
企業内ネットワークを経由した インターネット接続環境の構築について

もみじコンピュータサービス株式会社

■ 執筆者 Profile ■



土井 克己

2006年 現在 開発部所属 サブリーダー
オープン系開発担当

■ 論文要旨 ■

これまでインターネットを利用するにあたり、利用する部署あるいは個人ごとにインターネット接続専用 PC を設置し、INS 回線を増設、プロバイダとの個別契約を行ってきた。インターネットの普及とともに、利用機会、利用希望者の増加が著しくなったため、インターネット接続専用 PC の設置による必要経費の増加、ウイルス対策の対応状況のばらつきなどが問題となっている。

今回、企業内ネットワークを経由してインターネット接続を行うことにより、接続 PC の増加に伴う経費の増大、統一されたウイルス対策状況の実現、ユーザーの利便性の向上を図ることとした。

ネットワークを利用した接続によって、利用者の増加にともなう費用の増大の回避、ユーザーの利便性の向上、PC の設置スペースの削減が実現された。今後の課題として、ネットワークトラフィックの増加への対応、利用状況の制限・監視などがあげられる。

■ 論文目次 ■

1. はじめに	《 3》
1. 1 当社の概要	
1. 2 インターネット接続の概要	
2. 個別契約・個別接続の問題点	《 4》
3. 企業内ネットワークを利用したインターネット接続	《 4》
3. 1 インターネット接続方法の更改計画	
3. 2 運用	
4. 企業内ネットワークを使用したインターネット接続の評価	《 8》
4. 1 接続コストの増大の回避	
4. 2 ウイルス対策ソフトのアップデート状況の統一	
4. 3 利用者の利便性の向上	
5. 今後の課題	《 9》
6. おわりに	《 9》

■ 図表一覧 ■

図1 個別契約によるインターネット接続の概要図.....	《 3》
図2 企業内ネットワークを利用したインターネット接続の概要図.....	《 3》
図3 接続構成図.....	《 5》
図4 ルータ・ファイアウォールによるブロック.....	《 6》
図5 インターネット利用開始までのフロー.....	《 7》
表1 外部への接続サーバと使用プロトコル一覧.....	《 6》

1. はじめに

1. 1 当社の概要

当社はもみじ銀行の 100%出資のシステム関係会社として、コンピュータの運用・管理、コンピュータによる情報処理、コンピュータソフトウェアの企画・開発、コンピュータにかかわる専門サービスの提供を主業務としている。

