# CentreNET® AT-VPN Client

# ユーザーマニュアル

アライドテレシス株式会社

P/N J613-M4460-00 Rev.E 030616

# 目次

# 1 はじめに

このたびは CentreNET AT-VPN Client（以下 AT-VPN Client）をお買い上げいただきまして誠にありがとうございます。AT-VPN Client は、Windows コンピューターを IPsec[1] 準拠の VPN クライアント[2] として動作させるためのソフトウェアです。AT-VPN Client を使用すると、インターネットに接続されたコンピューター[3] と、あらかじめ指定しておいたサイト（AR ルーター）との間で VPN 通信[4] を行うことができます。また、指定したサイト以外（インターネット全般）に対しては通常の IP 通信を行えます。したがって、出張先のホテルからインターネットサービスプロバイダー（以下 ISP）にダイヤルアップ接続し、VPN 通信によって勤務先の LAN に安全にアクセスしつつ、インターネット上の Web サイトで情報収集などを行うことが可能です。

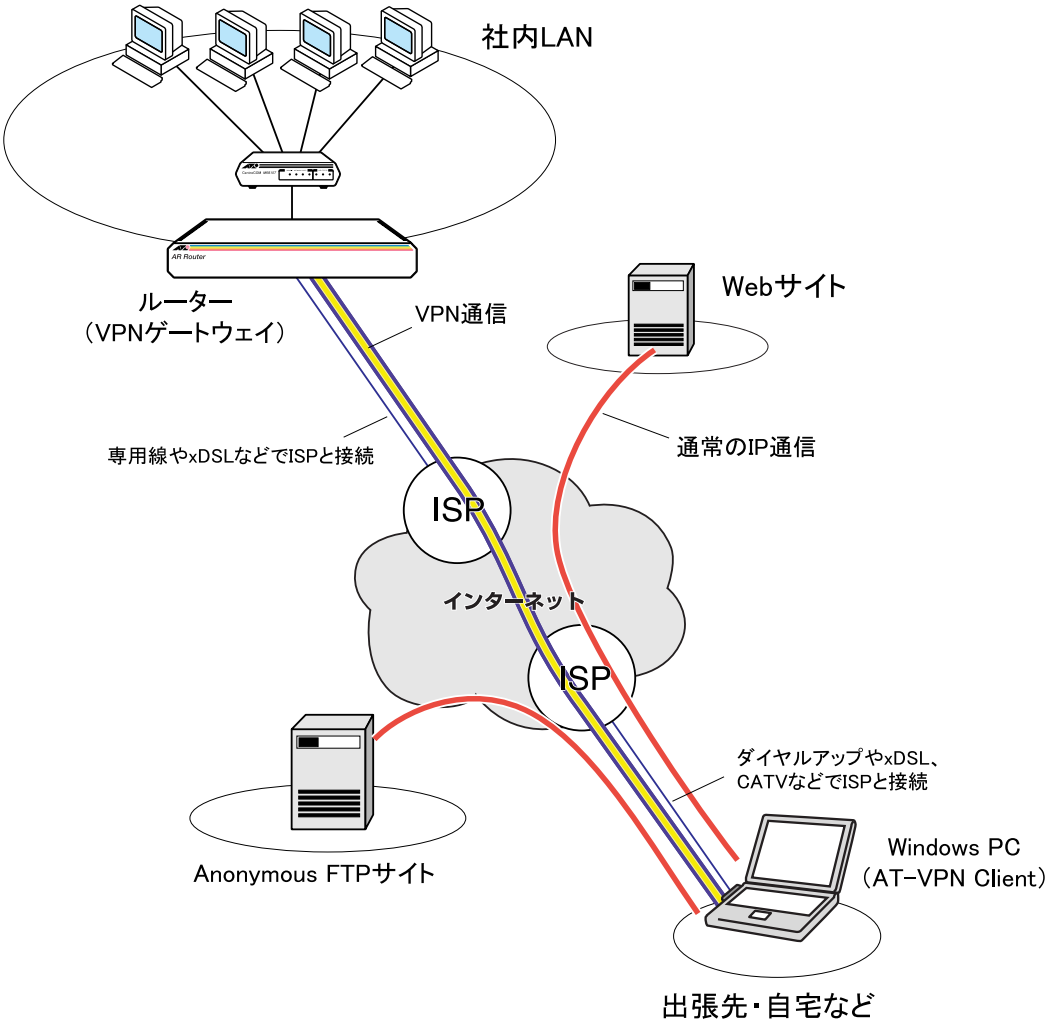


**図 1.0.1 AT-VPN Client の使用例**

1. IPsec（IP security）は、インターネットの通信プロトコルである IP（Internet Protocol）に暗号化や認証などの機能を与える一連のプロトコル / アーキテクチャーを総称したもので、後述する VPN の基盤として使用されます。
2. AT-VPN Client が動作しているコンピューター上で、Web サーバーや FTP サーバーなどのサーバーアプリケーションを運用することはできません。
3. モデムや TA によるダイヤルアップ接続環境だけでなく、事業所 LAN や CATV インターネットサービスなどを利用した LAN アダプター経由のインターネット接続環境でもご使用いただけます。また、xDSL など、PPPoE プロトコルによるインターネット接続環境での使用も可能です。さらに Version 1.5 からは、AT-VPN Client と AR ルーターの間にアドレス変換（NAT）装置が入るようなネットワーク構成でも VPN 通信ができるようになりました（UDP トンネリング機能（ESP over UDP））。
4. VPN（Virtual Private Network）は、特定の接続先との通信を暗号化することにより、盗聴やなりすましを防ぎ、インターネット上に仮想的なプライベートネットワークを実現する技術です。

## 1.1 本書の構成

本マニュアルは 2 部構成になっています。AT-VPN Client を使用するユーザーの方は第 1 部を、AT-VPN Client と AR ルーターを使って VPN を構築・管理するネットワーク管理者の方は第 1 部と第 2 部をお読みください。

- **第 1 部 ユーザー編**
  AT-VPN Client をコンピューターにインストールし、ネットワーク管理者から提供された情報をもとに VPN 通信を行うまでの手順について解説しています。AT-VPN Client をご使用になる方が対象です。

- **第 2 部 アドミニストレーター編**
  AT-VPN Client を使って VPN を構築するには、AR ルーター（VPN ゲートウェイ）と AT-VPN Client の両方の設定を行う必要があります。「アドミニストレーター編」では、AR ルーターと AT-VPN Client の基本的な設定例を紹介しています。また、AT-VPN Client の設定ファイルで使用するコマンドについてもまとめています。第 2 部は VPN の構築・管理を担当するネットワーク管理者が対象です。なお、管理者の方は第 1 部もあわせてお読みください。また、ルーターの設定方法については、AR ルーター付属の取扱説明書、コマンドリファレンス、設定例集などもご参照ください。

# 第 1 部 ユーザー編

「ユーザー編」では、AT-VPN Client を実際にご使用になるユーザーの方を対象に、AT-VPN Client ソフトウェアのインストールから VPN 通信を行うまでの手順について解説します。また、AT-VPN Client の各メニュー項目についてもまとめています。

# 2 概要

## 2.1 動作環境

AT-VPN Client を使用するためには、ご使用のコンピューターシステムが以下の要件を満たしている必要があります。[1]

- CPU：Pentium 133 MHz 以上
- メモリー：128MB 以上
- ハードディスク空き容量：10 MB 以上
- オペレーティングシステム（OS）[2]：
  日本語版 Windows 98、Windows 98 Second Edition、Windows Me（Millenium Edition）、Windows 2000 Professional（SP2 以上）
- ネットワークアダプター：
  Microsoft 製 PPP ダイヤルアップアダプター[3]、PPPoE アダプター[4]、Ethernet LAN アダプター
- その他：USB ポート（USB SecureKey を使う場合のみ）[5]

## 2.2 AT-VPN Client の使用開始まで

AT-VPN Client の使用を開始するまでの手順は次のようになります。

### 1 IP 通信の設定

AT-VPN Client を使用するためには、AT-VPN Client を実行するコンピューターと接続先の AR ルーター（VPN ゲートウェイ）との間で、IP による直接通信ができる必要があります。[6] AT-VPN Client をインストールする前に、インターネットサービスプロバイダー（ISP）に接続するための設定や、LAN アダプター、TCP/IP の設定等を完了しておいてください。

### 2 VPN 設定情報の入手

AT-VPN Client の設定は、VPN 設定情報（セキュリティーポリシー）を読み込ませることによって行います。ネットワーク管理者から次のいずれかを入手してください。これらの情報は、AT-VPN Client をインストールするときに必要になります。

- セキュリティーポリシーファイル（拡張子「.spl」のテキストファイル）[7]
- ポリシーサーバーの IP アドレス、パスワード、ユーザー名（オプション）

1. VPN ゲートウェイとして動作させる AR ルーターの要件については、「第 2 部 アドミニストレーター編」（p.26）をご覧ください。
2. 英語版 OS はサポート対象外です。
3. Windows 標準装備の「ダイヤルアップアダプタ」。別途、モデム、TA などが必要です。
4. NTT 東日本 / 西日本提供の「フレッツ接続ツール」付属 PPPoE ドライバー。
5. ご使用の OS 上で USB 機器が使用可能な状態になっている必要があります。
6. UDP トンネリング機能を利用すれば、AT-VPN Client と AR ルーターの間にアドレス変換（NAT）装置が入るようなネットワーク構成でも本製品を使用できます。
7. セキュリティー保護のため、セキュリティーポリシーファイルはフロッピーディスクなどで受け渡しを行い、第三者の手が届かない場所に保管することをお薦めします。

また、AT-VPN Client のインストール時に必要なシリアル番号も管理者から入手してください。[1]

### 3 USB SecureKey のドライバーのインストール（USB SecureKey を使用する場合のみ）

別売のハードウェアキー「CentreCOM USB SecureKey」を使用する場合は、AT-VPN Client をインストールする前に、USB SecureKey のドライバーを弊社 Web サイトからダウンロードし、コンピューターにインストールしておく必要があります。

### 4 AT-VPN Client のインストール

AT-VPN Client をインストールします。途中でセキュリティーポリシーを指定する箇所がありますので、管理者から入手したセキュリティーポリシーファイル、または、ポリシーサーバーのアドレス、パスワード、ユーザー名（オプション）を指定してください。

また、インストール時には、セキュリティーポリシーファイルを保護するための「パスワード」の入力が求められます。パスワードを指定することにより、セキュリティーポリシーファイルは暗号化された状態で AT-VPN Client のインストールフォルダーに保存されるようになります。[2] コンピューターの起動時にもパスワードが要求されるため、パスワードを知らない第三者は VPN 通信を行えません。

また、パスワードの代わりに、別売の USB SecureKey を使ってセキュリティーポリシーファイルを保護することもできます。この場合、インストール時に USB SecureKey の挿入が求められます。以後、ここで挿入した USB SecureKey を USB ポートに挿入しておかないと VPN 通信ができなくなります。また、AT-VPN Client の設定変更もできなくなります。

### 5 運用の開始

インストール後コンピューターを再起動すると、AT-VPN Client が自動的に起動・常駐し、セキュリティーポリシーで指定されたサイトとの間で VPN 通信が行えるようになります。また、指定されたサイト以外とは通常の IP 通信を行えます。[3]

1. シリアル番号がない場合でも、期間限定の「お試し版」としてインストールすることができます。
2. 暗号化されたセキュリティーポリシーファイルは、AT-VPN Client のインストールフォルダーに vpnclient.mpf という名前で保存されます。万が一このファイルが盗まれた場合でも、ここで指定したパスワードがないと、暗号化されたセキュリティーポリシーファイルは使用や変更ができません。
3. VPN の設定（セキュリティーポリシーの内容）に依存します。

# 3 インストール

## 3.1 USB SecureKey を使用するための準備

別売の USB SecureKey を使用する場合は、AT-VPN Client のインストールを始める前に、USB SecureKey のドライバーをインストールしておく必要があります。以下の手順にしたがって、ドライバーをインストールしてください。

1 弊社 Web サイトからドライバーをダウンロードしてください。
`http://www.allied-telesis.co.jp/`

2 ダウンロードしたアーカイブファイルをローカルディスク上の適当なディレクトリーに展開してください。ここでは C:¥tmp¥usbkey ディレクトリーに展開したものと仮定します。

