「IPv6 によるユビキタス環境構築に向けたセキュリティ確保に関する実証の請負」における IPv6 ネットワーク上でのセキュリティの確保とその応用

NTT コミュニケーションズ（株）
（株）三菱総合研究所

1 IPv6 におけるセキュリティ課題

IPv6 によるインターネットでは、その豊富なグローバルアドレスを利用することで、末端の端末同士が直接に通信し合う形態が、従来よりも遥かに増えるものと想定されている。そこでは、ファイアウォールやウィルス対策を中心とする従来のセキュリティ対策とは、まったく違った方法が求められることになる。

一方、IPv6 自身が、まだあまり普及しておらず、セキュリティ対策のための製品やサービスも少ないという現状では、従来のインターネットにおいて有効な対策が、そのまま IPv6 環境で応用できるのか、その検証すらほとんど行われていないのが実情である。さらに、デュアルスタック等の複合的な環境においては、IPv6 へのセキュリティ対策の遅れが、セキュリティホールに繋がるのではないかという危惧すら考えられる。

IPv6 におけるセキュリティ課題を分類すると下記のようなパターンに大別できるだろう。

(1) 積極的な攻撃への対策

DDoS 攻撃や SQL インジェクション、マルウェア等の外部からのサービス停止を狙った攻撃や内部への侵入･乗っ取りを目的とした攻撃など、積極的かつ過激な攻撃への対策は、IPv4 の世界においても日夜取り組まれているところである。これらの攻撃は、ネットワーク機器や OS、アプリケーションが持つセキュリティ上の脆弱性を突くものが多いが、攻撃が多い分、その対策体制も充実している。IPv6 では、対策体制はおろか、試験的な検証体制すらほとんど存在せず、IPv6 普及に向けての大きなミッシングピースの 1 つと言えるだろう。

(2) 認証／盗聴／成りすまし等への対策

IPv4 では、NAT により組織内ネットワークや家庭内ネットワークは簡易的に守られていたので、主に外部のネットワーク側やサーバー側において対策すれば良かった。しかし、IPv6 では、エンドーエンド間がグローバルアドレスにより通信可能になる。これは言い換えれば組織内や家庭内の端末に対して、外部からのアクセスが可能になるということであり、端末側にもそれなりの対策が必要になる。IPv6 では、IPsec が標準で仕様化され、認証と通信の暗号化等に使えるため、ある程度の対策が進んでいるが、設定の簡便さや使い勝手という面では、検証とブラッシュアップが必要である。

2　本実証*が対象とするセキュリティモデル

本実証では、主に **1.(2)**のエンドーエンド間での IPv6 通信を簡単かつ安全に取り扱えるようにするための仕組みについて検証している。このため、IPsec とともに、端末間の接続制御を行う SIP 技術を組み合せた m2m-x 技術を活用し、簡易な使い勝手と、確実な認証とデータの保護を両立して実現することを目指している。

実証においては、技術の実際の利用場面を考え、以下の3つのモデルを想定して、平成18年度より3ヶ年に渡って実施している。

(1) エンタープライズ利用モデル

大企業や政府組織等、組織内の情報システム部門がしっかりしており、その連携のもとに組織内にセキュリティ対策を浸透させることが可能なモデルである。一方、通信機器数や通信容量が大きいので、第三者的なセキュリティサービス組織に丸ごとアウトソーシングするような形態も考えられる。

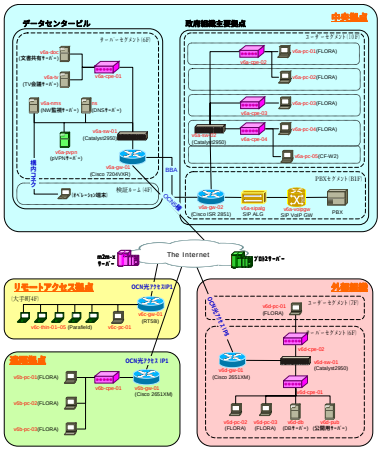
(2) So-Ho／中小企業利用モデル

情報システム部門があっても対応力が限られている、あるいは、情報システム部門が存在しないような中小の組織の場合、何らかの形で、第三者の支援が必要である。このような場合には、通信の相手からセキュリティ支援を受けるケースと、第三者的なセキュリティサービス組織の支援を受けるケースとが考えられる。