1. 2 インターネット接続の概要

個別契約によるインターネット接続概要を図 1 に、企業内ネットワークを利用したインターネット接続の概要を図 2 にそれぞれ示す。

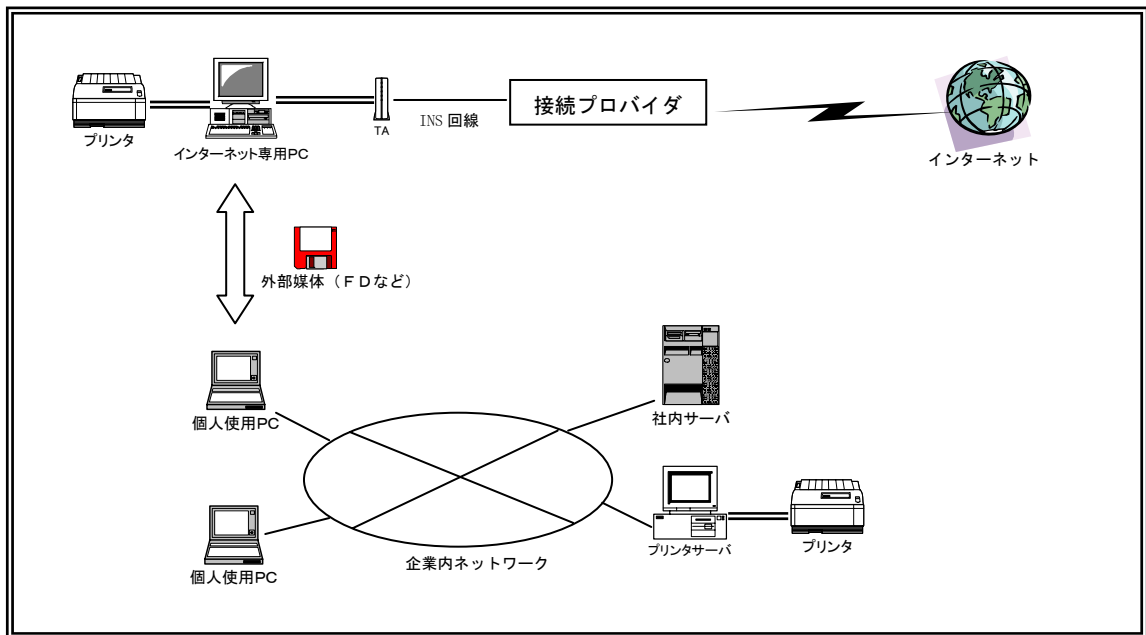


図 1. 個別契約によるインターネット接続の概要図

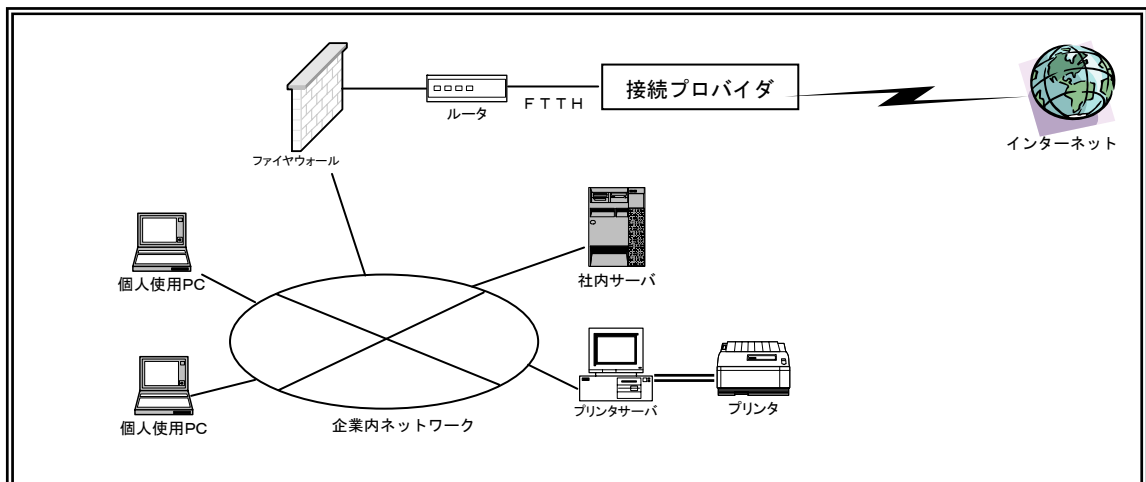


図 2. 企業内ネットワークを利用したインターネット接続の概要図

2. 個別契約，個別接続の問題点

- (1) 企業内ネットワークと隔離されたスタンドアロン PC でインターネット接続を設定するため，インターネット接続専用の PC とプリンタが必要である。
- (2) インターネットを利用する部署，個人ごとに専用 PC を設置し，電話回線（INS）を使用してプロバイダを経由して接続を行うため，利用 PC の増加とともに必要経費が増大する。また，PC およびプリンタの設置場所の確保も必要となる。
- (3) インターネット接続専用 PC の設置場所が利用者の席と離れていた場合，移動しなければならないため，不便である。また，他の人間が使用中の場合，順番待ちが発生する。
- (4) 利用者の作業用 PC とインターネット接続 PC とのファイルのやり取りは FD などの媒体を使用して行っているため，媒体，情報の管理が別途必要となる。
- (5) インターネット接続 PC はそれぞれスタンドアロンで動作しているため，ウイルス対策ソフトのパターンのアップデートなどが統一されていない。

