

# 企業向けネットワークソリューション

工藤和仁\*  
市橋立機\*  
秋山 誠\*  
小山幸春\*\*  
村上正信\*\*\*

## 要 旨

企業活動の拡大、発展に伴い、それを支えるネットワークに対する要求も高度化、多様化してきている。いつでも、どこでも、業務遂行に適した最適なネットワーク環境が求められている。これらユーザーニーズはたとえば、高速・広帯域、通信品質保証、高信頼、移動性、経済性などの具体的なネットワークの要求条件として顕在化し、これらが同時に要求されることも多くなってきている。

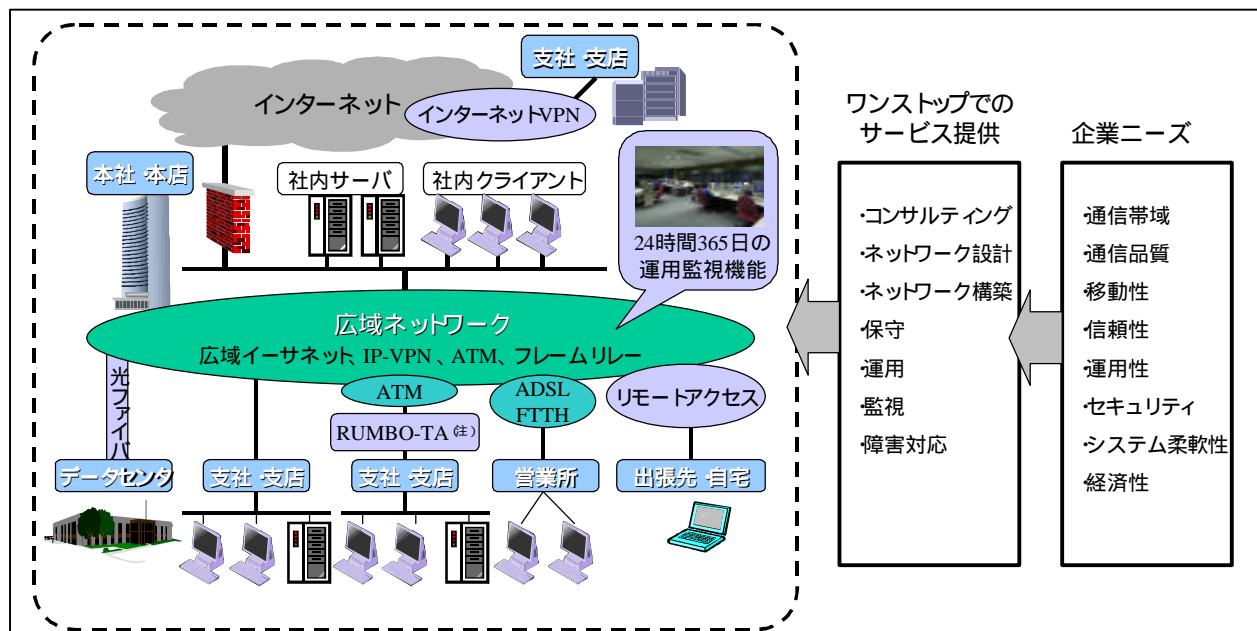
一方、これを実現する通信方式や通信サービス、構成機器は、様々な特性をもったものが利用可能になってきている。

三菱電機グループは、企業ネットワークの多様な要求に対するソリューションとして、コンサルティングからネットワーク設計・構築、保守、運用、障害監視までトータル

なサービスをワンストップで提供することを基本としつつ、同時に、重要な指標の一つである価格性能比の向上に向けた新製品開発や、ダークファイバーの活用、波長多重技術（WDM：Wavelength Division Multiplexing）などの先進的な技術を取り込むことによる、大幅にビット単価を低減したサービスの提供に取り組んでいる。

本稿ではセキュリティを確保したりリモートLANアクセス、通信性能/コストを大幅に改善できるATMターミナルアダプタRUMBO-TA<sup>(注)</sup>、低コストな広帯域通信の手段としてインターネットを利用したインターネットVPN及びダークファイバやWDM技術などの光ファイバ活用方式について述べる。

