2005－QAI－14（3）
2005／1／19

限定メンバ間でのIPv6セキュア通信設定手法の提案

屏　雄一郎†　勝野　聡†　阿野　茂浩†　山崎　克之†

† 株式会社 KDDI 研究所　〒 356–8502 埼玉県上福岡市大原 2–1–15
E-mail: †{hei,katsuno,ano,yamazaki}@kddilabs.jp

あらまし　現在，次世代インターネットプロトコルとして開発された IPv6 の導入が進んでいる．IPv6 の特徴として，豊富なグローバル IP アドレスの利用により，エンドホスト間双方向通信を簡易に実現できることがある．エンドホスト間双方向通信をよりセキュアに実現する技術は幾つか存在するが，その中で IPsec はインターネット層において暗号化や認証といったセキュリティサービスを提供するものであり，特に IPv6 ではエンドホスト間でのセキュア通信路確立に有用な技術である．しかし IPsec を使用するための設定は複雑であり，このためエンドホスト間通信で簡易に IPsec を利用することが困難となっている．そこで本稿では，複数のホストでチームを構成し，同じチームに属するエンドホスト間でのみ IPsec を利用して簡易にセキュア通信路を確立することを想定し，この場合の IPsec 自動設定手法を提案する．

キーワード　IPv6，IPsec，IKE，証明書，セキュア通信，自動設定

A Proposal of Configuring IPv6 End-to-End Secure Channels for Closed Members

Yuichiro HEI†, Satoshi KATSUNO†, Shigehiro ANO†, and Katsuyuki YAMAZAKI†

† KDDI R&D Laboratories Inc.　Ohara 2–1–15, Kamifukuoka-shi, Saitama, 356-8502 Japan
E-mail: †{hei,katsuno,ano,yamazaki}@kddilabs.jp

Abstract　The deployment of IPv6 as the next generation Internet protocol has been proceeding. As one of the features of IPv6, the bi-directional communication between end hosts can be done easily by using abundant global IP addresses. The bi-directional communication between end hosts should be done securely, for which there are several technologies to realize it. Among them, IPsec is useful especially in the establishment of IPv6 end-to-end secure channels, because IPsec can provide secure services such as the encryption and the authentication at the IP layer. However, IPsec is difficult to use because 1) there are many parameters to be set up for secure channels, and 2) the configuration for IPsec is complicated. This paper proposes an automatic configuration method for setting up the end-to-end secure channels between end hosts to use IPsec easily. In our method, several end hosts form a closed team, and secure channels can be established between hosts that belong to the same team.

Key words　IPv6, IPsec, IKE, Certification, Secure Channel, Autoconfiguration

1. まえがき

現在，次世代インターネットプロトコルとして開発された IPv6 [1] のネットワークへの導入が進んでいる．IPv6 では IP アドレス枯渇対策として，128 ビット長の広大なアドレス空間を確保しているため，IPv6 ホストにグローバル IPv6 アドレスを割り当てることにより，ホストを IP アドレスで一意に識別することが容易となる．従って IPv6 環境では，通信相手の直接指定によるエンドホスト間双方向通信が実現可能であり，例えば複数の企業や大学を跨ったグリッド環境構築等での利用などが考えられるが，そこではエンドホスト間のセキュア通信路を容易に確立可能とすることが求められる．

エンドホスト間セキュア通信路は，インターネットにおける各層で確立することができる．例えば，アプリケーションで独自にデータ暗号化等を施すことにより，各エンドホストで動作するアプリケーション間でのセキュア通信を実現することも可能であり，また SSL/TLS(トランスポート層) [2] [3] や IPsec(インターネット層) [4] を利用することもできる．その中で，エンドホスト間双方向通信のためのセキュア通信路を提供する手段として，IPsec の利用が最適であると筆者らは考える．その理

由は，IPsec はピアツーピア型の通信モデルであるとともに，全ての IP アプリケーションは，自身の通信を保護するために IPsec を利用することができるからである．また，IPv6 ホストには IPsec の実装が必須となっているので，IPv6 ネットワークでは IPsec が広く利用されると考えられるからである．

