セキュリティ・プロトコル講座

松本 直人（(株）インターネット総合研究所）

1999 年 12 月 16 日

Internet Week 99　パシフィコ横浜

（社）日本ネットワークインフォメーションセンター編

目次

1 概要

どれくらいの情報がネットワーク上を流れているかについて考えたことがありますか？　膨大な情報は、インターネットを含むネットワーク上をバイトストリームとして流れていきます。そのバイトストリームを、プロトコルによって解釈し、たとえば、HTTP リクエストや TELNET のセッションコマンドという意味のあるデータとして扱うことによって、処理が行われています。

ネットワーク上を流れるバイトストリームについては、暗号化されていない生のデータもあります。大事なデータが危ないことはないのでしょうか？

この講演では、データを守る「セキュリティ」について、次の事柄を説明します。

- セキュリティの概念と現状（2 を参照）
- セキュリティプロトコル概要（3 を参照）
- VPN の基本技術（4 を参照）
- セキュリティプロトコル詳細（5 を参照）
- 運用にあたって－まとめ－（6 を参照）
- 参考情報（7 を参照）

2 セキュリティの概念と現状

まず、「セキュリティ（Security）」という語の定義を確認しておきましょう。辞書を見れば、「安全、無事、安心、治安」、「防衛、防御、警備、保安」、「担保、抵当、保証」といった言葉が並んでいます。ネットワークセキュリティについても、その上を流れるデータを「守る」という点から、一般的なセキュリティの概念を当てはめてもかまわないと言えるでしょう。

ネットワークにおけるセキュリティの現状を見てみると、セキュリティというものを正しく理解せずに、「自閉症ネットワーク」となってしまっているネットワークがあるようです。ここで、自閉症ネットワークとは、次のような特徴を持ったネットワークを指します。

- 誰も信じない

  組織外部からの接続をいっさい認めないネットワークです。社内だけに閉じたネットワーク、勘定系システムのネットワークもその例ですし、以前から使われていた電話網における VPN も 1 つの例です。

- 誰も許さない

  基本的に一部のサービスの利用しか認めない（WWW とメールだけ等）、あるいは全部認めないネットワークです。

- 誰にも使わせない

  組織内での利用制限をかけているネットワークです。たとえば、金融システムにアクセスできるターミナルをターミナルルームだけに置き、入室申請を必要とする場合等です。

自閉症ネットワークは、ともすれば、より強固なセキュリティを保っていると過信しがちなネットワークとなってしまいます。このようなネットワークは、使っていて幸せなネットワークとは言えません。

セキュリティは、すべてを許す、許さないというものではありません。データを守ることによって、「ネットワークをより便利にするための概念」がセキュリティなのです。セキュリティをしっかりと理解し、考慮して使えば、閉鎖的でないネットワークができるはずです。

3 セキュリティプロトコル概要

3.1 3 つの基本的な分類

ネットワークのセキュリティプロトコルは、次の 3 つに分類されます。

- 認証（Authentication）

  ユーザが誰であるかを判別（認証）することです。組織内のユーザであることを確認し、もし、判別できなければアクセスを拒否します。

- 制御（Authorization。または Control）

  認証を基にユーザにサービスを割り当てることです。ユーザごとに、提供するサービスを管理します。サービスを利用する権限を与える、言い換えれば、制御を行うことになります。

- 防御（Defense）

  認証、制御で判断できないものを外敵とし、外敵から自らを防御することです。

認証、制御、防御のセキュリティフローは、図 1 のようになります。

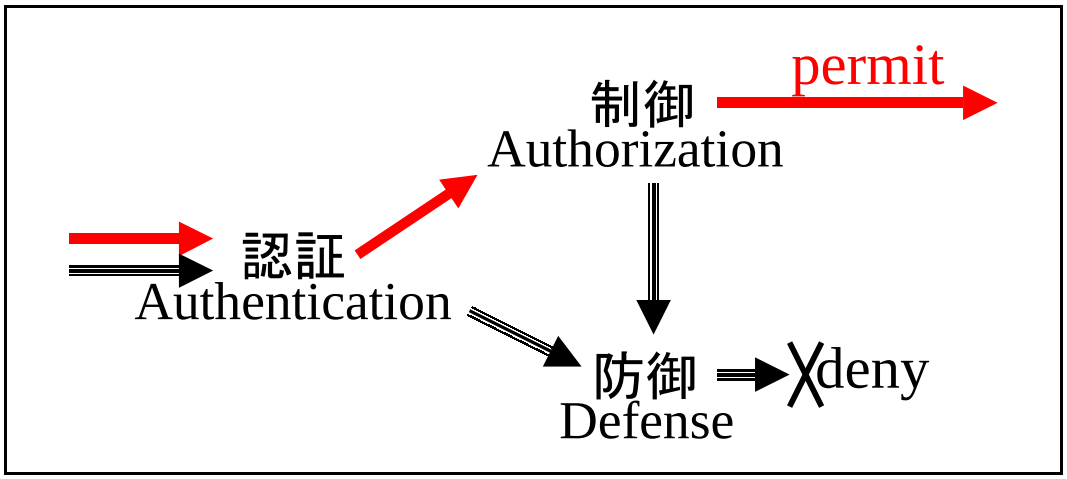


図 1：セキュリティフロー

セキュリティフローにおいて次のポリシーを守れば、セキュリティが保たれた状態でデータサービスが行えます。

1. すべては手順どおりに行われる。
2. 例外は存在しない。
3. 手順を満たさないものはすべて拒否する。

たとえば、特定のルータの enable 権限や特権モードが正しく設定され、権限が特定の人間に与えられ、認証が行われ、制御もされており、さらに何らかの形での防御も働いているとすれば、その組織は、セキュアチェーンでガードされていることになります。その様子を図 2 に示します。ここで、認証の箇所には鍵がかかっています。その鍵を開けるのはユーザ（もしくはマシン）です。

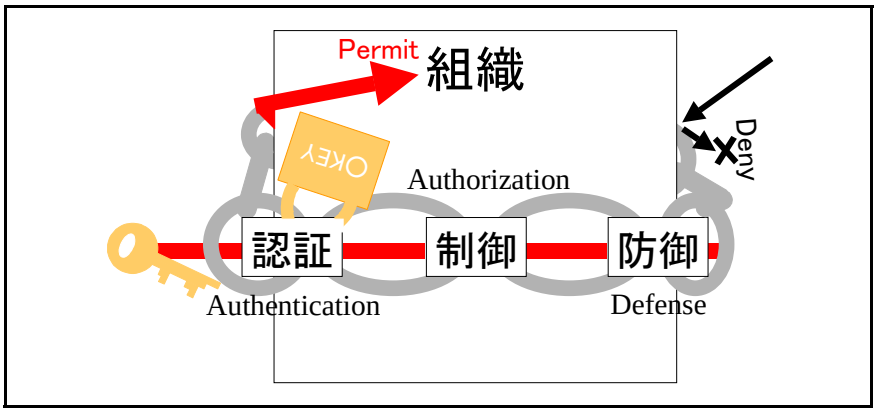


図 2：セキュアチェーン

3.2 認証

認証は、ユーザが誰であるかを判別することです。「家の鍵を持っている人が、その家に入ってもよい人である」というのと同じ考え方で、「認証情報を持っている（知っている）」ことによって、認証を行います。ただし、認証情報が容易に類推できるものだったら、認証のしくみが破綻してしまいます。

