IPv6 階層セキュリティモデルとその管理手法の研究

岩井　崇[†], 松本　実[†],　　金山　健一[‡], 廣海　緑里[‡]

[†]インテック・ウェブ・アンド・ゲノム・インフォマティクス(株)

[‡](株)インテック・ネットコア

概 要

これまでのネットワークセキュリティは OSI レイヤ別に議論されてきた。このモデルはスケーラビリティがある点で優れているが、下層のセキュリティ情報を利用することで、より強力なセキュリティモデルを構築することができ、多数の低機能な端末が接続される環境では有効である可能性がある。

我々はそのようなモデルの一例として、積み上げ型の「階層セキュリティモデル」を提案する。このモデルは端末の情報を下層から順次「認証シナリオ」によってチェックすることにより、関門ルータの動作を制御するものである。

階層化によって端末の挙動をネットワークから制御することが可能となるため、IPv6 におけるマルチプレフィックスモデルをデバイスに対して適用する場合において、特に有効に動作すると考えられる。我々は 2005 年末に向け、その有効性を検証する実験を計画中である。

キーワード　P2P セキュリティ、IPv6、無線 LAN、管理システム

A Study of IPv6 Multi Layer Security Model and Management Method

Takashi IWAI[†], Minoru MATSUMOTO[†],　[‡]Ken-ichi KANAYAMA, [‡]Ruri HIROMI

[†]Intec Web and Genome Informatics Corp.

[‡]Intec Netcore, Inc.

Abstract

Most network-security models are based on separate OSI layer and carried out on a specific layer then such models have large scalability. But it maybe better to construct a security model taking a same account information into the other layer interaction, which model is effective for a network connecting large amount of non-pc terminals.

Here we propose a new network security model called "multi-layered security model (MLS)". In the MLS system, every terminal is certified by the "scenario", which means a terminal certified at each layer and the accumulated (certified) results control the gate router by filtering.

The MLS can control the action of a terminal on the network. This feature is preferred on the multi-prefix service model on the IPv6. We are now planning the experiments to confirm this feature at the end of 2005.

Keyword　P2P Security, IPv6, Wireless LAN, Management System

1　目的

広大なアドレス空間を持つ IPv6 の普及により、通信の質の変化が予想される[1]。具体的には、あらゆるモノがネットワークへ接続可能になり、ネットワーク間を移動する端末なども増加すると考えられる。接続端末の種類が、これまでの PC や PDA といったものからセンサーデバイスなどに広がっていくことにより、特定のモノへの高い利便性を提供するピア・ツー・ピア（以下、P2P）通信が盛んになると思われる。

こうした通信を安全確実に行うには通信のセキュリティが確保されなければならない。端末をネットワークに安全・安心に接続し、端末特性に従った通信環境を提供し、また、必要に応じて P2P の暗号化通信についても利用許可の仕組みや通信管理を提供することが求められる。

これまでのネットワークセキュリティは、OSI 通信レイヤ別に議論されてきた。例えば、データリンク層を保護する仕組みとして IEEE 802.1X 認証[2][3]、IPsec 通信[4][5]を行うための IKE プロトコル[6][7]等である。このような通信レイヤ別のセキュリティモデルは対象を制限し、別の通信レイヤと分離することによって、適用範囲を拡げることに成功したモデルである。一方、対象の限定は管理リソースの増大や、冗長な実装を招くことにつながる。センサーネットワークのように、リソースが制約される中では一定のセキュリティを確保しなければならない。

目的の違う機器群がネットワーク内に混在するような環境では、それぞれの機器群が必要なサービスを受けられる xSP(any type of Service Provider: 集中管理されたサービスを複数顧客に提供する事業者)へと接続する必要がある。IPv6 技術の重要な応用分野である非 PC 端末が接続するネットワークでは、より進化した接続基盤モデルの確立が求められる。しかし、この分野において OSI レイヤモデルは、しばしば足かせとなり得る。

セキュリティ対策という観点では、接続時のアクセス認証、TLS(Transport Layer Security)[8]などにおける証明書認証や basic 認証[9]、アプリケーション利用時の利用許可やパーソナルファイアウォールによるデータチェックなど、レイヤやサービスなどによってわかれたものをそれぞれの局面で組み合わせることによって実現している。セキュリティ対策をユーザの端末管理に任せ、ネットワーク全体としての統合的な管理がされない場合もある。

こうした現状の問題点の解消と、IPv6 のメリットを考慮し、かつ想定した機能の提供を安全・安心に運用するために、OSI 通信レイヤ別に認証されている情報を垂直統合し、下層の認証情報を上層において再利用するという手段と共に認証情報を統合管理する必要がある[10-12]。

