第 XIII 部

IP パケットの暗号化と認証

第 13 部
IP パケットの暗号化と認証

第 1 章　IPsec ワーキンググループ 2005 年度の活動

IPsec ワーキンググループは IPsec（RFC4301 他）に関わる事項（実装、運用など）を扱っており、現在主に活動している項目は以下のとおりである。

(1) IPsec で利用する複数の鍵交換プロトコル（IKEv2、KINK）を利用可能にするアーキテクチャ
(2) 上記アーキテクチャの実装（名称：racoon2）（注：racoon2 のアーキテクチャについては 2004 年度 WIDE 報告書を参照）

racoon2 の特徴を以下に挙げる:

- IKEv2[1]、KINK[2]と 2 つの鍵交換プロトコルをサポート
- 複数の OS 上で動作（Linux、NetBSD、FreeBSD）

本年度は、この racoon2 の開発において基本機能の実装を完了させ、多くの人々に使用してもらうため一般向けにリリースを行った。また Mobile IP への対応作業を行った。

第 2 章　racoon2 リリース

長らく開発中であった racoon2 であるが、今年度初めて一般向けにリリースを行った。リリースは計 3 回実施されソースコードの形で公開された。なお、racoon2 のソースコードは、`ftp://ftp.kame.net/pub/racoon2/` より取得可能である。

- 第 1 回目のリリース（1 月 28 日）
  このリリースでは鍵交換プロトコルとして KINK プロトコルのみをサポートしている。
- 第 2 回目のリリース（6 月 25 日）
  このリリースでは、KINK に加えて IKEv2 も鍵交換プロトコルとしてサポートされている（ただし、Transport モードのネゴシエーションのみ）。
- 第 3 回目のリリースは（11 月 2 日）
  このリリースでは、IKEv2 で Tunnel モードのネゴシエーションもサポートされ、また IKEv2 Interoperability Workshop に参加した結果を踏まえてより相互接続性が向上されている。

第 3 章　IKEv2 Interoperability Workshop 参加

WIDE IPsec ワーキンググループでは 1 つのプラットフォームで複数の鍵交換プロトコルをサポートするためのデーモン群 racoon2 を開発している。その開発者のうち株式会社東芝研究開発センターの福本淳と神田充、横河電機株式会社の坂根昌一の 3 名が、9/18 から 9/23 に ICSA Labs が主催した IPsec/IKEv2 の相互接続テストに、IKEv2 部分をテストするために参加してきた。今回のテストは、オープンで比較的大規模な IKEv2 の相互接続テストとしては第 2 回となる。

場所はカナダのオンタリオ州トロントの郊外のホテル Holiday Inn で開催された。100 人程入るミーティングルームを 24 時間 6 日間借り切って、朝は 8:00 から夜は遅いときは 11 時過ぎまでテストが実施されていた。参加した企業は 12 社で、14 実装が持ち込まれた。

テストは厳密に定められた形式はなく、互いに声を掛け合い、主催者の ICSA Labs から配布されたノートに記述された大まかなパターンにそって、テストする項目を交渉してから始められた。

1 対 1 で行うわけではないので、また不具合を修正した後の検証は相手に付き合ってもらうことにな

1　IKE（Internet Key Exchange）v2: RFC4306 にて定義される鍵交換プロトコル。
2　KINK（Kerberized Internet Negotiatoin of Keys）: `draft-ietf-kink-kink-11` にて定義されるノードの認証に Kerberos を利用した鍵交換プロトコル。

るので、こちらから積極的に声をかけないとテストが進まないことになる。我々を含め各自頻繁にテーブルを行き来していた。

事前に用意されたパターンとしては、以下の基本パターンと、いくつかの状況を設定したパターンがあった。

基本パターン

暗号アルゴリズム	AES-CBC-128
PRF	HMAC-SHA1
認証アルゴリズム	HMAC-SHA1-96
DH GROUP	5
その他	NO ESN、単純な TS

その他のパターン

1) 送信側が DH グループとして X、Y の順でプロポーザルを送信し受信側が Y を選択した場合
2) Cookie Notify を使った場合
3) 送受信側で異なるライフタイムを採用した場合の rekey
4) 証明書を使う場合
5) NAT-T[3]をする場合
6) EAP を使った場合
7) CP Payload を使う場合