ユーザが組織にとって既知であることは、データベース上の情報と照らし合わせて確認します。データベース上にそのユーザの情報がなければ、拒否します。データベース上で管理される認証情報には、次のようなものがあります。

- Legacy password
- PassPhrase（パスワードより長いもの）
- OTP（One Time Password）
- Authentication Device （指紋、網膜、人相）
- Digital Sigunature（デジタル署名）

認証は、次の実装と密接に関連して機能します。

- RADIUS
- TACACS
- SecureID
- defender
- LDAP（データ保持の方法やプロトコルで使われる。認証スキームそのものではない）

3.3 制御

制御は、認証を終えたユーザに対して、適切なサービスを提供するものです。どのサービスを提供してよいかという情報については、やはりデータベース上で管理されます。

制御の実装は、認証の制御と一体であるケースが多いのが特徴です。標準化に伴い淘汰が進み、現在使われているのは次のプロトコルです。

- RADIUS
- TACACS
- TACACS ＋
- DAIMETER（RADIUS の次世代形）

3.4 防御

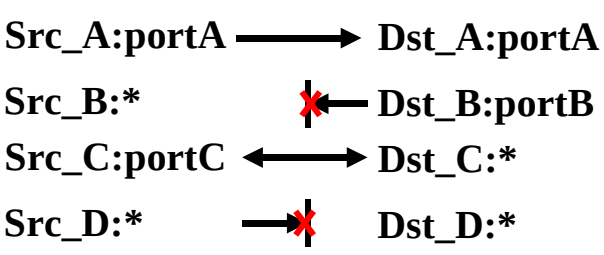
防御は、認めるべきではないサービスをはねつけるものです。外からのアクセスだけでなく、組織内から出て行くものも防御の対象となります。

防御は、主にファイアウォールの次の機能として実現されています。Replay Attack Detect と State Inspection については別の講演で詳しく説明されていますので、ここでは Packet Filtering についてのみ、さらに説明します。

- Packet Filtering（特定のパケットのみ通す）
- Replay Attack Detect（何回もリクエストしてくるものを検知する）
- State Inspection（ステートを見て判断する。たとえば、SMTP セッションが 100 張られっぱなしで、さらに増えていったらおかしい等）

図 3（A）に示すように、Packet filtering は「このソースアドレスからのパケットは通さない」、「このソースアドレスとこのポートからのパケットは通す」というように、あらかじめ防御項目を設定しておくことによって防御を実現するものです。図 3（B）のように、ファイアウォールについてアクセスグループを設定するのも一例です。

(A)



(B)

```
interface Ethernet 0/0
  ip access-group 110 in
  ip access-group 111 out
  !
  access-list 110 deny   udp any 224.0.0.0 31.255.255.255 eq syslog
  access-list 110 deny   udp any host 10.238.101.17
  access-list 110 permit udp any eq 500 any eq 500
  !
  access-list 111 deny 50 any any

  access-list 111 permit udp any eq 500 any eq 500
```

図 3：Packet Filtering

防御は、ネットワーク上の組織に対する攻撃（アタックやクラック）に対して有効に働きます。防御を行う上では、「ネットワークは脆弱的システムで構成されている」ということを念頭に置き、未知のシステム脆弱性の防御、既知のシステム脆弱性の防御、その両方に対する防御方法を理解することが必要です。既知のシステム脆弱性を知るためには、BUGTRAQ や Firewall Defenders（アクセス先については 21 ページの「参考情報」を参照）等から情報を積極的に集めるとよいでしょう。

今まで説明してきた、認証、制御、防御を的確に機能させれば、ネットワークは「確実に管理された網」となります。これらをインターネットに適用すれば、インターネットは利便性の高い組織ネットワークともなります。

4 VPN の基本技術

4.1 VPN の概要

最近のインターネットの動向を見ると、インターネットの規模拡大やモバイル環境の普及に伴い、接続形態が多様化していることと、VPN（Virtual Private Network）のニーズが高くなっていることが挙げられます。VPN と言えば、以前は電話網におけるものでしたが、最近は主にインターネットにおけるものを指すようになっており、ここでもインターネットの VPN について説明します。

VPN は、たとえばモバイル PC と企業のネットワークをインターネット経由で接続することによって、インターネットを利用した仮想的な専用ネットワークを構築するものです。VPN はトンネリング技術の集積技術です。よく誤解されることですが、「VPN ＝セキュリティ」ではありません。VPN のセキュリティ機能はオプションです。

VPN には、データの暗号化による暗号化機構と接続認証機能による認証機構があり、それらによってセキュリティを実現することができます。認証、制御、防御を的確に VPN に適用すれば、より柔軟な広域組織ネットワークを構築することができるのです。

4.2 VPN の種別

VPN には、次のように階層モデルごとにさまざまなものがあります。

- アプリケーション層での VPN
  - SOCKS
  - SSL（Secure Socket Layer）
  - SSH（Secure Shell）
- IP 層での VPN
  - IPsec（IP Security）
  - IPinIP
  - MobileIP
- データリンク層での VPN
  - L2TP（Layer 2 Tunneling Protocol）
  - PPTP（Point-to-Point Tunneling Protocol）
  - L2F（Layer 2 Forwarding protocol）
  - MPLS（Multi-Protocol Label Switch）
  - MPOA（Multi-Protocol Over ATM）
  - MobilePPP

