日本ルーセント・テクノロジー（株） 石川　徹

ネットワーク・セキュリティとポリシー・サーバ

これまで，VoIPを中心にした製品と技術の動向を説明してきたが，IPネットワークとインターネット利用の進展に伴い，音声だけでなく，企業や個人のさまざまな利用形態の進展によって，電子商取引（e-コマース）を中心に，安全で信頼性のある通信を前提にして，企業内あるいは企業間の通信でインターネットの活用が想定され，進められようとしている．こうした爆発的な利用機会が進展する一方，インターネットを経由したウイルスの進入などにより，ネットワークのセキュリティに対する関心度および需要も急激に高まっている．

従来のネットワーク・セキュリティの枠組みでは，インターネットとの接続口であるファイアウォールとネットワーク機器の設置方法が議論の中心となりがちであった．しかし，通常のオフィスでも玄関でセキュリティ・チェックがあるだけでなく，セキュリティの高いフロアでは，各フロアや居室ごとに厳重なセキュリティ・ロックがかけられ，部外者の侵入が排除される．また，場合によっては監視カメラが装備されており，そこで扱われている業務の内容によって，さまざまなレベルのセキュリティが施されている．ネットワーク上で利用されるアプリケーションの発展によって，これらの利用されるデータおよび業務上でのセキュリティ問題の与える深刻さが増大するため，こうしたオフィス・レベルでのセキュリティと同様に，ネットワークのセキュリティを考える必要性がある．

そこで，ネットワーク・セキュリティという観点で考えた場合に，想定される次のようなケースと今後の対策を述べてみよう．

(1) ネットワークのポート・レベルでの侵入対策
(2) ネットワーク上での盗聴対策
(3) ネットワークを経由した侵入対策

ネットワークのポート・レベルでの侵入対策

イーサネットの同一セグメント上では，すべてのトラフィックを共有できることから，ネットワークに容易に接続できること自体に，セキュリティへの懸念が以前から持たれていた．ネットワーク管理機能を持ったシェアード（共有）HUBの時代から正規に利用しているポートだけを使える状態にし，それ以外の空いているポートは厳格に管理するといった運用方針がそれである．そうした要求を受けて，端末を接続しても電気レベルでのリンクを確立しない，もしくは，誰かが管理者に無断で端末を接続した場合は，管理端末に対して警告が自動的に発せられるというような，管理者個々のポートに対する設定操作による厳格な運用は，比較的早くから実践されていた．

これまでのコラムの中で述べてきたように，ネットワークの運用を管理者側で決定したポリシーを実行するポリシー・サーバによる運用の場合は，さらに，ポリシー・サーバ側で勤務時間に合わせて，こうした設定を自動化することによって，厳格な運用時間帯の管理をポートに対して徹底することができるようになるのである．

ネットワーク上での盗聴対策

盗聴対策といえば，企業内のローカル・エリア・ネットワーク（LAN）の場合は，すべてのポートをスイッチで構成することが代表例としていわれている．これは，ネットワークの帯域を有効活用すると同時に，関係のあるポートにだけパケットを流すことによって，同時に盗聴対策も図ることができるという考え方からくるものである．ただし，これらはあくまでも管理可能なネットワークの範囲内での手段である．これが，新旧の設備の混在する巨大なキャンパスやインターネットを経由する通信となると，こうした保証を徹底することは難しくなる．そのため，こうしたネットワークの構成機器による保証ではなく，パケットそのものを暗号化するというような手法が必要なる．

こうした手法の代表的なものとして，本コラムの中でも紹介しているVPN（Virtual Private Network）があげられる（**図-1**）．VPNの実現手法としては，IPパケットの認証と暗号化機能を行うIPsec（IP Security Protocol），第2層レベルでのパケットをIPのネットワークを経由して転送するL2TP（Layer 2 Tunneling Protocol），リモート・アクセス・ユーザがPPP（Point-to-Point Protocol）通信を暗号化して行うPPTP（Point to Point Tunneling Protocol）などがある．ただし，この中でL2TPはあ

くまで2層レベルのパケットをIPのネットワーク上で転送することが目的であるため，盗聴対策としての手段ではない．VPN用として，専用線による事業所間通信のインターネットを使った代替え策と考えると，コスト面でのメリットに注目が集まることになるが，これを盗聴対策として考えるならば，新旧の設備が混在するような巨大な事業所内でのセキュリティ対策として考えることができる．つまり，建物や部門間等の管理しきれないバックボーン部分をIPsecによる暗号化で盗聴不可能にすることによってセキュリティを確保するのである．これにより，ネットワーク上の個々の端末に対する変更なしに，暗号化による盗聴対策を行うことができるのである．

