

**Sterling B2B Integrator**



## **EBICS Banking Server の概念**

バージョン 5.2.5



**Sterling B2B Integrator**



## **EBICS Banking Server の概念**

バージョン 5.2.5

**注記**

本書および本書で紹介する製品をご使用になる前に、 25 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、Sterling B2B Integrator のバージョン 5 リリース 2 モディフィケーション 5、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

© Copyright IBM Corporation 2000, 2015.

---

## 目次

<b>EBICS Server の概念 (V5.2.5 以降)</b> . . . . .	<b>1</b>	鍵の管理 . . . . .	13
EBICS Banking Server のアーキテクチャー . . . . .	2	EBICS レポートの生成と取得 . . . . .	15
サブスクリプション・マネージャー情報の管理 . . . . .	6	EBICS サーバーの管理 . . . . .	16
EBICS トランザクションの管理 . . . . .	9	システム・オーダーの管理 . . . . .	16
サブスクリャイバーからのアップロード (FUL) . . . . .	9	オーダー・データの処理 . . . . .	19
EBICS サーバーからのダウンロード (FDL) . . . . .	10	Sterling File Gateway との統合 . . . . .	22
セグメンテーションおよびリカバリー . . . . .	11		
VEU 処理 . . . . .	12	<b>特記事項</b> . . . . .	<b>25</b>



---

## EBICS Server の概念 (V5.2.5 以降)

Electronic Banking Internet Communication Standard (EBICS) はインターネット・ベースの通信およびセキュリティー規格で、主に、企業の支払取引において組織と銀行間のリモート・データ転送に使用されます。

EBICS を使用すると、メッセージの規格や形式に関係なく、データ・ファイルを交換することができます。EBICS では、確立されたデジタル署名と暗号化手順が使用されます。その機能は、XML、HTTPS、TLS、SSL など、インターネット通信およびセキュリティー強化の国際規格に基づいています。また、EBICS にはマルチバンク機能が備わっており、EBICS を採用している国の企業クライアントは、同じソフトウェアを使用して、それらの国の銀行と取引を行うことができます。

(パートナーに関連する) ユーザーが特定の銀行と銀行特有の EBICS トランザクションを実施するには、ユーザーが一連の前提条件を満たしている必要があります。EBICS トランザクションを実施するための基本的な前提条件は、パートナーと銀行間の契約への署名です。この契約で合意する詳細は次のとおりです。

- パートナーが銀行と実施するビジネス・トランザクション (銀行特有オーダー・タイプ) の性質
- ユーザーの銀行口座に関する情報
- 銀行のシステムを使用するパートナーのユーザー
- ユーザーが所有する権限および許可

契約への署名が完了すると、パートナーは銀行のアクセス・データ (銀行パラメーター) を受け取ります。銀行は、契約上の合意に従って、パートナーおよびユーザーのマスター・データを銀行システムで設定します。

その他の前提条件として、サブスクリバターの初期化、ユーザーによる銀行のパブリック証明書のダウンロード、および銀行によるユーザーのパブリック証明書の検証があります。

Sterling B2B Integrator EBICS Banking Server は、銀行とパートナーに関わる、ユーザー管理、証明書管理、安全なファイル・トランザクション、エラー・リカバリー、およびレポート作成の機能を備えた完全な EBICS ソリューションです。EBICS トランザクションの送受信には、Sterling B2B Integrator を使用してください。

Sterling B2B Integrator EBICS Banking Server は、フランス語実装とドイツ語実装の両方について EBICS 仕様 V2.5 をサポートしています。

Sterling File Gateway は Sterling B2B Integrator プラットフォームで作動し、同一または異なる通信プロトコル、ファイル命名規則、およびファイル・フォーマットを使用する内部および外部パートナー間の安全なファイル転送を可能にします。

Sterling File Gateway は、プロセス指向の、拡張性の高いフレームワークでファイル移動の可視性を確保しながら、大規模な大量のファイル転送による移動をサポートします。これにより、プロトコルとファイルのブローカリング、自動化、データ・セキュリティーなどのファイル転送の難題が軽減されます。

## FDL 要求のファイル・システム・スペース所要量

FDL オーダー・タイプはファイル・システムを使用してペイロードを保管するので、それに応じてファイル・システム・ストレージを計画することが重要です。大規模 FDL ペイロードの場合、ペイロード・サイズ自体の約 6 倍のファイル・スペースが必要です。例えば、要求を処理するには、5 GB のペイロードの場合 Sterling B2B Integrator に 30 GB を超えるファイル・スペースが必要です。

クラスター環境で EBICS Banking Server を使用するときは、デフォルトのドキュメント・ストレージ・タイプが「データベース」に設定されている場合であっても、ノード間の共有ファイルシステムをドキュメント・ストレージとして構成する必要があります。詳しい指示については、適切な *Installation* のドキュメンテーションを参照してください。

---

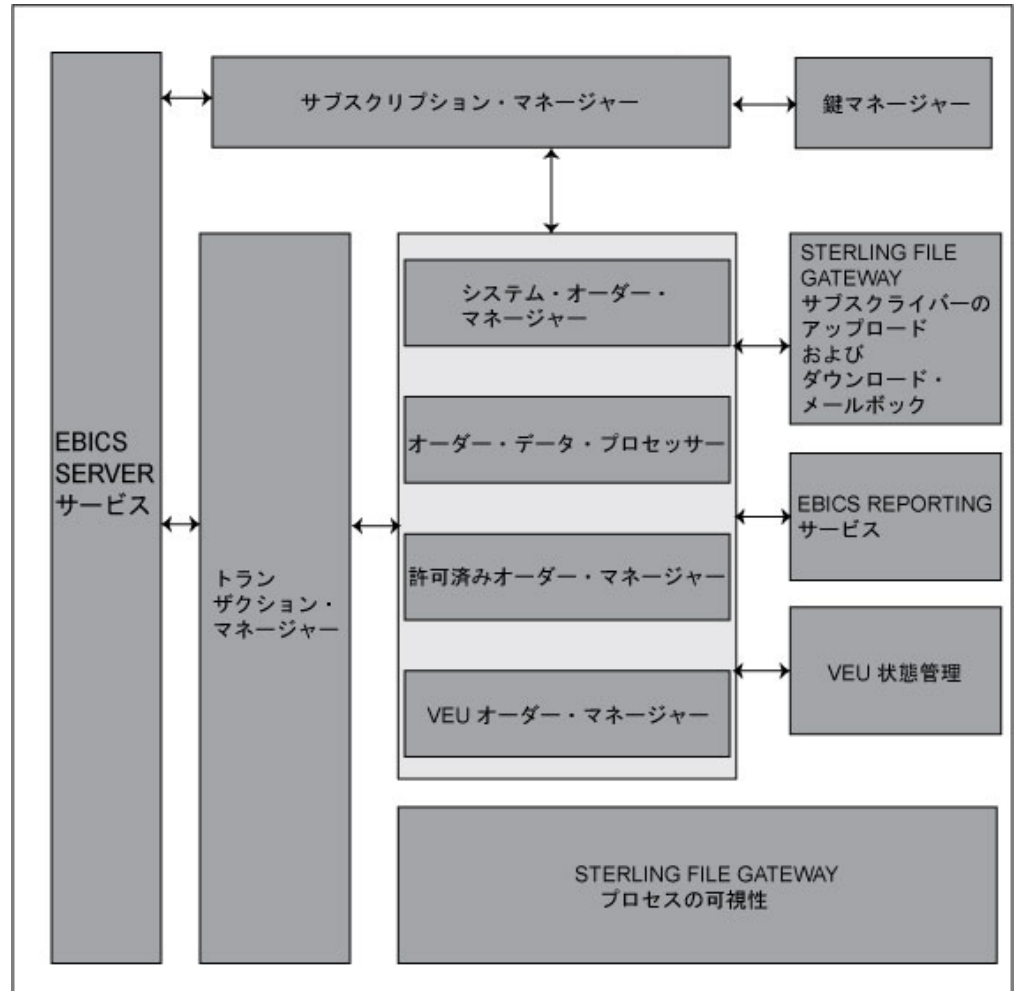
## EBICS Banking Server のアーキテクチャー

EBICS Banking Server では、EBICS を使用してパートナーおよびユーザーと取引を行うことができます。

例えば、プロファイル (銀行、パートナー、およびユーザー) の作成と管理、パートナーおよびユーザーとオーダー・タイプおよびファイル形式との関連付け、ユーザー許可の割り当て、証明書の作成と管理、オーダー・データの処理、プロファイル情報、証明書、およびメッセージの保管と取得、メッセージ・フローおよびトランザクション・フローの管理、安全なプロトコルを使用したファイル転送などの機能があります。