3. 企業内ネットワークを使用したインターネット接続

3. 1 インターネット接続方法の更改計画

第2項であげた問題点を解消するため，企業内ネットワークを利用した一括接続とすることで，以下のことを目標とする。

- (1) インターネット接続にともなう経費の削減
 - a. 電話回線使用料
 - b. 接続プロバイダ費用
 - c. 電話回線敷設工事費用
 - d. インターネット接続専用 PC 設置費用（新規購入の場合の PC 購入費用を含む）
- (2) ウイルス対策ソフトの集中管理による統一されたパターンファイル・検索エンジンなどのアップデート状況を実現する。
- (3) インターネットを使用するにあたって，ブラウザによる WEB サイト閲覧，Eメールの使用を可能とする。
- (4) インターネット接続専用 PC を撤去することにより，部署内空間の有効利用を図る。
- (5) インターネット使用時の利用者の利便性の向上を図る。

3. 1. 1 接続に関して

INS 回線を使用しているものを集約するため，回線容量の確保，将来の社内運用サーバの構築・運用を考慮して，光回線接続・固定 IP アドレスサービスを選択する。

今回の計画においては NTT 西日本の B フレッツビジネス（IP 8）サービスを採用することとした。

インターネットへの接続はルータによって接続することとし，ファイアウォールに富士通製「Net Shelter F/W」を採用することとした。

3. 1. 2 DNS サーバ

DNS サーバは既存の管理業者に委託しているものを継続して使用することとした。

3. 1. 3 メールサーバ

メールサーバは構築費用・管理運用面を考慮して業者によるレンタルサーバサービスを使用することとした。

レンタルサーバサービスはNTTコミュニケーションズの「Mail & Web Pro」を採用することとした。

メールサーバの変更により、既存の契約プロバイダから貸与されているメールアドレスが使用不可となることから、新規でメールアドレスを作成し、旧アドレスからの移行期間を設けることとした。

