L-047

Security Policy Advertisement と IPsec VPN Convergence を実現する IKE Negotiation 拡張

平 河 内　竜 樹†

現行の IKE 仕様は SPD の維持・管理を管轄外としている．本論文ではより拡張性の高い IPsec VPN の構築を実現するため IKE を利用して Security Policy を広告することを提案し，その実現方法と利点について言及する．

1. 背　　景

IPsec は，主に機密性及び完全性を確保する機能を提供し，IP 通信を保護するものである．IPsec を使用することによって，利用者は Public Network 上で安全な IP 通信を行うことができる．また，Tunneling 機能を有効化もしくは併用することにより，VPN を実現することが可能となる．Internet が中継網として利用可能になったことによって安価な拠点接続が実現され，IPsec を中核技術とした Internet VPN は年を重ねる毎に利用が拡大している．IPsec は，Internet VPN の構築や WAN のセキュリティ強化等を主な用途として，今後も活用されることが期待される．本論文では，Security Policy Database（以下，SPD）Entry の自動生成という観点から，IPsec VPN の拡張性と柔軟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 を有効にする際は，処理対象やトンネル終端アドレス（Local Tunnel Address, Remote Tunnel Address）等を定義するために，Security Policy を設定する必要がある☆．Security Policy のうち処理対象を指定する Traffic Selector の種類には，IP アドレス（Local Address, Remote Address）・次レイヤプロトコル・ポート番号等が定められている．しかし，IPsec VPN 構築の実際においては，IP アドレスのみを利用する方法が主流である．この方法では IPsec 処理対象となる IP アドレスのリストを用意し，トラフィック転送時にパケットの IP アドレスと照合することで処理対象の識別を実現している．

Traffic Selector や Tunnel Address の指定に対し静的に値を設定する場合，以下のような問題が発生する．

- **アドレッシングの変更やセグメントの追加に伴い設定を更新する必要がある**
  - Traffic Selector：Local Address 更新への対応
- **Security Gateway の追加に伴い他の Security Gateway の設定を更新する必要がある**
  - Traffic Selector：Remote Address 更新への対応
  - Remote Tunnel Address 更新への対応

上記の問題は IPsec VPN のアドレッシング変更や拠点追加を困難にしてしまう．この問題に対する解決策として，実装上，Security Policy の設定を簡素化・自動化するアプローチが活用されている．具体的には Traffic Selector に全ての値を表す ANY を利用する方法，Tunneling 処理を IPsec 処理の前段に実行し Traffic Selector の値を Tunnel Address と一致させる方法，IPsec 処理を Interface として捉え処理を Routing で制御する方法，CHILD_SA 確立の過程で交換した Traffic Selector と Tunnel Address を元にその Peer 向けの SPD Entry を生成する方法，Dynamic DNS や NHRP を利用し Tunnel Address に対して登録と解決の機構を適用する方法等が挙げられる．これらは組み合わせて活用されるケースも多く，特に Routing で制御するアプローチは Traffic Selector を Routing Information へ間接的に代替・統合することが可能であり，Dynamic Routing Protocol を併用することによって拠点追加への対応も容易となる．

しかし Routing Protocol の活用は処理負荷の増加という側面において無視できない要素となる．特に大規模ネットワークに適用した際は IKE/IPsec よりむしろ Routing Protocol の負荷が規模の限界を狭める要因になり得る．また IKE/CHILD_SA の生存確認として DPD☆☆ の実行を考慮した場合，同一の Path 上で Routing Protocol Neighbor と SA の二階層で Keepalive を実行することになり，Path 上の障害検知という点において無駄が生じている．

加えて，IPsec 処理の制御を通常の Routing のみに依存する場合，宛先アドレス以外の情報に基づいて処理を分類することができない．この場合 Traffic Selector の値として主眼に置かれることは経路情報に対して矛盾が無いか否かであり，宛先アドレス以外の情報に基づいたアクセス制御は困難となる．

3. 本論文のアプローチ

3.1 IKE を通じて Security Policy の Advertisement を実施し SPD Entry の生成を自動化

本論文では，IPsec VPN を形成する各 Security Gateway に対して，Traffic Selector と Tunnel Address の広告・学習能力付与を目的とした IKE の拡張を提案する．本提案によって SPD を動的に構築することが可能となり，LAN Prefix や WAN アドレスの追加・変更・削除を検知し，SPD を自動で更新する IPsec VPN が実現される．