3 コンピューターの USB ポートに USB SecureKey を挿入してください。

4 USB SecureKey が検出され、次のようなダイアログが表示されます。「次へ」をクリックしてください。[1]

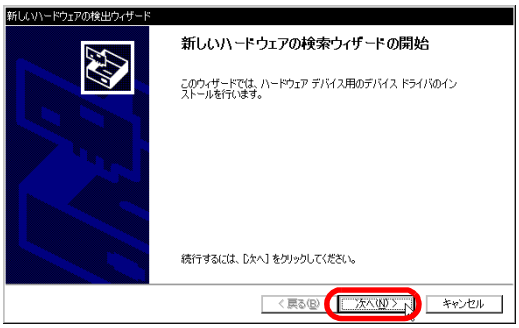


**図 3.1.1**

5 「デバイスに最適なドライバを検索する（推奨）」を選択（デフォルト）し、「次へ」をクリックしてください。

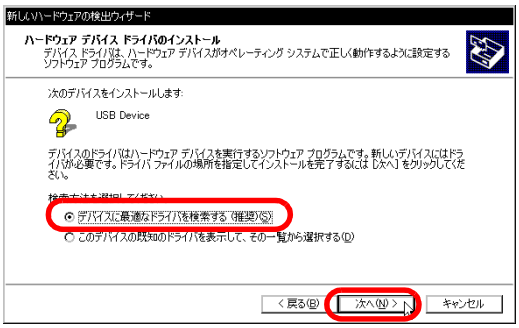


**図 3.1.2**

6 「場所を指定」をチェックし、「次へ」をクリックしてください。

1. 以下は Windows 2000 での画面例です。

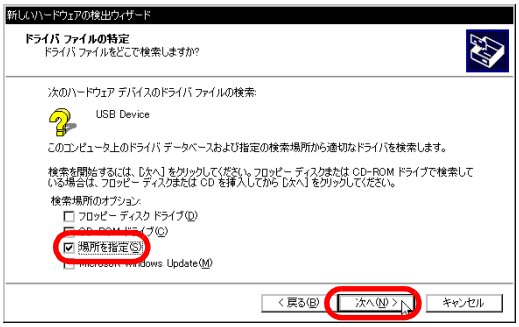


**図 3.1.3**

**7** アーカイブファイルを展開したディレクトリーを入力して、「次へ」をクリックしてください（ここでは、「C:¥tmp¥usbkey」）。

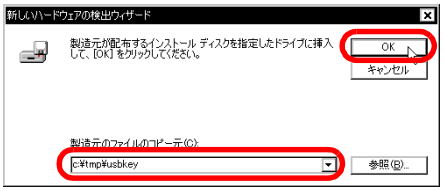


**図 3.1.4**

**8**「次へ」をクリックしてください。

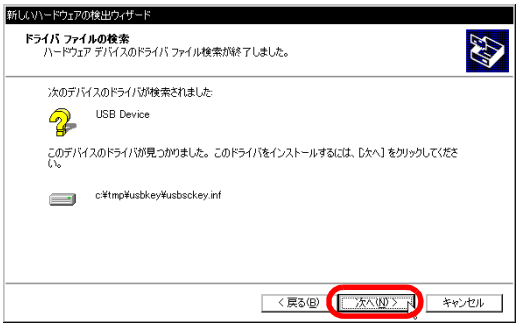


**図 3.1.5**

**9** ドライバーファイルがコピーされ、次のダイアログが表示されます。「完了」をクリックしてください。

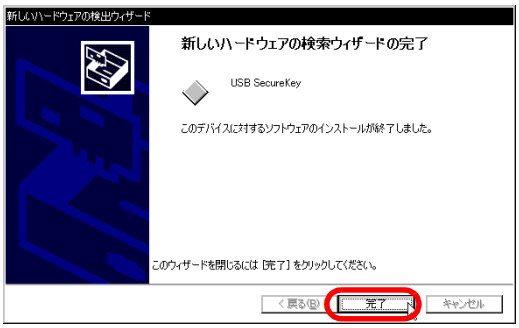


**図 3.1.6**

**10** これで、USB SecureKey のドライバーのインストールは完了です。「3.2 AT-VPN Client のインストール」（p.11）に進んでください。

## 3.2 AT-VPN Client のインストール

AT-VPN Client ソフトウェアのインストールは以下の手順にしたがって行います。USB SecureKey をご使用になる場合は、**USB SecureKey をコンピューターに取り付けていない状態で**インストールを始めてください。

**1** インストーラーのアイコンをダブルクリックしてください。


**図 3.2.1**

**2**「Next」をクリックしてください。

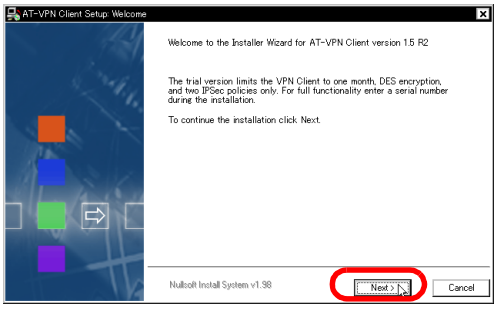


**図 3.2.2**

**3**「License Agreement」（ソフトウェア使用権許諾契約書）が表示されます。よくお読みになり、同意する場合は「Next」を、同意しない場合は「Cancel」をクリックしてください。「Cancel」をクリックした場合、インストールは中止されます。

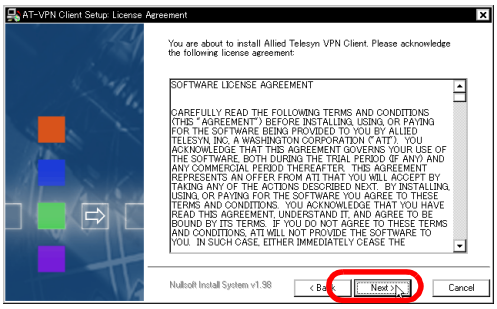


**図 3.2.3**

**4**「User Name」（ユーザー名）、「Company Name」（会社名）、「Serial Number」（シリアル番号）を入力し、「Next」をクリックしてください。
シリアル番号は、「AEAAA-000123-3ABC5ZYXW」のような 22 桁の文字列です。管理者から通知された番号を入力してください。「trial-version」を入力した場合は「お試し版[1]」として動作します。

1. 「お試し版」では、IPsec ポリシーを 2 つまでしか作成できないため、VPN セッションを 1 本しか張ることができません。また、15 分ごとにお試し版を示すダイアログが表示され、インストール後 30 日間しか使用できません。ユーザーサポートも受けられません。

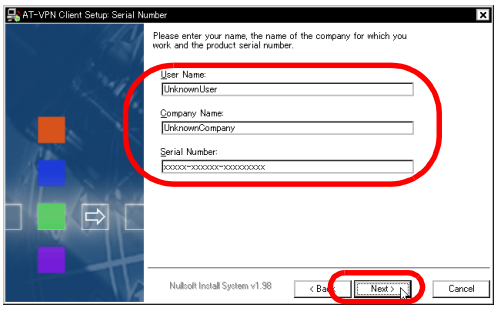


**図 3.2.4**

シリアル番号は、ユーザーライセンスをご購入いただくことにより入手できます。
10、25、50 ユーザーライセンスの場合、シリアル番号は同梱の「シリアル番号 / 認証キー」シールに記載されています。同シールには 2 種類の番号が印字されていますので、間違えないようご注意ください（図 3.2.5）。

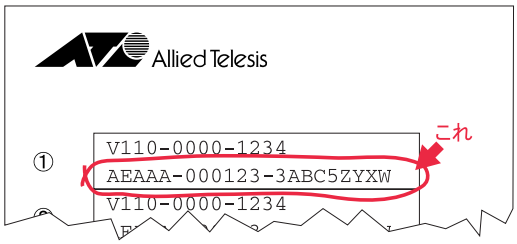


**図 3.2.5 「シリアル番号 / 認証キー」シールの例**

100 ユーザー以上のライセンスの場合、シリアル番号は同梱のフロッピーディスクに CSV（カンマ区切り）形式のテキストファイル「XXXXuser.csv」（XXXX はユーザー数）として収録されています。テキストエディターや表計算ソフトなどで開き、コピー＆ペーストしてご利用ください（図 3.2.6）。

```
...
このシリアル番号・認証キーの一覧ファイルは、csv ファイル形式になっています。
MS-Excel などで読み込む場合は、ここから下を切り出してご使用ください。

No., シリアル番号（S/N）, 認証キー（A/K）
1,Vxxx-0000-00xx,AEAAA-0000xx-xxxxxxxxx
2,Vxxx-0000-00xx,AEAAA-0000xx-xxxxxxxxx
...
```

**図 3.2.6 「XXXXuser.csv」ファイルの例**

**5** インストール先フォルダーを指定し、「Install」をクリックしてください。

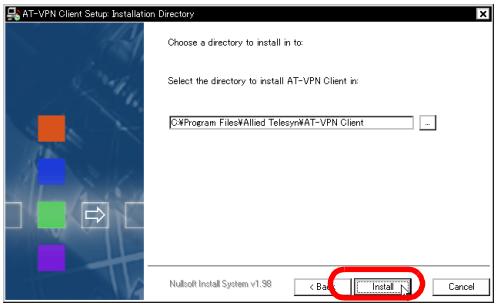


**図 3.2.7**

6 ファイルのコピーが行われます。コピー中は進行状況が表示されます。途中で「デジタル署名が見つかりませんでした」というダイアログが表示された場合は、「はい」をクリックしてインストールを続行してください。完了したら「Next」をクリックしてください。

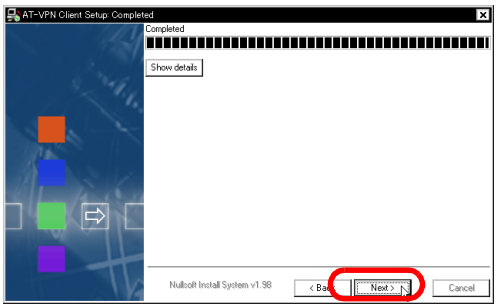


**図 3.2.8**

7 「Next」をクリックしてください。

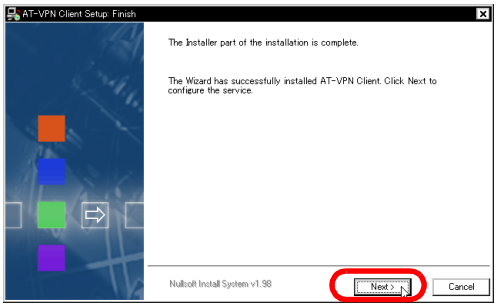


**図 3.2.9**

8 セキュリティーポリシー（VPN 設定情報）の保護方法を次の 3 つから選択します。

- Encrypt configuration using password（パスワードで保護）
- Use hardware key（ハードウェアキー（USB SecureKey）で保護）
- Store configuration as clear text（保護しない）

- パスワードで保護する場合は「Encrypt configuration using password」を選択し、「Enter password:」と「Verify password:」に同一のパスワードを入力して、「Next」をクリックしてください。[1] パスワードには、32 文字までの半角英数字と記号の一部が使えます。大文字、小文字は区別されます。

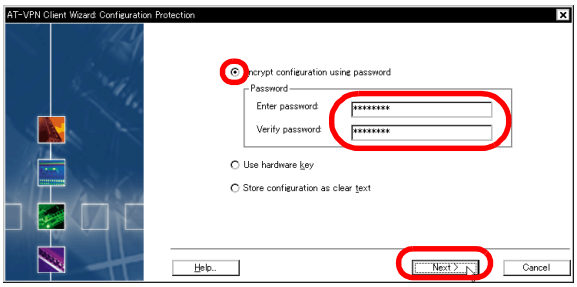


**図 3.2.10**

1. 「Encrypt configuration using password」を選択した場合、手順 9 で指定するセキュリティーポリシーファイルは暗号化され、vpnclient.mpf という名前で AT-VPN Client のインストールフォルダーに保存されます。また、AT-VPN Client の起動時や設定変更・表示の際にパスワードが要求されるようになります。

- USB SecureKey を使用する場合は、「Use hardware key」を選択して「Next」をクリックしてください。[1] 次のメッセージが表示されたら、コンピューターの USB ポートに USB SecureKey を挿入してください。[2]

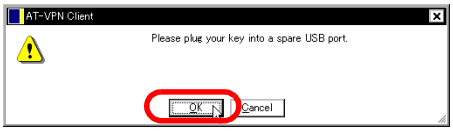


**図 3.2.11**

  - すでに USB SecureKey のドライバーがインストールされている場合は、USB SecureKey が自動認識され、USB SecureKey の LED が点灯します。この場合、「OK」ボタンをクリックし、手順 9 に進んでください。
  - 挿入後に「新しいハードウェアの追加ウィザード」が起動した場合は、図 3.2.11 の**「OK」ボタンをクリックせず**、「3.1 USB SecureKey を使用するための準備」(p.9) の手順にしたがって USB SecureKey のドライバーをインストールしたのち、図 3.2.11 の「OK」ボタンをクリックしてください。

- 「Store configuration as clear text」を選択した場合は、セキュリティーポリシーが平文のまま保存されます。[3] 第三者に不正使用される可能性がありますので、通常はパスワードか USB SecureKey によって保護してください。

**9** セキュリティーポリシーの取り込み方を指定します。

- 管理者からセキュリティーポリシーファイルを受け取っている場合は、「From file」(ファイルから取り込む) を選択し、セキュリティーポリシーファイル[4] の場所を指定して、「Next」をクリックしてください。

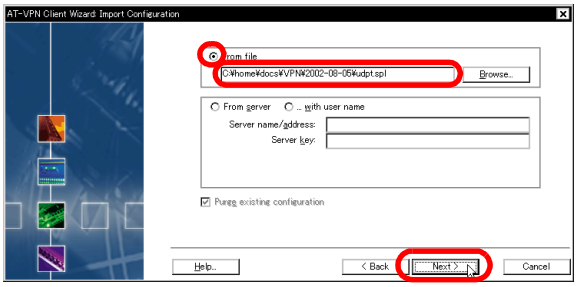


**図 3.2.12**

1. 「Use hardware key」を選択した場合、手順 9 で指定するセキュリティーポリシーファイルは暗号化され、vpnclient.mpf という名前で AT-VPN Client のインストールフォルダーに保存されます。以後、ここで指定した USB SecureKey を USB ポートに挿入しておかないと VPN 通信を行えません。また、AT-VPN Client の設定変更なども行えなくなります。
2. **USB SecureKey を抜き差しするときは、必ず 10 秒以上間隔をあけてください。また、USB SecureKey は、複数同時に使用しないでください(弊社 USB SecureKey だけでなく、他社の類似製品の併用もできません)。**
3. 「Store configuration as clear text」を選択した場合、手順 9 で指定するセキュリティーポリシーは、平文のまま vpnclient.mpf という名前で AT-VPN Client のインストールフォルダーに保存されます。
4. セキュリティー保護のため、平文テキストのセキュリティーポリシーファイルは、フロッピーディスクなどに保存し、第三者の手が届かない場所に保管することをおすすめします。ポリシーファイルの作成については、「7 設定例」(p.28) をご参照ください。

- 管理者からポリシーサーバーの IP アドレスとパスワードを通知されている場合は、サーバーとの通信ができるようになっていることを確認した上で[1]、「From server」（サーバーからダウンロード）を選択し、「Server name/address」（サーバーの IP アドレスかホスト名）と「Server key」（ダウンロード用パスワード）を入力し、「Next」をクリックしてください。
これにより、指定したポリシーサーバーからセキュリティーポリシーファイルがダウンロードされます。[2]