このうち 4、5、6、7 に関しては我々の実装が追い付いていないので、全くテストできなかった。

我々は、Linux 2.6 と NetBSD 2.0 をプラットフォームにし、2 実装を除く 11 実装と基本的な接続性を確認した。2 実装のうち 1 つは時間が調整できずにテストができなかった。もう一方は実装がまだ追い付いていないようでテストにならなかった。接続性を確認した相手とは、テストの最中にさまざまな不具合を修正しながらテストを続け、また互いに仕様の誤解を見つけたりもし、非常に有意義なテストができた。

全体の傾向として、テストでは Tunnel mode が主であり特に事前にことわらない限り Tunnel mode を前提としてどこの参加者もテストを行っていた。IPv4 NAT Traversal はほとんどの実装がその機能を供えており相互接続を考えると racoon2 でも必要であると感じた。TS のネゴシエーションは実装にばらつきがあったため、単純な TS を使った場合はつながるものの、それ以外の場合だとつながらないことがあった。TS は相互接続性の問題点になりそうである。運用の際には事前に調整し同じ TS を使った方が無難かもしれない。また、IKEv2 の仕様として rekey の開始は実装依存にしているため相互接続性に少なからず影響がでる要因になると感じた。残念ながら IPv6 に関しては高々 1 実装のみが公式に対応していた。

IKEv2 はワイヤーに流れるメッセージは可能な限り符号化するのでデバッグが簡単ではない。これを助けるために送信時の符号化する前、受信時の復号化した後のメッセージを 1 つの PCAP 形式ファイルに保存するコードをテスト期間中に実装した。このファイルを ethereal などで見ると何を送受信しているのかが一目瞭然になる。実際に、これを使ってテスト相手のバグを指摘することができた。

テスト最終日の金曜日の午前中には、テストで問題があったか、何を明確に記述すべきかなどのヒアリングがあった。この結果は IKEv2 Clarifications and Implementation Guidelines の次の版に反映される。

以下に関連する URL を列挙する。

- 相互接続テスト結果
  `https://www.icsalabs.com/icsa/docs/html/communities/ipsec/bakeoff/Bakeoff_II%20Results.pdf`
- ICSA Labs 相互接続テスト
  `https://www.icsalabs.com/icsa/docs/html/communities/ipsec/bakeoff/Registration_2.html`
- IKEv2 ドラフト
  `http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-17.txt`
- IKEv2 Clarifications ドラフト
  `http://www.ietf.org/internet-drafts/draft-eronen-ipsec-ikev2-clarifications-05.txt`

3　NAT-T（Network Address Translation-Traversal）: NAT 配下にいるノードでも IPsec により保護された通信を行なうための技術、RFC3715[3]、RFC3948[113] などにて定義されている。

第 4 章　開発項目

4.1 IKEv2

racoon2 の IKEv2 部分は本年度着実に開発が進み基本的な機能はほぼ実装を終えることができた。主な開発完了項目を以下に挙げる：

- Tunnel モード/Transport モードのネゴシエーション
- 鍵の再更新（rekey — IKE_SA 及び child SA[4]）
- デリートペイロード（Delete Payload）
- OS ごとの PF_KEY[5] 実装の違いを吸収するためのタイマー
- アルゴリズムの追加（AES-CTR と CMAC）

また、IKEv2 の基本機能ではないが、Mobile IP の拡張作業も行った。詳細は次節に記す。

4.2 KINK

racoon2 の KINK プロトコル部分は、インターネットドラフトの更新（`draft-ietf-kink-kink-06` から `draft-ietf-kink-kink-11`）に伴なう変更を行った。

`draft-ietf-kink-kink-11` での主な変更点を以下に挙げる：

- Cksum フィールドの位置が、ヘッダ直後からメッセージの最後に移動し、それにともない計算方法が変更された
- Kerberosの仕様に従ったため、CksumLenフィールドが 1 octet から 2 octet に変更され、ヘッダ内のフィールドの位置も変更された
- 将来の Kerberos の更新に追従しやすくするため、KINK_ENCRYPT ペイロードの暗号化の方法が変更された
- ISAKMP[6] Delete ペイロードには送信者から見て inbound の SPI を含めると明示された
- KINK のペイロードタイプを ISAKMP registry から取得するのではなく、我々で定義するようになった
- KINK_TGT_REQ/KINK_TGT_REP ペイロードのフォーマットが変更された（racoon2 ではまだ実装していないので修正点は無し）

