップロードされたファイル数	すべてのユーザーによりアップロードされたファイル数。
ダウンロードされたファイル数	すべてのユーザーによりダウンロードされたファイル数。
削除されたファイル数	削除コマンドを使用して、すべてのユーザーにより削除されたファイル数。
アップロードされたバイト数	アップロードされたバイトの総数。
ダウンロードされたバイト数	ダウンロードされたバイトの総数。
現在のログイン数	存在するログインを表示します。
合計のログイン数	最終のリセット以来の合計のログイン数。
失敗したログイン数の合計	失敗したログインの総数。
現在の接続数	最終のリセット以来の現行接続。
合計の接続数	最終のリセット以来の合計の接続数。

3. 現在のログイン数を最新表示するために**「再ロード」** をクリックします。
4. **「リセット」**をクリックして値をリセットします。

FTP 接続

以下に説明するステップに従って「FTP 接続」を表示します。

1. **「ツール」 > 「FTP レポート」 > 「FTP 接続」をクリックします。**
2. レポートに次の接続情報が表示されます。

表 43. FTP 接続

値	説明
ログイン名	この接続用のログイン・ユーザー ID。これがブランクである場合、ユーザーは接続のみを確立しているがログインしていないことを意味します。
ログイン時刻	ユーザーがログインした時刻。これがブランクである場合、ユーザーは接続のみを確立していることを意味します。
最終アクセス時刻	ユーザーがこの接続に最後にアクセスした時刻。これがブランクである場合、ユーザーはログインのみを行い、まだ何のコマンドも発行していないことを意味します。
クライアント・アドレス	ユーザーがログインしたクライアント IP。

用語集

［ア行］

アカウント管理 (Account Admin). アカウント管理モジュールを使用すると、会社をネットワークに識別させる情報を表示したり編集したりできる。また、組織内のほかの担当者へのコンソール・アクセス権を管理する場合にも、この画面を使用する。

アクション (Action). (1) パートナー間のビジネス要件との文書の互換性を確保するために、システムによって文書に実行されるアクション。 (2) 文書の妥当性検査および変換などの一連の処理ステップ。

アクション・インスタンス ID (Action Instance ID). 購入注文、RFQ など、ビジネス関係の内容を持つ文書を示す。

宛先 (Destination). 別のネットワークへの入り口として働く B2B のネットワーク・ポイント。宛先を使用すると、データ変換と互換性の問題を解決し、データ転送を成功させることができる。

アラート (Alert). アラートは、事前設定した運用制限が破られたときに通知と解決方法を迅速に提供する。アラートは、テキスト・ベースの E メール・メッセージから構成され、ネットワーク内かその外側にいるユーザーまたは主要担当者の配布リストに送信される。アラートは、システム・イベントの発生または予想されるプロセス・ボリュームに基づいて生成できる。

イベント (Event). システムで生成される、文書の処理に関連したメッセージ。

インバウンド・マネージャー (Inbound Manager). NAS から文書を検索し、ビジネス・プロセス・エンジンによる適切なアクション・タスク用に準備する。

エンベロープ解除 (De-envelope) . EDI エンベロープから文書を抽出すること。

応答中受信側 ID (In Response to ID). ビジネス・アクション応答の ID 番号。

応答中ビジネス・アクション (In Response Business Action). 同じプロセスのアクションへの応答として送信されるビジネス文書のタイプを示す。

［カ行］

外部パートナー (External Partner). ビジネス・トランザクションを内部パートナーと交換するハブ・コミュニティー・メンバー。

可視性 (Visibility). 可視性では、パートナー (ローカル) または内部パートナー (グローバル) によって担当者をアラートに割り当てることができるかどうかを定義する。

活動化 (Activation). パートナーをシステムに接続すること。

グループ (Group). 選択機能の実行のためユーザーに与えられたコンソールへのアクセス権の集合。

クローズ (Closed). プロセスの最後の文書が処理されたかプロセスが取り消された日時。

グローバル (Global). パートナーおよび内部パートナーは担当者にアラートを割り当てることができる。

検証 (Validation). 検証とは、指定された要件とプロセスのサブトランザクションとを比較し、妥当であるかどうかを判断することである。通常、内容やトランザクション・シーケンスをパラメーターとして指定する。

コミュニティー・コンソール (Community Console). コミュニティー・コンソールは、内部パートナーまたは外部パートナーと会社とのビジネス文書フローをモニターするために使用される Web ベースのツールである。

コレオグラフィー (Choreography). ビジネス・プロセスを正しく完了するために必要な文書の順序。

［サ行］

サービス (Service). メッセージが RosettaNet ベースであるかどうかを示す。

サーブレット (Servlet). 受信文書を NAS に書き込む、Web サーバー上で実行される小さなプログラム。

サブスクライブ済み連絡先 (Subscribed contact). サブスクライブした連絡先は、E メールによるアラートの受信が指定されたユーザーを示す。

シグナル (Signal). アクションに応答して送信される文書。

シグナル・インスタンス ID (Signal Instance ID). アクションに応答して送信される確認通知または否定応答である文書を示す。

シグナル・バージョン (Signal Version). シグナルとして送信されるビジネス・プロセスのバージョン。

試行カウント (Attempt Count). トランザクションが最初の試行であるか、再試行であるかを示す。1 は最初の試行を示す。2 以上は再試行の回数を示す。

