無線 LAN 等リモートアクセス環境下での
インターネット VPN 利用検証報告書

平成 15 年 4 月 30 日

NPO　日本ネットワークセキュリティ協会
2002 年度インターネット VPN ワーキンググープ

取扱い注意事項

本報告書は、NPO 日本ネットワークセキュリティ協会（以下：JNSA と記す）インターネット VPN ワーキンググループが作成したものであり、著作権は当該 NPO に属するが、本報告書は公開情報として提供されるものである。本報告書をご参照、ご利用される場合は、以下の事項に従ってください。

- ご利用にあたっての注意事項
  - 著作権は NPO 日本ネットワークセキュリティ協会に属します。
  - 本報告書の一部、全文に係わらず引用される場合は、必ず引用元として『JNSA インターネット VPN ワーキンググループ 2002 年度活動報告書』を明記してください。
  - 本報告書の一部、全文に係わらず、書籍、雑誌、セミナー資料などに引用される場合は、事前に sec@jnsa.org 宛にご連絡ください。
  - 本報告書を利用した事によって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

― 目 次 ―

1 はじめに

平成 14 年度 インターネット VPN ワーキンググループでは、ラストワンマイルに公衆無線LANサービスを使用したインターネットVPNについて調査をおこなった。公衆無線 LAN サービスは以前、「ホットスポット」と呼ばれていたが、NTT 系のサービス提供者が「ホットスポット」を商標登録したため、現在では公衆無線 LAN サービスという呼称が一般的に使用されているため、本報告書でもこれを採用している。また、本報告書で使用している「公衆無線 LAN サービス」とは、ファーストフード店舗やホテルなど不特定多数の方が利用する施設において、無線 LAN を使用して高速インターネット接続を提供する有償・無償のサービスのことであり、そこには実験サービスも含まれる事を予めご了承いただきたい。

公衆無線 LAN サービスは、無線 LAN 製品の低価格化が始まった平成 13 年後半から急激にその数を増やし続けているが、実際の利用者数は予想を大きく下回っているのが現状である。しかし、ユビキタス・コンピューティングのインフラとして期待の高いサービスであることや、調査開始時期は無線 LAN のセキュリティに関する関心が非常に高く、無線 LAN を使用している公衆無線 LAN のセキュリティについても WEP による暗号化では、同一 SSID 内では盗聴が可能でのあるなどビジネスで使用する上では多くの問題があったことから、「公衆無線 LAN サービスをビジネスで使用可能とする時の課題を明らかにする」事を調査目的とした。また、その結果を企業の情報システム担当者の方々が利用できる形でまとめることを、ワーキンググループ活動の最終目的としている。したがって、報告書の内容はインターネット VPN を利用してリモートアクセス環境を導入する際の注意事項も包含する形でまとめている。そして、本報告書を有効に使用していただくために補足資料として調査で使用したプロトコルである IPsec の技術説明を添付しているのでインターネット VPN 導入・運用時の参考文献としても利用していただける形にまとめた。

2 VPN とは

2.1 IP-VPN と インターネット VPN

この報告書を読み進む前に VPN の定義をはっきりさせておきたい。この報告書の中で VPN とは、「公のネットワークの中で、トンネリング技術を用いる事により仮想的に閉域ネットワークと見せかける技術」としている。もう少し分かり易く述べると、インターネットのような公のネットワークの中で、IPsec というトンネリング技術を用いて仮想的にできたクローズ（閉域）ネットワークが VPN という事である。ここで注意が必要で、VPN はトンネリング技術であり、暗号技術では無いことである。VPN ＝ 暗号通信技術と解釈されている方が以外に多いが、VPN ＝ トンネリング技術である事を理解していただきたい。

VPN の定義が理解できたところで良く耳にする、「IP-VPN」と「インターネット VPN」の違いについて簡単に説明する。そもそも、「IP-VPN」とは公の IP ネットワークで VPN を使用する。または使用したネットワークのことを意味している。したがって公の IP ネットワークであるインターネットを使用した VPN、すなわち広義では「インターネット VPN」も「IP-VPN」に含まれる物と考えて良い。しかし現在では一般的に、「IP-VPN」というと、NTT-XXX や、大手キャリアが自前のバックボーンに顧客ごとに閉域性を持たせ、あたかも専用線のように使用させるサービスのことを「IP-VPN」と呼び、インターネットで IPsec, SSH などのトンネリング技術を使用してインターネットに閉域性を持たせ、あたかも専用線に見せかけたネットワークの事を「インターネット VPN」と呼んでいる。どちらの VPN も回線コストを削減するメリットは得られるが、その実現方法は全く違う。

この報告書はインターネット VPN について記載されたものであり、以後、単に VPN と記載されている場合は、インターネット VPN を指すものであると理解していただきたい。

2.2 インターネット VPN を実現するプロトコル

インターネット VPN を実現可能なトンネリング技術は標準化されているものだけでも多数存在する。ここではそれを全て紹介する事はできないため、代表的な技術だけを紹介する。

- SSL（Secure Socket Lyer）

  インターネットでオンラインショッピングなどを利用する際などに、ブラウザの右下辺りに鍵マークが表示される事でおなじみのプロトコルである。SSL は、サーバークライアントのアプリケーション間で暗号と認証機能を提供するセッション層に位置するプロトコルである。SSL 単体では、VPN の定義であるトンネリング技術を提供する事はできないが、最近では複数のメーカから、SSL とプロキシー技術を応用し、仮想的にトンネリング見せかけ VPN を実現する製品が出てきて注目を浴びている。

- SSH（Secure Shell）

  SSH は様々な AES や 3DES など様々な暗号方式、公開鍵認証や Hostbase 認証などの認証方式をリモートログイン環境に提供する。また、ポートフォワーディング機能より、サーバークライアント間で確立した SSH セッションの中に、HTTP や POP3 など（TCP を使用しているプロトコルであればほとんど全て）の通信を通す事が可能であり、この機能を活用する事で容易に VPN 環境を構築できる。インターネット VPN を構築する際に必要となるファイヤ

ーウォールの設定も SSH だけを許可すれば良いだけなので、既存ネットワーク環境に与える影響も少ない利点もある。

- IPsec

  IP に暗号、認証などのセキュリティ機能を提供するプロトコルで、現在、インターネット VPN を構築する際に最も使用されるプロトコルである。ネットワーク層に位置するため、上位アプリケーションやネットワーク形態に影響されない利点がある一方、標準機能だけでは NAT 環境に対応できないことや、IPsec 通信に先立ち行われる IKE ネゴシエーションの複雑であるため運用には相応のスキルが必要になるなどの問題もある。

- PPTP(Point to Point Tunneling Protocol)

  PPP パケットをインターネットなどの IP ネットワーク上に流す為のトンネリング機能と、データを暗号化するための機能を提供する。PPP という言葉からも分かるようにダイヤルアップ環境からインターネットを経由して、社内のネットワークにアクセスする際に使用される。また WindowsNT 4.0 以降の Microsoft 社には標準実装されているため、比較的手軽に使用することが可能なプロトコルである。

- L2TP（Layer 2 Tunneling Protocol）

  Microsoft 社などが開発した PPTP と Cisco が開発した L2F というトンネリング技術を統合して標準化されたプロトコル。PPP パケットをインターネットなどの IP ネットワークに流すためのトンネリング機能とエンド to エンド認証機能を提供する。PPTP では提供されていた暗号機能は、IPsec を使用する。Microsoft 社の Windows2000 以降で標準実装されている。

レイヤ	プロトコル	機能概要
アプリケーション	SSL	ｻｰﾊﾞとクライアント間で暗合/認証機能を提供。Webの暗合通信でもっとも一般的なﾌﾟﾛﾄｺﾙ。SSLとプロキシー機能を利用した、VPN製品が現在注目されている。
	SSH	ssh(Secure Shell)は、強力な認証と暗号通信機能を提供する。ポートフォワーディングを活用する事で、比較的容易にVPN環境を構築する事が可能
ネットワーク	IPsec	IPﾊﾟｹｯﾄに暗号/認証機能/電子署名機能を提供するﾌﾟﾛﾄｺﾙ。
データリンク	PPTP	PPPデータフレームに対しカプセリング機能と暗号機能を提供
	L2TP	PPTPの拡張版。ﾃﾞｰﾀをIPｶﾌﾟｾﾙ化すると同時に，ｴﾝﾄﾞ・ｴﾝﾄﾞでﾕｰｻﾞｰ認証機能を提供。

表 2-1 VPN を実現するプロトコル

2.3　調査で使用したプロトコル

今回の調査では、ラストワンマイルに公衆無線 LAN を使用したときのインターネット VPN についてまとめているが、使用したプロトコルは IPsec である。IPsec を対象とした理由は、現在 企業ユーザがインターネット VPN を導入する際に最も多く利用されているプロトコルであることが要因である。また、IPsec をサポートする製品は市場に多く出回っており、企業ユーザが製品を選択する際に他のプロトコルと比較して困難であることから、本報告書が最も利用される可能性があるのは IPsec であると判断したためである。

3 インターネット VPN の影響

3.1　インターネット VPN を取り巻く環境

ここ１～２年で企業の利用が加速的に進んでいるインターネット VPN であるが、そもそもどのように発展してきたものであり、今後どのように利用されていくのか、いったん技術的な考察とは離れ、その成り立ちと利用者にあたえる影響について考えてみたい。

そもそもインターネット VPN の基本になっている通信技術はというと、前項でも説明されているが、IPsec、PPTP 等様々である。

そのインターネット VPN の基本となっている通信技術は実はかなりの歴史があるものである（現在もっとも利用が盛んである IPsec の基本的な勧告※は１９９５年に発表されている）。

※RFC1825 Security Architecture for the Internet Protocol aug/1995

ではなぜいまインターネット VPN が脚光を浴びているかというと、インターネット接続回線の高速化･低価格化が驚異的な速度で普及したためであると思われる。

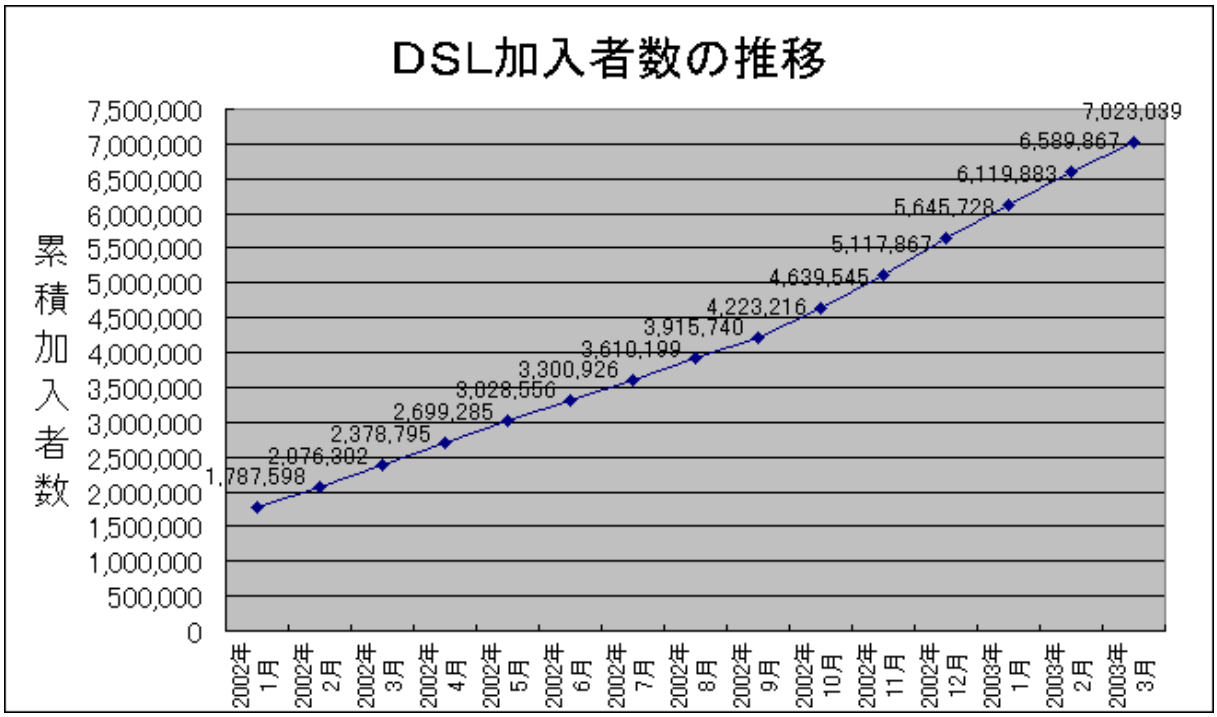


図 3-1　DSL 加入者の推移

（出典）総務省　DSL 普及状況公開ページ　2002 年 4 月現在）

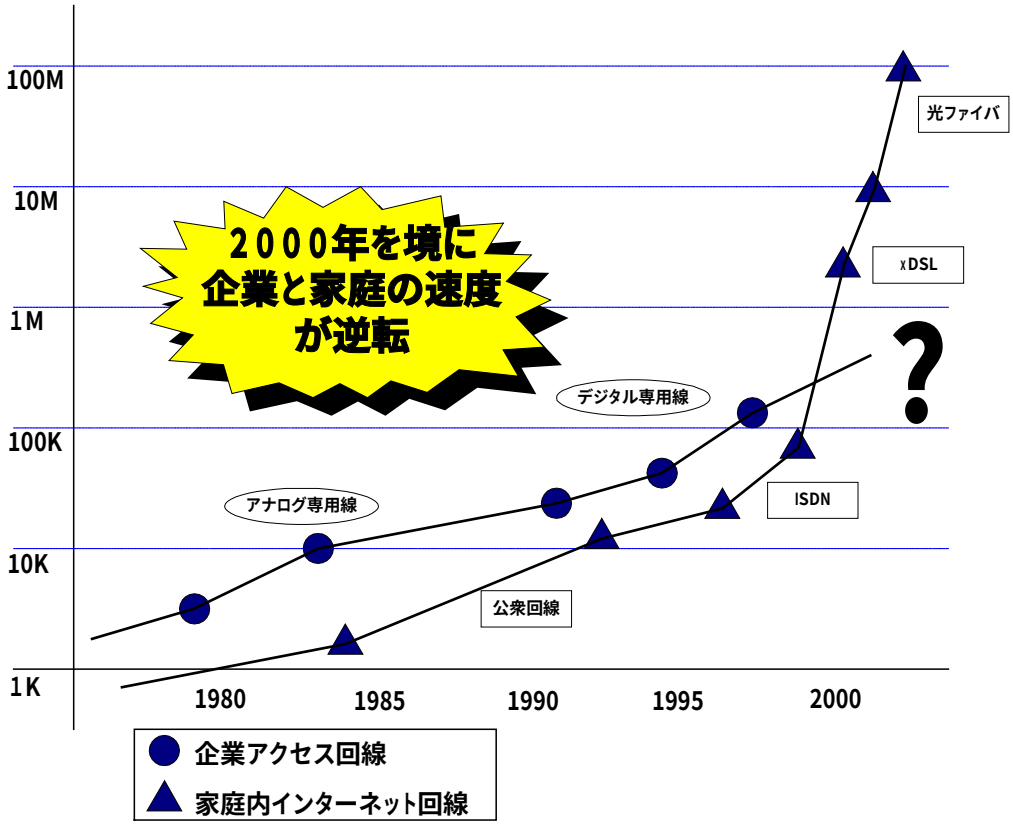


図 3-2　インターネット接続回線の速度推移

VPN の利用促進の原因は家庭内のブロードバンド回線だけではなく、モバイル環境が整備されつつあることにも関連していると思われる。

無線 LAN については、セキュリティについて懸案が払拭されていない側面はあるものの、家庭内や企業での導入が進んでいる。また、公衆無線 LAN サービスについても、若干その展開にとまどっているが、IP 電話などとの組み合わせにより今後利用が促進されるものと思われる。

一方、携帯電話（PHS）については、通信速度には制限がある物の定額制サービスなどが複数の事業者より提供され始めているので、次世代の移動体通信とともにますます環境が整備されている。

このように、インターネットアクセスが場所を問わず高速で安価になっていく状況下で、利用者の特にビジネスにおける作業効率や生産性を向上させる効果的なツールとしてインターネット VPN の利用がますます促進していくと考えられる。

次頁以降に生産性や作業効率をあげるための VPN の利用方法について考えてみたい。

3.2　インターネット VPN で利用できるコンテンツ

インターネット VPN をどのように利用すれば生産性や作業効率の向上を図れるかについて、具体的なソリューションについては後述することにし、まず大容量で低価格なインターネット回線が利用できると、いままでの従量制の高価な遅いインターネット回線を使っているのとどのような変化が発生するのかを考えてみたい。

回線速度	利用可能コンテンツ（例）	アクセス手段
２０Mbps 強	高解像度 TV（DVD 等）	光ファイバ
１０Mbps 弱	通常の TV 画像	xDSL 以上
数 Mbps 程度	動画	xDSL 以上
５００Kbps 程度	静止画像、音声等	ケーブル TV 以上
５６～６４Kbps	電子メール、Web 閲覧	ISDN、公衆回線

表 3-1　通信速度と利用可能コンテンツ

従来の個人用のインターネット接続回線では、主にテキストデータや静止画像の送受信（インターネットメール、シンプルな WEB）に利用する事が精一杯であったが、ケーブル TV や xDSL，FTTH などの家庭用ブロードバンド回線を利用することにより、高解像度の静止画像や動画、音声などのデータ量の大きい、リッチなコンテンツがストレス無く扱えるようになっている。

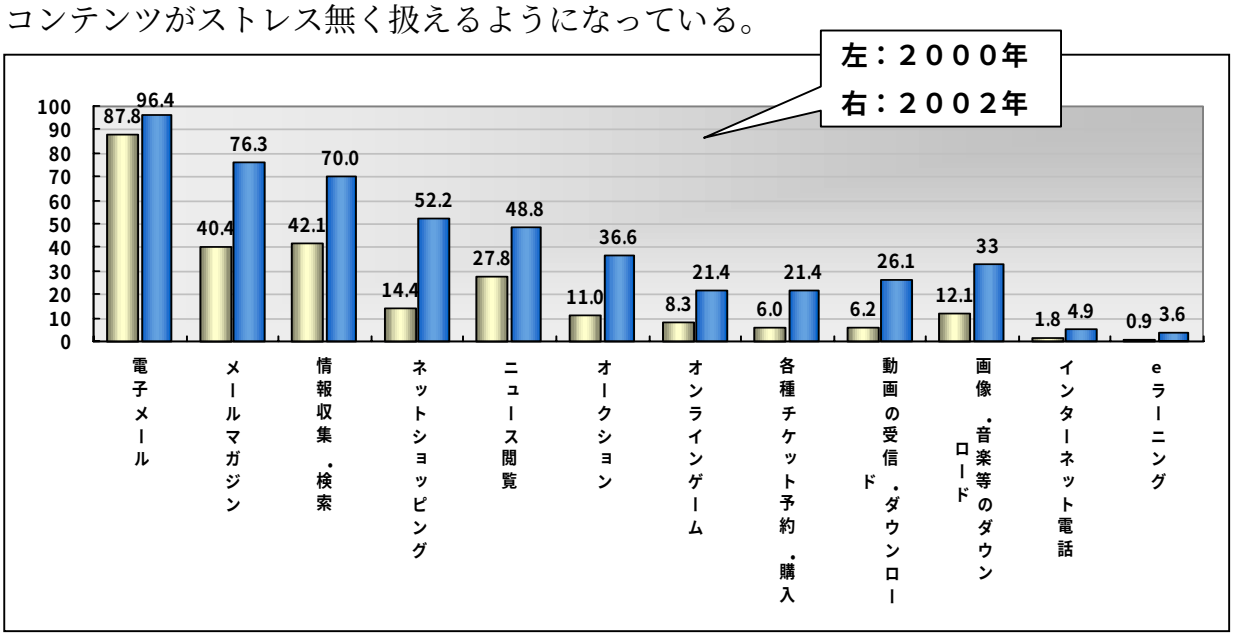


図 3-3　用途別インターネット利用率

（出典）総務省「ＩＴと国民生活に関する調査分析」（ウェブ調査）（2002 年 3 月調査）

また、数値としては表しにくいものであるが、従量制から定額の常時接続に変わることによって、利用者の心理的側面についても触れておきたい。

たとえば、インターネット上で商品を購入しようと思ったとき、接続時間の事を気にしていて購買意欲が湧くだろうか？

また、使っても使わなくても料金が一緒になってくると、利用者としては出来るだけ利用時間を長くしたいと思うのが人情である。現在でも自宅でテレビを見ながらインターネットに接続している「ながら利用」など、インターネットを利用する形態は様々に変化している。

	優位点	用途
高速・広帯域	・ 動画等の大容量なデータの送受信が可能になる ・ 社外においても、快適に企業内の情報資源にアクセスが可能になる	・ 映画や音楽などの配信ビジネスが可能になる ・ テレビ会議や在宅勤務など、就労形態が変化する
常時接続	・ 接続時間の増加 ・ 低価格化が進んだことによる利用者の増加（従量課金ユーザの乗り換え）	・ インターネットを利用した商取引の規模が拡大する ・ 行政サービスなどの対応も増加する ・ PC 以外の媒体からも利用が可能となり、利用がさらに促進される

表 3-2　ブロードバンド環境がもたらす影響

以上はブロードバンド回線を導入することでの利用者ベネフィットであるが、この利便性の高い通信インフラ上に安全な仮想的伝送路（VPN）を、利用者の自宅や外出先から企業内の VPN 機器につなぐことで、オフィスの省力化や移動コストの削減につながっていく。

