2014 年 2 月 28 日　　別添
2016 年 2 月 10 日　一部改正
2017 年 4 月 27 日　一部改正
2024 年 4 月 26 日　一部改正

日銀ネット端末装置と利用先社内ネットワークの接続要件

１．接続の目的

利用先の日銀ネット端末装置と利用先社内ネットワークの接続は、「日本銀行金融ネットワークシステム利用細則（共通事務）」等で定められた日銀ネットの利用に必要なファイル(注)を、USB メモリ等の外部記憶媒体を使用せずに、ネットワーク経由で日銀ネット端末装置と利用先システムとの間で授受することを目的とします。

（注）ファイルアップロード・ダウンロード機能や照会データファイル取得機能等に関するファイル

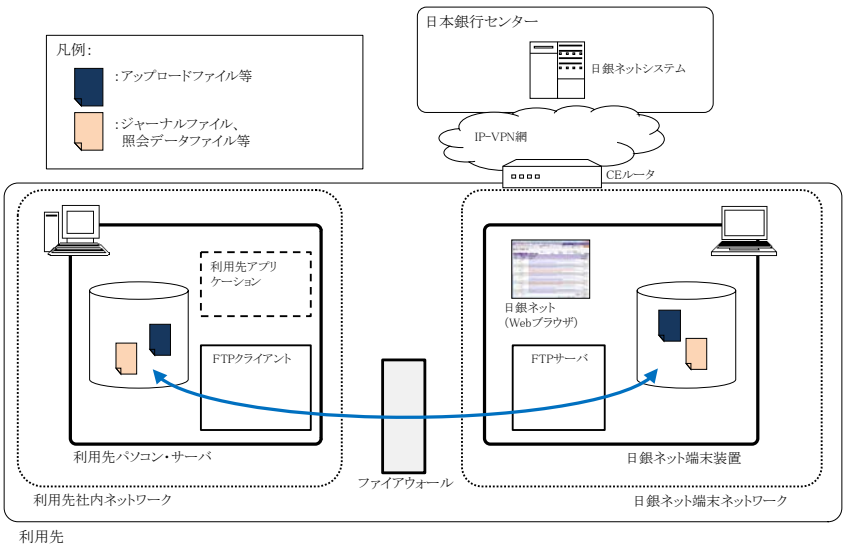
２．接続の概要

接続に際しては、日銀ネット端末装置を接続するためのネットワーク（以下、「日銀ネット端末ネットワーク」といいます。詳細は後述３．参照。）と利用先社内ネットワークの間にファイアウォール専用装置を設置し、日銀ネット端末装置および日銀ネットシステムに対する利用先社内ネットワークからの目的外の通信を遮断します。

ファイルの転送には FTPS（FTP over SSL）を使用します。日銀ネット端末装置に FTP サーバを構築し、ファイルの転送を行いたい利用先システムを構成するパソコンやサーバ上の FTP クライアントから日銀ネット端末装置上の FTP サーバに接続し、ファイルの転送を行います。接続に際しては、利用先において、日銀ネット端末装置と接続している利用先システムと外部ネットワークとの接続制限、利用先システムのウィルス検知、ファイアウォール専用機器や FTP の ID・パスワード管理など、適切なセキュリティ対策を講じることとします。