次の図は、EBICS Banking Server のアーキテクチャーを示しています。





サブスクリプション・マネージャーには次のような機能があります。

- プロファイル管理 - 銀行、パートナー、およびユーザーのプロファイルを作成し、管理します。
- オーダー・タイプの構成 - オーダー・タイプおよびファイル形式を構成します。
- オファターの構成 - オーダー・タイプおよびファイル形式のセットを顧客のリストにまとめます。
- ユーザー許可の構成 - オーダー・タイプおよびファイル形式をユーザーに割り当てます。
- サブスクリプション・マネージャー情報のインポート - 銀行、パートナー、ユーザー、オファター、ユーザー許可、オーダー・タイプ、およびファイル形式に関連する構成の詳細を外部リポジトリから EBICS Banking Server にインポートします。
- サブスクリプション・マネージャー情報のエクスポート - 銀行、パートナー、ユーザー、オファター、ユーザー許可、オーダー・タイプ、およびファイル形式に関連する構成の詳細を EBICS Banking Server から外部リポジトリにエクスポートします。

サブスクライバーのアップロードおよびダウンロード・メールボックスは、ユーザー・サブスクリプションの設定時にサブスクリプション・マネージャーで構成します。

鍵管理は、主にサブスクリプション・マネージャーと連携して、証明書を作成、更新、削除、および照会します。

鍵管理には次のような機能があります。

- 自己署名証明書 - 鍵の長さが 2048 ビットの自己署名証明書を生成し、管理します。
- CA 証明書 - CA 証明書を管理します。
- 鍵保管 - 証明書の鍵を保管し、証明書の更新や有効期限を管理します。
- 証明書のインポートおよびエクスポート - 証明書をインポートおよびエクスポートします。
- サブスクライバー・鍵の検証 - ユーザー証明書のハッシュ値を検証します。
- 証明書のハッシュ値 - SHA256 を使用した証明書ハッシュ値の作成をサポートします。

EBICS Server サービスは、サブスクリプション・マネージャーと連携して、メッセージおよびトランザクションの検証と認証に必要な銀行、パートナー、ユーザー、およびオーダー・タイプのプロファイル情報を取得します。また、トランザクション・マネージャーと密接に連携して、すべての EBICS トランザクションを処理します。

EBICS Server サービスには次のような機能があります。

- 要求および応答 - EBICS プロトコル仕様に従って (HTTP および HTTPS 経由の) 着信 EBICS 要求を処理し、適切な応答を生成して要求側に返します。
- メッセージ・フロー - EBICS トランザクションの初期化およびファイル転送フェーズのメッセージ・フローを管理します。
- 認証および承認 - メッセージ認証およびユーザー承認チェックを実行します。

トランザクション・マネージャーは、EBICS Server サービスと密接に連携して、システム・オーダー・タイプと銀行特有オーダー・タイプのアップロードおよびダウンロード・フローを管理します。

トランザクション・マネージャーには次のような機能があります。

- 非同期トランザクション - 銀行特有のアップロード・オーダー・タイプ (FUL) の非同期トランザクション・フローを管理します。また、オーダー・データ・プロセッサと連携して、承認オーダーの処理フローを管理します。オーダー・データをアンパックし、アンパックしたオーダー・データを、ユーザー・プロファイルの設定で定義された宛先のアップロード・メールボックスに送信します。
- 同期トランザクション - アップロードおよびダウンロード・システムのオーダー・タイプおよび銀行特有オーダー・タイプに関する同期トランザクション・フローを管理します。また、システム・オーダー処理、レポート処理 (FDL, PSR)、および銀行特有のダウンロード・オーダー (FDL) 処理のフローを管理します。

- セグメンテーションおよびリカバリー - 再生なしのセグメンテーションおよびエラー・リカバリーを管理します。

システム・オーダー・マネージャーは、鍵管理情報とユーザー参照情報を更新および照会します。

システム・オーダー・マネージャーは、トランザクション・マネージャーおよびサブスクリプション・マネージャーと密接に連携して、ユーザーの鍵証明書および参照情報の更新と照会のほか、銀行パラメーターおよび銀行証明書のダウンロードを行います。

承認オーダー・マネージャーは、オーダー・データ・プロセッサを開始して、FUL オーダー・タイプの要求から受け取ったオーダー・データをアンパックします。さらに、アンパックしたオーダー・データをバックエンド・サブスクライバーのアップロード・メールボックスに転送し、定義された命名規則に従って名前を変更します。

VEU オーダー・マネージャーは、VEU オーダー (オーダー・タイプ HVD、HVE、HVS、HVT、HVU、または HVZ) を処理します。

オーダー・データ・プロセッサは、オーダー・データをパックおよびアンパックします。また、サブスクリプション・マネージャーおよびトランザクション・マネージャーと連携して、オーダー・データのパックとアンパックに必要な関連情報を取得します。オーダー・データ・プロセッサには次のような機能があります。

- パック - オーダー・タイプの要件に応じて、署名、圧縮、暗号化、Base64 エンコードなど、オーダー・データのパックを行います。
- アンパック - オーダー・タイプの要件に応じて、検証、圧縮解除、暗号解除、Base64 デコードなど、オーダー・データのアンパックを行います。

レポート・サービスは、銀行特有のオーダーのトランザクション・フローの非同期アップロード時に行われるオーダー・データのアンパックに関連する支払ステータス・レポート (PSR) を生成します。

VEU 状態管理では、完全には許可されていない (例えば、保留中の署名がある) VEU オーダーに関する情報が保持されます。

*Sterling File Gateway* はテンプレートを使用して各 EBICS トランザクションが解釈される方法を記述し、EBICS トランザクションが送信される方法と場所を判別し、監査およびトラブルシューティングのために転送の詳細を表示可能です。

*Sterling File Gateway* には次のような機能があります。

- ファイルまたはファイル名の変換 - ファイル名、システム全体のポリシー、グループ・ポリシー、パートナー固有のポリシー、および圧縮と圧縮解除、PGP 暗号化と暗号解除、署名などの共通的なファイル処理タスクを入力ファイルと出力ファイルの間でマッピングします。
- ファイル転送の可視化 - 監視およびレポート作成を目的として、イベントを記録します。また、入出力ファイルの構造の処理や動的なルート決定を詳細に追跡します。すべてのユーザーのデータ・フローを表示およびフィルタリングすることもできます。

