

# 企業ネットワークの課題と構築事例

## Problems with Business Networks and Construction Case Study

越野由裕 \*

Yoshihiro Koshino

\* 営業・SE 第一グループ 第一システム統括部 第二インフラシステム部

ブロードバンドの普及と TCP/IP のトラフィック量の急増によって、企業では、ネットワークが帯域不足になりつつある。その状況に対応するため、回線のスピードアップが必要となり、しかもコストの削減も図らなければならないという難しい課題を抱えている。また、キャリアの回線サービスも多様化し、回線の選定も難しい状況となっている。このような企業ネットワークの悩みに応え、PFU では回線の選定も含め、最適なネットワークインフラを構築している。

With the growing popularity of broadband and the sharp increase in the volume of TCP/IP traffic, it is becoming apparent that networks have insufficient bandwidth. Faced with this situation, businesses are having to seek faster line speeds and lower costs. The line services provided by carriers are also diversifying and it is becoming more complicated to select an appropriate line. In response to these difficulties surrounding business networks, PFU is building an ideal network infrastructure that includes line selection.

### 1 まえがき

インターネット、TCP/IP の普及に伴い、ネットワークの高速化、大容量化が加速している。それに合わせて、機器や回線サービスもブロードバンド対応と低価格化が進み、さらに IP 電話などの付加価値を持った新サービスも提供され始めている。

ネットワークが多様化する状況の中で、企業ではネットワークのスピードアップが必要となり、しかもコスト削減も図るといった難しい課題を抱えている。これらユーザーのニーズにこたえるためのネットワークの企画設計、構築のポイントを説明する。

本稿では、まず背景となるネットワークの動向と企業ネットワークの課題を説明し、実際に PFU が担当したネットワークの再構築事例を紹介する。

### 2 ネットワークの動向

#### 2.1 回線サービス

従来の専用線やフレームリレーに変わり、新しいタイプの回線サービスとして主流になってきたものとして、

IP-VPN と広域イーサネットが挙げられる（表 - 1 参照）。これらのサービスは、従来のサービスに比べ、より高速で低価格なサービスとして、企業ネットワークに採用されている。その IP-VPN と広域イーサネットの特徴について次に述べる<sup>1)</sup>。

##### (1) IP-VPN

IP-VPN は、IP ルータを利用した閉域ネットワークサービスである。IP パケットにラベルをつけて、そのラベルに基づき高速に転送する MPLS という技術を利用している。ユーザごとにラベルをつけることで、セキュリティを確保しており、イントラネットとして企業内部だけで利用する専用ネットワークとして使うことができる。

##### (2) 広域イーサネット

広域イーサネットは、LAN スイッチ<sup>注1)</sup>を利用して、

注1) ネットワーク中継機器の一つで、データリンク層（レイヤ2）の情報を元にパケットを転送する L2 スイッチと、ネットワーク層（レイヤ3）の情報を元に転送する L3 スイッチがある。ハードウェアで転送するため、従来のブリッジルータと比べ転送性能が高い。

表 1 IP-VPN と広域イーサネットの比較

	IP-VPN	広域イーサネット
特徴	ルータによるネットワーク	LAN スイッチによるネットワーク
閉域性確保のための技術	MPLS	VLAN
アクセス回線の種類	専用線, ADSL, ダイアルアップなど多数	少ない
オプションサービス	インターネット接続, モバイルなど多数	少ない
プロトコル	IP のみ	マルチプロトコル可
ルーティング	BGP-4 <sup>注1)</sup> , スタティック <sup>注2)</sup>	制限なし

注 1) Border Gateway Protocol-4 の略。インターネットのプロバイダ等の AS (自律システム) 間で主に利用されている経路制御プロトコル。

注 2) ルーティングのための情報をあらかじめルータに設定しておき、常に固定的なルートを探る方法。

イーサネットでは提供される全国規模の広域ネットワークサービスである。LAN において物理的な接続形態とは独立して端末の仮想的なグループを設定する技術である VLAN 技術を利用している。ユーザごとに VLAN を分けることによって、閉域性を確保している。