また、KINK のインターネットドラフトの変更ではないが、間接的に利用している `draft-ietf-krb-wg-crypto-07` が RFC 3961 になる際に、prf の計算方法が変更されたためこちらについても対応を行った。

第 5 章　racoon2 の SHISA 対応

5.1 はじめに

racoon2 に対し BSD 上の Mobile IPv6 実装である SHISA との協調動作を可能にする機能拡張を行った。現状、IPsec や IKE の利用は固定したネットワーク環境における VPN 用途がほとんどを占めており、IP モビリティ環境への適用は考慮されてはいなかった。そこで新たな利用対象として Mobile IPv6 環境に着目する。実際、Mobile IPv6 の本格的な運用や、高度なセキュリティ（アンチリプレイ攻撃）を実現するためには自動鍵交換が不可欠である。

racoon2 の大きな特徴の 1 つとして IKEv2 のサポートが挙げられる。そのため IKEv2 を利用した Mobile IPv6 との協調動作を実現する。そのために racoon2 に必要な要求事項を挙げ、それに対する設計・実装を示す。

5.2 前提

5.2.1 Mobile IPv6 における IPsec の適用範囲

Mobile IPv6 における IPsec/IKE(v1) を用いたモビリティシグナリングやユーザトラフィックの保護については、RFC3775、RFC3776 に記述されており、移動ノード（MN）とホームエージェント（HA）との間の通信に IPsec を適用する。仕様では手動鍵交換のサポートを必須（MUST）、そして自動鍵交換のサポートを推奨（SHOULD）としている。以下、それらによって実現される必要がある IPsec の適用範囲を示す。

4　SA（Security Association）：単方向の論理的なコネクションでセキュリティサービスを提供するための情報の単位。
5　PF_KEY：RFC2367[177] で定義され、BSD socket API を持つアーキテクチャにおいて SA を管理するためのインターフェース。
6　ISAKMP（Internet Security Association and Key Management Protocol）：RFC2408[172] で定義されるインターネット上で SA と鍵を交換するためのフレームワーク。

トランスポートモードの IPsec 適用対象は Mobility Header（MH）の Binding Uupdate （BU）/ Binding Acknowledg（BAck）メッセージと、ICMPv6 の MPS（Mobile Prefix Solicitation）/ MPA（Mobile Prefix Advertisement）メッセージである。BU/BAck は ESP のサポートが必須（MUST）であり、使用が必須（MUST）である。また ICMPv6 の MPS/MPA は ESP のサポートが必須（MUST）であり、使用が推奨（SHOULD）である。

トンネルモードの IPsec 適用対象は Mobility Header（MH）の Home Test Init（HoTi）/Home Test（HoT）メッセージと MN のホームアドレス（HoA）を利用した通信のペイロードデータである。HoTi/HoT は ESP のサポートが必須（MUST）であり、使用が推奨（SHOULD）である。ペイロードデータは、サポートが任意（MAY）であり、使用も任意（MAY）である。

以上のようにそれぞれのメッセージに IPsec が適用されるような Security Policy（SP）と Security Association（SA）の設定が手動鍵交換、自動鍵交換共に必要である。

5.2.2 IPsec と Mobile IPv6 との連携

5.2.2.1 連携の必要性

Mobile IPv6 では、MN と HA の間で双方向トンネルを張り、MN の HoA を利用した通信はそのトンネルを経由する。先述した IPsec のトンネルモードはその双方向トンネルを代用するために使われる。MN が移動するたびに IPsec トンネルのエンドポイントアドレス（トンネルの外側のヘッダの送信元アドレスもしくは宛先アドレス）を変更させる必要があるため、更新情報を Mobile IPv6 側から IPsec 側に伝える必要がある。

