第9回

VoIPを想定したネットワーク管理

ポリシー管理とリソース管理

日本ルーセント・テクノロジー（株）　石川　徹

前回では，IPで実現されたネットワークで利用されるVoIP関連のアプリケーションを紹介した．VoIPのアプリケーションを，IPのネットワーク上で実際に運用していくことを想定した場合に，最も注意を必要とすることは，音声の再生に必要な帯域と遅延特性の継続的な保証である．

従来のデータ・ネットワークで運用されているアプリケーションのほとんどは，秒単位でエンド・ツー・エンド（端末間）の到達性が確保されていれば通信そのものの目的は達成される．もちろん高速であるに越したことはないのであるが，瞬間的にでも，他の端末間の通信の影響による低速状態が発生しても，あまり問題にはならない．ところが，音声データの転送途中で秒単位の間隔が空いてしまったらどうなるであろう．単純にその部分が無音の状態になるだけでなく，そのフレーズそのものの意味を把握できなくなってしまうため，本来の目的である「意を伝える」という目的が達成できないことになるのである．従来のネットワーク上のアプリケーションにも，こうしたネットワークを経由した応答特性に対して鋭敏に反応するアプリケーションは存在していた．

また，従来のネットワーク管理では，多くの場合，こうした要求に対しては，アプリケーションで不都合が発生しないだけの十分な帯域を，

①ネットワークを分離する

②十分な帯域が確保できるだけの太い帯域を物理的に増設する

などの手法で，必要よりも十分なリソース（帯域）を物理的に割り当てるという考え方で運用してきているのが実状である．確かに，こうした手法で従来のアプリケーションに対しては，かなりの確率で対応することができたが，最近のPCの基本性能を見てみるとどうであろうか．100BASE-TXのインタフェースを標準で装備し，カラーの動画像を音声とともに苦もなく再生することができるのである．こうしたPCが，数メガバイトの大きなデータを瞬時のうちにネットワークを経由してデータの受け渡しを頻繁に行っているのが，今日の現実のネットワークである．

したがって，VoIPで必要なネットワークの特性を十分に確保できるだけの帯域を確保したつもりでも，そうした特性をいつでも継続的に保証していくためには，これらの現実のネットワークで発生している大量データの瞬間的な転送に対して何らかの秩序を持たせる必然性に気づいている管理者は少なくないはずである．

※

従来のネットワーク管理

従来のネットワーク管理では，多くの場合，SNMP（Simple Network Management Protocol，TCP/IP対応の簡易ネットワーク管理プロトコル）によって，ネットワークを構成する主要な機器やアプリケーションを搭載しているサーバなどの機器管理と性能管理を目的とする手法が使われてきている．すなわち，各機器の持つMIB（Management Information Base）情報をSNMPによって収集することで，各機器の内部にある各種の管理データを取り出すのである．これらによって，機器個々の性能管理に必要なデータが入手され，並行してpingやtracerouteといったコマンドにより，それらの管理対象機器の経路性能が管理されてきた．つまり，従来のネットワーク管理の中で捉えている管理プレーン（管理機能）としては，機器管理とそれらの性能管理である．こうした手法によって，情報を獲得した場合，その瞬間の性能データを入手をすることは可能であるが，そのネットワークの帯域がいつでも保証されているとは限らないのである．つまり，これらの手法によって得られるものは，その瞬間の実績としての性能であり，VoIPを使おうとした時に，

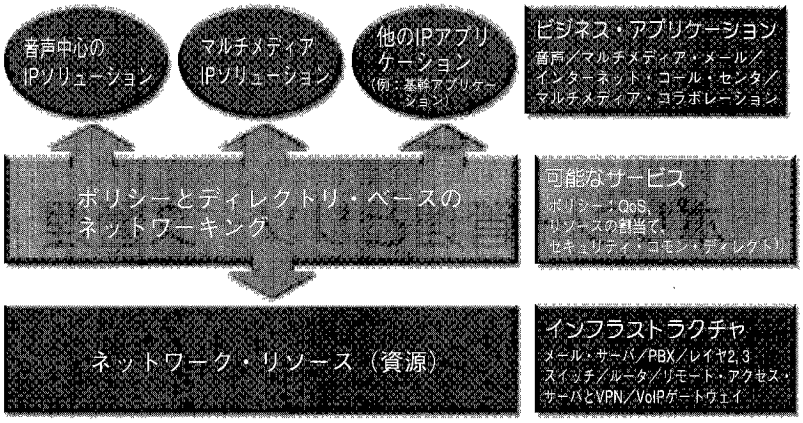

図-1　ポリシー・サービス

いつでも必要な帯域が確保されているとは限らないのが，実状なのである．

ATMでは，こうしたアプリケーションごとの特性を考慮しながら，統計多重効果（通信に使用するセルを制御することによって回線を効率的に使用できるようにする手法）によるコストメリットを得られるようQoS（Quality of Service）がサポートされている．この機能によって，アプリケーションごとに必要な帯域の特性をATMのプロトコル層でサポートすることができるようになっている．これが，ATMではなく，イーサネットの場合はどうであろう，誰かが，バースト・トラフィック（一時的な大量データ）を流してしまえば，容易にそれらの帯域が侵食されてしまうことになる．これは，イーサネットが安価に効率的な高速の通信を実現することを目的として開発され，今日的な広がりを見せながらも，元来，基本的に内在している課題である．したがって，VoIPを既存のデータ・ネットワークの中で安定的に利用していくためには，瞬間的な性能を測定するネットワーク管理ではなく，VoIPのトラフィックについては，ある一定の帯域を定常的に優先処理して確保するような，ポリシー（企業システムなどの運用の方針）をベースにした管理が必要となる．これらのポリシー管理に従って，運用したネットワークで，各種のポリシーに関して実現されている性能を測定し，機器の運用を行うことになるが，これは，従来のネットワーク管理の延長線にある性能管理の形態である．

