記事

次世代情報ネットワーク技術の展望
－高速・大容量・高機能－

*日本電信電話(株)　第一法人営業本部　システムサービス部　ソリューション開発グループ

1．はじめに

クライアント PC の急激なパフォーマンス向上とともに LAN をベースとしたプライベートネットワークに求められる条件も変化している。チップの高速化がハードウェアの進歩を推し進め、快適なネットワークの利用環境を提供するとともにソフトウェアの高度化がさらに便利な利用方法を生み出している。ユーザは一旦手に入れたネットワーク環境に対して、決して満足することなく、すぐに既存ネットワークの限界を超える要求を行いだす。

例えば帯域については、つい５年ほど前までは 10Mbps を複数ユーザでシェアするような利用環境でもそれなりにことは足りていたが、現在ではデスクトップで 100Mbps を占有することはごく当たり前になっており、バックボーンネットワークのギガビットオーダの高速化も必然的に要求されてきている。またユーザがストレスを憶えずにネットワークを利用するには単純なバックボーンの帯域増では解決されず、サーバ周りや LAN/WAN 通しで極力ボトルネックを排した構成であることが重要な要件である。またオープンなネットワーク上でセキュリティを担保し、より確実（安全）に情報を流通させることは、VPN に代表されるように既存の通信網の利用方法を大きく変える方向に加速させる。本稿では、これら日々高度化するユーザニーズに応える技術的トレンドを俯瞰することとしたい。

2．高速 NW（ATM、GigabitEthernet, FibreChannel, WDM）の特徴と活用法

ギガビットクラスの高速・大容量・高品質ネットワークが普及しつつある。これらの技術はバックボーンネットワークという同じ適用領域を持つため、排他的に比較されることがあった。しかし最近ではそれぞれ固有の特徴に着目し、これらの技術を組み合わせるマルチテクノロジー環境が望まれるようになってきた。そこで、技術の特徴とマルチテクノロジー環境を意識した適用方法について考察する。

ATM は広域で大規模なネットワークの構築に適している。ATM は統計多重効果によって物理回

*〒108-8019　東京都港区港南 1-9-1　NTT 品川 twins アネックス
TEL：03-5463-2049　FAX：03-5463-8937　ohba@ss.bch.ntt.co.jp

線を高い通信密度で使用できるため、帯域の狭いWANで効率的にデータを伝送できるからだ。また、伝送距離が長いこと、安定した帯域や小さな遅延を要求するマルチメディアアプリケーション（以後AP）などの多様なトラフィックにも対応できることから、ATMは長距離伝送に最も適しているといえる。

ATMの注目すべき動向として昨年7月に仕様が確定したMPOAが上げられる。MPOAは送信先のATMアドレスが解決されると、送受信を行う端末間を直接結ぶ論理的な伝送路（ショートカットVVC）を確立する。この伝送路が一度確立されると両端末の中継ノードでルーティング処理が行われないため、伝送遅延が大きく削減される。ルータにかかる負荷を分散させる効果もありネットワーク全体のスループットも向上する。さらにATMフォーラムのQoSに対応するため、アプリケーションに応じて必要なサービスを提供する。さらに、物理的な配線にとらわれず論理的にサブネットを分けるEmulated LANをサポートしており、ネットワーク構成の管理や変更を容易することができる。今年度中にはMPOA対応製品が本格的に出荷される。MPOAはネットワーク機器を多く利用する大規模ネットワークの性能と運用性を向上させる技術として期待が大きい。

WANと同様LANでマルチメディアAPを導入とするならATMが求められる。TV会議やVoDなどのAPは遅延による品質への影響が大きく、安定した帯域が必要だからだ。また、LANへ適用される注目すべきATM技術としてワイヤレスATMがあげられる。ワイヤレスATMは来年初めに仕様が確定する予定で、無線環境で25Mbit/sの帯域を実現する。ネットワーク全体をATMのみで構築するため、MPOA同様に端末間でのQoSが提供される。ワイヤレスATMによって、既存の無線LANにはない新たな付加価値ネットワークを実現される。

GigabitEthernet（以下GbE）は従来のイーサネットの性質を継承しており、データ系トラフィックを中心に扱うLANに適している。GbEは非コネクション型の技術で、バースト性が高く遅延に対して強い耐性を持つデータ系APを得意としている。また、データリンク層に既存のイーサネットを流用しており、既存のイーサネットLANと親和性が高い。デスクトップでは10/100Mbit/s環境が浸透しており、GbEはクライアントサーバ方式のワークグループやバックボーンにおいてデスクトップイーサネット環境の拡張に向いている。