基本指針を次に示す．最初に，事前に必要なアドレス情報として，各 Security Gateway に配下の保護対象ノード群を示す Traffic Selector：Local Address と Peer とのトンネルを終端する Local Tunnel Address を設定する．次いで，IKE Peer を示すアドレスを手動で指定し，IKE_SA を確立する☆☆☆．IKE_SA 確立後より本提案の拡張 Negotiation へ移行し，CHILD_SA

† Net One Systems Co., Ltd.

☆ 本論文中では Action における BYPASS 及び Transport Mode の適用は考慮しないものとする．

☆☆ RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers

☆☆☆ SA の確立に際し，不整合の無い SA パラメータ・認証情報設定が条件となる．以降，これらの条件は満たしていることを前提とする．

確立のための Payload 交換の前に，事前に設定した Local の情報を新規 Payload を使用して互いに広告する．そして学習した Peer の Traffic Selector と Tunnel Address を Local の情報と関連付け，Entry として SPD に登録する．このフェーズによって IKE Peer との IPsec 通信に必要な SPD Entry を自動で追加することができる．さらに，広告対象の情報として既に学習した Remote の情報を追加することによって，SPD を複数の Security Gateway 間で同期することが可能となる．

上記の動作によって Security Policy の手動設定が省略される．IKE Initiation Trigger を Security Policy に依存する場合も，IKE_SA を確立するための SPD Entry を一つ作成するだけで良い．IKE_SA さえ確立することができれば，その時点の SPD が意図する IPsec 通信に対して不十分なものであっても，必要な Entry が自動で追加される．また Security Gateway が追加された場合，直接 SA を確立されなかった Gateway に関しても，他の Gateway から新規 Gateway の情報を更新情報として学習することによって接続に必要な SPD Entry が自動で生成される．結果，メッシュトポロジの SA を動的に確立することが可能となる．

複数のプロトコルを併用し類似した結果を得られる技術は既に存在する．また本提案では，広告・学習機構を組み込むことによって，IKE 単体の処理負荷は増大することが予想される．しかし，各々が指定した Traffic Selector を元に SPD を構築するため柔軟なアクセス制御が可能である点，Security Gateway 間の接続に関する制御を IKE へ統合することにより IPsec VPN のセッション管理における総合的なオーバーヘッドの削減や機能の有効化に必要な設定の簡素化を期待できる点は近年の技術と比較した場合においても優位であると推察される．

本提案を実現するための具体的な拡張を次項より示す．本論文中では実際の IPsec VPN において最も一般的な構成である Hub and Spoke☆トポロジへ適用することを前提として述べる．また，対象とする Traffic Selector の種類は Local Address, Remote Address のみとする．構成要素としては 単一の Hub と Hub に対して直接 SA を確立する Spoke だけを想定し，階層化トポロジへの対応や Security Gateway の冗長化等は考慮に入れないものとする．

3.2 Security Policy Advertisement に必要な Negotiation と Database

Negotiation Type	IKE Exchange Type
SA Establishing	IKE SA INIT, IKE AUTH CREATE CHILD SA
SA Rekeying	CREATE CHILD SA
SA Deleting	INFORMATIONAL
Keepalive	INFORMATIONAL
Configuration	INFORMATIONAL
Error Notification	INFORMATIONAL
Status Notification	INFORMATIONAL
SP Mode Notification	新たに提案
SP Update	新たに提案

表 1 既存と新規提案の Negotiation

Advertisement Mode	Description
Server	全ての情報を広告・学習
Client_Active	広告に制限，学習は全て
Client_Passive	広告と学習に制限

表 2 各 Security Gateway に設定される Advertisement Mode

本提案を実現するために必要な拡張 Negotiation（Security Policy Advertisement，以下 SPA）を表 1 における「新たに提案」の項として示す．それに伴い必要となる広告者としての様態を Advertisement Mode として表 2 に示す．また，Negotiation の詳細となる Message Type，IKE Payload☆☆ をそれぞれ表 3, 4 に示す．