ポリシー管理

既存のネットワークで運用ポリシーの適用範囲として想定されるものは，VoIPやビデオのような動画像だけとは限らない．既存のアプリケーションの中にも応答時間に対して感度の高いものもあり，機密データへのアクセスというような安全面もある．ポリシーの対象として考えられるものとしてはたとえば以下のようなものがある．

①VoIPや動画像のように安定した一定の帯域が必要なアプリケーション
②データベースやホスト・コンピュータへのアクセスを行う応答性能を重視する基幹業務アプリケーション
③担当者や組織に関してのアクセス制限を持たせたい安全性の確保
④HTTPのトラフィックについては，場合によっては帯域に上限を設ける
⑤業務上の重要なサーバのトラフィックについては，高い優先度を与える．
などが挙げられる．

こうしたポリシーの運用をイーサネットのネットワーク上で行おうとする場合，接続されている端末のトラフィックがポートごとに内部の処理として独立している2層および3層のスイッチにこれらのポリシーの遵守機能を実装することによって実現が可能になる．現在市販されているレイヤ2スイッチでIEEE802.1pの優先処理やレイヤ2スイッチの一部，ルータやレイヤ3スイッチに実装されている優先処理のフィルタ機能がそれである．

こうしたネットワークの構成機器が接続されている端末から各アプリケーションのフレームを受信すると，設定されている優先度に従って，所定の送信ポートに設定されている送信用のキュー・バッファに配置される．キュー・バッファの処理は，それぞれのポリシーに従った優先度と帯域で送信され，次もこうした構成機器であれば，同様なポリシーに従った処理がされることによって，目的端末にポリシーに従った伝達が行われるというものである．これらの処理が，想定したポリシーに従って処理されるかどうかは，

a. 経由するそれぞれのレイヤ2／レイヤ3スイッチなどのネットワーク構成機器で意図した処理性能でフレームの伝達処理が行われるか？
b. エンド・ツー・エンドのすべてのネットワーク構成機器で，統一されたポリシーの処理が設定されているか？

が，重要な鍵となり，これらのネットワーク構成要素の機器に対して，全体の運用ポリシーに従った設定を行っていくことによって実現するものである．ただし，これらの運用ポリシーをエンド・ツー・エンドで実現していくためには，こうした運用ポリシーをすべての関連する機器に対して設定していく必要がある．実際のこうした設定運用を考えると，ごく小規模なネットワークであれば，こうした設定を個々に行っていくことは可能ではあるが，規模の大きなネットワークでの実運用を考慮すると，何らかの機器管理を含めたシステムとしての連動が必要になってくる．

こうした場合に，これらのネットワークの構成機器だけでなく，これらにより構成されるネットワークの帯域も含めて，ネットワーク上のリソースとして管理していく考え方につながっていくことになる．

リソース管理

ネットワーク上のリソース管理の分野では，近年LDAP（Lightweight Directory Access Protocol）による管理が標準技術として進展しつつある．こうした流れの中で，ポリシーの運用についてもディレクトリ・サービスでこれらの管理対象機器をネットワーク・リソースとして管理し，ポリシー設定を行うユーザ・インタフェースのマネージャ・アプリケーションから行った個々の機器用の設定データをポリシー・サーバから個々の機器に対して割り振っていくことで，ネットワークの規模の拡大やダイナミックなポリシーの運用に対応していく動きになってきている．各機器から，このポリシー・サーバに対してポリシーに従った設定のデータを交換する時にLDAPが利用されるのである．

前述のポリシーの運用の対象としては，個々の接続端末によるアクセス制御を想定すると，前述のレイヤ２／レイヤ３スイッチのようなネットワークの構成機器だけではなく，ネットワークに接続されている個々の端末と上部構造のユーザ組織との関連性を持ったデータとしての構造が必要になる．実際にこれらの端末は，アドレス空間の効率的な運用とユーザの利便性の観点からDHCP（Dynamic Host Configuration Protocol）による動的なアドレス割付で運用されているケースが非常に多い．ここで，このDHCPでのアドレス割付について，ユーザ認証との関連を持たせるとどうなるであろう？

つまり，DHCPでアドレスの割付を行う際にネットワーク上でのユーザ認証を行い，そこで認証したユーザに対して，アドレスを割り振ることで端末のアドレスとユーザといった相互の関係データを持つのである．これによって，ユーザも含めたネットワーク・リソースの総合的なポリシー運用が可能になるのである．

※

以上，ネットワーク管理の観点からVoIPを実際のネットワークで運用していく場合の鍵になるポリシーとリソース管理についての概況と相互の関係についての概説を行った．これらの中には，すでに使われている技術と今まさに利用できる状態になっている技術などがあるが，総合的には今後の実用に際して必須の技術である．こうした技術と製品の活用によって，目前に迫っている音声とデータの“Convergence”（統合）を単にコスト削減というような切り口だけでなく，データ・ネットワークの発展的な活用を通しての利便性の追求と捉えていただきたい．

次回では，現状のネットワークから将来のConvergenceに移行する場合に考えられる移行のステップについて記述していく．

（平成11年10月29日受付）