## 2.2 ネットワーク技術

企業ネットワークでは、従来の基幹系業務（ホスト）中心の通信から、メールやインターネットなどの情報系業務の通信が急増し、それに伴い、全体のトラフィックに TCP/IP の占める割合が増加する傾向にある。そのため、利用されるネットワーク技術についても IP に関する技術が主流となっている。また、インターネットからの不正アクセス対策や認証技術など、セキュリティ関連技術も重要になっている。

その他、企業ネットワークで利用される技術として注目されており、今後利用が広まると予測されるネットワーク技術について以下に紹介する。

### (1) 無線 LAN

無線 LAN とは、無線技術を利用して LAN に接続する技術である。有線 LAN とは違い、ケーブルの敷設が不要になるため、レイアウト変更が多い場合や、会議室などから社内 LAN にアクセスしたい場合に利用される。

ただし、セキュリティ面で脆弱なところがあるため、

企業内で利用するには、認証サーバや VPN<sup>注2)</sup> 装置などと組み合わせることでセキュリティを強化して利用する必要がある。

### (2) VoIP (IP 電話)

VoIP とは、音声を IP プロトコルで伝送する技術である。VoIP を利用したものとして、IP 電話がある。例えば従来は、内線電話のためにデータとは別の回線を用意するか、または高価な TDM などを導入する必要があったが、VoIP の技術を用いることで、データと音声を同じ回線に通すことが可能になる。また、IP 電話を導入することにより、従来の PBX が不要になり、レイアウト変更のたびに必要であった PBX の設定変更も不要になるメリットがある。ただし、音声は遅延や揺らぎに弱いため、企業内での利用においては、QoS<sup>注3)</sup> 技術を使用して優先制御や帯域確保などを行い、音声をより安定して通信させる必要がある。

## 3 企業ネットワークの課題

一般的に企業ネットワークが抱える課題として、次のようなものがある。

- 1) トラフィック量の増大により、現行のネットワークが帯域不足に陥っている。
  - 2) ブロードバンド化を図りたいが、既存のネットワーク機器では対応できない。
  - 3) ブロードバンドの回線サービスの採用を検討したいが、種類が多く何を採用したらよいか分からない。
  - 4) インターネットからの不正アクセス対策やウィルス対策などで管理者の日々の運用での負担が増大している。
  - 5) コストの削減を図りたい。
  - 6) プロトコルを IP プロトコルに統一したいが、ホスト系のプロトコルが混在しており、対応が難しい。
- また、これらのユーザの悩みに加えて、これからのネットワークに期待する要件として、次のようなものが挙げられる。

注 2) Virtual Private Network の略。インターネットなどのネットワーク上の装置間を仮想的に専用線のように接続し、そのパケットの中身を暗号化して安全な通信を可能にするセキュリティ技術。

注 3) Quality of Service の略。ネットワーク上で、ある特定の通信のための帯域を予約し、一定の通信速度を保証する技術。音声や動画のリアルタイム配信やテレビ電話など、通信の遅延や停止が許されないサービスにとって重要な技術である。

### 1) ネットワーク環境の変化への対応

新しい回線サービスやネットワークの新技术など、将来のネットワーク環境の変化に柔軟に対応できるネットワークを構築したい。

### 2) IP 電話の導入

- ① 通話料の削減のため、外線発信を IP 電話にしたい。
- ② PBX が老朽化しているため、PBX を廃止するなど、PBX 関連の運用コストを削減するために内線網を IP 電話に移行したい。

### 3) モバイル環境の構築

- ① 出張先や自宅などから社内イントラネットにアクセスするためのモバイルアクセス環境を構築したい。
- ② 広い工場内での移動や会議室での利用などのため、無線 LAN を利用したモバイル環境を構築したい。

### 4) 新業務 (アプリケーション) への対応

テレビ会議システムやビデオ配信などの新アプリケーションに対応したネットワークを構築したい。

これらの課題や要件に対して、最適な回線サービスを選定し、ネットワーク技術を組み合わせて、ユーザのニーズにあったネットワークを設計する必要がある。

## 4 ネットワーク設計のポイント

### 4.1 設計のポイント

まずユーザの要件をもとにネットワークの企画・基本設計を行う。このフェーズで、使用するネットワーク機器の機種選定や利用する回線サービスの選定、さらにコストの算出を行い、ネットワークの基本構成を決定する。その検討のポイントについて次に述べる。