(3) 一般ユーザーモデル

一般ユーザーの場合、ITリテラシーのレベルはバラバラであり、一定品質以上のサービスをするためには、低いほうのレベルに合わせてサービス展開する必要がある。つまり、IT リテラシーをほとんど期待できないという前提のもとでも、簡単かつ確実なセキュリティを提供する必要がある。従って、通信の相手方またはその支援を行う第三者的なセキュリティサービス組織がセキュリティ支援を行うケースが考えられる。

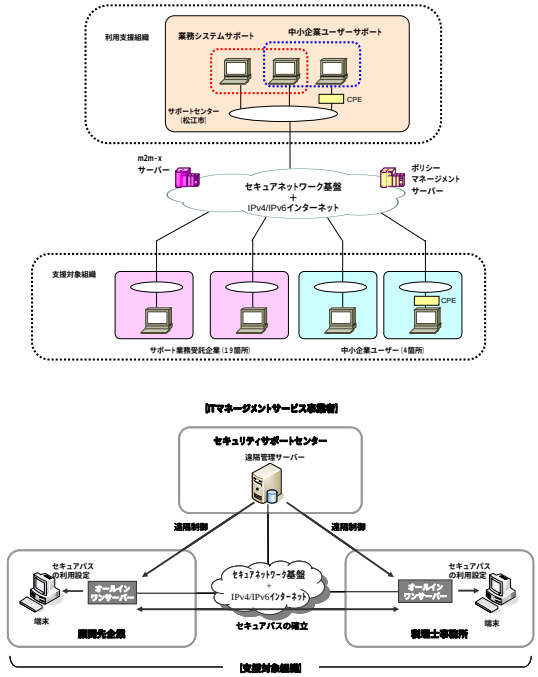
2.1　エンタープライズ利用モデル



平成 18 年度の実証においては、電子政府環境をターゲットに、中央省庁、地域拠点、外部組織、リモート拠点の 4 ヶ所を接続した構成モデルを取り上げた。これは、IT リテラシーの高い特定ユーザーをターゲットとしたもので、通信の当事者が限定されるというのも特徴である。この環境で、端末認証とアクセス制御、通信の暗号化のセキュリティ機能をネットワーク事業者の立場で参加した NTT コミュニケーションズのネットワーク基盤内に設置した m2m-x サーバーにより提供した。検証内容としては、ネットワーク

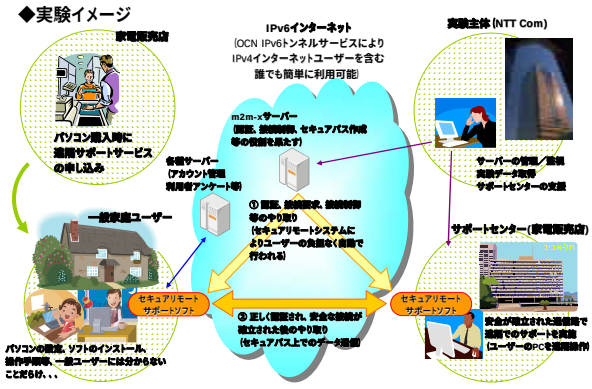
基盤が提供するセキュリティ機能が問題なく動作することやユーザーの使い勝手等について検証を行った。

