6D-1

エンドツーエンド IPSec 通信の実現を容易にする IKE 認証機構拡張

平 河 内　竜 樹†

現在の IPSec はエンドシステム間通信への適用が困難である．その理由の一つとして，現行 の IKE 仕様は相互認証を前提としていることが挙げられる．認証面からの適用困難性は認証方式の動的選択機構を取り入れることで改善されると推察される．本論文では上記を実現するための手法として認証リストの導入を提案する．

1. 背　　景

IPSec は主に暗号化及び完全性検証の機能を提供し，IP 通信に安全性を付与するものである．現在 IPSec は Tunnling 機能を併用して VPN を構築するために利用されるケースが多く, 拠点間を接続する Internet-VPN においては中核を成す技術として活用されている．しかしその反面，エンドシステム間通信のセキュリティを確保する技術としてはあまり使用されていない．IPSec は IP 通信であればアプリケーションに依存することなく安全性を高めることができるため，実用性が伴えばエンドシステム間通信においても価値の高い技術である．本論文では，IPSec の，エンドシステム間通信への適用容易性を高めるアプローチについて述べる．

2. 従来技術の問題点

IPSec の主な機能である暗号化や完全性検証を適切に実施するためには，使用するアルゴリズム等の同期や鍵設定，相手認証が必要となる．IPSec は IKE を利用してこれらの作業を自動化しているが，認証情報など，IKE の折衝で交換される情報の一部は手動で用意・設定する必要がある．IPSec を VPN で使用する場合，専用の設定が必要なノード数は配置するゲートウェイの数に限定される．また，配置される機器は自ドメインの管理下に置かれるため，同期した設定の投入も容易である．しかし，IPSec をエンドシステム間通信へと適用した場合，IPSec 対象通信の定義や使用するアルゴリズム等の設定作業が端末単位で必要となり使用者・管理者に大きな負担を強いることになる．加えてドメインを跨ぐ Internet 通信に適用した場合，管理外機器との通信になるため，互いの設定が都合良く一致しないケースが予想される．同様の理由で認証方式に共通鍵ベースのものを使用することも困難となる．

幅広く普及している Internet 上のセキュリティ技術として SSL が挙げられる．SSL の主な機能はアプリケーションメッセージ部の暗号化と完全性検証で IPSec と類似している．しかし，エンドシステム間通信での使用頻度という点からは SSL が優位である．その理由として次の項目が挙げられる．

- **多くのブラウザにおいて標準でサポートされている**
  - クライアントプログラムのセットアップ工数
- **URL のスキーム指定により折衝を始動できる**
  - 対象通信の指定：一般的な HTTPS の場合
- **認証に証明書を利用する**
  - 送信元の信頼性
- **クライアントの認証がオプションである**
  - クライアントの設定容易性

この中で認証機構という観点から IPSec と決定的に異なる事実は「クライアントの認証を必須としない」ことであり，特にこの相違点が IPSec のエンドシステム間通信を困難にするものと推察される（認証に起因する適用困難性）．よって IPSec の適用困難性は，工数面（専用リソースの配置や設定の実施など）だけでなく，クライアント・サーバ通信に適合し難い相互認証を前提としている点にも大きな原因があると言える．

Version 2 となった IKE では EAP がサポートされ，また提案パラメータのリスト化や認証方式の非対称性が許可された．しかし，相互認証が前提となっている点は不変である．相互認証を維持したまま不特定多数との IPSec 通信を実現する「便宜的暗号化☆」も RFC として存在するが，公開鍵を登録・配布する DNS が必要となり導入時の大きな障壁となる．

相互認証の前提を取り払うことを考えた場合，単純に Initiator の認証を無効とするだけでは「双方向認証」や「多重認証☆☆」が要求されるケースに対応できない．利用形態やアクセスする情報の機密度などによって要求される認証強度が異なる以上，認証機構に変更を加えるのであれば，要件に応じて認証の方向や方式を動的に選択できる機能が必要となる．