#### (1) 構成設計

ネットワークの接続形態を決定する。接続形態には、例えば、一つのセンターに他の拠点を接続するスター型ネットワーク、すべての拠点をそれぞれ接続するメッシュ型ネットワークなどがある。接続する拠点数、通信経路などから全体的な基本構成を検討する。

#### (2) 機能設計

ネットワークで必要な機能について検討する。例えば、冗長化のためには、BGP4 などのルーティングプロトコルやイーサネットでループ構成を回避するスパンニングツリープロトコル、VoIP を利用する場合には、QoS

機能などが必要となる。

#### (3) 帯域設計

業務アプリケーションなどで必要とされるレスポンス時間やトラフィック量を元に必要な回線帯域や QoS の方式について検討する。

#### (4) 信頼性設計

機器本体の冗長化や回線のバックアップ方法について、その機器や回線のネットワークにおける重要度から、リスクやコストを含めてその必要性について検討する。

#### (5) セキュリティ設計

インターネット接続において、第三者によるネットワークの不正アクセスを防ぐために必要となるファイアウォールや無線 LAN における認証、特定ネットワークに対するアクセス制御について検討する。

#### (6) 運用設計

ネットワークの監視方法やトラブル時の対応について検討する。

### 4.2 構築のポイント

ネットワークの基本設計が決定した後は、ネットワークの構築フェーズに入る。構築フェーズにおいては、いかに現行ネットワークの停止やエンドユーザでの設定の変更を少なくし、スムーズに効率よく移行できるかが、最も重要なポイントとなる。そのために必要なのが移行設計である。その内容について次に述べる。

#### (1) 作業項目の洗い出し

現行のネットワークから新ネットワークへ移行する場合にどのくらいの作業が必要かを具体的に洗い出す。例えば、移行に際してどんな作業が発生し、どのくらいの作業量でどの程度の時間が必要かなど、作業項目のレベルまで洗い出し、移行に必要な時間を算出する。当然、機器や回線の手配にかかる期間も考慮する。

#### (2) 移行手順の検討

洗い出した作業項目を元に、実際にどのような手順で移行するかを検討する。例えば、どの部分から移行し、そのときの影響範囲などについて調査し、必要な作業項目についても見直す。

リスクを考慮して、一度にすべてを移行するのではなく、モデル的に一部移行し、運用試験での動作確認後にそれを移行するような順次移行が望ましい。

#### (3) 試験項目と試験方法の検討

移行時に必要な試験項目について洗い出し、試験方法とその判定基準について検討する。

(4) 体制の検討

移行手順の作成と同時に、構築体制を検討する。作業項目や試験項目毎に作業分担を決定し、それに基づき必要な人員の確保や、ユーザの各部署や拠点におけるシステム管理者、代表者の選出、ベンダ側の担当や体制を明確にし、連絡網を整える。

また、万が一想定どおりに移行が進まなかった場合の作業の継続、中止、戻しの判断をだれがいつ行うかなども含めて検討する。

5 事例

本章では当社が担当した企業ネットワークの再構築事例について紹介する。

5.1 ネットワーク再構築の背景

今回紹介するお客様は、1996年から1997年にか

けて本社 - 支店間のネットワークインフラを整備し、また1999年には全国の営業所/事務所のリモート接続環境を構築している。当社はそれらのネットワーク構築を担当した経緯があり、2000年後半からのネットワークの再構築に関する検討にも参加した。2002年の4月に新ネットワークの導入が決定、今回の再構築に至った。

5.2 旧ネットワークと課題

(1) 旧ネットワーク構成

ネットワーク構成を図-1に示す。

旧ネットワークは、IP、IPX<sup>注4)</sup>、FNA<sup>注5)</sup>のマルチプロトコル環境であり、本社及び支店にマルチプロトコルルータを導入し、本社と支店を専用線で接続するスター型の構成を採っていた。さらに耐障害性も考慮して、専用線のバックアップ回線としてISDNを用意していた。