しかし IPsec や，自動鍵交換プロトコルで通常 IPsec とともに利用される IKE(Internet Key Exchange) [5] は，設定に必要なパラメータが多く複雑であるため，簡単には利用できない．さらにエンドホスト間で IPsec/IKE を使用する場合は，セキュア通信を行う相手ごとに設定が必要であり，事前にアドレス情報やポリシーなどの設定情報を交換した上で手動で設定する必要があるため，一層利用が困難となる．

そこで本稿では，IPsec/IKE によるエンドホスト間セキュア通信路の自動設定手法を提案する．提案手法ではまず前提として，相互にセキュア通信を行う必要がある複数のエンドホストでチームを形成し，エンドホスト間のセキュア通信路は同じチームに所属するホスト間でのみ確立されるとする．そしてセキュア通信設定手順として，(1) オンラインチームメンバの発見，(2)IPsec/IKE 設定に関するパラメータの取得・確認，(3) セキュア通信設定準備完了を示すメッセージの送信，の三つの過程を経て，各エンドホストにおいて相手ホストに対する IPsec/IKE 設定を自動で実施する．

2. 提案手法の概要

本節では，まず本稿で提案するエンドホスト間セキュア通信自動設定手法の概要を述べる．

2.1 エンドホストのグループ化

先にも述べた通り，エンドホスト間でのセキュア通信路は，インターネットにおける各層 (アプリケーション層，トランスポート層，インターネット層) で確立することが可能である．その中で，二台のエンドホスト (を利用するユーザ) が相互に面識がない場合におけるエンドホスト間セキュア通信は，例えば SSL を利用した Web アクセスや，PGP や S/MIME 等を利用したセキュアメール送受信など，トランスポート層やアプリケーション層において実現されることが多い．

しかし二台のエンドホストが相互に面識があり，様々なアプリケーションを利用した通信が日常的に行われる場合は，IPsec を利用したインターネット層でのセキュア通信路確立が有用である．また IPsec を利用したエンドホスト間セキュア通信は，現実世界において何らかの関係により，あらかじめ面識があるユーザが利用するホスト間でのみ行われるのが自然であると筆者らは考える．

以上の観点から本稿では，相互に面識のあるエンドホスト間における，IPsec/IKE を利用したセキュア通信路確立について検討する．そこで，複数のエンドホストでチームを形成し，同じチームに属するエンドホスト間でのみ，IPsec/IKE を利用したセキュア通信路を確立することを可能とする．この場合，エンドホスト間でのセキュア通信設定の際に，自身が相手ホストと同じチームに属しているかどうかを確認する相互認証が必要となる．そこで本提案手法ではエンドホスト間の相互認証を，

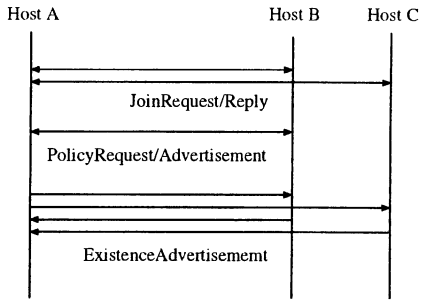

図 1 基本メッセージ手順

1) エンドホストのチーム所属証明には公開鍵証明書を利用，2) チームメンバの管理とエンドホストに対する証明書発行の役割を担うチーム／証明書管理サーバ (以下「管理サーバ」と呼ぶ) の導入，により実現する．

また，同じチームに属するエンドホストは，IPsec/IKE 設定に必要なポリシーやパラメータ (以下「IPsec/IKE ポリシー」と呼ぶ) をあらかじめ共有しておくとする．

2.2 セキュア通信路自動設定手順

図 1 に，エンドホストが，同じチームに属する他のホストに対する IPsec/IKE 設定を自動で行う際の基本メッセージ手順を示す．図 1 で，ホスト A，B，C は同じチームに属しているとする．またホスト B，C 間では既にセキュア通信路は確立しており，ホスト A は，これからネットワークに接続している同じチームに属するホストとのセキュア通信路を確立しようとする状況であるとする．