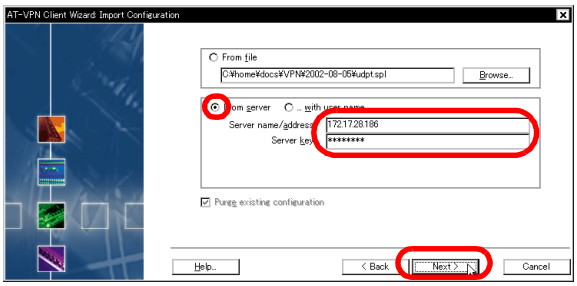


**図 3.2.13**

- 管理者からポリシーサーバーの IP アドレス、パスワード、ユーザー名を通知されている場合は、サーバーとの通信ができるようになっていることを確認した上で、「... with user name」(ユーザー名を指定してサーバーからダウンロード) を選択し、「Server name/address」(サーバーの IP アドレスかホスト名)、「Server key」(パスワード)、「User name」(ユーザー名) を入力し、「Next」をクリックしてください。
これにより、指定したポリシーサーバーからセキュリティーポリシーファイルがダウンロードされます。

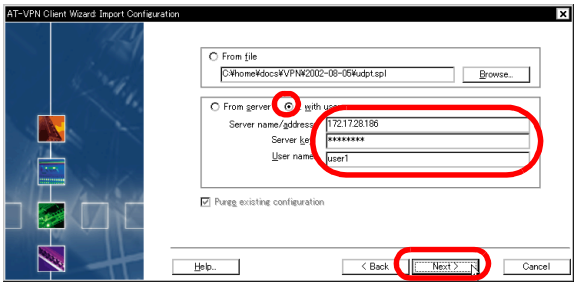


**図 3.2.14**

**10** VPN 通信で使用するネットワークアダプターにチェックを付けて「Next」をクリックしてください。

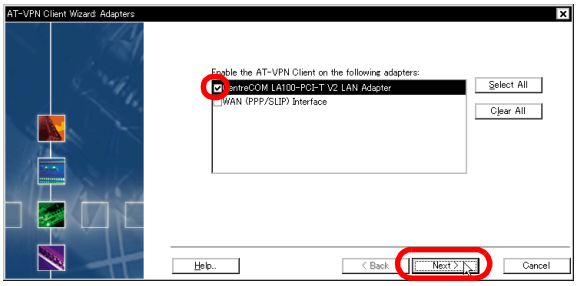


**図 3.2.15**

1. インターネットサービスプロバイダーへの接続動作（ダイヤルアップ接続や PPPoE 接続）が必要な場合は、あらかじめ接続をすませておいてください。
2. ポリシーファイルのダウンロードには、ISAKMP プロトコルが使用されます。ポリシーファイルは、暗号化された通信路上でやりとりされ、平文のまま流れることはありません。

**11** 以上でインストールは完了です。

- Windows 2000 の場合は、「Finish」をクリックしてダイアログを閉じ、コンピューターを再起動してください。[1]

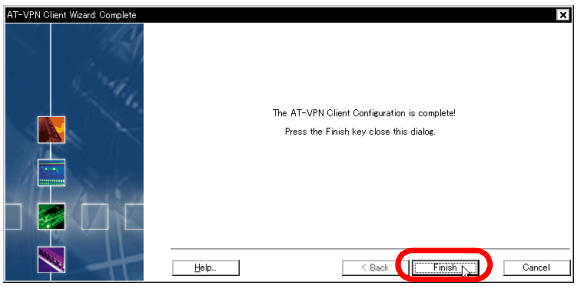


**図 3.2.16**

- Windows 98、Me の場合は、「Yes, reboot the computer for me now.」（今すぐ再起動する）を選択し、「Finish」をクリックしてください。

**12** コンピューターの再起動後、AT-VPN Client が自動的に起動・常駐し、以降セキュリティーポリシーの内容にしたがって VPN 通信が行えるようになります。

## 3.3 アンインストール

AT-VPN Client をアンインストールするには、次の手順にしたがってください。

**1** 「スタート」→「プログラム」→「AT-VPN Client」と進み、「Uninstall VPN client」をクリックしてください。

**2** 「Uninstall」をクリックしてください。アンインストールが行われます。

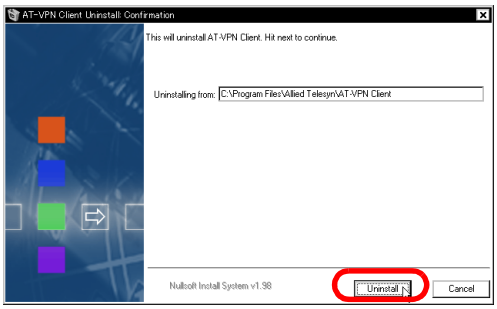


**図 3.3.1**

**3** 「Next」をクリックしてください。

1. ダイヤルアップや PPPoE でインターネットサービスプロバイダーに接続しているときは、先に接続を切ってからコンピューターを再起動してください。

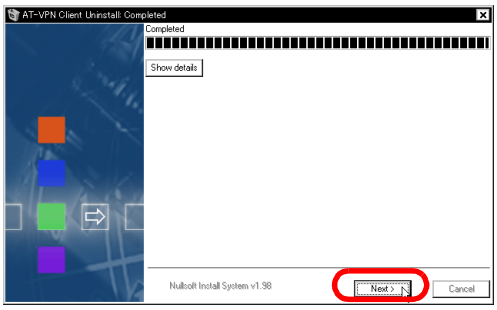


**図 3.3.2**

**4** 次のダイアログが表示されたらアンインストールは完了です。「Yes, reboot the computer for me now.」（今すぐ再起動する）を選択し、「Next」をクリックしてください。[1]

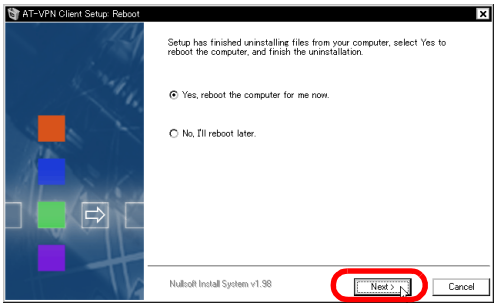


**図 3.3.3**

1. ダイヤルアップや PPPoE でインターネットサービスプロバイダーに接続しているときは、先に接続を切ってから「Yes, reboot the computer for me now.」を選択するか、「No, I'll reboot later.」を選択し、ISP との接続を切ったあとでコンピューターを再起動してください。

## 3.4 お試し版からライセンス版への移行

お試し版からライセンス版に移行するには、次の手順にしたがって AT-VPN Client を再インストールしてください。

1 「3.3 アンインストール」（p.16）にしたがい、お試し版としてインストールされている AT-VPN Client をアンインストールしてください。

2 「3.2 AT-VPN Client のインストール」（p.11）にしたがい、ご購入になった「CentreNET AT-VPN Client ライセンス」の「シリアル番号」を使用して再インストールしてください。

# 4 起動

1 インストール完了後、コンピューターを起動するたびに、AT-VPN Client が自動的に起動され、VPN 通信が行えるようになります。

- 「3.2 AT-VPN Client のインストール」の手順 8（p.13）で「Encrypt configuration using password」を選択した場合、コンピューターの起動直後に、手順 8（p.13）で入力したパスワードを要求されます。パスワードを入力して「OK」をクリックすると、AT-VPN Client が起動し、以後システムに常駐します（セキュリティーポリシーで指定した接続先との通信は、VPN 通信となります）。[1]

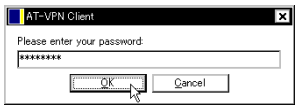


**図 4.0.1 パスワード入力ダイアログ**

「キャンセル」をクリックするか、パスワードを 3 回続けて間違えると、ダイアログが閉じ、AT-VPN Client は使用できない状態になります。このような場合は、タスクトレイの AT-VPN アイコン（図 4.0.5）をダブルクリックすることで、パスワード入力ダイアログを再表示させることができます。

- 「3.2 AT-VPN Client のインストール」(p.11) の手順 8 で「Use hardware key」を選択した場合は、コンピューターの起動時に次のダイアログが表示され、USB SecureKey の挿入を求められます。コンピューターの USB ポートに USB SecureKey を接続し「OK」をクリックすると、AT-VPN Client が起動し、以後システムに常駐します。


**図 4.0.2 USB SecureKey の挿入をうながすダイアログ**

- 「3.2 AT-VPN Client のインストール」(p.11) の手順 8 で「Store configuration as clear text」を選択した場合は、コンピューターの起動時にパスワードを聞かれることなく、AT-VPN Client が起動し、以後システムに常駐します。

2 AT-VPN Client の実行中は、タスクトレイに次のようなアイコンが表示されます。


**図 4.0.3**

VPN 通信中はアイコンの色が次のように変わります。

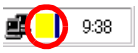


**図 4.0.4**

1. AT-VPN Client が実行されている状態で、ご使用のコンピューターの前から離れないでください。第三者が社内 LAN などのプライベートネットワークにアクセスする恐れがあります。コンピューターから離れるときは、必ずコンピューターをシャットダウンしてください。あるいは、USB SecureKey を使用している場合は、キーを抜いておいてください。

パスワードか USB SecureKey による保護を有効にしている場合、起動時にパスワードの入力をキャンセルしたときや、正しいパスワードを入力できなかったとき(3 回続けてパスワードを間違えたためダイアログが閉じたとき)、USB SecureKey を抜いているときは、アイコンが次のように変わり、VPN Client が使用できない状態にあることを示します。


**図 4.0.5**

この状態から VPN Client を使用できるようにするには、図 4.0.5 のアイコンをダブルクリックしてパスワード入力ダイアログ（図 4.0.1）を表示させ、正しいパスワードを入力するか、USB SecureKey を挿入してください。

# 5 メニュー

タスクトレイにある AT-VPN Client アイコンを右クリックすると、次のようなメニューが表示されます。このメニューからは、AT-VPN Client の設定変更や状態の確認などを行うことができます。以下、各メニューについて説明します。

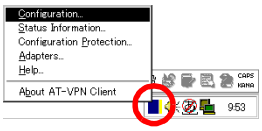


**図 5.0.1**

なお、パスワードによる保護を有効にしている場合は、セキュリティーにかかわる操作（設定変更や情報表示など）を実行するたびにパスワードの入力を求められます。また、USB SecureKey による保護を有効にしている場合は、キーを挿した状態でないとメニューの実行ができません。

- **Configuration（現在のセキュリティーポリシー）（p.21）**
  セキュリティーポリシーの確認、変更、初期化、削除などを行います。
- **Status Information（通信状態の詳細）（p.24）**
  ログ、デバッグ情報を表示します。
- **Configuration Protection（セキュリティーポリシーの保護方法）（p.25）**
  セキュリティーポリシーの保護方法の切り替え、パスワードの変更を行います。
- **Adapters（VPN 通信に使うネットワークアダプターの選択）（p.25）**
  VPN 通信に使用するネットワークインターフェースを変更します。
- **About AT-VPN Client（AT-VPN Client について）（p.25）**
  バージョン情報などを表示します。

## 5.1 Configuration（現在のセキュリティーポリシー）

次のダイアログで、セキュリティーポリシーの確認、変更、初期化、削除などを行うことができます。

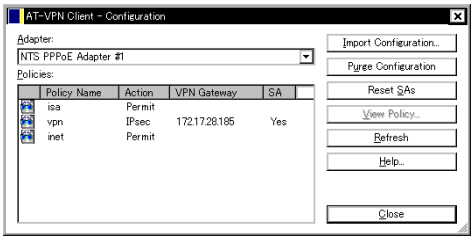


**図 5.1.1**

**Adapter（ネットワークアダプター）**

コンピューターにインストールされているネットワークアダプターが表示されます。セキュリティーポリシーの情報を確認するには、VPN 通信に使用しているアダプターを選択してください。[1]

1. VPN 通信に使用しないアダプターを選択しているときは、Policies ウィンドウに何も表示されません。

**Policies ウィンドウ**

Policies ウィンドウ には、セキュリティーポリシーデータベースに定義されている IPsec ポリシーの一覧が表示されます。各ポリシーの詳細を表示させるには、ポリシーを選択して「View Policy」をクリックするか、ポリシーをダブルクリックしてください。

**Policy Name（IPsec ポリシー名）**

IPsec ポリシー名が表示されます。

**Action（IPsec ポリシーの処理内容）**

このポリシーにマッチしたパケットの処理方法を示します。

**Permit**：IP パケットを暗号化せず、そのまま通信します。

**Deny**：IP パケットを破棄します。通信できません。

**IPsec**：IP パケットを暗号化し、VPN 通信を行います。

**VPN Gateway（VPN ゲートウェイ）**

VPN 通信の相手となる AR ルーター（VPN ゲートウェイ）の IP アドレスが表示されます。Action が IPsec のときだけ表示されます。

**SA（VPN コネクション）**

上記 VPN ゲートウェイとの間で VPN 通信が確立しているかどうかを「Yes」「No」で示します。Action が IPsec のときだけ表示されます。

**Import Configuration（設定の取り込み）**

新しいセキュリティーポリシー（VPN 設定情報）を取り込みます。詳しくは「 Import Configuration（設定の取り込み)」（p.22）をご覧ください。

**Purge Configuration（設定の削除）**

使用中のセキュリティーポリシーをすべて削除します。新しいセキュリティーポリシーを取り込むまで、VPN 通信ができなくなりますのでご注意ください。

**Reset SAs（VPN コネクションのリセット）**

現在確立されているすべての VPN コネクション（SA）を初期状態にします。

**View Policy（IPsec ポリシーの詳細表示）**

Policies ウィンドウ上で選択した IPsec ポリシーの詳細を表示します。IPsec ポリシー名をダブルクリックしても同じ動作になります。

**Refresh（最新の情報を表示）**

Policies ウィンドウに表示されている情報を最新の状態にします。

## Import Configuration（設定の取り込み）

セキュリティーポリシー（VPN 設定情報）を取り込み、VPN 通信の設定を変更または追加します。このダイアログは、「3.2 AT-VPN Client のインストール」の図 3.2.12（p.14）と同じです。