2.2 So-Ho／中小企業利用モデル



平成 19 年度の実証においては、十分な IT 部門を持たない中小企業とその従業員の低リテラシー層ユーザーに対し、外部のサポート事業者がインターネットを介してセキュアに遠隔サポートサービスを提供するモデルを取り上げた。そこでは、通信相手となるサポート事業者がセキュリティ管理を行うモデルと第三者のセキュリティ管理事業者がセキュリティ管理を行うモデルの 2 つを実験している。検証内容としては、いずれも、セキュリティ機能が正しく提供されることやユーザーの業務との親和性、使い勝手等について検証を行った。

2.3 一般ユーザー利用モデル



平成 20 年度の実証においては、基本的に IT リテラシーを期待出来ない一般のユーザーを対象に、パソコン等の IT 機器の利用のためのサポートをリモートから実施するモデルを取り上げた。サポートを受けるのは、一般家庭のユーザーであり、IT 機器の販売店である家電販売店のサポートセンターから、ネットワーク経由で遠隔でのサポートを受ける形である。

セキュリティ機能は IPv6 でのアクセスのためのネットワーク基盤を提供する NTT コミュニケーションズのネットワーク内に設置した m2m-x サーバーから提供し、ユーザー及びサポートセンターの設定負荷を減らすため、m2m-x と連携するセキュアリモートサポートソフトを利用している。検証内容としては、m2m-x サーバーとセキュアリモートサポートソフトの組み合せにおいて、セキュリティ機能が正しく提供出来ることや簡単かつ安全･安心なサポートが提供出来ることなどの評価を行う予定である。

3　実証成果

既に実証の終わった平成 18 年度及び 19 年度の実証成果の主なものを以下の通りである。

- 想定した各環境において、セキュリティ機能は問題なく提供することができた。
- 比較的短期間で安価にセキュリティ機能を提供することが出来た。
- m2m-x で接続先、接続元を認証し、通信履歴として残すことが可能なため、成りすましに対して効果的な対策になる。
- 今回のセキュリティ機能は低レイヤーで動作し、多くのアプリケーションにはあまり影響を与えないと考えられるが、一部の専用アプリケーションなどは対応していないものもあり、それらは調整やチューニングが必要となる。
- セキュリティ機器の故障に際して、故障時の動作を安全側に倒すためのフェイルセーフの仕組みが必要である。
- 組織によって、あるいは同じ組織でも部署や業務によって、必要とされるセキュリティのレベルが様々に異なる場合が多い。セキュリティレベルを高くすれば利便性を損なうという部分もあり、セキュリティレベルの設定に柔軟性や階層性を持たせることが必要である。
- セキュリティの設定状況により、例えばネットワークの到達確認等に支障が出る場合がある。ネットワークの構築にあたっては、設定の順序等の工程設計をきちんと行うことが重要である。また、現在、既に稼動しているネットワークに、後からセキュリティ機能を提供する場合には、ファイアウォール等の調整も必要となる。
- 複数の組織間を接続して業務を行う場合など、それぞれの組織間のセキュリティポリシーの調整等も必要となる。
- アクセス網の構成として、CPE で IPv6 トンネルを終端し、暗号化、アクセス制御等を実現する方式では、高いセキュリティ機能を実現可能であり、ユーザーにとっても安心感が高い。
- 安心感を持ってユーザーに使ってもらうために、セキュリティ機能の安全性を確認できる仕組みがあると良い。

4　課題

3 年間を通じて、エンタープライズ利用、中小企業利用、一般ユーザー利用という 3 段階で IPv6 ネットワーク上でのセキュリティ提供方式についての検証を行ってきた。実験を通して幾つかの課題も見つかっているが、IPv6 上でのセキュリティ利用が本格化して利用機会が増えれば、自然と知見も蓄積され、解決されていく類の問題である。

今後は更に、P2P やセンサーネットワーク（人以外のものへの応用）への適用の検討等、IPv6 ならではの応用場面への適用検討が求められることになると考えられる。

---

*本実証実験は、総務省「IPv6 によるユビキタス環境構築に向けたセキュリティ確保に関する実証」の一環として実施するものです

