第 XII 部

IPv6 環境におけるセキュリティ

第 12 部
IPv6 環境におけるセキュリティ

第 1 章　はじめに

「Security of IPv6」（secure6 WG）は、IPv6 ネットワーク環境におけるセキュリティのあり方を議論、提言するために 2003 年 9 月から活動している。

2004 年は、昨年からの活動を継続し、IPv6 ネットワーク環境の普及にともなうセキュリティ対策の変化を整理し、それによって顕在化する既存のセキュリティモデルの問題点を指摘するとともに、新たなセキュリティモデルに関する議論を行った。

特に、『検疫モデル』については、一般的なモデル定義を行い Internet Draft の発行、雑誌等への寄稿 [328] などモデルの提案を行うとともに、具体的な実装手法の検討として、PANA[102] フレームワークを用いた検証を行った。

本ドキュメントは、これらの 2004 年の主な WG 活動内容について報告するものである。

第 2 章　活動概況

本 WG の本年度の活動状況は、(1) 定例会やメーリングリスト、(2) 発表活動、(3) 文書化などの作業、(4) 検証作業の大きく 4 つに分類できる。それぞれの活動状況を簡単にまとめ、報告する。それぞれの成果については、以降の章で詳述する。

(1) 定例会

今年度の定例会は、昨年度のようなセキュリティモデルについて議論をつくすための対面ミーティングという形態から、各種の発表活動や執筆活動への準備や状況確認といった、より問題点を絞った形で実施された。ミーティングでの主な議題は下記のとおりである。

#1 2004.01.20
- IETF に向けて、ドラフト執筆などの打ち合わせ
- 実証実験構築に関しての意見交換

#2 2004.02.23
- WIDE 春合宿の BoF 内容についての打ち合わせ
- IETF v6ops WG での発表に関して・状況報告

#3 2004.04.22
- v6ops で発表のあった Distributed FW モデルに関しての議論
- PANA の紹介・説明
- 類似のモデル、既存の製品・ソリューションのまとめ
- 家庭・一般ユーザにおける検疫モデルの意義に関する議論
- Internet Draft のアップデートについて

#4 2004.05.25
- 総務省の v6 移行実証実験に関して
- PANA に関する技術的な解説
- PANA を検疫モデルで利用する際の技術的な議論

#5 2004.06.16
- Internet Draft の執筆・更新に関しての打ち合わせ

#6 2004.08.13
- 雑誌原稿執筆に関する打ち合わせ
- WIDE 秋合宿の BoF の打ち合わせ

#7 2004.10.18
- WG 活動内容、マイルストーンなどの更新に関する議論
- IPv6 ネットワークでのセキュリティ問題の整理について
- ドキュメント化に向けた検討
- ネットワーク分割手法に関しての技術的な議論
- PANA における実装方法について（EAP に対する実装方法）

#8 2004.11.24
- 60th IETF 報告、今後の IETF へのアプローチに関する議論
- BCP 主導のアプローチを検討する
- PANA による実装の状況報告

- 類似モデルに関してのディスカッション・情報交換
- 12 月研究会についての打ち合わせ

メーリングリストについては、議事録や各種活動報告や状況報告など、情報共有の場として、昨年度同様活用した。参加人数についての変動はほとんどなかった。

(2) 発表活動

2 月の 59th IETF でモデルの提案および Internet Draft のサブミットを実施した。これを受ける形で、Euro6 提案モデルとのコラボレーションなどの話が進んだ。

3 月と 8 月の WIDE 研究会では、これまでの議論のまとめの発表を広く行い、引き続きセキュリティモデルやその具体的要素について議論も実施した。

9 月には、ASCII 社発行の月刊誌への特集記事寄稿という形でも、WG の活動やセキュリティモデルの提言を実施した。

12 月の WIDE 報告会では、PANA を用いた検証についての報告を行い、多くの意見をもらった。

2005 年 1 月には、SAINT での発表を予定している。

(3) 文書化作業など

本年度は、前述のとおり、発表活動と連動した文書化作業が主なものだった。

(4) 検証作業

本年度は、PANA プロトコルの認証、端末検出、端末情報交換の仕組みなどを利用した検疫モデルの検証を実施した。PANA プロトコルを十分に活用することによりこのモデルの有効性を見極めることができたが、一方で IP アドレスの配布と取得など、実用面での課題も新たにわかった。

