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　はじめに

「Security of IPv6」(secure-6 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。

IPv6 環境では、従来の計算機と通信機器による構成から、情報家電やセンサー機器など身の周りのあらゆるものの接続が容易になると目されており、ネットワーク形態もモバイル性が高まり、これまでのファイアーウォールを中心としたセキュリティ設計思想とは留意点が異なってくると思われる。secure-6 WG では、情報家電ネットワーク、モバイル、動的なセキュリティウォールネットワークなどを対象に、各ネットワークモデルごとに問題領域を特定し、アドバイザリやユーザの啓蒙だけでなく、ソフトウェア技術者、実装およびベンダーへのリファレンスとなるべき White Paper の発行などの活動のほかに、ネットワークセキュリティを実現するための新たな手法・プロトコルの研究、提案および実装を行う。

今回の報告書では、第 2 章で WG 発足後に実施した過去 3 回のミーティングおよびメーリングリストでの活動報告を、第 3 章で第 3 回目までのミーティングでの議論のまとめ (White Paper 素案) を、第 4 章で今後の活動予定について報告する。また付録として、当 WG が考えるモデルと類似したものに関する情報と、ミーティング各回の議事録を添付する。

第 2 章　WG 概況

2.1 メーリングリスト登録者数など

2003 年 9 月にメーリングリスト作成後、12 月末までの登録者数は 46 人となっている。定期ミーティングは月 1 度程度の頻度で第 3 回目まで実施した。

2.2 WG 発足前夜

WG 発足に先駆けて、2003 年 6 月 6 日、「v6 時代のファイアーウォール」をテーマにブレインストーミングを実施し、20 名程度での議論を行った。ブレインストーミング実施にあたってのモチベーションは、「IPv6 時代、ユビキタス時代になると、これまでのファイアーウォール構築のアプローチとは違う観点が必要かもしれない。しかし、今のところ IPv6 対応ファイアーウォールと呼ばれているものは、そういうところまで踏み込んでいない。一方で、主に企業が IPv6 化しない理由の一つに、『ファイアーウォールの v6 未対応』と『IPv6 ネットワークのファイアーウォールシステムアーキテクチャがよくわからない』というものがある。v6 ネットワークにおける基本モデルは何であろうか。」というものであった。

主なトピックスを以下に挙げる。

- 従来の v4 ファイアーウォールとは
- ファイアーウォールに求めるもの
- v6 であることの留意点
- DoS 判定は別議論としたい

議論にあたっての共通・重要確認事項として、「ファイアーウォールに求める機能」には、

- 外からのアタックと中からのアタック防御ができる
- 管理ポイントの境界線である
- 外で感染、中で繁殖の防止をする

があり、IPv6 ネットワークである点について、以下の 3 つの留意点があげられた。

- non-pc などへの広がりを考慮しなくてはいけない
- IPsec の利用による変化を考慮しなくてはいけない
- entity 判断方法を持つ必要がある

このブレインストーミングでは、希望する解として

(1) IPv6 時代のファイアーウォールモデルを確立させたい
(2) IPv6 の利用方法を意識したファイアーウォールを作りたい

の 2 点を合意し、散会した。

2.3 WG 発足とその後

2003 年 9 月 9 日の WIDE 合宿にて BOF 開催を急遽決定し、実施した。BOF では、IPv6 ネットワークにおけるセキュリティを継続的、専門的に検討するために WG 化すること、またモビリティや non-pc へのネットワーク接続の拡大などを考慮し、自分たちが理想とする利用方法の実現のためのソリューション提示となるよう、ネットワークのモデル化から着手することを決定した。

WG 化後は、10 月、11 月に合計 3 回のミーティングを実施し、ネットワークモデル、想定している利用状態、制限や許可する目的や対象、その方法、類似例のケーススタディなど多岐にわたって、議論した。議論に参加できなかった人からのコメントはメーリングリストを活用し収集している。

平行して White Paper 作成に向けての整理も行った。

第 3 章　White Paper 素案

2003 年に実施したミーティングでの議論をもとに中間報告的にまとめた。

3.1 背景

ネットワークの安全性を実現するためには、「分割して統治する」方式でネットワークにセキュリティポリシーに従って論理的・物理的な境界を設け、境界の内側と外側との通信を制御・管理することによって、セキュリティポリシー境界の内側のネットワークの安全性を確保しようという考えが一般的であった。