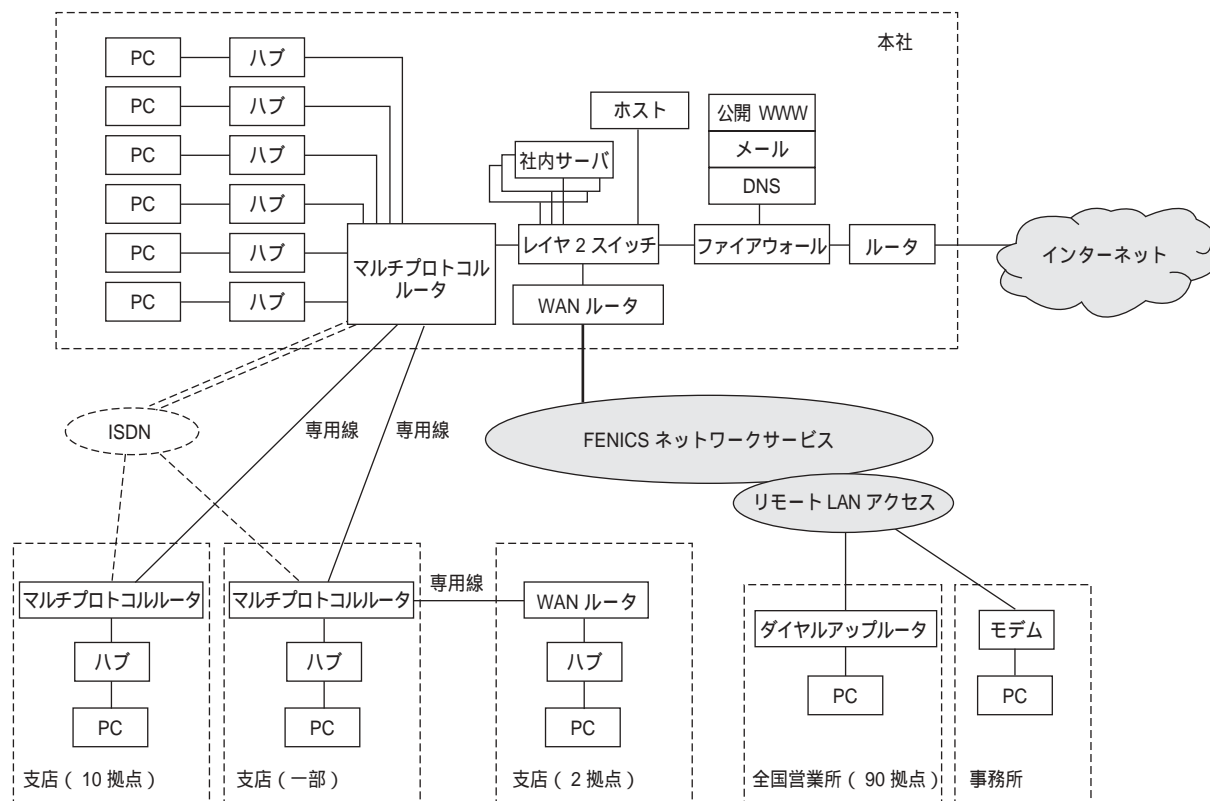


図 1 旧ネットワーク構成概略  
( Fig.1-Outline of the old network configuration )

注4) Internetwork Packet eXchange の略。IPX とは、NetWare (Novell 社のネットワーク OS) において、ネットワーク層プロトコルとして提供されているコネクションレス型のプロトコルである。

注5) Fujitsu Network Architecture の略。富士通 (株) が提供するネットワークアーキテクチャであり、通信に関する様々な制御を体系的に階層化したものである。

また、本社と営業所との間、又は事務所（約 90 箇所）との間に関しては IP のみの通信であり、FENICS リモート LAN アクセスサービスを利用したダイヤルアップ接続を採用し、各拠点にダイヤルアップルータを導入して本社と接続していた。

その他、インターネット環境に関しては、本社にファイアウォール及び DNS、メール、公開 WWW の各サーバを設置して接続、全拠点からのインターネット通信はすべて本社内 LAN を経由していた。

