第 XI 部

IPv6 環境におけるセキュリティ

第 11 部
IPv6 環境におけるセキュリティ

第 1 章　Security of IPv6 ワーキンググループ 2005 年度の活動

Security of IPv6（secure6）ワーキンググループでは、IPv6 環境により顕在化するセキュリティ問題について、その解決手法を検討することを主目的に活動している。

今年度は、以下の 3 つの計画にもとづいて、活動を行ってきた。

(1) IPv6 ネットワークにおけるセキュリティ問題の整理
(2) IPv6 ネットワークに適したセキュリティモデルの研究
(3) 検疫モデルの検証

以下、各章で詳細内容を報告する。

第 2 章　IPv6 ネットワークにおけるセキュリティ問題の整理

IPv6 ネットワークにより、顕在化するセキュリティ問題についてカタログ化し、脅威、危険度、影響範囲、現状での対策などをまとめる。IPv6 プロトコル、設計自身の問題や運用上の問題と、post firewall モデルが解決できる問題領域を明確にすることを目的とする。本活動は、3 ステップで計画しており、今年度はステップ 3 の段階として活動した。

- ステップ 1（2004/年末までに）
  - 過去の議論や雑誌原稿、I-D にて指摘した IPv6 ネットワークのセキュリティ問題をカテゴリわけして整理する。
  - 分類項目・テンプレートの整理
  - IPv6 高度利用移行推進協議会、セキュリティ SWG とのリレーション
- ステップ 2（2005/WIDE 春合宿ぐらいまでに）
  - セキュリティ問題カタログをもとに、現状での対策手法や、問題領域を切り分ける。
- ステップ 3（2005/July 63rd IETF ぐらいを目標）
  - WIDE メモとしてまとめる
  - v6ops ワーキンググループの ipv6ds デザインチームとのコラボレーション（I-D の執筆協力）

ipv6ds の活動成果として、以下の draft がある。また、分散セキュリティモデルについて「destsec」という public mailing list が用意され、活動の場を移して、BoF 開催に向けて準備を開始した。secure6 wg ではこの活動のサポートを行った。

- `draft-savola-distsec-threat-model-00.txt`
- `draft-vives-distsec-framework-01.txt`

第 3 章　IPv6 ネットワークに適したセキュリティモデルの研究

検疫モデルをはじめとする post firewall モデルについて、有益性を示すための理論的裏づけとなる議論を積み重ねる。

とくに、『セキュリティポリシに応じて内部ネットワークを複数の論理セグメントに多層的に分割する』というアプローチについて、従来のセキュリティモデルと比較してその利点や各デプロイメント環境での適用方法、推奨されるセグメント分割設計とポリシ定義についてのガイドラインを示す。

- 検疫モデルの研究
- 他のポストファイアウォールモデルの調査
- 多層化したネットワークセグメントによるセキュリティポリシ運用の効果の評価
- 各種ネットワーク利用環境（企業、SOHO、ホームなど）ごとの検疫モデルの適用手法の検討

第 4 章　検疫モデルの検証

検疫モデルの主に実装面に関する技術的検討を行う。具体的にはネットワーク分割手法と検疫検査処理のプロトコル、認証フレームワークとの統合方法などについて検討する。

- IPv6 ネットワークでのネットワーク分割技法の検証
- PANA を利用した検疫モデルの検証環境の構築
- DHCPv6 を利用したネットワーク分割手法
- TSP などのトンネリングを利用した手法について
- 802.1Q (Tag-VLAN)
- multi prefix 環境での source address selection 制御
- 検疫検査プロトコルの検討
- セキュリティポリシ管理サーバについて
  - セキュリティポリシ定義に利用する項目の整理と管理方法の検討
  - ポリシエンフォースメント機器へのマッピング・設定管理
- 認証フレームワークとの統合
  - EAP 拡張？

本年度は、DHCPv6 を利用したネットワーク分割に着手し、2006 年 3 月の WIDE 合宿ネットワークにおいての実験を予定している。

第 5 章　DHCPv6 による検疫ネットワークの検討

2005 年度の活動では、昨年 PANA を用いたセキュリティポリシベースのネットワークセパレーション手法の実装・検証に引き続き、DHCPv6 を利用したネットワークセパレーション手法の検証のための活動を進めた。

DHCPv6 を利用したネットワークセパレーション手法の特徴は、NDP を用いた自動コンフィグレーションと違い、ステートフルなアドレス設定により個々のノードのセキュリティポリシに応じて異なる IPv6 プレフィックスアドレスを振り出すなどの制御が容易に行える事にある。このことは、L3 での IP アドレスによるサブネットをセキュリティポリシに応じたセパレーションに利用する際に有効である。

5.1 過去のネットワークセパレーション手法の検討に対する検証

2004 年度の PANA によるネットワークセパレーション手法においては、ネットワーク上のノードに対して、セキュリティポリシに対応するすべてのネットワークセグメントのプレフィックスアドレスが、NDP プロトコルにより自動設定される。結果的に、ノードは、複数の IPv6 アドレスを持つことになり、ソースアドレス選択問題やマルチホーム問題などの課題に直面する事となった。