（注）RUMBOは三菱電機の登録商標である。



VPN : Virtual Private Network IP-VPN : Internet Protocol-Virtual Private Network,  
ATM : Asynchronous Transfer Mode,  
ADSL : Asymmetric Digital Subscriber Line、 FTTH : Fiber To The Home

## 企業向けネットワークの構成

拠点ごとに分散され配置されている社内サーバとそれを結ぶ広域ネットワーク。拠点ごとのデータ量、接続先、必要なセキュリティや信頼性、また、外出先からの接続要求などに対応するため、種々のネットワークサービス、ネットワーク機器を組み合わせる構成が必要である。連続稼働の必要性から、24時間365日の運用監視機能も重要な要件の一つである。

\*三菱電機情報ネットワーク(株) \*\* (株)ドリーム・トレイン・インターネット  
\*\*\*三菱電機インフォメーションテクノロジー(株)

## 1. ま え が き

企業内における情報の流れの変化、処理の多様化に伴うデータ量の急速な増大、対外接続の多様化などにより企業向けネットワークへのニーズが多岐にわたる傾向がある。本稿では、このような企業向けネットワークの機能変化に対応するための基盤技術や最新のネットワークサービス、ネットワーク機器などについて紹介する。

## 2. 企業内ネットワークの機能

### 2.1 集中処理から分散処理へ

コンピュータのダウンサイジング化に伴いホスト集中型のデータ処理から、パソコン+サーバの連携により部門に設置されたサーバで処理が行われ、拠点にも大容量のデータが蓄積されている。アプリケーション処理の上からも分散化が進み、Webベースアプリケーション、ロータスノート<sup>(注1)</sup>やMS-Exchange<sup>(注2)</sup>等のグループウェアの活用が進み、ネットワークのオーバーヘッドが大きくなってきている。また、社内環境から社外への接続のニーズも拡大しており、企業内でクローズしていたネットワークが、関連業界内で相互接続するような形へと変化してきている。

### 2.2 1対nのネットワークからn対nのネットワークへ

TCP/IPが標準サポートされたWindows95<sup>(注3)</sup>の登場により、ベンダの通信手順に依存しないオープンな手順によるネットワーク活用が進み、IPへの全面的な移行が進みつつある。これにより、アプリケーションに最適化したネットワークからアプリケーションを意識せずインフラとして独立したネットワークの構築へと転換が進んでいる。分散化されたサーバへ接続するネットワークは基本トラフィック量が増大すると共にWebベースのアプリケーション、グループウェアの利用が進むことで、総トラフィック量の急増、通信費の増大、セキュリティへの対応などを迫られ、その結果として回線帯域の柔軟な確保が必要となっている。

## 3. 企業内ネットワークの基盤技術

### 3.1 単一なネットワークから複合化したネットワークへ

拠点ごとの役割が細分化され、ネットワークに対する要求も多様化している。本社機能、サーバを集中設置するセンタ拠点、研究・開発部門、物流拠点、さらにSOHO (Small Office Home Office) や出先からの接続など、そのニーズは様々となっている。各拠点ごとに必要な機能、性能、セキュリティ、信頼性などを踏まえた上で、適切なネットワークを組み合わせる必要がある。そのため全拠点を単一のネットワークサービスで結ぶのではなく、帯域保証型(ATM、FR、専用線など)、ベストエフォー

ト型(IP-VPN、インターネットVPNなど) リモートアクセスなどのネットワークを組み合わせる複合ネットワークを構成していく必要がある。

### 3.2 24時間365日の運用監視技術

企業活動のグローバル化と共に、ネットワークの運用・監視、迅速な障害対応が重要な課題になってきた。

三菱電機情報ネットワーク株式会社(MIND)は東京、大阪の2箇所の統合管制センターを中心に、監視装置による自動監視と専門のエンジニアにより、基幹ネットワークからアクセス回線に接続したカスタマエッジのルータやファイアウォール装置まで、24時間365日の運用監視、障害対応のサービスを提供している。