- 広範な通信プロトコルのサポート - インストール時点で FTP、FTP/S、SSH/SFTP、SSH/SCP、および Sterling Connect:Direct がサポートされていますが、拡張機能を使用して、AS2、AS3、Odette FTP などの追加プロトコルを構成することもできます。
- パートナー・インターフェース (myFileGateway) - Web ブラウザー・ベースのインターフェースを使用して、パートナーはファイルのアップロードおよびダウンロード、イベントに関する通知の登録、パスワードの管理、ファイル転送アクティビティの検索と表示、ファイル転送アクティビティに関するレポートの生成を行うことができます。
- 柔軟なメールボックス構造 - パターン・マッチング・ポリシーを利用するメールボックス構造を指定したり、すべてのパートナーについて真 (true) でなければならない属性や一部のパートナーについて真 (true) でなければならない属性を指定したりすることができます。
- 動的ルーティング - メールボックス構造、ファイル名、ビジネス・プロセスから取得したコンシューマー名、またはマップから取得したコンシューマー名のいずれかを使用して、実行時にコンシューマーを決定します。

---

## サブスクリプション・マネージャー情報の管理

Sterling B2B Integrator の「サブスクリプション・マネージャー」メニューでは、次の作業を行うことができます。

- システム・データベースでの銀行、パートナー、およびユーザーのプロファイルの作成と管理
- オファーの作成と管理
- オファーへのオーダー・タイプおよびファイル形式の割り当て
- ユーザーへの許可の割り当て

銀行には、一意の銀行 ID を指定して、プロファイルを 1 つだけ作成することができます。銀行プロファイルに含まれる情報は次のとおりです。

- 銀行の一意の ID

注: 銀行 ID ごとに一意のポート番号が必要です。

- 銀行の名前
- 銀行の住所
- パブリックおよびプライベート暗号化、認証、および識別証明書
- 銀行の HTTP URL
- EBICS プロトコル・バージョン

1 つの銀行に複数の URL を指定することができます。要求を銀行に送信できるように、該当する銀行 URL をユーザーに割り当てます。Uniform Resource Indicator (URI) は、ポートで待機して EBICS 要求があれば受信するように、HTTP Server アダプター内で構成します。

サポートされている銀行プロトコルおよびプロセス・タイプのバージョンは、次のとおりです。

- EBICS プロトコル・バージョン - H004、H003H000

- 署名バージョン - A005、A006
- 認証バージョン - X002
- 暗号化バージョン - E002

各パートナーに 1 つ以上の口座情報とパートナー ID を指定することができます。口座番号は、国内標準 (ドイツ) または国際標準 (IBAN) 形式で指定する必要があります。パートナー ID は、オファーと関連付けることができます。パートナー・プロフィールに含まれる情報は次のとおりです。

- パートナーの一意の ID
- パートナーの組織コード
- パートナーの名前
- パートナーの住所
- 口座 ID および口座所有者の名前
- トランザクションを実行する際に使用する通貨
- 口座番号
- 銀行コード

ユーザーは、1 つ以上のパートナーに属することができます。銀行にユーザーを作成する際に、ユーザーをパートナーと関連付けても、関連付けなくてもかまいません。パートナーとユーザーの間で EBICS メッセージを交換できるようにするには、ユーザー ID をパートナー ID と関連付ける必要があります。

ユーザーは、次の 2 つの独立した通信パスを使用して、パブリック証明書を銀行に送信します。

- INI - 銀行特有の公開鍵を送信
- HIA - パブリック識別および認証鍵とパブリック暗号鍵を送信

ユーザーが最初にパートナーに割り当てられたとき、ユーザーのステータスは「新規」です。ユーザーが INI 要求のみを該当する銀行に送信した場合、ステータスは「一部初期化済み (INI)」に変わります。ユーザーが HIA 要求のみを銀行に送信した場合、ステータスは「一部初期化済み (HIA) (Partly Initialized (HIA))」に変わります。ユーザーが INI 要求と HIA 要求の両方を銀行に送信すると、ステータスは「初期化済み (Initialized)」に変わります。ユーザーは、INI キーおよび HIA キーの初期化文字を銀行に E メールで送信します。銀行は、INI および HIA の初期化文字を受け取ると、証明書のハッシュ値をデータベースと照合し認証します。検証が正常に完了すると、ユーザーのステータスは「準備完了 (Ready)」に設定され、ユーザーは銀行と取引を行えるようになります。ユーザーはその後、HPB システム・オーダー・タイプを使用して、銀行のパブリック証明書をダウンロードします。

ユーザー・ステータスが「準備完了」に設定された後、HKD および HTD のオーダー・タイプを使用して、銀行によって保管されたサブスクライバー情報を取得できます。

EBICS Subscription Manager サービスを使用して、INI および HIA の初期化文字に記載されたキーを検証します。検証が正常に完了すると、ユーザーのステータスが更新されます。例えば、「準備完了」は、ユーザーが HIA および INI の初期化文字を銀行に送信したことを示します。このサービスを使用して、銀行のシステム・

データベースとの間でサブスクリプション・マネージャーのデータをインポートしたりエクスポートしたりすることもできます。

ユーザー・プロフィールに含まれる情報は次のとおりです。

- ユーザーの一意の ID
- ユーザーの名前
- ユーザーの住所
- ユーザーが関連付けられているパートナー ID
- メッセージのアップロード、ダウンロード、およびアーカイブを行うためのメールボックスの設定

EBICS オーダー・タイプでは、EBICS サーバーと EBICS クライアントの間で実行できるさまざまなトランザクションを指定します。1 つのオーダーのタイプに複数のファイル形式を指定できますが、ファイル形式を指定しなくてもかまいません。ファイル形式は、銀行特有のアップロードおよびダウンロード・オーダー・タイプと関連付けることができます。EBICS クライアントから EBICS サーバーにオーダー・データをアップロードする場合にはアップロード・オーダー・タイプを使用し、EBICS サーバーから EBICS クライアントにオーダー・データをダウンロードする場合にはダウンロード・オーダー・タイプを使用します。オーダー・タイプに含まれる属性は次のとおりです。

- オーダー・タイプ
- EBICS プロトコル・バージョン
- 転送タイプ - アップロードまたはダウンロード
- オーダー・データ・タイプ - システムまたは銀行特有

ファイル形式に含まれる属性は次のとおりです。

- ファイル形式
- ファイル形式の国コード

銀行では 1 つ以上のオファーを作成することができます。オファーを使用すると、オーダー・タイプおよびファイル形式のセットをパートナーのリストに簡単にまとめることができます。銀行とパートナー間で取引を行えるように、各パートナーにオーダー・タイプのリストが割り当てられます。銀行は、オファーを使用することで、パートナーとの契約を簡単にセットアップすることができます。オファーに含まれる情報は次のとおりです。

- 銀行 ID
- オファーの名前
- パートナーがメッセージを交換する際に使用できるオーダー・タイプおよびファイル形式
- オーダー・タイプの権限のレベル
- オーダーを許可するのに必要な署名の数

パートナーは、1 人以上のユーザーと関連付けることができます。銀行は、次の許可をユーザーに割り当てます。

- ユーザーがメッセージを交換する際に使用できるオーダー・タイプおよびファイル形式

- オーダー・タイプの権限のレベル
- ユーザーが取引できる (特定パートナー・アカウントの) 最大金額 。複数のパートナー・アカウントを異なる最大金額に関連付けることができます。
- ユーザーの最高金額を指定する際に使用する通貨。通貨は、最大金額に関連付けられているパートナー・アカウントによって異なります。

---

## EBICS トランザクションの管理

EBICS サーバーのトランザクション・マネージャーは、トランザクションの状態を管理します。また、XML 応答メッセージを生成するのに必要なセグメントを特定します。

トランザクション・マネージャーでは、アップロードおよびダウンロード・トランザクション・フローが処理されるほか、オーダー・データのセグメンテーションとリカバリーがサポートされます。

