安心安全なネットワークサービスに向け キャリアに求められるセキュリティ要件

キャリアにとってのセキュリティとは？

キャリアのネットワークに対するセキュリティの考え方は一般的に非常に難しい。サービスの構成要素の中において、守るべきものの優先度を付けることがとても困難であるために、しばしば自己矛盾に陥ってしまうことがある。これらには２つの大きな理由があると考えられる。

１つは、そもそも一般企業とキャリアとでは守るべきものが違うということと、もう１つはキャリアがユーザデータをさわってはいけないという特殊な事情があるという点である。

キャリアが提供するサービスでは、ユーザトラフィックについてはその速度を最大限に保証するという努力は払われているものの、セキュリティという概念を、そのサービスの中にどのように盛り込むかについて色々な議論が存在しているように見える。むしろ、エンドユーザーからの脅威を恐れて、自網保護のためのセキュリティが必要以上に強力に施されているほどである。もちろんアクセス網の役目は、エンドユーザーとISP接続のためのアクセスラインを提供することであるから、とにかく接続するという使命にかけてはできる限り最新テクノロジーを採用しながら、高品質サービスを実現してきた経緯がある。それがFlet's などに代表されるサービスである。しかし、キャリアはユーザトラフィックについては、たとえそれがセキュリティ目的であったとしても一切タッチできない。これには過去の様々な経緯があり、キャリアにとって新たな収入源を求める上で大きなチャレンジであろう。

守るべきところは自網なのか？それともユーザトラフィックなのか？

「優先的に守るべきものは何か」というのは、キャリアにとっては意見の分かれるところであり、またセキュリティという観点からは、特にISP側インターネットからの脅威だけでなく、エンドユーザー自体が脅威となり得ることも想定しなければならない。

ファイアウォールという概念は、外（インターネット）にある脅威から中（イントラネット）を保護するという基本的な概念で理解され取り扱われてきたし、今まではそれで良かったのも事実である。しかし、残念ながら時代はそうではなくなってきている。脅威がネットワーク上のどこにあるか想定できないために、中から外への脅威、あるいは情報の漏洩といった従来とは逆のトラフィックに対してもセキュリティが必要になってきた。また、発信元に悪意があるかないかも問うことが難しい状態になってきている現状では、それを想定した上で対策を施す必要もでてきた。

ジュニパーネットワークス㈱
代表取締役　**大須賀　雅憲**氏

こうした状況についてジュニパーネットワークスの大須賀 雅憲代表取締役は次のように語っている。「キャリアモデルに当てはめると、中がエンドユーザーとして考えれば、今までの通り外（ISP側インターネット）から中（エンドユーザー）を守るということは容易に想像できますが、中から外というエンドユーザーからISPに流れるトラフィックに対してもセキュリティを考慮しなければならないことになります。キャリアがそこまでの責務を負うことはないという考えもあるかもしれませんが、もし仮にこういったビジネスモデルがあり得るとすれば、キャリアにとっては大きなビジネスチャンスになると思います。キャリア側

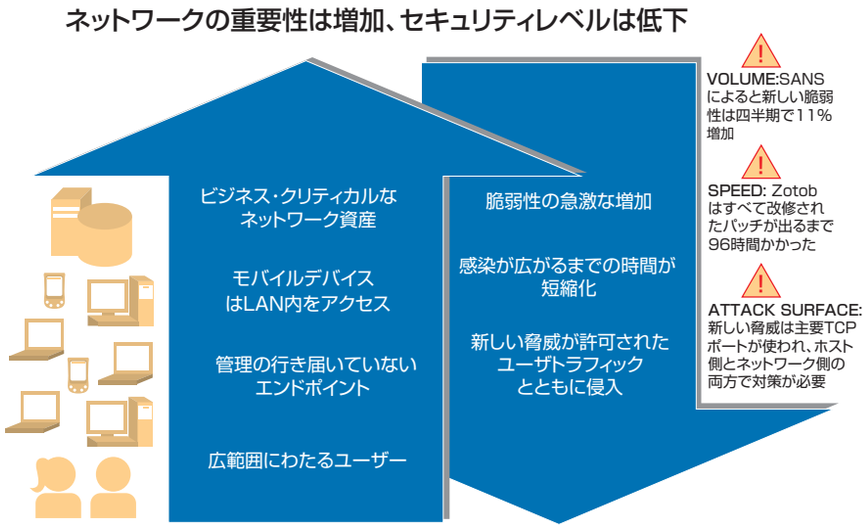

図1　ネットワーク・セキュリティのトレンド

ネットワークは、近い将来、それが当たり前の姿になってくるのではないでしょうか。」

セッション管理の必要性

セキュリティ機器にとって不可欠な技術は、セッションを1つの対象として管理するフローコントロールである。これは、従来のルーターやL3スイッチにあるような“packet by packet”の方法では、そのトラフィックが無害か脅威かの判断を付けることができないからである。ただしこの技術は、すでにキャリア側に導入済みの大半がレガシー機器で構成されているために、それによって構築されてしまったサービスとはそぐわないという課題が生じてしまう。あるいは、エンドユーザーやISPとの約款が古いままのためにそこから脱却できないという現状を見直さない限り、この課題を乗り越えることはできないのかもしれない。

ユーザーの求めるサービス

顧客がキャリアの提供するサービスを選択する際の第一の基準は、サービス品質の高さにあることは誰もが認めるところである。しかし安全という考えにおいてはどうであろうか？　現状は、ネットワーク同士を結ぶこと以外には何もなく、セキュリティという要素がそこには介在できないという本質的な課題がある。それはユーザトラフィックの品質保持とユーザトラフィックの検査（インスペクト）がある意味相反するという点に起因している。もちろんユーザー側にファイアウォールやIDS/IPSを設置するサービスも存在しており、これによりセキュリティを確保していることも事実である。しかし理想論からすれば、セキュリティも含んだアクセスラインサービスを提供することができれば、コストも含めてユーザーが求めるサービスに一層近づけることができる。

エンドユーザー側セキュリティ機器

一方、エンドユーザー側に設置されるセキュリティ機器に要求されるのは、高品質、低価格、多機能ということになる。新しい脅威が生まれてはネット上にはびこる現状を考えると、特にアンチ技術（アンチウイルス、スパム、スパイウェア等々）などの新しい脅威に対する技術をいち早く実装できることが求められる。それには、最新のテクノロジーを持っているベンダーと密接に連携をとり、自社のOSにいち早く実装できる体制をとっておくことが強力な武器になるといえる。もちろんOSのアーキテクチャ自体も新しい技術を容易に実装できるような作りになっていることも重要である。

超高速・大容量でセキュアなIPネットワーク上に固定・携帯を含む多彩な通信サービスやアプリケーションが統合される「NGN（Next Generation Network）の世界」が目前に迫っている。安心・安全のネットワークサービス実現に向け、大須賀 雅憲代表取締役は、「様々なトンネル技術を駆使し、自社のサービスを展開してきたキャリアは、その初期フェーズを終え、セキュリティを考慮した次フェーズに遷る必要がでてきたのではないでしょうか」と指摘する。