しかし、具体的にどのようなアプリケーションを活用すれば生産性の向上に結びつくかを説明するまえに、利用上の脅威と注意点について解説したい。

3.3　ブロードバンド環境下での脅威（暗号化通信の重要性）

いままでで、ブロードバンドの利点について述べてきたが、便利な反面インターネットの危険についても今まで以上に増加しており、問題の内容についてもますます重大になってきており、そのままビジネスに利用できる環境ではない。

たとえば、通常インターネットに接続している PC が送受信するデータはクリアテキストであり、通信経路中にモニタリングツールを設置することにより簡単にやりとりの内容を盗み見ることができ、その上内容を書き換える事も可能である。

企業で扱っている情報は、上記のような脅威にさらされてよい性質のものではなく、高い機密性を必要とするものが大半を占めると思われる。

快適なブロードバンド環境をビジネスに生かすためにはインターネット VPN など、暗号化通信などを利用が必須である。

インターネット上の３大脅威	
盗聴	第三者が他人向けのメッセージを盗み見る行為。盗聴者は組織の内外双方ともに存在する可能性がある。また、内部犯行の方については犯行が露見される可能性が低い（対策が困難である）。 具体的な脅威については、個人情報など機密情報の外部漏洩である。
改ざん	ホームページに掲載している情報を書き換えられたり、送受信しているデータの内容を変更されたりする可能性がある。 具体的な脅威については、企業情報の書き換えによるイメージダウンにより甚大な損害を被る可能性がある。
成りすまし	不正アクセス手段として多く用いられる。実施に必要とされるスキルについてもあまり必要としない。 基本的にはアクセスする権限を持っている人物のふりをし、個人情報等の機密情報を盗み出す行為である。

表 3-3　インターネット上の脅威

3.4　インターネット VPN の効果

現状の企業活動をみると、業種によって差があるが、業務のかなりのパーセンテージをネットワーク化されたコンピュータ上で行っている。

たとえば現在ではビジネス上必須のコミュニケーションツールとなったインターネット・メールや、予定やワークフローをオンラインで行うグループウェア、さらに情報化が進んだ企業では営業活動を効率化する SFA や、経営の効率化を図る ERP、それらをすべて WEB 画面に組み込んだ企業ポータルなど、企業活動で必要な情報はすべてネットワーク上のデジタルデータとして取り扱う方向に進んでいる。

そのため、たとえば自社のオフィスにいなくても、安全かつ快適に社内の情報資源に接続出来る手段さえあれば、コストを削減したり生産性を向上させることが可能になる。

コスト削減
・休日出勤や過剰な残業の削減 ・外出先での業務処理 ・アドレスフリーなオフィス環境を実現し、固定費を削減 ※社外からのメール送受信やグループウェアの利用により実現可能
就労環境の向上
・在宅勤務などを推進でき、柔軟な雇用形態を実現 ・知的労働者については ※IP 電話やテレビ会議などの活用
情報共有の効率化
・社内の情報資源に外出先（自宅）から自由に接続出来る ・社内 WEB ポータル、SFA、CRM 等との連携によりさらなる業務効率を向上することが可能になる ※ ファイル共有・DB への VPN 経由の接続を許可することにより可能になる

表 3-4　インターネット VPN を利用した生産性の向上例

4 調査内容

4.1 調査対象公衆無線 LAN サービス

表 4-1 が今回の調査対象となった、公衆無線 LAN サービスである。表に示されているサービス内容は、調査を実施した 2002 年 10 月現在のサービス内容であり、現在のサービス内容とは異なる可能性があるので、実際に使用される場合は各サービス事業者にご確認いただきたい。

サービス	有料/無料
Yahoo!BB／Yahoo!JAPAN	試験サービス中(無料)
JR東日本	試験サービス終了
Mzone／NTT DoCoMo	有料
HOTSPOT／NTTｺﾐｭﾆｹｰｼｮﾝｽﾞ	有料
ネオモバイル／NTT Me	有料
@Mobile／@ベンチャー	無料
FREESPOT／FREESPOT協議会	無料

表 4-1 調査対象公衆無線 LAN サービス

4.2 調査内容と調査対象機器

今回の調査内容では、大きく「通信環境調査」と「VPN 通信調査」の 2 つに内容を分けた。

通信環境調査では、サービス提供者が使用するアクセスポイントと利用者が使用する無線 LAN カードの相性、利用者に割り当てられる IP アドレス、利用者を認証する方法の 3 つの内容を調査した。なお、アクセスポイントと無線 LAN カードの相性の調査では、Cisco AIRONET350 を使用して調査をおこなった。

次に VPN 通信調査では、各サービス提供スポットに表 4-2 に示す調査対象クライアントを持ち込み、実際に VPN 通信を行う形式で調査を行った。VPN 通信可否は、社内の特定のサーバと ping が行えることで判断を行った。また、実際にビジネスで使用するためには、ファイル転送などが行われるはずであるので、この点については、ftp を使用してクライアントから社内の ftp サーバへファイル転送の可否を確認する put テストと、社内からファイルを入手するための get テストを行った。

なお、各製品が調査の際に設定した IPsec のパラメータは表 4-3 の通りである。

メーカー	VPN ゲートウェイ	クライアントソフト
Checkpoint	VPN-1	Securemote, SecureClient
Cisco	VPN3000	VPN3000 Client
NetScreen	NS204	NetScreen Remote
SSH	IPSEC Express Toolkit	SSH Sentinel

表 4-2 調査対象機器

メーカ	Phase1	Phase2	圧縮	NAT対応	認証
Checkpoint	MM 3DES/SHA-1 DH-2	3DES/SHA-1 Tuunel DH-2	なし	独自(UDP2746)	ハイブリッド
Cisco	AM 3DES/SHA-1 DH2	3DES/SHA-1 Tuunel DH-2	あり	独自(UDP 10000)	PSK/Xauth
NetScreen	MM 3DES/SHA-1 DH-2	3DES/SHA-1 Tuunel DH-2	なし	NAT-T(UDP 500)	PSK/Xauth
SSH	MM AES/SHA-1 DH-2	3DES/SHA-1 Tuunel DH-2	なし	NAT-T(UDP 500)	PSH/Cert

表 4-3 使用 IPsec パラメータ

4.3 調査結果

4.3.1 通信環境調査結果

各サービスの通信環境調査結果を表 4-4 に示す。調査を実施する前に懸念していた無線 LAN カードとアクセスポイントの相性に拠る通信障害については、すべての公衆無線 LAN サービスにおいても発生する事はなかった。

次にクライアントに割当てられる IP アドレスだが、ほとんどのサービスが Private IP アドレスを使用しているが、キャリア系 2 社は Global IP アドレスを使用している。Private IP アドレスを使用してサービスを提供しているうち、Yahoo!BB と FREESPOT については複数のサービス提供スポットで調査を行った。その結果、同一のネットワークアドレスを使用していることが判明した。したがって、その他の Private IP アドレスを使用しているサービスにおいても同様である可能性は非常に高いと考えられる。

通信環境調査とは直接関係ないが、FREESPOT と@Mobile は、PS（Privacy Separator）機能を持つアクセスポイントを使用しているため、他人の通信内容がキャプチャできない特徴を持っている事が分かった。これは単純にインターネットに接続するだけの用途であっても、他人に通信内容を覗き見られる心配が無いのでユーザにとってはうれしい機能ではないかと思う。

サービス	相性	WEP	IPアドレス	認証方式
Yahoo!BB／Yahoo!JAPAN	○	64	Private	ブラウザ
JR東日本	○	64	Private	ブラウザ／MACアドレス
Mzone／NTT DoCoMo	○	64	Global	ブラウザ
HOTSPOT／NTTｺﾐｭﾆｹｰｼｮﾝｽﾞ	○	64	Global	ブラウザ
ネオモバイル／NTT Me	○	64※	Private	MACアドレス
@Mobile／@ベンチャー	○	なし	Private	なし
FREESPOT／FREESPOT協議会	○	なし	Private	なし

相性：○はCisco AIRONET350で接続可能

WEP：※はWEP無しを選択することも可能

表 4-4 通信環境調査結果

4.3.2 VPN 通信調査結果

始めに VPN 通信の結果については、各サービス提供者の結果を実名入りで公表するのは差し控えさせていただく。これは、今回の調査は JNSA 独自で行ったものであり、各サービス提供者への配慮であるとお考え頂きたい。

すべてのサービスにおいて、すべての製品で VPN 通信が可能であることが確認されたのと同時に、VPN 通信が可能であれば、クライアントから社内のサーバに対するファイル転送も可能であることが結果から分かった。しかし、社内からのファイル転送は、製品とサービスにより異なる結果が得られた。これらの原因と対応策については、公衆無線 LAN で VPN を実現するための問題点と注意事項出説明する。

また、下表からはすべてのサービス提供スポットで VPN 通信が可能なように見える。しかし、FREESPOT はサービス提供スポットによってアクセス制御の設定が異なっており、実際には VPN 通信が出来なかったスポットもあったので注意していただきたい。

	Checkpoint			Cisco			NetScreen			SSH		
サービス	ping	put	get	ping	put	get	ping	put	get	ping	put	get
A社	○	○	○	○	○	○	○	○	○	○	○	○
B社	○	○	○	-	-	-	○	○	○	○	○	○
C社	○	○	○	○	○	○	○	○	○	○	○	○
D社	○	○	○	○	○	○	○	○	○	○	○	○
E社	○	○	○	-	-	-	○	○	○	○	○	×
F社	○	○	○	○	○	○	-	-	-	○	○	○
G社	○	○	×	○	○	○	○	○	×	○	○	○

×：失敗

ー：未調査

失敗の原因(SSH)：試験実施時の ftp サーバ側の DF ビットの設定が 0 だった為。

表 4-5 VPN 通信調査結果

5 リモートアクセス VPN を導入する際の注意事項

5.1 認証に関する問題

IKE の認証には Pre-Shared Secret とデジタル証明書の 2 つの方式が RFC で定義されている。認証に関する問題として、Phase1 の認証のためのデータが大きい場合、正常に認証が行えないということがある。このような問題は証明書での認証の場合に CRL（Certificate Revocation List 証明書失効リスト）が大きい場合や、認証に用いる証明書が大きい場合などで起こりやすい。認証データが 1 パケットに収まらない場合、VPN ゲートウェイまたは VPN クライアントは 1 メッセージとして認証データを送信するためにフラグメント化された UDP パケットを生成する。クライアントが NAT デバイスの背後にいる場合などで NAT デバイスがフラグメントされたパケットを扱えない場合、正常にネゴシエーションが行えない。この様な問題の対策として IKE の代りに TCP を用いた独自の鍵交換を行う実装が存在している。TCP によるオーバーヘッドを考慮する必要があり、あくまでも製品の実装依存になるが、これによりフラグメント化の発生を防ぐ事が可能となる。

また、IKE のペイロードで証明書や CRL そのものを直接交換するのではなく、それらにアクセスするための URL を交換する方法が考えられる。この場合はパケットサイズが大きくならない為フラグメントが発生しない。ただ、この様な仕様や実装は今のところ無いと思われる。

5.2 NAT に関する問題

IPsec には AH・ESP・IPCOMP などがあるが、AH ではパケットの認証（データの改ざんを防ぐ）のみ実装しているのに対して ESP はデータの暗号化と認証の両方を合わせ持つので、一般的には ESP が使われている。また、ESP でもトランスポートモード・トンネルモードの 2 つが存在するが、トランスポートモードでは IP ヘッダは変化せずそのまま利用するため、VPN ゲートウェイの内側のプライベートアドレスへのアクセスには利用できない。ESP トンネルモードでは元のパケットを IP ヘッダごと暗号化するので送信元・宛て先ともにプライベートアドレスであっても問題はない。よって一般的には VPN リモートアクセスソフトでは ESP のトンネルモードを採用しているものが最も多い。

このように、IPsec には AH/ESP/IPCOMP、トンネルモード/トランスポートモードという複数の組み合わせが存在するが、さらに NAT にも 1 対 1 の NAT と IP ヘッダだけでなく TCP や UDP のソースポートアドレスも変換する 1 対多の NAPT（Network Address Port Translator。IP マスカレードともいう）がある。これらの組み合わせによっては、経路上に NAT デバイスがあるとうまく通信できない。

これは NAT によるアドレスの書き換えが、IPsec での改ざんと見なされてしまっ

たり、ソースポートアドレスの変換を伴う NAPT に対応できなかったりするためである。このような問題を包括的に解決する手段として現在 NAT-Traversal と UDP encapsulation という下記のインターネットドラフトが提案されている。二つのドラフトを実装することにより、問題の解決が行われている。

http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-06.txt
http://www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-06.txt

今回は一般的に最もよく使われる ESP トンネルモードと NAPT の組み合わせについて考えてみる。

ESP トンネルモードではそのままでは NAPT はできない。ESP ではトンネルモード、トランスポートモードにかかわらず元のパケットの TCP や UDP のヘッダは暗号化されており NAPT で用いられているそれらのソースポートアドレスの書き換えが行えない為である。先述した NAT-Traversal / UDP encapsulation を利用することにより、IP ヘッダの直後に UDP ヘッダを挿入してカプセル化を行い、NAPT のポート変換を可能にすることができる。ただし、これらのカプセリング技術は VPN ゲートウェイと VPN クライアントソフトの両方で対応している必要がある。このカプセル化には NAT-Traversal では IKE と同じ UDP500 番が使われるが、製品によって全く異なるポートを使うものもある。経路上にこの UDP カプセリングで使うポートをふさぐようなデバイスがある場合、使用ポートを開ける必要がある。

製品名/メーカー名	鍵交換方式	カプセル化使用ポート
CheckPoint VPN-1	IKE または独自(TCP)	UDP 2746(または任意)
Cisco VPN3000	IKE または独自(TCP)	UDP 10000 / TCP 10000
SSH	IKE	UDP 500/4500(または任意)
Netscreen	IKE	UDP 500

表 5-1 UDP カプセリングのポート番号

NAT-Traversal は、Phase1 の最初の 2 つのメッセージでお互いが NAT-Traversal 対応であることを知らせる。両者が NAT-T 対応であった場合、Phase1 の 3 番目と 4 番目のメッセージで NAT-D（NAT-Discovery)ペイロードに「始点 IP アドレス/ポート番号」「終点 IP アドレス/ポート番号」をハッシュしたものをセットして、互いに送信する。受信した方は NAT-D ペイロードの中のハッシュと実際の IP アドレス・ポートのハッシュを比較して NAT の有無を検知する。始点 IP アドレスの方のハッシュが実際のものと違っている場合は、相手が NAT デバイスの後ろにいることがわかる。また終点 IP アドレス側のハッシュデータが違っている場合は自分の手前に NAT するデバイスがあることがわかる。NAT される場所を知ることは、VPN のキープアライブを送信する上で重要になる。なぜなら VPN キープアライブは

NAT 背後にいるクライアントへ向かっては送信できないので、必ず NAT 背後のクライアントから送信されなくてはならないからである。

NAT が検出されれば、あらかじめ決められたポートで（通常は UDP500 番ポート）で ESP をカプセル化する。UDP でカプセリングを行うことにより、送信元 IP ヘッダ・送信元ポートが変わっても通信が可能になる。なお、NAT-Traversal は現在 RFC での標準化が進められている。

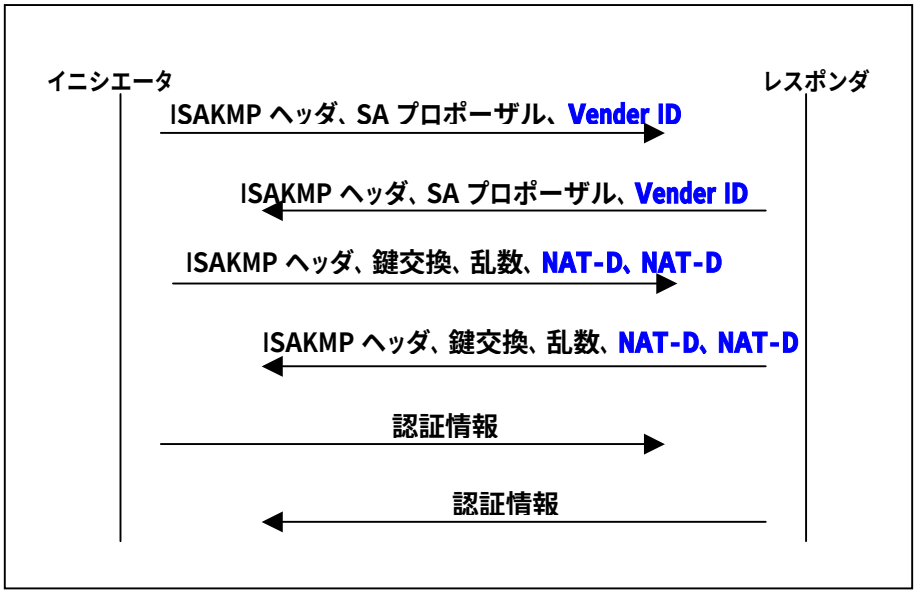


図 5-1 NAT-Traversal 時の IKE メインモード

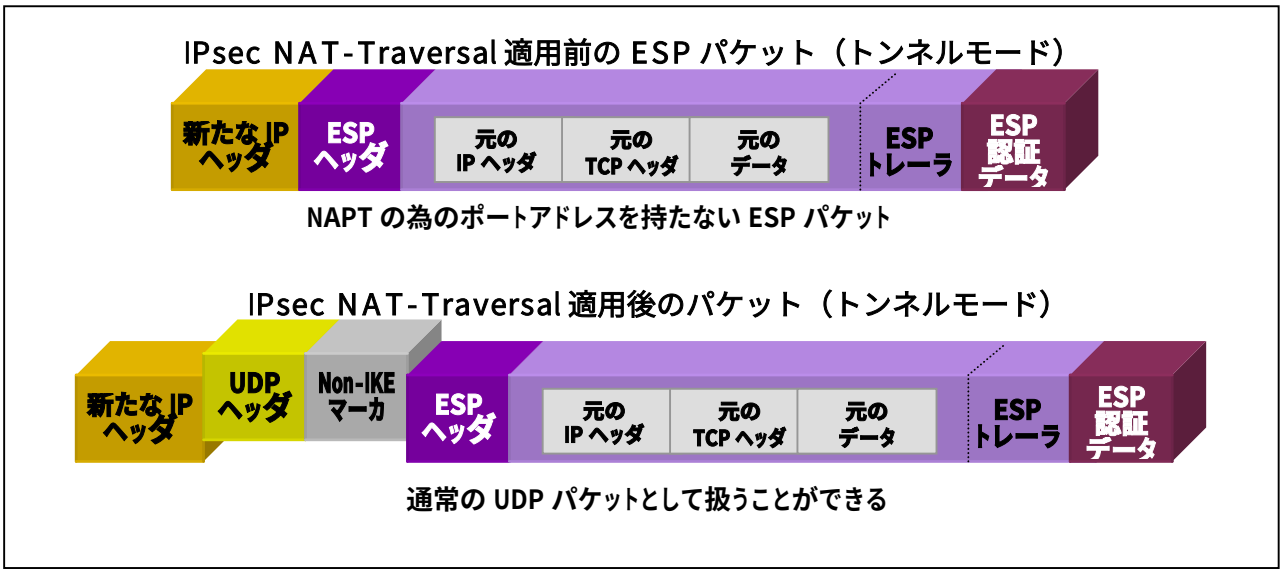


図 5-2 NAT-T パケット

5.3　アドレス重複に関する問題　その 1

商用の無線アクセスポイントサービスなどでは、すべてのアクセスポイントで同じサブネットアドレスを使っている場合がある。そのような場合、異なるユーザでありながら、同じ IP アドレスを持つ可能性がある。例えばアクセスポイント A に 192.168.0.1 のユーザ A がいるが、アクセスポイント B にも同様に 192.168.0.1 のユーザ B がいるような場合である。すでにユーザ A が IPsec SA を確立して VPN で通信しているところに新たにアクセスポイント B の同一 IP アドレスのユーザ B が同一の VPN ゲートウェイにアクセスしてくると、VPN ゲートウェイの IPsec SA が上書きされてしまい、もともと接続していたユーザ A の通信が途切れてしまうという問題等が発生する可能性がある。このような場合の回避策として、VPN ゲートウェイによっては、割り当てる IP アドレスをプールしておきクライアントが接続してきた時点で VPN のための新たな IP アドレスを割り振ることができる。

このように、クライアント側に実インターフェースとは別に仮想インターフェースを設け、これに対してそれぞれユニークなアドレスを割り当てることにより、この問題の解決を行うことが可能である。アドレスの割り当て方法については上記のように静的にプールされたアドレスから割り当てる方法、マニュアル(クライアント側で静的に割り当てる)定義の他に IPsec-DHCP や、ISAKMP Configuration Method(mode-config)などが挙げられる。

IPsec-DHCP については下記 URL から RFC が参照できる。

http://www.ietf.org/rfc/rfc3456.txt　(draft-ietf-ipsec-dhcp-13.txt)