### サブスクリャイバーからのアップロード (FUL)

FUL オーダー・タイプを使用して銀行にデータをアップロードします。

アップロード・トランザクションは、次のフェーズで構成されます。

- 初期化
- データ転送

ユーザーがアップロード (FUL) 要求を銀行に送信します。FUL は、銀行特有のアップロード・オーダー・タイプです。

**重要:** 大規模 FUL ペイロードの場合、EBICS Server サービスの最大アイドル時間 (MaxIdleTime) 設定を増加する必要があります。MaxIdleTime の設定時間が少なすぎると、トランザクションが完了前にキャンセルになる可能性があります。大規模 FUL ペイロードに適切な設定は 300 分です。

EBICS Order Authorization サービスは、銀行特有のアップロード・オーダー・タイプの着信オーダー要求を処理します。オーダーが必要な数の署名を入手していれば、そのオーダーはサブスクリャイバーのアップロード・メールボックスに転送されます。それ以外の場合、必要な数の署名が取得されるまで、オーダー・データはデータベースに保持されます。

handleEBICSRequest ビジネス・プロセスがユーザーの要求を受信します。ユーザーの要求にオーダー・データの最後のセグメントが含まれていれば、

EBICSOrderAuthorizationProcessing ビジネス・プロセスが非同期で起動して、オーダー・データがアンパックされて、次のファイルが生成されます。

**注:** オーダー・データのアンパックには、オーダー・データのデコード、暗号化解除、および圧縮解除が含まれます。

- .DAT - アンパックされたオーダー・データをユーザーのアップロード・メールボックスに格納します。
- .SIG - オーダー・データの署名をユーザーのアップロード・メールボックスに格納します。

- .PRM - オーダー・パラメーターをユーザーのアップロード・メールボックスに格納します。
- .PSR - 非同期処理のステータス・レポートをユーザーのダウンロード・メールボックスに格納します。

## 初期化处理

ユーザーが、着信オーダーに関する情報を含む要求を送信することによって、トランザクションを開始します。この情報に基づいて、EBICS サーバーでオーダー・タイプが検証されます。要求を受け付ける前に、メッセージの再生テストが行われて、メッセージ認証が検証され、ユーザー承認がチェックされます。

オーダー・データの検証が正常に完了すると、銀行はトランザクション ID を生成し、その ID をユーザーへの応答に挿入します。

## データ転送処理

オーダー・データの転送に複数のセグメントが必要な場合、銀行はメッセージ認証を実行して、トランザクション、およびセグメントの番号とサイズを検証します。EBICS サーバーがオーダー・データの最後のセグメントを受け取ると、オーダー・データ全体が EBICSOrderAuthorizationProcessing ビジネス・プロセスに非同期で転送されて、トランザクションが終了します。

EBICSOrderAuthorizationProcessing ビジネス・プロセスでは、オーダー・データがアンパックされ、ユーザーのアップロード・メールボックスに転送されます。また、ポストプロセッシング・レポート (PSR) が生成され、ユーザーのダウンロード・メールボックスに転送されます。このビジネス・プロセスではさらに、.SIG および .PRM ファイルが生成され、ユーザーのアップロード・メールボックスに転送されます。EBICSOrderAuthorizationProcessing ビジネス・プロセスで無効な電子署名などのエラーが検出されると、.err ファイルが生成されます。必要に応じて、.err ファイルを使用して、無効なオーダー・データ・ファイルを調べてください。

## EBICS サーバーからのダウンロード (FDL)

FDL オーダー・タイプを使用して銀行からデータをダウンロードします。

ダウンロード・トランザクションは、次のフェーズで構成されます。

- 初期化
- データ転送
- 承認

ユーザーが FDL オーダー・タイプを銀行に送信します。このユーザーは、FUL 要求のステータスを取得するために、.PSR レポートのダウンロードを要求します。FDL オーダー・タイプを使用して、.PSR 以外の有効なファイル形式のダウンロードを要求することもできます。

**重要:** 大規模 FDL ペイロードの場合、EBICS Server サービスの最大アイドル時間 (MaxIdleTime) 設定を増加する必要があります。この設定時間が少なすぎると、トランザクションが完了前にキャンセルになる可能性があります。大規模 FDL ペイロードに適切な設定は 300 分です。



## 初期化处理

銀行がユーザーからのメッセージを検証します。銀行は、ユーザーの要求を検証すると、要求のファイル形式情報に基づいて、ユーザーのダウンロード・メールボックスからオーダー・データを収集します。

ファイル形式と一致するメッセージが複数ある場合、銀行は各メッセージの内容を 1 つのオーダー・データに結合し、オーダー・データ・プロセッサを同期的に起動して、オーダー・データをバックします。

エンコードされた形式のオーダー・データが 1 MB を超えると、オーダー・データはセグメントに分割されます。オーダー・データの最初のセグメントとトランザクション ID がユーザーへの応答に挿入されます。

## データ転送処理

ユーザーが次のデータ・セグメントに対する要求を送信します。銀行がメッセージを認証し、トランザクション、およびセグメントの番号とサイズを検証します。

各転送フェーズで、オーダー・データの最後のセグメントがユーザーへの応答に挿入されるまで、銀行はすべてのセグメントを転送します。

## データ承認処理

オーダー・データの最後のセグメントを銀行から受け取ると、ユーザーは、データ転送が正常に完了したことを示す最後のフェーズ、承認要求を開始します。

ユーザーから肯定応答 (受信コード = 0) を受け取った場合、銀行は、ダウンロードしたメッセージをユーザーのダウンロード・メールボックスからユーザーのアーカイブ・メールボックスに移動します。ユーザーから否定応答を受け取った場合は、ダウンロードしたメッセージをユーザーのダウンロード・メールボックス内に保持します。

ユーザーがユーザーのアーカイブ・メールボックスから .PSR レポート以外の有効なファイル形式をダウンロードする場合は、EBICS 要求で日付範囲を指定する必要があります。ユーザーは、.DAT ファイルがユーザーのダウンロード・メールボックスからユーザーのアーカイブ・メールボックスに移動したときのドロップ日付と一致する日付範囲を指定しなければなりません。

## セグメンテーションおよびリカバリー

オーダー・データ要求 (アップロードまたはダウンロード) は、圧縮、暗号化、および Base64 でエンコードされた形式で 1 MB を超えることはできません。オーダー・データ要求が 1 MB を超える場合、エンコードされた形式をセグメントに分割する必要があります。EBICS Banking Server は、オーダー・データを元の形式に復元するために、これらのすべてのセグメントを結合します。

オーダー・データ・セグメントの配信中にエラーが発生した場合は、リカバリーを実行できます。ユーザーは、エラーの発生に応じてサーバーから送信されたリカバリー・ポイントに従って、適切なセグメントをダウンロードまたはアップロードすることができます。

リカバリーを実行することで、エラーが発生した場合でも、オーダーの送信を続行することができます。その際、正常に送信されたオーダー・データ・セグメントをすべて再送信する必要はありません。

リカバリー・ポイントを使用すると、一連のトランザクション・ステップでそのリカバリー・ポイントに続いて実行されるトランザクション・ステップからトランザクションを続行することができます。リカバリー・ポイントは、リカバリー・プロセス中に設定する必要があります。

- アップロード・トランザクションの場合、リカバリー・ポイントは、銀行が正常に要求メッセージを受信して、応答をユーザーに送信した最後のトランザクション・ステップです。リカバリー・ポイントは、銀行システムでのトランザクションの状態によって決定されます。
- ダウンロード・トランザクションの場合、リカバリー・ポイントが複数存在することがあります。銀行が正常に要求メッセージを受信して、応答をユーザーに送信した、トランザクションの以前のトランザクション・ステップすべてがリカバリー・ポイントとなります。