まずホスト A は，ネットワークに接続している (オンラインである) 同じチームのホストを発見するために，*JoinRequest* メッセージを送信する．なおホストは自身の証明書を管理サーバより発行してもらう際に，所属するチームのメンバリストも併せて取得しているとし，そのチームメンバリストに登録されているホストに向けて *JoinRequest* メッセージを送信する．*JoinRequest* メッセージを受信したホスト B，C は，その返答として *JoinReply* メッセージを送信する．このメッセージ交換において，互いに証明書とディジタル署名付きのメッセージを送信することにより，エンドホスト間の相互認証を実施する．

次にホスト A は，*JoinReply* メッセージの送信元ホストの中から一つを選択し，そのホストに対して，チームの IPsec/IKE ポリシーを取得するために *PolicyRequest* メッセージを送信する．*PolicyRequest* メッセージを受信したホスト (図 1 ではホスト B) は，それに対して *PolicyAdvertisement* メッセージによりチームの IPsec/IKE ポリシーを伝える．

その後ホスト A は，同チームのオンラインメンバホスト (= *JoinReply* メッセージを送信したホスト) に対して，定期的に *ExistenceAdvertisement* メッセージを送信する．ホスト A からこのメッセージを受信したホスト B，C も同様に，ホスト A に対して *ExistenceAdvertisement* メッセージを送信する．*ExistenceAdvertisement* メッセージを送受信した各エンドホス

トは，自身が保持する IPsec/IKE ポリシーに基づいて相手ホストに対する IPsec/IKE 設定を行う．つまり，同チームのエンドホスト間で *ExistenceAdvertisement* メッセージを交換することで，エンドホストは同チームの他のエンドホストとのセキュア通信を自動設定することが可能となる．

2.3 集中管理サーバの存在

提案手法では，チームメンバと証明書を発行・管理する集中管理サーバを必要とするが，IPsec/IKE ポリシーやチームメンバの存在等を管理する集中管理サーバは必要としない．従って本提案手法では，エンドホストは一度自身の証明書を取得すれば，以降は基本的に集中管理サーバに依らず，エンドホスト間でセキュア通信路を確立することが可能である．

一方，例えば SIP(Session Initiation Protocol) [6] 等のシグナリングプロトコルを利用し，SIP サーバ等の集中管理サーバを介してエンドホスト間でセキュア通信を確立する手法も考えられる [7]．しかしこの場合，集中管理サーバに障害が発生した場合はエンドホスト間でセキュア通信を確立することができなくなるので，集中管理サーバの冗長化等の対策が不可欠となり，サーバの管理コストなどが増大する．

提案手法では，エンドホスト間で交換するメッセージ量が多くなる欠点があるが，上記のように集中管理サーバがセキュア通信路確立における単一障害点となることはない，という利点がある．本稿では，(1) 集中管理サーバの簡易化，(2) エンドホストの高機能化，という観点から，集中管理サーバに依らないセキュア通信確立を目指し，後者の利点を重視する立場を取る．

2.4 適用範囲

本稿で想定するエンドホスト間セキュア通信は，例えば次のような状況での適用が考えられる．一つは，企業や大学等においてあるプロジェクトチームが形成された場合である．そこでそのチームメンバが使用するホストは，秘密情報が部外者に洩れないように，ネットワークにおいて互いにセキュアに通信する手段を確立する必要がある．また複数の企業や大学を跨ったセキュアグリッド環境構築の際にも適用可能と考えられる [8]．

別の例として，家族や友人がインターネット上で，写真やビデオクリップなどのプライベートメディアの交換や，IP 電話やチャット等による双方向コミュニケーションを楽しむ場合を想定する．この場合，交換するデータは十分なプライバシ保護がなされるべきであるので，家族や友人でチームを構成し，そのチーム内でのみセキュア通信を確立する手段が必要となる．

ネットワークに関しては，提案手法は主に IPv6 ネットワークに適用されることを想定している．すなわち，エンドホストにはグローバル IP アドレスが割り当てられており，そのため，エンドホスト間のメッセージ交換において，エンドホストは相手ホストに直接メッセージを送信することができるとする．