各層の VPN には、図 4 に示すような相関があり、ニーズ等に応じて選択することも可能です。

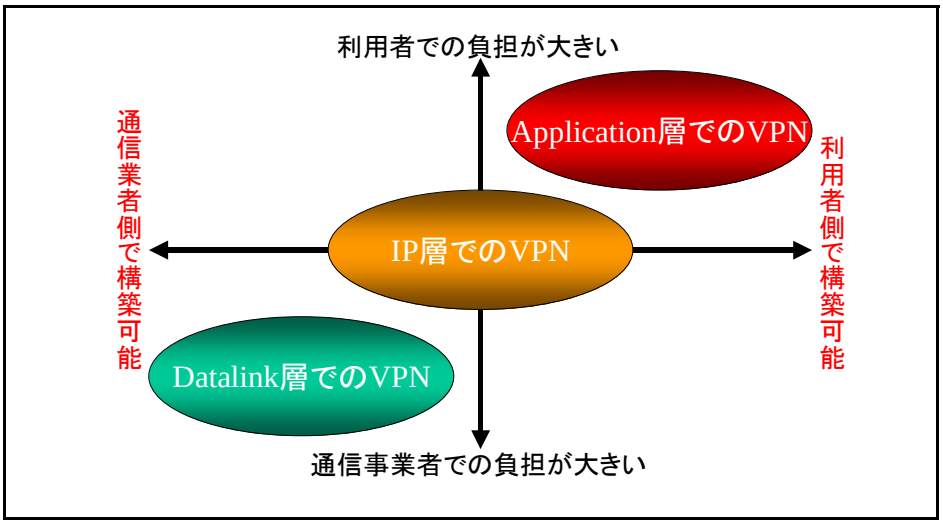


図 4：各層における VPN

4.3 VPN の使用形態

VPN の使用形態には 2 種類あります。図 5（A）に示すコンセントレータ型の使用形態では、すべての終端が集積されて、VPN Device からの単一方向での接続となります。その一方、図 5（B）に示すエンドーエンド型の使用形態はフルメッシュに近いもので、双方向の接続になります。

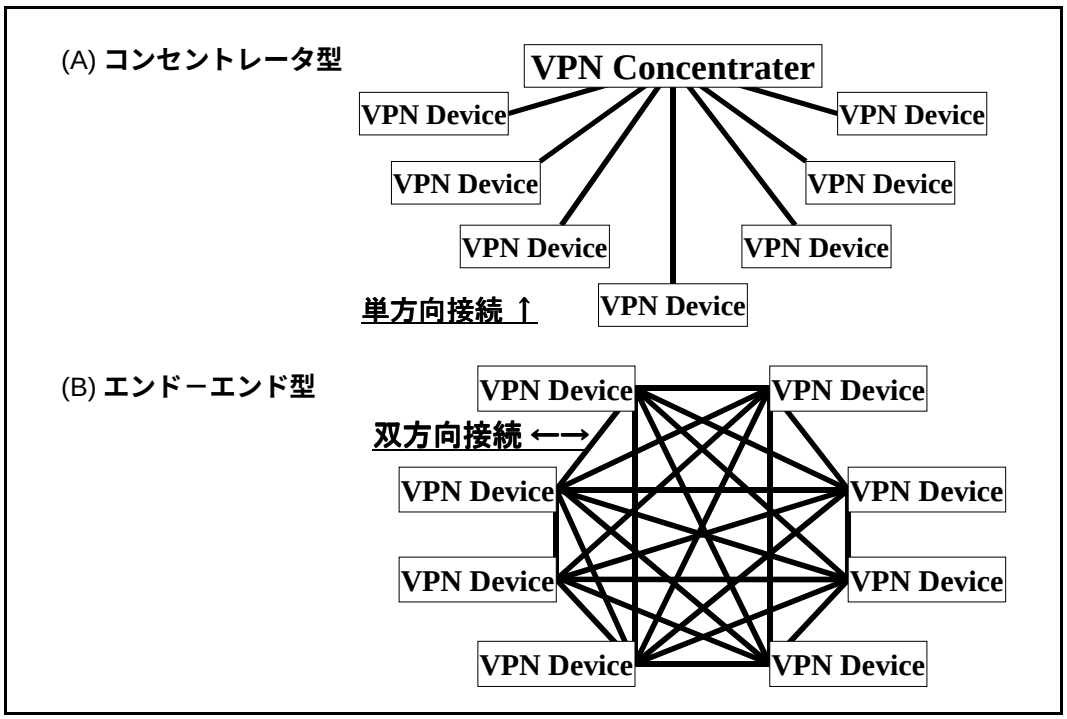


図 5：VPN の使用形態

5　セキュリティ・プロトコル詳細

引き続き、いくつかのセキュリティプロトコルについて詳細を説明します。ここで取り上げるのは、図 6 に示す 3 つのセキュリティプロトコルです。RADIUS が認証と制御の 2 つの機能を持つように、セキュリティプロトコルには、複数の機能を持つものが多数あります。

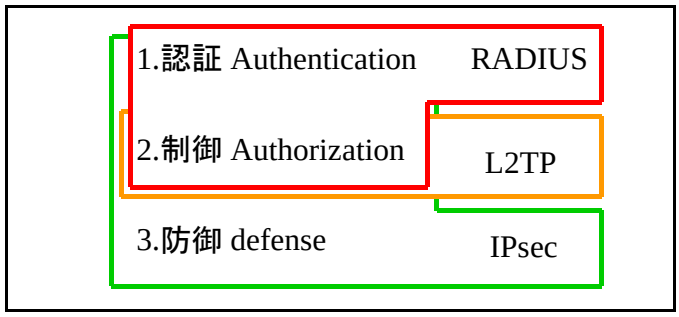


図 6：説明するセキュリティプロトコル

5.1 RADIUS

RADIUS（Remote Access Dail-In User Service）は、認証と制御の機能を持つプロトコルであり、リモートアクセスユーザ向けのサービスに利用されています。RADIUS に関しては、RFC2138 Standards Track に RADIUS 全般に関する記述があり、課金については RFC2139 で規定されています。

RADIUS は、RADIUS サーバと RADIUS クライアントというサーバクライアントモデルで動作します。NAS（Network Access Server）を RADIUS クライアントとした場合の例を図 7 に示します。