実動 (Production). ライブ文書の経路指定に使用される宛先ゲートウェイ。

種別 (Classification). ビジネス・プロセスでのパートナーの役割を示す。

状態 (State). (1) システムによって処理される文書は次の 4 つのいずれかの状態になる。 (2) 受信、進行中、失敗、成功。

証明書セット (Certificate set). パートナー接続に関連付けることができる 1 次および 2 次の証明書のセット。

[タ行]

置換 (Substitute). 事前定義したパラメーターに基づいてサブトランザクション内のデータをほかのデータに置き換えること。

ツール (Tools). ツール・モジュールを使用すると、欠陥のある文書、データ・フィールド、および関連イベントを調べ、プロセスの障害をトラブルシューティングできる。

データの軽減 (Data Mitigation). ビジネス・プロセス標準に基づいて、文書の構造とフォーマットのエラーをテストし修復するプロセス。

デジタル署名 (Digital Signature). デジタル署名は、パートナーの ID を認証し、送信された文書の元の内容が変更されていないことを確認するために使用される電子シグニチャーである。

テスト (Test). パートナーがプロビジョニング・プロセス中にデータ緩和またはビジネス規則テストを実行している状態。

動作モード (Operation Mode). テスト中またはライブ実動時に、特定のゲートウェイに経路指定された文書を示す。

トランザクション ID (Transaction ID). ビジネス・プロセスの ID 番号。

トランザクション (Transaction). パートナーでビジネスを行うため、 1 つの単位として扱われる一連の情報交換および関連の作業。

トランスポート・プロトコル (Transport Protocol). インターネット上のコンピューター間で、メッセージ単位の形式でデータを送信するために使用される規則 (プロトコル) の集合。例えば、HTTP、HTTPS、SMTP、FTP など。

[ナ行]

内部パートナーの子 (Internal Partner Child). 内部パートナーの子は特殊なパートナー・タイプの 1 つであり、コンソールではパートナーのように動作するが、経路指定では内部パートナーのように動作する。

[ハ行]

バージョン (Version). 文書プロトコルの特定のリリース。

パートナー接続 (Partner connection). パートナー接続は、 2 つの特定のコミュニティー・メンバーの環境間を結び、 1 つの固有のプロセスが実行される接続を定義する。

パッケージ (Packages). システムのサーバーで受信できる文書パッケージ化フォーマットを示す。例えば、AS1、AS2 など。

ビジネス・シグナル・コード (Business Signal Code). アクションに応答して送信されるシグナル (文書) のタイプを示す。例えば、受領応答、受諾応答、一般例外など。

ビジネス・プロセス (Business Process). ビジネスの目的を達成するために必要な作業の実行方法を表す一連の定義済みトランザクション。

ビジネス・ルールのテスト (Business Rules Testing). パートナー間で文書内容にエラーがあるかどうかをテストし修復するプロセス。

フィルター (Filter). 事前定義されたパラメーターに基づいてサブトランザクション内のデータを除去する。

プロセス・インスタンス ID (Process Instance ID). 特定のビジネス・プロセスに割り当てられた固有の識別番号。

プロトコル (Protocols). さまざまなビジネス・プロセスに対する文書フォーマットの特定のタイプを示す。例えば、RosettaNet、XML。

プロビジョニング (Provisioning). プロビジョニング (またはオンボード化) は、ユーザーの B2B ゲートウェイをシステム・インフラストラクチャーに接続するために必要な一連の手順を完了することを意味する。

プロファイル (Profile). プロファイル・モジュールを使用すると、会社をシステムに識別させる情報を表示したり編集したりできる。

文書 (Document). 組織の規則に従った情報の集合。情報には、テキスト、ピクチャー、音などがある。

文書定義 (Document Definition). コミュニティー・メンバー間での文書の受信、処理、および経路指定に必要なすべての情報をシステムに指定する。文書定義には、パッケージ、プロトコル、文書タイプ、アクティビティー、およびアクションなどのタイプがある。

文書プロトコル (Document Protocol). 情報のフォーマットを設定し、コンピューター・ネットワークを介して情報を送信するために使用される一連の規則と命令 (プロトコル)。RosettaNet、XML、フラット・ファイル、EDI などがある。

変換 (Transform). 文書の内容を相互参照テーブルのデータに置き換える。

変換 (Translation). 文書が特定のプロトコルから別のプロトコルに変換されること。

［ラ行］

ライブ (Live). パートナーがビジネス規則テストを正しく完了し、内部パートナーがサービス要求を出してライブ状況に移動した状態。

レポート (Reports). レポート・モジュールを使用すると、処理対象の文書のボリューム、およびシステムによって生成されるイベントに関する詳しいレポートを作成できる。