3. 提案手法の詳細

本節では，前節で述べた提案手法の詳細設計について述べる．

3.1 チームの生成

チームには「チームリーダ」となるホストが存在すると想定する．チームリーダは，チームを生成したホストか，または前チームリーダより権限を委譲されたホストであり，そのチームの IPsec/IKE ポリシーを決定するホストであるとする．

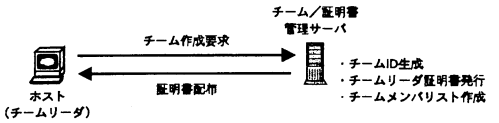

図 2 チーム生成手順

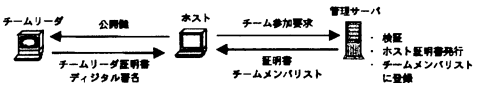

図 3 チーム参加手順

図 2 にチーム生成の手順を示す．チームを生成しようとするホストは，管理サーバに対してチームの生成を要求する．このとき，ホストは管理サーバに自身の公開鍵を提出する．管理サーバは乱数を生成し，その数を新規生成チームのチーム ID として割り当てる．そして，管理サーバはホストの公開鍵に対する証明書をチームリーダ証明書として発行し，チーム生成を要求したホストに配布する．なおチームリーダ証明書は，他のチームメンバの証明書とは区別可能な形式をとるとする．また管理サーバはチームメンバリストを作成し，そのリストにチームリーダの FQDN (Fully Qualified Domain Name) または IP アドレスを登録する．

3.2 チームへの参加

図 3 にチームへの参加手順を示す．あるチームへの参加を希望するホストは，管理サーバに対してチームへの参加を要求する．このとき，ホストは管理サーバに，(1) 自身の公開鍵，(2) 参加したいチームのチームリーダの証明書，(3) (1)，(2) に対するチームリーダによるディジタル署名，を提出する．なおホストはチームリーダの証明書とディジタル署名を，あらかじめ入手しておく必要があるとする．

管理サーバはホストから提出された証明書とディジタル署名を検証し，それが信頼できるものであれば，そのホストの証明書を発行する．そして管理サーバはそのホストをチームメンバリストに登録し，ホストに証明書とチームメンバリストを配布する．

3.3 オンラインチームメンバの発見

ホストはネットワークに接続すると，同じチームに属する他のホストとのセキュア通信路を確立するために，まずオンラインであるホストを発見する必要がある．図 4 にオンラインチームメンバの発見手順を示す．本手順において，オンラインであるチームメンバホストを発見し，発見したホストのリストをオンラインチームメンバリストとして保持する．なおホストは最初の *JoinRequest* メッセージを送出する前に，可能であれば管理サーバより最新のチームメンバリストを取得するものとする．

本手順では，各エンドホスト間で二往復のメッセージ交換を行う．最初のメッセージ交換では，ホストの資源消費等の

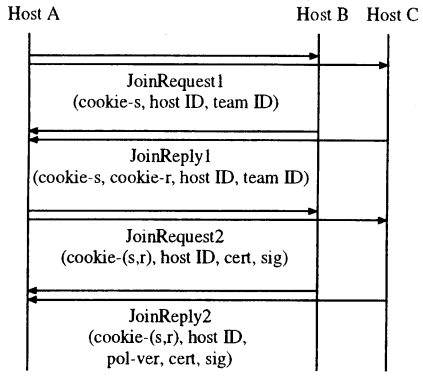

図 4　オンラインチームメンバの発見手順

DoS(Denial of Service) 攻撃防止を目的として，ランダム値であるクッキー交換のみ行う [9]．そして二回目のメッセージ交換において，ホストを相互に認証し，かつメッセージの完全性を検証するために，証明書とディジタル署名を含むメッセージを交換する．