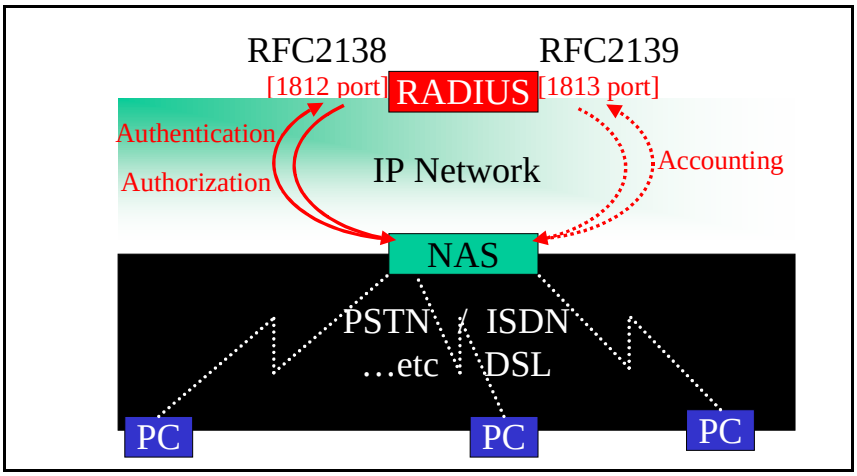


図 7：RADIUS のしくみ（1）

RADIUS においてどのような情報がやりとりされて、接続、切断が行われるかを図 8 に示します。

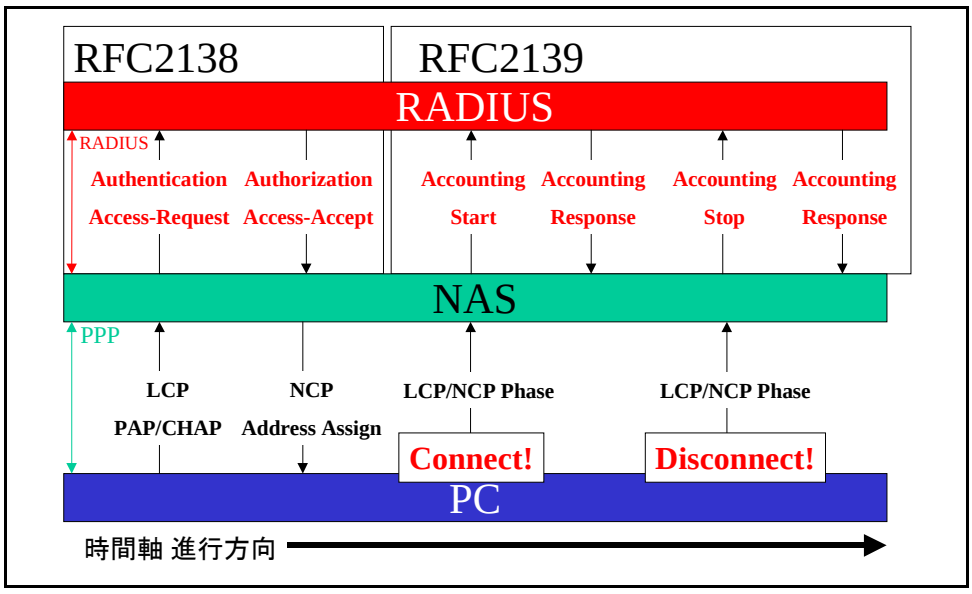


図 8：RADIUS のしくみ（2）

まず、Access Request では、RADIUS 接続を求めるユーザ名や暗号化されたパスワード等の情報が Radius サーバに送られます。Radius サーバには Authentication Database があり、そのデータとパスワードの対応を確認して認証が行われます。そして、Access Accept では、RADIUS サーバから取得したユーザサービスの設定情報が NAS に伝えられます。伝えられる情報には、そのユーザのタイムアウト時間等があります。

RADIUS では障害発生に備えて、図 9 に示すような冗長な構成をとることがあります。この場合、Authentication Database のデータを一元管理し、不整合が発生しないように注意する必要があります。

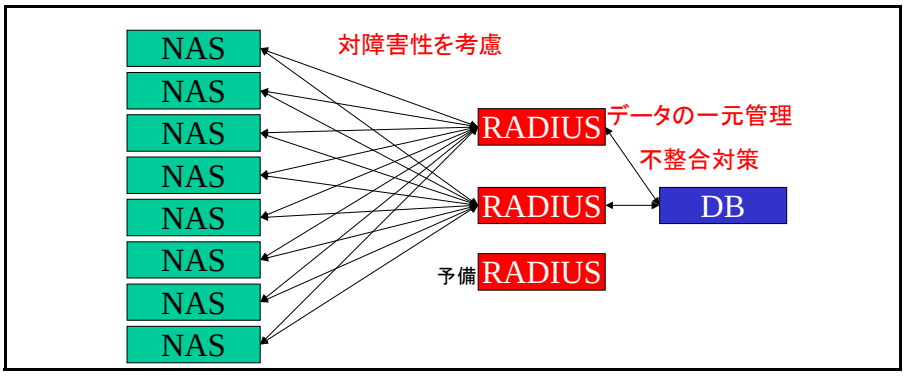


図 9：RADUIS の構成例

RADIUS サーバは、エラーや処理関連のログ（RADIUS システムログ）、および課金関連のログ（RADIUS アカウンティングログ）を蓄積します。図 10 に RADIUS システムログの例を示します。

```
Thu Feb  4 13:13:36 1999: Authenticate: Password check error for
                          ppp-joe: 10.238.101.162.1025, id=180
                           :
                           :
Wed Sep 15 11:51:35 1999: Calc_digest: Wrong NAS Address:
                            10.238.101.162.1025, id=133
Wed Sep 15 16:16:13 1999: Authenticate: Neither User Nor Default Name
                           for not@iri.co.jp: 10.238.101.17.1645, id=0
Wed Oct 13 20:48:21 1999: forward_duplicate_request: Backlog of 501
                                                  exceeds 500 requests
Tue Nov  9 15:05:30 1999: Authenticate: Neither User Nor Default Name for
                                not@iri.co.jp: 10.238.101.17.1645, id=12
```

図 10：RADIUS システムログ

図 10 のログからは、「ppp-joe というユーザがパスワード入力を間違ったこと」、「未定義の NAS からアクセスがあったこと」、「RADIUS request が何らかの問題により重複したこと」が分かります。RADIUS プロトコルは UDP で動作しているので、UDP の順序がおかしくなったりすると、重複が発生します。負荷が高いと重複が増え、場合によっては RADIUS サーバが落ちてしまうこともありますが、そこを狙ったクラッキングもありますので、注意が必要です。

5.2 L2TP

L2TP（Layer Two Tunneling Protocol）は制御の機能を持つプロトコルです。L2TP は最近 Standards Track となった RFC2661 で規定されており、次の機能を持ちます。

- PPP の終端先を IP 網の向こうに飛ばす。
- IP 網上に、PPP できる環境（回線環境管理を含む）を構築する。
- PPP の集積と処理を行う。

つまり、L2TP は「PPP over IP」を実現するための機能であり、PPP はトンネリング技術そのものと言ってもよいでしょう。L2TP によって、PPP が持つステート保持や再送等の機能を、本来ステートレスである IP 上で実現できます。このため、ISP の既存の接続環境資源を共有したり、ネットワークの既存ユーザと仮想ダイヤルアップユーザを共存させたりできるようになります。