## 4. ネットワークの活用技術

この章では企業内ネットワークに必要な技術基盤の中で実用化されているもの又は実用化に近いものに関して紹介すると共に、その技術基盤について述べる。

### 4.1 IP-VPN、広域イーサネット、リモートLANアクセス、IPv6

#### (1) IP-VPN

IP-VPNは伝送プロトコルをIPに限定した仮想閉域網サービスでIP専用の社内ネットワーク中継網として用いられる。プロトコルはIPに限定されること、接続する拠点数とその回線速度だけによって決まる距離概念のない料金体系などが特長である。安価で信頼性の高いn対nのネットワークが構築できるが、拠点数が少ない場合や比較的近距離拠点多い場合には、他のサービスで構築した方が安価な場合もある。プロトコルがIPに限定されるため、IPベース以外のアプリケーションを使っている場合にはIPにカプセルするなどの処置が必要となってくる。

#### (2) 広域イーサネット

社内LANで用いられるイーサネットを使った広域のLAN間接続サービスであり、事業者はLANスイッチで構築した網の中をバーチャルLANの技術でセキュリティを確保する。IPプロトコル以外のSNA<sup>(注4)</sup>、Apple Talk<sup>(注5)</sup>なども利用が可能で、接続インタフェースがイーサネットのため、安価な接続機器の活用、ルーティングプロトコルに制約がないなどが特長として挙げられる。提供エリアは通信事業者により同一都道府県内の拠点間、全国網の二種類に大別される。利用料金については距離依存のない体系となっているが全国網で利用した場合には中継網の帯域確保方法により異なってくる。

(注1) ノーツは、Lotus Development Corporationの商品名称である。

(注2) Microsoft Exchangeは、米国およびその他の国における米国Microsoft Corp.の登録商標である。

(注3) Windowsは、米国およびその他の国における米国Microsoft Corp.の登録商標である。

(注4) SNAは、米国International Business Machines Corp.のプロトコル名称である。

(注5) AppleTalkは、米国Apple Computer, Inc.の商品名称である。

### (3) リモートLANアクセス

外出先からアナログ電話、ISDN、PHS、携帯電話、インターネットなどを経由して社内ネットワークへ接続する通信サービスで、社外から直接社内ネットワークに接続するため、適切な認証機能によるセキュリティの確保、複数のネットワークを使い分ける際の操作性、経済性等が要点となる。MINDのサービス(図1)では、固定のパスワードのほか、ワンタイムパスワード、USBトークン、指紋照合などによる認証サービスを提供している。また国内、海外(46ヶ国)およびインターネットからのアクセスを同一のID、パスワードで行なうことができ、他事業者にはない特長を備えている。

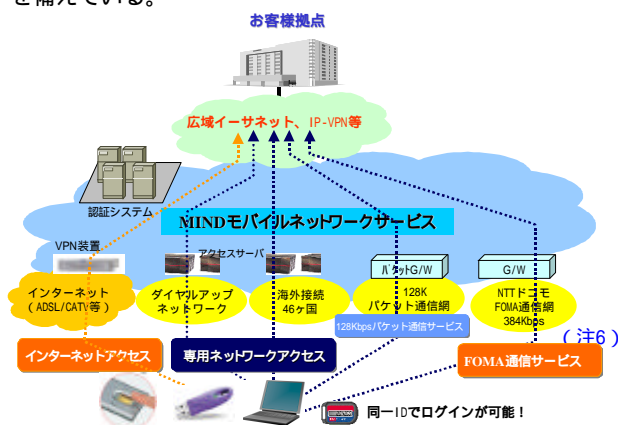


図1 リモートLANアクセスサービスの例

### (4) IPv6

枯渇が予想される現在のIPv4に変わる次世代のIP通信の規格として標準化された。次世代携帯電話、家電製品のIP化など機器への実装が進むと共に、128ビットのアドレス長を持つIPv6への移行が加速すると思われる。現状では実験サービスに留まっているが、アドレスの自動設定、セキュリティ機能(IPsec: Internet Protocol Security)、通信の優先制御機能などが標準機能として盛り込まれており、社内ネットワークにおいても活用が期待される。

### 4.2 ATMターミナルアダプタ (RUMBO-TA)

#### 4.2.1 概要

現在主流であるFR(フレーム・リレー)から、より高速で通信容量が大きく通信コストの低いネットワークへの移行が求められている。このソリューションとして、既存のFRネットワークをATMサービスに拡張するRUMBO-TA(型名MR25T-S)を製品化した(外観を図2に示す)。

