

本稿は英語版をもとに翻訳されたものであり、不一致がある場合、英語版が優先されます。IN CASE OF ANY DISCREPANCY OR CONTRADICTION BETWEEN THE ENGLISH VERSION AND THE JAPANESE VERSION, THE ENGLISH VERSION SHALL PREVAIL.

クライアント・データ・インテグレーション テクノロジー概要

ファクトセットは独自に収集したコンテンツ、800以上の商用データセット、クライアント独自のデータを統合した金融情報を提供します。



リサーチレポート、グローバルニュース、債券データ、ポートフォリオホールディングス等多数の情報をファクトセット独自のアプリケーションと組み合わせることで、ユーザーにユニークな市場分析を提供します。

本稿ではクライアントのコンテンツをファクトセットに統合する時の5段階のプロセスについて記述します。安全、安定かつ自動化されたデータ統合プロセスの設定を可能とするための推奨事項、参考例及びテクノロジーに関して詳しく説明します。ファクトセットは業界最先端のサービスを提供することに取り組んでおり、必要に応じて専門チームによるきめ細やかなサポートを実施しております。

クライアント・データ・インテグレーション プロセス概要

抽出: 会計管理システムや受注管理システム、データベース、フィードなどからデータが抽出され、ファクトセットのリアルタイムアプリケーション、Portfolio Analysis、FactSet Research Connectで使用するファクトセット専用フォーマットに変換します。データフィールドとフォーマットに関するドキュメント、抽出プロセスを自動化するサポートもご提供可能です。

送信: FTPまたはSFTP (推奨) を利用することで、インターネット経由の安全なデータ送受信が可能です。クライアントからファクトセットにファイルをプッシュ (推奨)、またはファクトセットよりクライアントのサーバーに接続し、弊社のファイル・トランスファー・システム (FTS) を使用して送受信が可能です。

格納: データは安全且つ冗長性を確保した形式で保存しています。セキュリティを強化するため、FTSにて送受信の際に暗号化することも可能です。FTSはファイル転送を容易にするシステムであるため、30日の保存ポリシーが適用されます。

プロセス: データがファクトセットのシステムに到着するとデータ利用時のニーズに合わせてアップロード、変換、検証されます。

転送: 処理されたデータはインタラクティブなファクトセットアプリケーション上でエンドユーザー側から利用可能になります。処理されたレポートとデータはFTPまたはSFTPを介してクライアントサーバーに配信されるだけでなく、データフィードの契約者による利用も可能です。また、FTS上でデータを再度取得することも可能となっております。

独自仕様データの統合

ポジション、リターン、取引などの独自データは顧客内部システムから直接、またはカストディアンなどのサードパーティーベンダーからもファクトセットに送信できます。特定の形式でデータに区切りを設けたテキストファイルとしてFTPまたはSFTPを介してファクトセットへの送信が可能です。ファクトセットは顧客IT担当者やサードパーティーベンダーと密に連携し、ファイル転送設定の円滑な実施に寄与します。ポートフォリオのアップロード要件に関するドキュメント、「ファクトセットパーサーガイド (FactSet Parser Guide)」は、アカウントチームまたはスペシャリストから入手できます。スペシャリストは抽出データの自動化、変換および送信を支援します。

リサーチレポート投稿者

FactSet Research Connectなどのアプリケーションで使用するためのレポートは、PDFまたはXML文書としてFTP、SFTP、Eメールなどを用いて送信可能です。レポートがFactSetに到達すると、カスタムアラート、リアルタイム更新、クライアント検索を通じて、権限のあるクライアントのみ利用できるように処理されます。

その他のデータ投稿者

ファクトセットは商用コンテンツプロバイダとビジネス関係を持ち、連携される情報はカスタムリスクモデルの定量分析および債券分析、ポートフォリオシミュレーション等に利用できます。利用可能なコンテンツセットについてはファクトセット担当者までお問い合わせください。

生データをファクトセットに転送:ファクトセットにファイルを転送する際、クライアントより接続(クライアント主導の接続)を開始し、ファイルが利用可能になったらアップロードすることを推奨します。ファクトセットがクライアントに接続する場合(ファクトセット主導の接続)、15分に1回、ファイルが正常に取得されるまで、最大で1時間まで特定の名前のファイルをポーリングします。

ファイル転送に最適なプロトコルを選択:ファクトセットは機密データおよび独自仕様データを安全に送信するためSFTPの使用を推奨します。ファイルに保護したい情報が含まれている場合、SFTP方式であれば常に通信が暗号化されるからです。SFTPを選択する場合、以下の認証方法があります:

- 鍵認証
- パスワード認証
- 鍵とパスワード認証

キーによる暗号化

SFTPとPGPIはどちらもデータを暗号化する手段として公開鍵暗号方式を使用し、公開鍵と秘密鍵からなる鍵ペアを作成することによって機能します。誰でも公開鍵を使用してデータを暗号化できますが、秘密鍵の所有者のみデータを復号化できます。

SFTPのファクトセットFTSサポート:

- SSHv2、SCP2、SFTP (pre-RFC v3)
- SSH2およびOpenSSH鍵フォーマット
- RSAおよびDSA鍵1024+ビット (FTSは2048ビットのRSAホストキーを使用)
- 最新の暗号化、ハッシュ、圧縮アルゴリズム

大容量のファイルを送受信する場合、転送時間を大幅に短縮するため、転送ファイルを圧縮(zip化)することを推奨します。パスワード保護されたzipファイルはファクトセットシステムではサポートされていません。1つのアカウントにつき1つのプロトコルと認証方法のみ選択可能であり、FTPとSFTPを同時に設定することはできません。また、SFTP接続が有効である場合、単一の認証方法のみ利用できません。適切なプロトコルと認証方法の選択に際しては、ファクトセットスペシャリストにご相談ください。

ファクトセットサーバーの詳細:

ファクトセットにおけるファイル転送関連のインフラではインターネット経由のFTPとSFTPがサポートされています。ファイルをファクトセットサーバーへプッシュする手法が推奨されており、これによってタイムリーなジョブスケジューリングとファイル処理が可能になります。一方で特定の日時に、ファクトセット側主導で顧客サーバからファイル抽出を実施することも可能です。

方法	インターネット
ホスト名	fts.factset.com (FTP) fts-sftp.factset.com (SFTP)
IPアドレス範囲	64.209.89.0/24, 192.234.235.0/24
FTPポート	21,20
SFTPポート	6671

クライアントプロダクション環境のファイアウォール経由で通信を行う場合、上記のIPアドレス範囲とポートを開放する必要があります。IPアドレス範囲の開放はクライアント主導の接続とファクトセット主導の接続の両方に必要であり、ポート開放はクライアント主導の接続を利用する際に必要となります。ファクトセット主導の転送には追加のポート許可が必要になる場合があります。ご質問がある場合はファクトセットまでお問い合わせください。

FTS ホスト公開鍵 (RSA 2048-bit, IETF SECSH フォーマット) クライアント主導のSFTPのみ

```
---- BEGIN SSH2 PUBLIC KEY ----
```

```
AAAAB3NzaC1yc2EAAAABIwAAAQEAx7vVeiK53RXIWwfx/Ajm-fkjr5AEeXzCMg4URy0Gc0HgzWqOMN3jooEu6DECv2rjmhcM/RT8iHomqcgvhCTxPgsh8ow1C6CUhSOWkVLjS3RL/S7HVJIFX-jmseF4R5zYRR5WpMogZdqLh/2LiyWzWl0rka4XoMsQoAZ3N-w9DvLIB3ags7bAChBbWrGh4ez5ccsihPbcCZPbuMCwPeB9L3Y-P162KaFjZQ/CBcjGbWLP9jPb6rY8YJTTDpjhod7EeOFsm/hqlsgD+c04MRbH0nXlyhjmjwAGGHt3m57FLVRUy2gj3ttg1l/aX3Ww3Tj1SlgN/8DZoWWTqA2My3CVVf2w==
```

```
---- END SSH2 PUBLIC KEY ----
```

The fingerprint (MD5) of the FactSet public SSH host key: bc:37:d9:2a:15:93:3c:a6:a0:e9:88:5e:86:81:8d:43

SSH鍵の詳細:

- 鍵交換: 接続テストを実行する前に、FTSに接続するための公開SSH鍵 (完全版) を cdis@factset.com に送信してください。
- 鍵フォーマット: FTSはOpenSSHおよびSSH2キーフォーマットのみをサポートします。
- 鍵パラメータ: FTSは原則としてRSA 2048ビットSSHキーを使用しますが、1024ビット以上のDSA、RSAキーのサポートも可能です。
- SSHプロトコル: FTSはSSHv2、SCP2、およびSFTP (pre-RFC v3) をサポートします。

FTSのほとんどのユーザーアカウントには30日のファイル保持ポリシーが適用されます。リサーチ投稿者など、一部のアカウントにアップロードされたファイルはバックエンドシステムに転送直後にFTSから削除される可能性があります