ここで注意が必要なのは、L2TP には暗号化アルゴリズムが含まれていない点です。L2TP による接続で暗号化を行うには、PPP Encryption（Layer 2 Encryption）、IPsec（Layer 3 Encryption)、Application Layer Encryption 等のプロトコルを併用します。また、L2TP は、制御については PPP とともに処理を行いますが、認証については RADIUS 等に依存し、防御に関しては上位層（IP 層）での機能に依存するということからも、他の機能との連携が必要です。

L2TP では、図 11 に示すように、PPP データグラムをカプセル化し、カプセル化データを搬送（UDP）する「LAC（L2TP Access Concentrator）」と、PPP データグラムをカプセルから抽出し、PPP 上で LCP/NCP 処理を実行する「LNS（L2TP Network Server)」が重要な役割を果たします。

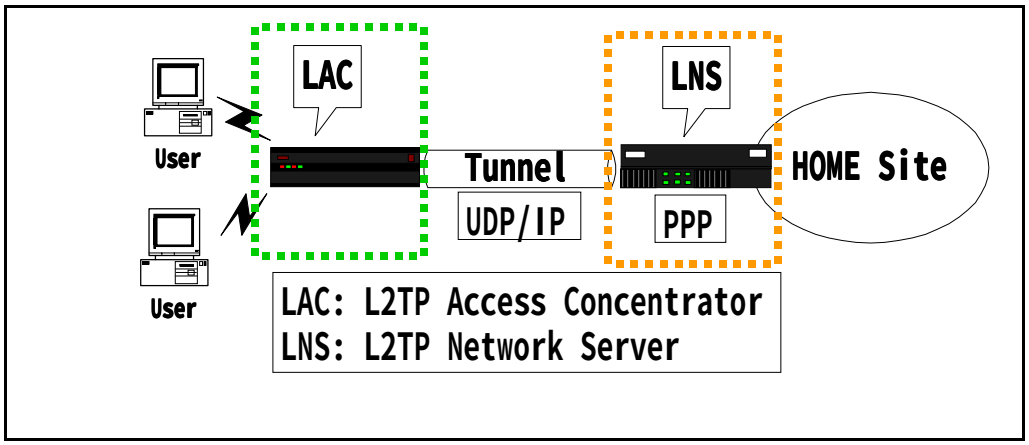


図 11：L2TP の処理イメージ

LAC（Cisco）の設定例を図 12 に、LNS（Assend Max）の設定例を図 13 に示します。

```
aaa new-model                                                  認証機能を定義
aaa authentication login default local
aaa authentication ppp default local
aaa authorization exec default local
aaa authorization network default local
vpdn enanle                                                    VPDN を有効化
vpdn domain-delimiter @ suffix                                 @ がデミリタ
vpdn-group 1
 request dialin l2tp ip 10.10.10.17 domain l2tp.net  @l2tp.net でマッチ
 local name LAC00                                              自分の名前は LAC
 l2tp tunnel password FoRL2TPPaSSwoRD                          L2TP Auth 用
```

図 12：LAC 設定例

```
Ethernet->Mod config ->L2 Tunneling options
  L2TP Mode=LNS                                  LNS として機能
  L2TP Auth Enabled=Yes                          L2TP Auth を使う
  L2TP System Name=LNS00                         自分の名前は LNS
Ethernet->Names / Passwords                      nat@l2tp.net 用プロファイル
  Name=nat@l2tp.net
  Active=Yes
  Recv PW=l2tpPaSSwoRD
Ethernet->Names / Passwords                      LAC-LNS 間用プロファイル
  Name=LAC00                                     LAC00 のプロファイル
  Active=Yes                                     有功化
  Recv PW=FoRL2TPPaSSwoRD
```

図 13：LNS 設定例

まず、ユーザが LAC に接続することによって処理が始まります。LAC は情報を取り出して、接続相手先を特定します。そして、LNS 上で L2TP トンネルの認証が行われ、L2TP が確立されます。LAC が L2TP パケットをすべて送出した後、処理が LNS に移ります。L2TP が確立されて初めて、PPP 処理が始まります。そして、PPP 接続が確立されると、接続完了となります。この様子を図 14 に示します。

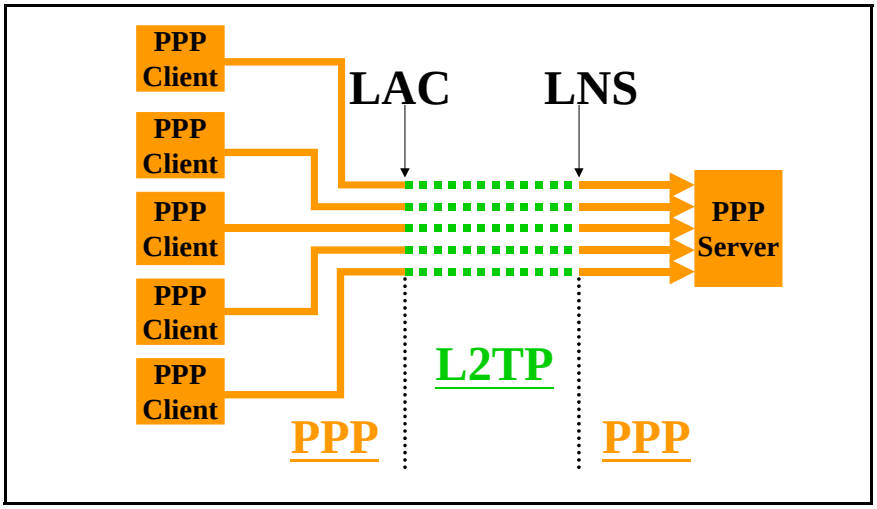


図 14：L2TP 網の状態

図 14 に示すように、L2TP によってインターネット上の PPP セッションが集約されますが、QoS や Diffserve を利用する場合は、1 つの PPP セッションに 1 つの L2TP ということもあります。

切断の際は、まず、PPP が終了し、次に L2TP が終了します。

L2TP については各ベンダーによる実装が行われていますが、異機種間の相互接続についてはほぼ問題ありません。今後は、スケールに応じた標準化が提唱され、実装の変更が求められていくでしょう。スケールのためには、外部でユーザ情報を持つ必要があります。そのためには、たとえば、RADIUS と L2TP の連携も求められます。

5.3 IPsec

IPsec（IP security protocol）は、IP 層で実装されるプロトコルであり、IP に認証と暗号化機能を付加し、IP だけのデータ伝送を行うものです。IPsec については、表 1 に示すように多くの RFC があります。