Negotiation Type	Message Type	Description
SP Mode Notification	SPMOD	広告モード通知
SP Mode Notification	SPMOD_OK	Peer のモード許可
SP Mode Notification	SPMOD_NG	Peer のモード拒否
SP Update	SPREQ_ALL	要求：全て
SP Update	SPREQ_PEER	要求：Peer の Local のみ
SP Update	SP_RENEW	更新：新規追加
SP Update	SP_ADD	更新：Selector 追加
SP Update	SP_CLEAR	更新：全消去
SP Update	SP_DELETE	更新：Selector 削除
SP Update	SP_ACK	確認応答
SP Update	SP_ERROR	エラー通知

表 3 新規 Negotiation の内訳となる Message Type

Message Type	Payload
SPMOD	SPMOD（新たに提案）
SPMOD_OK	N (Notify)
SPMOD_NG	N (Notify)
SPREQ_ALL	SPREQ （新たに提案）
SPREQ_PEER	SPREQ （新たに提案）
SP_RENEW	SP （新たに提案）
SP_ADD	SP （新たに提案）
SP_CLEAR	SP （新たに提案）
SP_DELETE	SP （新たに提案）
SP_ACK	N (Notify)
SP_ERROR	N (Notify)

表 4 各 Message で使用する Payload

Advertisement Mode（以下，Mode）は広告に関する役割を取り決める．Hub and Spoke トポロジの VPN 構築において，Remote 情報の広告能力を要求される Security Gateway は各 Spoke を収容する Hub のみである．Spoke は Traffic Selector：Local Address と Local Tunnel Address を Hub のみに対して通知するだけでよく，不要な広告能力を持たせることは管理・処理負荷の面から望ましくない．Local に加え Remote の情報も広告するものを Server, Local の情報のみ広告するものを Client と位置付け，Mode とする．また，Spoke 間 SA の有無が分かれる場合等を考慮し，Client の Mode は学習能力の観点からさらに二種へ分類する．Peer の Local, Remote の両情報を学習するものを Client_Active, Peer の Local 情報のみ学習するものを Client_Passive とする．

また，広告・学習能力とは別の観点で IKE AS 番号を定義し同時に通知するものとする．この情報は，広告領域を分割するケースや Tunnel Address に対して Traffic Selector を多重化するケースの，識別子としての役割を想定し定義している．

IKE AS 番号は任意の値を，Mode は自ノードの振る舞いを定めるもの（Local）と Peer として受け入れ可能なもの（Allowed）との二種についてそれぞれ定められた値を設定し，専用の Payload を利用して SPA の最初で互いに通知する．この時 IKE AS 番号が一致しない，もしくは許可しない Mode を提示された場合は NG を返答し，該当する IKE AS の SPA を中断する．IKE AS が複数存在する場合はそれぞれ確認を行い成否を決定する．この Negotiation を SP Mode Notification とする．

☆ 本論文中では Center Site とそれに接続する Branch Site を構成要素とする CPE based VPN を指し，Tunnel はメッシュ状になるケースも想定するものとする．

☆☆ 新規提案の Payload に関して，本論文中では詳細な Message Format の定義を割愛する．

次いで，SP Update について述べる．SPD Entry の基となる Update 情報は次のタイミングで送信される．

- **専用の Request に応じて Update を返答する**
  - Trigger ： 外部からの要求
- **SAD や SPD の更新を検知して Update を発信する**
  - Trigger ： 内部情報の変化検知

要求による Update は，SP Mode Notification 直後に実行される．SP Mode Negotiation によって互いの Mode を把握した後，必要な Request Message（SPREQ）を送信しその返答として SPD Entry の基となる Update 情報（SP）を得る．Update を返答する側は Mode として許可しない SPREQ を受信した場合，エラーを返答し SP を送信しないものとする（表５）．

SP Mode Notification 後，SPREQ に対する SP 受信以外の理由で SPD 更新が発生しそれを通知する必要が生じた場合は，事前に SPREQ を交換することなく SP を発信する．受信側は，SPREQ に対する SP 受信時と同様，Update 情報を基に SPD を更新する．また Mode として許可されない Update を受信した場合，エラーを返答し更新は行わないものとする（表６）．重要な点として，Client 間の SP Update は許可されないことが挙げられる．