まずホスト A は，チームメンバリストに登録されているホストに対して，*JoinRequest1* メッセージを送信する．このメッセージにはホスト A が生成したクッキー値，ホスト A のホスト ID，ホスト A が所属するチームのチーム ID が含まれるとする．*JoinRequest1* メッセージを受信したホストは，そのメッセージに含まれるチーム ID を調べ，それが自身が属するチームの ID である場合は，*JoinReply1* メッセージを返信する．*JoinReply1* メッセージには，*JoinRequest1* メッセージに含まれるクッキー値と，*JoinReply1* メッセージ受信ホストが生成したクッキー値のペアが含まれるとする．

JoinReply1 メッセージを受信したホスト A は，次に *JoinRequest2* メッセージを送信する．このメッセージには，*JoinReply1* メッセージからコピーしたクッキー情報，ホスト A の証明書，メッセージに対するディジタル署名が含まれる．*JoinRequest2* メッセージを受信したホストは，まずそのメッセージに含まれる証明書とディジタル署名を検証する．そしてそのメッセージが信頼できる場合は，受信ホストは *JoinREquest2* メッセージの送信元ホスト ID と証明書を対応付けて保持し，自身の証明書とディジタル署名を含む *JoinReply2* メッセージを返信する．また *JoinReply2* メッセージには，自身が保持する IPsec/IKE ポリシーバージョンのバージョン番号を含めるとする．ポリシーバージョン番号はポリシーの新しさを表し，番号が大きいほどより新しいポリシーであるとする．

JoinReply2 メッセージを受信したホスト A は，そのメッセージに含まれる証明書とディジタル署名を検証する．そしてそのメッセージが信頼できる場合は，ホスト A はオンラインチームメンバリストを作成し，*JoinReply2* メッセージの送信元ホストをそのリストに登録する．

3.4　ポリシー確認

オンラインであるチームメンバを発見したホストは，続いて

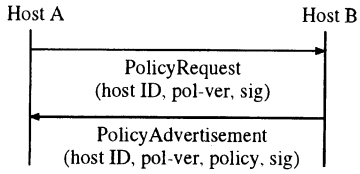

図 5　ポリシー確認手順

チームの IPsec/IKE ポリシーを取得するために，図 5 に示すポリシー確認を行う．

まずホスト A は，先に受信した *JoinReply2* メッセージから，同チームの他のオンラインメンバが持つ IPsec/IKE ポリシーのバージョンを調べる．もし自身が持つポリシーよりも新しいポリシーを持つホストが存在する場合は，ホスト A はその中で最新のポリシーを持つホストを選択し，そのホストに対して *PolicyRequest* メッセージを送信し最新のポリシーを取得する．なおホスト A が最新のポリシーを持っている場合，またはホスト A がチームリーダである場合は，図 5 に示すポリシー確認は行わないとする．

PolicyRequest メッセージを受信したホストは，*PolicyAdvertisement* メッセージにより自身が保持する IPsec/IKE ポリシーを返答する．なおこのメッセージは，*PolicyRequest* メッセージ送信元ホストの公開鍵で暗号化されて送信されるとする．

IPsec/IKE ポリシーとして，例えば以下のパラメータを含むとする．

（1） IPsec ポリシー

- セキュリティプロトコル (AH [10] または ESP [11])
- カプセル化モード (トランスポート または トンネル)
- プロトコル ID
- ポート番号

（2） IKE ポリシー

- フェーズ 1 での交換モード
- フェーズ 1 で使用する Diffie-Hellman グループ
- ISAKMP SA で使用する暗号化アルゴリズム
- ISAKMP SA で使用するハッシュアルゴリズム
- ISAKMP SA の生存時間
- IPsec SA で使用する暗号化アルゴリズム
- IPsec SA で使用する認証アルゴリズム
- IPsec SA の生存時間

3.5　存在広告

ポリシー確認手順完了後，ホストはオンラインチームメンバリストに登録したホストに対して，定期的に *ExistenceAdvertisement* メッセージを送信する．このメッセージは，メッセージ送信元はオンラインであることを示す一種の keep alive メッセージであり，メッセージにはホスト ID，IPsec/IKE ポリシーバージョン番号，ディジタル署名が含まれるとする．