エンドシステム間の IPSec 通信では IPSec 対象通信（Security Policy）の定義や使用するアルゴリズム等（SA Parameter）の設定作業及び設定の有効化も導入を困難にする要因として挙げられるが，本論文では認証に起因する適用困難性に絞って述べる．工数面の問題に対するアプローチは別の論文☆☆☆にて言及する．

3. 本論文のアプローチ

認証に起因する適用困難性への包括的な解決策として，本論文では認証リストの導入を提案する．これは柔軟な認証ポリシーの表現を目的としており，具体的には各認証方式への対応状態を定義した Authentication Policy （図１）と相手に応じてポリシーを選択するための Authentication Information Base （図２）から成る．また，認証リストは「認証される」場合（Done）と「認証する」場合（Doing）とで別個のものを用意する．

Authentication Policy【Done】は相手に対応状況を通知するためのポリシーで Status には Enable（有効） / Disable（無効）を設定する．Authentication Policy【Doing】は認証する相手に要求するポリシーで Status には Required（必要） / Optional（任意） / Disable（無効）を設定する．Authentication Information Base はピアを特定する ID からポリシーを索引するためのもので，ID 情報に対してポリシー番号を関連付ける．

† 無所属

☆ RFC 4322：Opportunistic Encryption using the Internet Key Exchange (IKE)

☆☆ RFC 4739：Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol

☆☆☆ エンドツーエンド通信用 IKE/IPSec ポリシーを配布・検索する DHCP と DNS の拡張（FIT2006：平河内竜樹）

Basic Authentication Policy
【Done】<Number 21>

ID	(Method)	Status
01	RSA-Sign	Enable
02	PSK	Disable
03	DSS-Sign	Disable

Basic Authentication Policy
【Doing】<Number 22>

ID	(Method)	Status
01	RSA-Sign	Optional
02	PSK	Disable
03	DSS-Sign	Disable

Extended Authentication Policy
【Done】<Number 21>

ID	(Method)	Status
00	Generic	Enable
01	Identity	Disable
02	Notification	Disable
03	Nak	Disable
04	MD5-Challenge	Disable
05	OTP	Disable
06	GTC	Disable

Extended Authentication Policy
【Doing】<Number 22>

ID	(Method)	Status
00	Generic	Required
01	Identity	Disable
02	Notification	Disable
03	Nak	Disable
04	MD5-Challenge	Disable
05	OTP	Disable
06	GTC	Disable

図 1 Authentication Policy の記述例

Authentication Information Base
【Done】<ID - IPv4>

Remote Host	Policy Number
10.1.1.2 /32	21
default	10

Authentication Information Base
【Doing】<ID - IPv4>

Remote Host	Policy Number
10.1.1.2 /32	22
default	10

図 2 Authentication Information Base の記述例

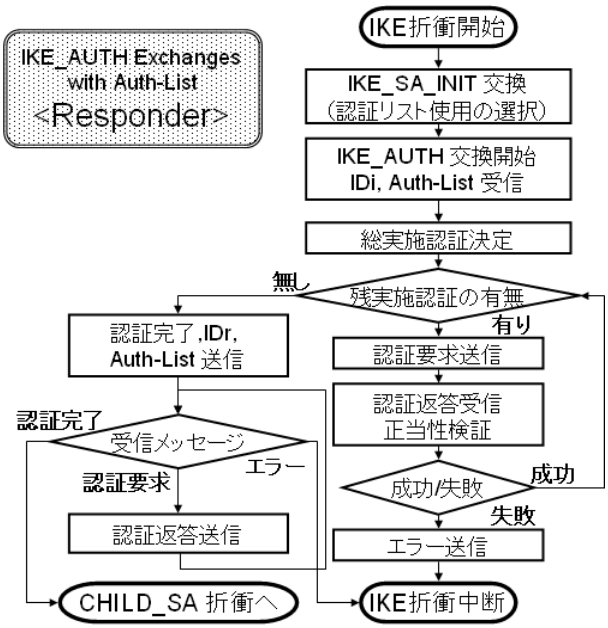

図 4 認証リストを用いた IKE_AUTH 交換：Responder

認証リストを用いた IKE_AUTH 交換は図 3，図 4 のようになる．認証実施側は受信した ID からピアを認証するためのポリシーを検索し，受け取ったポリシーと照合することで実際の認証動作を決定・実施する．この操作を Initiator/Responder 双方で行った後，CHILD_SA の折衝に移行する．

