

IPv6を取り巻く技術・標準化動向(1)

— IPsecと認証 —

1. IPsecとIPv6

IPに対するセキュリティアーキテクチャを定義したIPsecはオープンなIPv4のインターネットの普及とともに、その中でセキュリティを確保する技術として進歩を遂げてきた。現在では、FTTHやADSLのようなブロードバンドアクセスサービスの登場により、高速な回線が安価で利用できるようになり、これを利用して、企業の本社・支店間をIPsecで接続するインターネットVPNサービスに広く利用されている。また、これまで電話回線や

ISDNによるダイヤルアップ接続が中心であった企業へのリモートアクセスに関しても、同様にIPsecで接続する利用シーンが増えてきている(図1)。

IPv6技術は、潤沢なアドレス空間を利用し、アドレス変換機能が不要なエンド-エンド型の通信を目指して開発が進められている。この中ではセキュリティの必要性がよりいっそう重要になってくると考えられるため、IPv6ではIPsecの機能を標準機能として位置づけている。

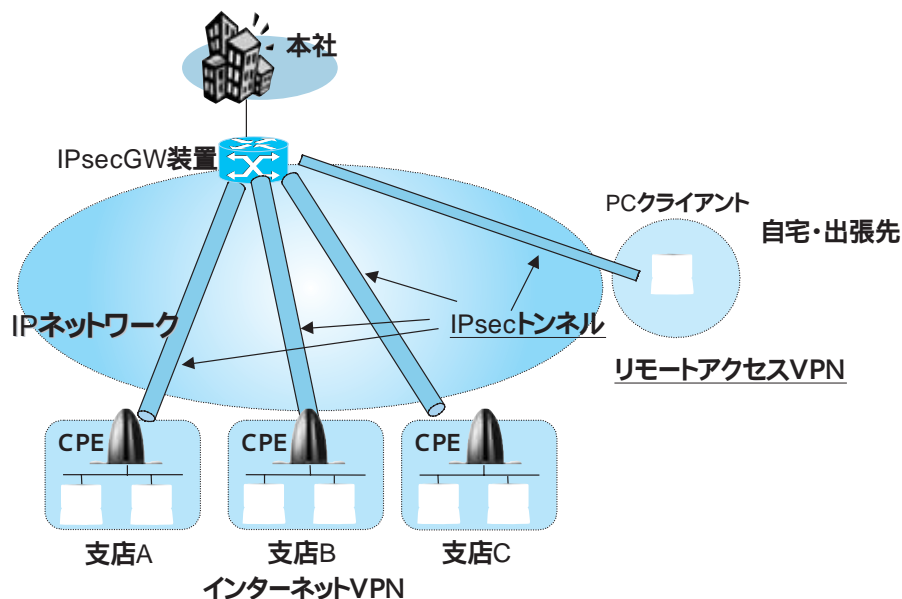


図1 IPsecの利用シーン

2. IPsecと認証技術

2.1 IKEとIPsec基本機能

IPsecはIPのレイヤでセキュリティの機能を実現することを特徴とする技術である。

ネットワーク上でのセキュリティ機能に関しては様々なものが考えられるが、IPsecでは主に次の2つの機能の提供が可能だ。

認証

- ・通信相手のなりすましを防止するための本人性確認
- ・通信経路上でのパケットの改竄を防止するための完全性保証

暗号化

- ・通信経路上での盗聴の防止のための暗号化

IPsecとは、SA (Security Association) と呼ばれるセキュアな通信路を構築する技術である。セキュリティプロトコルとして、暗号化ならびに認証機能を提供するESP (Encapsulating Security Payload) と認証機能のみを提供するAH (Authentication Header) の2つのプロトコルが規定されている。また、ホスト間でのIPsecを適用するためのトランスポートモードと主にルータ間で使用するトンネル

モードの2つが定義されており、トンネルモードはトンネリング技術としてVPNに使用することが可能である。

IKE (Internet Key Exchange) は、SAの生成に必要となる鍵を通信相手と交換を行い、SAの自動生成を行うことを目的として規定されたプロトコルである。SAにはライフタイムと呼ばれる有効期間がありこの期間を満了すると消滅する仕組みになっているが、IKEにより定期的な鍵交換を行い新たなSAを生成し切り替えていくことで、SAのセキュリティの強度を保ちながら通信を継続することが可能になる。IKEの考え方では、Phase1とよばれる処理により互いの装置間でIKEの制御用メッセージの通信を行うSAを最初に生成し、Phase2においてユーザデータの通信を行うIPsec SAが生成する構造になっている (図 2)

2.2 認証技術

IKEの接続を行う際に、相手が接

続を許可してよい正しい相手であることの認証を行う必要があり、この目的のために大きく次の2つの認証方式が利用されている。

事前共有鍵方式

接続する通信相手との間であらかじめ鍵情報を共有しておき、IKEのプロトコル処理の中でお互いの鍵情報が一致しているかどうかで相手が本人であることを確認する方式。比較的容易に実現可能な認証方式であるため現在広く利用されている。事前に通信相手に対して鍵情報を安全なかたちで配布し共有しておく必要があるため、鍵情報の管理が課題となる。

PKIを用いた方式

CA (Certification Authority) により発行された電子証明書により証明された公開鍵を用いることで本人性の認証を行う方式。事前共有鍵のように、通信相手とあらかじめ鍵情報を共有する必要はないが、PKI

