第 VII 部

BSD における IPv6/IPsec スタックの研究開発

第 7 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。本プロジェクトは 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、その後も一部のメンバを入れ替えながら活動を継続してきた。

これまでの実装の成果は、BSD 系 OS への開発成果のマージも含めて十分な成功を収めた。また、IPv6 の標準化および普及への貢献においてもプロジェクトの設立時の目的を達成したといえる状況となった。そこで、KAME プロジェクトは 2006 年 3 月をもって現状の基本プロトコル成果を完結し、プロジェクトとしての開発活動を完了する。

本稿では、今年度大幅に機能が向上した Mobile IPv6/NEMO BS（Network Mobility Basic Support）の詳細に触れる。また、プロジェクト完了に向けて今年度に注力した BSD への移管作業の詳細と、完了後の方向性について述べる。最後に、8 年間を総括した成果についてまとめて説明する。

第 2 章　Mobile IPv6/NEMO BS 詳細

2004 年 12 月に SHISA と呼んでいるユーザ空間ベースの新実装を公開後、1 月に TAHI Interop、3 月に Connectathon の 2 つの相互接続試験イベントに参加して、その相互接続性が良好であると確認した。その結果、設計上の大きな問題は発見されなかったので、この 1 年は信頼性の向上、安定化に注力した。これによって、ホームエージェントとコレスポンデントノードについては TAHI 仕様適合試験に対する適合性をほぼ満たすようになった。

この 1 年に導入された大きな機能は以下のとおり。

- babymdd の導入：従来使われていた移動検知デーモン mdd より単純で実用性の高い移動検知デーモンとして、単純な mdd という意味で babymdd という名前のデーモンを利用するようになった。
- config：従来はコマンドラインで指定するのみであった各デーモンのパラメータをファイルを通して設定できるようになった。
- migrate サポート：IKE（Internet Key Exchange）デーモンと移動管理系デーモン間でトンネルの終端アドレスが変更されたことを通知するための仕様（`draft-sugimoto-mip6-pfkey-migrate`）を実装した。これによって Mobile IPv6 の IPsec を IKE で管理することが可能になった。
- IPv4 Mobile Network Prefix サポート：IPv4 の移動ネットワークを NEMO BS を用いて実現するための仕様（`draft-shima-nemo-v4prefix`）を実装した。既存の IPv4 資産を利用しつつ、基盤ネットワークを IPv6 に変更する方法を提供した。

第 3 章　KAME プロジェクトの完了

1998 年 4 月の発足以来、KAME プロジェクトが開発してきた実装成果は、BSD 系 OS の一部として IPv6 および IPsec の標準的な実装としての地位を確立するに至った。一方、こうした直接的な成果の波及効果として KAME が取り組んできた IPv6 の普及にもこの 1 年で目処が立ったといえる。具体的には、IETF における標準化作業は基本プロトコルについてはほぼ収束し、IPv6 の商用サービスも日本や欧州を中心に立ち上がってきた。

こうした情勢から、KAME プロジェクトでは、その設立時の目的を十分に達成したと判断し、2006 年

3 月末をもって基本プロトコル開発グループとしての活動を完了する。完了に至る最終年度である 2005 年度は、KAME 内で開発済の機能のうち、標準化および実装状況が安定している部分を BSD にマージするとともに、完了後のコードの管理体制について各 BSD の開発者との合意を形成することに注力した。

3.1 各 BSD へのマージ作業

2005 年は、2006 年 3 月の KAME プロジェクトの完了を目前に控え、これまでに開発してきた機能を各 BSD へマージすることに専念した。マージ対象の技術および対応するプロトコル仕様は以下の通りである。

- 近隣探索プロトコル（NDP)
  - `draft-ietf-ipv6-2461bis-05.txt`（RFC2461 の改訂版）
  - `draft-ietf-ipv6-rfc2462bis-08.txt`（RFC2462 の改訂版）
- IPv6 アドレススコープ機能の拡張
  - RFC4007
- IPv6 拡張（Advanced) API
  - RFC3542
- アドレス選択アルゴリズム
  - RFC3484
- IGMPv3/MLDv2
  - RFC3376、RFC3590、RFC3810
- Mobile IPv6/NEMO BS
  - RFC3775、RFC3776、RFC3963

表 3.1 に 2005 年 12 月現在の各 BSD へのマージ状況を示す。

未着手の項目については、それぞれ以下のように対応する予定である。

- OpenBSD
  - FreeBSD、NetBSD へのマージ作業完了後に、萩野が中心となりマージを行う
- Mobile IPv6/NEMO BS
  - SHISA 実装（2 章参照）が安定したタイミングでマージを行う
- NetBSD IGMPv3/MLDv2
  - NetBSD のほかの項目のマージが完了次第、マージに着手する

3.2 開発を他のグループへ委託する機能

KAME では、安定した仕様のみならず、未だ積極的に技術仕様の検討が進められている先端技術も開発している。これらの技術に関連するコードは、まだ BSD にマージするほど安定していないため、KAME プロジェクト完了後は WIDE プロジェクトの他のワーキンググループで研究開発を継続する。表 3.2 に一覧を示す。

表 3.1.　KAME 完了に向けた BSD へのマージ状況（2005 年 12 月現在）

	FreeBSD	NetBSD	OpenBSD
近隣探索プロトコル	完了	作業中	未着手
IPv6 アドレススコープ機能の拡張	完了	作業中	未着手
IPv6 拡張 API	完了	作業中	未着手
アドレス選択	完了	作業中	未着手
IGMPv3/MLDv2	作業中	未着手	未着手
Mobile IPv6/NEMO BS	未着手	未着手	未着手