※なお、現在 IKE の次期バージョンとして IKEv2 の標準化が進められているが、IKEv2 では DHCP over IKE というドラフトが提案されている。DHCP over IKE では Phase1 の中で DHCP を利用する方法を定義している。資料については下記から参照できる。

http://www.ietf.org/internet-drafts/draft-ietf-ipsec-dhcp-over-ike-00.txt

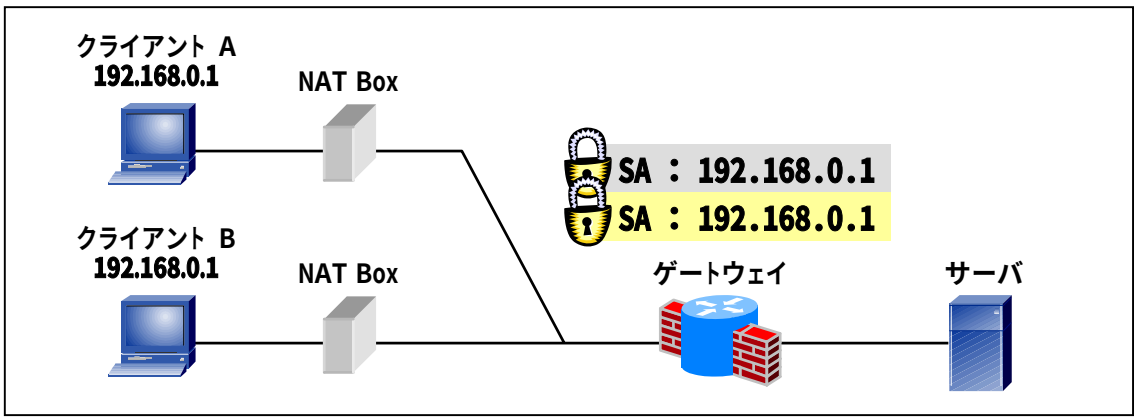


図 5-3 クライアントアドレス重複

VPN 接続する場合自動的に社内の DHCP サーバから IP アドレスをもらいたいということもあるだろう。IPsec-DHCP を利用することによって直接 社内の DHCP サーバから IP アドレスを割り当ててもらうことが可能になる。

IPsec-DHCP では IKE の Phase1 が確立したのちに、クイックモードで一時的な DHCP 用の SA を作成する。この時クライアントは ID として IP アドレス 0.0.0.0 ／プロトコル ID=UDP／ポート=67 を使用し、一方 VPN ゲートウェイは ID としてゲートウェイの IP アドレス／プロトコル ID=UDP／ポート=68 を使用する。このようにセットすることにより、プロトコルやポートを制限し DHCP でのみ使用できるようになる。クライアントはこのトンネルを使って DHCP 要求を VPN ゲートウェイに送信し、VPN ゲートウェイはイントラネット内の DHCP サーバに対して DHCP リレーを行う。DHCP のネゴシエーションが終わったら DHCP SA は削除され、クライアントは DHCP サーバから割り当てられた IP アドレスを ID として、改めて Phase2 の折衝が始まる。

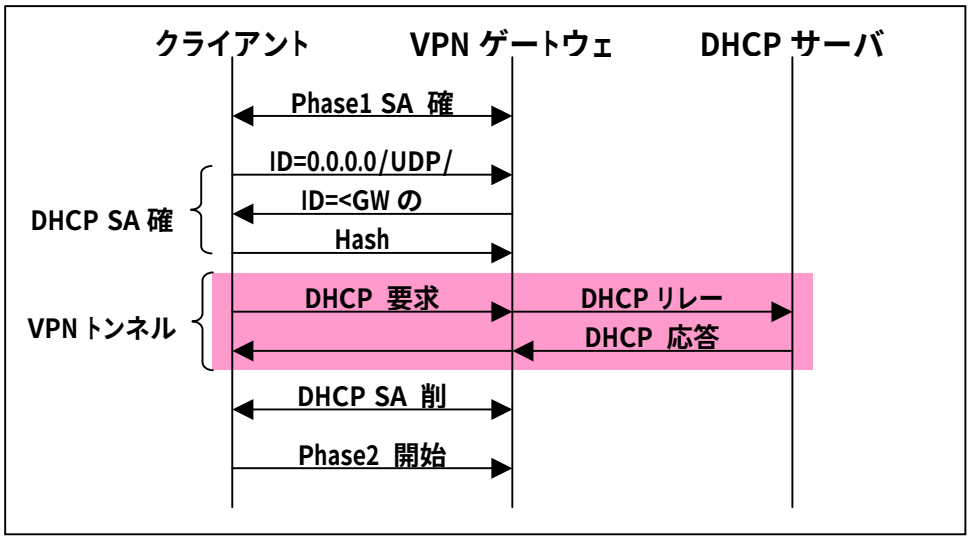


図 5-4 IPsec-DHCP ネゴシエーション

このようなアドレス割り当てが行われる場合、クライアントは VPN ゲートウェイとの接続には実インターフェースに割り当てられたアドレスを使用し、暗号化されるパケットの送信元 IP アドレスには、仮想インターフェースに DHCP サーバから割り当てられた IP アドレスを使用する。また、mode-config では直接 DHCP サーバとやりとりすることはなく、やはり Phase1 の確立後に ISAKMP_CFG_REQEST メッセージと ISAKMP_CFG_REPLY メッセージをクライアント－VPN ゲートウェイ間でやりとりすることによって VPN ゲートウェイから IP アドレス・サブネットマスク・DNS 情報を取得する。商用の VPN ゲートウェイ・クライアントソフトではこれらの機能を備えているものが多い。

これらをうまく利用することによりクライアントの IP アドレスの重複を防ぐことができ、社内のセキュリティゲートウェイで IP アドレスによる制限をかけてい

る場合であってもリモートアクセスのクライアントのためにポリシーを追加・変更する必要がなくなる。

5.4 アドレス重複に関する問題 その 2

リモートクライアントが、ブロードバンドルータの内側にある時などでクライアントのネットワークアドレスと、VPN ゲートウェイの内側のネットワークが同じアドレスを使っている場合、VPN 接続はできない。例えばクライアントが 192.168.1.x という IP アドレスを持っており、同じく 192.168.1.x という VPN ゲートウェイの内側のネットワークアドレスへ通信しようとしても、ローカル側の内部ネットワークと通信しようとしてしまい、パケットが VPN ゲートウェイへ送信されないということが起こる。このような問題についての根本的な解決策は現在存在しないので、VPN ゲートウェイ内の VPN でアクセスされるネットワークをなるべく使われにくいプライベートアドレスにし、バッティングが起こらないようにするほかない。リモートアクセスでは、場所によって様々な IP アドレスが割り当てられるため、必ずバッティングがないようにするということはできないが、なるべくそのような可能性のないようなネットワークにしておくことは有効である。公衆無線アクセスポイントの利用を考えるならば、無線アクセスポイントのサービス業者がどのようなネットワークアドレスを使っているかを予め調査しておくほうが良いだろう。なお、今回実際に無線アクセスポイントの調査を行った結果、192.168.x.x というアドレスを使っているところが多かった。ダイヤルアップで直接グローバル IP アドレスを持つような場合は、このような問題は起こらない。

5.5 IPsec パケットをハンドリングできないデバイスの問題

ブロードバンドルータにはフィルタリング機能がついているものが多いが、TCP/UDP しか制御できないものがあり、ESP プロトコルを許可することができないものもある。このような場合はフィルタリング機能を無効にするか、もしくは ESP を許可できるようなブロードバンドルータを用意する必要がある。このような機能は IP パススルーまたは VPN パススルーなどと呼ばれている。また、VPN ゲートウェイとクライアントで NAT-Traversal を使うようにすれば UDP500 番ポート・UDP4500 番ポートを許可するようにすればよい。また、UDP encapsulaion で他のポートを使う場合も同様にして対応するポートを開ける。いずれにしても VPN ゲートウェイとクライアントがどのようなポートを使用して IPsec を実現しているかを予め調査しておくことはトラブル時の切り分けに有効である。

クライアントにパーソナルファイアウォールがインストールされている場合、これがポートを塞いでいることがある。商用パーソナルファイアウォールでは VPN

（ESP パケット）を考慮して作られているものはまだ少ないようである。しかし多くのパーソナルファイアウォールでは TCP / UDP でのポートの許可が行えるので、回避策としては前項に述べたとおり、NAT-Traversal・UDP encapsulation を使って UDP での制御にするなどが有効である。しかしながらパーソナルファイアウォールと VPN リモートアクセスの両方を実現したいのであれば、VPN クライアントにパーソナルファイアウォールがついているものを選択するほうが、パーソナルファイアウォールが制御できるプロトコルと VPN クライアントの利用するプロトコル/ポートの組み合わせを考慮しなくて済むので、ユーザにとっては混乱が少なくスムーズに導入できるというメリットがある。

5.6　フラグメントの問題

通常のパケットを IPsec のパケットにする場合には新たに IPsec 用のヘッダが追加されるのでパケットのサイズが大きくなる。トンネルモードを利用する場合には IP ヘッダも新たに付け加えられるので、さらに大きくなる。この様な場合の対策として大きく分けて２つの方法がある。この様な場合の対策として大きく分けて２つの方法がある。

(i) パケットの分割(フラグメント)を行いそれぞれのパケットのサイズが MTU の大きさに収まる様にする。
(ii) そのパケットを送信したホストにパケットのサイズを小さくする様に伝え IPsec のパケットにした後でも MTU のサイズに収まる様にする。

まず最初に最も単純なリモート VPN 試験環境でこの問題を考える。

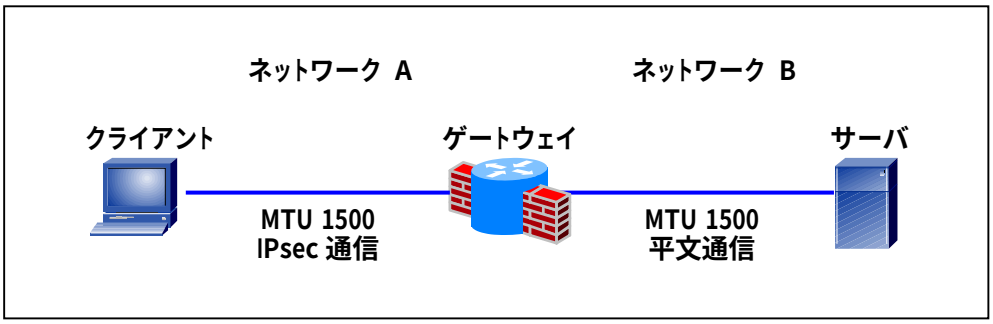


図 5-5 単純なネットワーク環境

ここでは図の通りクライアントとゲートウェイ間では IPsec の通信が行われており、ゲートウェイとサーバ間は通常の平分の通信が行われているとする。つまりネットワークＡをインターネット、ネットワークＢをイントラネットと見立てている。
例えばクライアント／ゲートウェイ間で IPsec 通信を確立後クライアントからサ

ーバにログインしなにかしらのデータをダウンロードする場合を考えてみる。サーバが小さなパケットを送信する場合、ゲートウェイがそれを IPsec パケットにした後でも MTU のサイズを越えることがないので問題は発生しない。しかし、サーバが 1500 バイトのパケットを送信した場合、それを IPsec のパケットにすると必ずパケットのサイズが 1500 バイトを越えるので、MTU に収まらないという問題が発生する。

この時、元のパケットの DF ビット(Don'tFragment ビット)が 0 の場合、パケットの分割が許可されていることからゲートウェイは IPsec 化を行い、その後パケットの分割を行いクライアントに送出する。

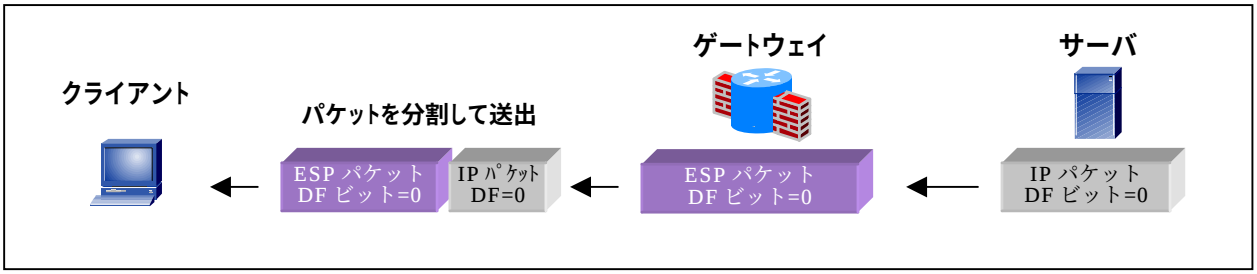


図 5-6 パケットの分割

また、元のパケットの DF ビットが１の場合、それを分割することが許されないので、送信者のサーバに ICMP のメッセージを送りパケットを小さくして送出させる様にする。それを受け取ったサーバはサイズを小さくし再送を行う。その結果 IPsec 化しても MTU サイズを越えることはなく、そのパケットはクライアントまで無事に到達する。

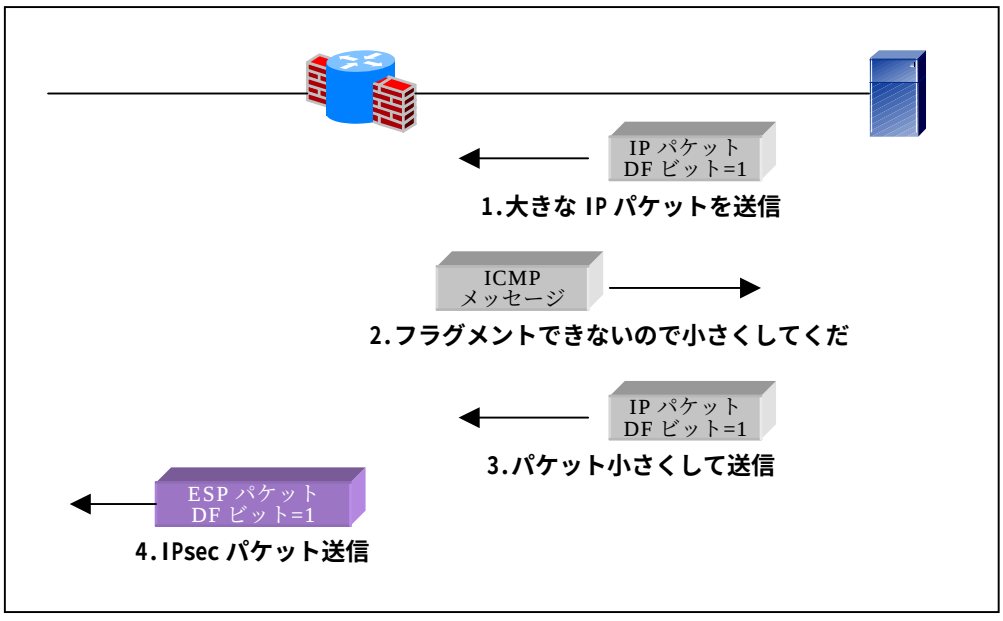


図 5-7 ICMP によるパケットサイズ調整

また、ゲートウェイが DF ビットをどの様に扱うかという点も考慮にいれる必要がある。設定や仕様によって異なってくるが以下の動作が考えられる。

(1) ゲートウェイが DF ビットの値を書き換える動作

- DF ビットが 0 または１のパケットを受け取った場合、それを IPsec 化する際常に DF ビットを 0 とする。
- DF ビットが 0 または 1 のパケットを受け取った場合、それを IPsec 化する際常に DF ビットを 1 とする。

(2) ゲートウェイは DF ビットの値を書き換えず元のパケットに従う動作

- DF ビットが 0 のパケットを受取った場合、それを IPsec 化した後も DF ビットは 0 とする。
- DF ビットが 1 のパケットを受け取った場合、それを IPsec 化した後も DF ビットは 1 とする。

なぜサーバ側で DF ビットが０だったり１だったりするのか？これはサーバとして使われているＯＳの設定に依存している。それぞれのＯＳの初期設定は我々グループで独自に調べてみる限り下記の通りであった。

OS	設定箇所	初期値
FreeBSD	net.inet.tcp.path_mtu_discovery	1
Windows NT/ 2000	[HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥Tcpip¥Parameters] EnablePMTUDiscovery	1
Linux	net.ipv4.ip_no_pmtu_disc	1
NetBSD	net.inet.ip.mtudisc	0
MacOS X	net.inet.tcp.path_mtu_discovery	1

表 5-2 各 OS の DF ビットのデフォルト設定

この設定を変更する事によってサーバが送出するパケットの DF ビットの状態が変わることが確認できた。

次に、実際の環境でこの問題について考えてみる。
実際の環境では、通常クライアントはインターネットを越えてゲートウェイにアクセスを行ってくる。インターネットでは途中の経路で MTU のサイズが異なって

いるケースが多々ある。またゲートウェイの背後には複数のサーバがありゲートウェイはこのことにも対応して振舞う必要がある。

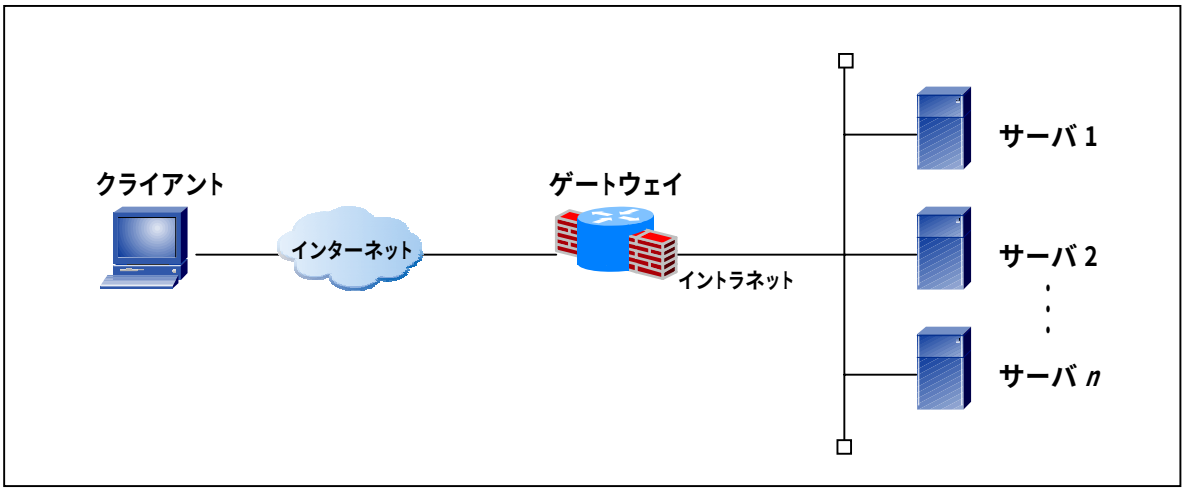


図 5-8 複数サーバ環境

元のパケットの DF ビットが 0 の場合、通常パケットは分割されてインターネットへと送出される。この場合途中の経路のルータ、NAT 装置、ファイアウォールなどがそのフラグメント化されたパケットを正しく扱える必要がある。更に必要があれば途中の経路で更にフラグメントを行う必要もでてくる。ここで途中の経路に一つでもフラグメントされたパケットが正しく扱えない様な、もしくはフラグメントされたパケットの通過を許可していない装置があれば、サーバからのパケットはクライアントまで届かず、結果的に通信が行えない状況が発生してしまう。

元のパケットの DF ビットが 1 の場合、試験環境の場合と同様 IPsec 化した後に MTU のサイズを越える場合には ICMP のメッセージをゲートウェイがサーバに対して送信して対応する。ただ上記の試験環境と実際の環境では異なってくる点として、ゲートウェイが送出した IPsec パケットに対してインターネット上のルータからさらにパケットサイズを小さくする様に通知が送られてくる場合がある。ゲートウェイはこれにも対応する必要がある。またこの場合は原因となったパケットを送出したサーバを特定する必要もある。

この一連の流れを下図で説明する。

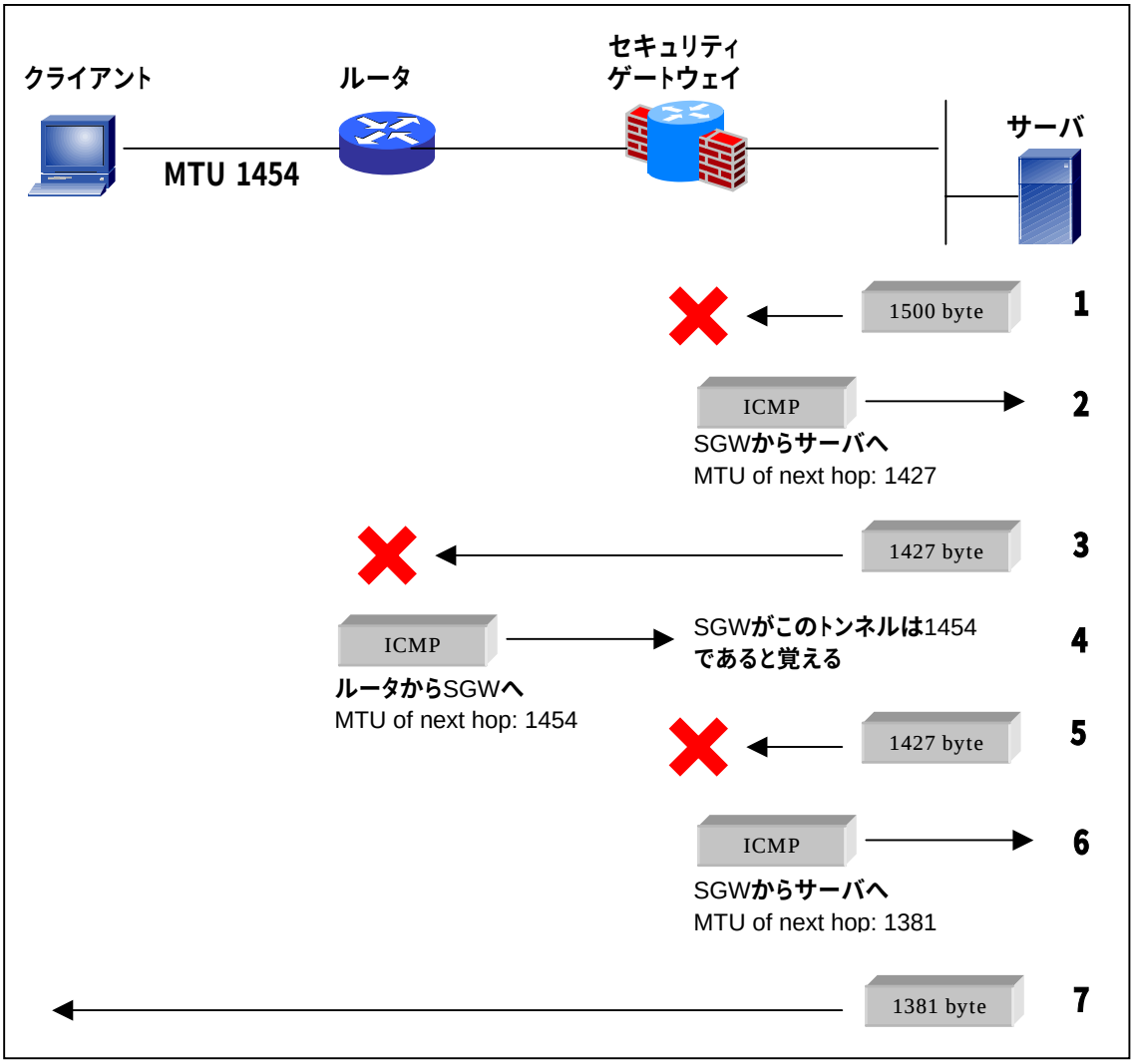


図 5-9 複数サーバ環境下のパケットサイズ調整

1．サーバから DF ビットが１で１５００バイトのパケットが送出される。しかし SGW はこれを IPsec のパケットにすると MTU サイズを超えてしまうので送出できなくなる。