3. 1. 4 ウイルス対策ソフトに関して

企業内ネットワークで使用しているトレンドマイクロ社のウイルスバスターコーポレートエディションを継続使用する。

3. 1. 5 ブラウザによるサイト閲覧

各インターネット接続 PC はファイアウォールの HTTP プロキシ機能を使用して WEB 閲覧を可能とする。

3. 1. 6 接続構成

最終的な接続構成図を図 3 に示す。

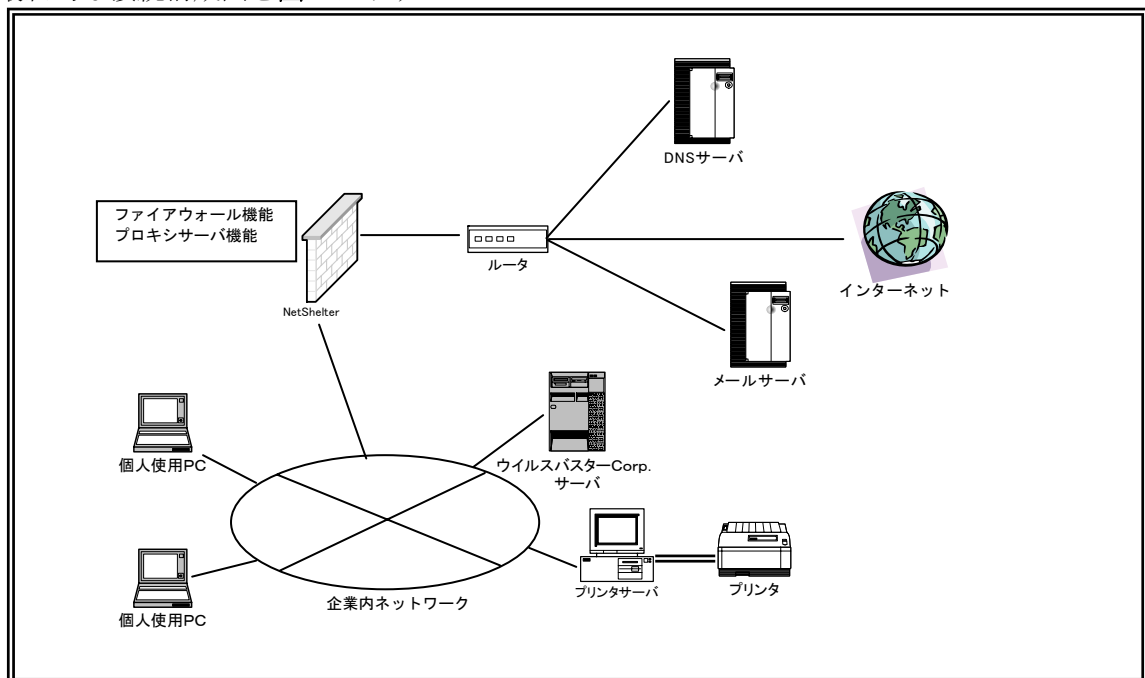


図 3. 接続構成図

3. 1. 7 セキュリティ

ファイアウォール・ルータの設定により、不正アクセスによる安全性を確保する。

(1) ルータ

IP フィルタリング機能によって、内部ネットワークのうちインターネット使用対象ネットワーク内の IP アドレス以外からの通過を許可しない設定とする。

(2) ファイアウォール

- a. 表 1 に示すように、接続対象サーバと使用プロトコルを限定し、これ以外の接続を許可しない設定とする。
- b. HTTP プロキシを使用する設定とし、内部ネットワークから接続する PC は外部の Web サーバと直接通信を行わないこととする。
- c. メールサーバ、DNS サーバへの接続は内部ネットワークの PC の IP アドレス、メールサーバの IP アドレスを設定することにより、直接接続を行うこととする。

表 1. 外部への接続サーバと使用プロトコル一覧

用途	対象サーバ	使用プロトコル
Web サイト閲覧	Web サーバ	HTTP (※)
メール送信	メールサーバ	SMTP
メール受信	メールサーバ	POP3
ドメイン	DNS サーバ	DomainUDP

