L_002

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

平河内 竜樹†

概要

本論文では，Host-to-Host の IPSec 通信で必要となる，端末への IKE/IPSec ポリシー設定を DHCP を通じて行うことを提案する．方式は動的なポリシー設定を可能にする他，通信開始時にポリシーが設定されていないという事態を未然に防ぐことができる．

また，宛先ノードのポリシーをネゴシエーション前に検知する方法として，DNS を利用することを合わせて提案する．この手法を適用すると，ポリシー不一致に因るネゴシエーション失敗を通信前に検出できるだけでなく，SA 確立の条件をイニシエータに提示することが可能となる．

1 背景

1.1 エンドツーエンド IPSec 通信の問題

IPSec は主に完全性の検証及び暗号化の機能を提供し，IP 通信に安全性を付与するものである．上記の機能を実現するため，IPSec を実行するノードは設定された SA パラメータを宛先ノードと折衝して同期を取り，その結果を Database（SAD）として格納する必要がある．つまり，IPSec を有効にするためには SA パラメータ等の「ポリシー*1を設定する」作業が必須となり，またその情報が同期できる，つまり「ノード間で互いに適切な値である」ことが条件となる．

現在 IPSec は VPN ゲートウェイ上で VPN を構築するために利用されることが多く，この場合 IKE/IPSec ポリシーの設定対象となるノード数はゲートウェイの数に限定される．また，ノード間で一貫したポリシーを適用することに障害は少ない．しかしユーザ端末がサーバ等の宛先ノードとエンドツーエンドの SA を確立するケースにおいては，端末単位で設定が必要となり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インターネットに適用した場合，常に適切なポリシーが設定されていることは期待できない．互いにパラメータとしてはユーザや管理者が許可を意図した設定がされているにも関わらず，組み合わせの漏れから「ポリシーとして合致する」という条件を満たせないために SA の確立を拒否してしまうことは十分に考えられる．

2 従来技術と本論文のアプローチ

2.1 ポリシーを配布するサーバの利用

ポリシーの設定には各製品に用意されているインタフェースを用いる他，MIB を利用する方法も提案されている．専用インタフェースや MIB の利用は VPN ゲートウェイの設定には有効であるが，端末単位のポリシー設定においては，前項で述べた作業量という問題を解決することは難しい．

ポリシーの選択肢という観点から，標準となるポリシーの使用を強く推奨し事実上一律に定めてしまう方法が挙げられる．初期状態で統一された設定が投入・有効化されていればユーザはポリシーの存在を意識することなく利用することができる．このように「選択肢を無くす」ことで不一致問題は回避できるが，パラメータ変更・拡張の余地を完全に排除してしまうため優れた解決策にはなり得ない*2．

不一致問題を緩和する方法としては，折衝時，ポリシーという単位を構築せずに許可するパラメータをリストとして渡す方法が考えられる．このアプローチはポリシーを網羅的に用意する方法と比較して漏れや無駄が少なくなる．しかしこれはパラメータネゴシエーションの根本的な仕様変更であり，また大幅な改善をもたらすものでないことから，普及が困難であることは明らかである．

「可変性のある」「ポリシーという単位を設定する」という作業を容易にするためには，ポリシーの配布を行うサーバを用意するというアプローチが適している．本論文ではポリシーの配布に専用のサーバを設置するのではなく，端末へのアドレス配布手段として広く利用されている DHCP に着目し，これに IKE/IPSec ポリシー配布の役割を担わせることを提案する．

2.2 ポリシーを検索するサーバの利用

ポリシー管理を行う専用のサーバを用意し，一元管理を可能にするシステムは既に製品化・販売されている．このようなクライアントのポリシーを一元的に管理・配布する製品を用いれば，管理下にある端末のポリシーを統一し，不一致問題を未然に防ぐことができる．しかしこの手法は限られたドメイン内にのみ適用できるものであり，ドメインを跨ぐ IPSec 通信の問題を解決することはできない．

ドメインを跨ぐ以上「ポリシーを統一する」というアプローチでは解決に至らない．本論文ではこの問題点に対する解決策として，パラメータネゴシエーションの前段階に「ポリシー解決」のフェーズを設けることを提案する．合わせて，ポリシー解決を担うプロトコルとして DNS を挙げる．