表 3.2.　KAME 完了後の研究開発予定および担当グループ

研究開発項目	今後の研究開発グループ
SCTP/DCCP	SCTP ワーキンググループ
Mobile IPv6/NEMO BS	Nautilus6 ワーキンググループ
IKEv2	IPsec ワーキンググループ
DHCPv6	sourceforge.net で WIDE-DHCPv6 project として継続
pim6sd/pim6dd	sourceforge.net で mcast-tools project として継続

第4章　8年間の総括

KAMEプロジェクトが8年間活動した総括として、実装した機能を解説する。実装した機能を大別すると以下のようになる。

- IPv6
- IPsec
- Mobile IPv6/NEMO BS
- マルチキャスト

以下でそれぞれの機能を説明する。

4.1 IPv6

KAMEスタックの前身であるHydrangeaをもとに各社のコードをマージした。マージ完了後は、RFCやInternet-Draftを積極的に実装した。実装の範囲は、基本仕様、自動設定機能、トンネル機能、経路制御機能、スコープ付きアドレス、API、DHCPv6など多岐にわたる。

BSDに組み込まれた後は、新しい悩みが生まれた。それは、Internet-Draftの改訂で仕様が大幅に変化すると、BSDユーザを混乱させてしまうことである。そこで、原則として、Internet-Draftの段階の仕様を実装したものはsnapで公開し、RFCに対する実装のみをBSDへ還元する方針をとった。

4.2 IPsec

IPsecコードは、カーネル空間でのIPsecそのものの実装とユーザ空間での鍵交換ソフトウェアに大別できる。我々のIPv4およびIPv6用のIPsecは、FreeBSDやNetBSDにマージされている。残念ながら我々のコードは、暗号ハードウェアとの相性がよいOpenBSD由来のコードで置き換えられるだろう。しかしながら、仕様をいち早く実装し、誰でも自由に使え、安定して動作するIPsecスタックを提供できたことの意義は大きいといえる。

鍵交換ソフトウェアの名前はracoonである。racoonバージョン1は、IKEバージョン1をサポートし、BSDのみならずLinuxでも採用された。現在、racoonバージョン1は、作者であるKAMEプロジェクトの手を離れ、IPsec-Toolsとしてsourceforge.netで保守されている。

一方、WIDE IPsecワーキンググループは、現在racoonバージョン2の実装に専念している。racoonバージョン2は複数のメンバーが協力して開発している。ポリシを管理する部分がユーザ空間で実装されていることと、IKEバージョン2およびKINK（Kerberized Internet Negotiation of Keys）の両方をサポートしていることが大きな特徴である。IKEバージョン2は、相互接続実験で良好な結果を出した。KINKは誰でも自由に使える実装としては世界初である。Linuxを最初からサポートしていることもバージョン1との違いである。現在、より仕様に忠実となるように、またMobile IPv6でも利用可能となるように開発を進めている。

4.3 Mobile IPv6/NEMO BS

第1期（1998–2000年）は、Ericssonがローダブルモジュールとして開発したMobile IPv6のコードをsnapにマージしていた。第2期（2000–2002年）からは、独自のコードをカーネル空間で開発し始めた。このコードは、仕様がRFCとなるまでに長い時間がかかったため、snapで提供されたのみだった。

現在、慶応大学で独自にMobile IPv6の実装を進めていたSFCのメンバと力を結集して、SHISAというコードを実装している。これは、古いコードを置き換えるかたちでsnapとして公開されている。

SHISAでは、移動に関する情報をやりとりする処理をカーネル空間からユーザ空間へ移した。この処理は仕様でしばしば変更されてきたが、さらなる変更があったとしてもSHISAの方式ではユーザ空間のプログラムを変更するだけでよい。このため、BSDカーネルへのマージに大きく影響することがなくなった。SHISAは、Mobile IPv6に加え、特許問題を解決したNEMO BSの実装も含む形でsnapとして提供されている。現在、SHISAをBSDへマージすることを検討している。

4.4 マルチキャスト

IPv4ではマルチキャスト中継機能が、OSごとに独立に実装されていた。そのためOSによってサポート状況が異なったり、マルチキャスト対応OS間でもAPIが異なったりしていた。こうした統一性のなさが、IPv4マルチキャスト普及の足枷の一因になっていた。

KAME プロジェクトでは、IPv6 マルチキャスト中継機能および経路制御ソフトウェアをすべての BSD に共通な形で実装し、すべての BSD へマージした。このため、どの BSD でも同じ IPv6 マルチキャスト経路制御ソフトウェアを使用できる。これは IPv6 マルチキャスト普及にとって、大きな前進であった。

なお KAME プロジェクトの開発した IPv6 マルチキャスト経路制御ソフトウェアは、現在 SSM（Source Specific Multicast）機能や Linux のサポートも含めた形で、sourceforge.net の mcast-tools プロジェクトにて保守されている。

さらに KAME プロジェクトでは、仏 INRIA の NetBSD 向け IGMPv3 ホスト実装をもとに、すべての BSD 向けの IGMPv3/MLDv2 ホスト機能を実装した。今後この機能を BSD へマージする予定である。

付録　各 BSD へマージされた日付

KAME プロジェクト発足時には、BSD 系 OS を対象とする IPv6 の実装としていくつかの競合相手が存在した。その中から最終的に KAME のコードが選ばれ、各 BSD へマージされることとなった。その記念すべき日付を以下に記す。

- BSD/OS 4.2　2000 年 11 月 29 日
- FreeBSD 4.0　2000 年 3 月 14 日
- NetBSD 1.5　2000 年 12 月 6 日
- OpenBSD 2.8　2000 年 12 月 1 日