表 1：IPsec の RFC

RFC	内容
RFC 1320	The MD4 Message-Digest Algorithm
RFC 1321	The MD5 Message-Digest Algorithm
RFC 1828	IP Authentication using Keyed MD5
RFC 1829	The ESP DES-CBC Transform
RFC 2040	The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms
RFC 2085	HMAC-MD5 IP Authentication with Replay Prevention
RFC 2104	HMAC: Keyed-Hashing for Message Authentication
RFC 2144	The CAST-128 Encryption Algorithm
RFC 2202	Test Cases for HMAC-MD5 and HMAC-SHA-1
RFC 2268	A Description of the RC2(r) Encryption Algorithm
RFC 2401	Security Architecture for the Internet Protocol
RFC 2402	IP Authentication Header
RFC 2403	The Use of HMAC-MD5-96 within ESP and AH
RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2406	IP Encapsulating Security Payload (ESP)
RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408	Internet Security Association and Key Management Protocol
RFC 2409	The Internet Key Exchange (IKE)
RFC 2410	The NULL Encryption Algorithm and Its Use With IPsec
RFC 2411	IP Security Document Roadmap

表 1：IPsec の RFC（続き）

RFC	内容
RFC 2412	The OAKLEY Key Determination Protocol
RFC 2451	The ESP CBC-Mode Cipher Algorithms
RFC 2631	Diffie-Hellman Key Agreement Method
RFC 2521	ICMP Security Failures Messages
RFC 2522	(E) Photuris: Session-Key Management Protocol
RFC 2523	(E) Photuris: Extended Schemes and Attributes
RFC 2709	Security Model with Tunnel-mode IPsec for NAT Domains

IPsec には次の 3 つのしくみがあります。それぞれについては後で説明しますが、IPsec 接続では図 15 に示すように、IKE で接続形態を調整した後に接続が開始されます。IPsec デバイス同士が、IPsec によって接続されている状態を「SA（Security Association）」と呼びます。

- IKE（Internet Key Exchange）
- AH（Authentication Header）：トランスポートとトンネルの 2 モード
- ESP（Encapsulating Security Payload ）：トランスポートとトンネルの 2 モード

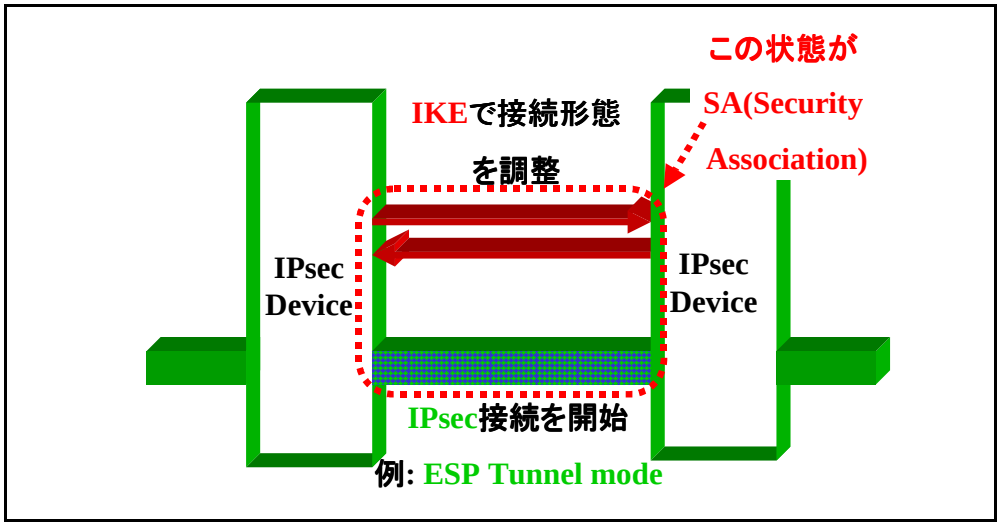


図 15：IPsec 接続

5.3.1 IKE

IKE（Internet Key Exchange）は、IP デバイス同士が「自分はこういう認証アルゴリズムを使っている」という情報を相互にやりとりするしくみです。やりとりは、UDP 500 番ポートを使って、IP 層上で行われます。そして、IKE によって接続形態が調整された後、SA が確立されます。

IKE でやりとりされる情報には、次のようなものがあります。

- Encryption algorithm（暗号化方式。DES-CBC 等）
- Hash algorithm（ハッシュ方式。MD5 等）
- Authentication method（認証方式。pre-shared key）
- Group Description（MODP、ECP、EC2N 等）
- Life Type（seconds、kilobytes）
- PRF（Pseudo-Random Functions）

5.3.2 AH

AH（Authentication Header）は IP パケット単位の認証機構であり、IP パケットに認証ヘッダを付加してやりとりするものです。認証ヘッダが付いていない IP パケットは受け付けません。なお、AH には暗号化機能は含まれません。

AH には、トランスポートモード、およびトンネル用の IP ヘッダも付加されるトンネルモードという 2 種類があります。AH のフォーマットを図 16 に示します。

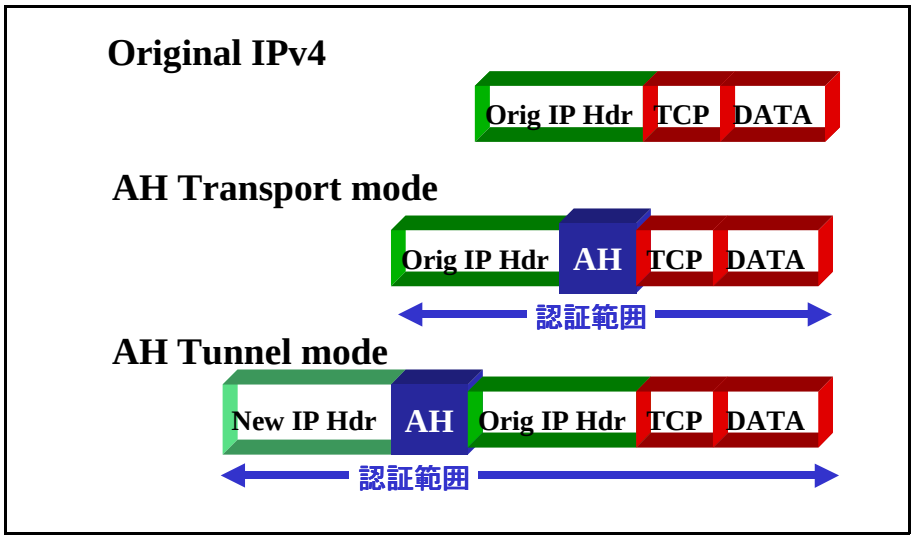


図 16：AH フォーマット

5.3.3 ESP

ESP（Encapsulating Security Payload ）は、AH と同様の IP パケット単位の認証機構であり、トランスポートモードとトンネルモードの 2 種類があります。ただし、AH とは異なり、ESP には IP パケット単位での暗号化機能が含まれています。

