# 第 IX 部

# IPv6 環境におけるセキュリティ

# 第 9 部
# IPv6 環境におけるセキュリティ

## 第 1 章　はじめに

security of IPv6 ワーキンググループ（secure6 ワーキンググループ）は、IPv6 ネットワーク環境におけるセキュリティについて技術的課題とその検討を行うために 2003 年より活動を行っている。これまでの活動の中では、おもにローカルネットワークセグメント内のセキュリティポリシーに反する端末の隔離によりセキュリティレベルを高める『検疫セキュリティモデル』を中心に、その検討を行ってきた。

## 第 2 章　活動概要

検疫セキュリティモデルを実現するためには、2 つの技術的課題がある。1 つはノードのポリシー検査手法とその信頼性基盤の構築、もう 1 つはポリシーにもとづいてノードを隔離または、多層なオーバーレイネットワークを構築するためのネットワークセパレーション手法がある。

### 2.1 エンドポイントでのポリシー検査

検疫セキュリティモデルを実現する技術的な課題の 1 つであるエンドポイントでのポリシー検査では、IETF において NEA（Network Endpoint Assesment）ワーキンググループが立ち上がり、活動を開始している。NEA では、おもに Trusted Computing Group による Trusted Network Connect などを主体とし、エンドポイントにおけるセキュリティ検査の仕様に関する標準化活動が行われている。

secure6 ワーキンググループでは、65th IETF における NEA ワーキンググループ立ち上げ準備のための BoF に参加し、動向の把握に努めた。

現在、各社より『検疫モデル』とよばれるさまざまな製品・ソリューションが提供されているが、相互運用性は保証されていない。しかしながら、NEA での活動を通じて標準的な仕様・プロトコルが規定され自由なシステム構成・運用を行う環境ができることが期待される。

エンドポイントでのポリシー検査を行う際の問題は、多様なソフトウェアバージョンの組み合わせのシステムに対して、エンドポイントのセキュリティレベルを定量的に規定するための手法がないことがあげられる。このような課題に対しては明確な方向性に対する議論が深まっておらず、検査ポリシールールや設定の管理などの煩雑化などの課題を残している。

### 2.2 ネットワークセパレーション

本 WG では、これまでの活動において、ネットワークセパレーション手法の技術的検討を重ねてきた。昨年は PANA を用いたネットワーク分離と IP アドレス管理手法の検討を行ったが、2006 年は、より簡易に利用可能な手法として DHCPv6 サーバーを拡張したダイナミックアドレス設定によるネットワークセパレーション手法についてプロトタイプを作成し検証を行った。

## 第 3 章　合宿実験の実施

2006 年 WIDE 春合宿において、DHCPv6 を利用したネットワークセパレーション手法についての実験を行った。実験の詳細については、WIDE memo（`wide-memo-secure6-meeting-20060309-00.txt`）を参照されたい。

### 3.1 実験の概要

この実験においては、WIDE DHCPv6 実装をもとに、エンドノードのポリシー管理 DB によるアドレスグループの振り分け機能を拡張したサーバーを利用した。

合宿ネットワークは、各 BoF 部屋ごとに異なるネッ

トワークアドレスが振り出され、それぞれの BoF 部屋ごとに、ポリシーに応じて定義した複数のネットワークアドレスを定義し、利用者はサーバーによる判断にもとづきいずれかのアドレスが割り振られるようにグループ化を行う機構を構築した。エンドノードの識別には、DHCPv6 にて利用されている DUID を用いた。DUID をキーにして、ポリシー DB を検索し、DUID に紐付けされているグループに応じて、払い出すアドレスを動的に決定した。

通常、エンドノードのポリシー検査に応じて決定されるエンドノードごとのセキュリティポリシーグループの決定は、Web アプリケーションによるクイズの回答をスクリプトにより集計することによって、DUID に紐付けされるグループを動的に決定し、エンドノードに対して振り出されるアドレスを変更した。

### 3.2 実験結果

合宿実験においては、いくつかの技術的な課題を洗い出すことができた。

(1) アドレスの手動設定ノードの対策

従来から指摘されていることではあるが、DHCPv6 サーバーによるアドレス配布を受けずに、手動によりアドレス設定したエンドノードを、どのようにして管理するかが課題として残されている。NDP を利用し DHCPv6 サーバーが振り出したアドレスではないアドレスについて、擬似的にアドレス重複状態を作り出すことによって対策を行うことは可能ではあるが、十分な解決策とはいえない。しかしながら、DHCPv6 を利用したネットワーク分離手法自体が簡易的な手法であるため、どの程度厳密な制御を行うことが求められるかという点では必要十分な対処法であるとは言える。

(2) 動的アドレス切り替え

合宿実験では、アドレスを動的に切り替えるため、アドレス割り当て時に設定している振り出しアドレスの有効期間を短くする事で、アドレスの再取得を促し、アドレス変更を通知するタイミングを得ている。アドレス開放と再設定をサーバー側から直接的に制御することができず、アドレス有効期限によるタイムアウト処理に依存している。

また、新たなアドレスが振り出された場合、DHCPv6 クライアントの実装によって動作が異なるが、一時的に古いアドレスと新しいアドレスの 2 つが有効なアドレスとして利用できる状態になるものがあるため、アドレス選択の問題も発生する。ソースアドレス選択はエンドホストにゆだねられてしまうため、ポリシー設定に紐付けるアドレスプールのネットワークアドレスを設定する際には、2 つのアドレスがエンドホストに振り出されているとき、セキュリティポリシーの厳しいアドレスが優先的に利用されないように考慮する必要がある。

この問題については、サーバー側からソースアドレス選択の優先順位を設定する機能や、サーバー側からのアドレス再取得要求を行うための拡張などの手法を検討する必要がある。

## 第 4 章　今後の課題

これまでの議論の中では、おもに固定系のネットワーク利用を前提としたセキュリティ対策とその課題について議論を重ねてきた。

今後の IPv6 の本格利用と普及において、IPv6 の利点がより享受できる利用形態や事例が進むと考えられる。今後は、このような IPv6 が得意とする分野（Mobile IPv6 など）や利用セグメント・シナリオにフォーカスした課題の検討と活動を進める必要がある。