第 3 章　IPv6 ネットワークにおけるセキュリティ上の脅威と課題

本 WG では、IPv6 ネットワークにおけるセキュリティ上の脅威の変化や課題について、整理を行った。これらの脅威の変化については下記の 3 つに分類できる。

(1) ネットワークの利用形態の変化による脅威

L3 のプロトコルバージョンに限らず、最近のネットワークの利用形態の変化により表面化したセキュリティ問題としては下記のものがある。

- ポートベースのフィルタリング
- アプリケーションレイヤ（L7）でのフィルタリング
- 端末識別子とセキュリティポリシ設定
- セキュリティポイントでのトラフィックボトルネック
- VPN、トンネリング

(2) IPv6 ネットワークでより顕在化するセキュリティ脅威

IPv4 でも同様なセキュリティ上の脅威が存在するが、IPv6 によってその脅威がより深刻化・顕在化するものとしては下記のものがある。

- Global Unicast Address と No-NAT 環境
- VPN
- IPsec
- Mobile IP
- 匿名性とプライバシ問題

(3) IPv6 特有のセキュリティ脅威

IPv6 プロトコルや仕様上特有なセキュリティ上の脅威には以下のものが挙げられる。

［技術的な問題］

- NDP とアドレス自動設定
- RA 詐称問題
- ICMPv6
- マルチキャスト
- トンネリング

［オペレーションの問題］

- 組み込み機器や Thin Client 端末
- End-to-End アプリケーション
- マルチホーム、multi prefix

これらの課題については、プロトコル・仕様の改善や拡張または新たな手法の実現によって解決すべきもの、フレームワークとして統合的に検討すべきレベル、運用・オペレーション、ユーザリテラシによって改善すべき点など、実際の対応については、それぞれのレイヤごとに検討を行う必要がある。2004 年ではこれらの課題の列挙にとどまったが、今後は WG として対処すべき課題の掘り下げと、対処すべきレイヤと手法の検討などが必要となる。

第 4 章　検疫モデルに関する考察

本 WG では、昨年度のネットワークセキュリティモデルに関する議論から『検疫モデル』を提唱し、モデルに関する議論を深めてきた。検疫モデルとは、ネットワークに端末が接続した際に、セキュリティポリシの適合性検査を行い、適合性の状態にしたがって、複数に分割されたネットワークセグメントのいずれかに端末を割り振るしくみを持つものを指す。それぞれのネットワークセグメントにおいては、管理者が定義したセキュリティポリシにしたがって、ルーティング経路やアクセス制限、トラフィック監視や帯域制御などネットワーク上のリソース、パラメータなどが設定され、セキュリティポリシの適合度に応じて端末がアクセスできるネットワークリソースを管理し、ネットワーク利用ポリシをネットワークセグメント単位に適用する。検疫モデルに関してはすでに Internet Draft として発行済みであり [169]、詳細はそちらを参照いただきたい。

本ドキュメントでは、以後 WG 内で議論が進められた点などを踏まえて、概要を報告する。

4.1 ネットワーク分割手法についての考察

検疫モデルにおけるネットワーク分割手法として、ネットワークレイヤ別（L2/L3）の手法がエンフォースメントポイントによって分類され、主に下記のものが利用できると考えられている。

(1) L2 でのネットワーク分割

L2 でのネットワーク分割手法は、VLAN（802.1Q）による方法が有望である。ただし、物理的なネットワーク構成や機器に依存する点がデプロイメント上の障害となる。現在、ルータ・スイッチなどの機器に対して、セキュリティポリシ設定に基づいた制御を行うための有効な標準化された手法はとくにない。SMTP や COPS-PR など、既存のプロトコルについては、検討・評価していかなければならない。