ExistenceAdvertisement メッセージを受信したホストは，まずディジタル署名を検証し，それが信頼できる場合は，ホストはその送信元ホストに関する情報 (IP アドレス，ポリシーバー

ジョン番号等) をホスト ID に対応付けて保持する．ホストがあるホストから初めて *ExistenceAdvertisement* メッセージを受信し，かつそのホストが自身が持つオンラインチームメンバリストに登録されていない場合は，その *ExistenceAdvertisement* メッセージの送信元ホストをオンラインチームメンバリストに登録し，そのホストに対して定期的なメッセージとは別に，ただちに *ExistenceAdvertisement* メッセージを送信する．

あるホストから初めて *ExistenceAdvertisement* メッセージを受信し，かつそのポリシーバージョン番号が自身のものと同じ場合は，ホストは IPsec/IKE ポリシーを参照して，*ExistenceAdvertisement* メッセージの送信元ホストに対する IPsec/IKE 設定を実行する．

ホストが受信した *ExistenceAdvertisement* メッセージに含まれるポリシーバージョン番号が，自身が保持する番号よりも大きい場合，ホストはそのメッセージの送信元に対して図 5 に示すポリシー確認を行い，最新のポリシーを取得する．

ホストは，一定期間あるホストから *ExistenceAdvertisement* メッセージを受信しなかった場合は，そのホストに対する IPsec/IKE 設定を削除するとともに，オンラインチームメンバリストからそのホストを削除する．

3.6 離脱広告

ホストが同チームの他のホストとのセキュア通信路を解除する場合，ホストは *LeaveAdvertisement* メッセージを送信する．このメッセージには，ホスト ID とディジタル署名が含まれるとする．またこの時ホストは，IPsec/IKE ポリシー，ポリシーバージョン番号，チームメンバリストは保持するが，オンラインチームメンバリストは保持しないとする．

LeaveAdvertisement メッセージを受信したホストはそのメッセージを検証し，それが信頼できる場合は，そのメッセージの送信元ホストに対する IPsec/IKE 設定を削除する．

3.7 ポリシー変更

あるチームの IPsec/IKE ポリシーは，チームリーダのみ変更することができるとする．チームリーダはポリシーを変更する場合，自身が保持するオンラインチームメンバリストに登録されているホストに対して，*PolicyChange* メッセージを送信する．*PolicyChange* メッセージは新しい IPsec/IKE ポリシー，そのバージョン番号，チームリーダ証明書，ディジタル署名を含む．またこのメッセージは，送信相手ホストの公開鍵で暗号化されて送信されるとする．

PolicyChange メッセージを受信したホストはそのメッセージを検証し，それが確かにチームリーダより送信されていると確認できた場合のみ，そのメッセージに含まれる新しい IPsec/IKE ポリシーを受け入れ，バージョン番号とともに保持する．なお新ポリシーは次の IPsec/IKE 設定から適用されるとし，既に設定・確立している IPsec/IKE に対して変更は行わない．

4. スケーラビリティに関する考察

4.1 メッセージ交換

本提案手法では，チームメンバホスト間でのメッセージ交換は全てユニキャストで行うことを想定している．この手法の問題点として，チーム数やチームメンバ数が増えるにつれて，交換されるメッセージ量が増大することがある．例えばあるチームにおけるメッセージ量は，全てのメンバがオンラインであった場合チームメンバ数の二乗のオーダーで増加する．

上記の問題を緩和する方法として，一つのチームに属することが可能なメンバ数に上限を設けることが考えられる．筆者らが想定する提案手法の適用範囲においては，例えば企業内のプロジェクトチームや家族・友人など，一つのチームのメンバ数はそれほど多くないと考えられるので (最大で数十程度)，チームメンバ数に関しては大きな問題とならないと考えている．

別の方法として，メッセージ交換でマルチキャストを利用することが考えられる．例えば，チームに対してマルチキャスト・アドレスを割り当て，ホストは *JoinRequest1* や *ExistenceAdvertisement* といったメッセージを，チームのマルチキャストアドレス宛てに送信する．マルチキャストの使用により，エンドホストにおけるメッセージの送出回数やメッセージ量を削減することが可能であり，またエンドホストはチームメンバリスト／オンラインチームメンバリストを保持する必要がなくなる．