既存ルータを流用し、設備・設定の変更を最小限に抑えられるので、ATMを利用したIP-VPNへの移行を容易かつ低コストに実現でき、また、通信速度を3倍強へ向上すると共に通信費用を1/3~1/4へ削減できる。

#### 4.2.2 仕様と特長(主要諸元を表1に示す)

##### (1) インターワーキング機能

AAL5カプセル化方式により、FRフレームをAAL5パケッ

トに変換する。変換方法は、ネットワークインターワーキングがFRF.5に、サービスインターワーキング トランスペアレントモード、サービスインターワーキング トランスレーションモードがFRF.8の規格に準拠している。

##### (2) 2VC多重通信機能(帯域管理、優先制御)

本装置は、2VC(Virtual Channel)多重通信をサポートしておりVC単位での帯域管理、優先制御機能を持つ。

(a)帯域管理: VCグループ内VC間で帯域共用が可能で、各VCの最低帯域保証、1VP(Virtual Path)内のVCグループ間帯域公平性保証など、高度な帯域管理が実現できる。最低帯域を超えるトラフィックはFRフレーム単位で該当セルの廃棄優先度付け(CLPタギング)し、最高帯域を超えるトラフィックはFRフレーム単位で該当セルの廃棄を行い、帯域の有効利用を可能とする。

(b)優先制御: VCグループ内VC間で優先制御が可能で、企業内アプリケーションや業務毎の優先度設定が可能になり、最適なネットワーク品質が確保できる。

表1. 主要諸元

項目	仕様概要	
回線側	インタフェース	ATM 25M (I.432.5準拠)
	ポート数	1回線
	AAL	AAL5
	シェーピング	VP-VCシェーピング: 64k ~ 1024kbps (64kbps単位)、100K ~ 10Mbps (100k bps単位)
	PVC数	2VC
	端末側	インタフェース
ポート数		1ポート
接続コネクタ		ISO2593 34ピンコネクタ(メス)
通信速度		64k bps ~ 8M bps (64k bps単位)
通信プロトコル		FR
保守・管理機能	SNMP (簡易MIB)、telnet、TFTP、Ping	



図2. RUMBO-TA MR25T-Sの外観

### 4.3 インターネットVPN

最も回線コストを抑える手法として、(株)ドリーム・トレイン・インターネット(DTI)のようなインターネットサービスプロバイダ(ISP)が提供するインターネットVPNがある。インターネットVPNは、高速で安価なインターネット網とVPN装置とを組合せて実現するネットワークであり、VPNの名の通り、仮想的に専用線を使った環境とそれほど変わらない企業ユースのネットワークが構築できる。

例えば、企業の本部と拠点をインターネットVPNにて接続する場合は、図3のようにISPのインターネット網と、それに接続するためのアクセスライン(NTTフレッツ(注7)サービスなど)及びVPN装置で構成される。

インターネットVPNは安価である反面、専用線ほどの高い安全性と信頼性は無い。しかしVPN装置が備える機能に

(注6) FOMAは、(株)NTTドコモの登録商標である。  
(注7) フレッツは、(株)日本電信電話(株)の登録商標である。

よってある程度の安全性と信頼性は確保可能である。安全性(セキュリティ)の面では、VPN装置に搭載されるデータ暗号化技術「IPsec」により、データ改ざんを防ぐことができる。また信頼性(回線品質)の面では、図4のようにバックアップ回線が収容可能なVPN装置を使って、万一の回線障害や定期メンテナンスによる回線停止が発生しても、データ転送をほとんど止めることなく稼働できる。

また、アクセスラインとして多く利用されるのがNTTフレツサービスに代表されるFTTHやADSLであり、これらは回線速度を保証しないベストエフォート型のブロードバンド回線と呼ばれ、手軽で安価に広帯域回線が使えることから企業での活用も多くみられ、FTTHやADSLの普及がインターネットVPNの普及へとつながっている。

