

## 第 VIII 部

# BSD における IPv6/IPsec スタックの研究開発



## 第 8 部

## BSD における IPv6/IPsec スタックの研究開発

## 第 1 章 はじめに

KAME プロジェクトは、IPv6 および IPsec の参照実装を BSD 系 OS 上で開発、フリーソフトウェアとして公開し、それによってこれらの技術を広く普及させることを目的とした研究開発グループである。このプロジェクトは 1998 年に WIDE プロジェクト内の IPv6 関連研究者によって結成され、その後一部メンバの入れ替えをしつつ活動を続けている。

KAME プロジェクトが開発した実装成果は、すでに IPv6 および IPsec の標準的な実装としての地位を確立しており、基本プロトコルは各 BSD の一部としてマージされている。また、実装の成果を元に、IETF における標準化作業にも貢献しており、これまでに多数のインターネットドラフトを提案し、3 本の RFC を発行している。

## 第 2 章 2003 年の活動

2003 年は、IPv6 普及の流れを一層強固なものとするための応用的な機能を中心に、実装および標準化作業を進めてきた。ここでは、個別の技術項目について、標準化との関連と BSD へのマージ状況・予定を含めた開発面の成果について述べる。

## Advanced API

Advanced API とは、IPv6 拡張ヘッダや path MTU 情報などの応用機能を扱うための API 仕様である。KAME ではこの仕様の改訂版に対して、標準化および実装の両面で深く関与してきた。KAME プロジェクトのメンバが編者として加わった標準化作業は 2003 年 5 月に RFC3542 という形で完了した。また、標準化の過程を通

じて随時仕様変更に対応した実装を提供しており、参照実装としての役割も担っている。RFC 発行時点で、“r” コマンド用の拡張の一部を除くほとんどすべての API 仕様の実装済みである。仕様が RFC として発行されたことから、今後適切な段階で各 BSD へのマージ作業を進める予定である。

## Default Address Selection

複数のアドレスを使い分ける場面が多い IPv6 における選択の既定値を与える仕様が、2003 年 2 月に RFC3484 として発行された。KAME では、この仕様の草案段階から参照実装を提供し、その実装・運用結果を標準化の過程で反映させてきた。この仕様に含まれる選択ルールのほとんどは既に実装済みであり、標準化が完了したことから、今後各 BSD へのマージを進める予定である。

## DHCPv6/Prefix Delegation

DHCPv6 の仕様は 2003 年 7 月に RFC3315 として正式に発行された。KAME では、この仕様策定中を通じて、仕様変更に対応しながら独自の実装を提供し、またその成果を標準化作業にも反映させてきた。実際、仕様草案の最終段階において、IESG から仕様のレビューも依頼されている。

2003 年は、他の DHCPv6 実装との相互接続実験にも積極的に参加した。具体的には、1 月の TAHI、3 月の Connectathon、7 月の IETF 後の試験 (NEC 主催) に参加し、5 つ以上の異なる実装との相互接続性を確認している。

KAME の DHCPv6 実装には、アドレス設定に関する設計・運用方針に基づき、アドレス割り当ての機能は実装されていない。しかし、DHCPv6 の重要な応用である DNS サーバアドレス配布機能やプレフィクス割り当て (prefix delegation) 機能は実装済みであり、他の実装との相互接続性を確認した上で、実運用ネットワークにおいて利用されている。

DHCPv6 の基本仕様の標準化が終わり、主な応用オプションのオプション番号が正式に割り

当てられたことを受けて、今後各 BSD へのマージも進める予定である。

#### Multicast DNS (mDNS)

KAME では mdnsd というデーモンで multicast DNS を実装している。これは draft-ietf-dnsext-mdns-03 に基づく実装であり、現行のドキュメント (mdns-27) と大きな隔りがある。開発を進めていない理由は、IETF での標準化動向が不明確であること、および multicast DNS 実装としてもっとも普及している Apple Rendezvous と IETF 仕様の相互運用性に関して未だ議論が分かれていることである。

各 BSD へのマージ予定は未定である。

#### Stream Control Transmission Protocol (SCTP)

KAME では CISCO 社の Randall Stewart 氏のグループと共同で BSD 用 SCTP の実装を行っている。IETF において SCTP そのものの仕様は固まっている。