ESP のフォーマットを図 17 に示します。

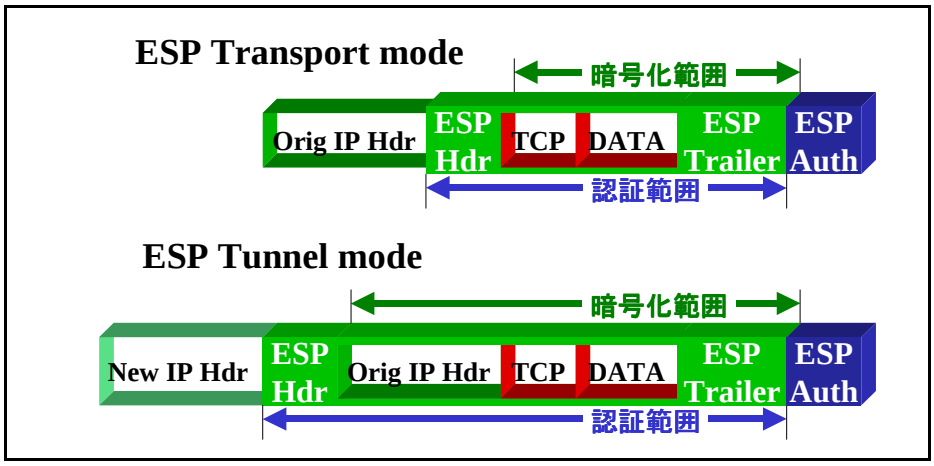


図 17：ESP フォーマット

5.4 IPsec の実装

IPsec の実装にあたっては、次の 2 種類の形態があります。「IPsec ＝ VPN」ということではないのですが、形態は VPN によく似ています。

- コンセントレータ型

  図 18（A）に示すように、IPsec クライアントと IPsec コンセントレータを接続し、IPsec クライアントからの単方向接続を行うものです。

- エンドーエンド型（(B)）

  図 18（B）に示すような形で、VPN デバイスと複数の IPsec SGW（Security GateWay）を接続し、双方向接続を行うものです。

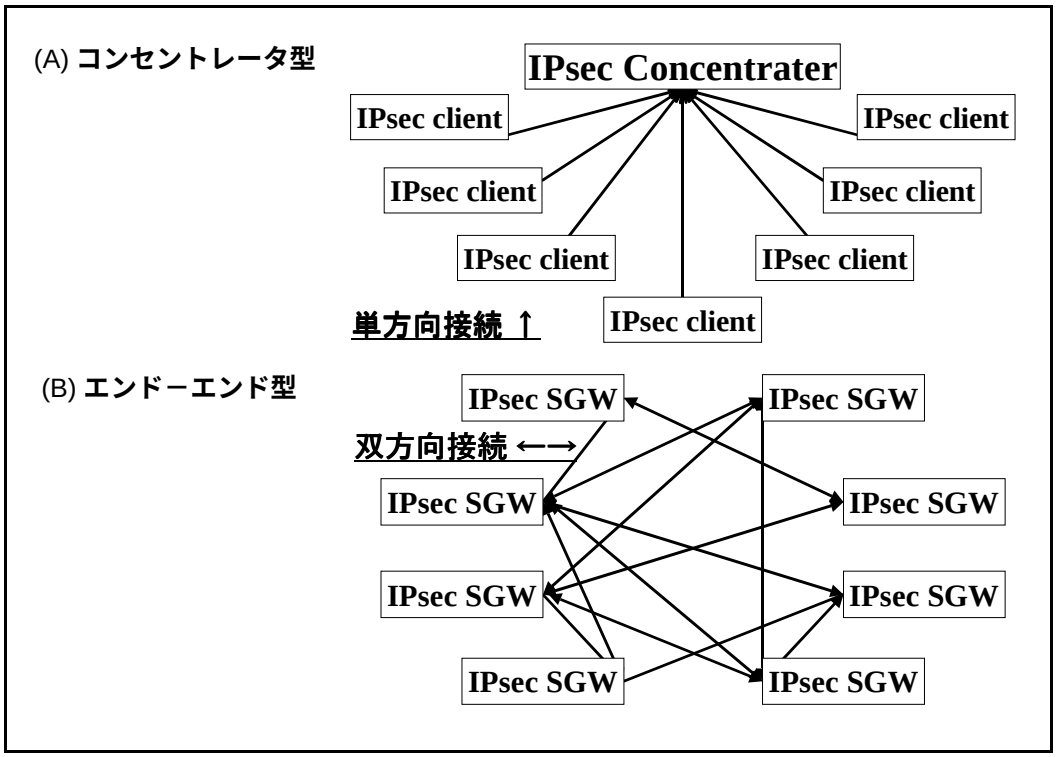


図 18：IPsec の実装形態

ここで、IPsec の具体的な実装について、設定例をいくつか紹介しましょう。

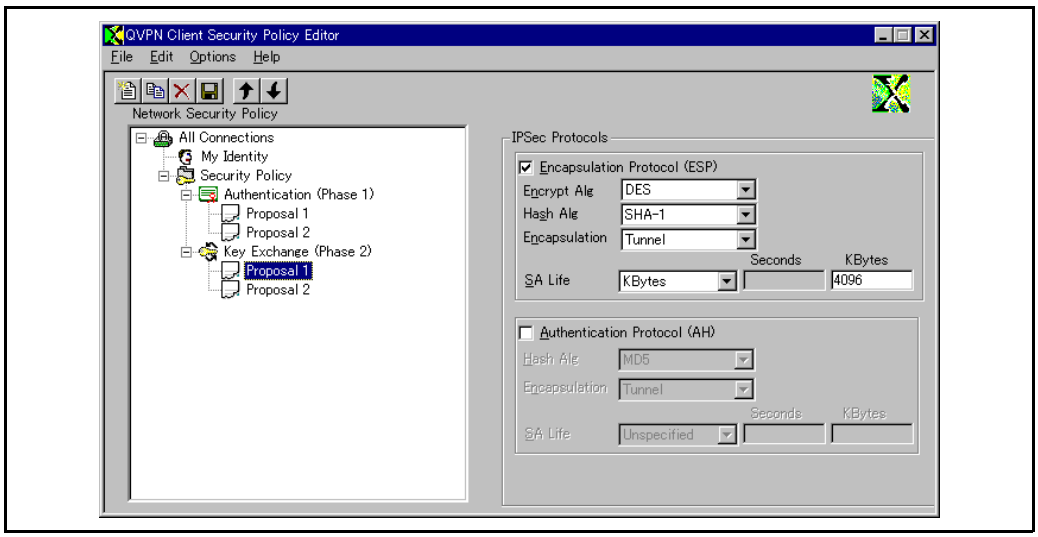


図 19：IPsec の実装（1）

図 19 はコンセントレータ型の実装で、暗号化方式に DES を、ハッシュ方式に SHA-1 を使う ESP の設定を行っています。複数のフェーズごとに設定を変えられるようになっています。これは IPsec の良いところでもあり、複雑なところでもあります。