接続概要図およびファイルアップロード・ダウンロード機能を例とした操作概要は以下のとおりです。

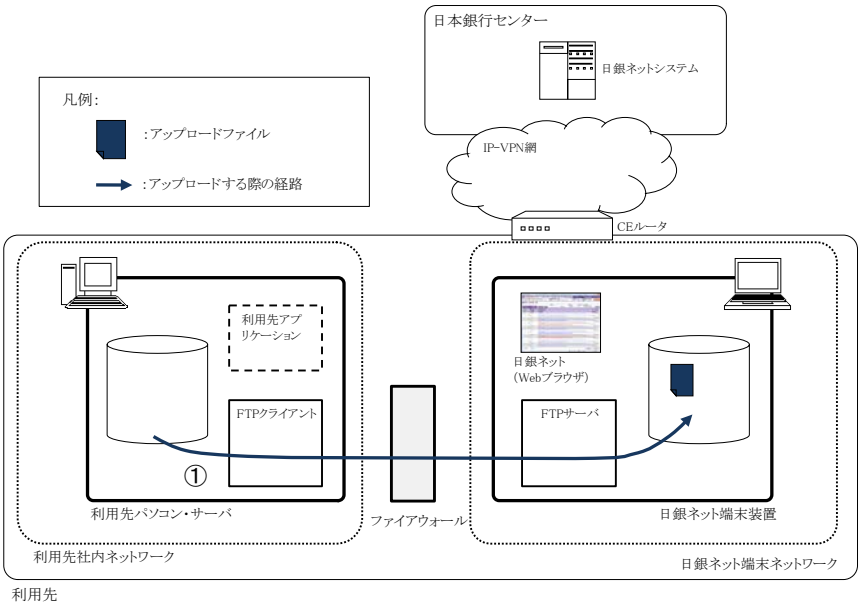
＜接続概要図＞



＜操作概要＞

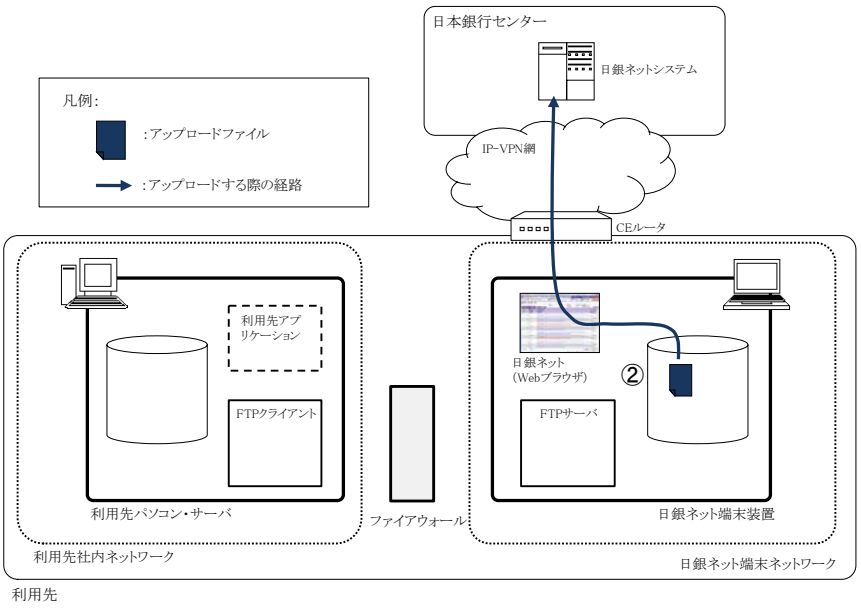
（1）アップロード

① 利用先システムを構成するパソコンまたはサーバを操作し、利用先システムで作成したアップロードファイルを利用先社内ネットワーク経由で日銀ネット端末装置のハードディスクにファイル転送する。



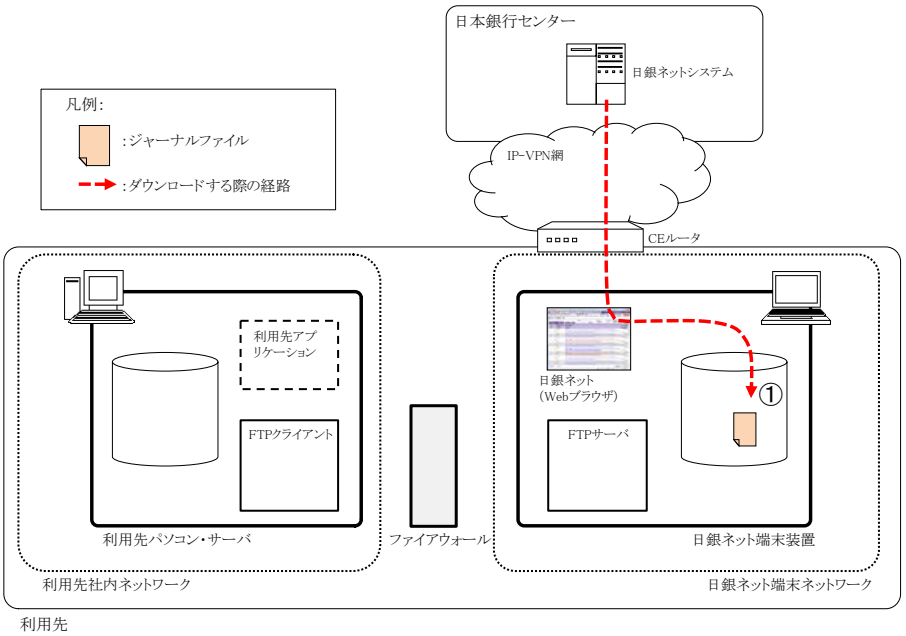
―― ファイル転送を行うアップロードファイルについては、日本銀行センターに送信する前に必ずウイルスチェックを行う必要があります。