(2) ネットワークの課題

前回の構築から数年経過しており、以下のような課題があると理解した。

- 1) 現在使用しているネットワーク機器がブロードバンドに対応しておらず、ブロードバンド化できない。
- 2) 専用線と比較して低価格な IP-VPN などの回線サービスを利用し、コストダウンを図りたいが、IP プロトコル以外のホスト系のプロトコルが残っている。
- 3) ネットワーク機器のリースアップの時期が近づき、1 年後には更改しなければならない。

5.3 新ネットワークに対する要件

新ネットワークに対する要件として以下に示すようなものがあった。

- 1) コストの削減
- 2) 帯域の拡張（回線速度の増速）
- 3) 旧ネットワークからのスムーズな移行
- 4) エンドユーザの作業の最少化（IP アドレス体系の踏襲など）

これらを踏まえて次節に示すようなネットワーク設計を行った。

5.4 ネットワークの設計

新ネットワークの構成を図 - 2 に示す。

基幹回線網であるバックボーンには IP-VPN を採用した。当初は広域イーサネットの選択肢も検討したが、IP-VPN では、

- 1) ADSL などの低価格なアクセス回線を選択可能。
- 2) インターネット接続などのオプションサービスが利用可能。

などの理由で IP-VPN を採用することとなった。

また広域イーサネットは広帯域で自由度も高く魅力的

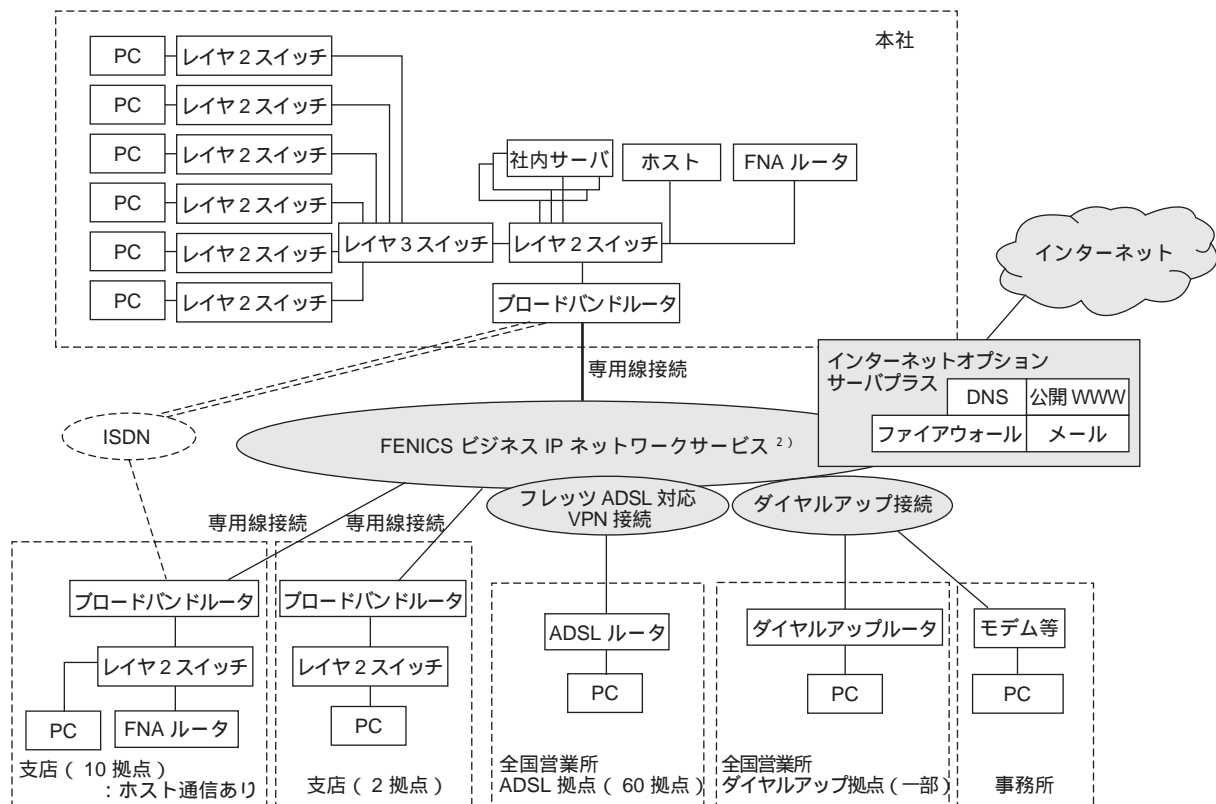


図 2 新ネットワーク構成概略  
( Fig.2-Outline of the new network configuration )