本稿では、これらの課題を解決するために IPv6 で改良、拡張された機能である、(1)プラグ・アンド・プレイ、(2)端末インタフェースへの複数 IP アドレスの付与、(3)IPsec のプロトコル標準実装などに着目し、これらの通信レイヤ別機能を活用したセキュリティモデルとして、「階層セキュリティモデル」を提案し、その有効性を検証することを目的とする。

2　階層セキュリティモデル

ここでの「階層」とは、1 章で既に述べたとおり、ネットワークセキュリティ対策の不完全性から従来で言うところの OSI レイヤのことではなく、広くセキュリティ対策を段階的に積み上げていき、全体としてより高いセキュリティレベルを確保するためのセキュリティ対策レベルの階層であると定義する。

また、各通信レイヤにおける認証方法、認証対象などの情報を一元的に表現する記述言語として認証シナリオを定義する。

階層セキュリティモデルは、以下の機能によってシステム化される。

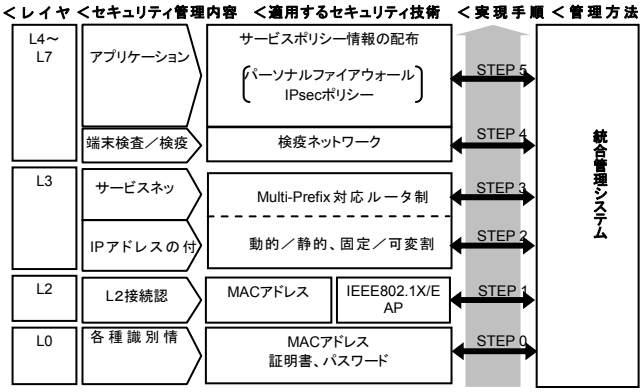
- 階層制御器
  ある認証対象に対して各階層における認証アクションを指示する機関。
- リソース管理データベース
  このサービスネットワークを利用したいデバイスの状態情報を保存するもの。
- 情報伝達通信器
  階層セキュリティモデルを搭載したシステムとそれ以外の外部システムとの情報交換する仕組みを提供するもの。
- 認証シナリオ解析器
  認証シナリオを階層制御器が理解でき

る情報に変換する仕組みを提供するもの。

- 認証局(CA)
  端末もしくは xSP を認証する上で必要となる第三者機関。
- 統合管理サーバ
  今回提案する方式では、端末の設定情報及びステータス情報を一元管理し、これを実施する中枢機能を統合管理システムと呼び、このシステムを提供するサーバを統合管理サーバとする。

階層セキュリティモデルをシステム化した上で、具体的な技術を当てはめて実現方法を検討した。以下に階層セキュリティモデルの概念図(図 1)を示し、その各サブ機能を列挙する。また、統合管理システムの実装例を図 2 に示す。

図 1　階層セキュリティモデル(完全版)



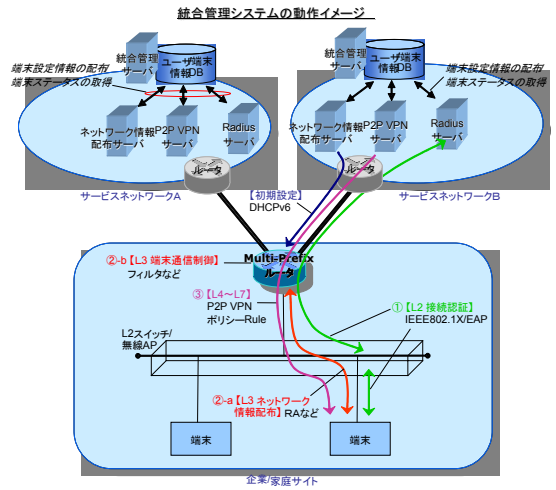


図 2　統合管理システムの実装例

2.1　各通信レイヤのセキュリティ機能の一元管理

統合管理サーバは、各通信レイヤのセキュリティ機能と協調動作するインタフェースを持ち、それぞれのセキュリティ機能へ必要な端末情報を提供する。また、それぞれのセキュリティ機能から端末のステータス情報をリアルタイムに取得、管理する。端末のステータス情報は、必要に応じて上位レイヤのセキュリティ機能へ提供される。