SPD Entry は手動で，もしくは複数の IKE AS から作成される可能性がある．よって，SPA の Database（以下，SPAD）では生成元の情報を管理する必要がある．

Local Mode	Remote Mode	Sent/Allowed SPREQ
Server	Server	（本論文中では対象外）
Server	Client_Active	SPREQ【全て】
Server	Client_Passive	SPREQ【全て】
Client_Active	Server	SPREQ【全て】
Client_Active	Client_Passive	（要求／応答しない）
Client_Active	Client_Passive	（要求／応答しない）
Client_Passive	Server	SPREQ【Peer の Local のみ】
Client_Passive	Client_Active	（要求／応答しない）
Client_Passive	Client_Passive	（要求／応答しない）

表 5 Mode と SP Request Message の関係

Local Mode	Remote Mode	Sent/Allowed SP
Server	Server	（本論文中では対象外）
Server	Client_Active	SP【全て】
Server	Client_Passive	SP【全て】
Client_Active	Server	SP【全て】
Client_Active	Client_Passive	（送信／受信しない）
Client_Active	Client_Passive	（送信／受信しない）
Client_Passive	Server	SP【Local のみ】
Client_Passive	Client_Active	（送信／受信しない）
Client_Passive	Client_Passive	（送信／受信しない）

表 6 Mode と SP Message の関係

SPA は 以上の情報・折衝を基に実行される．SPAD の設定例を図 1 に示す．また，実行される Negotiation の例を図 2 に示す．

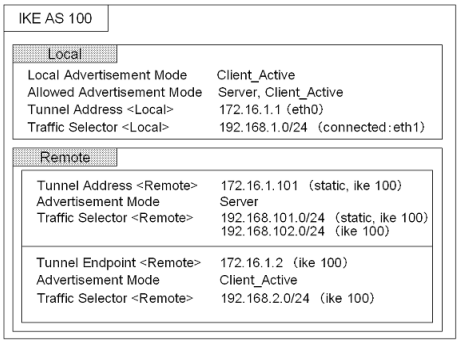

図 1 SPA Database の設定例

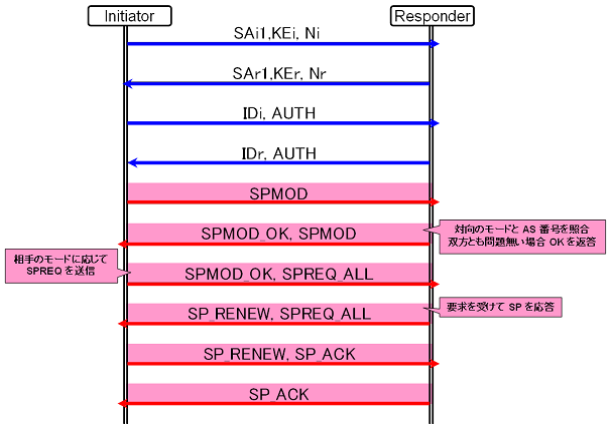

図 2 SPA を実現する Negotiation の例

3.3 経路情報との互換性を実現する Policy 間 Redistribution

SPA を機能させるための事前設定として Traffic Selector：Local Address，Local Tunnel Address，IKE Peer アドレスの三点を手動で指定する必要がある．

IKE Peer アドレスは Server Mode の Security Gateway 接続するために，DNS で解決可能な名前で指定する等の方法を取ることは可能であるが，Responder としてのみ動作させる場合を除き最低一つは手動で指定しなければならない．

Local Tunnel Address も同様で，こちらはローカルで参照可能な Interface 名を指定する方法がよく用いられる．この場合，IPCP や DHCP によって割り当てアドレスの変更が発生する環境においても設定更新を行う必要がない．

Traffic Selector：Local Address は多くの場合において範囲で指定する必要があり，且つ変更が十分に予想される項目である．よってここに特定の値を設定した場合，拡張性を低減させる結果となる．各 Security Gateway は End-to-End の到達性を確保するために Static で，もしくは Routing Protocol を使用し経路情報を管理している．また，照合される Traffic Selector が IP アドレスのみであれば経路情報は保護すべきノード群を示す情報に等しい．これより，Routing Table の Prefix を SPA Database の Traffic Selector：Local Address に注入することができれば指定情報を参照点として保有することができ，アドレッシングの変更に自動で対応することが可能となる．この関係を図 3 に表す．