また KAME 由来の IPsec スタックや Linux の IPsec スタックでは、Security Association Database（SADB）に付随して、Security Policy Database（SPD）の更新も必要である。SPD エントリは、セレクタにマッチしたパケットに適応するべき IPsec 処理（つまり該当する SA エントリ）を特定する情報をテンプレートとして保持している。このテンプレートには SA の情報（トンネルモード SA の場合、トンネルのエンドポイントアドレスを含む）を含んでいるためこれらの情報も同時に更新する必要がある。

また、K-bit とよばれる機能を実現するためには、IKE デーモンもそれらの情報を知る必要がある。K-bit は、BU/BAck に含まれるフラグの一部で、MN および HA 上で動作する IKE デーモンが、互いに張る論理的なコネクション（IKE_SA）を MN の移動にともなって維持することが可能かどうかを示すものである。K-bit のサポートによって、MN と HA 上で動作する IKE デーモンは、MN が移動し、IKE のエンドポイントアドレスが変化した場合でも既存の IKE_SA を継続して利用することが可能となる。これによって IKE のシグナリングコストが抑えられ、必要な処理時間と帯域を削減することが可能となる。

5.2.2.2 連携用 API：PF_KEY MIGRATE

前節の要求に応えるために、PF_KEYv2 の拡張である PF_KEY MIGRATE メッセージが提案されている（`draft-sugimoto-mip6-pfkey-migrate-01`）。PF_KEY MIGRATE には更新すべき SP を特定する情報（セレクタの送信元アドレス、宛先アドレス、カーネル内での SP の識別子（spid））および、更新すべき SA エントリを特定する情報（変更前のエンドポイントアドレス（送信元アドレス、宛先アドレス）アドレスカーネル内での SA の識別子（reqid））、そして新たなトンネルモード SA の情報が含まれている。

そして、Mobile IPv6 はこのメッセージを必要に応じて非同期に発行し、IPsec および IKE に移動の事実を通知する。MN は移動にともない気付けアドレス（CoA）が変化するが、それを BU の送信後 PF_KEY MIGRATE メッセージを用いることで通知する。一方、HA は、MN からの BU を受信することによって MN の CoA が変化したことを知る。HA はこのタイミングでシステムに PF_KEY MIGRATE メッセージによって MN の移動を IPsec および IKE に通知する。カーネル内の IPsec スタックはこのメッセージを受信し、処理が適切に済んだ場合、これを PF_KEY ソケットにブロードキャストする。IKE デーモンは通常 PF_KEY ソケットを常に見張っているため、そのブロードキャストされた PF_KEY MIGRATE メッセージを受信することで、MN の移動による変化を把握することが可能となる。

5.2.2.3 SHISA の PF_KEY MIGRATE への対応状況

本来 PF_KEY MIGRATE メッセージは Mobile IPv6 側のユーザランドから更新情報を IPsec 側に通知するためのしくみであるが、SHISA の場合カーネル内で Mobile IPv6 処理部が SADB や SPD の更新まで行うため、現時点では処理が適切に済んだ後に PF_KEY ソケットにブロードキャストされるだけである。ユーザランドからの通知には対応していない。

5.2.2.4 SHISA で PF_KEY MIGRATE を発行可能にするための要求事項

カーネル内の処理において、移動前の SADB/SPD のエントリを検索する場合、検索キーに移動前のアドレス（旧 CoA）を使うことは相応しくない。一度でもアドレスの変更に追従できなかった場合、それ以降エントリの検索が不可能になるためである。そのため SHISA では reqid とよばれる値をエントリの検索に利用している。reqid とは SADB のエントリを一意に示す値であり、ある SP のセレクタに適合したパケットに対し、適用する SA を明示的に指定するために使われている。つまり PF_KEY MIGRATE の発行を可能とするためには、SP の設定において IPSEC_LEVEL を UNIQUE に指定し、さらに reqid を指定すること、またそこで指定した値と同じ値を reqid として使用し SA を設定する必要がある。

5.3 IKE デーモンの SHISA 対応のための要件

IKE デーモンが SHISA 対応するために必要な機能を以下に挙げる。

- 手動鍵交換の時と同様な SA 設定
- Mobile IPv6 との連携
- interface に付く IP アドレスの動的な変更への対応
- proxy mode(∗) への対応
  （∗ IKE を動作させるアドレスとは違うアドレスの IPsec SA の確立）

