

第 IX 部

BSD における IPv6/IPsec スタックの研究開発

第 9 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、その後一部のメンバの入れ替えをしつつ活動を継続している。

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。

2004 年は、従来からの活動を継続しつつ、IPv6 の普及にむけて仕様や実装をより洗練させる作業や、マルチキャストや Mobile IPv6/NEMO (Network Mobility) 等の応用機能の実装にも注力した。また、知的財産権 (Intellectual Property Right, IPR) とくに特許に抵触する技術に対して以前より積極的に関与し、知財権の保持者との交渉を通じてこうした技術についても開発対象とできるような体制を整えた。

以下、個々の具体的な成果についてより詳細に述べる。

第 2 章 BSD へのマージ状況

2004 年に KAME が行った BSD へのフィードバックは、以下の 3 つである。

- 細かなバグ修正

- onlink assumption の削除 (v6fix WG 活動参照)
 - DHCPv6 クライアント/リレー/サーバ実装のパッケージ (FreeBSD ports) 提供
- その他 BSD への追従・サポートプラットフォームの整理を行った。詳細は以下の通りである。

- BSDI3/4 — サポート終了
- FreeBSD2/3 — サポート終了
- FreeBSD4 — 4.10 をサポート。但し 2005 年頭にサポート終了
- FreeBSD5 — 5.3 をサポート
- NetBSD — 1.6.3 2.0
- OpenBSD — 3.5 3.6

第 3 章 IPv6 アドレス自動設定機能の改訂

IETF では現在、IPv6 のアドレス自動設定機能の仕様 (RFC2462) を改訂中である。KAME プロジェクトの神明が改訂版の編者として作業を進めている。KAME プロジェクトではまた、この改訂仕様を実際にも実装してその動作を確認し、仕様の改訂作業にもその結果を反映させてきた。具体的な改訂項目としては、主に以下の 2 点である。

- 重複アドレスの検出において、その直前に送信するマルチキャスト受信者探索パケットがほかのノードと衝突しないようにランダムな遅延を設けた。
- 重複アドレスの検出により、ハードウェアアドレスから生成したインタフェース ID を持つリンクローカルアドレスが重複していると判定された場合には、そのインタフェース上での IPv6 機能を停止するようにした。

第4章 DHCPv6 拡張

従来から KAME プロジェクトで提供してきた DHCPv6 の実装に対し、2004 年には RFC3315 の一部として定義されている認証機能を新たに実装した。また、その実装過程で仕様に不明確な点が判明したため、それらをまとめたインターネットドラフトを投稿した。このドラフトは IETF の dhc WG の正式ドキュメントとして採用されている。KAME プロジェクトによる DHCPv6 の実装は、従来は KAME のスナップショットとしてのみの公開であったが、2004 年 8 月には、認証等の拡張機能も含めて FreeBSD の ports コレクションの一部として公開した。

第5章 IPv6 fix 関連の実装

IPv6 fix とは、IPv6 の仕様・実装・運用における不具合を解消することで IPv6 への移行に向けての障害を取り除くことを目的とした活動である。この活動に関連して、KAME プロジェクトでは、DNS の IPv6 関連レコードへの問い合わせに正しく応答しないサーバに対応するためのクライアント（リゾルバ）側での改良機能を実装した。この機能の詳細については v6fix WG での報告書において述べる。

第6章 マルチキャスト

マルチキャスト関連では、IGMPv3/MLDv2 関連の実装活動を行っている。

2004 年 1 月、第 5 回 TAHI 相互接続試験にて KAME MLDv2 ホスト実装の conformance（仕様適合性の検証）テストを実施した。発見されたバグの分析を行い、KAME MLDv2 ホスト実装の修正や conformance テストのバグ指摘を行った。その他、

tcpdump、Ethereal へ MLDv2/IGMPv3 のコードを提供した。

昨年からの残課題であった IGMPv3/MLDv2/関連 API の各 BSD へのマージ作業は、Apple 社特許問題が未解決のためまだ保留中である。

第7章 Mobile IPv6/NEMO

KAME の Mobile IPv6 コードは従来すべてカーネルで実装されていたが、カーネルの肥大化や拡張性の問題を抱えていた。今年度、慶応大学で独自の Mobile IPv6 コードを開発していたメンバを新たにコアメンバに迎えて、その多くの部分をユーザーランドに移行させることを決定した。実装方針は大きく変更されたが、コードは KAME、慶応大学が過去に開発してきたコードが再利用できたため、ほぼ半年で実装が完了した。また、同時に NEMO の実装も完成させた。