また、エンドポイントでの VLAN 制御については、管理者による手動設定が主体であって、検疫検査に応じて設定を制御するために実際に利用可能な手法については今後の検討課題として挙げられる。

(2) L3 でのネットワーク分割

IPv6 の prefix を利用して IP アドレスレベルでのネットワーク分割を行う手法である。L3 によるネットワーク分割の課題の多くは端末へのアドレス設定手法とその制御に依存している。IPv6 の設計ポリシの 1 つである Auto Configuration と検疫モデルなどのセキュリティ対策上の考え方とは大きく異なるため、既存のアドレス設定プロトコルを利用した場合には、整合性を保つのが難しい。特に RA による prefix 情報の配信などステートレスプロトコルの場合には、端末ごとに異なる prefix を割り振ることができない。

また、IP アドレスの詐称や prefix を手動設定した端末の特定と隔離、MAC アドレスをベースとした端末識別の詐称など、端末特定や詐称問題に対する有効な対策を検討しなければならない。

prefix によるネットワーク分割には、一度配布した prefix 情報の無効化、別の prefix への端末の再設定などの制御に関する問題も残されている。既存の prefix 情報配信では、prefix の有効期間などの制御は可能であるが、適時、特定の端末に対する prefix 情報を変更・引き剥がすことは考慮されていない。

複数のセキュリティセグメントに所属する端末の場合には、複数の prefix を持つことになるが、この場合は一般的なマルチ prefix、マルチホーム問題も解決しなければならない。

今後は、DHCPv6 プロトコル拡張、TSP などトンネル設定を利用した制御、IPsec のセキュリティアソシエーション設定を利用した End-to-End ベースのネットワークアクセス制御などについて、実現可能性を検討する予定である。

(3) トンネルを利用したネットワーク分割

IPv6 のトンネルサーバを利用して、IPv6 デュアルスタック環境であっても、トンネルサーバを経由して通信を行うことによって、トンネルサーバをセキュリティエンフォースメントポイントとしてネットワーク分割を行う手法も 1 つの実現方法として検討の余地がある。TSP などトンネル設定プロトコルを拡張することによって、検疫検査に応じた適切なトンネルサーバに端末を誘導し、トンネルサーバにてアクセス制御を行うことで物理的なネットワークトポロジに依存してルータ・スイッチ上でのアクセス制御を行う代わりにセキュリティポリシに応じた

ネットワーク分割を実現する。

デュアルスタック環境においても、常にトンネルサーバを経由して通信を行うため、多少のオーバーヘッドが懸念されるが、通信効率などについては今後の実装検証が必要となる。

(4) アクセスポリシによるネットワーク分割

いわゆる分散ファイアウォールと呼ばれる手法のように、エンドホストがもつアクセス制御機能に対して、ポリシルールを配信することによって、ネットワーク分割を行う方法もある。セキュリティ境界がエンドホストにあるため、より厳密なアクセス制御、ネットワーク分割、端末の隔離を行うことが可能であるが、ポリシの記述方法、配信プロトコルなどについては、明確な標準仕様が存在しない。実装による検証のためにはこれらの仕様の整備が必要となる。

また、ネットワークから配信されるセキュリティポリシと、端末利用者があらかじめ設定してあるポリシとの整合性問題についても、解決しなければならない点として挙げられる。

4.2 検疫検査内容についての考察

既存の検疫検査機能を実装したものには、Microsoft 社の Microsoft Baseline Security Analyzer（MBSA）[193]、FreeBSD を対象とした PortAudit[250] などが存在する。これらのほかにも各ベンダよりいくつか類似の製品が開発されているが、いずれも相互運用性や脆弱性データベースの共用といったことは可能ではなく、独自仕様のものになっている。これらの点は、一般的な PC だけではなく、情報家電や組み込み機器など、多様なマルチベンダ環境が当たり前となることが考えられる IPv6 ネットワークの場合に有効に運用していくことは難しい。

標準的な脆弱性情報記述形式や情報交換のためのフレームワークなど、標準化作業が必要であるが、現状では活発な活動は見られていない。

また、セキュリティポリシを策定する際に、どのような検査基準を設けるのか、といった検査対象に対する基本的な考え方も明確に定まっていない点が、検疫検査の有効性と客観的な評価の指針を検討するうえでの課題となっていることが挙げられた。