② 日銀ネット端末装置を操作し、ファイルアップロード機能の操作画面（ファイル登録：業務処理区分コード 005401、ファイル送信：業務処理区分コード 005402）により、アップロードファイルを日本銀行センターに送信する。

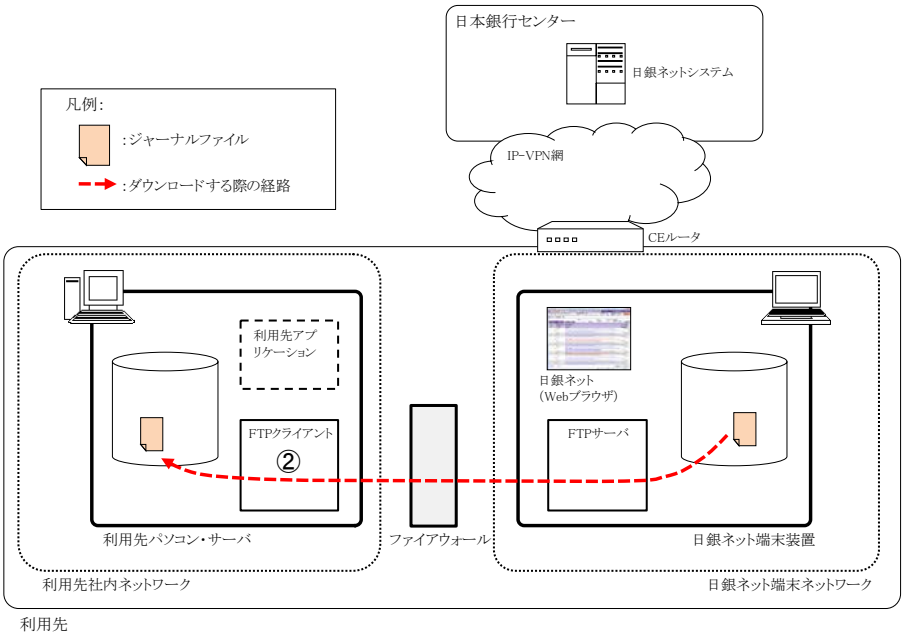


（２）ダウンロード

①日銀ネット端末装置を操作し、ジャーナルダウンロード機能の操作画面（業務処理区分コード 005403）により、ジャーナルファイルを日銀ネット端末装置のハードディスクに格納する。



②利用先システムを構成するパソコンまたはサーバを操作し、日銀ネット端末装置のハードディスクに格納されたジャーナルファイルを利用先社内ネットワーク経由でファイル転送により利用先システム内に取得する。



―― 照会データファイル取得機能により日銀ネット端末装置のハードディスクに格納した照会データファイルは、②と同様の操作により、利用先システムを構成するパソコンまたはサーバに取得することが可能です。