［ワ行］

ワイルドカード (Wildcard). ワイルドカード検索の検索条件には、アスタリスク (*) が使用される。

D

DUNS. D&B D-U-N-S 番号は、固有の 9 桁の識別番号列であり、単一のビジネス・エンティティーの固有 ID を提供する一方で、企業ファミリー構造をリンクする。D&B は、全世界の 6,400 万以上の企業ファミリー・メンバーについて、親会社、子会社、本部、および支店の D&B D-U-N-S 番号をリンクしている。世界で最も影響力がある標準規定組織で使用されており、国際連合、米国連邦政府、オーストラリア政府、欧州委員会など、50 以上の国際機関、業界団体、および通商機関で認識、推奨されており、必須とされることも多い。今日の世界経済で、D&B D-U-N-S 番号は、世界のビジネスを追跡する標準となっている。

E

EDI. 構造化され、フォーマットが事前設定された情報のコンピューター間での転送。従来、EDI の活動は購入注文、送り状など、事前定義された業務フォームを同様に定義された電子フォームに置き換えることに重点が置かれている。

F

FTP. File Transfer Protocol (FTP)。インターネットの標準プロトコルである FTP は、インターネット上のコンピューター間でファイルを交換する最も簡単な方法である。

H

HTTP. Hypertext Transfer Protocol (HTTP) は、Web 上でファイル (テキスト、グラフィック・イメージ、音、ビデオ、およびその他のマルチメディア・ファイル) を交換するための規則 (プロトコル) の集合である。

HTTPS. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) は、ユーザー・ページ要求および Web サーバーで返されたページの暗号化と暗号化解除を行う Web プロトコルである。

P

PIP (Partner Interface Process). 内部パートナーとパートナー (WebSphere Partner Gateway では、パートナーは参加者) の間のビジネス・プロセスを定義する。各 PIP では特定のビジネス文書とその処理方法を示す。

R

RNIF. RosettaNet Implementation Framework (RNIF) は、すべての Partner Interface Processe (PIP) 用標準エンベロープ・コンテナーを作成するためのガイドラインである。

RTF. リッチ・テキスト・フォーマット (RTF) は、異なるオペレーティング・システムの異なるワード・プロセッサー間でテキスト・ファイルを交換できるようにす

るファイル・フォーマットである。例えば、Windows 98 で Microsoft Word を使用してファイルを作成し、RTF ファイルとして保管し (.rtf ファイル名サフィックスが付く)、Windows 3.1 で WordPerfect 6.0 を使用するユーザーに送信できる。

S

SMTP. Simple Mail Transfer Protocol (SMTP) は E メールの送受信に使用されるプロトコルである。

SR. サービス要求 (Service request)。

SSL. Secure Sockets Layer (SSL) は HTTP プロトコルを使用したセキュアなデータ送信方法である。

U

URL. URL (Uniform Resource Locator) は、インターネット上でアクセスできる文書またはプロセス (リソース) のアドレスである。

特記事項

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。

〒106-8711
東京都港区六本木 3-2-12
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。

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。

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。

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。

Websphere Partner Gateway には、ICU4J というコードが含まれています。ICU4J のコードは、IBM の「プログラムのご使用条件」に基づきその「適用除外コンポーネ

ント」の条項に従うことを条件に使用許諾されます。 ただし、IBM は以下の条項を明示することを義務付けられています。

著作権および許可に関する注意事項

本「プログラム」は、IBM 社およびその他の著作権により保護されています。
Copyright (c) 1995-2008

All rights reserved.

このソフトウェアおよびその関連文書ファイル (以下「ソフトウェア」といいます) を取得する人には、この「ソフトウェア」の、使用、複製、変更、結合、出版、配布またはソフトウェアの複製を販売する権利を含め、制約なく取引する権利を無償で許可し、また、「ソフトウェア」を与えられた人にも、この権利が与えられます。ただし、上記の著作権表示およびこの許可通知が、すべてのこの「ソフトウェア」の複製に記載され、また上記の著作権表示およびこの許可通知が、関連文書に記載されている場合に限ります。

ソフトウェアは、特定物として現存するままの状態で提供され、第三者の権利の不侵害の保証、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または保証条件を負わないものとします。さらに、著作権者またはこの注意事項に含まれている権利の所有者は、このソフトウェアの使用または実行に起因するものであれ、関連するものであれ、契約、過失、不法行為のいずれによるものであれ、使用、データまたは利益の喪失から発生する請求、あるいは特別、直接的、間接的、結果的損害、または他の一切の損害について、何等の責任も負いません。

この通知に記されているもの、および事前の書面による承認がある場合を除き、著作権者の名前を、このソフトウェアの広告、または販売、使用、取引の促進のためにご使用になることはできません。

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。

警告: 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、International Business Machines Corporation の米国およびその他の国における商標です。

IBM、 IBM logo、 AIX、 CICS、 DB2、 DB2 Universal Database、 IBMLink、 IMS MQSeries、 MVS、 OS/390、 WebSphere、 z/OS

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 バージョン 6.1。

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]

[ヤ行]

[ラ行]

[ワ行]

[数字]

A

B

D

E

F

J

R

S

V

W

X

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12