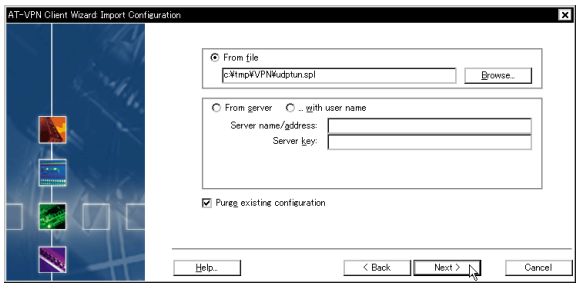


図 5.1.2

**From file（ファイルから取り込む）**

あらかじめ用意しておいたセキュリティーポリシーファイルを取り込みます。ファイル名を指定してください（拡張子「.spl」）。

**From server（サーバーからダウンロード）[1] [2]**

ポリシーサーバーから、セキュリティーポリシーファイルをダウンロードして取り込みます。「Server name/address」と「Server key」を指定してください。

**(From server) ... with user name（ユーザー名を指定してサーバーからダウンロード）[3]**

ポリシーサーバーから、セキュリティーポリシーファイルをダウンロードして取り込みます。「Server name/address」、「Server key」、「User name」を指定してください。

**Server name/address（サーバーアドレス）**

ポリシーサーバーとして動作しているARルーターのIPアドレスかホスト名を指定します。「From server」か「... with user name」を選択した場合、管理者から通知されたアドレスを入力してください。

**Server key（サーバーキー）**

ポリシーサーバーからセキュリティーポリシーファイルをダウンロードするときに使用するパスワードを指定します。「From server」か「... with user name」を選択した場合、管理者から通知されたパスワードを入力してください。

**User name（ユーザー名）**

ポリシーサーバーからセキュリティーポリシーファイルをダウンロードするときに使用するユーザー名を指定します。「... with user name」を選択した場合、管理者から通知されたユーザー名を入力してください。

**Purge existing configuration（現在の設定情報を削除する）**

新しいセキュリティーポリシーを取り込むときに、既存の設定情報を消去します。この項目をチェックしなかった場合は、現在の設定情報に対して、新しい情報が追加されます（現在の情報と新しい情報の間に矛盾がある場合は、エラーとなります）。

1. 「From server」「... with user name」を選択するためには、接続先のARルーターがポリシーサーバーとして動作するようセットアップされている必要があります。
2. セキュリティーポリシーファイルは、インターネット経由でダウンロードすることができます。ポリシーファイルのダウンロードには、ISAKMPプロトコルが使用されます。ポリシーファイルは、暗号化された通信路上でやりとりされ、平文のまま流れることはありません。
3. 「From Server」との違いは、ユーザー名を指定できる点です。ARルーター上に複数のポリシーファイルが置かれている場合に使います。

## 5.2 Status Information（通信状態の詳細）

ログ、デバッグ情報を表示するダイアログです。

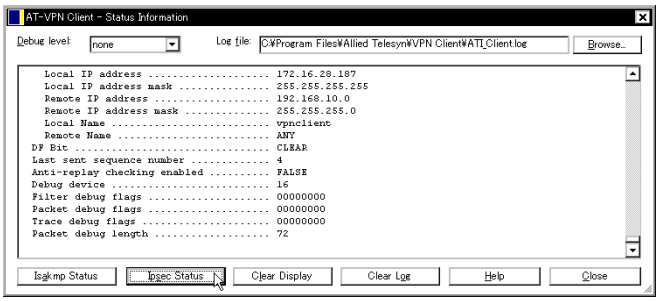


**図 5.2.1**

**Debug level（デバッグレベル）**

通信状態の表示レベルを指定します。ここでの指定に応じて、表示される内容が異なります。通常は「none」のままご使用ください。

**Log file（ログファイル）**

各種情報が書き出されるログファイルの名前が表示されます。デフォルトは、AT-VPN Client インストールフォルダーの「ATI_Client.log」です。ログファイルを変更するには、「Browse」ボタンをクリックし、ファイル選択ダイアログで指定します。

**Browse...（ファイル選択ダイアログを開く）**

上記の「Log file」を変更するときにクリックします。ファイル選択ダイアログが表示されるので、ログファイル名を指定してください。

**Isakmp Status（ISAKMP の状態を表示）**

ISAKMP プロトコルに関する各種状態を表示します。

**Ipsec Status（IPsec の状態を表示）**

IPsec に関する各種状態を表示します。

**Clear Display（画面をクリア）**

表示画面をクリアします。

**Clear Log（ログをクリア）**

ログをクリアします。

## 5.3 Configuration Protection（セキュリティーポリシーの保護方法）

AT-VPN Client のインストールフォルダーにファイルとして保存されるセキュリティーポリシーの保護方法を指定するダイアログです。詳しくは、「3.2 AT-VPN Client のインストール」の手順 8（p.13）をご覧ください。

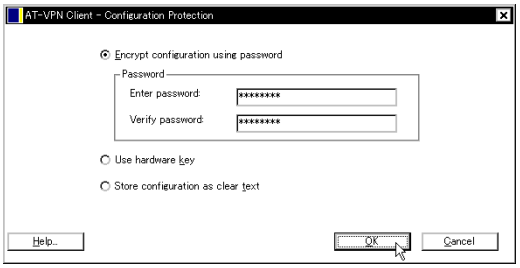


**図 5.3.1**

## 5.4 Adapters（VPN 通信に使うネットワークアダプターの選択）

VPN 通信を適用するネットワークアダプターを選択するダイアログです。[1]

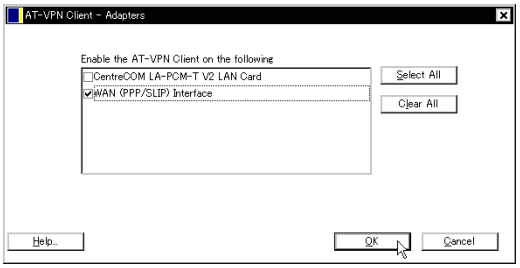


**図 5.4.1**

## 5.5 About AT-VPN Client（AT-VPN Client について）

バージョン情報などを表示します。

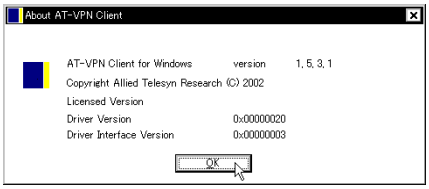


**図 5.5.1**

1. ここですべてのチェックを外すと、VPN 処理が適用されず、すべての IP 通信が平文で行われます。いったん起動・常駐した AT-VPN Client をアンロードすることはできませんが、このダイアログですべてのチェックを外すことにより、動作的にはアンロードしたのと同じ状態にすることができます。

# 第 2 部 アドミニストレーター編

「アドミニストレーター編」では、AT-VPN Client と AR ルーターによる VPN を構築・管理するネットワーク管理者の方を対象に、AT-VPN Client の設定ファイル（セキュリティーポリシーファイル）の書き方と AR ルーターの設定方法を示します。また、AT-VPN Client の設定ファイルで使用できるコマンドの一覧も掲載しています。

なお、設定にあたっては、AR ルーターに付属の取扱説明書、コマンドリファレンス、設定例集もあわせてご参照ください。

# 6 VPN 構築の概要

AT-VPN Client と AR ルーターを使って VPN を構築するには、次の作業が必要です。

**1 AR ルーター（VPN ゲートウェイ）の設定**

AR ルーターに対して次のような設定を行います。

**(1) インターネットサービスプロバイダー（ISP）に接続するための設定**

ご利用のネットワーク形態にあわせて ISP に接続するための設定を行います。必要に応じて、ファイアウォールや NAT の設定も行ってください。

**(2) VPN ゲートウェイとしての設定**

AT-VPN Client からの VPN 接続を受け入れるための設定を行います。AT-VPN Client にセキュリティーポリシーをダウンロードさせる場合は、ポリシーサーバーとしての設定も行います[1]。

**2 AT-VPN Client の設定ファイル（セキュリティーポリシーファイル）の作成**

AT-VPN Client に取り込むセキュリティーポリシーファイルを作成します。セキュリティーポリシーファイルは IPsec 関連コマンドを記述した平文のテキストファイルです。VPN ゲートウェイの設定にあわせて、必要なコマンドを記述してください。複数の AT-VPN Client から接続を受け付けるときは、AT-VPN Client の数だけセキュリティーポリシーファイルを作成する必要があります。

**3 AT-VPN Client の設定情報をユーザーに提供・通知**

作成したセキュリティーポリシーファイルは、フロッピーディスクなどで AT-VPN Client のユーザーに渡すか、AR ルーターのポリシーサーバー機能を使ってユーザーがダウンロードできるようにします。

セキュリティーポリシーファイルを直接ユーザーに渡すときは、ファイルの拡張子を .spl としてから渡してください。ポリシーサーバー機能を使うときは、ファイルの拡張子を .scp としてポリシーサーバー上に置き、ユーザーに「サーバーのアドレス」と「ダウンロード用ユーザー名」、「ダウンロード用パスワード」を通知してください。

## 6.1 動作環境

VPN ゲートウェイとして使用する AR ルーターは以下の要件を満たしている必要があります。

- ファームウェアバージョン 2.2.2PL8（AR300 シリーズ）、2.2.2PL10（AR700 シリーズ）、2.3.4PL0（AR410 V2）以降を搭載していること
- IPsec をサポートしている機種であること[2]
- 暗号ボード[3] を搭載していること

1. VPN ゲートウェイとポリシーサーバーは別の AR ルーターでもかまいません。ただし、以下の各例では 1 台の AR ルーターが両者を兼ねることを想定しています。
2. 2003 年 6 月現在、AR300V2、AR300L V2、AR410 V2、AR720、AR740 が対応しています。ただし、ポリシーサーバー機能については AR410 V2 と AR700 シリーズのみの対応となります。
3. 暗号ボードの対応機種については、弊社 Web サイトなどでご確認ください。

# 7 設定例

AR ルーターの設定と、対応するセキュリティーポリシーファイルの記述例を示します。セキュリティーポリシーファイルの記述内容は、AR ルーター側の設定に依存します。

ここでは、以下の設定例を示します[1]。実際に設定を行う際の参考にしてください。

- **基本設定（XAUTH 認証）（p.33）**
  アドレス不定の AT-VPN Client から VPN 接続を受け付ける構成例です。IPsec の拡張仕様である XAUTH（Extended Authentication）を用いて、ユーザー名 / パスワードベースの認証を行います。セキュリティーポリシーはファイルで提供します。

- **基本設定（ID 認証）（p.35）**
  アドレス不定の AT-VPN Client から VPN 接続を受け付ける構成例です。XAUTH 認証と異なり、IPsec の基本仕様の範囲内でクライアントの認証を行います。セキュリティーポリシーはファイルで提供します。

- **ポリシーサーバー（1 ユーザーのみ）（p.36）**
  「基本設定（XAUTH 認証）」にポリシーサーバーの設定を追加します。この機能を利用すると、AT-VPN Client が使用するセキュリティーポリシーをルーター側で管理できるようになります。ユーザーには、ポリシーサーバーの IP アドレスとパスワードだけを通知します。ただし、本設定例ではユーザー名を指定できないため、1 ユーザー分のポリシーしかダウンロードさせることができません。複数ユーザーにセキュリティーポリシーを提供したいときは、次の「ポリシーサーバー（複数ユーザー対応）」をご覧ください。

- **ポリシーサーバー（複数ユーザー対応）（p.39）**
  「基本設定（ID 認証）」にポリシーサーバーの設定を追加します。この例では、ID 認証を用いることで、ユーザーごとにセキュリティーポリシーを提供できるようになっています。各ユーザーには、ポリシーサーバーの IP アドレス（共通）と個別のユーザー名、パスワードを通知します。

- **UDP トンネリング（NAT 越えの VPN 接続）（p.41）**
  AT-VPN Client と VPN ゲートウェイ（AR ルーター）の間に NAT 装置が入る場合の基本的な設定例を示します。UDP トンネリング（ESP over UDP）に必須な内部 NAT の使用方法も説明しています。

- **UDP トンネリング＋ポリシーサーバー（p.44）**
  「UDP トンネリング（NAT 越えの VPN 接続）」にポリシーサーバーの設定を追加します。この例では、ユーザーごとにセキュリティーポリシーを提供できるよう設定しています。

1. ポリシーサーバー機能は AR410 V2 と AR700 シリーズのみの対応となります。

## 7.1 想定するネットワーク構成

### NAT 装置をはさまないケース

「7.2 基本設定（XAUTH 認証）」（p.33）～「7.5 ポリシーサーバー（複数ユーザー対応）」（p.39）の各例は図 7.1.1 のネットワーク構成を前提としています。同構成のポイントは次のとおりです。