今年には実際のアプリケーションプログラマに対する見せ方やエラー時の挙動 (例: 通信相手ホストが SCTP を実装していなかった場合のタイムアウト) に関して考察や実装を行った。各 BSD へのマージ予定は未定である。実装の安定度、アプリケーションに対する影響などを考えつつ来季に持ち越したい。

#### ESpV3/AH 2402bis

IETF において ESP および AH の改版作業が勧められている。パケットフォーマットは変わらないが、セキュリティポリシのモデルや再送攻撃防御のためのカウンタが 64 bit になった点 (パケット上には下 32 bit しか現れないが両端では上 32 bit も数える) が異なる。

KAME としては今年度中に仕様が固まることを期待し実装準備や調査をしていたが、仕様が固まらなかったため実装は来季に持ち越すこととなった。

#### Key Management Protocol (KMP)

IETF では IKE の第 2 版である IKEv2 の仕様策定を進めている。これは VPN を構成するための KMP であり、end-to-end の IPsec のための KMP としては冗長に作られている。一方、IETF では KMP を 1 つに定めることをせず状況に応じた KMP の使用を許している。そのため複数の KMP が標準化されようとしている。

その 1 つに Kerberos を使った KINK が挙げられる。

KAME プロジェクトでは IKEv2 に代わる end-to-end のための KMP を実装する予定だったが、候補を絞り切れずに終わった。一方で、IKE、IKEv2、KINK を 1 つのプラットフォームで動かすための枠組の設計を USAGI プロジェクトと共に進めている。

#### Source Specific Multicast (SSM)

昨年実装した IGMPv3/MLDv2/関連 API を標準化完了次第各 BSD にマージすることを、今年度の目標としていた。

SSM 実現に必要な要素技術 (IGMPv3、MLDv2、関連 API、SSM アーキテクチャ) は、全て IESG で承認され RFC となった。しかしながら Apple 社が SSM 技術使用者に対して自社特許への有償契約を要求しているため、KAME は現在マージ作業を見合わせている。現在 Apple 社のエンジニア経由で同社法務担当者へ問い合わせ中である。

Juniper 社の Tom Pusateri 氏 (IETF PIM WG 議長) から KAME IGMPv3、MLDv2 実装の FreeBSD へのマージ要求があり、KAME に対するマージ作業への期待は依然として高い状態である。

#### ISATAP

昨年度実装した ISATAP を標準化完了次第各 BSD にマージすることを今年の目標としていた。しかしながら 2003 年 7 月、SRI 社が ISATAP 実装者に対して自社特許へのライセンス契約を要求した。ライセンスは無償であるものの、同社ライセンスが KAME のライセンスと整合性があることを SRI 社へ問い合わせても確認できないため、KAME は 2003 年 11 月 ISATAP 実装の公開を中止した。

#### PIM

IPv6 にて PIM-SM を実現する際に生じる問題を解決するため、Hello メッセージを拡張するよう 2003 年 3 月 IETF に提案した。この提案は KAME の実装に基づいた拡張方式である。提案内容は PIM-SM 基本仕様へマージされ、現在 WG で last call にかけている。また、基本仕様において拡張用のオプション番号が正式に割り当てられたことを受け、正式な番号に対

応できるよう実装も修正した。

#### Datagram Congestion Control Protocol (DCCP)

KAME では Lulea 大学による FreeBSD5 用の実装をベースにして各 BSD 用の DCCP 実装を行っている。IETF において、DCCP そのもの、Congestion Control ID2 (TCP-like) および Congestion Control ID3 (TFRC) の改版作業が行われている。各 BSD へのマージ予定は未定である。

#### X Window System

昨年度 X Window System のトランスポートレイヤの IPv6 対応を実装した。しかしながら SUN Microsystems 社による実装が x.org に採用された。この実装に対して KAME での実装を元に IPv4/v6 dual socket 対応など必要な部分をフィードバックした。

#### VRRP

昨年度実装した VRRPv3 を標準化動向にあわせて改版することを目標としていた。しかしながら VRRPv3 実装者に対して Cisco 社の特許へのライセンス契約が必要であることが判明した。同社ライセンスが KAME のライセンスと整合性がないため、KAME は 2003 年 8 月 VRRPv3 の実装の公開を中止した。

#### Mobile IPv6

KAME Mobile IPv6 グループは、Mobile IPv6 自体の開発に加え、Nautilus6 WG と協力しつつ Mobile IPv6 技術の普及に向けた技術研究を進めた。KAME Mobile IPv6 に関する研究開発活動については、Nautilus6 WG の報告で詳述している。