## VEU 処理

EBICS Banking Server は分散電子署名 (VEU) をサポートしています。これにより、複数のパートナー (またはサブスクリイバー) がオーダーを許可できます。

VEU は、分散電子署名 (Distributed Electronic Signature) を意味するドイツ語の略語です。VEU を使用すると、複数のパートナー (またはサブスクリイバー) がオーダーを許可できます。異なる顧客の異なるパートナーまたは同じ顧客の異なるパートナーが特定のオーダーに署名できます。パートナーは、保留中の署名があるオーダーを要求すること、およびそれらに署名することやキャンセルすることができます。以下のいずれかが発生するまで、EBICS Banking Server の VEU 管理システムにより、異なるパートナーからの署名が保留中のオーダーが保存されます。

- 必要な数の許可済み署名を受信した。
- オーダーがキャンセルされた。

VEU は以下のオーダー・タイプを使用します。

- HVU
- HVD
- HVZ
- HVE
- HVS
- HVT (オプション)

顧客の許可済み署名者は、各種署名プロセスを使用できます。これらのプロセスでは、各種ハッシュ値を生成する各種ハッシュ・プロセスがサポートされている場合があります。VEU プロセスでは、オーダー・タイプ HVD および HVZ が実行されると、オーダー・データのハッシュ値が提供されます。このハッシュ値は、HVZ および HVD を実行するサブスクリイバーが使用する署名バージョンから導出されます。このハッシュ値は、使用されている署名バージョンで、属性として提供されません。

通常の VEU プロセスの要約を以下に示します。

1. EBICS 顧客 (PartnerA) が、オーダー属性 OZHNN および署名クラス E または T の署名を使用した EBICS トランザクションでオーダー・データを転送することでオーダーを開始します。
2. これを EBICS Banking Server が受信すると、VEU 管理システムがオーダー・タイプおよび既に送信されている署名 (それらのクラスを含む) を分析します。オーダーの処理のためにさらに署名が必要な場合、そのオーダーは VEU プロセスの途中でそのハッシュ値とともに保管されます。
3. 保留中の署名があり、保管されているオーダーに署名する必要がある別の EBICS カスタマー (Partner B) が、オーダー・タイプ HVU または HVZ を使用して照会を行い、署名を許可されているオーダーを検出します。この応答には、以下に関する情報が含まれます。
  - オーダー・タイプ
  - オーダー番号
  - 必要な署名の数と既に提供されている署名の数 (それらの独自の署名がまだ必要か、または既に提供されているかを含む)
  - 元のオーダー・パーティー
  - 解凍されたオーダー・データのサイズ
  - (オーダー・タイプ HVZ のみ) オーダー・データのハッシュ値オーダー・タイプ HVZ が使用されている場合、次のステップはスキップされません。
4. パートナー B がオーダー・タイプ HVD を使用してオーダーをチェックし、そのオーダーのハッシュ値を取得します。
5. オプション。オーダー・タイプ HVT を銀行がサポートしている場合、パートナー B はオーダー・タイプ HVT を使用して追加のオーダー詳細をダウンロードできます。要求パラメーターに基づき、個々のオーダー・トランザクションに関する情報 (口座データ、金額情報、処理日付、利用データ、およびその他の説明) または完全なオーダー・データを受け取ります。
6. 必要な情報をすべて受け取った後、パートナー B はオーダー・タイプ HVE を使用してオーダーに署名できます。EBICS Banking Server の VEU 管理システムにより、署名が検証され、オーダーに追加されます。
7. パートナー B は、オーダー・タイプ HVS を使用してオーダーをキャンセルすることを選択できます。
8. すべての署名が完了した後、EBICS Banking Server はオーダーを完全に処理します。

---

## 鍵の管理

Sterling B2B Integrator リポジトリに存在する証明書を挿入、更新、および取得することができます。

Sterling B2B Integrator リポジトリでは、Base64 でエンコードされた証明書 (パブリックまたはプライベート) の挿入や、証明書のインポートおよびエクスポートを行うことができます。

Sterling B2B Integrator では、次のタスクを実行することもできます。

- 鍵の長さが 2048 ビットの EBICS 用自己署名証明書の作成
- CA 証明書の管理
- 証明書の保管、および証明書の更新や有効期限の管理
- ユーザーのパブリック証明書の承認
- ハッシュ・アルゴリズムとして SHA256 を使用した、次のサブスクリャイパー・キーの検証
  - 識別および認証鍵のハッシュ値 (16 進数フォーマット)
  - 暗号鍵のハッシュ値 (16 進数フォーマット)
  - 電子署名鍵のハッシュ値 (16 進数フォーマット)

Sterling B2B Integrator 内の証明書を外部システムにエクスポートするには、EBICS Export Certificate サービスを使用します。このサービスは、Sterling B2B Integrator 内の証明書を外部データベースまたは外部システムと同期させる場合に使用します。

外部リポジトリの証明書を Sterling B2B Integrator に追加するには、EBICS Import Certificate サービスを使用します。有効期限が切れた証明書や無効な証明書を削除することもできます。

## 鍵マネージャーの機能

鍵の管理と保管では、以下の機能が実行されます。

- 重複鍵の検証 - 認証または暗号化に使用する証明書を ES 証明書と同じにすることはできません。認証または暗号化のための固有の鍵セットおよび署名を使用してください。
- X.509 キー使用の拡張 - EBICS Banking Server は、キー使用の拡張として X.509 の使用をサポートしています。
- OCSP および CRL 証明書の検証

鍵マネージャーは、Sterling B2B Integrator リポジトリ内の証明書を管理します。鍵マネージャーは、Sterling B2B Integrator リポジトリに証明書を挿入し、またリポジトリ内の証明書を更新、および取得します。さらに証明書のハッシュ値の計算などの機能を証明書において実行します。

鍵マネージャーは、サーバーにチェックインされているクライアント証明書を使用前に検証します。認証局から CA 署名証明書を取得する必要があります。CA 署名証明書では、発行者が証明書に署名します。ユーザー証明書の認証性を検査するために、EBICS Banking Server はルート CA 証明書までのチェーン署名検証を実行します。

EBICS 管理者は、EBICS トランザクションを開始する前に、Sterling B2B Integrator CA 証明書ストアに CA 署名証明書および中間 CA 署名証明書をチェックインする必要があります。

クライアントは、次の 3 種類の証明書を提供する必要があります。

- 認証証明書
- 暗号化証明書

- 電子署名 (ES) 証明書

デジタル署名を検証するために、認証証明書の公開鍵が使用されます。認証証明書は CA 署名または自己署名を使用できます。認証証明書の鍵使用フィールドの値は「デジタル署名」です。デジタル署名は、エンティティー認証やデータ送信元認証で整合性を保つために使用されます。

オーダー・データを暗号化するために、暗号化証明書の公開鍵が使用されます。暗号化証明書として CA 署名または自己署名を使用できます。暗号化証明書の鍵使用フィールドの値は「鍵暗号化 (Key Encipherment)」です。EBICS では、暗号化済みまたは暗号化解除済みオーダー・データをストリーミングするために対称鍵が使用されます。この対称鍵は、移送のために暗号化証明書の公開鍵値で暗号化されません。鍵を暗号化するプロトコルを使用する証明書が存在する場合、鍵暗号化が使用されます。

オーダー・データの署名を検証するために、電子署名 (ES) 証明書の公開鍵が使用されます。電子署名証明書の公開鍵値は、認証または暗号化証明書と同じにはできません。電子署名証明書の鍵使用フィールドの値は「否認防止」です。否認防止では、署名エンティティーがアクション (証明書または CRL の署名を除く) を誤って拒否しないように保護できます。電子署名は次の 2 つのタイプがあります。