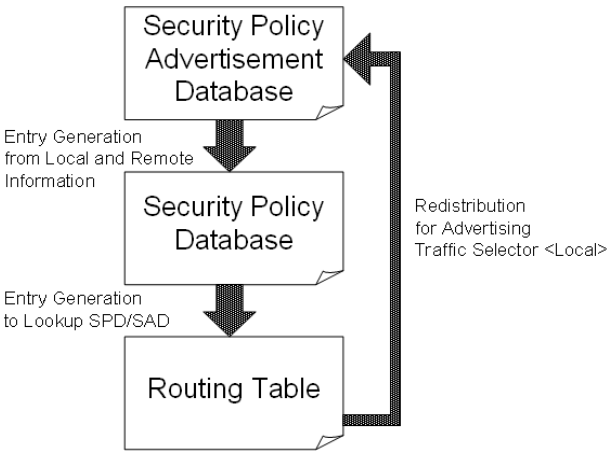

図 3 SPAD, SPD, Routing Table の関係

3.4 SPD Entry から経路情報を生成

SPA によって SPD Entry の生成を自動化することができる．しかし，SPD を参照し SA を適用するためには，転送テーブルに対象トラフィックを制御する経路情報を追加する必要が

ある．Routing Table では経路情報の Prefix とパケットの宛先アドレスが照合され，パケットは適合した Entry の Output Interface へ送出される．よって，Traffic Selector：Remote Address の Prefix と SPD の参照が実行される Output Interface を，SPD Entry 生成時もしくは CHILD_SA 確立時に，Routing Table に注入することができれば自動で IPsec 処理を有効にすることが可能となる．図 3 の Routing Table と SPD の関係はこの機構を示している．Traffic Selector：Local Address は Routing Table 参照時には照合されないが，Routing の結果 SPD の参照を開始することができれば，Local Address を識別子として処理を決定することが可能となる．