4.3 セキュリティポリシ

検疫モデルでは、端末のセキュリティ対策状態など管理者のセキュリティ運用ポリシ基準に応じて複数のネットワークセグメントに分割し、管理するアプローチを提唱しているが、どのようなセキュリティポリシを定義するのが有効なのか、その場合の検査基準にはどのようなものがあるかといった運用上の知見については十分な議論がなされていない。単純に通常セグメントと隔離セグメントの 2 つに分けるだけで十分なのか、より細やかなネットワーク分割とポリシ定義の有効性などについては、検証環境が十分に整い、実験環境での継続的な運用経験などが必要となる。

4.4 認証フレームワーク

検疫モデルにおいては、802.1X/PANA に代表される既存の認証フレームワークとの統合が 1 つの課題として挙げられてきた。2004 年は主に PANA フレームワークを用いた実装を検証することによって、これらの課題を確認することができた。

検疫検査においては、検査対象、検査情報など、従来の認証フレームワークが想定していたアカウントベースの端末・利用者認証と比較して、より多くの複雑な情報をやり取りしなければならないが、既存の認証フレームワークのメッセージフォーマットである EAP を拡張して対応することには限界があることが検討の結果明らかになっている。

検疫検査については、独自のプロトコル上で行い、シングルサインオンのために、認証結果をダイジェスト情報として、EAP メッセージに付加するといったような手法が必要となる。

今後は、検疫検査プロトコルや実装、EAP へのダイジェストメッセージの実装使用などの検討を行う予定である。

第 5 章　今後の課題と活動方針

(1) 文書化

これまでの議論の成果は、雑誌の特集記事への寄稿という形でまとめることが出来たが、WIDE Project

のWGとしての成果の発表という点では課題が残る。セキュリティ研究者などからのコメントを広く集め、またリファレンスされるために、WIDE Draftとしてこれまでの WG での議論の成果をまとめる必要がある。

近年、WG内で議論していた『検疫モデル』に類する実際の製品が各ベンダより発表されているが、機能の差異や比較のために基準となる指針、一般的なモデルの提示や共通概念としてのタームの定義などが、リファレンス・ドキュメントとして求められる。

(2) ユースケースによるセキュリティモデルの評価

実際のセキュリティ対策や問題点の質は、利用シーンや対象となるユーザのネットワーク環境や利用者によって、かなり大きく異なることが、これまでの議論の中で指摘されてきた。今後は、SOHO・家庭ユーザ環境、モバイル、エンタープライズなど各セグメントごとのユースケースを分析し、それぞれの環境で求められるセキュリティの要求分析をもとに、モデルの評価を実施していかなければならない。

(3) 実証実験・周辺技術・仕様の評価

2004年は、実証実験として主にPANAフレームワークを利用した検疫モデルの構築を目指してきた。まずは、これらの実証評価のレポート、評価キットなどの公開、諸問題の提示など、これまでの検証で得られた知見を公開してゆく。

また、2005年は他の技術要素を用いた検証をはじめ、各実装手法ごとの特徴、利点と問題点を整理するなど、解決すべき問題点の提示とともに今後の WG での研究対象を定めたい。

(4) リエゾン・標準化活動・実装評価

既存の周辺技術・使用に基づいた検疫モデルの実装の評価や実証実験で得られた知見を元に、必要に応じて新規プロトコルや拡張機能の提案などの活動が必要と考えられる。

現在、IPv6上で利用されている各標準化プロトコルには、特にprefixアドレス設定に関しては、ホストコンフィグレーションとネットワーク分割手法上、WGで検討している新しいセキュリティモデルの実現のためには、より効率的なアプローチや新たなプロトコルの設計・提案が必要となる。本WGでは、実証実験や既存手法の評価や問題点の指摘とともに、それらを解決できる新たなソリューション、プロトコルの実装の提示といった活動を視野に入れていくことを検討している。