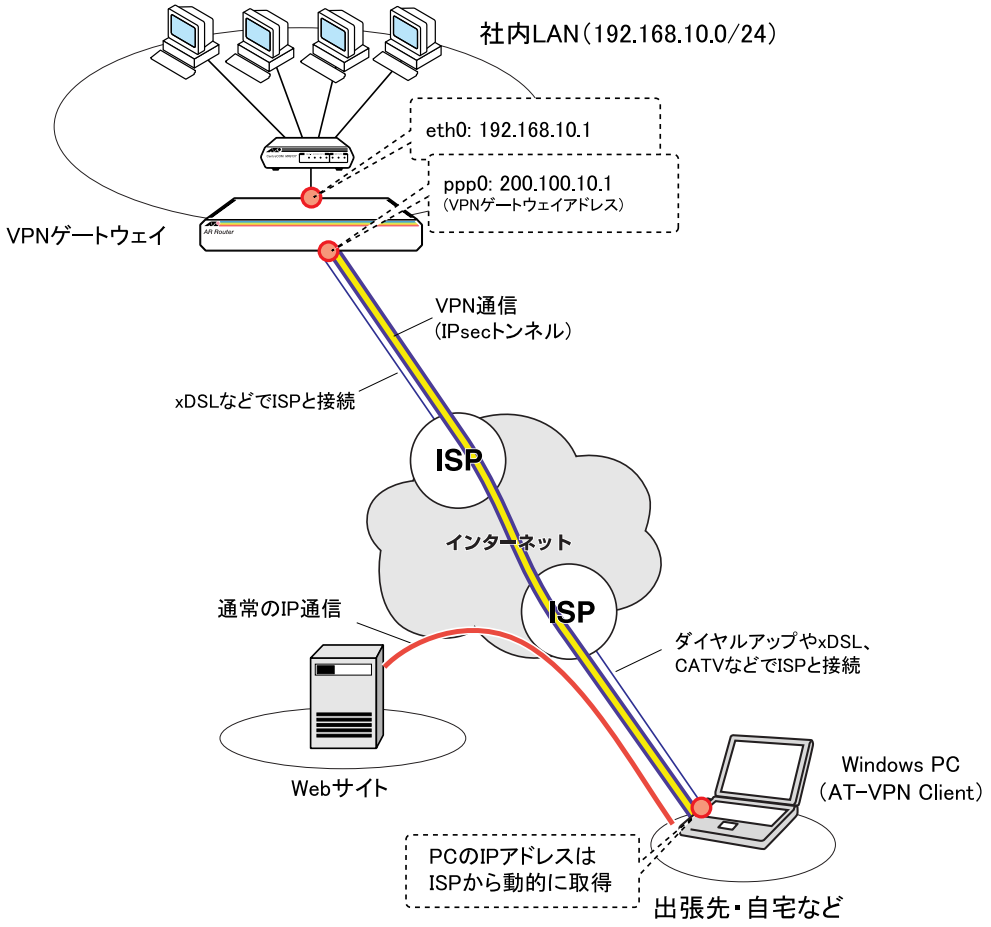


**図 7.1.1 NAT 装置をはさまないネットワーク構成例**

- VPN ゲートウェイ・ISP 間は xDSL などで常時接続されている。VPN ゲートウェイの WAN 側（ppp0）には、ISP から 1 個固定で割り当てられたグローバル IP アドレス 200.100.10.1 を設定する[1]。また、LAN 側（eth0）には、プライベートアドレス 192.168.10.1 を設定する。
- VPN ゲートウェイにファイアウォールとダイナミック ENAT の設定を施し、外部からの不正アクセスを防止しつつ、LAN 側端末にインターネットへの接続性を提供する。
- AT-VPN Client（Windows PC）は、ダイヤルアップや xDSL などで ISP に直接接続する。AT-VPN Client の IP アドレスは、ISP への接続時に動的に割り当てられる。
- AT-VPN Client・社内 LAN 間では、暗号化された VPN 通信を行う[2]。
- AT-VPN Client からインターネット（Web サイトなど）へは通常の IP 通信を行う。

1. VPN ゲートウェイとして機能させるためには、ルーター自身にクライアントから到達可能なグローバル IP アドレスを設定しておく必要があります。したがって、WAN 側が Unnumbered の場合は、LAN 側をマルチホーミングしてグローバルアドレスを設定するなどの工夫が必要です（本例では不要）。
2. AT-VPN Client とルーター（VPN ゲートウェイ）の間に IPsec のトンネルを張ります。このとき、AT-VPN Client 側のアドレスは ISP から動的に割り当てられたアドレス、ルーター側のアドレスは ppp0 に割り当てたグローバルアドレスとなります。

VPN ゲートウェイのインターネット接続設定（PPP、IP、ファイアウォール）まではすべての例で共通なため、最初に共通部分だけを示しておきます。ここでは xDSL + PPPoE[1] で ISP に接続していると仮定していますが、実際にはご使用の接続形態にあわせて設定してください。

**1** PPPoE 接続の設定を行います。ルーターの Ethernet インターフェースは、eth0 を LAN 側、eth1 を WAN 側（PPPoE 用）として使うものとします。

```
CREATE PPP=0 OVER=eth1-any
SET PPP=0 OVER=eth1-any USER=user@ispA PASSWORD=isppasswdA LQR=OFF
     BAP=OFF ECHO=ON
```

**2** IP の基本設定を行います。IP モジュールを有効化し、各インターフェースに IP アドレスを割り当て、デフォルトルートを WAN 側（ppp0）に向けて設定します。

```
ENABLE IP
ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0
ADD IP INT=ppp0 IP=200.100.10.1 MASK=255.255.255.255
ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
```

**3** ファイアウォールとダイナミック ENAT の基本設定を行います。

```
ENABLE FIREWALL
CREATE FIREWALL POLICY=net
ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
DISABLE FIREWALL POLICY=net IDENTPROXY
ADD FIREWALL POLICY=net INT=eth0 TYPE=PRIVATE
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
ADD FIREWALL POLICY=net NAT=ENHANCED INT=eth0 GBLINT=ppp0
```

**4** VPN 通信に必要なパケットを通すためのルールを追加します。1 行目は VPN ゲートウェイ自身に宛てられた ISAKMP パケットを通過させるためのルール、2 行目は LAN 側ネットワーク宛ての IPsec パケットを通過させるためのルールです。

```
ADD FIREWALL POLICY=net RU=1 AC=ALLOW INT=ppp0 PROT=UDP PORT=500
     IP=200.100.10.1 GBLIP=200.100.10.1 GBLPORT=500
ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=ppp0 PROT=ALL
     IP=192.168.10.1-192.168.10.254 ENCAP=IPSEC
```

共通部分はここまでです。以下の各例では、VPN に直接関係する項目だけを解説していきます。

1. ここでは、説明を簡潔にするため、PPPoE セッションを自動的に再接続するためのトリガー設定を省いています。詳しくはルーター付属の「設定例集」をご覧ください。

## NAT 装置をはさむケース

「7.6 UDP トンネリング（NAT 越えの VPN 接続）」（p.41）～「7.7 UDP トンネリング＋ポリシーサーバー」（p.44）の各例は、VPN ゲートウェイ・AT-VPN Client の間に NAT 装置が入る図 7.1.2 のネットワーク構成を前提としています。同構成のポイントは次のとおりです。

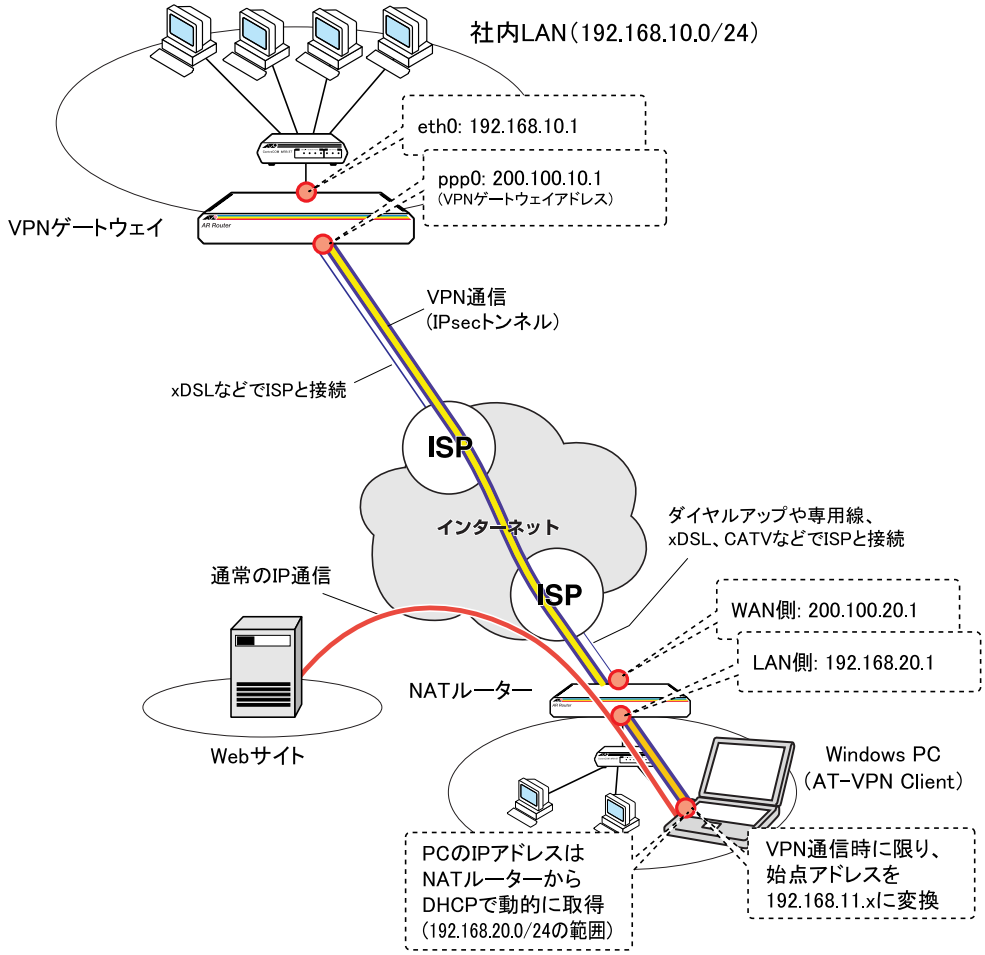


**図 7.1.2 NAT 装置をはさむネットワーク構成例**

- VPN ゲートウェイ･ISP 間は xDSL などで常時接続されている。VPN ゲートウェイの WAN 側（ppp0）には、ISP から 1 個固定で割り当てられたグローバル IP アドレス 200.100.10.1 を設定する[1]。また、LAN 側（eth0）には、プライベートアドレス 192.168.10.1 を設定する。
- VPN ゲートウェイにファイアウォールとダイナミック ENAT の設定を施し、外部からの不正アクセスを防止しつつ、LAN 側端末にインターネットへの接続性を提供する。
- AT-VPN Client（Windows PC）は、NAT ルーター背後の LAN 側ネットワークに接続されており、NAT ルーター経由でインターネットにアクセスする。
- AT-VPN Client の IP アドレス（プライベート）は、NAT ルーターから DHCP で動的に割り当てられる。

1. VPN ゲートウェイとして機能させるためには、ルーター自身にクライアントから到達可能なグローバル IP アドレスを設定しておく必要があります。したがって、WAN 側が Unnumbered の場合は、LAN 側をマルチホーミングしてグローバルアドレスを設定するなどの工夫が必要です（本例では不要）。

- AT-VPN Client・社内 LAN 間では、暗号化された VPN 通信を行う[1]。また、NAT 越えの通信を可能にするため、ESP パケットを UDP でカプセル化する UDP トンネリング（ESP over UDP）を用いる。
- AT-VPN Clientは、社内LAN宛てパケットの始点アドレスを内部NAT機能により192.168.11.xに変換してからカプセル化する。
- AT-VPN Client からインターネット（Web サイトなど）へは通常の IP 通信を行う。

最初に VPN ゲートウェイ（ルーター）のインターネット接続設定（PPP、IP、ファイアウォール）までを示します。ここでは xDSL + PPPoE[2] で ISP に接続していると仮定していますが、実際にはご使用の接続形態にあわせて設定を変更してください。

**1** PPPoE 接続の設定を行います。ルーターの Ethernet インターフェースは、eth0 を LAN 側、eth1 を WAN 側（PPPoE 用）として使うものとします。

```
CREATE PPP=0 OVER=eth1-any
SET PPP=0 OVER=eth1-any USER=user@ispA PASSWORD=isppasswdA LQR=OFF
     BAP=OFF ECHO=ON
```

**2** IP の基本設定を行います。IP モジュールを有効化し、各インターフェースに IP アドレスを割り当て、デフォルトルートを WAN 側（ppp0）に向けて設定します。

```
ENABLE IP
ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0
ADD IP INT=ppp0 IP=200.100.10.1 MASK=255.255.255.255
ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
```

**3** ファイアウォールとダイナミック ENAT の基本設定を行います。

```
ENABLE FIREWALL
CREATE FIREWALL POLICY=net
ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
DISABLE FIREWALL POLICY=net IDENTPROXY
ADD FIREWALL POLICY=net INT=eth0 TYPE=PRIVATE
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
ADD FIREWALL POLICY=net NAT=ENHANCED INT=eth0 GBLINT=ppp0
```

**4** VPN 通信に必要なパケットを通すためのルールを追加します。1、2 行目は VPN ゲートウェイ自身に宛てられたISAKMPパケット、UDPトンネリングパケットを通過させるためのルール、3 行目は LAN 側ネットワーク宛ての IPsec パケットを通過させるためのルールです。

```
ADD FIREWALL POLICY=net RU=1 AC=ALLOW INT=ppp0 PROT=UDP PORT=500
     IP=200.100.10.1 GBLIP=200.100.10.1 GBLPORT=500
ADD FIREWALL POLICY=net RU=2 AC=ALLOW INT=ppp0 PROT=UDP PORT=2746
     IP=200.100.10.1 GBLIP=200.100.10.1 GBLPORT=2746
ADD FIREWALL POLICY=net RU=3 AC=NONAT INT=ppp0 PROT=ALL
     IP=192.168.10.1-192.168.10.254 ENCAP=IPSEC
```

共通部分はここまでです。

1. AT-VPN Client とルーター（VPN ゲートウェイ）の間に IPsec のトンネルを張ります。このとき、AT-VPN Client 側のアドレスは NAT ルーターの WAN 側アドレスに変換されます。ルーター側のアドレスは ppp0 に割り当てたグローバルアドレスとなります。
2. ここでは、説明を簡潔にするため、PPPoE セッションを自動的に再接続するためのトリガー設定を省いています。詳しくはルーター付属の「設定例集」をご覧ください。

## 7.2 基本設定（XAUTH 認証）

図 7.1.1（p.29）のネットワーク構成において、XAUTH 認証を用いてアドレス不定の AT-VPN Client から VPN 接続を受け付ける設定を示します。ここでは、以下の 2 ユーザーからの接続を想定します。セキュリティーポリシーはファイルでユーザーに提供します。

| フェーズ 1 ID | IKE 事前共有鍵 | XAUTH ユーザー名 | XAUTH パスワード | フェーズ 2 ID |
|---|---|---|---|---|
| IP アドレス（不定） | secret | user1 | passwd1 | user1 |
| IP アドレス（不定） | secret | user2 | passwd2 | user2 |

### AR ルーターの設定

**1** AT-VPN Client ユーザー user1、user2 を登録します（XAUTH ユーザー名とパスワード）。

```
ADD USER=user1 PASSWORD=passwd1 LOGIN=NO
ADD USER=user2 PASSWORD=passwd2 LOGIN=NO
```