†無所属

*1本論文中で述べる「ポリシー」は暗号化処理対象を定義する SPD だけでなく，設定する SA 情報等の「パラメータ群」を包括して指す．

*2必ず適合するポリシーを用意するという観点から，最低優先度のドメインに囚われない統一したポリシーを設定必須とする意義はある．

3 ポリシーを配布するDHCPの拡張

3.1 DHCP でポリシーを配布する利点

端末のポリシー設定作業を自動化するために DHCP を利用する．専用のポリシーサーバでなく，DHCP を用いる利点は以下の通りである．

- データ通信開始時にポリシーが設定されていないケースを回避できる
  - IP アドレス等の情報と同時に設定できる
- 監視・許可対象が増えない
  - 新たにプロトコルを追加する必要がない
- DHCP の利点をそのまま引き継ぐことができる
  - サーバをブロードキャストでディスカバリできる
  - 認証機構を利用できる

本方式では IP アドレッシングを DHCP で管理している限り，アドレス割当と同時にポリシーの設定を行うため，SA の確立を試みる段階でポリシーが設定されていないという事態を未然に防ぐことができる．

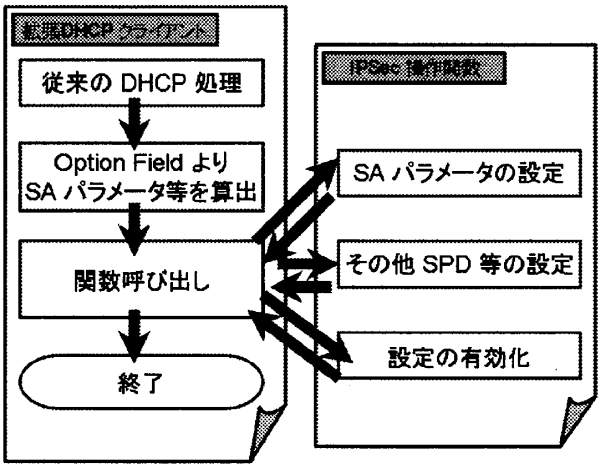

図 1: 本論文で示す DHCP の動作概要

3.2 拡張を実現するための仕様

DHCP はベンダー拡張用にオプションフィールドが定められている．このフィールドをポリシー交換用に定義し，ポリシーの構成要素であるパラメータ値を引き渡す．渡す手段として，パラメータ毎に対応した値を用意する方法と，SSL/TLS で定められているような Cipher Suite を定義し一つの値として渡す方法の 2 通りが考えられる．今回は拡張性に重点を置き，それぞれのパラメータについて別個専用のフィールドを設けた．その内訳を表 1 に示す．

パラメータの値が示す内容は RFC, Internet-Draft で定められているものに準拠する．Option フィールドは NAT-Traversal 等の拡張仕様ために確保した．IPComp の定義は利用頻度の理由から今回は除外した．

id	Field	bit
01	Code	8
02	Length	8
03	IKE Policy Number	8
04	IKE Policy Priority	8
05	Version	8
06	Exchange Type	8
07	Identitiy Type	8
08	Encryption-Algo	16
09	Key-Length	16
10	Hash-Algo	16
11	Oakley Group	16
12	Auth-Method	16
13	Life-Type	16
14	Life-Duration	32
15	Option Number	8
16	Option Type	8
17	Option Value	variable
18	IPSec Policy Number	8
19	IPSec Policy Priority	8
20	Security Protocol	8
21	Encap-Mode	8
22	Encryption-Algo	16
23	Key-Length	16
24	Hash-Algo	16
25	Oakley Group	16
26	MinLifetimeSecs	32
27	MaxLifetimeKB	32
28	ReplayPrevention	8
29	Option Number	8
30	Option Type	8
31	Option Value	variable

表 1: DHCP Option for IKE/IPSec Policy

なお，SA を確立するピアのアドレスと処理対象を定義するセレクタは配布情報として除外した．Host-to-Host で SA を確立する場合，通信相手全てが IPSec ピアとなる．このため，その全てを予め用意することは困難である．同様の理由でセレクタを細かく設定する方法も現実的ではない．IPSec ピアのアドレスは，通信相手のアドレスに等しいことから，通信時 DNS で取得したものを適用することで解決できる．セレクタに関しては「全通信を処理対象」とし，実行の制御は後に述べるポリシー解決用に拡張した DNS を用いて実現する．

4 ポリシーを検索する DNS の拡張

4.1 IKE/IPSec ポリシーの DNS への適用

IPSec 通信では，ポリシーの設定作業を自ノードに行えば SA を確立するためのネゴシエーションを開始することができる．しかし従来の設定とネゴシエーションでは，イニシエータは選択されたポリシーもしくは失敗であったことを知らせる情報しか受け取れず，レスポンダに用意されたポリシー設定の詳細を知ることはできな