- トランスポート署名 – CA 署名または自己署名を使用できます。
- 個人署名 – CA 署名を使用する必要があります。

---

## EBICS レポートの生成と取得

各アップロード・オーダー (FUL) 要求で支払ステータス・レポート (PSR) を生成するには、EBICS レポート・サービスを使用します。.PSR レポートは XML 形式で、pain.002.001.02 スキーマに準拠しています。.PSR レポートが正常に生成されると、EBICS ユーザーのダウンロード・メールボックスに格納されます。

.PSR レポートは、各 FUL の非同期オーダー処理後に生成されます。ユーザーは、FileFormat を pain.002.001.02.ack に指定して FDL 要求を送信することで、.PSR レポートを取得できます。EBICS 要求で日付範囲が指定されていない場合、銀行はユーザーのダウンロード・メールボックスで PSR レポートを連結し、オーダー・データを EBICS 応答にパッケージ化します。

FDL 要求の FDLOrderParams 要素で指定されたパラメーター値に基づいて、銀行がユーザーから肯定応答を受け取ると、ユーザーのダウンロード・メールボックス内の .PSR レポートがユーザーのアーカイブ・メールボックスに移動されます。指定されたタイムアウト期間が経過しても、ユーザーから肯定応答を受け取らなかった場合、EBICS Server サービスのスケジューラーによって、ユーザーのダウンロード・メールボックス内の .PSR レポートの抽出可能カウントが 1 に戻され、ユーザーは再度 .PSR レポートをダウンロードすることができます。

ユーザーがユーザーのアーカイブ・メールボックスから .PSR レポートをダウンロードする場合は、EBICS 要求で日付範囲を指定する必要があります。ユーザーは、.PSR レポートがユーザーのダウンロード・メールボックスからユーザーのアーカイブ・メールボックスに移動したときのドロップ日付と一致する日付範囲を指定しなければなりません。

---

## EBICS サーバーの管理

EBICS サーバーは、Sterling B2B Integrator のサービスとして実装されます。EBICS Server サービスは、EBICS プロトコル仕様に従って (HTTP および HTTPS 経由の) 着信 EBICS 要求を処理し、適切な応答を生成してユーザーに返します。

EBICS サーバーは、電子署名 (ES) の生成と検証、および EBICS メッセージの識別と認証を処理します。また、サブスクリプション・マネージャーと連携して、メッセージおよびトランザクションの検証と認証に必要な銀行、パートナー、ユーザー、およびオーダー・タイプのプロファイル情報を取得します。FUL や FDL などの要求の処理フロー (非同期および同期) も、このサービスによって管理されます。EBICS リポジトリを更新し、同期トランザクション中に外部アプリケーションにイベント通知を送信するようにサービスを構成することができます。EBICS トランザクションの初期化および転送フェーズのメッセージ・フローを管理することも、このサービスの重要な役割の 1 つです。銀行システムでの EBICS トランザクションのライフサイクルおよび未完了トランザクションのステータスは、送信されたオーダー・データ・セグメントおよび電子署名 (ES) の中間ストレージとしても機能する EBICS サーバーによって管理されます。

銀行特有のオーダー・データをダウンロードする際、EBICS サーバーは使用可能なすべてのオーダー・データをユーザーのメールボックスに収集し、1 つのドキュメントに連結します。さらに、そのドキュメントをオーダー・データ・プロセッサに送信して、ドキュメントをバックします。つまり、ドキュメントの署名、圧縮、暗号化、およびエンコードを行います。

EBICS Server サービスの構成については、「*EBICS Server* サービス」を参照してください。

---

## システム・オーダーの管理

システム・オーダー・マネージャーは、トランザクション・マネージャーおよびサブスクリプション・マネージャーと密接に連携して、ユーザーの鍵証明書および参照情報の更新と照会のほか、銀行パラメーターおよび銀行証明書のダウンロードを行います。また、プロファイル情報に基づいて、XML オーダー・データを生成および取得します。

さらに、システム・オーダー・マネージャーは、アップロードおよびダウンロード・システム・オーダーの実装を処理します。次の表は、EBICS トランザクションについてサポートされているアップロード・システム・オーダー・タイプのリストです。

アップロード・システム・オーダー・タイプ	説明
INI	サブスクリプターの初期化で使用されます。顧客の銀行特有のパブリック証明書を EBICS Banking Server に送信します。オーダー・データは圧縮され、Base64 でエンコードされます。

アップロード・システム・オーダー・タイプ	説明
HIA	サブスクライバーの初期化のフレームワーク内で、識別、認証、および暗号化に関するユーザーのパブリック証明書を送信するのに使用されます。オーダー・データは圧縮され、Base64 でエンコードされます。
PUB	顧客の証明書を更新するのに使用されます。EBICS Banking Server を更新するために、顧客の銀行特有のパブリック証明書を送信します。オーダー・データは署名、圧縮、および暗号化され、Base64 でエンコードされます。
HCA	顧客の証明書を更新するのに使用されます。EBICS Banking Server を更新するために、次の証明書を送信します。 <ul style="list-style-type: none"> <li>• 識別および認証パブリック証明書</li> <li>• 暗号化パブリック証明書</li> </ul> オーダー・データは署名、圧縮、および暗号化され、Base64 でエンコードされます。
HCS	顧客の証明書を更新するのに使用されます。EBICS Banking Server を更新するために、次の証明書を送信します。 <ul style="list-style-type: none"> <li>• 銀行特有のパブリック証明書</li> <li>• 識別および認証パブリック証明書</li> <li>• 暗号化パブリック証明書</li> </ul> オーダー・データは署名、圧縮、および暗号化され、Base64 でエンコードされます。
SPR	ユーザーのアクセス許可を保留するのに使用されます。オーダー・データは署名、圧縮、および暗号化され、Base64 でエンコードされます。

次の表は、EBICS トランザクションについてサポートされているダウンロード・システム・オーダー・タイプのリストです。

ダウンロード・システム・オーダー・タイプ	説明
HPB	EBICS Banking Server から銀行のパブリック証明書をダウンロードするのに使用されます。オーダー・データは圧縮および暗号化され、Base64 でエンコードされます。応答メッセージには、認証証明書を使用して XML デジタル署名が行われます。オーダー・データには署名は行われません。

ダウンロード・システム・オーダー・タイプ	説明
HPD	EBICS Banking Server から銀行パラメーターをダウンロードするのに使用されます。オーダー・データは圧縮および暗号化され、Base64 でエンコードされます。応答メッセージには、認証証明書を使用して XML デジタル署名が行われます。オーダー・データには署名は行われません。
HEV	サポートされている EBICS バージョンに関する情報をダウンロードするのに使用されます。応答メッセージは平文です。HEV 応答にオーダー・データはありません。
HKD	顧客データおよびサブスクリイパー・データをダウンロードするために使用されます。ユーザーが「準備完了」ステータスのときに使用できます。銀行が保管した、サブスクリイパーの会社および関連するサブスクリイパーに関する情報を取得します (銀行の独自情報を含む)。オーダー・データは圧縮および暗号化され、Base64 でエンコードされます。応答メッセージには、認証証明書を使用して XML デジタル署名が行われます。オーダー・データには署名は行われません。
HTD	顧客データおよびサブスクリイパー・データをダウンロードするために使用されます。ユーザーが「準備完了」ステータスのときに使用できます。銀行が保管したサブスクリイパーの会社に関する情報または銀行の独自情報を取得します。オーダー・データは圧縮および暗号化され、Base64 でエンコードされます。応答メッセージには、認証証明書を使用して XML デジタル署名が行われます。オーダー・データには署名は行われません。