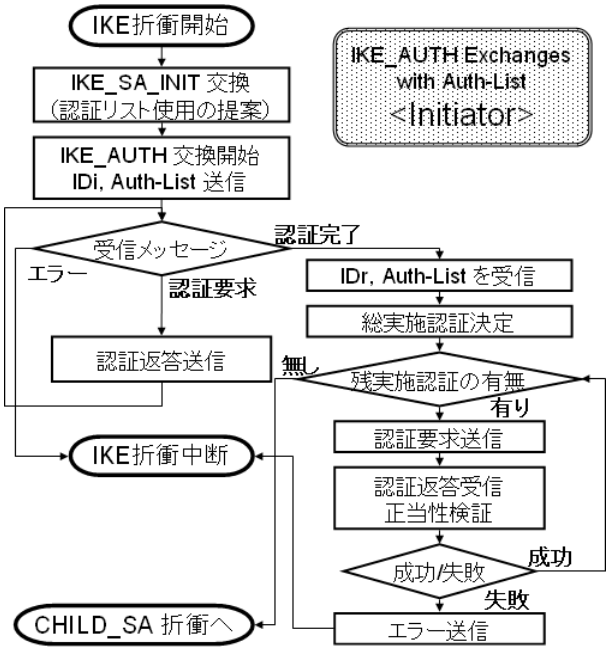

図 3 認証リストを用いた IKE_AUTH 交換：Initiator

4. 認証リストの適用例

4.1 エンドシステム間 Client/Server 通信

Initiator となるクライアントは Authentication Policy【Done】の Status を全て Disable に設定する．これはクライアントが自らの正当性を示すものを提示しないことを意味する．この場合 Authentication Policy【Doing】に Required の項目が無いサーバに限り，SA を確立し安全性の高い通信を行うことができる．サーバの運用ポリシーとして「クライアントの認証を必須としない」ケースで有効である．

4.2 リモートアクセス VPN

Responder となる VPN サーバは Authentication Policy【Doing】の RSA-Sign と OTP の Status を Required に設定する．また，VPN クライアントの【Doing】においても RSA-Sign を Required に設定する．この場合クライアントは証明書とワンタイムパスワードの二重認証を通過する必要があり，サーバの正当性も証明書によって検証することができる．上記のようなポリシーの設定により，強固な認証システムを採用するケースにも対応可能である．

5. 考　　察

認証方式を選択・多重化できる場合，通過した認証の種類や数に応じて，リモートホストのアクセスを制御することが考えられる（認可への応用）．例えば認可レベルに差を設けたアドレスの割り当てが挙げられる．認証の結果に応じたアドレスを配布することでアドレスに基づいたアクセス制御が容易となる．マルチプレフィックス環境では，サービス毎にアドレスを用意することで，適用の幅が広がる可能性も考えられる．

Authentication Policy Status における Optional の存在は認可レベルに差異を付けることを想定している．認可レベルに許可もしくは拒否の選択肢しかない場合は Optional を設定してもセキュリティレベルの向上には寄与できない．

6. ま と め

本論文では IPSec のエンドシステム間エンドーツーエンド通信への適用を容易にする手段として認証リストの導入を提案した．認証リストを利用することにより，一元的にセキュリティレベルを落とすことなく片方向認証を利用できる．また，相手に応じて認証方式を柔軟に選択することが可能になる．

参 考 文 献

1) RFC : 4306 - Internet Key Exchange (IKEv2) Protocol, 4478 - Repeated Authentication in Internet Key Exchange (IKEv2) Protocol, 4718 - IKEv2 Clarifications and Implementation Guidelines, 4739 - Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol 他
2) Internet-Draft : draft-ietf-btns-core, draft-ietf-btns-prob-and-applic 他
3) マスタリング IPsec 初版/第二版 (O'reilly Japan)