2．SGW は１、を回避する為にサーバに対して ICMP のメッセージを送信してパケットのサイズを小さくさせる。

3．サーバは SGW からの ICMP を受けてパケットサイズを小さくして再送する。SGW はこれを IPsec のパケットにして送出する。この時も DF ビットは元のパケットに従い１となっている。

4．インターネット上の MTU が小さくなっている箇所のルータがこの IPsec パケットを先のネットワークに対して送出できないので、SGW に対してパケットを小さくする様 ICMP のメッセージを送信してくる。SGW はこの ICMP を受けてこの経路に対しての MTU を記録する。

5．サーバは次のデータを SGW に送出してくるが、これの宛先が先ほどの MTU が小さくなっている経路であることを事前に確認できる。

6．SGW はサーバに対してさらにパケットサイズを小さくする様に ICMP のメッセージを送信する。

7．サーバはこの ICMP を受けてさらにパケットサイズを小さくして送出し、このパケットは最終宛先のクライアントまで到達する事が可能となる。

この一連の ICMP メッセージの働きは PMTU ディスカバリーとして知られている。ここでは次の様な ICMP が用いられている。

ICMP [type 3 subtype 4, ICMP_UNREACH_NEEDFRAG, MTU of next hop: 数値]

また通常 PMTU ディスカバリーを動作させるには DF ビットが１である必要がある。

その他の対処方法として次の様な対策が考えられる。

VPN 経由でアクセスされると予め分かっているサーバは予め MTU を下げフラグメントされない様にする。

これは非常にシンプルな対策だが PMTU ディスカバリーが ICMP の通信を前提にしている以上ICMP の通信が許可されていない様な環境では有効な手段と言える。ただあまりサーバの MTU サイズを下げすぎるとパフォーマンス上問題が発生してくる。現在広く用いられている PPPoE 回線業者などの MTU 値を考慮にいれると 1380 バイト付近が妥当な値ではないかと考えられる。

今まではサーバからクライアントに送信する場合を考えてきたが、実際に通信を行うには当然その逆方向、すなわちクライアントからサーバへの通信も考える必要がある。

VPN クライアントの仕様に依存するがバンプインザスタック（OS の IP 機能に IPsec の機能を後から追加する方式）のクライアントソフトウェアの場合、基本的な動作の流れとしては次の様になる。

自分自身が送出するパケット(OS から送出されたパケット)が 1500 バイトで、IPsec 化した後、MTU サイズをオーバーして送出できない状況になった場合、クライアントソフトウェアがローカルスタック(自分自身の OS の IP 層)に内部的に ICMP を送ってパケットサイズを調整させる。

このように、フラグメントの問題については PMTU でパケットサイズを調整するアプローチと、予めサーバやクライアントの MTU を小さくするアプローチがあるが、どちらも完全な解決策ではない。PMTU については VPN の経路上のデバイスすべてにおいて PMTU-Discovery を扱えるようにしておく必要があり、なおかつ DF ビットが 1 のパケットでないと実際に PMTU によるサイズ調整は期待することができない。一方 MTU を手動で下げる方法は間違いのない方法ではあるが個々に設定を行う必要があり、手間がかかる。しかしながら本来 VPN 経路上のすべてのデバイスがフラグメントされたパケットも扱うことができれば通信できないという問題は起こらない。経路上のすべてのデバイスをチェックすることは困難だが、ユーザ側でブロードバンドルータなどを置く場合はフラグメントパケットを通すこと

のできるものにする、また企業内のルータ等においては PMTU を通すように予め設定しておくなど、できるだけの注意を払っておくべきである。

5.7 内部 DNS の参照に関する問題

通常インターネット接続されたクライアントは ISP から取得した情報に基づいて自分の参照する DNS サーバを決定する。その後 IPsec ゲートウェイとの間に VPN トンネルを張った後もクライアントの参照する DNS サーバの設定はそのままであるので VPN ゲートウェイ内の Internal DNS を参照することはできない。また、DNS のクエリは VPN の対象にはなっていないことが多く、Internal DNS へ IPsec の処理をせずに送ろうとしてしまうため、結果として Internal DNS にパケットが届かず、参照できないということが起こる。つまり、通常のインターネットへのアクセスには ISP から取得した DNS サーバを参照し、VPN ゲートウェイの内部ホストへアクセスする場合には、DNS クエリを IPsec で処理し、VPN トンネルを通ってイントラネット内の名前解決が可能な DNS サーバを参照するようにしなくてはならないということである。

これらの具体的な設定方法はそれぞれのクライアントソフトウェアのマニュアル等に譲ることとする。

6 考察

6.1 接続環境・サービスについて

検証結果から見て取れるように、公衆無線 LAN サービスを利用した VPN 接続に関しては、ほぼ実用的なレベルに達しているものと思われる。VPN の接続性やスループットもとりわけ問題はない。ただ、サービススポットによっては、電波の入りが弱くインターネットへ接続できないケースや、椅子や机が整備されていないため長時間の利用に耐えられない場所があるなど、事業者側に改善を要望したいと思われるケースがいくつかみられた。今後、アクセスポイントの増強や環境整備などを通じ、サービスレベルの向上に期待したいところである。

複数の公衆無線 LAN サービスを利用する場合、接続時の認証情報を事業者ごとにセットアップしなければならず、不便に感じることがある。一つのサービス事業者が提供しているエリアが広ければさほど問題とならないが、現在のように、提供しているエリアが一部に限られている場合、どうしても複数のサービスを利用しなければならないケースも出てくる。今後、事業者間でのローミングサービスや、プリペイド課金の導入など、利用者が手軽に利用できる環境が整備されることを期待したいところである。

6.2 VPN 利用における留意点

VPN に限ったことではないが、リモートアクセス環境を構築するためにはユーザを認証するための仕組みが必要である。VPN(IPsec)では、一般的に Pre-Shared Secret 認証を利用するが、リモートアクセスユーザを認証する場合には不十分な場合もある。そのため、XAUTH や Hybrid Auth といったパスワードベースの認証やデジタル証明書を利用した認証を利用することが期待される。

XAUTH は IKE において認証方式を拡張する規格で、パスワード認証やワンタイムパスワード認証が利用できる。また、RADIUS 認証を利用できるようになるため、既存のダイアルアップサーバと認証アカウントを統合することも可能となる。
Hybrid Auth も XAUTH と同様認証方式を拡張するものだが、VPN 機器は証明書、クライアントはパスワード認証といったように、認証方式を切り替えることができるのが特徴である。

デジタル証明書で認証を行えば、パスワードで認証を行った場合に比べ、セキュアな環境を構築できる。デジタル証明書認証では、CA（認証局）から発行された証明書と対になる秘密鍵が必要であるため、パスワード認証に比べなりすましが格段に難しい。また、証明書を PC に直接インストールせず IC カードや USB トークンなどに保存しておけば、ハードデバイスを利用した本人認証を行うことが可能となるため、より強固な認証が行える。ただし、CA の構築はより多くの費用と労力を

必要とする。そのため、自社で CA を構築することが難しい場合は、証明書発行をアウトソースすることも検討材料となるであろう。デジタル証明書は、ユーザの認証にとどまらず、アプリケーションのアクセスコントロールにも利用できるため、PKI によるシングルサインオンの実現などそのメリットは大きいと思われる。

公衆無線 LAN サービスでは多くのアクセスポイントが Private IP アドレス環境で構築されていた。Private IP アドレス環境から NAT(NAPT)を経由して VPN を利用するには、5.2 で述べたが NAT-Traversal / UDP encapsulation が必要である。このことから、公衆無線 LAN サービスからの VPN 接続を想定する場合、NAT-Traversal / UDP encapsulation に対応した環境が構築できるかどうかがカギになるものと思われる。

公衆無線 LAN サービスを利用している場合、アドレス重複問題に対しても十分注意しなければならない。このことは、クライアントに対して Private IP アドレスを割り振る事業者が大半であること、アクセスポイントから割り振られる IP アドレスが、各アクセスポイント共通のアドレス体系で割り振る事業者があることなど、その影響は顕著に現れるものと思われる。そのため、5.3 で述べたとおり、仮想インターフェースにユニークな IP アドレスを割り振ることによりアドレス重複を回避する方法が望ましいと思われる。

サーバ側の環境にも留意が必要な点がある。5.6 で述べたが、パケットのフラグメントが起きたときに、通信できない場合がある。今回の調査では、フラグメントされたパケットが NAT デバイスで落とされてしまい、通信できない場合があった。フラグメントに対する対策として、サーバ側の MTU を小さくしておく、ICMP の PMTU を有効にしておくといった対策が必要と思われた。

クライアントのデスクトップセキュリティに関しても留意が必要である。PC へのウィルス感染や社内システムへの蔓延を防止するため、ウィルス対策ソフトを導入したり、データの盗難や踏み台攻撃などの不正アクセスを防止するために、パーソナルファイアウェールを導入することは有効な対策になる。ただし、パーソナルファイアフォールの導入は、設定によっては VPN で必要な通信ポートを閉じてしまう場合があるので、注意が必要である。

今回の調査では、IKE や NAT-Traversal / UDP encapsulation で利用されるポートをフィルタリングしているようなケースは見られなかった。ただ、アクセスポイントによっては、パケットフィルタリングができる機器もあり、決められたポートしかあけていないアクセスポイントもあるかもしれない。もし、パケットフィルタリングなどにより、IKE や NAT-Traversal / UDP encapsulation が利用できない環境があるならば、SSL や SSH による VPN を利用することも有効な手段であると考えられる。

6.3　ブロードバンドを利用する際の脅威

IPsec を使用した VPN によって、ネットワークのセキュリティは保たれた。しかしながら、ネットワークがセキュアであっても、使い方一つでアンセキュアなネットワークになってしまう。ここでは、人的要因の問題点を検討する。

6.3.1 ウィルス

外部でウィルス感染した PC を用いて VPN 接続した場合、簡単に社内ネットワーク中に感染してしまうだろう。例えば、インターネットとのゲートウェイのみウィルス対策を施して、社内のクライアント PC に対して無防備な場合である。特にワーム系のウィルスに感染してしまった場合、1 台ずつ駆除していかなくてはならないので、注意が必要だ。VPN 接続前には、必ずウィルスチェックを行いたい。

6.3.2 盗聴・盗撮

パスワードの管理は重要である。当たり前のことだが、人に話したり、紙に書いたりしてはいけない。どこで誰が聞いているかなどわからないので、人前でパスワードについて話してはならない。さらに、パスワードをデスクトップの付箋紙のようなものに書き留めておくのも厳禁だ。前述のウィルスの中には Key Logger のように、文字を入力する動作をすべて記録するような盗聴ソフトも存在するので、さらに注意が必要だ。ネットカフェの PC に Key Logger を仕掛けておき、オンラインバンキングで多額の現金を送金した事件があったのは記憶に新しい。また、どこでビデオカメラが回っているかもわからないので、パスワードの入力時にも注意が必要だ。最近のデジタルカメラの小型化や、携帯電話のカメラ機能の高性能化は目覚しいため、簡単に撮影することができてしまうだろう。

6.3.3 盗難・紛失

NotePC は持ち運びが便利な反面、高価であるため盗難の被害が多い。また、NotePC と言えどもそれなりの大きさがあるにもかかわらず、紛失の被害も多い。「盗まれてしまったからしょうがない」とか、「無くしたのだからしょうがない」というわけには行かないだろう。なぜならば、NotePC に残っている情報から、何をされるかわからない。従って、使っていた人のアカウントを一時的に削除する、パスワードを変更するなどの対策が必要になってくる。

例えば、クレジットカードを紛失したとしよう。盗まれたと気づいた時点で、クレジットカード会社に連絡し、クレジットカードを無効にしてもらうだろう。NotePC であってもクレジットカードと同じように考えるべきである。盗難や紛失

という事態に備えて、どのような報告が必要か、どのような対応が必要かをあらかじめ決めておき、事前に徹底する必要があるだろう。

6.3.4 廃棄

廃棄する際も気をつけなければならない。先日も、市役所の所員が廃棄したNotePC が拾われ、中から住民の個人情報が出てきたという話があった(そもそも、個人情報を NotePC にコピーできる(している)時点でセキュリティ上の問題があるようにも思われるが)。廃棄には専門の業者を手配するなどの配慮が必要である。

6.3.5 機密情報漏洩

外出先や自宅から VPN で社内ネットワークを利用できるようになった場合、すべての社内リソースが利用できてよいものだろうか。確かに通信自体はセキュアだが、社外秘の資料まで利用できて良いだろうか。やはり、社外秘情報のサーバを用意し、VPN ではアクセスできないような制限が必要だろう。または、接続ユーザによってアクセスできる権限を段階的に変えるなどの工夫をすることにより、よりセキュリティが高まる。

6.3.6 取引先や提携先

取引先や提携先などは、比較的簡単に社内に出入りできる。社内だから安全というわけではなく、前述のとおり、どこで何をされるかわからないので注意が必要だ。また、社内に提携先が常駐する場合もあるだろう。常駐しているからといって、安易に VPN のアカウントを発行し、使用させるのは問題がある。VPN のアカウントは社員だけに留める必要があるだろう。

6.3.7 内部犯行

セキュリティを脅かすタイプで、厄介なのが内部犯行だろう。管理者は、いつ、誰が、どこからアクセスして、何をしたかといった情報(ログ)を管理するべきである。何か問題があった場合、原因を早急に突き止めるためにもログ管理は重要である。逆に、必要な情報をログとして管理できないような製品は、使用するべきではない。

6.3.8 セキュリティの意識欠如

これまでに挙げた 7 項の問題は利用者個々が注意すれば防ぐ事が可能な問題であ

る。便利で、かつセキュリティを保つためには、管理者は利用者に対して、十分な教育と啓蒙活動が必要だ。もちろん、管理者もセキュリティを維持するために、十分な知識と情報が必要だろう。セキュリティは目に見えないもので、投資効果も数字に出るものではない。しかし、セキュリティはお金を払って買わなければならない。情報が流出してしまった場合の被害額,損害額を考えれば、セキュリティに投資すべき金額もおのずと導かれるのではないだろうか。1 度失った信頼を取り戻すのが容易でないことは、近年の企業の不祥事から廃業,倒産まで追い込まれる事件を見ていれば実感できるはずである。リスクに対する保険は必要だという認識を持っていただきたい。

7 Appendix A　IPsec ＆ IKE 解説

7.1　IPsec の概要

インターネット VPN を実現するために使用される IPsec と呼ばれているプロトコルは、通信の機密性を確保するための暗号機能、通信の送信元を認証するための認証機能、受信したデータの完全性を確保するための改ざん検知の機能を提供するほか、シーケンス番号によるリプレイ攻撃防御機能と対象となる通信のみに IPsec 通信を適用するアクセス制御機能も提供するプロトコルである。

7.1.1 ２つのモード

IPsec はトンネルモードとトランスポートモードの 2 つのモードをサポートしている。トンネルモードは、VPN を使用する際に使用されるものであり、トランスポートモードは、主にローカルネットワークでセキュアな通信を行いたい時に使用されるモードである。

(1) トンネルモード

トンネルモードは図 7-1 のように、ローカルネットワーク上のホストが送信したパケットに VPN ゲートウェイが、IP ヘッダと IPsec に関するヘッダを追加する。具体的には、IP ヘッダの送信元は VPN ゲートウェイ自身のアドレスが入り、宛先には対向となる VPN ゲートウェイのアドレスが入る。IPsec に関するヘッダは後述のパケット形式により内容が異なる。トンネルモードでは元のパケットに新たな IP ヘッダ等が追加されるため、ローカルアドレス同士の通信であってもインターネットを介して行う事ができ、元のパケット全体が認証、暗号、完全性の対象となるため、インターネット VPN では一般的にトンネルモードが使用される。

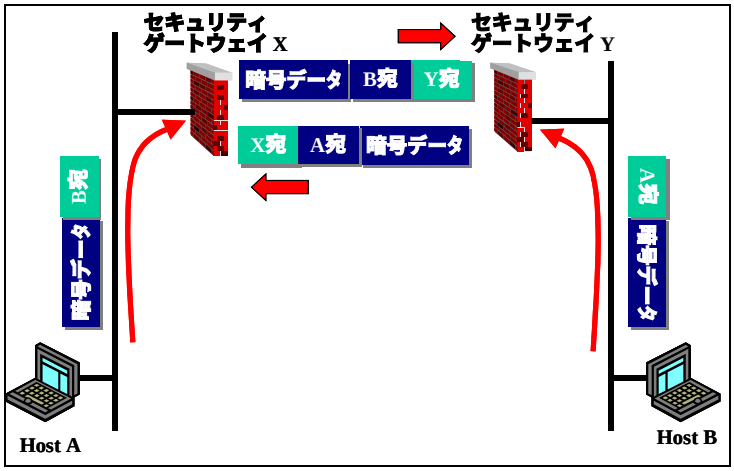


図 7-1 トンネルモード

(2) トランスポートモード

トランスポートモードは元のパケットのデータ部分（TCP/UDP ヘッダ以降）が IPsec 化処理される（図 7-2 参照）モードである。元のパケットの全てが暗号、認証、完全性の対象とはならないため、主にローカルネット上の端末間でセキュアな通信を行いたいときに使用される。

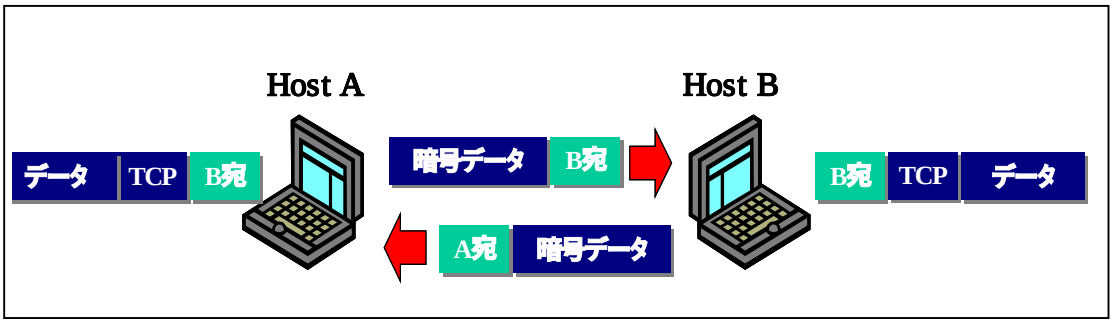


図 7-2 トランスポートモード

7.1.2 ２つのヘッダ

IPsec のヘッダには、データを暗号化する ESP とデータを暗号化しない AH の２つがある。現在では、AH はほとんど使用されず、暗号化通信が必要ない場合には Null Encryuption（暗号化しない） ESP が使用されている。

(1) ESP（Encapsulating Security Payload）

ESP の IP プロトコル番号は 50 である。IP パケットに対し、認証、データ暗号機能、完全性確保の機能を提供する。暗号アルゴリズムは DES が実装必須となっているが、現在では DES よりも暗号強度の高い 3DES や AES を実装した製品がほとんどである。