この実装を完成させるために 2004 年 4 月から計 3 回の実装合宿を催した。2004 年 10 月には、最新の実装を持ってフランス・カンヌで開催された ETSI IPv6 Plugtests に参加し、その基本動作、および他社 Mobile IPv6 実装との基本的な相互接続性を確認した。

先に述べた通り、新規実装は NEMO コードを含んでいる。NEMO は IPR の問題を抱えていたため、当初は KAME が公開しているレポジトリとは別のレポジトリで開発されていた。KAME プロジェクトでは、Mobile IPv6/NEMO を IPv6 および今後のインターネットで重要な位置を占める技術だと認識しており、コードの公開に向けて IPR 保持者との直接交渉を続けてきた。その結果、NEMO の IPR 問題は解決し、新規実装が 2004 年 12 月に公開 KAME レポジトリにマージされた。IPR 問題の詳細に関しては、第 9 章で述べる。

なお、旧実装に関してはすでに多数の相互接続テストイベントで機能を確認済みである。2004 年 1 月の TAHI 相互接続試験、2004 年 3 月の Connectathon では、基本的な相互接続性に加え、IPsec を用いて Mobile IPv6 の制御パケットを保護する機能に関して重点的に相互接続性を検証した。

第 8 章 IPsec (racoon2: IPsec WG 参照)

KAME プロジェクトの IPsec に関わる活動として今年度は以下を予定していた。

- IPsec 仕様の改訂版の実装
- IKEv2 の実装
- IPsec API

ietf では、IPsec の基本仕様 (RFC2401) や ESP (RFC2406)、AH (RFC2402) を改訂しようとしている。KAME プロジェクトでは、これらの仕様に基づき実装を進める予定だったが、それぞれの仕様が RFC になってから実装することにした。

現在の鍵交換プロトコルの標準は IKEv1 だが、これを置き換えるプロトコルとして IKEv2 の仕様が決まりつつある。KAME プロジェクトでは、WIDE IPsec WG とともにこれを実装した。またこの活動の一貫として Kerberos (RFC1510) を利用した鍵交換プロトコル KINK (draft-ietf-kink-kink-05.txt) や、IPsec ポリシ管理デーモンも実装した。詳細は IPsec WG の報告を参照されたい。

ietf に参加している一部の IPsec の開発者は、アプリケーションが IPsec を利用しやすくするための API を定めようとしている。KAME プロジェクトでも、この活動に参加しているが、参加メンバの都合により今年度は着手できなかった。

第 9 章 IPR 関連

IPv6/IPsec 関連技術の普及を促進するため、KAME では設立当初からライセンス契約が必要な技術を意図的に実装せず、自由に利用できる技術のみを開発、提供してきた。しかしながら、近年、特許に対する注目が高まり、特許を事前に申請し、技術の利用にライセンス契約を要求する形態が増加している。多くは、防衛目的の特許と思われるが、ライセンス契約が必要なため KAME では実装を見合わせていた。ライセンス契約と KAME のソフトウェ

ア配布ポリシとの整合性が不明確なためである。

ライセンス契約など、知的財産権に関連した問題 (以下「IPR 問題」) を抱えた技術の中で、KAME が注目しているものとしては、ISATAP、NEMO、SSM、IKEv2、SEND、VRRP などが挙げられる。これらの中には、IPv6/IPsec 技術の普及のために重要な技術も含まれている。そこで今年度より、KAME では、IPR 問題を持つ技術を単に無視するのではなく、技術的に重要であれば、積極的に問題を解決し、実装を公開してインターネットの発展に寄与する方針で進むことにした。

現在、KAME では IPR 問題を持つ重要技術に関して、各技術保持者と個別交渉を実施している。KAME が目標としている理想的な交渉結果は、権利保持者がライセンス契約不要な形で技術提供を許可することである。

今年度は、NEMO と ISATAP に関して進展が見られた。NEMO に関しては Cisco と Nokia が、ISATAP に関しては SRI が IPR を主張している。これらの組織との交渉の結果、両者が納得する形で交渉を終えることができた。現在 KAME では、その結果を踏まえ、NEMO と ISATAP の実装を公開、配布している。