GbEの今後の動向として、IEEE802.3abの1000BASE-Tの標準化が期待される。1000BASE-TはUTPケーブルを採用し、現在ドラフト初期段階にある。1000BASE-TはサーバNICなどデスクトップへの普及を促す起爆剤になるため、注目すべき分野である。

また、GbEを含むイーサネット全体に共通した機能として、IEEEを中心としたVirtual LAN（以下VLAN）や優先制御の標準化に注目が集まる。VLANはATMのEmulated LANと同じ機能を持ち、論理的にサブネットを設定して構成管理や運用性を向上させる。さらにIEEE802.1qは、イーサネットフレームにVLANを識別するために17バイトのタグ（フレーム）を規定し、1つの物理回線に複数のVLANを束ねるVLANタギングを審議している。スイッチ間ではVLANごとにひとつの物理回線が必要だったが、この機能によって効率的に使用できるようになり、製品化も進んでいる。IEEE802.1p（現在は802.1d）では、IEEE802.1qのタグに含まれる3bitを使用して8段階の優先順位を設定している。このビットを利用してスイッチ間で優先順位を伝達し制御することができる。目下これらについては相互接続性の実績を積み上げているところである。(*1)

FibreChannel（以下FC）はチャネル接続の領域であるコンピュータ周辺装置のストレージインターフェースにネットワークの概念（Storage Area Network＝SAN）を導入し、高速化を実現

する技術である。この領域はSCSIを始めとして古いアーキテクチャーが多く残されており、バックボーンやサーバに次ぐ新たなボトルネックの要因になっている。ストレージは個々のサーバに付属しておりコスト面・運用面の無駄も多い。コンピュータの処理形態は一極集中型から複数のコンピュータを組み合わせた分散処理型へ移行しつつあり、ストレージアクセスの高速化と効率化をすすめるFCへの期待感は高まっている。

FCの特徴はIPのネットワーク接続とSCSIのチャネル接続の特性を兼ね備えているため、既存チャネル技術にはない高い拡張性を提供している点にある。FCの伝送速度は最高で4Gbit/s、最大距離10Kmと長く、接続台数も最大1600万台を数える。さらに、VLANやマルチキャスト、フロー制御や送信順序保証を規定した3つのサービスクラスを実現する製品が既に出荷されている。FCはANSIで標準化が議論されており、帯域を保証する4つめのサービスクラスも標準化が完了した。

FCの今後の動向として、ANSIの分科会FC-Backboneで審議されているATMやGbEとのインターワーキングに関心が集まっている。NTTのマルチメディアネットワーク研究所はFCとATMの接続変換装置を開発し、標準化の進展に寄与している。FCとGbEを接続する方法として、ワークステーションにルートデーモンをインストールしてルーティング処理をさせる方法があるが、ソフトウェアで処理されるためボトルネックとなっていた。しかし、今年度中に同研究所からFCとGbEの接続変換装置も開発され、出荷される予定である。

WDM (Wavelength Division Multiplexing) はチャネルごとに複数の異なる波長を割り当てて光信号を多重する技術である。光ファイバーで通信するにはデータを送受信するための光源や受光器を使うが、現時点におけるこれらの実現レベルの限界は10Gbit/sである。したがって、現在のように光ファイバーを1対向して通信する場合、技術を問わず10Gbit/sが最大速度となり、それ以上の帯域を実現するには新たにファイバーを用意しなければならない。WDMはチャネルごとに波長を変えてひとつのファイバー上に複数対向の通信を載せることを可能にしている。光ファイバー上で流れるATMやGbE、FCやSONETまで多重化して伝送できる利点という持つ。国内外とも高帯域・大容量を要求するキャリアやISPを中心に導入が進んでいる。WDMはキャリアやISPから導入が始まり、次に大学等の広域ネットワークやMAN (Metropolitan Area Network) へ普及すると思われる。

3．イントラネットを高速化する新たな波

ギガビット速度のネットワークに注目が集まっており、多くのユーザがバックボーンネットワーク等への導入を進めている。しかし、バックボーンを高速化するだけでは、**END-END** でのネットワークのパフォーマンスを向上させることはできない。なぜなら、サーバや **WAN** へのアクセスも合わせて高速化する必要があるためだ。