これらのセキュリティポリシー境界を実現する手法としては、ルータおよびファイアーウォール機器が挙げられるが、それらのセキュリティ対策はすでに限界を迎えている。

- 組織内は安全という幻想
- 全トラフィック検査とスループット
- P2P など新しいアプリケーション・サービスとの親和性
- 外部からの安全なアクセス
- 端末はネットワーク内外を移動する

3.2 概要

- 組織内セキュリティポリシーの維持
  ネットワークに接続し、他の端末と通信を行う際には、自身の安全性を証明しなければネットワークに参加することを許可しない。あるいは何らかの制限を行う。このようにネットワークの終端（エッジ）にてネットワークに接続する機器の安全性を検証することによって、ネットワークに自由に接続・移動するノードに対しても、セグメント内にセキュリティポリシーに違反した危険な端末の進入を防ぐ。
- 検査対象トラフィックの絞込み
  また、ワームなどの検査など通信パケットに対する詳細な検査・検証の対象として、これらの安全性が保証されていない端末間・ネットワークセグメント間の通信に絞ることによって、全流量検査を省き現実的な検査を行うことを可能とする。
- 軽量クライアントへの対応
  セグメント外部からの通信はすべて、セキュリティポリシーに沿った端末からの通信であることを保証することによって、端末内部でのファイアーウォールや IDS などのパケット検査などの負荷を軽減する（IPv6 であれば、特定の機器以外のリンクローカルアドレスからの通信を制限することによって安全性の確認されていない端末からの通信を簡易に遮断することが可能となる）。

3.3 安全性の評価

安全性の検証・検疫確認には、下記のような手法が考えられる。

- 製造者 ID、シリアル番号による照合
  製品の製造者 ID、製造番号（シリアル番号）とメーカーなどが提供する安全性データベースなどを照合して判断する（組み込み系機器など、出荷後に内部のソフトウェア・ファームウェアの書き換えなどが比較的少ない機器などの場合）。
- セキュリティ対策ソフトによる検査・評価結果
  脆弱性検証プログラム・アンチウィルスソフトウェアなどによる、端末の安全性評価を基準に判断する。これらの評価結果については有効期限を設け、適時検査結果を更新する。

- ユーザ認証など既存の認証システムとの連携
  ネットワーク認証では、RADIUS の利用、SSH の利用、IEEE802.1x の利用などがあり、基本的にネットワークに接続する際に認証される仕組みである。これに対して、IPsec や SSL といったプロトコルはアプリケーションに組み込むことが容易である。

3.4 ネットワークセグメント・組織などの安全性評価

組織間の各通信の検疫検査の評価基準として、相手のセグメントに対する安全性評価・確認手段が必要となる。

- 組織間の通信においては、相手のセグメントの安全性評価と自身のセキュリティポリシーを比較し、検証対象となる相手端末および通信を決定する。
  例）セキュリティ対策がほとんどなされていない端末を抱える組織、セグメントからの通信は重点検査の対象とする。

3.5 セキュリティ監査・評価機関

セグメントの安全性を評価・確認する手段、組織間のセキュリティポリシーネゴシエーション時の評価値としてセキュリティ監査（格付け）機関による評価値を利用する。

セキュリティ監査・評価機関は、各サイトの安全性を定期的にモニタし、アセスメント結果に基づいて安全性の評価を行う。評価は、定期的に行われ、評価内容に応じて更新し、またその評価結果および手法なども広く公開されるものとする。

セキュリティポリシー作成者が、対象組織のセキュリティ安全性基準・評価を確認する際には、これらの機関の信頼性を勘案しその評価を利用することとなる。例）セキュリティ監査機関 XYZ による評価、数ヶ月間のモニタリング結果における評価が AAA の組織とは自由に通信を許可する、など。

3.6 検疫確認の場所

検疫確認には、以下の状況が考えられる。

- 端末がネットワークに参加する際。
- 組織の境界（ボーダー）と他の組織間の通信が行われる時。

3.7 検疫処理時の動作

検疫確認の結果に応じて、以下のような動作を行う。

- 検査合格
  最低限の検査を除き、すべての通信を自由に行える。ただし通信相手の組織のポリシーによっては、相手先とのポリシー調整の結果、相手組織の境界に位置する機器、または自組織の境界上の機器にて詳細検査が必要となる。
- 詳細検査
  危険性のある端末・通信と判断された場合には、管理者のポリシーなどに従って、パケット検査など、より詳細なチェックを行う。
- 隔離処理
  グローバルアドレスプレフィックスを通知しない、他のセグメントへの通信をすべて遮断する、特定の VLAN にアサインするなどネットワーク上から隔離を行う（IPv6 の場合、リンクローカルアドレスからの通信先を制限するなど）。