しかし現状でのマルチキャストネットワークの導入状況を考えると，マルチキャストの利用は困難である．例えば企業 LAN のようなローカルなネットワークでは，マルチキャストの利用は可能である場合もある．しかしインターネットにおける AS 間のマルチキャストは，IPv4/IPv6 とも mbone 等の実験目的での導入事例はあるが，商用 ISP での導入事例はほとんどないので，インターネットでのマルチキャスト利用は事実上不可能であると言える．

4.2 ホストに設定する SPD/SAD エントリ数と通信性能

IPsec を利用するホストは，送受信されるパケットのセキュリティポリシーを登録した SPD (Security Policy Database) と，IPsec におけるセキュア通信路を表す SA(Security Association) の情報を格納した SAD(Security Association Database) の二つのデータベースを持つ．各エンドホストで IPsec/IKE 設定を行う場合，ホストに設定される SPD/SAD のエントリ数が多くなると，データベース検索時間の増加等によりホストの通信性能に影響が出ることが考えられる．そこでホストに設定する SPD/SAD エントリ数を変化させた場合の通信性能として，IPv6 ネットワークにおける TCP スループットとホスト間 RTT(Round Trip Time) を測定した．

図 6 に実験ネットワーク構成を示す．ホストは CPU 速度 1.2GHz，メモリ 256MB，OS は Linux(Fedora Core 2，カーネル 2.6.5) を搭載したノート PC で，ネットワーク速度は 100Mbit/s(First Ethernet) である．ホストが持つ SPD/SAD は，KAME [12] の IPsec ツールの Linux 移植版である IPsec-

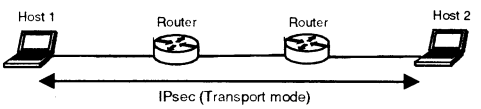

図 6 実験ネットワーク

SPD/SAD ペア数	0	1	10	100	1000	3000
スループット (Mbit/s)	92.7	42.8	42.9	43.2	42.8	43.0

表 1 SPD/SAD ペア数に対する TCP スループット

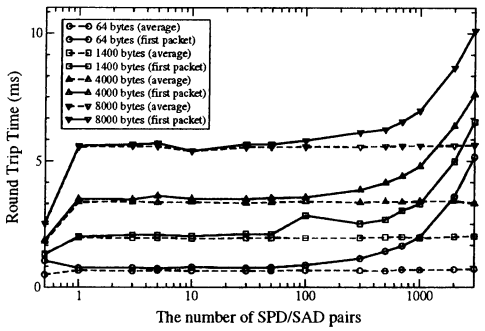

図 7 SPD/SAD ペア数に対する RTT

Tools [13] の *setkey* コマンドを使用して設定した．ホスト間の IPsec 通信は ESP のトランスポートモードにより行い，暗号化アルゴリズムは AES(鍵長 128 ビット)，認証アルゴリズムは HMAC-SHA1 を使用した．なお図 6 のホスト 1-ホスト 2 間の IPsec においてホスト 1 に設定される SPD は，ホスト 1 からホスト 2 に向かうパケットに一致するエントリと，ホスト 2 からホスト 1 に向かうパケットに一致するエントリの二つのエントリを持つ．またホスト 1 に設定される SAD も，ホスト 1 →ホスト 2 の SA とホスト 2 →ホスト 1 の SA を表す二つのエントリを持つ．従って以降は上記二つのエントリを合わせて「SPD/SAD ペア」と表記する．

表 1 に TCP スループットの測定結果を示す．測定には TCP/UDP 帯域測定ツール Iperf [14] を使用した．ホストのウィンドウサイズは 64Kbytes とし，各 SPD/SAD ペア数に対して 1 回 60 秒間の測定を 3 回行い，その平均値をスループット測定結果とした．なお SPD/SAD ペア数 0 は，IPsec を使用しない場合の結果を意味する．また SPD/SAD ペアが 1 より大きい場合は，ホスト 1，ホスト 2 にダミーの SPD/SAD エントリを設定している．表 1 より，エンドホストが持つ SPD/SAD のエントリ数は，エンドホスト間の TCP スループットにはほとんど影響を与えないことが分かる．