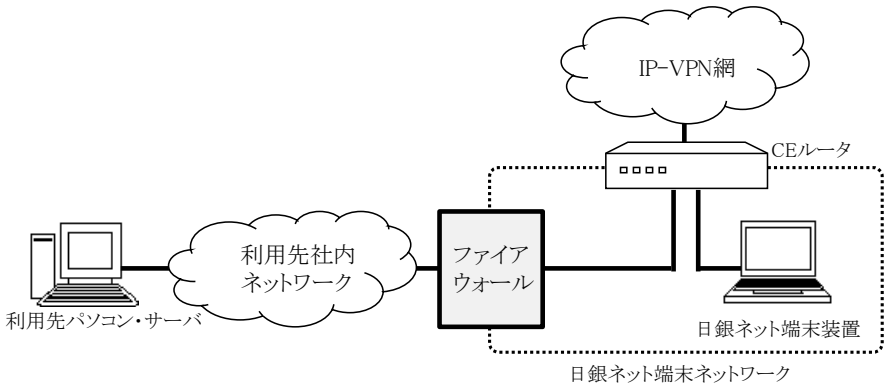
３．接続の構成

日銀ネット端末ネットワークは、日銀ネット端末装置、ネットワークプリンタ、HUB、日銀ネットの IP-VPN 網の CE ルータとこれらの機器を接続する LAN ケーブルから構成されます（「日本銀行金融ネットワークシステム利用細則（共通事務）」参照）。

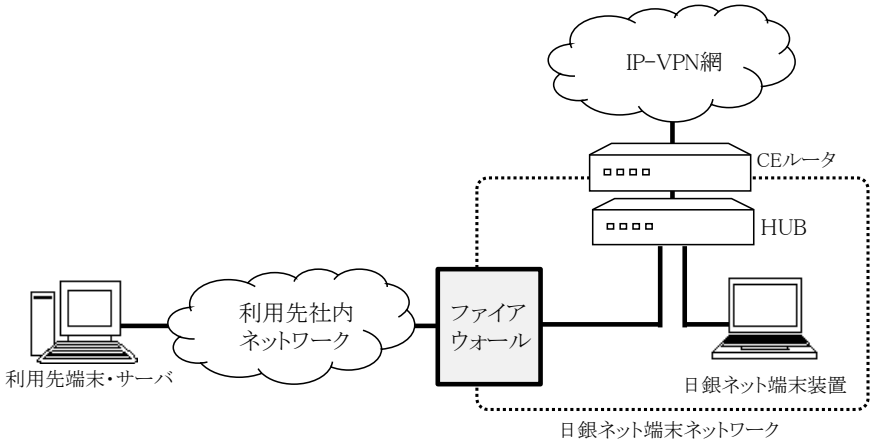
日銀ネット端末ネットワークに含まれない機器（他のネットワークで使用しているスイッチおよびルータ等の通信機器、日銀ネットの IP-VPN 網ではない通信回線の CE ルータ等）は、その使用目的に関わらず利用先社内ネットワークと位置付けられます。このように定義された利用先社内ネットワークと日銀ネット端末ネットワークを接続する際は、必ずファイアウォール専用機器を両ネットワークの間に設置する構成としてください。

日銀ネット端末ネットワークと利用先社内ネットワークは、以下の例のような接続が可能です。

＜CE ルータにファイアウォール専用装置を直接接続する場合＞



＜HUB にファイアウォール専用装置を接続する場合＞



なお、日銀ネット端末ネットワーク内における機器の接続方法は、日銀ネット端末ネットワークと利用先社内ネットワークの間にファイアウォール専用機器を設置する構成であれば、上記例のほか、例えば「日銀ネット端末装置は HUB に接続するが、ファイアウォール専用装置は CE ルータに直接接続する」等、設置場所や機器構成に応じた接続方法を選択することが可能です。

４．接続に必要な機器の詳細

（１）日銀ネット端末装置

日銀ネット端末装置のスペック、バージョン等は、以下の情報を参照してください。

（掲載場所）日本銀行ホームページ―業務上の事務連絡―日銀ネット関連―
諸規程・マニュアル類
＜https://www5.boj.or.jp/bojnet/rulesmanuals.htm＞

（掲載情報）「日銀ネットを利用するための機器等（端末装置用）」

（２）ファイアウォール専用機器

ファイアウォール専用機器は、下記の３つの機能を有する必要があります。

―― 下記の機能を満たせば、ブロードバンドルーター等でも差し支えありません。

①ダイナミックパケットフィルタリング機能（注１）またはステートフルインスペクション機能（注２）

②NAT（Network Address Translation）機能

③通信接続用ポートを２個以上有する

（注１） 利用先システムを構成するパソコンまたはサーバから日銀ネット端末装置へ通信する際に、日銀ネット端末装置から返信されるパケットを予測し、そのパケットの受信に必要なポートのみを状況に応じて動的に開放する機能。