※HTTP プロトコルはプロキシサーバを経由することとする。

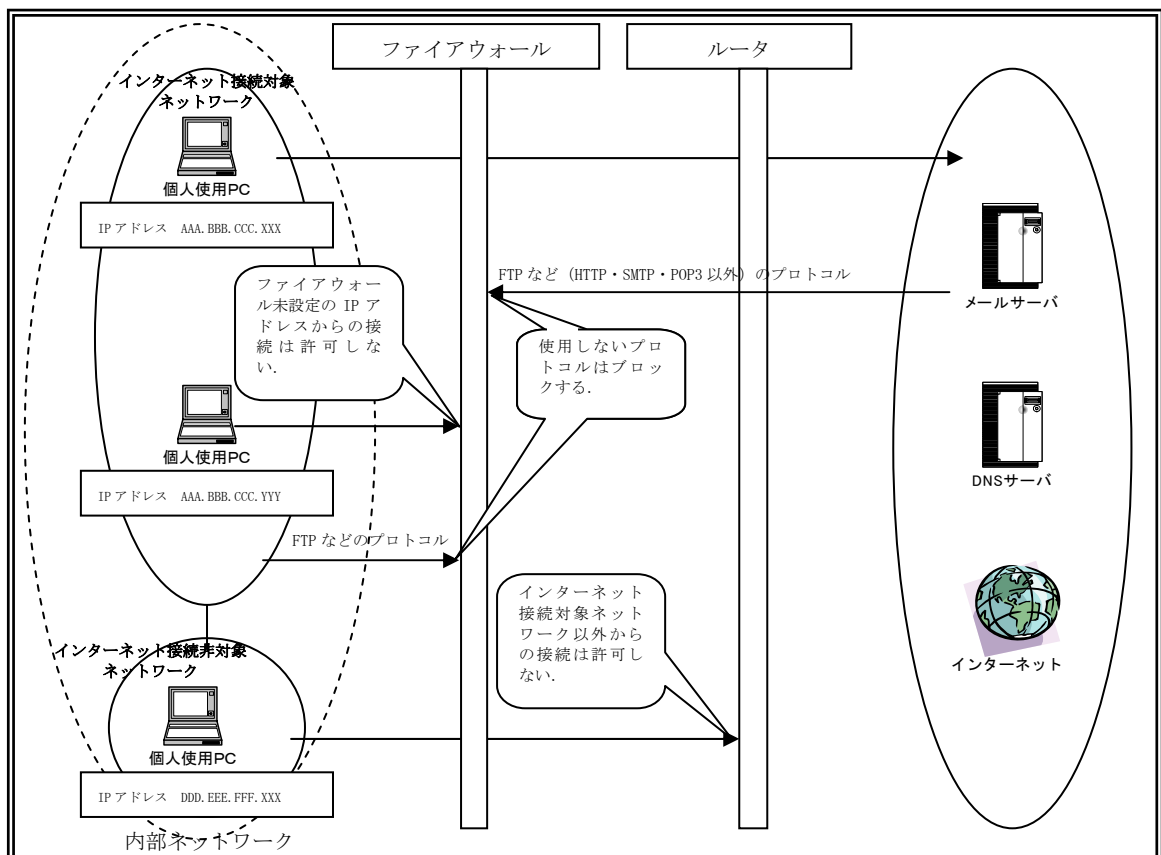


図 4. ルータ・ファイアウォールによるブロック

(3) メールサーバ・DNSサーバ

外部業者に委託管理しているサーバ（メールサーバ・DNSサーバ）のセキュリティについては、委託業者に一任することとする。

3.2 運用

企業内ネットワークは他の情報系閲覧にも使用されているため、インターネット利用によるネットワーク資源を節減することを目的として、企業内ネットワークに接続しているすべてのPCでの使用は行わないこととし、許可制とする。