ではあったが、コスト面で IP-VPN より高く非採用となった。

(1) アクセス回線の選定

1) 本社, 支店

本社 - 支店間では FNA によるホスト系の通信を使用している。ホスト系通信は基幹業務で利用されるため、安定した回線で使用する必要がある。そのため、品質面を重視し、本社及び支店のアクセス回線は専用線接続を採用した。

2) 営業所と事務所

営業所と事務所に関しては、品質面よりもコスト面を重視し、アクセス回線はベストエフォート型<sup>注6)</sup>で月額費固定のサービスであるフレッツ ADSL 対応 VPN 接続を採用した。フレッツ ADSL の場合、地域 IP 網を経由するため、セキュリティ面での考慮が必要である。そのため、IP-VPN と VPN で接続し、通信を暗号化することによって、セキュリティを確保している。

3) インターネット

インターネット接続は、日々のウィルス対策や不正アクセス対策などの運用が必要である。それら運用面の軽減と、サーバの保守費用の削減を目的として、インターネットオプションを利用した、ファイアウォール、WWW サーバのアウトソーシングを採用した。

(2) IP プロトコルへの統合

IP-VPN では IP プロトコル以外のプロトコルは通過させることができない。したがって、本社 - 支店間で使用している FNA プロトコルをそのまま通信させることができなかった。そこで、本社（ホスト側）と支店（端末側）に FNA ルータを新たに導入し、FNA を IP でカプセル化して通信させる方式（FNA ルーティング）を採用することによって、IP-VPN 上で FNA の通信を可能にした（図 - 3、図 - 4 参照）。

(3) バックアップに対する考慮

1) 本社

新ネットワークでは本社側の回線がダウンすると本社サーバと全拠点との通信ができなくなってしまうが、そこを二重化しなかった。理由は、これまで本社側で回線がダウンした実績がなかったこと、本社側の回線を二重化する場合回線業者を分けるような考慮も必要になり、コストが大幅にアップするからである。

これらの理由から最終的に本社側の回線障害は考慮しないこととした。

2) 支店

支店側に関しては、これまでも回線側の障害がたびたびあった。例えば、支店側には本社のようなコンピュータ室がなく、通常フロアにルータが設置してあるため、レイアウトの移動などによって、回線用のケーブルをデスクの脚で踏んでしまい、結果的に回線が切れてしまったなど、設置環境の問題による障害もあった。したがって、旧ネットワークと同様に同時に 2 支店までは、ISDN によるバックアップを行えるように考慮した。

(4) IP-VPN での経路制御

IP-VPN でバックアップを行うためには、経路制御に BGP4 を使用する必要がある。

バックアップの動作概要を図 - 5 に示す。

本社側のルータは IP-VPN から経路情報を BGP4 で受信し、通常は支店との通信を IP-VPN 経由で行う。支店側で回線障害が発生した場合は、IP-VPN から通知される経路情報からその支店の情報が消え、その結果、本社ルータにスタティックで設定した代替ルートの情報が有効になり、経路が ISDN 側に切替る。同様に支店側ルータもメインの回線が切れるため、代替ルートの情報が有効になり、バックアップ回線での通信に切替る仕組みである。

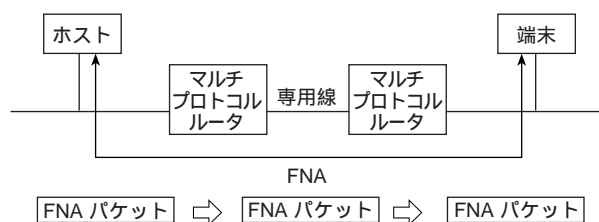


図 3 FNAブリッジでの通信（旧ネットワーク）  
(Fig.3-Communication using an FNA bridge (old network))