IPアドレス制限

セキュリティ強化のため、ファクトセットのFTPおよびSFTPサーバへの接続は、お客様が事前にご登録いただいたIPアドレス範囲に限られています。

IPアドレス管理:

IPアドレス範囲の登録、ファイル転送アカウントの過去30日間のFTPとSFTP履歴の閲覧、登録のないIPアドレスから接続が試みられた履歴の確認が可能となります。ファクトセットコントロールセンターのアクセス権限がない方は、ファクトセット担当者にご連絡ください。

- factset.net IDを使用し、[FactSet Control Center](#)にログインする
- 左側のナビゲーションメニューより[Security・セキュリティ]カテゴリを展開し、[File Transfers・ファイル転送]をクリックする

IPアドレス登録:

このプロセスはファクトセットへ初めてデータを転送、もしくはIPアドレスの追加・更新がある場合に必要となります。

- [File Transfers・ファイル転送] ページで、[New IP Range・新しいIP範囲] セクションがあることを確認する
- [Description・説明] と [Range・範囲] を入力後、[Add Rule・ルールの追加] ボタンを押下し登録する

ファクトセット ファイル・トランスファーシステム (FTS) アンケート

このドキュメントはファクトセットのスペシャリストが要件を識別し、ニーズに合わせてFTSを設定するときに利用するインプット資料です。FTSはファクトセットのバックエンドシステムと外部ソースとの間のファイル転送を簡易化し、多岐にわたる認証オプションで双方向のFTPとSFTPをサポートします。FactSetはPGPファイルの暗号化と復号化も完全にサポートしていますが、データ転送経路を保護できるSFTPの使用を強く推奨します。

名前: _____

会社名: _____

電話番号: _____

Eメール: _____

ファクトセットはアンケートを受取った後、セットアップ手続きに関してご連絡いたします。

プロンプトが表示された場合、Adobe JavaScriptオプションを有効にする必要があります。

クライアントからファクトセットに接続する場合

一つ選択してください:

- SFTP-SSH (セキュア) ファイル転送プロトコル
- FTP-ファクトセットが電話にてパスワードを提供

ファイル転送サーバーの名前とバージョン:

SFTP認証オプションを一つ選択してください:

- 鍵認証のみ (クライアントがファクトセットに公開鍵を提供)
- パスワード認証のみ (電話にてファクトセットが提供)
- パスワードと鍵認証 (上記の両ステップが必要)

FTP用PGP暗号化 (任意):

- ファクトセットが復号化 (ファクトセットが公開鍵を提供)
- 自分で復号化 (公開鍵を提供下さい)

更なる保護のためファイルに署名することも可能

完全公開鍵: _____

(SFTPとPGPのみ): _____

ファクトセットの公開SSH鍵(ホスト鍵)の同意を求められる場合、以下が鍵のフィンガープリント(MD5)となります:

bc:37:d9:2a:15:93:3c:a6:a0:e9:88:5e:86:81:8d:43

任意 (分かれば教えてください) _____

ファクトセット担当者: _____

ファクトセットアカウント: _____

目的 (例 ポートフォリオアップロード): _____

アンケート回答を含め、ファクトセットの連絡先をEメールもご記載ください。

ファクトセットからクライアントに接続する場合

一つ選択してください:

- SFTP - SSH (セキュア) ファイル転送プロトコル
- FTP

ファイル転送サーバーの名前とバージョン:

SFTP認証オプションを一つ選択してください:

- 鍵認証のみ (ファクトセットが公開鍵を提供)
- パスワード認証のみ (クライアントが電話にてファクトセットに提供)
- パスワードと鍵認証 (上記の両ステップが必要)

FTP用PGP暗号化 (任意):

- ファクトセットが復号化 (ファクトセットが公開鍵を提供)
- クライアントが復号化 (公開鍵を提供下さい)

更なる保護のためファイルに署名することも可能

プライマリサーバー

アカウント名: _____

アドレス/ポート: _____

ホスト鍵 (SFTPのみ): _____

セカンダリサーバー

アカウント名: _____

アドレス/ポート: _____

ホスト鍵 (SFTPのみ): _____

電話にてアカウントパスワードをご連絡ください (該当する場合)

例: fts-sftp.factset.com#6671.

アンケート回答後、貴社のネットワーク/ファイアウォール管理チームに連絡し、ファイアウォールが正しく設定されていることをご確認ください。
アンケートはファクトセットスペシャリストにEメールにてご返信ください。