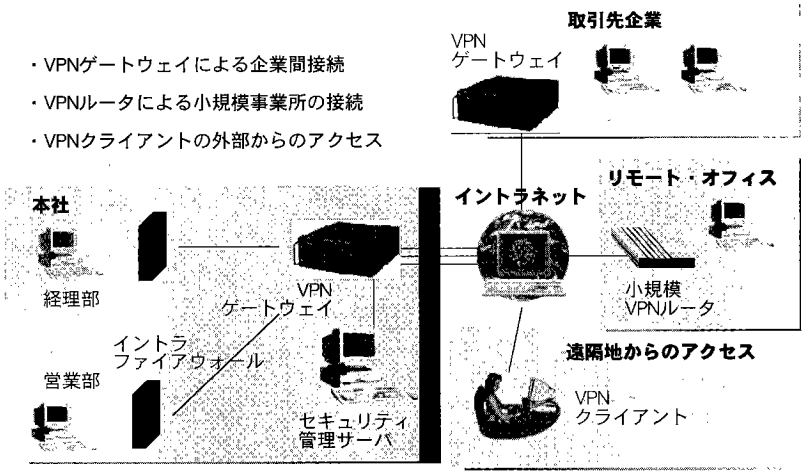

図-1　企業でのVPNの利用モデル

VPNは，ネットワーク層で暗号化を行っているが，さらに上位層のセッション層で暗号化を行う技術として，たとえば，経理部門の特定の限られたアプリケーションの通信のみ，暗号化を行いセキュリティを確保したいといった要求に対しては，SSL（Secured Socket Layer）といった技術が利用されている．通常のネットワークを利用するアプリケーションは，ネットワーク・アクセスについてソケット（Socket）という簡易インタフェースを利用してプログラム開発が行われるが，SSLでは，このソケットの内部処理として暗号化機能を備えている．つまり，SSLを使ったライブラリでアプリケーションを構成することによって，そのアプリケーションのネットワーク上でのソケット内のデータが暗号化されるため，盗聴ができなくなるのである．

これらの暗号化については，データ交換を行う両者間で認証と暗号化の手法に関する合意を行った上で，暗号解読のための鍵を入手しなければ解読ができないわけである．実際に，こうした鍵による手法がインターネットを経由した電子商取引に利用され，広く互換性の高い認証機能を確立するために，公開鍵（Public Key Infrastructure）に関する標準化の活動が急速に進められている．

ネットワークを経由した侵入対策

インターネットの接続口であるファイアウォールについては，すべての企業で最も注意が払われているが，実際のこうしたファイアウォールはUNIXベースのプラットフォームを用いた汎用のハードウェアで実現したり，従来型のルータで実現されている．インターネット接続のコストの低下と活用機会が増大したことによって，インターネット上で交換されるトラフィックが増加してきているため，侵入対策（セキュリティ対策）のために何重にも設定されたパケットの通過条件（フィルタリング・ルール）処理が，これらのファイアウォール上で実行される．また，電子メールやHTTPのトラフィックに載せて入ってこようとするコンピュータ・ウイルスの対策処理を，個別の利用者ごとの端末上のウイルス防止機能で予防するだけでなく，ファイアウォール上で排除するといった考え方も出てきていることから，ファイアウォールのこうした処理能力そのものが，インターネットへの接続帯域の拡大と共にボトルネックとなることも想定される．

こうした傾向に対して，従来型の汎用プラットフォームではなく，耐障害性の高い専用ハードウェアを使い，さらにVPNでの暗号化の処理もDSP（Digital Signal Processor）技術で高速化を行うといったものが登場している．また，こうしたファイアウォールの考え方が，単にインターネットという外部のネットワークとの防護壁にとどまらず，経理部門や開発部門等のセキュリティを要求されるイントラネット内での防護壁として利用されていくことも，こうしたファイアウォールの処理能力の向上によって可能になるのである．

以上のように，IPネットワークの進展に伴い，セキュリティによる防護機能が強化され，セキュリティ・ロックがネットワーク上で多数存在することが十分想定される．こうした状況で即座に問題となるのが，その管理・運用のしくみである．従来のようにネットワーク管理者による手動での個別管理では，こうした厳格な運用が防護壁となると同時に利便性に対する障壁となってしまうことが容易に懸念される．このため，今までの連載の中でも何度か登場している，ポリシー・サーバを中心としたサーバ機能による遠隔での自動運用と集中管理が必要になってくる．

これらによって，ネットワークのトラフィックそのものが，オフィス内の人の動きと同様に，厳重なセキュリティのポリシーの元に運用されることで，利便性と安全性の両立が実現されることになる．

（平成12年1月17日受付）