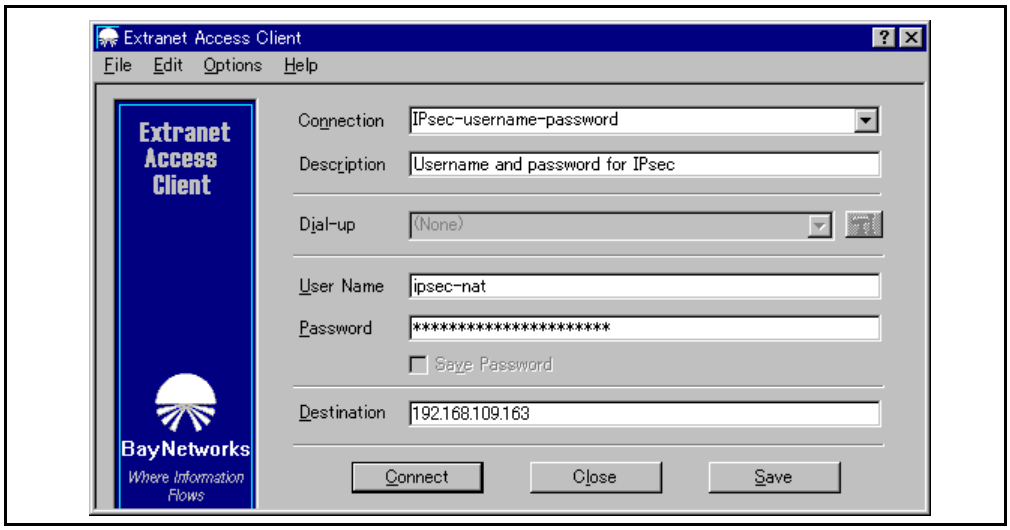


図 20：IPsec の実装（2）

図 20 もコンセントレータ型の実装です。プリシェアードキーではなく、ユーザ名とパスワードを使用しています。

```
# RT100i Rev.3.01.13 (Thu Mar 25 11:35:41 1999)
ipsec auto refresh on
ipsec ike host 10.13.10.26
ipsec pre-shared-key 10.13.10.26 text himitsu
ipsec sa policy 101 10.13.10.26 esp des-cbc md5-hmac
tunnel select 1
ip tunnel route add net 192.168.101.0/24 2
ipsec tunnel 101
tunnel enable 1
```

図 21：IPsec の実装（3）

図 21 はエンドーエンド型の実装における IPsec SGW の設定例です。

設定に従って、IPsec が正しく機能し、きちんと接続されているかどうか、実際の動作内容がどうか等を確認するためには、IPsec ツールを利用する必要があります。例として、フリーソフトのIPsecツールであるThe Ethernet Network Analyzer を図 22 に示します。

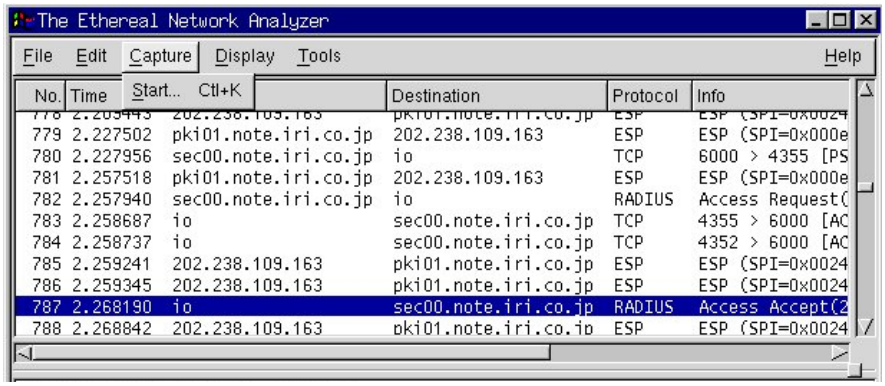


図 22：IPsec ツールの例

6 運用にあたって－まとめ－

セキュリティの概念に始まり、VPN やセキュリティプロトコルについて説明してきましたが、最後に、ネットワーク運用にあたっての注意事項をまとめます。

セキュアなネットワーク運用を行うための第一歩は、セキュリティ担当者を組織に置くことです。ネットワークにとってが何が怖いのか、何が危ないかをしっかり把握している人物が組織には必要です。セキュリティ担当者は、幅広い視野を持って、セキュリティプロトコルの内容をしっかり理解しなければなりません。

技術習得はどこから始めてもかまいません。たとえば、「まず、L2TP から始めよう」と決めたなら、そこから上下の層へと広げていけばよいのです。運用の中で、必然的に他のセキュリティプロトコルについても学んでいくことになります。

セキュリティ担当者は、セキュリティプロトコルの最新動向にも注目しておく必要があります。さまざまな標準化が進み、実際に使われ始めています。実装についても、やはり情報を集めなくてはなりません。相互接続については、最近はほぼ問題なく繋がるようにはなっていますが、今なら、たとえば、Windows 2000 の IPsec について、自分が管理しているデバイスが対応できるかどうかを調べておくといったことも必要かもしれません。

また、大変重要なのが、セキュリティホールに関する情報をしっかり集め、設定変更等によってそれに対応することです。どんなセキュリティプロトコルが開発されて、実装されていったとしても、セキュリティホールはどうしても出てきます。その確実なフォローを行うためにも、セキュリティ担当者が必要であることを組織は認識し、その担当者を支えていくべきでしょう。

7 参考情報

- BUGTRAQ

  BUGTRAQ-JP@SECURITYFOCUS.COM
  BUGTRAQ@SECURITYFOCUS.COM

- Firewall Defenders

  http://www.firewall.gr.jp/

- RADIUS-JP ML（RADIUS Discussion List in Japan）

  http://www.certworks.net/radius/

- VPN Operators Homepage

  http://www.vpnops.org/

  「公開できるものは公開しあおう」というポリシーの下、相互接続の実験や勉強会も開催（現在、600 名のメンバー）。

- PKI-Talk/JP ML（PKI Talk List in Japan）

  ppserv@certworks.net
  http://www.certworks.net/pki/

- IDS（Intrusion Detection Systems：進入者検知システム）

  ids-jp@certworks.net

  メーリングリスト運用開始。