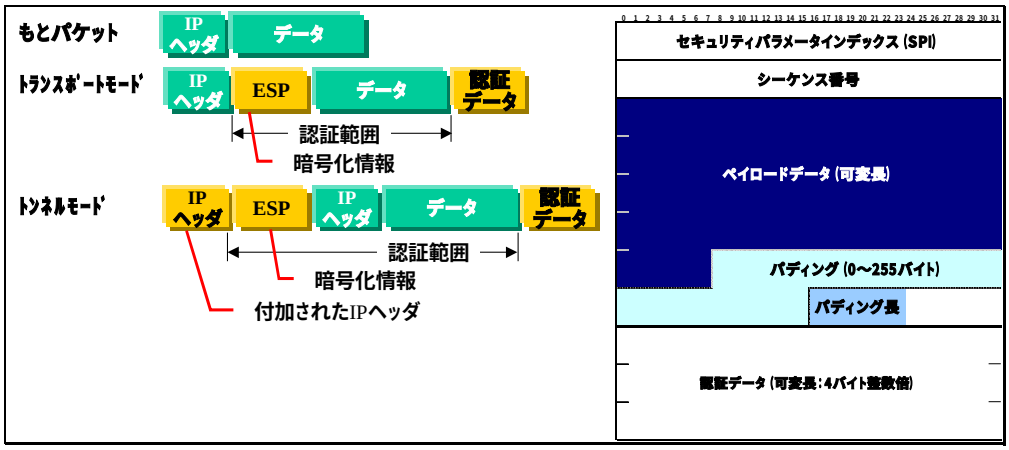


図 7-3 ESP パケットフォーマット

(2) AH（Authentication Header）

AH の IP プロトコル番号は 51 である。IP パケットに対し、、認証と完全性の確保の機能を提供する。図 7-4 を見ると分かるように、AH ではトンネルモード、トランスポートモードのどちらのモードを利用しても IPsec パケット全体が完全性確保の対象となっているが、IP ヘッダの TTL、TOS、フラグ、フラグメントオフセット、ヘッダチェックサムは経路途中で値が変更されるため、完全確保の対象外としている。

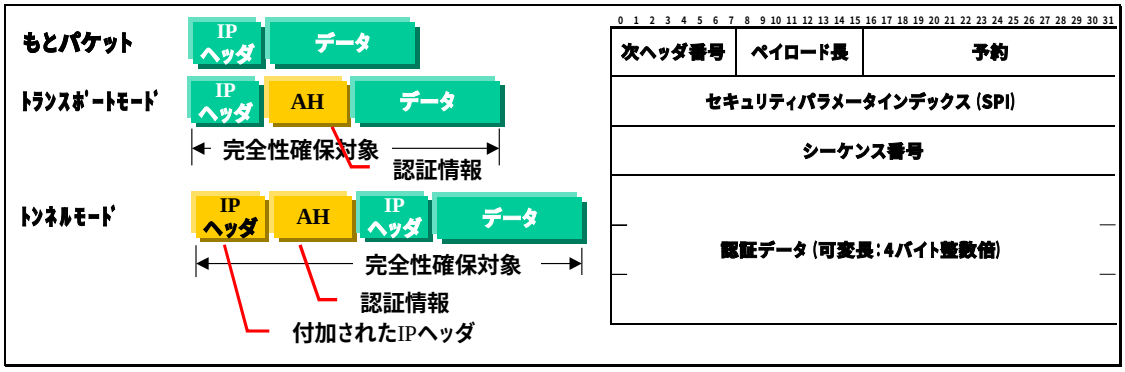


図 7-4 AH パケットフォーマット

7.1.3 IPsec 通信までの流れ

(1) SAD（Security Association Database）と SPD（Security Policy Database）

ここでは、IPsec 通信がどのように行われるのかを順を追って説明する。IPsec は認証、完全性確保、データ暗号機能を提供するため、事前に認証や暗号アルゴリズムを使用するか取り決めておく必要があり、IKE（Internet Key Exchange）機能を使用して実現している。

IKE によって取り決められた情報は Security Association（SA）と呼ばれ、Security Association Database（SAD）に格納される。IPsec 通信で使用される SA には方向性があるため送信用の SAD と受信用の 2 つの SAD を持つ必要がある。

SAD に格納された情報は、Security Parameter Index（SPI）と呼ばれる識別子によって管理され実際に IPsec 通信の行う際に、ESP または AH ヘッダにこの値が入れられる。一度確立した SA をそのまま使用し続けるとセキュリティレベル低下するため SA には有効期限があり、これも SPI に対応付けられて管理される。(図 7-5 参照)

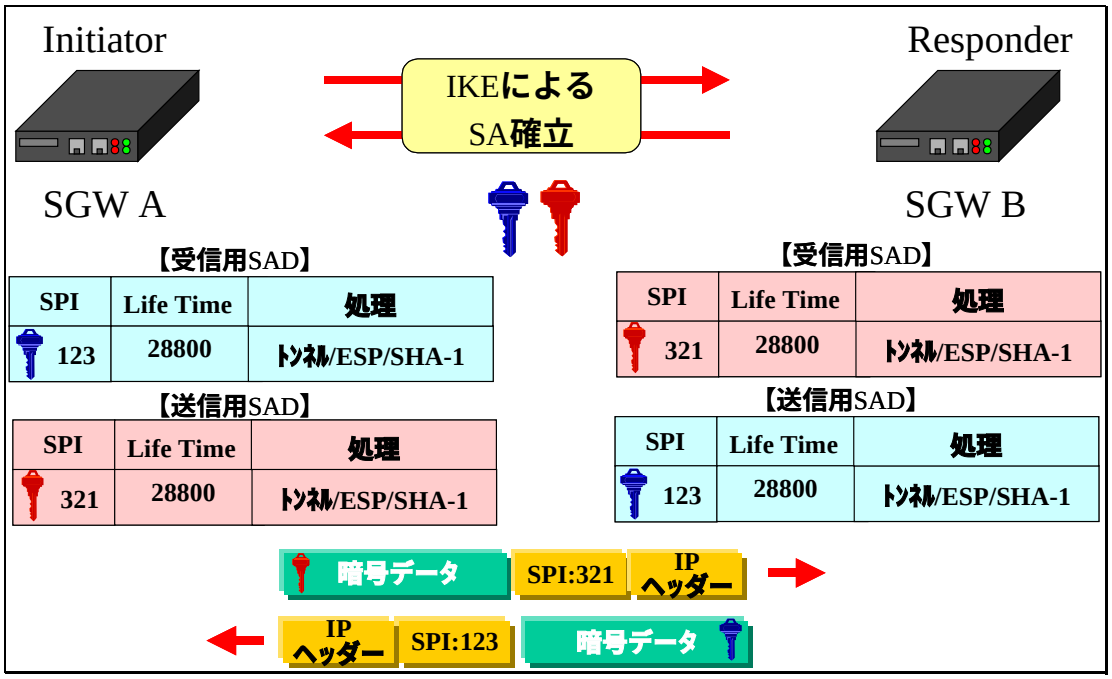


図 7-5 SAD と SA の関係

ここまでの内容では、どの通信が IPsec 通信の対象になるか VPN ゲートウェイは判断できないため、「送信元」「宛先」「プロトコル」「宛先ポート」「該当するパケット処理内容」を予め設定をしておく必要があり、この設定内容はセキュリティポリシーと呼ばれセキュリティポリシーはセキュリティポリシーデータベース（SPD）に保存される。先にも述べたように、IPsec で使用される SA には方向性があるため、SPD にも送信用と受信用の 2 つの SPD が存在する。

(2) IPsec 通信が行われるまでの流れ

(a) IP パケット ⇒ IPsec 処理 (図 7-6 参照)

- IP パケットを受信したセキュリティゲートウェイは SPD から該当するルールを検索する。
- パケットの処理が「パケット破棄(Discard)」の場合は、パケット破棄。パケットの処理が「パケット通過(Bypass)」の場合は、IPsec 処理を行わずにパケット通過。パケットの処理が「IPsec 適用(Accept)」の場合は、IPsec 処理を行うために以下に続く。
- SAD を検索し IP パケットで使用可能な SA を検索する。
- 検索した結果 SA が合った場合は、IPsec 通信を開始する。
- 検索した結果 SA が無い場合は、IKE により SA を確立するよう促す。
- IKE により SA が確保すると SAD に格納され、IPsec 通信が開始される。

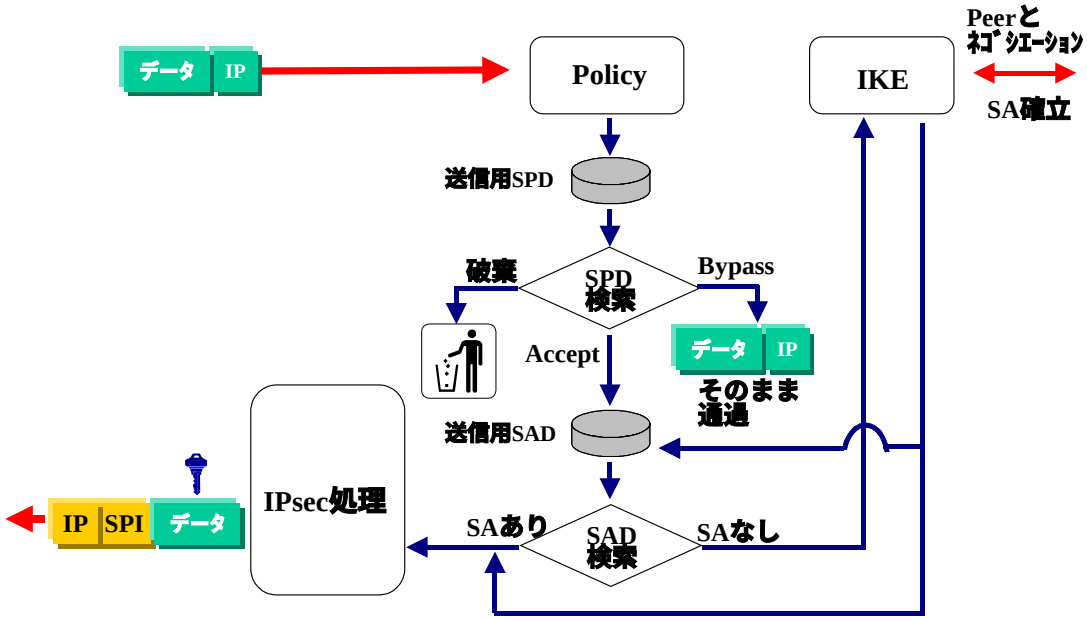


図 7-6 IPsec 処理の流れ（送信時）

(b) IPsec パケット => IP パケット処理(図 7-7 参照)

- 受信した IPsec パケットを受信したセキュリティゲートウェイは SAD から該当する SPI を検索する。
- 該当する SPI が無い場合は、IPsec パケットを破棄し、パケット送信元に「INVALID SPI」エラーメッセージを送信する。該当する SPI がある場合は、SAD の情報に則り IP パケット化する。
- IP パケット化したパケットの送信元、宛先等を元に、SPD を検索し該当する処理を行う。
- パケット処理が破棄の場合は、パケットを破棄し、許可の場合、宛先がセキュリティゲートウェイ宛の場合は上位層に引渡し、宛先がセキュリティゲートウェイ以外の場合は、パケットを転送する。

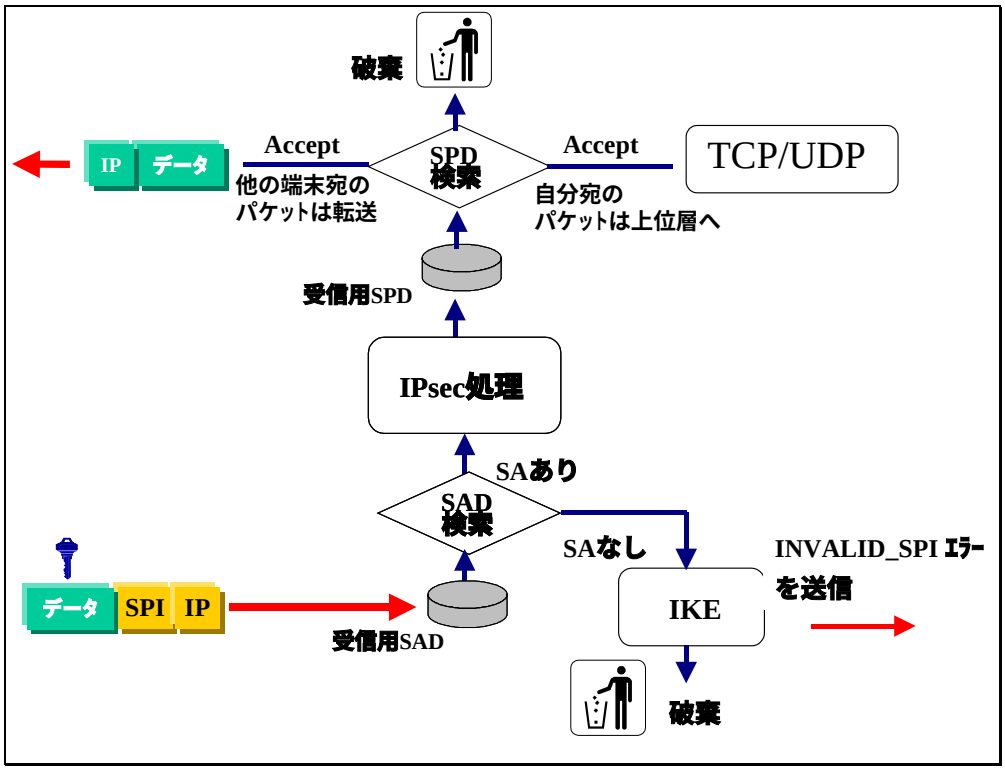


図 7-7 IPsec 処理の流れ(受信時)

(c) IPsec 処理の流れ

(i) AH の IPsec 処理（送信時）

- SAD の処理にしたがい、トンネルモードの場合は元の IP パケットの前に、新たな IP ヘッダとそれに続いて AH ヘッダを挿入する。トランスポートモードの場合は、IP ヘッダと上位層の間に AH ヘッダを挿入する。
- リプレイ攻撃防止用のシーケンス番号を生成し、AH ヘッダに挿入
- AH ヘッダを挿入した後のパケットに対して、SAD の処理に従った認証アルゴリズムと鍵を使用して完全性確保の為の値を計算し認証 AH ヘッダの認証フィールドに挿入

(ii) AH の IPsec 処理（受信時）

- 受信したパケットの SPI を元に、SAD を検索し該当する SA の存在有無を確認する。該当する SA が無い場合はパケットを破棄し、パケット送信元に対し「INVALID SPI」エラーを送信
- シーケンス番号を確認し、既に同じシーケンス番号の IPsec パケットを受信している場合はパケットを破棄する。
- 受信した IPsec パケットに対し、SAD の処理に従った認証アルゴリズムと鍵を使用して完全性確保の値を計算し、受信した IPsec パケットの認証フィールドの値と比較する。計算した値と認証フィールドの値

が一致しない場合は、認証失敗と判断しパケットを破棄する。
- AH ヘッダを削除する。

(iii) ESP の IPsec 処理（送信時）
- SAD の処理に従った暗号アルゴリズムでデータを暗号化する際に必要となる、IV(Initial Vector)を生成する。IV は SA 確立後、最初のパケットを暗号化する際に送信側で生成する必要があり、同一 SA を使用する 2 番目以降のパケットについては、その前に送信した暗号データの最終ブロックが IV となる。
- SAD の処理に従った暗号アルゴリズムに従い、データを暗号化する。トンネルモードの場合は、元の IP パケット全体が暗号され、その前に新たな IP ヘッダと ESP ヘッダが挿入される。トランスポートの場合は IP ヘッダ以降のデータ部分が暗号化され、IP ヘッダと暗号化されたデータとの間に ESP ヘッダが挿入される。
- リプレイ攻撃防止用のシーケンス番号を生成し、ESP`ヘッダに挿入
- ESP ヘッダを挿入した後のパケットに対して、SAD の処理に従った認証アルゴリズムと鍵を使用して完全性確保の為の値を計算し、暗号化されたデータの後に付加する。

(iv) ESP の IPsec 処理（受信時）
- 受信したパケットの SPI を元に、SAD を検索し該当する SA の存在有無を確認する。該当する SA が無い場合はパケットを破棄し、パケット送信元に対し「INVALID SPI」エラーを送信
- シーケンス番号を確認し、既に同じシーケンス番号の IPsec パケットを受信している場合はパケットを破棄する。
- 受信した IPsec パケットに対し、SAD の処理に従った認証アルゴリズムと鍵を使用して完全性確保の値を計算し、受信した IPsec パケットの認証フィールドの値と比較する。計算した値と認証フィールドの値が一致しない場合は、認証失敗と判断しパケットを破棄する。
- SAD の処理に従った暗号アルゴリズムに従い、データを複号化する。

7.2 IKE(Internet Key Exchange)について

IPsec 通信を行うには IKE により SA が確立されなければならないため、IPsec を理解するためには IKE を無視する事ができない。ここでは IKE が SA を確立するまでの通信内容を解説する。

IKE は IPsec 以外にも使用可能な鍵管理プロトコルであるため、IPsec に特化している部分は IPsecDOI（Domain of Interpretation）で吸収している。また、IKE は ISAKMP のフレームワークのもと、Oakley 機能などを踏襲して開発された鍵管

理プロトコルであり、IPsec に対してはフェーズ１，フェーズ２と呼ばれる 2 つのフェーズを用い SA を確立する機能を提供する。

7.2.1 フェーズ１（Phase1）

(1) フェーズ１が提供する機能

フェーズ１の役割は、IKE SA の確立である。フェーズ１の後で行われるフェーズ２の通信を安全に行うための「共有秘密鍵の生成」と「SA を確立する相手が正当な相手かどうかの認証」の機能を提供する。なお、IKE SA には方向性がないため、IPsec 通信を行うペアで１つの SA が確立される。

(2) 認証

もっとも重要な認証については４つの方式が用意されており、IKE の通信を始めた（イニシエータ）が、どのような認証方式を使用するかを決定する。この時、IKE 通信の相手となる（レスポンダー）がイニシエータの提案する認証方式をサポートしていない場合は、提案内容を拒否する事になる。以下に IKE が用意する４つの認証方式について簡単に説明する。

- 事前共有秘密鍵認証方式（Pre-Shared Secret）
  - あらかじめ IPsec 通信を行う 2 者間で秘密鍵を取り決め、これを用いて認証を行う。
- 電子署名認証方式
  - IPsec 通信を行う 2 者間で電子署名を互いに検証し認証を行う方式である。この方式では CA が必須となる。
- 公開鍵暗号認証方式
  - 乱数を IPsec 通信を行う相手の公開鍵で暗号化し、相手側で正しく複合化されることを確認することで認証を行う。現在では改良型公開鍵暗号方式を使用。
- 改良型公開鍵暗号認証方式
  - 公開鍵暗号認証方式の暗号・複合処理を軽減するために開発された認証方式で、認証方式は同じである。

最も一般的に使用されているのは事前共有秘密鍵認証方式であるが、認証情報に IP アドレスを使用するため VPN クライアントやダイヤルアップ環境などの IP アドレスが固定されない環境では使用出来ない問題がある。このような環境では電子署名方式を使用するかまたは、後述のアグレッシブモードを使用する必要があるので注意が必要である。

(3) ２つのモード

Phase1 は SA を確立するまでの通信回数が異なる、「メインモード」と「アグレッシブモード」の 2 つのモードが用意されている。メインモードは計 6 回の通信で IKE SA を確立し、認証情報が暗号化されている。もう一方のアグレッシブモードは、計 3 回の通信で SA を確立するが認証の情報が暗号化されないなどの問題点があるために、一般的にはメインモードが使用されている。なお、IKE の通信は UDP 500 番ポートを使用して行われる。

(4) 暗号鍵素材

フェーズ１のネゴシエーションについての詳細を説明の前に暗号鍵の計算方法を簡単に説明する。フェーズ１の擬似乱数発生関数の鍵として使用される SKEYID の計算は認証方式によって異なる。

事前共有秘密鍵認証方式　：　SKEYID=prf(事前共有秘密鍵，Ni_b | Nr_b)
電子署名認証方式　　：　SKEYID=prf（Ni_b | Ni_r，ｇ＾xy）

SKEYID が元になり、「IPsec 通信時に使用される暗号鍵の SKEYID_d」、「フェーズ２のメッセージ認証に使用される SKEYID_a」、「IKE 暗号通信に使用される SKEYID_e」の３つの暗号鍵が用途別に計算される。

SKEYID_d=prf（SKEYID，g^xy | CKY-I | CKY-R | 0）
SKEYID_a=prf（SKEYID，SKEYID_d | g^xy | CKY-I | CKY-R | 1）
SKEYID_e=prf(SKEYID，SKEYID_a | g^y | CKY-I | CKY-R | 2)

prf は擬似乱数発生関数であり、prf（hoge，hogehoge）とあった場合は、hoge を鍵として hogehoge に対して擬似乱数発生関数を使用することを表す。また、「Ni_b」はイニシエータが発生した乱数、同様に「Nr_b」はレスポンダーが発生した乱数を意味し、「｜」は前後のメッセージを連結することを意味する。したがって、事前共有秘密鍵認証方式の SKEYID=prf(事前共有秘密鍵，Ni_b | Nr_b) は、鍵として事前共有秘密鍵を鍵として、Ni_b と Nr_b を連結したメッセージに対して擬似乱数発生関数を使用することになる。ｇ^xy は Diffie-Hellman 鍵共有アルゴリズムによる鍵交換で生成された共有秘密鍵である。CKI-I と CKY-R はイニシエータクッキーとレスポンダークッキーをそれぞれあらわす。なお、イニシエータクッキーとレスポンダークッキーは IKE ネゴシエーションのパケットヘッダの先頭に位置するフィールドの値である。

(5) フェーズ１ネゴシエーションの詳細

今回説明するのは一般的に使用されているメインモードの事前共有秘密鍵認証方式と電子署名認証方式である。フェーズ１メインモードのネゴシエーションは、「パラメータ折衝」、「暗号鍵素材の交換」、「認証」の３つのステージで行われる。

(a) パラメータ折衝(図 7-8 参照)