このようなイントラネットを高速化する技術として注目されているものに、（1）サーバ負荷分散装置（2）**Web** キャッシュ（3）**WAN** 帯域制御装置などがある。これらの技術は **ISP** 市場から導入が始まり、徐々に企業へ浸透している状況であり、今後の市場への普及が注目されるものである。

これらの装置は、これまで **LAN** 機器としては認知されていない機能を持っている。つまり、既存のルータやハブの他に新たにネットワークに追加することでサービスを提供しようというも

のだ。

例えば、サーバ負荷分散を行う方法としては、DNS ラウンドロビンという方法があった。この方法は１つのホスト名に対して、複数のサーバの IP アドレスを DNS に登録する。DNS サーバがクライアントからの要求に対して、ラウンドロビンで IP アドレスを答えることで負荷分散を行っていたのだ。しかし、この方法では CPU 能力の異なるサーバでも同じように負荷分散されてしまう。これに対し、主流になりつつあるサーバ負荷分散では各サーバのロードを分析し、その負荷に合わせてパケットの転送先を決めることができる。また、利用できるサーバの機種も選ばない。これにより、各サーバの性能の総和を引き出すことも可能なのだ。この装置は、現状ではコンテンツ同期の取れた Proxy や FireWall や静的な WWW コンテンツを提供するサーバの負荷分散において有効になる。また、障害サーバを除いて負荷分散させる機能も充実しており、サーバのアベーラビリテイ向上という側面からも導入しているケースがある。

Web キャッシュは、Squid 等のソフトウエアが一般的だが、キャッシュ専用機が次々と登場している。WAN の高速化が進まない日本のインターネットの現状を考えると、キャッシュ技術の動向は非常に興味深いことである。このキャッシュ専用機は、キャッシュ専用 OS を持ち、キャッシュ性能を最大限に引き出すように設計されている。NTT のベンチマークでは、汎用 UNIX 機上で Squid を動作させのに比べ、10 倍のパフォーマンスを示す装置もあった。キャッシュ技術としては ICP（Internet Caching Protocol）の標準化による階層キャッシュの普及も合わせて、今後の動向が気になるところだ。その昔、ルータが汎用機上のソフトで動いていたように、キャッシュが同じ道のりをたどることがあるのだろうか…。また、サーバ負荷分散装置と組み合わせることで、ブラウザの Proxy 設定が必要ないトランスペアレントキャッシュ環境を構築し、柔軟で高速なネットワークを利用しているユーザも増えているようである。

WAN アクセスを効率化する方法としては、Web キャッシングにより Web トラフィックを抑制するという方法の他に、トラフィックを制御することで効率化を実現する帯域制御装置に注目が集まっている。この装置は、ルータの手前に接続するタイプとルータ機能を併せ持つものがある。トラフィック制御のアルゴリズムとしても、フローコントロールによる方法や Class Base Queuing（CBQ）による方法がある。EC 時代となり、特にトラフィックが混雑する WAN 部分でのトラフィック制御の必要性が高まっており、どのような技術がユーザのニーズにマッチするか今後の動向が注目されるところだ。

機器の選定においては、スループット・操作性・運用性などに重点がおかれ、弊社でも先の 3 分野の国内外製品を一同に集め評価を行っている。(*2)

４．ネットワークを安全に利用するセキュリティ技術

データ通信におけるセキュリティ技術を大きく分類すると、①個人認証、②アクセス制御、③暗号通信の３つに分けることが可能である。

個人認証はネットワークを利用するユーザを特定するための技術であり、主にワンタイムパスワード方式を用いて行われている。ワンタイムパスワード方式とは文字通り一度限りのパスワードで、認証サーバとパスワードを生成するトークンにより構成される。ワンタイムパスワード方式には３種類の方式があり（時間同期方式、チャレンジ＆レスポンス方式、カウンタ同期方式）、

今主流になっているものは時間同期方式である。６０秒毎にトークンに表示されるパスワードが変更になり、自分しか知り得ないＰＩＮコード（キャッシュカードの暗証番号の様なもの）と共にネットワークにログイン要求画面に入力することで個人を認証するのである。また、ネットワークのログイン時に利用した認証パスワードのみで、ネットワーク内に散在するサーバ群の個々のサーバに対してユーザ認証を行わなくて済む（ネットワーク認証と共にサーバへのログイン認証を行う）、シングルサインオン技術も普及してくる。