また、経路上のルータ・ファイアウォールなどと連携し、アクセスルールを動的に更新する事によって、ポリシに応じたセグメントのアドレス以外からの通信を遮断する必要があった。このため、許可されていないセキュリティポリシに割り当てられたセグメントのソースアドレスを選択した場合には、パケットがアクセスルールにより単純に破棄されるため、別のソースアドレスでの再送信などフォールバックに絡む問題を解決する事ができなかった。

動的なアクセスルールの更新は、システム全体のスケーラビリティ上も問題となる。また、LAN 内部にもセキュリティ境界上アクセスルールを適用するポリシ適用ポイントを多数設置しなければならない。

このようなことからも L3 におけるネットワークセパレーションを行う際には、DHCPv6 などのステートフルのアドレス設定機構が必要である。

5.2 DHCPv6 によるネットワークセパレーションの実装

- DHCPv6 サーバの拡張

  DHCPv6 によるネットワークセパレーション手法の実現のため、DHCPv6 サーバに対して機能拡張を行った。具体的には KAME プロジェクトの DHCPv6 サーバ実装である dhcp6s に対して下記の機能の追加を行った。
- アドレスプール設定への対応

  セキュリティポリシに対応するセグメントは、アドレスプールによる定義によって対応づけを

おこなう。そのため dhcp6s に対してアドレスプール設定に対応できるよう拡張を行った。これにより、セキュリティポリシに対応するセグメントをアドレスプールにより定義する事が可能となった。

- DUID をもとにしたアドレスプールの選択

  DHCPv6 サーバは、DUID をもとにノードを識別し、アドレス割り当てを決定する。ノードがどのセキュリティポリシに割り振られたかは、DUID とアドレスプール名をひも付けしたデータベースに格納され、検疫検査処理によって、適時更新される。DHCPv6 サーバからこれらのデータベースへの問い合わせ API とプラグインモジュールを定義し、MySQL サーバへの問い合わせモジュールの実装を行った。

- 技術的な課題

  DHCPv6 によるネットワークセパレーション手法には、いくつかの課題が存在する。

  1) DUID の詐称によるすり抜け

  DUID はノードごとにユニークになるように MAC アドレスなどをもとに生成されるが、あくまで端末の一意性を識別するために利用され、その真正性を検証するしくみは DHCPv6 プロトコルにはない。他のノードの DUID の取得、およびその詐称を簡単に行うことができる。この問題に対しては、MAC アドレスベースで生成する DUID の代わりに、検疫検査時に検疫サーバから DUID を発行するなど、検疫のしくみと組み合わせた DUID を利用する方法が考えられる。これらは、DHCPv6 プロトコルにおける DUID タイプの拡張を必要とする。今後は、このようなセキュリティポリシ検査にもとづいた識別子の定義と DUID としての利用を今後の研究課題の一つとしたい。

  2) 手動アドレス設定ノードの検知と排除

  DHCPv6 を利用せずに、手動設定などで IPv6 アドレスを設定した場合には、DHCPv6 サーバによるネットワークセパレーション制御を経ずに、ネットワークセグメントに参加する事ができる。このようなノードに対しての検知・排除機構は必須である。これらの不正ノードに対する対処としては、ICMPv6 のアドレス衝突検出メッセージをノードに通知することで排除することが考えられる。この場合、擬似的にアドレス衝突検出メッセージを応答する監視装置が必要となる。

5.3 2006 年 3 月の WIDE 合宿での実証実験に向けて

2006 年 3 月に行われる WIDE 合宿において、DHCPv6 を用いたネットワークセパレーション手法の実現性を検証するため実験を計画している。この実験では、DHCPv6 によるアドレス振り出し、ポリシに応じた動的な切り替えに付随するオーバーヘッド、トラフィックに与える負荷、アドレス切り替えに関する技術的課題などについて、実際のデータを取る事によってこれらの課題を客観的に検討する材料とすることを考えている。

5.4 今後の展望

インテリジェントスイッチなどとの協調動作により Tag VLAN による L2 でのセパレーションとの統合などに必要な機器間制御などが、今後の研究課題として挙げられる。このような複合的ネットワークセパレーションにおいては、機器間での制御に対する標準的なプロトコルや、論理的なネットワークセパレーションと物理的なネットワーク・機器構成とのマッピングをいかにして実現するかが課題といえる。

今後とも、必要に応じて IETF などでの標準化活動をふまえて現実的なベストカレントプラクティスを実現するノウハウの集積と検証に努めたい。

第 6 章　まとめ

本年度の secure6 ワーキンググループの活動は、DHCPv6 によるネットワーク分割と IETF に集まる有志による distsec/ipv6ds の活動支援の 2 つをメインとして行ってきた。今後は、前述の活動を進め、その成果をもとに、非 pc を含めた次世代のネットワーク環境へのセキュリティフレームワーク作りや提案を行っていきたい。なお、これまでの secure6 wg が取り上げてきたトピックス、作成した資料や関連ドキュメントなどは、secure6 wg の wiki ページ[1]で参照可能である。

1　http://www.secure6.org/pukiwiki/pukiwiki.php