システム・オーダー・マネージャーは、銀行が保管したサブスクリイパーの会社に関する情報を取得します。サブスクリイパーは、ユーザー・ステータスが、ユーザーと銀行が取引できることを示す「準備完了」に設定された後、HKD および HTD オーダー・タイプを使用して、銀行が保管した、サブスクリイパーの会社とすべての関連サブスクリイパーに関連する情報を取得できます。銀行の応答には、顧客の口座のリストが含まれます。

以下の条件が少なくとも 1 つ満たされる場合、口座情報が HKD 応答に含まれます。

- 銀行との契約上の合意で、口座の収支報告書が顧客と共有されることが指定される。
- 顧客のサブスクリイパーの少なくとも 1 人に口座に署名する許可が与えられている。



サブスクライバーは、HTD オーダー・タイプを使用して、銀行が保管したサブスクライバーの会社に関する情報、または銀行の独自情報を取得できます。ただし、会社の関連サブスクライバーに関する情報は、このオーダー・タイプでは共有されません。会社および関連サブスクライバーに関する情報（銀行の独自情報を含む）を取得するには、HKD オーダー・タイプを使用する必要があります。HKD 応答および HTD 応答では、サブスクライバーがアクセス権を持つ、パートナーの関連口座がリストされます。

HKD ダウンロード・システム・オーダーの応答メッセージには、以下のパラメーターが含まれます。

- HostID
- PartnerInfo - 住所、サブスクライバーがアクセス権を持つ口座情報、パートナーが使用を許可されているオーダー・タイプなど、パートナーの詳細が含まれます。
- UserInfo - ユーザー ID、サブスクライバーのステータス、ユーザー許可情報など、サブスクライバーの詳細が含まれます。ユーザー許可情報には、許可レベルのリスト（オーダー・タイプ、関連する口座、限度額など）が含まれます。

---

## オーダー・データの処理

オーダー・データを安全に転送するには、オーダー・データをバックする必要があります。オーダー・データのバックには、オーダー・タイプの要件に応じて、署名、圧縮、暗号化、および Base64 エンコードが含まれます。受信者が属性を表示するには、オーダー・データをアンパックする必要があります。オーダー・データのアンパックには、オーダー・タイプの要件に応じて、検証、圧縮解除、暗号化解除、および Base64 デコードが含まれます。

オーダー・データ・プロセッサは、オーダー・データをバックおよびアンパックします。また、サブスクリプション・マネージャーおよびトランザクション・マネージャーと連携して、オーダー・データのバックとアンパックに必要な関連情報を取得します。例えば、プロファイル情報には、トランザクション ID、フローの方向（アップロードまたはダウンロード）、応答タイプ（同期または非同期）、必要なプロセスのタイプ、暗号化された鍵のオブジェクト ID、電子署名 (ES) のオブジェクト ID が含まれる場合があります。EBICS Order Processing サービスは、EBICS トランザクションおよびユーザーの取得と、暗号化された対称鍵のバックおよびアンパックを実行します。取得されたプロファイル情報に基づいて、EBICS Order Processing サービスは、オーダー・データのバックまたはアンパックが必要かどうかを判断し、適切なバックまたはアンパック・サービスを呼び出します。

承認オーダー・マネージャーは、オーダー・データ・プロセッサを開始して、FUL オーダー・タイプの要求から受け取ったオーダー・データをアンパックします。さらに、アンパックしたオーダー・データをバックエンド・サブスクライバーのアップロード・メールボックスに転送し、定義された命名規則に従って名前を変更します。

EBICS Order Processing サービスとは別に、Sterling B2B Integrator では、オーダー・データの処理に次のサービスを使用することができます。

- EBICS Order Authorization サービスは、銀行特有のアップロード・オーダー・タイプ (FUL) の着信オーダー要求を処理します。オーダーが必要な数の署名を満たしていれば、このサービスによりそのオーダーはサブスクライバーのアップロード・メールボックスに転送されます。そうでない場合は、オーダーを保留中のオーダーのメールボックスに転送します。
- EBICS Order Streaming サービスは、Sterling B2B Integrator のパイプライン機能を使用して、オーダー・データをパックおよびアンパックします。
- EBICS ES Packaging サービスは、ES の署名および検証時に使用される鍵情報をパックまたはアンパックします。
- EBICS Compression サービスは、パイプライン・モードで zlib を使用して、オーダー・データの圧縮および圧縮解除を実行します。
- EBICS Encryption サービスは、パイプライン・モードで AES-128 アルゴリズムを使用して、オーダー・データの暗号化および暗号化解除を実行します。E002 暗号化アルゴリズムがサポートされています。
- EBICS Encoding サービスは、パイプライン・モードで Base64 方式を使用して、オーダー・データのエンコードおよびデコードを実行します。
- EBICS Signing サービスは、パイプライン・モードで計算された SHA-256 ダイジェストに対してオーダー・データの署名および検証を実行します。A005 および A006 署名アルゴリズムがサポートされています。

アップロード・トランザクションについてはオーダー・データをアンパックし、ダウンロード・トランザクションについてはオーダー・データをパックする必要があります。

パック・プロセスには次の手順が含まれます。ただし、オーダー・タイプによっては、次の 1 つ以上のプロセスが不要な場合もあります。

1. 署名
2. 圧縮
3. 暗号化
4. Base64 エンコード

次の例は、オーダー・タイプの暗号化を示しています。ビジネス・プロセスが暗号化サービスを呼び出します。オーダー・データが署名されている場合は、ビジネス・プロセスが暗号化サービスに対称鍵を渡します。オーダー・データが署名されていない場合は、暗号化サービスが対称鍵を生成し、ビジネス・プロセスに戻します。対称鍵が作成されると、ビジネス・プロセスが、出力メッセージ・タイプを setEncryptedKey に設定して、EBICS Order Processing サービスを呼び出します。

アンパック・プロセスには次の手順が含まれます。ただし、オーダー・タイプによっては、次の 1 つ以上のプロセスが不要な場合もあります。

1. Base64 デコード
2. 暗号化解除
3. 圧縮解除
4. 署名の検証

次の例は、オーダー・タイプの暗号化解除を示しています。ビジネス・プロセスが、出力メッセージ・タイプを `getEncryptedKey` に設定して、EBICS Order Processing サービスを呼び出します。Base64 でエンコードされた秘密鍵が取得され、暗号化サービスに使用できるようにプロセス・データで設定されます。

## 電子署名

電子署名 (ES) により、オーダー・データを認証できます。署名により、クライアントから Banking Server に送信されるオーダー・データの整合性および否認防止が保証されます。

EBICS では、ES の 2 つの署名クラスを指定します。

- 個人署名
  - タイプ E の単一署名
  - タイプ A の 1 番目の署名
  - タイプ B の 2 番目の署名
- タイプ T のトランスポート署名

Sterling B2B Integrator は以下のシグニチャー・タイプをサポートしています。

- タイプ T のトランスポート署名
- 個人署名またはタイプ E の銀行特有 ES - 単一署名

トランスポート署名として、自己署名証明書または CA 署名証明書を使用できません。個人証明書は、CA 署名でなければならず、銀行が認識する必要があります。トランスポート署名を使用してオーダーを送信し、個人署名を使用してオーダーを許可します。

個人署名では、オーダー・データを処理する契約で、オーダー・タイプまたはファイル・フォーマットごとに署名の数を指定する必要があります。許可される個人署名の最大数は 2 です。タイプ E の個人署名には、以下の署名を含めることができます。