**2** IKE フェーズ 1 の相手認証に使う事前共有鍵を作成します。**このコマンドはコンソール上で入力した場合のみ有効です。設定スクリプトファイル（.cfg）に記入した場合は無効ですのでご注意ください。**本例では、フェーズ 1 で個々のクライアントを識別できないため、事前共有鍵は全クライアント共通になります。

```
CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret
```

**3** ISAKMP ポリシーを作成し、ISAKMP を有効にします。ここでは、XAUTH を使用するすべてのクライアントからの IKE 要求を 1 つの ISAKMP ポリシー「ux」でまかないます。

```
CREATE ISAKMP POLICY=ux PEER=ANY KEY=1 XAUTH=SERVER SENDN=TRUE SETC=TRUE
ENABLE ISAKMP
```

**4** IPsec 通信の内容を規定する SA スペックとバンドルスペックを作成します。[1]

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
```

**5** IPsec ポリシーを作成し、IPsec を有効にします。「is」は IKE パケットを通過させるためのポリシー、「v1」「v2」は user1、user2 との VPN 通信用ポリシー、「in」はインターネットとの平文通信を行うためのポリシーです。RNAME は各ユーザーのフェーズ 2 ID[2] です。

```
CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
CREATE IPSEC POLICY=v1 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v1 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=user1
CREATE IPSEC POLICY=v2 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v2 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=user2
CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
ENABLE IPSEC
```

**6** Security Officer レベルのユーザー secoff を登録し、ルーターの動作モードをセキュリティーモードに切り替えます。[3]

1. AT-VPN Client では IPcomp（IP ペイロード圧縮）は使えません。
2. ここでは、わかりやすくするため XAUTH ユーザー名と同じにしています。

```
ADD USER=secoff PASS=PasswordS PRIVILEGE=SECURITYOFFICER
ENABLE SYSTEM SECURITY_MODE
```

## AT-VPN Client の設定

AT-VPN Client ユーザー user1、user2 用のセキュリティーポリシーファイル c1.spl、c2.spl を下記の内容で作成します。

**表 7.2.1 ポリシーファイル c1.spl（ファイルで提供）**

```
1 CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret
2 CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 XAUTH=CLIENT
      XAUTHNAME=user1 XAUTHPASS=passwd1
3 SET ISAKMP POLICY=i SENDN=TRUE SETC=TRUE
4 CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
5 CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
6 CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
7 CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
      PEER=200.100.10.1
8 SET IPSEC POLICY=vp LNAME=user1 RAD=192.168.10.0 RMA=255.255.255.0
9 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

**表 7.2.2 ポリシーファイル c2.spl（ファイルで提供）**

```
1 CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret
2 CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 XAUTH=CLIENT
      XAUTHNAME=user2 XAUTHPASS=passwd2
3 SET ISAKMP POLICY=i SENDN=TRUE SETC=TRUE
4 CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
5 CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
6 CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
7 CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
      PEER=200.100.10.1
8 SET IPSEC POLICY=vp LNAME=user2 RAD=192.168.10.0 RMA=255.255.255.0
9 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

以下に要点を示します。

- 1行目のVALUEには、ARルーターとのIKEネゴシエーションに使う事前共有鍵の値を指定します。この例では全クライアント共通になります。
- 2、7 行目の PEER には、AR ルーターの IP アドレスを指定します。
- 2 行目の XAUTHNAME、XAUTHPASS には、各クライアントの XAUTH ユーザー名とパスワードを指定します。
- 6、7、9 行目の INT には、VPN 通信に使うインターフェースの種類（PPP、Ethernet など）に関係なく、常に「ppp0」を指定します。
- 8行目のLNAMEには、クライアントのフェーズ2 ID（ARルーター側のRNAMEに指定した値）を指定します。クライアントごとに異なる値を使います。
- 8 行目の RAD、RMA は、VPN 通信の相手となるアドレス範囲（AR ルーター側の LAD、LMA に指定した値）を指定します。この値は AR ルーターのフェーズ 2 ID にもなります。

これらのファイルは、フロッピーディスクなどに入れて各ユーザーに渡してください。

3. セキュリティーモードでは、Security Officer レベルのユーザーでないと管理作業を行えません。また、手順 2 で作成した鍵の情報は、セキュリティーモードでないとルーターの再起動によって消去されてしまいます。

## 7.3 基本設定（ID 認証）

図 7.1.1（p.29）のネットワーク構成において、Aggressive モードで ID 認証を行い、アドレス不定の AT-VPN Client から VPN 接続を受け付ける設定を示します。ここでは、以下の 2 ユーザーからの接続を想定します。セキュリティーポリシーはファイルでユーザーに提供します。

| フェーズ 1 ID | IKE 事前共有鍵 | フェーズ 2 ID |
|---|---|---|
| user1 | secret01 | user1 |
| user2 | secret02 | user2 |

### AR ルーターの設定

**1** IKE フェーズ 1 の相手認証に使う事前共有鍵を作成します。**このコマンドはコンソール上で入力した場合のみ有効です。設定スクリプトファイル（.cfg）に記入した場合は無効ですのでご注意ください。**本例では、Aggressive モードと FQDN 形式の ID を用いることにより、フェーズ 1 で個々のクライアントを識別できるため、ユーザーごとに鍵を作成します。

```
CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret01
CREATE ENCO KEY=2 TYPE=GENERAL VALUE=secret02
```

**2** ISAKMP ポリシーを作成し、ISAKMP を有効にします。ここでは Aggressive モードを使い、ユーザーごとにポリシー「u1」「u2」を用意して（REMOTEID で区別）、事前共有鍵を個別に指定しています。

```
CREATE ISAKMP POLICY=u1 PEER=ANY KEY=1 MODE=AGGRESSIVE REMOTEID=user1
SET ISAKMP POLICY=u1 SENDN=TRUE SETC=TRUE
CREATE ISAKMP POLICY=u2 PEER=ANY KEY=2 MODE=AGGRESSIVE REMOTEID=user2
SET ISAKMP POLICY=u2 SENDN=TRUE SETC=TRUE
ENABLE ISAKMP
```

**3** IPsec 通信の内容を規定する SA スペックとバンドルスペックを作成します。[1]

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
```

**4** IPsec ポリシーを作成し、IPsec を有効にします。「is」は IKE パケットを通過させるためのポリシー、「v1」「v2」は user1、user2 との VPN 通信用ポリシー、「in」はインターネットとの平文通信を行うためのポリシーです。RNAME は各ユーザーのフェーズ 2 ID[2] です。

```
CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
CREATE IPSEC POLICY=v1 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v1 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=user1
CREATE IPSEC POLICY=v2 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v2 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=user2
CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
ENABLE IPSEC
```

**5** Security Officer レベルのユーザー secoff を登録し、ルーターの動作モードをセキュリティーモードに切り替えます。[3]

1. AT-VPN Client では IPcomp（IP ペイロード圧縮）は使えません。
2. ここでは、わかりやすくするためフェーズ 1 の ID と同じにしています。

```
ADD USER=secoff PASS=PasswordS PRIVILEGE=SECURITYOFFICER
ENABLE SYSTEM SECURITY_MODE
```

### AT-VPN Client の設定

AT-VPN Client ユーザー user1、user2 用のセキュリティーポリシーファイル c1.spl、c2.spl を下記の内容で作成します。

**表 7.3.1 ポリシーファイル c1.spl（ファイルで提供）**

```
1 CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret01
2 CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 MODE=AGGRESSIVE
3 SET ISAKMP POLICY=i LOCALID=user1 SENDN=TRUE SETC=TRUE
4 CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
5 CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
6 CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
7 CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
      PEER=200.100.10.1
8 SET IPSEC POLICY=vp LNAME=user1 RAD=192.168.10.0 RMA=255.255.255.0
9 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

**表 7.3.2 ポリシーファイル c2.spl（ファイルで提供）**

```
1 CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret02
2 CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 MODE=AGGRESSIVE
3 SET ISAKMP POLICY=i LOCALID=user2 SENDN=TRUE SETC=TRUE
4 CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
5 CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
6 CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
7 CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
      PEER=200.100.10.1
8 SET IPSEC POLICY=vp LNAME=user2 RAD=192.168.10.0 RMA=255.255.255.0
9 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

以下に要点を示します。

- 1行目のVALUEには、ARルーターとのIKEネゴシエーションに使う事前共有鍵の値を指定します。この例ではクライアントごとに異なる値を使っています。
- 2、7 行目の PEER には、AR ルーターの IP アドレスを指定します。
- 3 行目の LOCALID には、各クライアントのフェーズ 1 ID を指定します。
- 6、7、9 行目の INT には、VPN 通信に使うインターフェースの種類（PPP、Ethernet など）に関係なく、常に「ppp0」を指定します。
- 8行目のLNAMEには、クライアントのフェーズ2 ID（ARルーター側のRNAMEに指定した値）を指定します。クライアントごとに異なる値を使います。
- 8 行目の RAD、RMA は、VPN 通信の相手となるアドレス範囲（AR ルーター側の LAD、LMA に指定した値）を指定します。この値は AR ルーターのフェーズ 2 ID にもなります。

これらのファイルは、フロッピーディスクなどに入れて各ユーザーに渡してください。

## 7.4 ポリシーサーバー（1 ユーザーのみ）

3. セキュリティーモードでは、Security Officer レベルのユーザーでないと管理作業を行えません。また、手順 1 で作成した鍵の情報は、セキュリティーモードでないとルーターの再起動によって消去されてしまいます。

ここでは、AR ルーターをセキュリティーポリシーサーバーとして動作させるための設定について説明します。セキュリティーポリシーサーバー機能は、ISAKMP プロトコルをもとに AR ルーターが独自に実装した機能です。この機能を使用することで、AR ルーターから AT-VPN Client にセキュリティーポリシーファイルをダウンロードすることができます。なお、本例ではダウンロード時にユーザー名を指定できないため、提供できるポリシーファイルは 1 つだけとなります。複数ユーザーにポリシーファイルを提供したいときは、「7.5 ポリシーサーバー（複数ユーザー対応）」（p.39）をご覧ください。

ここでは、図 7.1.1（p.29）のネットワーク構成において、以下の 2 ユーザーからの接続を想定します。user1 にはポリシーサーバーの IP アドレスとダウンロード用パスワードを通知し、セキュリティーポリシーをダウンロードしてもらうようにします。user2 にはファイルでセキュリティーポリシーを提供します。

| フェーズ 1 ID | IKE 事前共有鍵 | XAUTH ユーザー名 | XAUTH パスワード | フェーズ 2 ID |
|---|---|---|---|---|
| IP アドレス（不定） | secret | user1 | passwd1 | user1 |
| IP アドレス（不定） | secret | user2 | passwd2 | user2 |

## AR ルーターの設定

**1** AT-VPN Client ユーザー user1、user2 を登録します（XAUTH ユーザー名とパスワード）。

```
ADD USER=user1 PASSWORD=passwd1 LOGIN=NO
ADD USER=user2 PASSWORD=passwd2 LOGIN=NO
```

**2** IKE フェーズ 1 の相手認証に使う事前共有鍵を作成します。**このコマンドはコンソール上で入力した場合のみ有効です。設定スクリプトファイル（.cfg）に記入した場合は無効ですのでご注意ください。**本例では、フェーズ 1 で個々のクライアントを識別できないため、事前共有鍵は全クライアント共通になります。

```
CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret
```

**3** ISAKMP ポリシーを作成します。ここでは、XAUTH を使用するすべてのクライアントからの IKE 要求を 1 つの ISAKMP ポリシー「ux」でまかないます。

```
CREATE ISAKMP POLICY=ux PEER=ANY KEY=1 XAUTH=SERVER SENDN=TRUE SETC=TRUE
```

**4** ポリシーサーバーとしての設定を追加します。ダウンロード用パスワードとして「getget」、ポリシーファイルとして「c1.scp」を指定し、ISAKMP とポリシーサーバー機能を有効にします。AR ルーター上にポリシーファイルを置くときは、拡張子を .scp にしてください。

```
CREATE ENCO KEY=10 TYPE=GENERAL VALUE=getget
CREATE ISAKMP POLICY=polserv PEER=ANY KEY=10
ENABLE ISAKMP POLICYSERVER=TRUE POLICYFILE=c1.scp
```

**5** IPsec 通信の内容を規定する SA スペックとバンドルスペックを作成します。[1]

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
```

1. AT-VPN Client では IPcomp（IP ペイロード圧縮）は使えません。

**6** IPsec ポリシーを作成し、IPsec を有効にします。「is」は IKE パケットを通過させるためのポリシー、「v1」「v2」は user1、user2 との VPN 通信用ポリシー、「in」はインターネットとの平文通信を行うためのポリシーです。RNAME は各ユーザーのフェーズ 2 ID[1] です。

```
CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
CREATE IPSEC POLICY=v1 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v1 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=user1
CREATE IPSEC POLICY=v2 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v2 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=user2
CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
ENABLE IPSEC
```

**7** Security Officer レベルのユーザー secoff を登録し、ルーターの動作モードをセキュリティーモードに切り替えます。[2]

```
ADD USER=secoff PASS=PasswordS PRIVILEGE=SECURITYOFFICER
ENABLE SYSTEM SECURITY_MODE
```

## AT-VPN Client の設定

AT-VPN Client ユーザー user1、user2 用のセキュリティーポリシーファイル c1.scp、c2.spl を下記の内容で作成します。ファイルの内容は「7.2 基本設定（XAUTH 認証）」(p.33) と同じですが、user1 用ポリシーファイルの拡張子が .scp である点に注意してください。

**表 7.4.1 ポリシーファイル c1.scp（ポリシーサーバーからダウンロード提供）**

```
1 CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret
2 CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 XAUTH=CLIENT
      XAUTHNAME=user1 XAUTHPASS=passwd1
3 SET ISAKMP POLICY=i SENDN=TRUE SETC=TRUE
4 CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
5 CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
6 CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
7 CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
      PEER=200.100.10.1
8 SET IPSEC POLICY=vp LNAME=user1 RAD=192.168.10.0 RMA=255.255.255.0
9 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