アクセス制御についてはネットワークに対するアクセス制御や、サーバに対するアクセス制御に分類することが可能である。ネットワークに対するアクセス制御は主にファイアウォールによりコントロールされる。ファイアウォールにはアプリケーションゲートウエイ方式とパケットフィルタリング方式があり、アプリケーションゲートウエイ方式は、ＩＰパケットをユーザデータまで分解しパケットを確認するために、パケットフィルタリング方式よりもセキュリティ度が高いと言われている。サーバに対するアクセス制御は、前述の認証システムと組み合わせる事により、ディレクトリやコンテンツへのアクセスを制御する技術であり、ディレクトリサービスなどに利用可能である。

暗号技術は、回線上を流れるデータを一定の法則に基づきスクランブルする技術で、送り側と受け側で、方式、暗号アルゴリズム、暗号鍵が同一のものでなければならない。その為今まで、同一メーカでも異なる機種間では暗号通信が行えない事さえあった。その問題点を解決した技術が IPSec である。IPSec は IP パケット自体に認証機能や暗号機能等を持たせた、IPV6 用に標準化された技術である。しかし、IPV4 においてもオプションにより利用することが可能である。IPSec の技術は認証、暗号、自動鍵交換に分けることができるが、標準化作業が終了しているものは認証、暗号技術のみである。自動鍵交換技術については、９月頃に標準化されるとの話もあるが定かではない。この IPSec の標準化により、各メーカは暗号通信の機器を独自方式から IPSec 準拠へ切り替えている。そこで現在各社製品について相互接続性の検証が盛んに行われている。暗号アルゴリズム DES(鍵長 56bit)、米国輸出規制をクリアした日本で正式に利用可能な IPSec 準拠製品について検証の結果、１７製品中６製品については相互接続性の確認がとれた。ただし、自動鍵交換（ISAKMP/OAKLEY）はインターネットドラフト段階であるため、メーカ毎に仕様が異なり相互接続性は確認できなかった。(*3) 以上より現段階では固定の鍵を使い続ける事になるが、一つの鍵を使い続ける事は暗号データを解析される確率が高く非常に危険であるため、直接ユーザにお勧めすることは時期尚早である。しかし、この IPSec 製品の相互接続性が高まることにより、インターネットを介した他企業との VPN を安全に安価に行う事が可能となり、インターネット VPN が関連企業との通信の要になる時代が来ると思われる。

最近のセキュリティ関連でホットな製品は、ネットワークのセキュリティホールを探すツールである。この製品は既知のハッカーが行うハッキング手法を自動的に行い、約５００項目に及ぶ調査項目を調査することにより、構築されたネットワークのセキュリティホールを自動で探す事が可能なツールである。また、見つかったセキュリティホールについても対策を教えてくれる事により、簡単にセキュリティホールを潰していく事が可能となる。弊社でもこのツールを利用してセキュリティ調査サービスを行っている。セキュリティに対するユーザ関心度が高まり、調査を依頼される件数が最近急増している。

今後、セキュリティ製品はセキュリティポリシーを司るサーバから全てのセキュリティ製品をコントロールする事が可能となると思われる。しかし、製品及びセキュリティ技術は一段と複

雑になり、また全てのコントロールを自動化することは不可能である為、どうしても人の手を煩わせる事になる。企業の情報システム部門の管理者でも管理が容易にできなくなり、また、自社で管理するために莫大な費用を掛けなくてはならなくなる。そこで、セキュリティのアウトソーシングサービスを利用するユーザが増える事と思われる。セキュリティポリシーの作成からネットワークの構築、保守メンテナンスまでを全て委託することにより、トータルコストを下げることが可能になる。

5．おわりに

以上、現在最も動向が注目されるネットワーク関連技術について縦覧したが、各々の分野で最新テクノロジーを実装した製品のリリースラッシュが続いている。既存設備との親和性も考慮しつつ、これら新たな製品群をいかに効果的に組み合わせ、スムーズに実運用に供すためには、製品の実力の見極めと相互接続性の確認というプロセスが極めて重要な意義を持つ。今後も技術トレンドのサーベイと実機評価・検証を進め、ネットワークユーザにより高い利便性を実感してもらうよう取り組んでいきたい。

参考文献

(*1)　日経ｺﾐｭﾆｹｰｼｮﾝ 1998.6.15(No.272)：「VLAN と優先制御の相互接続性確認」(pp82)
(*2)　LAN TIMES 11 月号(ｿﾌﾄﾊﾞﾝｸ社)　及び、 http://www.ss.bcse.co.jp/BL-3000/　にて掲載予定
(*3)　NTT 内部データ