図 7 に，ホスト 1-ホスト 2 間の RTT 測定結果を示す．測定は *ping6* コマンドを使用して行った．ICMPv6 パケットサイズを 64，1400，4000，8000 バイトとし，各測定においてパケットを 1 秒おきに 100 回送出した場合の，最初のパケットの RTT と 100 回平均の RTT を計測した．なお図 7 の一番左のプロットは，IPsec を使用しない場合の結果を示している．

この結果，100 回平均の RTT は SPD/SAD ペア数に関係なくほぼ一定であるが，最初のパケットの RTT は，全ての場合において 100 回平均の RTT よりも大きくなっており，SPD/SAD ペア数が 100 を越えたところから，その差は SPD/SAD ペア数の増加に従って大きくなることが分かった．最初のパケットの RTT が大きくなる要因として，1) IPv6 での近隣探索 [15] による MAC アドレス解決時間，2) SPD/SAD エントリの検索時間，などが考えられる．SPD/SAD ペア数が少ない場合の RTT 増加は 1) による要因が大きく，SPD/SAD ペア数が増加するにつれて，2) の要因が RTT 増加に大きく効いてくると考えられる．ただし平均値は SPD/SAD ペア数に関係なくほぼ一定であることから，本実験で使用した OS には，二回目以降の SPD/SAD 検索を高速に実行できるように何らかのキャッシュ機構が実装されていると考えられる．

以上の性能評価により，本稿で想定する状況においては，一台のホストが持つ SPD/SAD ペア数は高々数十程度であると考えられるので，SPD/SAD ペア数の増加によるホストの通信性能の低下は大きな問題とはならない．

5. むすび

本稿では主に IPv6 ネットワークでの適用を目的として，同じチームに属するホスト間での IPsec/IKE を利用したセキュア通信路の自動設定手法を提案した．提案手法では，集中管理サーバに依らずエンドホスト間でセキュア通信路を確立するので，集中管理サーバの障害によるセキュア通信路確立の失敗は発生しない．また，本提案で想定する適用範囲においては，一台のホストが持つ SPD(Security Policy Database)/SAD(Security Association Database) エントリ数は高々数十と考えられるが，その範囲においては IPsec 設定による通信性能の低下は大きな問題とならないことを示した．今後は提案手法の実装と実ネットワークでの利用・評価を行う．

文　献

[1] S.Deering and R.Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Dec. 1998.

[2] A.Freier, P.Karlton and P.Kocher, "The SSL Protocol Version 3.0", http://wp.netscape.com/eng/ssl3/draft302.txt, Nov. 1996.

[3] T.Dierks and C.Allen, "The TLS Protocol Version 1.0", RFC 2246, Jan. 1999.

[4] S.Kent and R.Atkinson, "Security Architecture for the Internet Protocol", RFC 2406, Nov. 1998.

[5] D.Harkins and D.Carrel, "The Internet Key Exchange (IKE)", RFC 2409, Nov. 1998.

[6] J.Rosenberg, et al., "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[7] 小野，立元，平松，"SIP シグナリングを利用した End-to-End セキュア通信"，信学技報，NS2002-250，2003 年 3 月．

[8] 史，武田，長谷川，伊達，水野，下條，"IPv6 によるスケーラビリティに優れたセキュアグリッド環境の構築"，情処学研報，2003-HPC-94，2003 年 6 月．

[9] P.Karn, W.Simpson, "Photuris: Session-Key Management Protocol", RFC 2522, March 1999.

[10] S.Kent and R.Atkinson, "IP Authentication Header", RFC 2402, Nov. 1998.

[11] S.Kent and R.Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, Nov. 1998.

[12] http://www.kame.net

[13] http://ipsec-tools.sourceforge.net

[14] http://dast.nlanr.net/projects/Iperf/

[15] T.Narten, E.Nordmark and W.Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, Dec. 1998.