5.3.1 Mobile IPv6 との連携

鍵交換デーモンは SADB/SPD の動的変更への追従が必要である。そこで PF_KEY MIGRATE などの連携 API の利用が必要である。鍵交換デーモンは SADB/SPD の値のコピーを保持していることがあるため、そのコピーをカーネル内の変化に追従させる必要がある。追従させない場合、SA の lifetime などをデーモン内で管理している場合、整合性がとれなくなる。また K-bit への対応も必要である。

5.3.2 proxy mode

BU 完了前には HoA を使用することはできない。そのため鍵交換デーモンは CoA を用いて IKE の処理を行い、HoA をパラメータとして持つ IPsec SA を確立する必要がある。IKE の処理を行う IP アドレスとは違う IP アドレスの IPsec SA を確立する際には、authorizaion 上の問題が存在する。MN(A) が、MN(A) の HoA_A ではなく MN(B) の HoA_B を設定してしまうことが無いように保障する必要がある。

5.4 関連：racoon（version1）の SHISA 対応

racoon は IKEv1 をサポートする鍵交換デーモンである。racoon では SP は setkey(8) コマンドで事前に設定する。setkey によって IPSEC_LEVEL を UNIQUE にし、reqid を指定することが可能である。また proxy mode として CoA で bind し HoA の SA を作るためには、phase2 の ID ペイロードを利用する。静的に設定ファイルである racoon.conf に指定するためには、HoA の IP アドレスと HA の IP アドレスを phase2 の ID ペイロードの値として指定する。動的に行う方式としては、PF_KEY_ACQUIRE メッセージの拡張（SADB_X_PACKET 拡張）が提案されている。SADB_X_PACKET 拡張では、BU のメッセージそのものを PF_KEY ACQUIRE メッセージに追加する。racoon はそこから BU をデコードすることで、HoA を取得し、IPsec SA の設定のために利用可能となる。racoon に存在する問題として、IKEv1 のみのサポートであること以外に、設定ファイルである racoon.conf の構造上の問題として HA が複数の MN を管理できない問題が存在する。

5.5 racoon2 の SHISA 対応の設計と実装

鍵交換アーキテクチャ racoon2 は、プロトコルごとの鍵交換デーモンとセキュリティポリシ管理デーモンと、ライブラリから構成される。iked(8) は IKEv2 をサポートする鍵交換デーモンであり、spmd(8) は SP を管理するデーモンである。libracoon.a がライブラリである。

IKEv2 による Mobile IPv6 のためのシグナリング保護に関する仕様としては既に I-D（draft-ietf-mip6-ikev2-ipsec-04）が存在する。上記 I-D および IKEv2 の仕様自体は、RFC4301（以前は rfc2401bis と呼ばれていた）を前提としている。しかし今回は、現状での IPsec 実装状況を考慮し、RFC2401 上における IKEv2 を前提にする。racoon2 の実装ステータスとしてトランスポートモードとトンネルモードの IPsec SA が設定可能と re-key が可能なった状況において、さらに SHISA 対応するために必要な要素は以下の機能であった。

- IPSEC_LEVEL 設定機能（spmd、racoon2.conf）
- reqid の指定機能（spmd、racoon2.conf）
- ルーティングソケットによる listening socket の動的更新
- PF_KEY MIGRATE 対応（libracoon.a、iked）
- TS のアドレスレンジ存在時の不具合の修正
- TS の MH/ICMPv6 対応
- 細粒度セレクタ設定
- road warrior への対応
- SA エンドポイント指定を利用した proxy mode
- proxy mode 時の authorization 問題対応
- return home 時のトンネルモード SP の自動 bypass（spmd）
- SADB_X_PACKET 拡張 ACQUIRE への対応