なお、統合管理システムは各通信レイヤにおいて協調動作するセキュリティ機能として下位から順に次のものに対応する。

- 端末認証
  データリンク層における認証技術に基づいて、端末を認証し、通信可不可を決定する。
- アドホック通信
  データリンク層の通信プロトコルに、無線 LAN(IEEE 802.11a/b/g)を利用する。
  - 検疫ネットワーク
    検疫ポリシによる端末検査を実施する。端末検査結果を受けて IP アドレスが付与される。
  - マルチプレフィックス制御技術
    検疫結果とネットワークポリシに基づいてセキュアにIPアドレスの管理と付与を行う。また、ルーティングテーブルの変更を行い、払いだしたプレフィックス自身の管理と経路制御も行う。
- P2P VPN（Virtual Private Network）システム
  端末のエンドツーエンドのセキュア通信を実現する。
- 統合管理
  端末認証の結果、検疫結果、接続しているネットワークポリシ、端末の接続状況などを統合管理する。階層の連携のための情報管理を行う。
- デバイス監視
  統合管理システムが認証シナリオに基づいてデバイスが正常なセキュリティを確保したままサービスネットワークを利用しているかどうか常時監視する。

2.2 端末情報の管理機能

統合管理システムは、各端末の初期登録情報として証明書やパスワードなどの情報を管理する機能を有する。この情報は、統合管理システムと各階層のセキュリティ機能との連携動作の際に利用する。

2.3 端末認証機能との連携機能

統合管理システムは、レイヤ２のセキュリティ対策技術として端末認証機能と連携する機能を有する。ここで取得した端末のステータス情報は、統合管理システムとその他の通信レイヤのセキュリティ機能と連携動作の際に利用する。

2.4 IP アドレス付与機能との連動機能

IPアドレス付与機能では、端末に関する初期登録情報に基づいて、端末ごとに適切なネットワーク情報(割り当てプレフィックスを含む)を配布し、端末が利用するサービスネットワークとのみ通信を許可するクローズドネットワークの機能を実現している。本提案モデルでは、IPアドレス付与機能と統合管理システム間が連携動作するためのインタフェースを提供する。これにより、2.3節の端末認証機能により得られる端末の認証結果情報を、IPアドレス付与機能による端末識別に利用することができる。

2.5 P2P VPN システムとの連携機能

端末のエンドツーエンドのセキュア通信を実現するP2P VPNシステムに統合管理システムと連動する制御インタフェースを提供する。これにより、統合管理システムが管理する端末のステータス情報のうち、P2P VPNシステムへ必要な情報を提供し、端末の通信ポリシ設定の動的生成を実現する。また、P2P VPNシステムからは、端末の通信記録を統合管理システムに提供し、端末通信のトラッキングを可能とする。

2.6 必要するセキュリティ強度のレベルに応じたセキュリティ制御機能

サービスネットワークごとに必要なセキュリティ強度は異なると想定し、それぞれのネットワークに求められるセキュリティレベルに応じたセキュリティ機能の取捨選択を実現する機能を有する。

3 管理手法

階層セキュリティモデルを使ってどのように管理するべきかを検討した。以下に、その検討結果を述べる。

① 図 1より、全体像は、xSP/家庭(ユーザ)サイトに接続する端末が必要とする階層ごとのセキュリティ機能制御を一元的に統合管理する統合管理システムとなる。

② xSP/家庭(ユーザ)サイトに提供される各サービスネットワークが、認証シナリオを持ち、ネットワーク利用に必要なセキュリティ強度に応じて各通信レイヤで使用するセキュリティ機能の組み合わせを記述できるものとする。統合管理システムは、そのシナリオを解析し、階層制御を実施する。

③ 統合管理システムにより端末情報（証明書、パスワードなど）を管理する。

④ 統合管理システムがIEEE802.1X機能と連携動作し、ここで取得した端末のステータス情報をその他の階層のセキュリティ機能との連携動作の際に利用する。

⑤ マルチプレフィックス制御技術と統合管理システムが連携動作し、端末ごとのサービスネットワークの動的な選択利用を可能とするよう制御する。

⑥ P2P VPNシステムと統合管理システムが連携動作し、P2P VPNシステムが各端末へのIPsecポリシを動的に生成、配布し、端末がそのIPsecポリシに基づいたセキュア通信を行えるように制御する。

⑦ 認証シナリオに記述された全てのセキュリティ階層レベルをクリアした端末のみがxSPサービスネットワークの利用していることを常時監視する。

4 実装と実験

4.1 実験内容

本稿では、2 及び 3 章で提案した階層セキュリティモデルをフルモデルとする。開発中の実装および実験では、このモデルを元に、その中でも最も必要かつ重要な機能である部分を抜き出して最小構成モデルを構築した（**図 3** の斜線部分）。そのモデルは、無線 LAN アクセスにおける 802.1X 認証と検疫結果による IP アドレスの配布と暗号化通信環境を使ったモデル