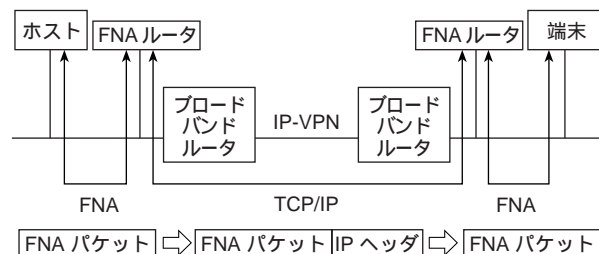


図 4 FNAルーティング（新ネットワーク）  
(Fig.4-FNA routing (new network))

注 6) 通信速度が保証されないデータ通信方式。可能な範囲で最大の通信品質が提供される。

5.5 ネットワークの構築

次の四つのフェーズに分けて移行を行った（図 - 6 参照）。

- 1 次構築：本社 IP-VPN 接続とインターネット環境移行
- 2 次構築：本社 - 支店間ネットワーク移行
- 3 次構築：本社 LAN 再構築
- 4 次構築：営業所 / 事務所ネットワーク展開

(1) 本社 IP-VPN 接続とインターネット環境移行

1) 本社 IP-VPN 接続

まず本社を IP-VPN に接続し、全国の営業所や事

務所を接続している既存のリモート LAN アクセスの回線を IP-VPN のダイヤルアップ接続に移行した。このとき各営業所や事務所で特に変更作業は必要なく、契約の変更だけで対応した。

最初に本社を IP-VPN と接続することによって、回線を二重に契約している期間を短くすると同時に、本社からインターネットオプションで提供されるサーバへのアクセスを可能として、メールサーバへのアカウントの登録や公開 WWW へのコンテンツアップなどの移行準備を行う環境を整えた。

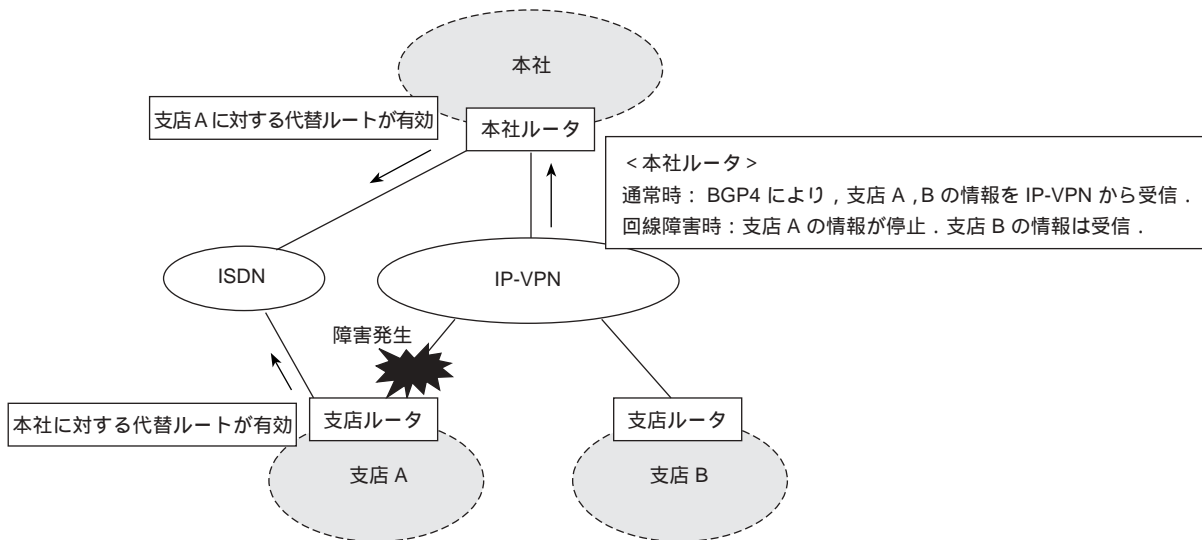


図 5 IP-VPN でのバックアップ動作 (Fig.5-Backup operation using IP-VPN)

	2002 年			2003 年								
	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月
< 1 次構築 > 本社 IP-VPN 接続とインターネット移行	回線申請・機器発注・ネットワーク移行											
< 2 次構築 > 本社 - 支店間ネットワーク移行		モデル展開, 本番展開										
< 3 次構築 > 本社 LAN 再構築				事前試験, 切替え試験								
< 4 次構築 > 全国営業所 / 事業所ネットワーク展開								試験環境構築, 展開準備, 全国展開				