（注２） パケットフィルタリング機能を拡張した機能で、ファイアウォールで最初のパケットを受信した際にルールを検査し、動的に必要なポートを開放する機能。

５．ファイアウォール専用装置の設定

ファイアウォール専用機器に対し、パケットフィルタおよびNATに関する設定を行ってください。また、ファイアウォール専用装置の設定を変更できるIDおよびパスワードは利用先の責任者が厳格に管理し、利用先の責任者の関与なしに同装置の設定が変更されることのないようにしてください。

ファイアウォール専用装置に設定する内容および設定例は、以下のとおりです。

（１）パケットフィルタの設定

イ．FTPの制御コネクション用通信：

通信を許可する対象は、ファイル転送を行いたい利用先システムを構成するパソコンまたはサーバのIPアドレスと、日銀ネット端末装置のIPアドレスおよび制御コネクション用ポート（一般的には21番ポート）とし、利用先システムと日銀ネット端末装置のみ通信できるように設定してください。

必要に応じて複数の利用先システムを構成するパソコンまたはサーバと複数の日銀ネット端末装置の通信を許可できます。ただし、日銀ネット端末装置との通信が必要ない利用先のパソコンまたはサーバと日銀ネット端末装置間で意図しない通信が発生

しないよう、セグメント単位での通信の許可は絶対に行わないでください。

ロ．FTP のデータコネクション用通信：

通信は常時許可せず、制御コネクションを既に確立している利用先システムを構成するパソコンまたはサーバと日銀ネット端末装置の間の通信のみ、ダイナミックパケットフィルタリング機能またはステートフルインスペクション機能を使用し、動的に許可してください。

ハ．上記以外の通信：

全ての通信を拒否してください。

（2）NAT の設定

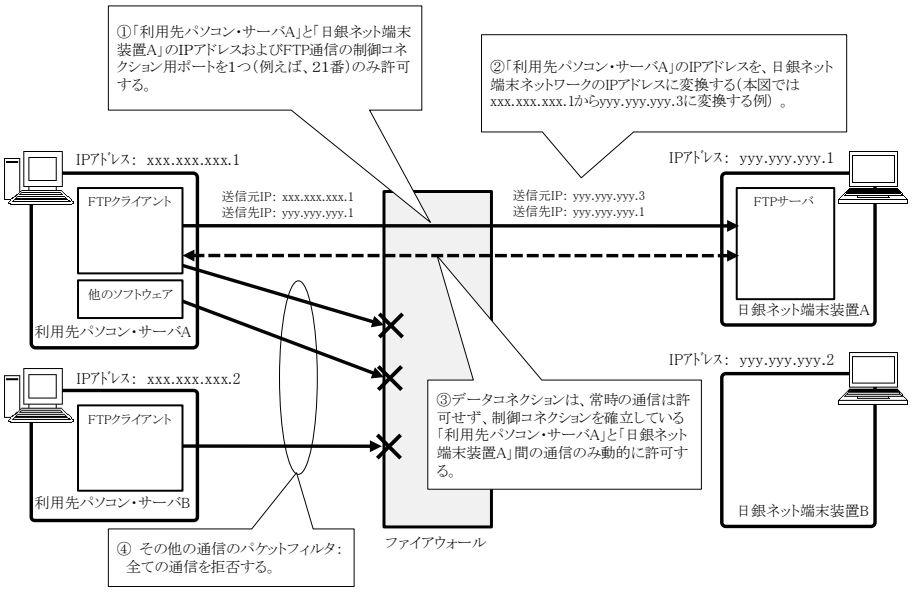
ＦＴＰクライアントとしてファイル転送を行う利用先システムを構成するパソコンまたはサーバの IP アドレスを、利用先に割当てられた日銀ネット用 IP アドレス(注)のうち、日銀ネット端末装置やネットワークプリンタで使用していない任意の IP アドレスに変換してください。

必要に応じ、利用先社内ネットワーク内での日銀ネット端末装置の IP アドレスを、日銀ネット端末ネットワークの IP アドレスから任意の IP アドレスに変換することができます。

（注）日銀ネットの IP-VPN 網の利用開始時に交付された「日本銀行金融ネットワークシステム用ＩＰアドレス通知」参照。

（3）設定例

利用先システムを構成するパソコンまたはサーバ A と日銀ネット端末 A の間でファイル転送を行う場合の設定例は以下のとおりです。



以　上