(Public Key Infrastructure) と呼ばれる認証基盤が必要になる。今後PKIの整備が進むにつれて広く利用されていく方式だと考えられる。

2.3 IKE 拡張機能

これまでに説明したIKEの基本機能以外に、ネットワークのプロトコルとしてIPsec技術を使用する際には、IKEの拡張機能を利用する必要がある。

たとえば、接続先の相手装置の生死確認を行ういわゆるkeepaliveの仕組みは、IPsecを利用してサービスを実現する場合には重要な機能となるが、多くのIPsec装置メーカーが独自の仕様を実装しているため相互接続が困難である。IETFではDPD (Dead Peer Detection) がinformational RFCとしてまとめられているため、今後はこの方式が広く利用されていくことが期待される。

リモートアクセス型のIPsecのネットワークを用いる際には、接続し

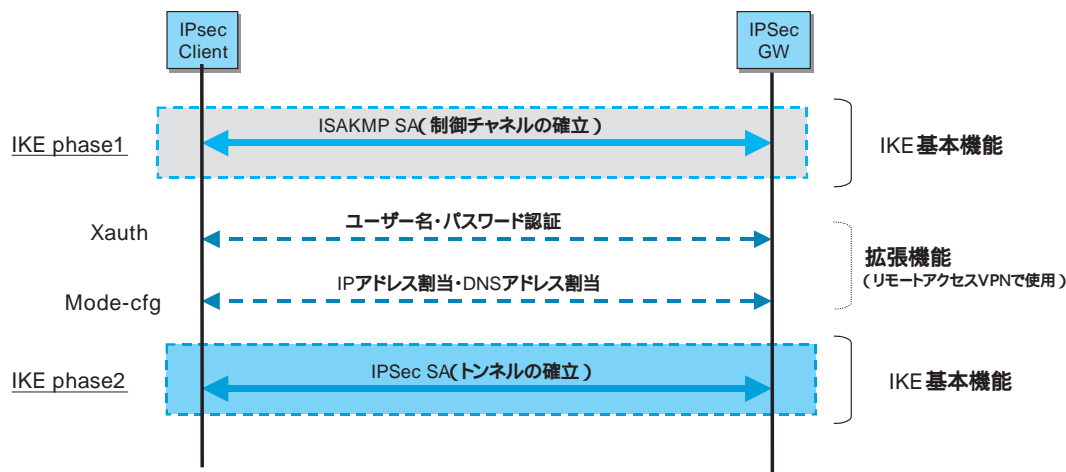


図 2 IKE シーケンス概要

てくる端末のIPアドレスが特定できないため、ユーザー名ならびにパスワードの認証を併用することでセキュリティを高める必要がある。これを実現するプロトコルとしてXauth (Extended Authentication) と呼ばれるプロトコルが使用される。また、VPN内で用いる内部IPアドレスならびにDNSアドレス等のネットワークパラメータを接続時にユーザー端末に通知することで、ユーザー端末側での設定項目を少なくすることが可能となる。これを実現するプロトコルとしてmode-cfg (The ISAKMP Configuration Method) と呼ばれる技術が用いられている。これらのリモートアクセス型のIPsecを実現するために必要となるXauthならびにmode-cfgは、デファクト標準として広く利用されている。

3. 今後の技術動向

3.1 IKEv2

IPsec技術に関連した最近のトレンドとしては、IETFにおいてIKEv2の標準化が進められていることがあげられる。IKEv2の大きな特徴は、これまで拡張機能として実現されてきたリモートアクセス型のIPsecの機能が正式にIKEの標準機能として盛り込まれたところにある。

これまでに説明してきたユーザー認証のためのXauthについては、IKEv2ではEAP Payloadという形で定義されている。EAP (Extensible Authentication Protocol) はもとも

とPPPの認証方式の一つとして開発された技術であり、無線LANの802.1xの認証技術にも利用されている。認証プロトコルのフレームワークを定義しているため、様々な認証方式を実装可能となっており拡張性が高いのが特徴である。IKEv2になりEAPが採用されたことにより、ユーザー名・パスワードに基づく認証方式が正式にサポートされた他、EAPによる様々な認証方式をサポートすることが可能になり、IPsec技術の適用領域拡大につながる事が期待されている。

また、アドレス割当機能のためのmode-cfgについては、Configuration Payloadとして正式に定義された。ここで定義されているパラメータはmode-cfgのdraftと同じものが基本的に採用されており、mode-cfgからの移行が容易であるといえる。

3.2 高速化

一般に、IPsecの通信を行う際に用いられる暗号化ならびにハッシュの処理は、処理負荷が重いため高速なスループットの実現は困難だと考えられている。しかし、今後のIPsecの利用シーンの増加を考えると、高速化への対応は解決すべき技術課題と位置づけられるだろう。

解決へのアプローチとしては、現在広く利用されている暗号化アルゴリズムのDES (Data Encryption Standard) あるいは3DESに代わり、より軽量かつセキュリティのレベルも上がっているAES (Advanced Encryption

Standard) を使うことがあげられる。軽量なアルゴリズムを採用することは、PCクライアント等の暗号化の演算をソフト処理で実行する装置と通信する場合に有効な方法と考えられる。

また、他のアプローチとしては、暗号化の処理をハード化したセキュリティチップを装置へ組み込むことで高速化を実現する方法がある。ハードウェアチップとしては数Gbpsの処理速度が可能なセキュリティチップも製品化されてきており、大容量なIPsec装置が実現されていくと考えられている。また、IPパケット処理を高速化するためにIP関連装置で利用されるネットワークプロセッサが暗号化処理の演算機能を取り込む動きもあり、このような形態が進めば装置内でのチップ数を削減できるため、コストの低減につながる可能性があるだろう。

4 まとめ

今後のネットワークサービスを考えると、今回紹介したIPsecや認証技術を用いたセキュリティの機能はますます重要度を増していくと考えられ、IPsecにより実現されるセキュアなコネクティビティを利用したサービスは、IPv6ネットワークの更なる展開を促進していくと考えられる。