5.5.1 PF_KEY MIGRATE 対応についての詳細（libracoon.a、iked）

PF_KEY MIGRATE を用いて行うことが必要なのは iked が内部で保持している IKE_SA の更新と CHILD_SA の更新である。CHILD_SA に関しては reqid を用い必要なものを識別して更新を行う。spmd による SP の初期設定としては、IPsec SA のエンドポイントの値の MN 側には HoA を設定し、SPD に適用させる。その後 MN が移動し、アドレスが CoA に変わった場合、CHILD_SA 内のエンドポイントの値を MIGRATE メッセージを使って適宜 CoA に更新し続ける。また racoon2 以外から発行された MIGRATE メッセージの受信にも対応した。

5.5.2 TS のアドレスレンジ存在時の不具合修正（iked）

トンネルモードの IPsec 適用対象である HoTi/HoT およびペイロードに対しては、セレクタの指定において、src または dst に ::/0 を指定することが必要である。しかし mask ビット操作にバグが存在し、prefix 長がセレクタに指定されていた場合に動作していなかった。

5.5.3 TS の MH/ICMPv6 対応（未完了）（iked）

ICMPv6/MH における type/code 値を TS で運ぶために、type 値を TS の Start Port（2 octets）の最上位 8 bit、code 値を最下位 8 bit にすると I-D では規定されている。

5.5.4 細粒度セレクタ設定（spmd）

spmd によって MH/ICMPv6 の type/code まで含んだセレクタの設定を可能とする必要がある送信元アドレスの port に type 値、宛先アドレスの port に code 値を入れて SADB_SPDADD/SADB_SPDUPDATE を行うことで実現する。

5.5.5 road warrior 対応（iked）

road warrior とは未知の動的 IP アドレスから接続してくるクライアントのことである。road warrior からの IKE_SA_INIT リクエストメッセージに対応するために必要である。レスポンダにおいて、default 節を導入し対応を行う。IKE_SA_INIT には default 節内のパラメータを使い応答を行い、IKE_AUTH リクエストメッセージの受信後、IKE_AUTH リクエストに含まれる IDi ペイロードから相手を検索し改めてパラメータを取得し、その後の応答を行う。

5.5.6 proxy mode 時の authorization 問題への対応（iked）

設定ファイルである racoon2.conf における remote 節と policy 節内の remote_index（remote 節へのポインタ）が指すものが同一か確認を行うことである相手が他の人用の SA を設定してしまうことがないことを保障する。

5.5.7 return home 時のトンネルモード SP の自動 bypass（未完了）（spmd）

トンネルモードの SP は Linux 上での Mobile IPv6 実装である MIPL では、return home 時 PF_KEY MIGRATE によってエンドポイントのアドレスの一方が HoA となった段階でその SP を bypass としている。しかし、SHISA では return home 時、

MIGRATE が発行されず旧 CoA のままであるため racoon2 としてどう動作するのが正しいのかは検討する必要がある。

5.5.8 SADB_X_PACKET 拡張 ACQUIRE への対応（未完了）（iked）

今後、Mobile IPv6 の Dynamic Home Assigment への対応を想定した場合、SADB_X_PACKET 拡張に対する対応は必要である。また racoon2 が今後、複数 TS に対応した場合もその中の 1 つの TS の値として、HoA を racoon2 が正確に取得し使用するためにもこの拡張は必要となるはずである。

5.6 racoon2 の SHISA 対応状況

RFC2401 上での IKEv2 を利用した Mobile IPv6 のための鍵交換は動作可能となっている。IPsec SA の確立は可能であり、rekey も行える。また、Mobile IPv6 との連携機能によって MN の移動後も確立済みの IKE_SA および IPsec SA は継続して利用することが可能となっており、Mobile 環境に適応可能な IKE デーモンとしての racoon2 は実現されているといえる。しかし return home 時の挙動や、今後の Dynamic Home Assigment を想定した場合への対応が未完了である。

5.7 今後の課題

SHISA 以外に MIPL-2.0 上でも動作するか試験する必要がある。また return home 時の挙動や、今後の Dynamic Home Assigment を想定した場合への対応などを進めていく必要がある。

第 6 章　まとめと今後の課題

racoon2 の各鍵交換プロトコル部分に関しては、基本的な機能に関してはほぼ実装を終えた状態である。今後 NAT-T（IKEv2）など未実装部分に関して作業を進めていく。また、これら racoon2 を用いた利用シーンにおいてより応用的な事項について、研究および実装を行っていく予定である。