結果的に、セキュリティ対策を行っていない端末、安全性が確認されない端末からの通信は隔離・遮断および重点検査されることになり、ネットワーク全体の安全性を高めると共に、安全性が確認された端末間・組織間の通信などは最小限のオーバーヘッドのみで質の高い安全な通信環境を利用することが可能となる。

3.8 セキュリティポリシーの作成

各組織は、自組織のネットワークセグメントと外部に対してのセキュリティポリシーを設定する必要がある。ここでは、何を基準として相手がセキュリティ上安全と評価するのか、安全であると認識した場合、どこまでの接続性などを許可するのかといった基準を示すことは難しく、セキュリティポリシー作成上の課題ともなる。安全性の検証・評価のひとつの指針として、セキュリティ監査機関によるレポートおよび評価基準の明確化、格付けなどの数値化などポリシー作成に必要な補助的な判断材料の質・信頼性・客観性が強く求められることになる。

ただし、ここでいう組織が個々の家庭や SOHO ネットワークを指す場合、セキュリティポリシー策定に関する専門知識を前提にすることは難しいため、サービスの一部として ISP などのインターネット接続サービス業者がポリシー作成を補うなどの仕組みが必要となると考えられる。

3.9 動的モニタリング

検疫検査を通り、安全な通信相手と認証した場合においても、トラフィックの動的モニタリングなどの結果に応じて、確認を行うことも検討する（特定トラフィックの異常増加など）。

3.10 緊急警報によるセキュリティレベル（DefCon）コントロール

端末のセキュリティ安全性検証では、未知の危険性については 100%検知、判断することは現実的に難しい。場合によっては端末の検疫検査に問題がなかったとしても、未知のワームやセキュリティホールによる攻撃を受ける危険性が存在する。

検疫検査には平常時のほかに、Network Worm の発生など緊急時におけるポリシーの規定、および自己組織・端末・ネットワークの防衛の観点からの緊急動作を規定する必要がある。

セキュリティレベル（DefCon）には以下のものが考えられる。

- CERT などセキュリティ監視機関や認証機関から発せられるものに基づいて決定されるネットワーク全体の安全性状態を示すもの
- 組織内のセキュリティポリシーによって規定され、組織のセグメント内のポリシー違反率や、ワームなどの発見数、トラフィック異常、外部からの攻撃の検知などによって組織防衛的に決定されるもの
- 各組織にて検出したセキュリティ警告情報の共有による、相互分散協調的なネットワーク状態の判断に基づいた自立的なセキュリティレベル

第 4 章　今後の課題

2004 年には、さらに議論を進め、まとめたものを発行する予定である。この活動を、IETF やその他 WIDE 内外にも広げ、セキュリティ指針として活用されるような働きかけも検討していく。

具体的な活動目標として、以下に 4 点を挙げる。

(1) 文書化

White Paper とも呼んでいるものを､次の WIDE 合宿までにまとめ、発表する。

(2) WIDE 合宿での実験

White Paper の提案に基づくセキュリティモデルの実証実験を行う。

(3) IETF

Internet-Draft (informational) でここでの議論のまとめを出す方向で検討する。関連技術・プロトコルの研究者などとの議論・意見交換。必要に応じて、検疫モデルの実装のために必要なプロトコル拡張、データフォーマットなどの標準化作業を行う。

(4) その他団体とのコラボレーション

検疫モデルの実装・実験などに関連し、他のセキュリティ関連団体、WG などとの連携を模索する。

付録 A　他の類似モデル

ネットワーク、セキュリティベンダ各社からも類似のモデルに基づいた製品・サービスが発表、発売されている。「検疫モデル」は今までのボーダーセキュリティ対策上の問題を解決する手法として注目を集めつつある。

- Cisco NAC (Network Admission Control)
  `http://www.cisco.com/warp/public/779/largeent/nac/AdmissionControlQA_v41.pdf`
- NEC 検疫システムソリューション
  `http://www.nec.co.jp/press/ja/0401/2904.html`
- Integrity
  `http://www.zonelabs.com/`

付録 B　各回の議事録

◇ 9 月 10 日　WIDE 合宿 BOF

主なトピックス

- “セキュリティ” についてのおさらい
  – 認証、盗聴や改ざん防止、ウィルス・ワーム

対策駆除、DoS 攻撃などセキュリティ分野の概要と領域を説明。

- IPv6 で考えられるセキュリティ問題についてのブレインストーミング
  - ネットワークの理想から出発しよう。現実をみると NAT や dialup など妥協の産物をまた産むことになる。
  - OS（windows, opensource）の評価の話も入れたい。