イニシエータのセキュリティゲートウェイは SPD に設定された処理内容に従い、レスポンダーに SA パラメータの提案を行う。このときに提案されるパラメータの内容は以下の通りである。

- 暗号アルゴリズム　：DES、3DES、AES など
- ハッシュアルゴリズム　：SHA1、MD5 など
- 認証手順　：事前共有秘密鍵認証方式、電子証明方式など
- DH Group　：768bit Gourp、1024bit Group など
- Life Type　：Time 、Byte
- Life Duration　：秒

イニシエータのセキュリティゲートウェイは上記パラメータに対し各々１つの値を選択したうえで、SA パラメータグループ化してレスポンダーに送信する。この時、複数の SA パラメータグループをレスポンダーに提案することが可能である。一方レスポンダー側では対応することが可能な SA パラメータグループを選択し、その内容をイニシエータに送信しなければならない。このときレスポンダー側で対応できる SA パラメータグループが複数あった場合は、セキュリティ強度の高いものが採用され、採用可能な提案が無かった場合は、イニシエータに対し「No Proposal Chosen」通知メッセージを返信する。

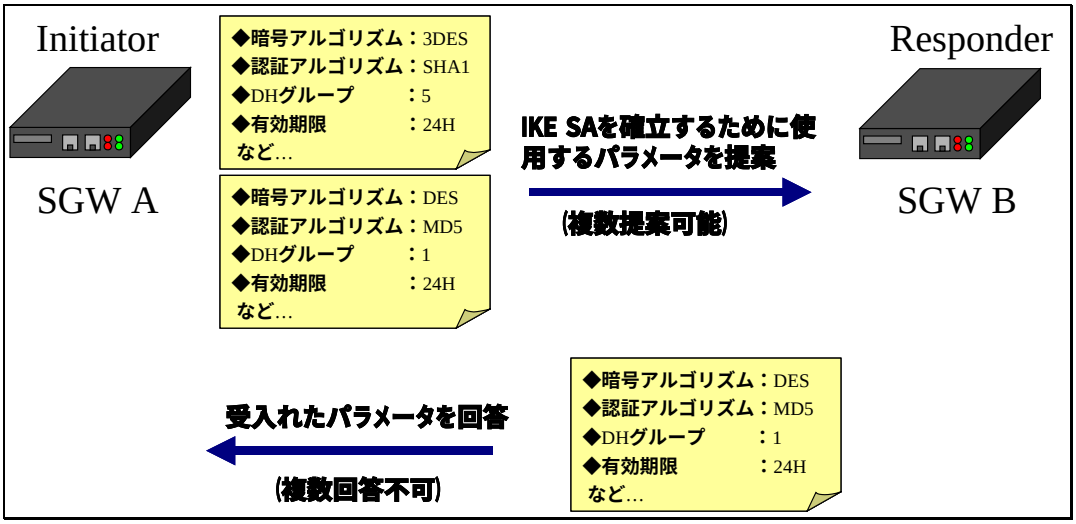


図 7-8 パラメータ折衝

(b) 暗号鍵素材の交換(図 7-9 参照)

イニシエータから、DH 鍵素材である「g^xi」と乱数「Ni_b」が送信され、レスポンダーからも同様に DH 鍵素材である「g^xr」と乱数「Nr_b」が送信される。これにより SKEYID の計算に必要な、DH 共有秘密鍵「g^xy」が求められ、それ以外にも必要な乱数「Ni_b」、「Nr_b」もこの通信で求められるため、このあと続く認証の通信からは IKE SA による暗号通信となる。

電子署名認証方式を採用した場合、認証に証明書を使用するため、「Ni_b」、「Nr_b」に続き、証明書要求ペイロードが付加される。

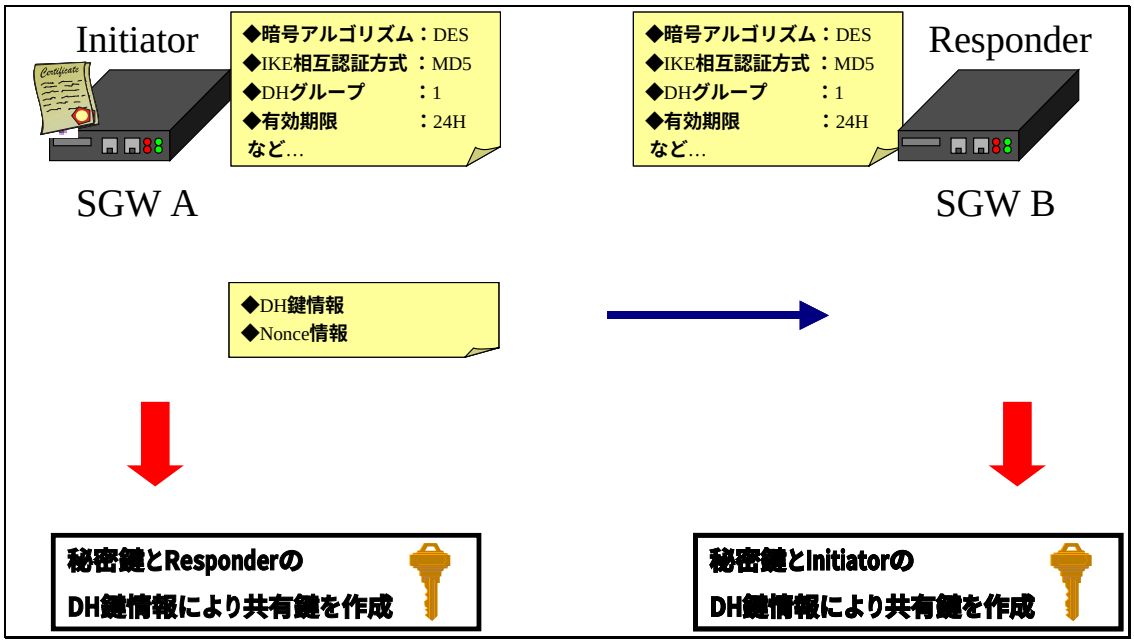


図 7-9 鍵素材の交換

(c) 認証（図 7-10，図 7-11 参照）

(i) 事前共有秘密鍵認証方式

イニシエータから ID 情報として「IP アドレス」とパラメータ折衝によって決定したハッシュアルゴリズムを使用して求められたハッシュ値がレスポンダーに送信される。レスポンダー側では受信したハッシュ値と、計算により求められたハッシュ値を比較し一致したら鍵交換とイニシエータの認証が成功と判断する。レスポンダーからも同様にイニシエータに対し ID 情報とハッシュ値が送信され、受信したハッシュ値と計算により求められたハッシュ値を比較し一致したら鍵交換とレスポンダーの認証が成功となり、フェーズ 2 ネゴシエーションに引き継がれる。

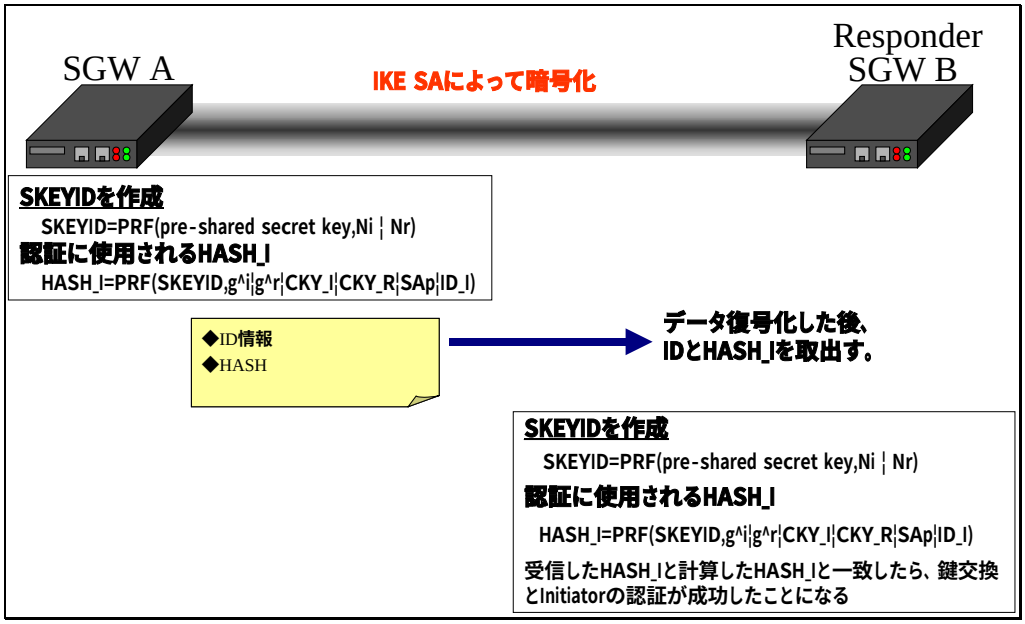


図 7-10 事前共有秘密鍵認証(イニシエータ⇒レスポンダ)

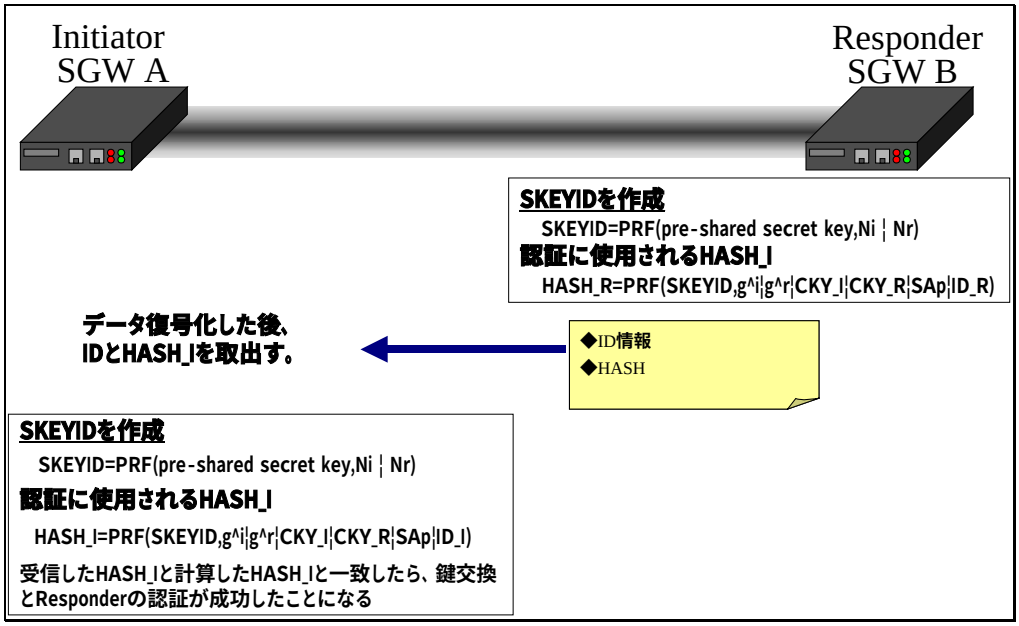


図 7-11 事前共有秘密鍵認証(レスポンダ⇒イニシエータ)

(ii) 電子署名認証方式（図 7-12，図 7-13 参照）

イニシエータからの ID 情報として「証明書の Subeject または SubjectAltName」と「電子署名」が送信される。電子証明書は事前共有秘密鍵と同様にもとめられたハッシュ値をイニシエータの秘密鍵を使用して暗号化することで作成される。電子証明書の送信はオプションであるが、ほとんどの製品が証明書を送信する仕様になっている。電子証明書を電子署名と一緒に受信したほうが、電子署名の検証が容易であるからであると考えられる。イニシエータから情報を受信したレスポンダー側では、電子署名を複合化し、

受信した情報から求められたハッシュ値と比較して一致したら鍵交換と認証が成功と判断する。レスポンダーも同様にイニシエータに ID 情報と電子署名を送信し、イニシエータが受信した情報から求められたハッシュ値と、電子署名を復号化して得られた情報を比較し一致したら鍵交換と認証成功と判断し Phase2 に引き継がれる。

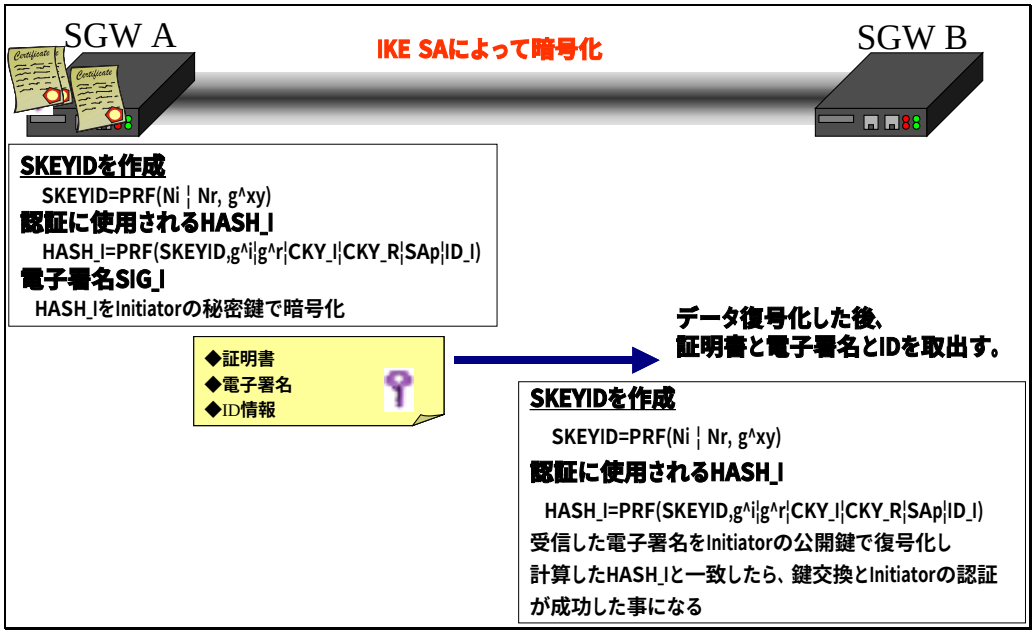


図 7-12 電子署名認証（イニシエータ⇒レスポンダ）

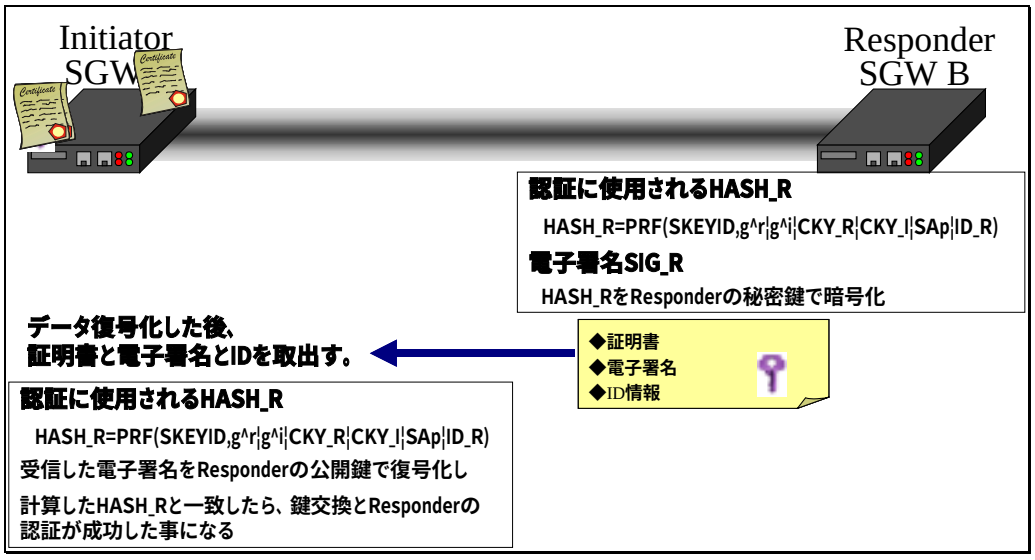


図 7-13 電子署名認証（レスポンダ⇒イニシエータ）

7.2.2 フェーズ２

(1) フェーズ２が提供する機能

フェーズ２の役割は、IPsec SA の確立であり、フェーズ２で生成した、共有秘密鍵が実際の IPsec 通信に使用される。IPsec SA には方向性があるため、IPsec 通信を行うペアで IPsec SA は 2 つ確立する。また、フェーズ１では SA 確立までの通信回数が異なる、２つのモードが用意されていたがフェーズ２は 3 回の通信で SA が確立するクイックモードしか用意されていない。

(2) フェーズ２ネゴシエーションの詳細

(a) パラメータ折衝（図 7-14，図 7-15 参照）

イニシエータの「ハッシュ値」に続き、SA パラメータの提案を行う。このときに提案されるパラメータの内容は以下の通りで、メインモードと同様に複数の SA パラメータグループをレスポンダーに対し提案することが可能である。

- Life Type ：Time 、Byte
- Life Duration ： sec 、 Byte
- 認証アルゴリズム ：HMAC-MD5、HMAC－SHA1
- Encapsulation Mode ：Tunnel 、Transport

SA パラメータ以降、「乱数ペイロード」、「ID ペイロード」と続く、ID ペイロードはイニシエータ側の IPsec 通信対象、レスポンダー側の IPsec 通信対象の情報が入る。したがって、インターネット VPN で LAN 間通信を行う際などには、イニシエータ側のローカルネットワークアドレスと、レスポンダー側のローカルネットアドレスが ID ペイロードに入ることになる。

イニシエータからの提案を受けたレスポンダーは、提案を受けた SA パラメータグループから対応することが可能な SA パラメータグループを、「ハッシュ値」に続き返信する。

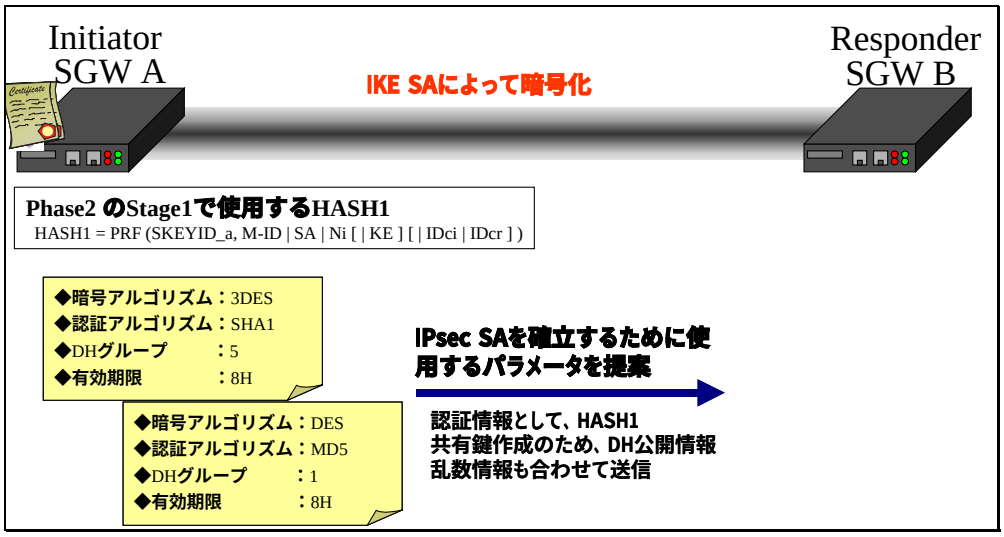


図 7-14 フェーズ２パラメータ折衝（イニシエータ⇒レスポンダ）

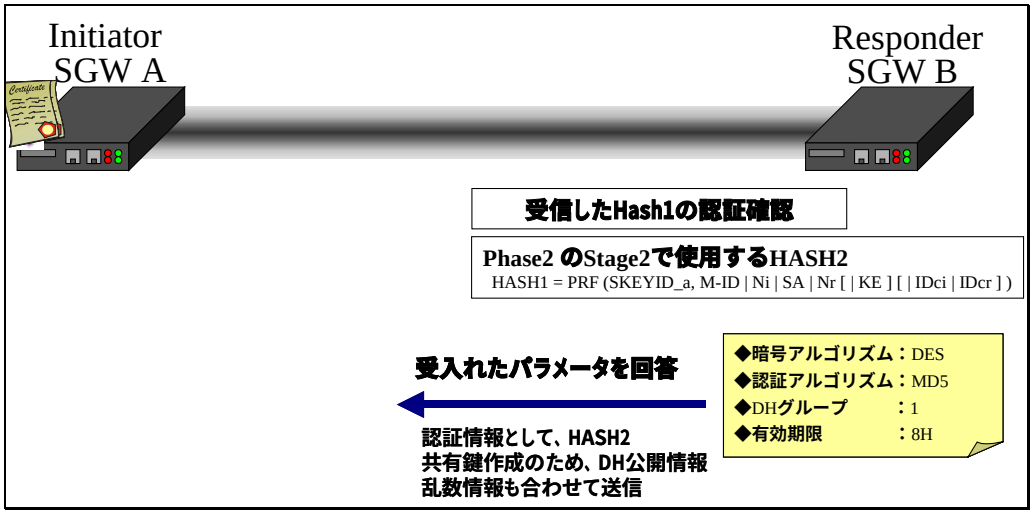


図 7-15 フェーズ２パラメータ折衝（レスポンダ⇒イニシエータ）

(b) 認証確認（図 7-16 参照）

イニシエータはレスポンダーからの情報受信した後、「ハッシュ値」をレスポンダーに送信する。この通信はイニシエータの生存証明のための通信であり、これを送信した時点でイニシエータ側は IPsec SA が正常に確立したと判断する。一方レスポンダー側は、イニシエータからの「ハッシュ値」を検証した時点で、IPsec SA が正常に確立したと判断する。