- 単一
- 任意指定の 2 つ
- 必須の 2 つ

## 事前検証

銀行特有のアップロード・オーダー・タイプを使用する場合、サブスクライバーは、最初のトランザクション・ステップで情報を銀行に送信できます。銀行はオーダー・データを事前検証できます。オーダー・データの事前検証には、以下が含まれます。

- データ・ダイジェストの検証
- 口座の許可
- 限度額の検証

オーダー・データの事前検証が成功した後、銀行システムは FUL ファイルを受け取ります。以下の前提条件が満たされている場合、銀行は事前検証を使用してオーダー・データを処理できます。

- 銀行が事前検証機能をサポートしている。
- Prevalidation ノードが着信要求に存在する。

#### データ・ダイジェストの事前検証

以下の前提条件が満たされている場合、銀行はデータ・ダイジェストを検証できません。

- 銀行が事前検証機能をサポートしている。
- Prevalidation または DataDigest ノードが着信要求に存在する。
- オーダー・タイプがアップロード・オーダー・タイプに設定されている (SPR 要求を除く)。

#### 口座の許可および限度額の事前検証

以下の前提条件が満たされている場合、銀行は口座の許可および限度額を検証できません。

- 銀行が事前検証機能をサポートしている。
- Prevalidation または AccountAuthorization ノードが着信要求に存在する。
- 着信要求で OrderAttribute 属性が DZHNN に設定されていない。
- 着信要求でオーダー・タイプが特有アップロード・オーダー・タイプ (FUL) に設定されている。
- 契約許可で署名者の署名クラスが B 以上である。

事前検証では、オーダーを許可するために必要な個人署名の最小数および最大数が定義されている場合に、署名者指定の口座情報および限度額が検証されます。

AccountAuthorization の下にリストされている口座は、有効なパートナー口座でなければなりません。すべての署名者に、Prevalidation にリストされているすべての口座に対するユーザー許可を構成する必要があります。指定の通貨の金額値が、署名者のユーザー許可構成で設定されている最大金額を超過しないようにする必要があります。

---

## Sterling File Gateway との統合

Sterling File Gateway は、同一または異なる通信プロトコル、命名規則、およびファイル・フォーマットを使用する内部および外部パートナー間の安全なファイル転送を可能にします。Sterling File Gateway は、プロセス指向の、拡張性の高いフレームワークでファイル移動のエンドツーエンドの可視性を確保しながら、大規模な大量のファイル転送による移動に対して EBICS をサポートします。これにより、プロトコルとファイルのブローカリング、自動化、データ・セキュリティなどのファイル転送の難題が軽減されます。

EBICS サーバーと Sterling File Gateway の間では、共有メールボックスとパートナーを通じてファイルの移動が行われます。パートナーの作成時に、サブスクリプション・マネージャーによって、ユーザー/パートナー/受信ボックスという構造でメールボックスが作成されます。

Sterling File Gateway では、ルーティング・チャンネル・テンプレートの定義の一部としてプロビジョニング・ファクトを使用します。EBICS シナリオで使用されるル

ーティング・チャンネル・テンプレートには、プロビジョニング・ファクトが構成されている必要があります。そのテンプレートを使用するルーティング・チャンネルには、プロビジョニング・ファクトの値が指定されている必要があります。

インバウンド・シナリオの場合、EBICS オーダー・データ・プロセッサ (ODP) が EBICS クライアントから EBICS サーバーへの EBICS オーダー・ファイルのアップロード (FUL) を取得し、ペイロードをアンパックして、ユーザー/パートナー/受信メールボックス構造に格納します。Sterling File Gateway は、ダウンストリーム処理およびコンシューマーへの最終的な配信のために、そのメールボックスからルートするように構成されています。

アウトバウンド・シナリオの場合、Sterling File Gateway は、コンシューマー・メールボックスにメッセージを格納するように構成されています。メッセージは、そのメールボックスからユーザー/パートナー/送信ボックスにルートされて保管されます。EBICS サーバーから EBICS クライアントへの EBICS オーダー・ファイルのダウンロード (FDL) では、EBICS オーダー・データ・プロセッサ (ODP) がメッセージをパッケージ化し、クライアントで使用できるようにします。

Sterling File Gateway を使用すると、オペレーターは、トランザクションを検索したり、ルートや配信の詳細を表示したりすることができます。

Sterling File Gateway との統合を開始するには、特定の手順が必要です。Sterling File Gateway との統合について詳しくは、[http://www.ibm.com/support/knowledgecenter/SS4TGX\\_2.2.0/com.ibm.help.sfg\\_ebics/doc/SFGEB\\_IntegrationwEBICS.html](http://www.ibm.com/support/knowledgecenter/SS4TGX_2.2.0/com.ibm.help.sfg_ebics/doc/SFGEB_IntegrationwEBICS.html) の「*Sterling File Gateway Integration with EBICS*」を参照してください。



---

## 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510

東京都中央区日本橋箱崎町19番21号

日本アイ・ビー・エム株式会社

法務・知的財産

知的財産権ライセンス渉外

**以下の保証は、国または地域の法律に沿わない場合は、適用されません。** IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、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 Corporation*

*J46A/G4*

*555 Bailey Avenue*

*San Jose, CA 95141-1003*

*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せんが、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。その測定値が、一般に利用可能なシステムのも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認できません。**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をお願いします。

**IBM** の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

表示されている **IBM** の価格は **IBM** が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:



本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態を提供されるものであり、いかなる保証も提供されません。IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

当該のサンプル・プログラムの複製物のそれぞれ、またはそのあらゆる部分、あるいはすべての派生的創作物にも、次のように著作権表示を入れていただく必要があります。

© IBM 2015. このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。© Copyright IBM Corp. 2015.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

## 商標

IBM、IBM ロゴおよび [ibm.com](http://ibm.com)<sup>®</sup> は、世界の多くの国で登録された International Business Machines Corp. の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、<http://www.ibm.com/legal/copytrade.shtml> の「Copyright and trademark information」をご覧ください。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

IT Infrastructure Library は英国 Office of Government Commerce の一部である the Central Computer and Telecommunications Agency の登録商標です。

Intel、Intel (ロゴ)、Intel Inside、Intel Inside (ロゴ)、Intel Centrino、Intel Centrino (ロゴ)、Celeron、Intel Xeon、Intel SpeedStep、Itanium、および 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。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

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。

ITIL は英国 Office of Government Commerce の登録商標および共同体登録商標であって、米国特許商標庁にて登録されています。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java およびすべてのJava 関連の商標およびロゴは Oracleやその関連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。

Cell Broadband Engine, Cell/B.E は、米国およびその他の国における Sony Computer Entertainment, Inc. の商標であり、同社の許諾を受けて使用しています。

Linear Tape-Open, LTO、LTO (ロゴ)、Ultrium および Ultrium (ロゴ) は、米国およびその他の国における HP、IBM、および Quantum の商標です。

Connect Control Center<sup>®</sup>、Connect:Direct<sup>®</sup>、Connect:Enterprise<sup>®</sup>、Gentran<sup>®</sup>、Gentran<sup>®</sup>:Basic<sup>®</sup>、Gentran:Control<sup>®</sup>、Gentran:Director<sup>®</sup>、Gentran:Plus<sup>®</sup>、Gentran:Realtime<sup>®</sup>、Gentran:Server<sup>®</sup>、Gentran:Viewpoint<sup>®</sup>、Sterling Commerce<sup>™</sup>、Sterling Information Broker<sup>®</sup>、および Sterling Integrator<sup>®</sup> は、Sterling Commerce<sup>®</sup>, Inc.、IBM Company の商標です。





Printed in Japan