**表 7.4.2 ポリシーファイル c2.spl（ファイルで提供）**

```
1 CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret
2 CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 XAUTH=CLIENT
      XAUTHNAME=user2 XAUTHPASS=passwd2
3 SET ISAKMP POLICY=i SENDN=TRUE SETC=TRUE
4 CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
5 CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
6 CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
7 CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
      PEER=200.100.10.1
8 SET IPSEC POLICY=vp LNAME=user2 RAD=192.168.10.0 RMA=255.255.255.0
9 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

- ポリシーファイル c1.scp を AR ルーターのファイルシステム上に置き、ユーザーuser1 に次の情報を通知してください。
  - ポリシーサーバーの IP アドレス（ここでは 200.100.10.1）

1. ここでは、わかりやすくするため XAUTH ユーザー名と同じにしています。
2. セキュリティーモードでは、Security Officer レベルのユーザーでないと管理作業を行えません。また、手順 2 で作成した鍵の情報は、セキュリティーモードでないとルーターの再起動によって消去されてしまいます。

- ダウンロード用パスワード（ここでは getget）

- ユーザーuser2 には、ポリシーファイル c2.spl をフロッピーディスクなどで渡してください。

## 7.5 ポリシーサーバー（複数ユーザー対応）

ここでは、AR ルーターをセキュリティーポリシーサーバーとして動作させるための設定について説明します。セキュリティーポリシーサーバー機能は、ISAKMP プロトコルをもとに AR ルーターが独自に実装した機能です。この機能を使用することで、AR ルーターから AT-VPN Client にセキュリティーポリシーファイルをダウンロードさせることができます。管理者はクライアントユーザーにポリシーサーバーの IP アドレス、ダウンロード用ユーザー名とパスワードを通知するだけですむため、システムの管理が容易になります。本例では、Aggressive モードで ID 認証を行うことにより、複数のユーザーにポリシーファイルを提供できます。

ここでは、図 7.1.1（p.29）のネットワーク構成において、以下の 2 ユーザーからの接続を想定します。各ユーザーには、ポリシーサーバーの IP アドレスとダウンロード用ユーザー名、パスワードを通知し、それぞれ自分用のセキュリティーポリシーをダウンロードしてもらいます。

| フェーズ 1 ID | IKE 事前共有鍵 | フェーズ 2 ID |
|---|---|---|
| user1 | secret01 | user1 |
| user2 | secret02 | user2 |

### AR ルーターの設定

**1** IKE フェーズ 1 の相手認証に使う事前共有鍵を作成します。**このコマンドはコンソール上で入力した場合のみ有効です。設定スクリプトファイル（.cfg）に記入した場合は無効ですのでご注意ください。**本例では、Aggressive モードと FQDN 形式の ID を用いることにより、フェーズ 1 で個々のクライアントを識別できるため、ユーザーごとに鍵を作成します。また、これらの鍵はポリシーをダウンロードするときのパスワードにもなります。

```
CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret01
CREATE ENCO KEY=2 TYPE=GENERAL VALUE=secret02
```

**2** ISAKMP ポリシーを作成し、ISAKMP とポリシーサーバー機能を有効にします。ここでは Aggressive モードを使い、ユーザーごとにポリシー「u1」「u2」を用意して（REMOTEID で区別）、事前共有鍵とポリシーファイルを個別に指定しています。また、REMOTEID（フェーズ 1 ID）は、ポリシーダウンロード時のユーザー名にもなります。

```
CREATE ISAKMP POLICY=u1 PEER=ANY KEY=1 MODE=AGGRESSIVE REMOTEID=user1
SET ISAKMP POLICY=u1 POLICYFILE=c1.scp SENDN=TRUE SETC=TRUE
CREATE ISAKMP POLICY=u2 PEER=ANY KEY=2 MODE=AGGRESSIVE REMOTEID=user2
SET ISAKMP POLICY=u2 POLICYFILE=c2.scp SENDN=TRUE SETC=TRUE
ENABLE ISAKMP POLICYSERVER=TRUE
```

**3** IPsec 通信の内容を規定する SA スペックとバンドルスペックを作成します。[1]

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
```

1. AT-VPN Client では IPcomp（IP ペイロード圧縮）は使えません。

4 IPsec ポリシーを作成し、IPsec を有効にします。「is」は IKE パケットを通過させるためのポリシー、「v1」「v2」は user1、user2 との VPN 通信用ポリシー、「in」はインターネットとの平文通信を行うためのポリシーです。RNAME は各ユーザーのフェーズ 2 ID[1] です。

```
CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
CREATE IPSEC POLICY=v1 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v1 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=user1
CREATE IPSEC POLICY=v2 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v2 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=user2
CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
ENABLE IPSEC
```

5 Security Officer レベルのユーザー secoff を登録し、ルーターの動作モードをセキュリティーモードに切り替えます。[2]

```
ADD USER=secoff PASS=PasswordS PRIVILEGE=SECURITYOFFICER
ENABLE SYSTEM SECURITY_MODE
```

## AT-VPN Client の設定

AT-VPN Client ユーザー user1、user2 用のセキュリティーポリシーファイル c1.scp、c2.scp を下記の内容で作成します。内容は「7.3 基本設定（ID 認証）」（p.35）と同じですが、拡張子が異なる点にご注意ください。

**表 7.5.1 ポリシーファイル c1.scp（ポリシーサーバーからダウンロード提供）**

```
1 CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret01
2 CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 MODE=AGGRESSIVE
3 SET ISAKMP POLICY=i LOCALID=user1 SENDN=TRUE SETC=TRUE
4 CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
5 CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
6 CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
7 CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
      PEER=200.100.10.1
8 SET IPSEC POLICY=vp LNAME=user1 RAD=192.168.10.0 RMA=255.255.255.0
9 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

**表 7.5.2 ポリシーファイル c2.scp（ポリシーサーバーからダウンロード提供）**

```
1 CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret02
2 CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 MODE=AGGRESSIVE
3 SET ISAKMP POLICY=i LOCALID=user2 SENDN=TRUE SETC=TRUE
4 CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
5 CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
6 CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
7 CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
      PEER=200.100.10.1
8 SET IPSEC POLICY=vp LNAME=user2 RAD=192.168.10.0 RMA=255.255.255.0
9 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

ポリシーファイル c1.scp、c2.scp を AR ルーターのファイルシステム上に置き、各ユーザーに次の情報を通知してください。

- ポリシーサーバーの IP アドレス（ここでは 200.100.10.1）

1. ここでは、わかりやすくするためフェーズ 1 の ID と同じにしています。
2. セキュリティーモードでは、Security Officer レベルのユーザーでないと管理作業を行えません。また、手順 1 で作成した鍵の情報は、セキュリティーモードでないとルーターの再起動によって消去されてしまいます。

- ダウンロード用パスワード（ここでは secret01 か secret02）
- ダウンロード用ユーザー名（ここでは user1 か user2）

## 7.6 UDP トンネリング（NAT 越えの VPN 接続）

ここでは、AT-VPN Client と VPN ゲートウェイ（AR ルーター）の間に NAT 装置が入る場合の設定例を示します。

IPsec パケット（ESP パケット）には TCP、UDP のようなポート番号という概念がないため、通常 NAT 装置を通過できません。このような環境においても、本製品の UDP トンネリング（ESP over UDP）機能を利用すれば VPN 通信が可能です。UDP トンネリングは、ESP を UDP で包み込んで（カプセル化）送信することにより、NAT 装置を通過できるようにする機能です。受信側の VPN ゲートウェイでは UDP から ESP パケットを取り出し、あたかも AT-VPN Client から ESP パケットを直接受け取ったかのように処理します。

なお、UDP トンネリングを使用する場合は以下の制限がありますのでご注意ください。

- セキュリティープロトコルとして AH を使うことができません。これは、NAT 装置によって外側 IP ヘッダーが書き換えられてしまうためです。[1]
- IPsec ポリシーのパケット選択パラメーター(セレクター)として LNAME を使用することはできません。必ず内部 NAT を使用して、VPN 通信用の始点アドレスが固定されるようにしてください。詳細は設定例をご覧ください。

本例は、図 7.1.2（p.31）のネットワーク構成を前提としています。ここでは、以下の 2 ユーザーからの接続を想定します。セキュリティーポリシーはファイルでユーザーに提供します。

| フェーズ 1 ID | IKE 事前共有鍵 | フェーズ 2 ID | 内部 NAT アドレス |
|---|---|---|---|
| user1 | secret01 | user1 | 192.168.11.1 |
| user2 | secret02 | user2 | 192.168.11.2 |

### AR ルーターの設定

**1** IKE フェーズ 1 の相手認証に使う事前共有鍵を作成します。**このコマンドはコンソール上で入力した場合のみ有効です。設定スクリプトファイル（.cfg）に記入した場合は無効ですのでご注意ください。**本例では、Aggressive モードと FQDN 形式の ID を用いることにより、フェーズ 1 で個々のクライアントを識別できるため、ユーザーごとに鍵を作成します。

```
CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret01
CREATE ENCO KEY=2 TYPE=GENERAL VALUE=secret02
```

**2** ISAKMP ポリシーを作成し、ISAKMP を有効にします。ここでは Aggressive モードを使い、ユーザーごとにポリシー「u1」「u2」を用意して（REMOTEID で区別）、事前共有鍵を個別に指定しています。

1. AH では、外側 IP ヘッダー（の一部）までをデータ認証の対象とします。

```
CREATE ISAKMP POLICY=u1 PEER=ANY KEY=1 MODE=AGGRESSIVE REMOTEID=user1
SET ISAKMP POLICY=u1 SENDN=TRUE SETC=TRUE
CREATE ISAKMP POLICY=u2 PEER=ANY KEY=2 MODE=AGGRESSIVE REMOTEID=user2
SET ISAKMP POLICY=u2 SENDN=TRUE SETC=TRUE
ENABLE ISAKMP
```

**3** IPsec 通信の内容を規定する SA スペックとバンドルスペックを作成します。[1]

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
```

**4** IPsec ポリシーを作成し、IPsec を有効にします。「ud」は UDP トンネリングパケットを通過させるためのポリシー、「is」は IKE パケットを通過させるためのポリシー[2]、「v1」「v2」は user1、user2 との VPN 通信用ポリシー、「in」はインターネットとの平文通信を行うためのポリシーです。RAD は各クライアントの内部 NAT アドレスです[3]。また、UDPTUNNEL = TRUE を指定して UDP トンネリングを使うよう設定しています。

```
CREATE IPSEC POLICY=ud INT=ppp0 AC=PERMIT LPORT=2746 TRANS=UDP
CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 TRANS=UDP
CREATE IPSEC POLICY=v1 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v1 LAD=192.168.10.0 LMA=255.255.255.0 RAD=192.168.11.1
SET IPSEC POLICY=v1 UDPTUNNEL=TRUE
CREATE IPSEC POLICY=v2 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v2 LAD=192.168.10.0 LMA=255.255.255.0 RAD=192.168.11.2
SET IPSEC POLICY=v2 UDPTUNNEL=TRUE
CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
ENABLE IPSEC
```

**5** Security Officer レベルのユーザー secoff を登録し、ルーターの動作モードをセキュリティーモードに切り替えます。[4]

```
ADD USER=secoff PASS=PasswordS PRIVILEGE=SECURITYOFFICER
ENABLE SYSTEM SECURITY_MODE
```

## AT-VPN Client の設定

AT-VPN Client ユーザー user1、user2 用のセキュリティーポリシーファイル c1.spl、c2.spl を下記の内容で作成します。

1. AT-VPN Client では IPcomp（IP ペイロード圧縮）は使えません。また、UDP トンネリング使用時は AH（認証ヘッダー）も使えません。
2. AT-VPN Client から送られてくる ISAKMP パケット（UDP）の始点ポート番号が NAT で変換されるため、本設定例では「RPORT=500」を付けていないことに注意してください。
3. UDP トンネリング使用時は RNAME パラメーターは使えません。
4. セキュリティーモードでは、Security Officer レベルのユーザーでないと管理作業を行えません。また、手順 1 で作成した鍵の情報は、セキュリティーモードでないとルーターの再起動によって消去されてしまいます。

**表 7.6.1 ポリシーファイル c1.spl（ファイルで提供）**

```
1  ADD FIREWALL POLICY=net RU=1 AC=NAT INT=ppp0 GBLIP=192.168.11.1
       REMOTEIP=192.168.10.0-192.168.10.255 PROTO=ALL
2  CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret01
3  CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 MODE=AGGRESSIVE
4  SET ISAKMP POLICY=i LOCALID=user1 SENDN=TRUE SETC=TRUE
5  CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
6  CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
7  CREATE IPSEC POLICY=ud INT=ppp0 AC=PERMIT LPORT=2746 TRANS=UDP
8  CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
9  CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
       PEER=200.100.10.1
10 SET IPSEC POLICY=vp LAD=192.168.11.1 RAD=192.168.10.0 RMA=255.255.255.0
11 SET IPSEC POLICY=vp UDPTUNNEL=TRUE UDPHEARTBEAT=TRUE
12 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