また、セキュリティ、およびネットワーク資源の有効利用を考慮した運用を策定する。

3.2.1 インターネット利用までの流れ

インターネット利用までの流れを図5に示す。

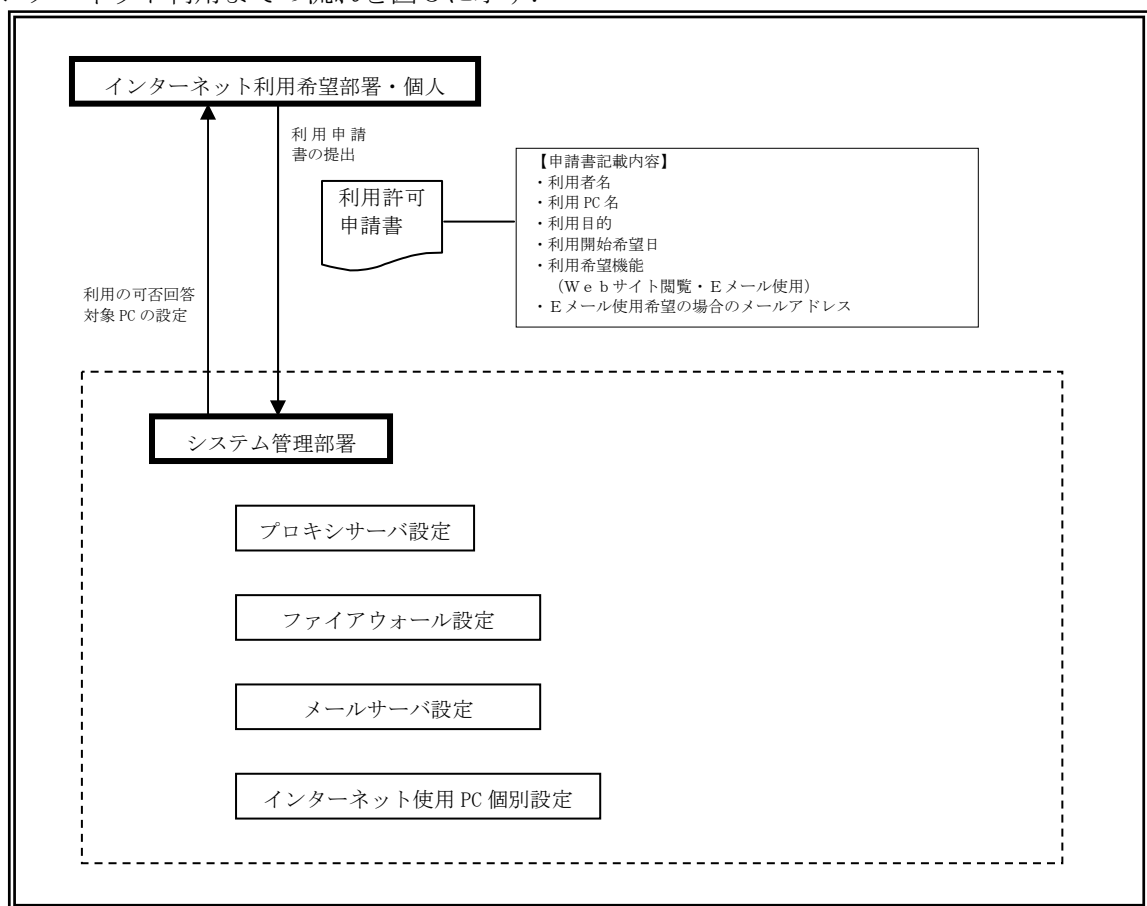


図5. インターネット利用開始までのフロー

3.2.2 申請→許可

インターネット利用に関して、サイト閲覧、Eメール利用の2種類を用意し、それぞれにおいて許可制とする。

(1) サイト閲覧

ブラウザを使用したWebサイト閲覧

(2) Eメール使用

Eメールの送受信

3. 2. 3 ファイアウォール・メールサーバ設定

申請された PC の IP アドレスに対して、ファイアウォールを通過可能となるように設定を行う。

Net Shelter F/Wはブラウザを使用したコンソールを採用しているため、システム管理部署内での設定が可能となっている。

また、メールサーバのコンソールも同様にブラウザを使用しているため、対象 PC 固別設定以外はすべてシステム管理部署で行う。

3. 2. 4 インターネット使用 PC 個別設定

許可された PC に対しての接続設定を行う。

(1) ブラウザ

接続設定を LAN による接続とし、プロキシサーバを使用する設定とする。

(2) メールソフト

メールアドレス、メールサーバの設定を行う。

3. 2. 5 使用ソフトウェア

インターネット接続で使用するソフトウェアは以下のものとする

(1) ブラウザ

Microsoft Internet Explorer

(2) メールソフト

Microsoft Outlook Express

3. 2. 6 その他制限事項

その他、インターネットを利用するにあたり、制限事項を設けることとし、一定期間ごとあるいは随時チェックを行うこととする。

(1) 業務に関係のないサイトの閲覧制限

業務に無関係なサイトの閲覧は行わない。

ファイアウォールのプロキシログにて接続サイト先アドレスと、接続 PC の IP アドレスが取得可能であるため、これを利用して監視することとする。

(2) メール送信時の添付ファイル制限

重要情報を含むファイルをメールに添付して送信する場合は暗号化ソフトによる暗号化を行う。

メールサーバのログから送信内容の確認が可能であるため、これを利用して監視することとする。

4. 企業内ネットワークを使用したインターネット接続の評価

4. 1 接続コストの増大の回避

企業内ネットワークを経由した一括接続を行うことにより、回線使用料、接続プロバイダ費用は一定額となったため、インターネット接続 PC の台数の増加にともなう回線使用料、接続プロバイダ費用の増大は回避できた。

4. 2 ウイルス対策ソフトのアップデート状況の統一

ネットワークに接続されている PC はウイルスバスターコーポレートエディションによる一括アップデートを行うため、統一されたアップデート状況の実現ができた。

4. 3 利用者の利便性の向上

個人で使用している PC がそのままインターネットへ接続されるため、インターネット使用時に移動する必要がなくなった上、使用順番待ちをすることもなくなった。

また、メールに添付されたファイルを媒体によって移動することがなくなった。

このことにより、インターネット使用時における移動時間がなくなったため、一定の利用者の利便性の向上は達成できた。

5. 今後の課題

今後の課題として、以下の項目があげられる。

- (1) インターネット利用 PC の増大によるネットワークトラフィックの増加
- (2) 業務範囲外での利用状況の制限・監視の強化
 - a. 閲覧先サイトの監視・制限
 - b. メール送信先の監視・制限
 - c. メールに添付されたファイルの監視・制限

6. おわりに

企業内ネットワークを利用したインターネットの一括接続を行うことにより、一定の目標は達成できた。

接続方法変更から3年が経過したが、接続に関する基本構造の変更をすることなく正常に稼動している。