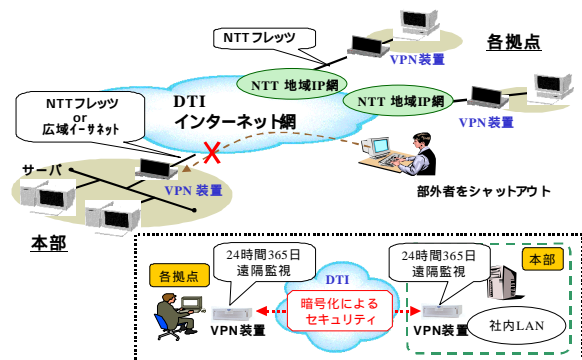


図3. インターネットVPNの構成図

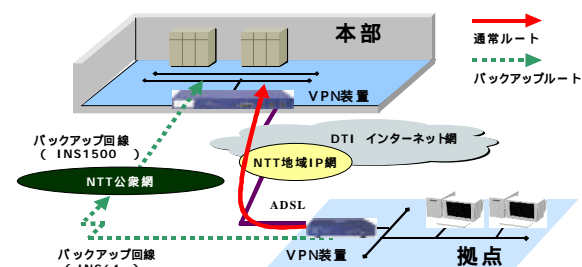


図4. バックアップ回線を使った構成

#### 4.4 光ファイバーの活用

この節では以上のようなネットワーク基盤に期待されている広帯域・低価格化への実現の手段として従来のメタル回線に変わる光ファイバーの活用について述べる。

日本はこれまで、NTTなどによる光ファイバー敷設推進施策により、光ファイバーの敷設密度は世界一と言われており、光ファイバー活用技術の進歩も手伝って安価な通信サービスの提供が可能になっている。

##### 4.4.1 ダークファイバーの利用

これまでファイバーを敷設してきた通信事業者、鉄道・電力等の公益事業者、自治体などが光ファイバーをダ

ークファイバーとして貸し出すケースが一般的になっている。“ダークファイバー”とは光が通っていない(暗い)ことを意味している。MINDにおいても“TMR(注8)(Tokyo Metropolitan Ring)”等のネットワーク構築にダークファイバーを活用しており、構築コストの削減を実現している。

一方、広帯域を安価及び柔軟に利用したい企業にとって、ダークファイバーの活用は有力な選択肢になりつつある。2001年頃から新興通信事業者が直接企業に提供するサービスを開始し、更に鉄道や電力会社なども提供を始めている。都内のオフィス間など近距離(数km)の拠点間を接続する場合に、専用線サービスより割安になるケースが多く、ダークファイバーをWDM装置やメディアコンバータなどを用いて接続し、LAN間接続、SAN(Storage Area Network)などに利用している。この動きは拠点間通信の大容量化要求に従って一層強まっていくと思われる。

##### 4.4.2 WDM技術の適用

光ファイバーの利用技術では、従来、複数の光波長を伝送可能なWDM技術が、第一種電気通信事業者に利用されている。これまでは主に長距離区間での利用が中心であったが、MAN(Metropolitan Area Network)向けにコストを抑えた製品が出ており、通信サービスの低価格化、大容量化に寄与している。

##### 4.4.3 FTTHにおけるイーサネットPON技術

イーサネットPON(Passive Optical Network)はFTTHのアクセス回線に用いる技術で、これを利用すると、スプリッタ(光分岐装置)だけで通信事業者の局舎とお客様間のファイバーが有効活用可能である。現在、IEEE(Institute of Electrical and Electronic Engineers)にてイーサネットPONの標準化作業が行われている。

## 5. むすび

本稿では企業向けネットワークソリューションについて説明したが、今後もネットワークに対するニーズは多様化し、さらに広帯域・低価格なネットワークを構築可能とする様々なネットワークサービス、ネットワーク機器が登場してくる。多様化するニーズへの対応のため、これらのサービス・機器を組み合わせた複合型の企業向けネットワークの構築が必要となる。

### 参考文献

- (1) Frame Relay/ATM PVC Network Interworking Implementation Agreement、FRF.5、Frame Relay Forum(1994)
- (2) Frame Relay/ATM PVC Service Interworking Implementation Agreement、FRF.8、Frame Relay Forum(1995)

(注8) TMRは、三菱電機情報ネットワーク(株)の登録商標である。