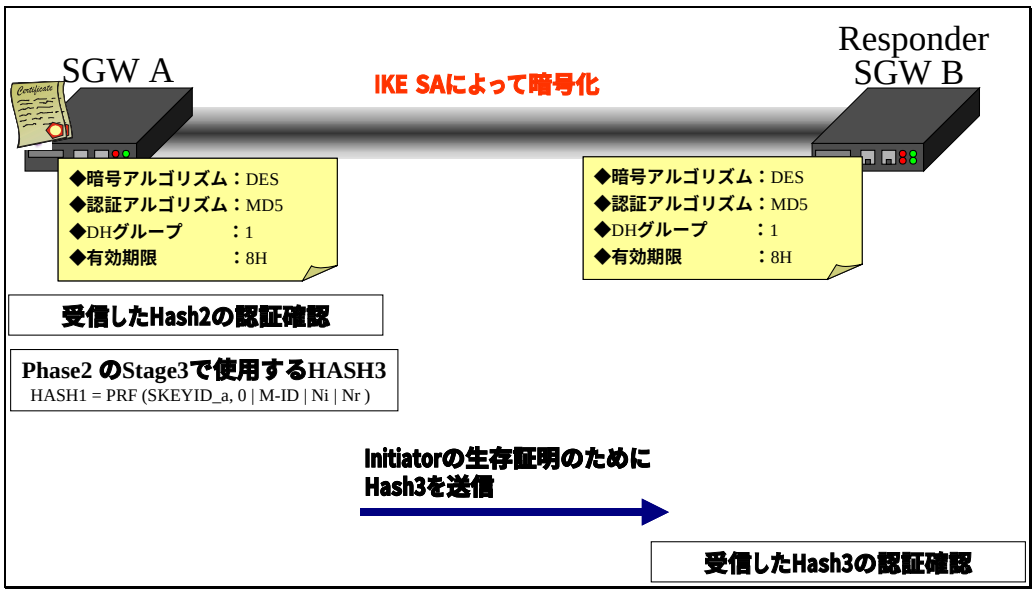


図 7-16 フェーズ２認証確認

(3) PFS(Perfect Forward Secrecy)

フェーズ２では IPsec 通信で使用する共有秘密鍵を生成するが、これまでの説明では鍵情報の交換が含まれていない。フェーズ２のデフォルトでは、秘密鍵を生成するための鍵素材はフェーズ１と同様の物を使用するのである。これでは、フェーズ１の鍵が漏洩してしまうとフェーズ２の鍵も合わせて漏洩したことになりセキュリティ上大きな問題が発生する。そこで IKE では、PFS(Perfect Forward Secrecy)と呼ばれる機能を提供しており、これを使用するとフェーズ１とフェーズ２で異なる鍵素材を使用することが可能となる。この機能を実装した製品では、この機能を使用することを推奨する。

8 Appendix B　NAT-Traversal 技術詳細

公衆無線 LAN で IPsec を使用する際に必須となる NAT-Traversal は現在、03 年 5 月現在標準化の最終段階に入っている。この文書は draft-ietf-ipsec-nat-t-ike-05.txt および 03 月 5 月 28 日に公開された最新版の draft-ietf-ipsec-nat-t-ike-06.txt を元に NAT-Traversal の詳細について解説するものである。

8.1　背景と目標

今日、NAT(ネットワークアドレス変換)が非常に普及している。組織の大小を問わずほとんどの会社、家庭、公衆無線 LAN スポットなどではプライベートアドレスが用いられており、これらのネットワークからインターネットなどの外部のネットワークへのアクセスには必ずといって良いほど NAT 装置が介在している。また、現在広く一般に使われている IPv4 での IPsec は NAT との協調がもとから考慮されていないため、組み合わせて利用することができなくなっている。

主な理由としては次の様なことが挙げられる

AH では IP ヘッダーも認証範囲に入るので、これを NAT で変更してしまうと相手側で改ざんが行われたと判断されてしまう。

ESP のトンネルポートモードではパケットのデータ部分に含まれる IP アドレスが暗号化されているので NAT 装置はこれを書き換えることができない。FTP、IRC、LDAP など。

ESP は TCP や UDP のヘッダも暗号化するので、NAPT(後述)を用いることができない。

しかしながら、非常に大多数なユーザはすべての種類の NAT とすべての種類の IPsec をシームレスに組み合わせて利用したいといった要望がある。下記に主な組み合わせの要素を記す。

8.2　様々な NAT(ネットワークアドレス変換)技術

IP アドレスと IP アドレスを 1:1 に対応させる NAT、ベーシック NAT、スタティック NAT、などと呼ばれている。(IP ヘッダのみの書き換えが行われる)

一つの IP アドレスと複数の IP アドレスを対応させる 1:n の NAT、ポート NAT、NAPT、IP マスカレード、などと呼ばれている。(IP ヘッダ以外に TCP/UDP のソースポートアドレス書き換えも行われる) [RFC 3022]

IPv4、IPv6 のプロトコル変換を行うプロトコル NAT、NAT-PT[RFC 2766]

8.3　様々な IPsec トランスフォーム

AH(Authentication Header、認証ヘッダ)プロトコル番号 51 [RFC 2402]

ESP(Encapsulating Security Payload､暗号ペイロード)プロトコル番号 50 [RFC 2406]

IPCOMP(IP Payload Compression Protocol、IP ペイロード圧縮プロトコル) プロトコル番号 108 [RFC 2393]

8.4 様々な要求事項

途中の経路上に存在するネットワーク機器、ルータやファイアウォール、NAT 装置などには一切の変更を要求したくない。

利用者には完全に透過的でなければいけない。

IPsec スタックへの変更は最小限にしたい。

イニシエーターのみならずレスポンダーが NAT される場合にも対応させたい。

通常の IPsec との互換性ももちろん必要である。

その他の問題点として IPsec での鍵交換プロトコル IKE と NAT についても考えてみる必要がある。IKE は UDP を使いソースポート、ディスティネーションポートともに 500 番を使うがこれがポートアドレス変換(NAPT)により正しく行えない可能性もある。

8.5 解決策の候補

そこで解決策として上記の要望を満たせないものもあるがとりあえず考えられるものを以下に示す。

IPv6 の到来を待つ: IPv6 環境では NAT は不要なので、IPsec にとって都合の良い環境である。ただ 2003 年の現実を考えると解決策にはなり得ない。

RSIP(Realm Specific IP)の機能を用いる: ホストやゲートウェイの実装に変更が必要で IPv6 との共存が困難でこれもあまり現実的な解決策にはなり得ない。[RFC 3102]

NAT 装置を変更する: IPsec パケットに変更を加えないで送出する。複数のホストが NAT 装置配下にある場合、それらの判別が困難となる。VPN パススルー機能などと呼ばれている。

IPsec の通信者間でコネクションの変更を行う: このアプローチでの一番手間が少なく応用範囲が広く現実的な解決策であると言える。ここでさらに以下の方法が考えられる。

TCP でカプセル化する: この場合､セッションの確立など通信上の負荷が大きい。

UDP でカプセル化する: これが現在最も有力な解決策で draft でありながらすでに広く一般に浸透しているに NAT-Traversal（ナットトラバーサル）である

8.6 NAT-Traversal とは

NAT-Traversal は先にも述べた通り IETF にオープンスタンダードとしてドラフトが公開されていおり 2003 年 5 月 2 日現在での最新の版は 05 となっている。

http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-06.txt

多くのベンダーがこれを支持しており先に挙げたすべての IPsec と NAT の組み合わせで発生する問題が解決されている。また、実装の変更は IPesc の通信者のみとなっておりルータ、ファイアウォール、NAT 装置に一切の変更を求めていない。また、利用者には透過的になっており、NAT-Traversal を実装していない IPsec との互換性が保たれている。

8.7 NAT-Traversal 操作手順概観

NAT-Traversal が必要とされた場合、互いにネゴシエーションされた IPsecSA に基づいてパケットを UDP にカプセル化して通信を行う。この時この UDP ヘッダにはリモートの通信相手が元のパケットを取り出せるようにする為の幾つかの小さな情報が付加されている。これが NAT-Traversal ヘッダである。

詳細は後述する事とする。また、本来の UDP ヘッダはどんな NAT 装置でも通過できるようにする為にある。この UDP の通信は IKE の通信と同じ経路を流れ、この通信は他の NAT-Traversal をサポートしていないものからは無効な IKE のパケットの様に見える。

以下にカプセル化の手順を示す。これは必ず IPsec 処理の後に行われる。

UDP ヘッダと NAT-Traversal ヘッダは元の必要最低限の IP ヘッダの直後に挿入される。(NAT-T は必要最低限の IPv4 ヘッダしか必要としない)

元の IPv4 ヘッダ長は NAT-T ヘッダに格納される。

IPv4 ヘッダ長は 20 バイトに設定され、プロトコルは UDP として設定される。

元の AH パケット　<IP><AH><ESP><IP><TCP><app><ESP> NAT-T パケット　<IP><UDP><NATT><AH><ESP><IP><TCP><app><ESP>

以下にこの UDP カプセルから取り出す手順を示す。これは必ず IPsec 処理を行う前に行われる。

1. プロトコルが UDP で宛先が IKE ポートであることが確認される。
2. もし、UDP ペイロードが空であった場合は到達性情報が更新され、そのパケットは破棄される
3. リモートの IP アドレスとポートアドレスのペアが IKE/IPsec のそれぞれでデータが確認できる様に通知される。これが失敗する場合、そのパケットは破棄される。
4. NAT-T ヘッダからヘッダ長と ID が IP パケットにコピーされる。NAT-T のタイプに従ってプロトコルタイプが設定される。
5. 送信元アドレスと送信先アドレスが IPsec エンドポイントによって変更され、UDP ヘッダと NAT-T ヘッダはパケットの中から取り除かれる。

IPSecSA が IKE によってすでに成立しているものに対してそれをそのまま自動

的にNAT-Traversal及びUDPのカプセル化を適応してはいけない。NAT-Traversalは IKE のネゴシエーションのなかで正しく必要とされた場合、もしくは、マニュアル鍵 IPsecSA で NAT-Traversal を使う様に設定されている場合にのみ使われなければならない。

また、オーバーヘッドとして NAT-T ヘッダ 12 バイト、UDP ヘッダ 8 バイトの計 20 バイトがあげられる。NAT-T ヘッダの内容は下記の通りである。

Non-IKE マーカー8 バイトの 0(通常の IKE パケットと区別する為のマーカー)
次ヘッダタイプ(AH, ESP など)
IP ヘッダ長
TOS フィールド
ID フィールド

8.8 NAT-Traversal プロトコル詳細

以下にプロトコルの詳細を記す。これは下記からの抜粋である。
draft-ietf-ipsec-nat-t-ike-05.txt, draft-ietf-ipsec-udp-encaps-06.txt

8.8.1 フェイズ 1

NAT-Traversal と IKE の通信が行われる経路上に NAT 装置があるかどうかの検出がフェイズ 1 で行われる。NAT はおそらく IKE の UDP ソースポートの変換行う。よって受信側は IKE のソースポートが 500 番以外であったとしてもこれを処理する必要がある。例えば次の様な場合 NAT 装置はソースポートの変更を行わない。

- NAT 装置背後に IPsec ホストが一つしかない場合
- IPsec を行う最初の 1 台目のホストがおこなう IKE のソースポートは 500 番のまま保たれ IP アドレスのみの書き換えが行われる

受信側はパケットのソースポートアドレスに対して返信を行わなければならない。これは元のレスポンダーが開始する鍵交換や通知の送信などにも当てはまる。また、元のイニシエーターも最後に行われた IKE と必ず同じポートアドレスと IP アドレスの組み合わせでパケットを送信しなければいけない。(ソースポートアドレス、デスティネーションアドレス、IP アドレスは必ず同じでなければならない)

例えば、イニシエーターがソースとディスティネーションアドレスが 500 番のパケットを送信した場合、NAT 装置はこれのソースアドレスを 12312 番に変更し、ディスティネーションは 500 番ポートのままとする。レスポンダーは必ずこのソースポート 12312 のパケットを処理しなくてはならない。また次にソースポート 500 番、ディスティネーション 12312 番を使って返信しなくてはならない。NAT 装置はこのパケットをソース 500 番、ディスティネーション 500 番に変換し直す。

8.8.2 NAT-Traversal サポートの検出

リモートホストの NAT-Traversal 機能の検出はベンダーストリングの交換によっておこなわれる。フェイズ 1 の最初の２つのメッセージで“ RFC XXXX ”-[“ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX ”]の MD5 のハッシュを NAT-Traversal のスペックとしてベンダーID ペイロードにて交換する。NAT-Traversal の検出を継続する場合は必ず互いに送信しなくてはならない。

8.8.3 NAT 装置の存在の検出

NAT-D ペイロードの目的は２つある。NAT 装置の存在の確認だけでなく、その NAT 装置がどこに存在するのか、の確認が行われる。なぜなら NAT 装置の場所を特定することは、キープアライブ開始する上で重要だからである。NAT 装置の背後にあるホストから開始される必要がある。NAT-D（NAT-Discovery）ペイロードに「始点 IP アドレス/ポート番号」「終点 IP アドレス/ポート番号」をハッシュしたものをセットして、互いに送信する。受信した方は NAT-D ペイロードの中のハッシュと実際の IP アドレス・ポートのハッシュを比較して NAT の有無を検知する。始点 IP アドレスの方のハッシュが実際のものと違っている場合は、相手が NAT デバイスの後ろにいることが分かる。また終点 IP アドレス側のハッシュデータが違っている場合は自分の手前に NAT するデバイスがあることがわかる。

もし、送信者が自分の使っている IP アドレスが分からない様な場合もある（例えば複数のインターフェイスを持っている場合など）が、全てのインターフェイスのローカルハッシュを送信しても構わない。この場合は全くどれにもマッチしなかった場合のみ NAT 装置が存在していると判断される。これらは一連の NAT-D ペイロードとして送信される。それぞれのペイロードには一つのみのハッシュが含まれる。よって、複数のハッシュを送信する場合複数の NAT-D ペイロードとして送信される。通常は２つの NAT-D ペイロードが存在することになる。

NAT-D ペイロードは、メインモード上の 3 番目と 4 番目のパケット及び、アグレッシブモード上の 2 番目と 3 番目に含まれている。

NAT-D パケットフォーマットは図 8-1 の通りである。

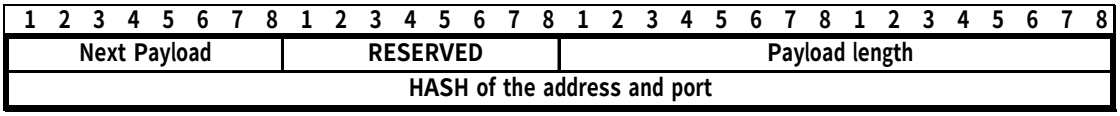


図 8-1 NAT-D ペイロードフォーマット

NAT を検出するためのペイロードタイプは 15 である。

ハッシュは以下のように計算される。

HASH = HASH(CKY-I | CKY-R | IP | Port)

既にネゴシエーションされたハッシュアルゴリズムを使用する。そのハッシュ中

の全てのデータはネットワークバイトオーダーとなっている。上記 の ”IP ”は、IPv4 の場合 4 オクテットであり、IPv6 の場合は 16 オクテットである。上記の ” Port" はネットワークバイトオーダーで 2 オク テットにエンコードされている。その最初の NAT-D ペイロードは、リモートエンドの IP アドレスとポート（すなわち相手先の UDP パケットのアドレス）を含んでいる。残りの NAT-D ペイロードは、可能なローカルエンドの IP アドレスとポート（すなわち可能な全ての UDP パケットのソースアドレス）を含んでいる。

もし、NAT が双方に存在しなければ、最初の NAT-D は、ローカル NAT-D パケット(すなわち、その NAT-D ペイロードをこのホストが送り出す)の一つと合致するはずである。そして、他の NAT-D ペイロードの一つは、そのリモートエンドの IP アドレスとそのポートと合致するはずである。もし、 最初のチェックが失敗すると(すなわち最初の NAT-D ペイロードが、他のどんなローカル IP アドレスとポートに合致しなければ)、それは双方の間にダイナミック NAT が存在することを意味し、こちら側からに、[Hutt02]で定義される Keepalives の送信を開始する。

CKY-I と CKY-R は、イニシエータークッキー、レスポンダークッキーとなる。またそれらは、IP アドレスとポート番号を割り出す攻撃を不可能にするためにハッシュに加えられる。

以下に、メインモード(署名を使用した認証)での、NAT-Traversal を使用したフェイズ 1 を例として述べる。

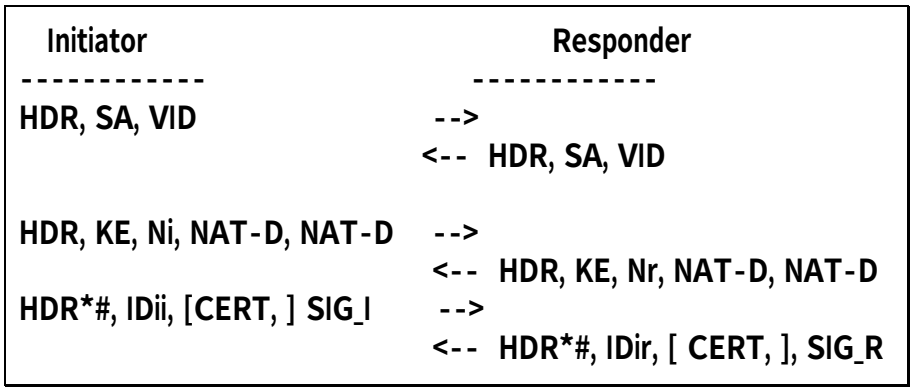


図 8-2 NAT-T 使用時のフェーズ 1（メインモード）

以下に、アグレッシブモード(署名を使用した認証)での、NAT-Traversal を使用したフェイズ 1 を例として述べる。

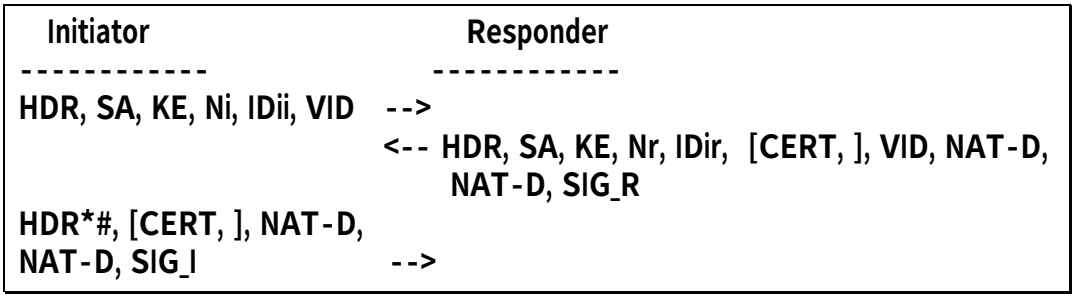


図 8-3 NAT-T 使用時のフェーズ 1（アグレッシブモード）

'#'は、もし NAT が検出されている場合にそれらのパケットがポートを変更するために送られたものであるかを示すサインである。

8.8.4 新しいポートへの変更

IPsec を認識する NAT 装置は問題を引き起こす。いくつかの NAT 装置は、背後で多数のクライアントが接続されていようとしても IKE ソースポート を変更しない。それらは、またそのソースポートで分離する代わりに、IKE クッキーを使ってマッピングする。これらは一般的に NAT の透過性の問題を引 き起こす。なぜならば、IKE で NAT の有無を見つけるのが困難となるからである。一番良いアプローチとしては、単純に IKE トラフィックでの 500 番 ポートをできるだけ早く無効にし、IPsec を認識する NAT 装置が特別に振舞ってしまうことを回避することである。この問題を最小限にする為、一般的な場合でイニシエーターが NAT 装置の背後にいる場合、NAT の存在が確認されたら 4500 番ポートに速やかに移行することである。

メインモードではもし NAT 装置が存在する場合イニシエーターは ID ペイロードを送信する際に必ずポートの変更を行わなくてはならない。またイニシエーターは UDP のソースポートとディスティネーションポートを必ず 4500 番にしなくてはならない。このホストに対してその後に発生する(インフォメーショナルーノーティフィケーションを含む)パケットは全て 4500 番ポートを使って送られなくてはならない。さらに、[Hutt02]で定義されるトラフィックの分離を可能にするために IKE のデータには non-ESP マーカーを付加しなければならない。

この様に IKE のパケットは以下の様になる。

IP UDP(4500,4500) <non-ESP marker> HDR*, IDii, [CERT,] SIG_I

署名を用いた認証では 4 バイトの non-ESP マーカーが[Hutt02]で定義されている。

レスポンダーがこのパケットを受け取った場合、これを通常通り処理する。もしこれが成功したならばローカルステートを更新してこれに続くパケットを全て新しいポートを使って送信しなくてはならない。有効な受信パケットに新しい IP アドレスが含まれている可能性もある。そのポートは通常と異なっている、なぜならNAT 装置は通常 UDP(500,500)を UDP(X,500)にマッピングし、UDP(4500,4500)を UDP(Y,4500)にマッピングします。事前に交換された IP アドレスはまずめったに変更されることは無い。レスポンダーはこのホストに対して続く IKE パケットを全て UDP(4500,Y)を使って送信しなくてはならない。