い．もしネゴシエーション前にレスポンダのポリシー設定を知ることができれば，ポリシー不一致が原因のネゴシエーション失敗を事前に回避することができる．また不一致の結果をトリガとして，ユーザに宛先のポリシー設定を通知することやポリシーを合致させるための設定変更処理に移行することも可能になる．図 2, 3 は，出力にユーザビリティは考慮していないが，ポリシー解決の結果からユーザに分岐の判断を委ねている例である．ポリシー解決を実現できればこのような動作を行うことが可能になる．

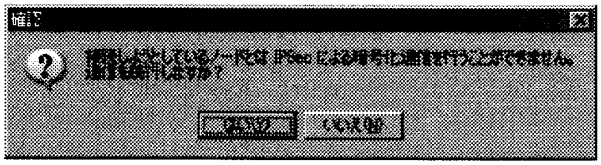

図 2: ポリシーの照合より IPSec を利用できないことが判明

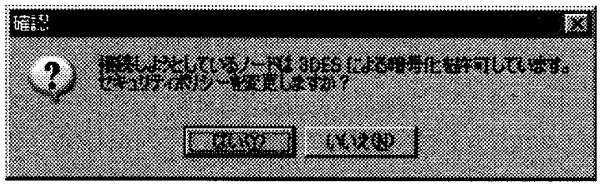

図 3: ポリシーの照合より Encryption-Alog の不一致が判明

セグメントを越えて宛先に関する情報を取得する場合，解決を行うサーバのアドレスを有する必要がある．ポリシー解決実現の手段として専用のサーバを配置することが考えられるが，この場合新たなサーバ情報を端末に通知する作業が生じてしまう．IP 通信においてはホスト名から宛先 IP アドレスを索引するために DNS が利用されており，各端末は DNS サーバを参照するためのアドレス情報を保持している．DNS サーバのアドレスは，エンドユーザが指定する宛先情報の多くはホスト名／ドメイン名であることから，ほとんどの端末に設定されている情報である．よって DNS を拡張しポリシー解決の作業を担わせることできれば，端末に設定するアドレス情報を増やすことなく宛先となるレスポンダのポリシーを検索することが可能になる[*3]．

SA の確立において，宛先ホストが有する IP アドレス以外の情報取得に DNS を利用するというアプローチは RFC 4322 にて既に提言されている．これは DNS を通じて公開鍵を管理し，認証に利用するというものである．具体的には DNS セキュリティ拡張（RFC 2535）にて定義されている「KEY Resource Record」を用いて鍵配布が可能な環境を構築し，通信時に宛先ノードの公開鍵を取得する．その結果，「可能であれば」暗号化通信を行い，そうでなければ通常の通信を行う．

この「可能であれば」という判断はあくまでも SA 確立の成否に基づくものであり，対向ノードのポリシーに関

[*3]従来の DNS サーバと同一のホストでの実行を必須とすれば，プロセスを分離しても，別のアプローチを用いても，アドレス通知の手間は不変である．

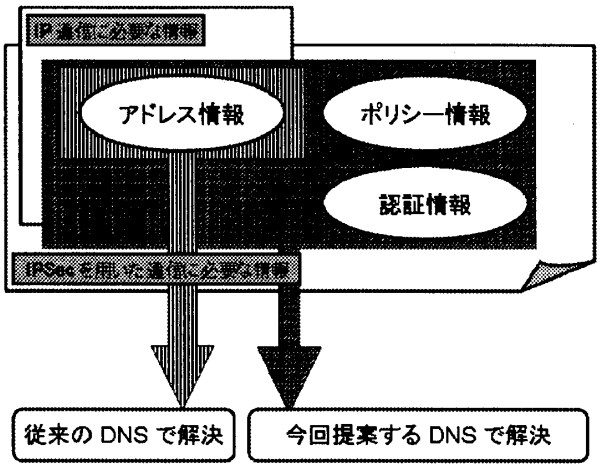

図 4: 本論文で提案する DNS で解決する範囲

与しているわけではない．本論文では宛先の「IP アドレス」「認証情報」に加え「ポリシー情報」も DNS で解決することを提案している（図 4）．なお各端末はデジタル証明書の発行を受けていることを前提とし，認証情報としてこれを DNS に登録する[*4][*5]．以上より，今回提案する拡張 DNS では証明書レコード（RFC 2538）と前項で定義した IKE/IPSec ポリシーを格納する IKE/IPSec ポリシーレコードが必要になる．後者は前項の拡張 DHCP で定義したフォーマットをオプションリソースレコード（RFC 2671）のデータ部に挿入することで実現する．