決定したこと

(1) WG 化
(2) v6 の理想的なネットワークに根ざしたセキュリティモデル作り
(3) White Paper 作成

◇10 月 7 日　第 1 回ミーティング

主なトピックス

- 理想的なセキュアネットワークを考える前提として、まず IPv6 技術が出てきた背景、目指したものの再確認
  - いつでもどこでも connectivity がある。
  - end to end のアプリケーションが広がる。
  - QoS が確保されている。
  - mobility との親和性が高い。
  - 軽量クライアントへの接続と利用が広がる。
  - multihome
  - 自分の物は自分が使いたい。そして、どこからでも使いたい。
  - v4 の uncontrolled なネットワーク上の安全性ではなく、controlled なネットワーク上での安全性が欲しい。
- 既存のセキュリティモデルが直面している問題（ユーザーの見地からの議論）
  - ノード間の通信管理（制限する、ではなく通す方向で）
  - 制限なく通信ができるようにしたい。
- セキュアなネットワークを構成する要素（player）
  - ポリシーを決め、宣言する人（ユーザ）
  - 実現する人（ネットワーク管理者、ISP）
  - 実装する機器、実現ポイント
- 電話システムなど既存の他の通信サービスをアナロジーとして、セキュリティ面についてディスカッション
  - end-to-end 通信である。
  - アクセスコントロールはあまり使われていない。
  - 悪い事をした人を特定できる。
    - ＊悪い事を特定できると迷惑な事は減る。
    - ＊v4 世界のような、危険の可能性だけで filter out されるのは何とかしたい。
- 他の例
  - 国際貨物のセキュリティチェック
  - NDA のある会議での携帯撮影の制限
  - フリーネットワークと公共ネットワーク

決定したこと・議論で得られた内容

- セキュリティモデルの方向性

「安全なネットワーク上での信頼できるノードには制限のない自由な通信を許可できる仕組み」

◇10 月 30 日　第 2 回ミーティング

主なトピックス

- UNIX Magazine 11 月号「Firewall の限界」について
  - 既存の firewall テクニックは機能、構成、性能的に限界。全パケットのチェックは無理。これも我々の動機を裏付けてくれる話である。ここでの課題解決が新しいモデルに必要である。
  - v4/v6 のトラフィックを分離、色分けする装置を置くモデルへ
    - ＊検疫 over クラスタ化されたファイアーウォール
    - ＊高速 path と低速精密検査 path による負荷分散
- トラフィックの検閲（split/marking）
  - 検疫済みのノードを区別して、それらは安心して自由にネットワークを使えること。
    - ＊ネットワークに入る時に検疫をかける。
    - ＊ノードの信頼性はいつまでも続かない。風邪も怪我もある。
  - 健康診断・Yellow Card・ノード内のセキュリティ検査などを経過し、常によい健康状態で利用できるようにする。
  - 暴れた人は制裁をうける仕組みもいるかもしれない。
  - 動的な管理が必要。

- linklocal は取り扱いを注意する。間違った RA を流したら blacklist 入りさせるなど。
- 802.1x 認証を信用するか？
  - ＊信用して、信頼できるセグメントへ。
  - ＊それ以外はセキュリティ検査・フィルタリングルールの厳しいセグメントへ。
  - ＊セグメントの安心状況の指標になるか？