同様にして、もしレスポンダーがフェイズ 1 SA の鍵交換をする必要があった場合、必ず UDP(4500,Y)をつかってネゴシエーションを開始しなくてはならない。NAT-Traversal をサポートするどのような実装であっても 4500 番ポートをで開始されるネゴシエーションをサポートしなくてはならない。もし 4500 でネゴシエーションが開始されるのであれば、その他の全ての交換は全く変更する必要はない。

一旦ポートの変更が発生したならば、もし 500 番のパケットを受け取ったならそのパケットは古いと言える。もし、そのパケットがインフォメーショナルの場合、ローカルポリシーが許可しているならそれは処理される場合もある。もし、それがメインモードやアグレッシブモードであった場合それば無視されるべきである。

図 8-4 は NAT-Traversal を用いた(認証は署名)フェイズ 1 の交換である。

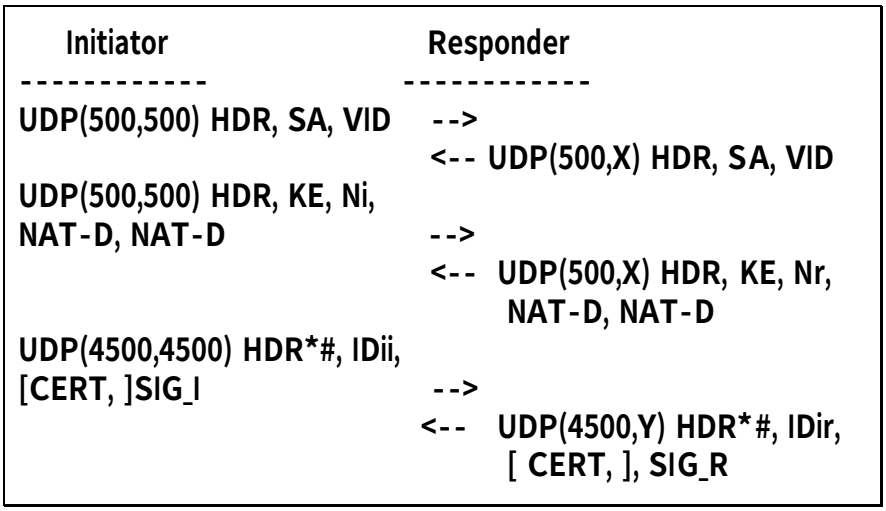


図 8-4 NAT-T 使用時のフェーズ１（メインモード）

アグレッシブモードの場合でも非常に似ている。NAT が検出された後、イニシエーターは IP UDP(4500,4500) <4 bytes of non-ESP marker> HDR*, [CERT,], NAT-D, NAT-D, SIG_I を送信する。レスポンダーはこれを上記と同様に処理し、もし成功したならば内部の IKE のポートをアップデートしなくてはならない。また、レスポンダーは続く IKE のパケットを UDP(4500,Y)を使って送信しなくてはならない。

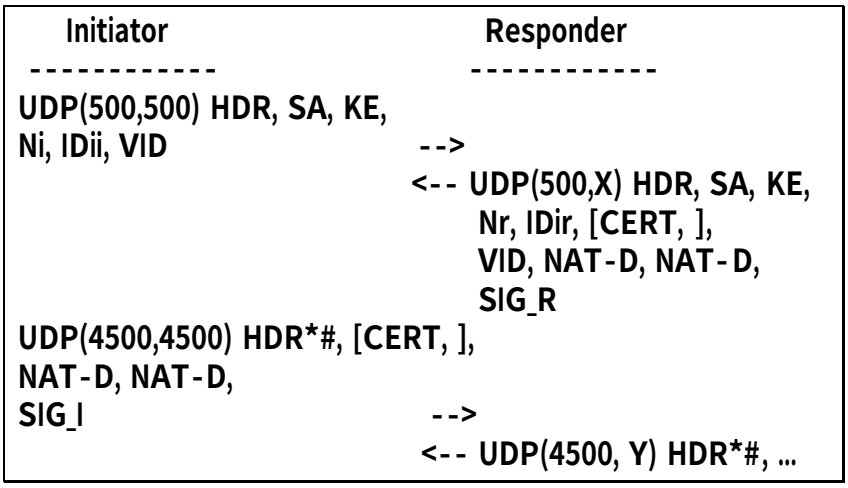


図 8-5 NAT-T 使用時のフェーズ１（アグレッシブモード）

ポートを変更している間は、ID ペイロードに格納される port はメインモード・アグレッシブモード共に 0 でなくてはならない。

レスポンダーが NAT される場合通常は一対一のアドレス変換が行われる。この場合イニシエーターは両方のポートを 4500 に変更する。レスポンダーは上記と全く同じ振る舞いとなる。この場合 Y は 4500 のままである。なぜなら一対一のアドレス変換ではポート番号の変更は行われないからである。

別のポート変更が発生する場合として、out-of-band 検出がある。例えばレスポンダーがポート変換を行う NAT 装置の背後にありイニシエーターが最初にそれにアクセスしなければいけない場合、イニシエーターはまずどのポートが使われているのか知っておく必要がある。一旦それをイニシエーターが分かったとしてそれは UDP(Z,4500)となっていてこれを用いてアクセスする事が可能になる。これは上記で説明しているレスポンダーからの鍵交換と似ている。ポート番号が分かってさえいればその他はなにも変更しなくて良い。

8.8.5 クイックモード

フェイズ 1 の後、互いの間に NAT 装置があると分かったとする。最後に残るのはクイックモードである。NAT-Traversal の利用はクイックモードの SA ペイロードの交換で行われるネゴシエーションである。クイックモードでは両者はトランスポートモードの場合に元の IPsec パケットを他方に送信することができる。なので、他方は TCP/IP のチェックサムフィールドを NAT の後に修正する必要がある。

(1) NAT-Traversal カプセル化のネゴシエーション

NAT-Traversal カプセル化のネゴシエーションは二つの新しいカプセル化のモードを追加することによって行われる。これらのカプセル化のモードは下記の通りである。

- UDP-Encapsulated-Tunnel 3
- UDP-Encapsulated-Transport 4

これはトンネルモード、トランスポートモードの両方で有用というわけではない。もし通常のトンネルモードやトランスポートモードのカプセル化では間に NAT 装置があった場合、おそらくそれは動作しない。またもし、NAT 装置が存在しないのであれば、これは全く無意味である。イニシエーターは通常のトンネルモード、トランスポートモードと UDP カプセル化されたトンネルモード、トランスポートモードなどをプロポーザルに含めるべきではない。

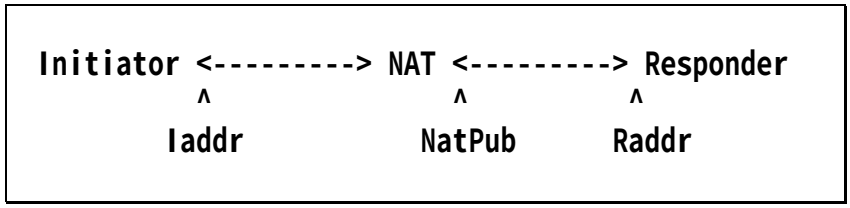
(2) 元のソースアドレス、デスティネーションアドレスの送信

増加する TCP チェックサムの修正を行う為に、両者は互いの元の IP アドレスを知る必要がある。イニシエーター側では元の自身のアドレスを定義する。元のレスポンダーのアドレスも受信相手の IP アドレスとして定義する。レスポンダー側では元のイニシエーターのアドレスは通信相手のアドレスとして定義される。元のレスポンダーのアドレスはレスポンダーの IP アドレスとして定義される。

元のアドレスは NAT-OA(NAT Original Address)ペイロードを使って送信される。

イニシエーターの NAT-OA ペイロードが最初である。レスポンダーの NAT-OA ペイロードが次ぎになる。

(a) Example 1:



NAT 装置の背後のイニシエーターはレスポンダーのパブリックアドレスに対して通信を開始する。イニシエーターとレスポンダー、NAT 装置はそれぞ下記の様にアドレスを持っているものとする。

Initiator:

NAT-OAi = Iaddr

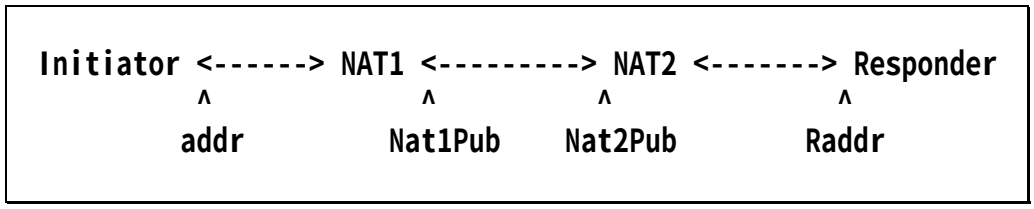
NAT-OAr = Raddr

Responder:

NAT-OAi = NATPub

NAT-OAr = Raddr

(b) Example 2:



ここではNAT2はレスポンダーのアドレスを公開するものとして使われている。

Initiator:

NAT-OAi = Iaddr

NAT-OAr = Nat2Pub

Responder:

NAT-OAi = Nat1Pub

NAT-OAr = Raddr

トランスポートモードの場合両者は互いに元のイニシエーターとレスポンダーのアドレスを送信しあわなければならない。トンネルモードの場合は他方に元のアドレスを送信すべきではない。NAT-OA ペイロードはクイックモードの 1 番目と 2 番目のパケットの内部で送信される。UDP カプセル化されたトランスポートモードを利用する場合イニシエーターは必ずこれを送信しなくてはならない、レスポンダーはもし、この UDP カプセル化されたトランスポートモードを選択する場合のみこれを送信しなくてはならない。すなわちイニシエーターはカプセル化されたトランスポートモードでもトンネルモードでも NAT-OA を送信する。それで、レスポンダーが UDP カプセル化されたトンネルモードを選択しても NAT-OA ペイロードは送信しない。

NAT-OA パケットは図 8-6 の通りである。

1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
Next Payload	RESERVED	Payload length	
ID Type	RESERVED	RESERVED	
IPv4 (4 octets) or IPv6 address (16 octets)			

図 8-6 NAT-OA パケットフォーマット

NAT-OA のペイロードタイプは 16 である。

ID タイプは RFC-2407 で定義されている。ID_IPV4_ADDR と ID_IPV6_ADDR タイプのみ許可されている。ID タイプの後ろの予約フィールドは必ず 0 でなくてはならない。

NAT-OA を使ったクイックモードの例は下記の通りである。

```
Initiator                          Responder
----------                         -----------
HDR*, HASH(1), SA, Ni, [, KE]
  [, IDci, IDcr ]
  [, NAT-OAi, NAT-OAr] -->
                              <-- HDR*, HASH(2), SA, Nr, [, KE]
                                    [, IDci, IDcr ]
                                    [, NAT-OAi, NAT-OAr]
HDR*, HASH(3)
```

図 8-7 NAT-OA を使用したクイックモード

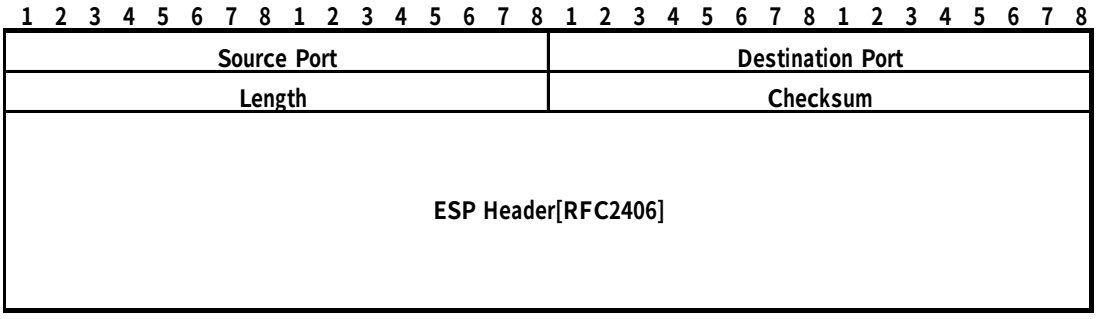
8.8.6 イニシャルコンタクト通知

NAT 装置の背後のイニシャルコンタクト通知でのソース IP アドレス、ソースポートアドレスの通知は意味のあるのもではない。なので、IP アドレスとポート番号は IKE や IPsec の SA を削除する為に使われるべきではない。代わりに ID ペイロードが使われるべきである。すなわち、イニシャルコンタクト通知を受け取った場合、受け手側は全ての同じ ID ペイロードを持つ、すでに確立された SA を破棄するべきである。

8.8.7 NAT 装置のマッピング情報が破棄された場合の復旧

通信はすでに確立しているが NAT 装置のマッピング情報がなんらかの理由によって破棄される場合がある（例えば、キープアライブが長すぎる場合、NAT 装置が再起動した場合）この様な状況から回復するには NAT 装置の背後ではない側から最後に受け取った有効な認証されたパケットから IP アドレスとポートを確認すべきである。NAT 装置の背後にあるホストからこれを決して行ってはならない。なぜなら DoS 攻撃の可能性があり、相手のアドレスとポートは変更されていないからである。

8.8.8 UDP カプセル化された ESP のヘッダフォーマット



UDP ヘッダは[RFC 768] にて定義されているヘッダである。

- ソースポートとディスティネーションポートはIKEで使われているものと同じでなくてはならない。
- チェックサムは0で送信されるべきである。
- 受信者はUDPチェックサムに依存してはならない。ESPヘッダのSPIフィールドは0であってはいけない。

8.8.9 IKE ヘッダフォーマット

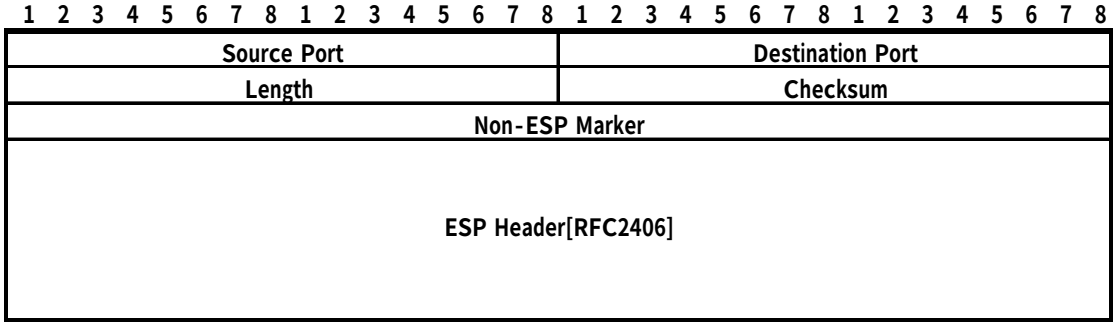


図 8-8 IKE ヘッダフォーマット

UDPヘッダは[RFC 768] にて定義されているヘッダである。[Kiv05]で定義され使われているものである。ここではIKEのパケットのチェックサムの扱いについてはなにも要求していない。Non-ESPマーカーは4バイトの0の並びである。

8.8.10 NAT キープアライブパケットフォーマット

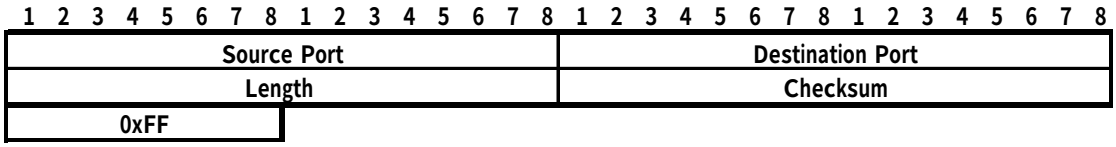


図 8-9 NAT キープアライブパケットフォーマット

UDPヘッダは[RFC 768] にて定義されているヘッダである。

- ソースポートとディスティネーションポートはUDPカプセル化されたESPパ　ケットのものと同じでなくてはならない。
- チェックサムは0で送信されるべきである。
- 受信者はUDPチェックサムに依存してはならない。

送信者は１バイトの 0xFF のペイロードを送るべきである、受信者はこの NAT キープアライブパケットを無視すべきである。

8.8.11 NAT されているトンネルモードのカプセルからの取り出し方法

パケットがトンネルモードで送信されてくる場合、内部の IP ヘッダは現在のネットワーク関係の無いアドレスが含まれる場合がある。この手順はどのようにして現在のアドレスに関連あるアドレスにすればよいのかを定義するものである。ロー

カルポリシーに依存するが、下記のどれかが必ず行われなければならない。

A. もし、ポリシーによって有効なソース IP アドレスが定義されているのであれば、相手から受信したパケットの内部の IP アドレスを確認することができる。
B. もし、リモートの相手の為にアドレスをアサインしているのであれば、内部の IP アドレスがそれと同じかどうか確認することができる。
C. NAT がパケットに対して行われており、それがローカルネットワークに対して運搬を行っている。

8.8.12 トンネルモードの UDP カプセル化と取り出し方法

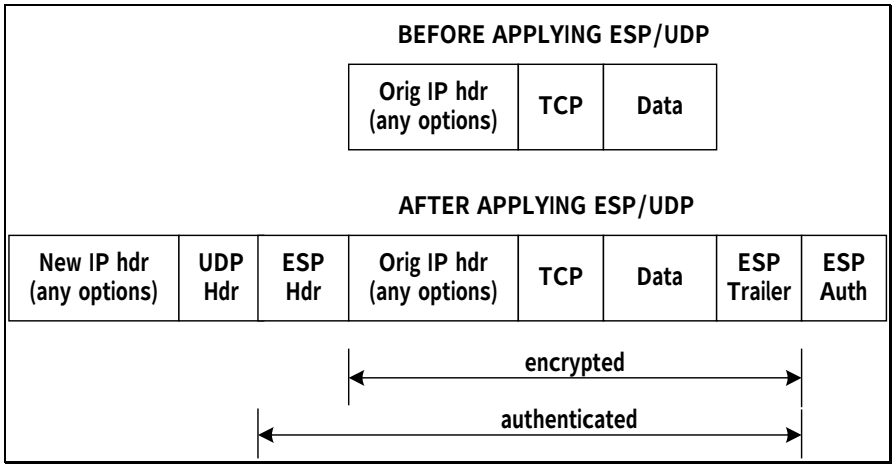


図 8-10 トンネルモードの UDP カプセル化フォーマット（ESP）

(1) カプセル化手順

1. 通常の ESP カプセル化を実行する。
2. 上記の様に正しいフォーマットの UDP ヘッダを挿入する。
3. パケット長、プロトコル、ヘッダチェックサムを結果として新しい IP パケットとして成立するように修正する。

(2) カプセル化からの取り出し手順

1. UDP ヘッダをパケットから取り除く。
2. パケット長、プロトコル、ヘッダチェックサムを結果として新しい IP パケットとして成立するように修正する。
3. 通常の ESP からの取り出し手順を実行する。
4. トンネルモードの NAT カプセルからの取り出しを行う。

8.8.13 トンネルモードコンフリクト

下記の様な状況が発生した場合、アドレスの重複が発生して A,B が同時に Server と通信を行う事ができなくなる。

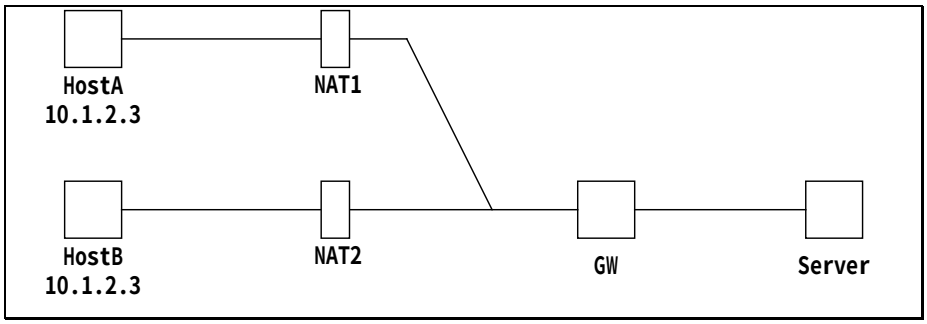


図 8-11 NAT コンフリクト

GW は 10.1.2.3 に対する SA を重複して持つ可能性がある。

これらの解決策として GW は HostA,HostB に対して DHCP over IPsec や NAT を用いて HostA,HostB をユニークに判別できる様にしてから Server へパケットを送出できるようにする必要がある。

8.9 まとめ

NAT-Traversal 技術はこの様に IPsec と NAT の組合せを可能にし、特に IPsecVPN 技術に必要不可欠な要素となりつつある。また、IPv6 の普及はアドレスの枯渇問題を払拭し IPsec にとって有利な状況をもたらすが、それでも今しばらくは IPv4 は必須であり、IPv6 に移行する状態では何らかの IPv4-IPv6 の変換技術も必要となってくるだろう。この様な状況下でも NAT-Traversal 技術は必要とされてくる。さらに、NAT-Traversal 技術は近い将来 IETF のスタンダードとなりマルチベンダー環境での相互接続性、信頼性に大きく貢献するものとなるだろう。

9 Appendix C 検証参加者

- ✧ SSH コミュニケーションズ・セキュリティ株式会社
  古川 徹
- ✧ 新日鉄ソリューションズ株式会社
  松島 正明
- ✧ セコムトラストネット株式会社
  若林 進二郎
- ✧ ソフトバンク BB 株式会社
  野尻 佐智子
- ✧ ソフトバンク･テクノロジー株式会社
  佐々木 憲一
- ✧ 株式会社ディアイティ
  山田 英史
- ✧ 株式会社ヒューコム
  加納 隼人
- ✧ 三菱電機株式会社
  宮川 明子

(50 音順)

- ✧ 学校法人工学院大学
  松木 和彦