4.2 拡張 DNS への情報登録と解決

レコードの参照・追加・変更・削除という観点より，ポリシー解決型の DNS で必要となるメッセージとして表 2 のものが挙げられる．

id	Message-Type
01	Policy Resolution Request
02	Policy Resolution Reply
03	Policy Registration Request
04	Policy Registration Reply
05	Policy Purge Request
06	Policy Purge Reply
07	Certification Resolution Request
08	Certification Resolution Reply
09	Certification Registration Request
10	Certification Registration Reply
11	Certification Purge Request
12	Certification Purge Reply
13	Error indication

表 2: Message Type for Registration & Resolution Policy

セグメントを越えた宛先情報の解決という点で共通している，NHRP とほぼ同じメッセージタイプとなる．

[*4]DNS サーバ自体の信頼性は DNSSEC を用いて確保することができる．

[*5]認証情報として端末毎にデジタル証明書を発行すれば，DNS サーバへポリシー情報を登録する際のクライアント認証にも利用できる．

登録要求メッセージの送出が必要となるタイミングはポリシー設定に変更が加えられた時である．的確に登録要求を実行するためには，変更の操作をトリガとして付随的に実行させるか一定間隔でポリシー設定を監視する必要がある．ホスト単位でポリシーを登録する場合は，解決要求の際に送信元のポリシーを添付しそれを追加する形で実現する方法も考えられる．

ポリシー解決用のレコードは上記の登録作業を経て作成される．要求に応じてレコードを参照し，ヒットしたレコードの情報を元に作成した返答メッセージをクライアントに返すことでポリシー解決は実現される．

5 まとめ

本論文ではエンドーツーエンド IPSec 通信に関して，ポリシーの設定容易性を向上させる手段として DHCP を利用することを提案した．また，ポリシー設定の柔軟性を高めるために宛先ノードのポリシー情報をネゴシエーション前に検索することを提案し，その実現方法として DNS の拡張仕様を示した．

6 考察

6.1 セレクタ情報の配布

「あるホストとの通信では暗号化を行わない」「特定のトラフィックをだけを対象とする」等の条件があればセレクタを配布する必要が生じる．但しセレクタはシステム内で実装の自由が許されているため，それに伴い引き渡す情報も複雑且つシステムの独自性が強くなる．この場合「セレクタ専用」のオプションを設け，定義のアプローチに応じてオプション番号を変更した方が実装が容易になると推察される．

6.2 ドメイン単位の解決と自動事前登録

本論文では DNS サーバにホストのポリシーと証明書を登録する手法を示したが，この場合全端末の情報を登録する必要があるため，サーバの保持するレコード数が莫大なものになると予想される．ここでは機器・回線の負荷削減及びより効率の良いポリシー登録方法について考察する．

証明書は端末が別個に保有する必要があるが，ポリシーに関しては，特に前述した拡張 DHCP を用いて一元的に設定した場合，ドメイン内で共通の設定を行っている可能性が高い．そこで DHCP サーバに「ドメイン単位のポリシー登録」の機能を持つ DNS クライアントを実装し，ドメイン単位でポリシー情報を登録すれば，ホスト単位で登録した場合と比較してレコード数を大幅に削減することができる．ドメイン単位の登録はメッセージタイプとレコードタイプを変更することによってホスト単位の登録と区別すれば，ホスト単位の情報まで索引しなくても終端することを明示できる．また DHCP サーバが実行する場合，ホストが自発的な通信を開始せずともホストの情報登録を行うことができる．

同様に CA サーバに DNS クライアントの機能を持たせれば，証明書の発行と同時に DNS への登録を行うことができる．証明書は集約することができないのでレコード数の削減には至らないが，前述したポリシー登録が同時に実施されていれば，ホストは DHCP サーバと CA サーバから情報を割り当てられるだけで IPSec のイニシエータだけでなくレスポンダにもなることができる．

参考文献

[1] RFC : 1533 - DHCP Options and BOOTP Vendor Extensions, 2332 - NBMA Next Hop Resolution Protocol (NHRP), 2535 - Domain Name System Security Extensions, 4025 - A Method for Storing IPsec Keying Material in DNS 4034 - Resource Records for the DNS Security Extensions 4109 - Algorithms for Internet Key Exchange version 1 (IKEv1), 4305 - Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), 4322 - Opportunistic Encryption using Internet Key Exchange 他

[2] Internet-Draft : draft-ietf-ipsp-spd-mib-06.txt, draft-ietf-ipsp-ikeaction-mib-01.txt, draft-ietf-ipsp-ipsecaction-mib-01.txt 他

[3] マスタリング IPsec (O'reilly Japan)