- 異なる検疫機構のすり合わせ
- 安全基準とサイト評価、格付け機関

◇11 月 28 日　第 3 回ミーティング

主なトピックス

- IETF58 での v6ops のセキュリティ議論についてと IETF59 に向けて
  - Pekka Slova より提出されているセキュリティシナリオについて、ここでの議論を生かせそうである。
  - IETF59 に持ち込んでみる。v6ops が適切か、どのように持ち込むかなどは次回作戦会議する。
- イエローカードモデル、検疫モデルのおさらい
  - 端末がネットワークに参加する際にセキュリティチェックをして許可。
  - トラフィックの全文検査はパフォーマンス的に難しい、色分けなどが必要。
  - 攻撃は外からだけではない。blaster のように内側からも発生する想定を。
  - 端末はネットワーク内外を動き回る前提
  - セキュリティポリシーに合致している安全性を保証して接続させる。
  - つながったあとは、安心して各種サービスを利用でき、ネットワーク利用に制限がないので嬉しい。
- 検査装置
  - 「装置」というより「ポイント」。ネットワーク的な“場所”として考える境界を分け、switch/filter するためのプロファイル提供、検査を実施。
- 端末〜装置の間のプロトコル
  - 802.1x で認証することを推奨という前提とし、VLAN グループを作る時にセキュリティポリシーを検査する仕組みを入れるなどできるのではないか？
  - 認証情報として何をみるか
    - ＊ID/passwd のほかに OS が何で、アプリケーションは何を入れているかなど、ノードに関する様々な情報の取得・確認ができるような拡張性が必要。
- 検査とは
  - トラフィックの種類をみて検査するという方向で議論されていた。
  - このモデルはトラフィックの種類とアクセス方法（VPN）の推奨だけではなく、認証方法、端末特定、端末内部情報も取り扱うことになる。
  - 認証とアクセス方法だけではなく、端末の持つ安全性確認も必要。具体的には、セキュリティアップデートをしっかりしているかなど。
  - VPN している A-B 間における通信ではなく、A 内で発生させるトラフィックの検査装置
  - 認証をトリガーにポリシー検査することと、通過するトラフィックの検査を分ける。
  - 粒度をどう設定するか、レイヤ毎にできることの定義がいる。
  - トラフィックの流れや負荷はシンプルにすることとのバランスも取ること。
- 内部汚染について
  - セキュリティ境界を出て行く時だけ検査するだけでなく、内部に持ち込まれた後の措置を考慮する。
  - 疑わしき端末からのパケットはそのセグメントに流さない措置など。
  - 危ないという判断があったら切り離す、対処がされたら再接続する対処
- セキュリティアップデート対処
  - セキュリティアップデートしているかどうか判定し、していなければオートアップデートをかける手法を盛り込むかどうか？
  - 何か事がおきたら、処理が集中しそう。スケーラビリティを考慮する。
- inspection とクイズ
  - 動作内容端末をつなぐと、802.1x の認証が走り、v6 のやり取りがあり、イエローカードのポートでチェックされる。
  - 安全性確認のクイズを端末に出す。対処してあれば答えられる質問
  - Q-A のタイムラグを考慮すること。
  - カンニングできないような仕掛けであること。

- 検疫セキュリティモデルの応用
  - ホームネットワークの場合 ISP 側にポリシー DB があり、サービスとしてセキュリティレベルに応じたものが用意されていて、コンシューマユーザはそれを選んでネットワークを利用。利用者の端末のセキュリティ対策状況に応じて、通信の制限・自由度が異なる。セキュリティ対策を怠っている端末には、接続制限、パケット検査などが行われる。
  - ネットワーク天気予報、セキュリティ予報局
- 危惧される点
  - セキュリティレベルが下がった場合の自動対処を盛り込むと、障害発生・セキュリティ問題発見からの対応処理が煩雑になることが懸念される。
  - CERT 情報で情報提示だけではなく、オートアップデートも考慮し、それらの情報をプログラムなどで直接利用できるようにならないか？
  - 隣のネットワークセグメントは信用できるか？信用情報を直接取り交わすパターンと信用情報 DB 参照パターンなどに分類可能。
- セキュリティポリシー間境界と端末の移動
  - 別ネットワークから移動してきた端末が入ってきた場合、その別ネットワークのセキュリティポリシーを検査する仕組み
  - 端末がどういうネットワークに過去属していたかがわかるような仕組みとしてログ収集アクションを取ることを推奨、traceback との組み合わせも検討する。
  - いくつかのネットワークを経由して相手と通信する場合の経由するネットワークのセキュリティチェックを行う仕組み
  - ネットワークポリシーの入れ子はあるが、セキュリティポリシーの入れ子はないか検討が必要。
- エンドユーザー・ISP へのモチベーション
  - ネットワーク・ISP 事業者のセキュリティレベルによる格付け
    - ＊ISP-X は優良ユーザばかりなので A ランク、ISP-Y はセキュリティ対策を怠っているユーザの割合が多いので B ランクといったように、帯域幅やスループットといった指標以外にセキュリティ対策面で ISP のサービスを評価する指標を考えてみる。
  - ユーザーにセキュリティ対策を行い自身の端末のセキュリティレベルを上げるモチベーションとなるようにモデル提示していく
  - ‘fear’ によるセキュリティ対策ではなく、‘benefit’ を得られること。

決定したこと

- IETF59 に持ち込む
- Internet-Draft 執筆（検疫モデルについて）