図 6 ネットワーク移行スケジュール (概略) (Fig.6-Network migration schedule (outline))

## 2) インターネット環境の移行

移行準備完了後、DNS のレコードを新ネットワーク側の DNS サーバに移行し、同時にメールや公開 WWW の各サーバも新ネットワーク側のサーバに移行した。このとき、DNS のレコードの更新に時間を要するため、タイミングによっては旧メールサーバにもメールが届いてしまうことが想定された。したがって、移行日を利用の少ない週末にし、旧メールサーバをインターネットから切り離すなどの対応を行った。

## (2) 本社 - 支店間ネットワークの移行

### 1) モデル展開

専用線から IP-VPN へ移行するにあたり、まずモデル店でテスト導入を行った。このテスト導入により、想定している移行手順に問題がないか、FNA ルーティングの動作やバックアップの切替動作などの確認を実施し、次の本番展開に向けた手順の確認を行った。

### 2) 本番展開

1 日 5 拠点毎で 2 日に分けて展開した。本社側に待機して、支援する体制をとった。支店側はモデル展開を元に作成した手順書に従って作業を実施し、予定通り移行を完了した。

## (3) 本社 LAN 再構築

本社の基幹として使用していたマルチプロトコルルータを廃止し、新規に L3 スイッチを導入した。各フロアには L2 スイッチを配置して、VLAN にも対応可能な構成とした。LAN の配線は変えずに単純に機器を置き換えることだけで効率よく機能・性能のアップを図った。

## (4) 営業所や事務所ネットワーク展開

### 1) 本社試験環境構築

全国展開の前に本社内に ADSL 回線を引き込み、試験環境を構築した。この本社試験環境は、実際の導入拠点の 1 拠点として構築し、展開で使用する設定の確認を行うために使用した。

また、営業所や事務所にはシステム管理者がいないため、不具合があった時の切り分けが困難である。したがって、この試験環境で想定される不具合についても検証した。

### 2) 全国展開

本社試験環境での検証結果から、設定の雛型と設置のための手順書を作成して全国展開を実施した。展開方法としては、まず当社のインストールセンターで

ADSL ルータに各営業所や事務所向けの設定をインストールして出荷、各営業所や事務所では添付した手順書を元に既存のダイヤルアップルータから新規に届いた ADSL ルータへ交換をし、不要になったルータを返却するという方法を採用し、短期間で展開を実施した。

## 5.6 ネットワーク再構築の効果

このネットワークの再構築によって、回線速度を速くし、しかもコストを削減するという課題をクリアした。低価格な回線サービスが提供され始めたこともあるが、ネットワーク機器自体が低価格になった効果が大きいと考える。ネットワーク機器の低価格化により、保守費用が下がり、その分、ランニングコストが抑えられる。今回も回線を増速したため、回線費用自体は再構築前と大差ないが、機器の保守費用が大幅に下がり、トータルコストの削減ができた。

## 6 むすび

今回紹介した事例は、企業ネットワーク構築に対する当社の取組みの一つの例である。企業ネットワークと一口に言ってもその企業によりネットワークの利用形態は様々である。

今後は、企業でも IP 電話による内線化や外線での IP 電話サービスの利用が増え、さらに既にある社内での無線 LAN 利用や社外からのモバイルアクセスなどに対するセキュリティ対策などの要件も増えると予測している。実際、紹介した事例のネットワークでも IP 電話サービスの導入も構想に上ったが、今回は時期尚早ということで具体的な検討を見送った経緯がある。

これらのユーザの要件にしっかりと応えていくために、常に新しいノウハウを蓄積して、最新のサービスや技術に対応した、最適で高信頼なネットワークインフラの提供に努めていく。

### 参考文献

- 1) 松田次博：企業ネットワークの設計・構築技法 - 広域イーサネット / IP 電話の高度利用，日経 BP，1 版，東京，(2003)。
- 2) FENICS ネットワークサービス紹介ホームページ  
<http://fenics.fujitsu.com>