

光・IPネットワークの将来展望

東日本電信電話株式会社
ネットワーク事業推進本部 設備部
ブロードバンドネットワークアーキテクチャ部門
担当部長 渋谷 直樹



はじめに

昨年11月にBフレッツの単月での純増数がADSLを上回った。これは、アナログ電話、ISDN、ADSLと移行してきた主力の通信サービスが、いよいよ光ブロードバンドサービスという集大成に向けて進み始めたと感じさせる出来事であった。また、そのような中、NTTグループの中期経営戦略が昨年11月に発表され、多彩なブロードバンドサービスやユビキタスサービス、固定通信と移動通信の融合などの実現を目指すとともに、光とIPによる次世代ネットワークの構築が主要な取組みの一つとして位置づけられた。

このような方針を受け、NTT東日本としても、高品質で柔軟な光・IPネットワークを構築することで、サービスの多様化やネットワークコスト低減などを目指すことになるが、その一方で、今後は、ブロードバンドネットワークがこれまでの電話網に代わる社会インフラとしての役割を担うようになり、「安心・安全にご利用いただけるネットワーク」としての役割がますます重要になってくると考えている。

本稿では、「安心・安全なネットワーク」を提供するために必要となる機能として、ネットワークの信頼性、品質、セキュリティの確保の3つの視点について考えてみたいと思う。

ネットワークの信頼性

情報通信市場が発展するにしたがって、光・IPネットワークの重要性が高まってきている。既に現在でも、インターネットや電子メールが使用できなくなると、企業や一般のお客様に多大なご迷惑をお掛けすることになるが、光ブロードバンドサービスの普及本格化によって、この傾向はさらに強まるであろう。そこで、お客様に安定したサービスを提供するために、光・IPネットワークの規模拡大に合わせて、信頼性も高めていく必要がある。

光・IPネットワークの信頼性を高めていくには2つの視点から信頼性を捉えた目標設定と設計手法を確立する必要があると考えている。1つ目は、通信事業者として、「安心・安全なサービスを提供するために必須の信頼性設計」である。これは例えば電話局で火災が発生したり、地震などの災害が発生した時を

想定した対策など、全てのサービスで共通的に必要となる対策が該当する。2つ目は、「お客様ニーズやサービスコンセプトに合わせた信頼性設計」である。これはサービス毎に、お客様に満足いただける料金や信頼性を考慮して設計する信頼性対策が該当する。

こうした信頼性目標と設計手法を確立するために以下の3つのアプローチから検討を進めている。

これまで培った、固定電話の信頼性設計ノウハウを応用する

IPネットワーク独自の特徴を踏まえた対策を加える

ガス・水道・電力など他インフラ設備の信頼性ノウハウを応用する

このような検討を通して、光・IP時代に相応しいネットワークの信頼性設計手法を確立していく必要があると考えている。

ネットワークの品質

これまでの電話を中心とした通信の世界は変革の時代を迎え、多様なお客様ニーズに柔軟に対応すべく様々なブロードバンドアプリケーションの提供が検討されている。

光・IPネットワークでは、音声・文字・データからイメージ・映像まで幅広い形態の情報が流通するが、それらの情報は全てIPパケット化されて伝達される。

これまでの電話ネットワークでは、サイズ固定の音声データを扱う電話サービスを中心として、ネットワークの品質管理や制御が行われてきた。しかしながら、様々なサービスが提供される光・IPネットワークでは、ベストエフォートサービスから品質保証サービスまでサービス毎に異なる要求条件がネットワークに求められ、多種多様なサイズやトラフィック特性のデータがネットワークを共有する。そのため、品質確保のためには従来の電話ネットワークとは異なる取組みが必要になってくる。

具体的には光・IPネットワークを安定的・効率的に運用していくためには、次のような点について、光・IPならではの手法を確立する必要がある。

設計：サービス個々に異なるトラフィック特性を考慮したネットワーク設計方法

制御：サービス品質を保持するためのNW制御技術、優先制御および帯域確保技術等

品質管理：お客様に提供するサービス品質をエンド～エンドで管理する手法

また、光・IPネットワークならではの特徴から、あるノードの不具合が他ノードに波及し通信障害がネットワーク全体に波及する「連鎖故障」の恐れも出てくる。「連鎖故障」

は、インターネットのようなオープンなネットワークほどその発生確率は高くなる傾向がある。こういった連鎖故障を防止できるような対応策の検討は、まだまだ初期段階だが、継続した取組みが必要な分野だと考えている。

ネットワークのセキュリティ

ブロードバンドの普及に伴い、ネットバンキング、インターネットオークション、電子商取引などで、住所、氏名、年齢、性別、年収、趣味、キャッシュカード番号、パスワードなどの重要な個人情報がネットワークを介して流通する機会が増加し、個人情報が盗まれたり、流出するリスクが高まっている。

光・IPネットワークでの脅威としては不正アクセス、盗聴、改ざん、偽造、なりすまし、ウイルス、DoS攻撃などがあり、ウイルス対策ソフトの普及やファイアウォールの設置などの対策が取られるようになってきている。しかし、常時接続ユーザーが増加するとともに次々と新たな脅威が生まれており、被害全体としては毎年拡大傾向にある。

そのため、十分なセキュリティ対策機能を持った強固なネットワークを構築するとともに、攻撃をされても被害を最小限に食い止められるような制御・運用体制の確立を並行して進めていくことが必要になってくる。具体的な取組みには次のようなものがある。

不正アクセス対策：悪意のユーザ

ーからの不正アクセスの遮断

不正トラフィック対策：不正トラフィックの検出と排除

被害食い止め：ウイルス感染の発見と感染端末の切り離し

おわりに

インターネット革命を主導し、IP網の構築でも先行した米国市場においても、2001年にAT&Tのバックボーンネットワークの大規模輻輳が発生、2002年にもIPバックボーンキャリア大手のUUNetのネットワークが9時間に渡り接続不能となるなどIP網の大規模障害が発生し、ユーザーへ大きな影響を及ぼすとともに、長年培ってきた顧客からの信頼を失う結果となった。

これからのブロードバンド社会を支えるインフラとして、光・IPネットワークの役割はますます重要になってきている。信頼性や品質、セキュリティなどはどうしても低価格化や新サービスの提供と比較すると後回しにされる傾向があるが、お客様からの信用は一旦失うと容易には戻ってこない。光・IPネットワークが安心して使っていただける社会インフラになるためにも、信頼性、品質、セキュリティの3つのキーワードは忘れてはいけない視点だと考えている。

お問い合わせ先

東日本電信電話株式会社
設備部 BBNWA部門
TEL：03-5359-5326