この要件を満たす機能は既にベンダー実装として存在しているが，生成した SPD Entry を参照するための仕組みとして必要な機構であるため，言及した．

4. 適　用　例

本方式の適用例を図 4-6 に示す．

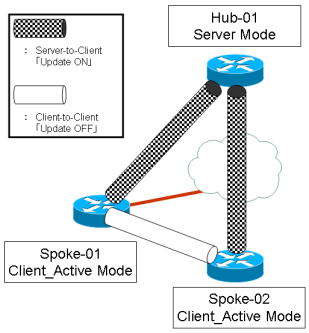

図 4　初期状態

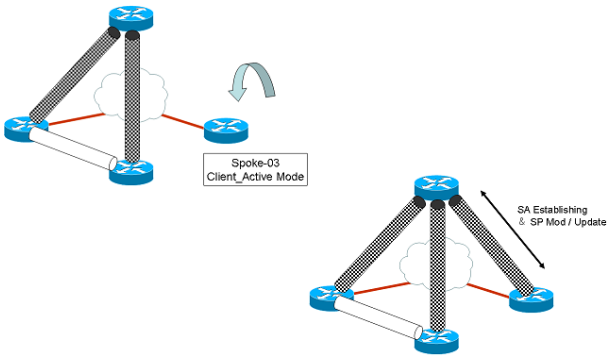

図 5　Spoke の追加→ Hub-新規 Spoke 間 SP Update

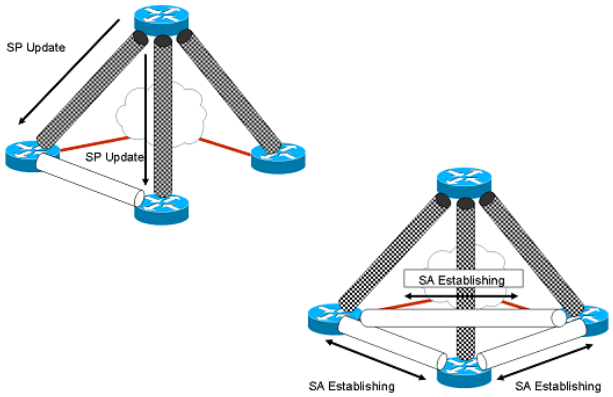

図 6　Hub-既存 Spoke 間の SP Update →フルメッシュ SA の確立

適用例では，新規 Spoke の追加に伴い Hub-新規 Spoke 間，次いで Hub-既存 Spoke 間で SP Update が交換され IPsec 通信に必要な SPD の構築及び経路情報の生成が自動で行われる．SPA が終了・収束すると フルメッシュの SA 確立が可能な状態となる．

以下，本提案で実現される通信の制御方法に関して補足する．

Spoke 間の通信を制御する場合は Client_Passive Mode を Spoke に適用する．Spoke は Hub 以外の Remote Tunnel Address を学習できず，全ての IPsec 通信が Hub 宛となる．Spoke 間で Hub 経由の通信を許可する場合は Default Route の Redistribution を活用する．

パーシャルメッシュトポロジを実現する時は Client_Active Mode 使用し，直接通信を行う Security Gateway 間でのみ番号が同一になるよう IKE AS を設定する．この時，互いに IKE AS が異なる Security Gateway 間では直接 SA が確立されない．End-to-End の到達性は IKE AS 間で Redistribution を実行することによって確保する．

また，LAN 側のセグメントを IKE AS によって区分し一組の Security Gateway 間内部通信を制御することも可能である．この場合，複数の IKE AS を設定し，非干渉とするセグメントについて互いに AS 番号が異なるよう Traffic Selector を指定する．この方法によって，同一 Security Gateway 間の通信においても，異なる AS に所属する Prefix 間では到達性が得られない結果となる．

アクセス制御に関する長所として，アクセス可否のリストを作成する方法と異なり事前に静的な値を設定しておく必要が無い．また，単一のセグメントを複数の IKE AS に所属させることによって，転送テーブルインスタンスを作成する方法と比較して柔軟なアクセス制御が可能であることが挙げられる．

5. 考　　察

5.1 Traffic Selector への IP アドレス以外の適用

本論文中では Traffic Selector として Local Address, Remote Address に着目して述べたが，SPA の機構に適用することで，他種類の Traffic Selector 統合も可能となる．留意点として，他 Traffic Selector の適用では，設定に際し Redistribution のアプローチは困難であることが挙げられる．

5.2 重複情報と冗長化・負荷分散構成への対応

例えば，Routing Table Entry 及び SPD Entry の基となる SPAD の中で Traffic Selector / Tunnel Address の情報が重複した場合はそれらを選出する仕組みが必要となる．具体的な方法として，事前に優先度となる値を各 Security Gateway に設定し SP Mode Notification 中に交換，メトリックとして SPAD に登録することが考えられる．

6. ま　と　め

本論文では Security Policy の Advertisement 機構を IKE に組み込むことを提案した．本提案では Traffic Selector や Tunnel Address の追加・変更・削除が存在する環境でも IPsec VPN を容易に展開することができる．加えて Mode と AS の概念によって柔軟なアクセス制御を実現することが可能となり，IPsec 通信に必要となる総合的なセッション維持負荷の削減や設定の簡素化に繋がることも期待される．

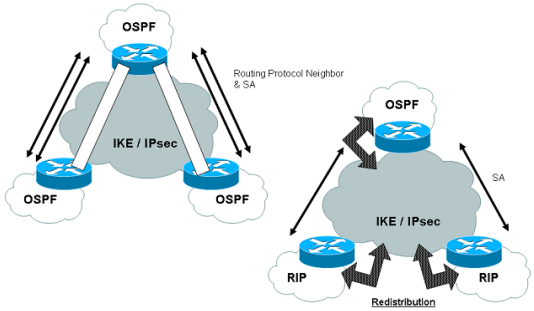

図 7　従来の方式（左）と制御を IKE に統合した本方式（右）

参　考　文　献

1) RFC 4301 Security Architecture for the Internet Protocol
2) RFC 4306 Internet Key Exchange (IKEv2) Protocol
3) マスタリング IPsec 第二版，O'reilly Japan