であり、フルモデルの有効性を十分に検証できるものであると考えている。

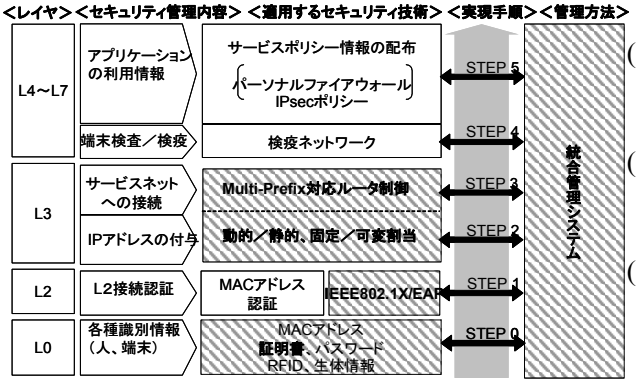


図 3　階層セキュリティモデル(本実験版)

表 1　各検査要素における実験課題

検査要素	検査場所	課題
IEEE802.1X	サーバ	・ 電子証明書発行管理 ・ 端末管理
	ユーザ端末	・ 電子証明書に基づく認証
検疫		・ ローカルスコープアドレス・ネットワークに接続し、端末検査 ・ マルチプレフィックス制御技術によりグローバルスコープアドレス再配布
IP アドレス付与	サーバ	・ ポリシ管理（IEEE802.1X 認証結果に基づく） ・ ポリシに基づくアドレス配布
	ユーザ端末	・ 複数アドレスの取得

4.2　実験環境

4.1 節で述べた実験内容を基に、統合管理システムの実装/動作として図 4 を模した実験環境を構築し、本実験を行う。

4.3　本実験で開発する機能と実証課題

実験システムの各機能について、連携動作によるセキュリティ上の有効性を検証する。

本実験を行うにあたり、いくつかの検査要素があるが、それらの検査要素において、表 1 のような課題が挙げられる。これらの課題を解決していることを、2005 年末までに検証し、成果を出す予定である。

(１) 端末認証
IEEE802.1X を利用した、電子証明書ベースの端末認証を行う。

(２) アドホック通信
データリンク層の通信プロトコルに、無線 LAN（IEEE802.11a/b/g）を利用する。

(３) IPv6 ベースの検疫ネットワーク
検疫ポリシによる端末検査を実施する（ネットワーク参加時のみ。分離やセキュリティ対策処置などは今回対象外）。
端末検査結果を受けて IPv6 アドレスが付与される。IP 通信プロトコルとして、IPv6 を利用する。

(４) セキュアな IP アドレス付与と管理
マルチプレフィックス制御技術で、検疫結果をネットワークポリシに反映した、IP アドレスの払い出しを実施する。

(５) 統合管理
端末認証の結果、検疫結果、接続しているネットワークポリシ、端末の接続状況などを統合管理する。レイヤ間の連携のための情報管理を行う。

5　まとめと今後の展望

本稿では、積み上げ型の階層セキュリティモデルを提案し、その管理手法について検討した。

このモデルは、階層化によって端末の挙動をネットワークから制御することが可能となるため、IPv6 におけるマルチプレフィクスモデルをデバイスに対して適用する場合において特に有効に動作すると考えられる。我々は 2005 年末に向け、その有効性を検証する実験を独立行政法人情報通信研究機構の研究(※)を受託して実施中である。

(※)平成 17 年度情報家電の IPv6 化関連研究開発事業の委託研究

【参考文献】

[1] IPv6 －インターネット新時代－　並木純治監修　社団法人　電子情報通信学会
[2] “Port-Based Network Access Control”, IEEE Comuputer Society, IEEE 802.1X-2001
[3] “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines”, IETF, RFC3580
[4] “Security Architecture for the Internet Protocol”, IETF, RFC2401
[5] “IP Security Document Roadmap”, IETF, RFC2411
[6] “The Internet Key Exchange (IKE)”, IETF, RFC2409
[7] “Negotiation of NAT-Traversal in the IKE”, IETF, RFC3947
[8] “The TLS Protocol Version1.0”, IETF, RFC2746
[9] “HTTP Authentication Basic and Digest Access Authentication”, IETF, RFC2617
[10] UNIX Magazine 2004 年 11 月号　特集『ポスト・ファイアウォールとセキュリティ』
[11] ″Quarantine Model Overview for IPv6 network security″, IETF,draft-kondo-quarantine-overview-01.txt
[12] Trusted Computing Group, https://www.trustedcomputinggroup.org/specs/IWG/TCG_1_0_Architecture_Overview.pdf