**表 7.6.2 ポリシーファイル c2.spl（ファイルで提供）**

```
1  ADD FIREWALL POLICY=net RU=1 AC=NAT INT=ppp0 GBLIP=192.168.11.2
       REMOTEIP=192.168.10.0-192.168.10.255 PROTO=ALL
2  CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret02
3  CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 MODE=AGGRESSIVE
4  SET ISAKMP POLICY=i LOCALID=user2 SENDN=TRUE SETC=TRUE
5  CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
6  CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
7  CREATE IPSEC POLICY=ud INT=ppp0 AC=PERMIT LPORT=2746 TRANS=UDP
8  CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
9  CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
       PEER=200.100.10.1
10 SET IPSEC POLICY=vp LAD=192.168.11.2 RAD=192.168.10.0 RMA=255.255.255.0
11 SET IPSEC POLICY=vp UDPTUNNEL=TRUE UDPHEARTBEAT=TRUE
12 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

以下に要点を示します。

- 1 行目は IPsec 対象パケットに適用する内部 NAT の設定です。社内 LAN 宛てのパケット（終点アドレスが 192.168.10.0 ～ 192.168.10.255）は、始点アドレスを 192.168.11.1、192.168.11.2 に変換してから ESP でカプセル化します。
- 2 行目の VALUE には、AR ルーターとの IKE ネゴシエーションに使う事前共有鍵の値を指定します。この例ではクライアントごとに異なる値を使っています。
- 3、9 行目の PEER には、AR ルーターの IP アドレスを指定します。
- 4 行目の LOCALID には、各クライアントのフェーズ 1 ID を指定します。
- 7、8、9、12 行目の INT には、VPN 通信に使うインターフェースの種類（PPP、Ethernet など）に関係なく、常に「ppp0」を指定します。
- 10 行目の LAD には、1 行目で指定した NAT 後のアドレス（GBLIP）を指定します。UDP トンネリング使用時は LNAME パラメーターは使えません。
- 10 行目の RAD、RMA は、VPN 通信の相手となるアドレス範囲（AR ルーター側の LAD、LMA に指定した値）を指定します。この値は AR ルーターのフェーズ 2 ID にもなります。
- 11 行目の UDPTUNNEL=TRUE は UDP トンネリング（ESP over UDP）を使うための設定です。また、UDPHEARTBEAT=TRUE は、定期的に UDP パケットを送信することで、NAT 機器のセッションテーブルが消去されないようにする設定です。ただし、通信経路

上にダイヤルオンデマンド回線（ISDN など）がある場合は、回線が切断されなくなりますので「UDPHEARTBEAT=TRUE」を付けないでください。

これらのファイルは、フロッピーディスクなどに入れて各ユーザーに渡してください。

## 7.7 UDP トンネリング＋ポリシーサーバー

ここでは、UDP トンネリングの設定例にセキュリティーポリシーサーバーの設定を追加します。

セキュリティーポリシーサーバー機能は、ISAKMP プロトコルをもとに AR ルーターが独自に実装した機能です。この機能を使用することで、AR ルーターから AT-VPN Client にセキュリティーポリシーファイルをダウンロードさせることができます。管理者はクライアントユーザーにポリシーサーバーの IP アドレス、ダウンロード用ユーザー名とパスワードを通知するだけですむため、システムの管理が容易になります。本例では、Aggressive モードで ID 認証を行うことにより、複数のユーザーにポリシーファイルを提供できます。

ここでは、図 7.1.2（p.31）のネットワーク構成において、以下の 2 ユーザーからの接続を想定します。各ユーザーには、ポリシーサーバーの IP アドレスとダウンロード用ユーザー名、パスワードを通知し、それぞれ自分用のセキュリティーポリシーをダウンロードしてもらいます。

| フェーズ 1 ID | IKE 事前共有鍵 | フェーズ 2 ID | 内部 NAT アドレス |
|---|---|---|---|
| user1 | secret01 | user1 | 192.168.11.1 |
| user2 | secret02 | user2 | 192.168.11.2 |

### AR ルーターの設定

**1** IKE フェーズ 1 の相手認証に使う事前共有鍵を作成します。**このコマンドはコンソール上で入力した場合のみ有効です。設定スクリプトファイル（.cfg）に記入した場合は無効ですのでご注意ください。**本例では、Aggressive モードと FQDN 形式の ID を用いることにより、フェーズ 1 で個々のクライアントを識別できるため、ユーザーごとに鍵を作成します。

```
CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret01
CREATE ENCO KEY=2 TYPE=GENERAL VALUE=secret02
```

**2** ISAKMP ポリシーを作成し、ISAKMP とポリシーサーバー機能を有効にします。ここでは Aggressive モードを使い、ユーザーごとにポリシー「u1」「u2」を用意して（REMOTEID で区別）、事前共有鍵とポリシーファイルを個別に指定しています。また、REMOTEID（フェーズ 1 ID）は、ポリシーダウンロード時のユーザー名にもなります。

```
CREATE ISAKMP POLICY=u1 PEER=ANY KEY=1 MODE=AGGRESSIVE REMOTEID=user1
SET ISAKMP POLICY=u1 POLICYFILE=c1.scp SENDN=TRUE SETC=TRUE
CREATE ISAKMP POLICY=u2 PEER=ANY KEY=2 MODE=AGGRESSIVE REMOTEID=user2
SET ISAKMP POLICY=u2 POLICYFILE=c2.scp SENDN=TRUE SETC=TRUE
ENABLE ISAKMP POLICYSERVER=TRUE
```

**3** IPsec 通信の内容を規定する SA スペックとバンドルスペックを作成します。[1]

1. AT-VPN Client では IPcomp（IP ペイロード圧縮）は使えません。また、UDP トンネリング使用時は AH（認証ヘッダー）も使えません。

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
```

**4** IPsec ポリシーを作成し、IPsec を有効にします。「ud」は UDP トンネリングパケットを通過させるためのポリシー、「is」は IKE パケットを通過させるためのポリシー[1]、「v1」「v2」は user1、user2 との VPN 通信用ポリシー、「in」はインターネットとの平文通信を行うためのポリシーです。RAD は各クライアントの内部 NAT アドレスです[2]。また、UDPTUNNEL = TRUE を指定して UDP トンネリングを使うよう設定しています。

```
CREATE IPSEC POLICY=ud INT=ppp0 AC=PERMIT LPORT=2746 TRANS=UDP
CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 TRANS=UDP
CREATE IPSEC POLICY=v1 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v1 LAD=192.168.10.0 LMA=255.255.255.0 RAD=192.168.11.1
SET IPSEC POLICY=v1 UDPTUNNEL=TRUE
CREATE IPSEC POLICY=v2 INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1 PEER=DYNAMIC
SET IPSEC POLICY=v2 LAD=192.168.10.0 LMA=255.255.255.0 RAD=192.168.11.2
SET IPSEC POLICY=v2 UDPTUNNEL=TRUE
CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
ENABLE IPSEC
```

**5** Security Officer レベルのユーザー secoff を登録し、ルーターの動作モードをセキュリティーモードに切り替えます。[3]

```
ADD USER=secoff PASS=PasswordS PRIVILEGE=SECURITYOFFICER
ENABLE SYSTEM SECURITY_MODE
```

## AT-VPN Client の設定

AT-VPN Client ユーザー user1、user2 用のセキュリティーポリシーファイル c1.scp、c2.scp を下記の内容で作成します。内容は「7.6 UDP トンネリング（NAT 越えの VPN 接続）」(p.41）と同じですが、拡張子が異なる点にご注意ください。

**表 7.7.1 ポリシーファイル c1.scp（ポリシーサーバーからダウンロード提供）**

```
1  ADD FIREWALL POLICY=net RU=1 AC=NAT INT=ppp0 GBLIP=192.168.11.1
       REMOTEIP=192.168.10.0-192.168.10.255 PROTO=ALL
2  CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret01
3  CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 MODE=AGGRESSIVE
4  SET ISAKMP POLICY=i LOCALID=user1 SENDN=TRUE SETC=TRUE
5  CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
6  CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
7  CREATE IPSEC POLICY=ud INT=ppp0 AC=PERMIT LPORT=2746 TRANS=UDP
8  CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
9  CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
       PEER=200.100.10.1
10 SET IPSEC POLICY=vp LAD=192.168.11.1 RAD=192.168.10.0 RMA=255.255.255.0
11 SET IPSEC POLICY=vp UDPTUNNEL=TRUE UDPHEARTBEAT=TRUE
12 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

1. AT-VPN Client から送られてくる ISAKMP パケット（UDP）の始点ポート番号が NAT で変換されるため、本設定例では「RPORT=500」を付けていないことに注意してください。
2. UDP トンネリング使用時は RNAME パラメーターは使えません。
3. セキュリティーモードでは、Security Officer レベルのユーザーでないと管理作業を行えません。また、手順 1 で作成した鍵の情報は、セキュリティーモードでないとルーターの再起動によって消去されてしまいます。

**表 7.7.2 ポリシーファイル c2.scp（ポリシーサーバーからダウンロード提供）**

```
1  ADD FIREWALL POLICY=net RU=1 AC=NAT INT=ppp0 GBLIP=192.168.11.2
       REMOTEIP=192.168.10.0-192.168.10.255 PROTO=ALL
2  CREATE ENCO KEY=1 TYPE=GENERAL VALUE=secret02
3  CREATE ISAKMP POLICY=i PEER=200.100.10.1 KEY=1 MODE=AGGRESSIVE
4  SET ISAKMP POLICY=i LOCALID=user2 SENDN=TRUE SETC=TRUE
5  CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
6  CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1"
7  CREATE IPSEC POLICY=ud INT=ppp0 AC=PERMIT LPORT=2746 TRANS=UDP
8  CREATE IPSEC POLICY=is INT=ppp0 AC=PERMIT LPORT=500 RPORT=500 TRANS=UDP
9  CREATE IPSEC POLICY=vp INT=ppp0 AC=IPSEC KEY=ISAKMP BUNDLE=1
       PEER=200.100.10.1
10 SET IPSEC POLICY=vp LAD=192.168.11.2 RAD=192.168.10.0 RMA=255.255.255.0
11 SET IPSEC POLICY=vp UDPTUNNEL=TRUE UDPHEARTBEAT=TRUE
12 CREATE IPSEC POLICY=in INT=ppp0 AC=PERMIT
```

ポリシーファイル c1.scp、c2.scp を AR ルーターのファイルシステム上に置き、各ユーザーに次の情報を通知してください。

- ポリシーサーバーの IP アドレス（ここでは 200.100.10.1）
- ダウンロード用パスワード（ここでは secret01 か secret02）
- ダウンロード用ユーザー名（ここでは user1 か user2）

# 8 コマンドリファレンス

AT-VPN Client のセキュリティーポリシーファイルの中で使用できるコマンドについてまとめます。AR ルーター（VPN ゲートウェイ）側の設定コマンドについては、AR ルーターの取扱説明書、コマンドリファレンス、設定例集などをご覧ください。コマンド構文の表記は、AR ルーターのコマンドリファレンスに準じています。

**表 8.0.3 コマンド構文の表記規則**

| 表記 | 意味 |
|---|---|
| UPPER | 大文字（UPPERCASE）の部分はコマンド名やパラメーター名などのキーワード（予約語）を示します。基本的にそのまま入力してください。ただし、キーワードは大文字小文字の区別がないので、小文字で入力してもかまいません。一方、キーワードでない部分（パラメーター値など）には、大文字小文字を区別するものもありますので、各パラメーターの説明を参照してください。 |
| *italic* | 斜体（*italic*）は変数をあらわします。コマンド入力時には、環境に応じて異なる値が入ります。たとえば、GBLIP=*ipadd* のような構文では *ipadd* の部分に具体的な IP アドレスを入力します。 |
| *1..32* | 「*x..y*」は x ～ y の範囲の数値を指定することを示すもので、いわば変数の一種です。おもに、パラメーターごとに値の範囲が異なるようなコマンドの構文表記に使われます。 |
| {A\|B\|C} | ブレース（{ }）で囲まれた部分は、複数の選択肢からどれか一つを指定することを示します。選択肢の各項目は縦棒（\|）で区切られます。たとえば、PROTOCOL={AH\|ESP} は、PROTOCOL パラメーターの値としてキーワード AH か ESP のどちらか一方だけを指定することを示しています。 |
| [ ] | スクエアブラケット（[ ]）で囲まれた部分は省略可能であることを示します。 |
| **bold** | 太字（**bold**）の部分は、必ず入力しなくてはならない部分を表しています。より具体的には、[ ] で囲まれていない部分がこれに相当します。 |

## ADD FIREWALL POLICY RULE

**構文** **ADD FIREWALL POLICY=*policy* RULE=*rule-id* ACTION=NAT INTERFACE=*interface***
**PROTOCOL=ALL GBLIP=*ipadd* REMOTEIP=*ipadd*[-*ipadd*]**

**解説** 内部 NAT の変換ルールを設定する。内部 NAT は、トンネルモード SA において内側 IP ヘッダーの始点 IP アドレスを書き換える機能。VPN 通信時に、ISP から割り当てられたグローバルアドレスではなく、接続先ネットワークの構成に適したアドレス（プライベートアドレスなど）を使いたい場合などに使う。また、UDP トンネリングを使う場合は内部 NAT によるアドレス変換が通常必須。

なお、本コマンドは AR ルーターのコマンド体系を踏襲しているため名前に「Firewall」という単語が含まれているが、AT-VPN Client にはファイアウォール機能はないので注意。純粋に NAT の設定を行うコマンドである。

**パラメーター** **POLICY**

ファイアウォールポリシー名。AT-VPN Client では意味を持たないので「net」など任意の名前を指定する

**RULE**

ルール番号。NAT ルールは番号の若い順に検索され、最初に一致したものが適用される

**ACTION**

ルールの処理内容（アクション）。AT-VPN Client では「NAT」しか指定できない

**INTERFACE**

ルールを適用するインターフェースの名前。AT-VPN Client では意味を持たないので「myadapter」など任意の名前を指定する

**PROTOCOL**

IP 上のプロトコルタイプ。AT-VPN Client では常に ALL（全プロトコル）を指定して、すべての IP パケットが変換対象になるようにする

**GBLIP**

変換後の IP アドレス（内部 NAT アドレス）。終点アドレスが REMOTEIP の範囲におさまるパケットは、始点アドレスが GBLIP に書き換えられた上で送信される

**REMOTEIP**

リモート側 IP アドレス。AT-VPN Client では、VPN 通信の相手となるネットワーク（社内 LAN など）のアドレス範囲を指定する。本パラメーターで指定したアドレス宛てのパケットだけが NAT の対象となり、その他のパケットは変換なしでそのまま送信される

**例**

- サブネット 192.168.10.0/24 との通信時には、始点 IP アドレスを 192.168.11.1 に書き換える。

```
ADD FIREWALL POLICY=net RULE=1 ACTION=NAT INT=ppp0 PROTO=ALL
   GBLIP=192.168.11.1 REMOTEIP=192.168.10.0-192.168.10.255
```

## CREATE ENCO KEY

**構文** **CREATE ENCO KEY=*key-id* TYPE={GENERAL|DES} VALUE=*value***

**解説** 暗号化や認証に用いる鍵の値を指定する。VPN ゲートウェイ（ルーター）に設定してあるのと同じ値を指定すること。

**パラメーター**

**KEY**

鍵番号（0 ～ 65535）。CREATE IPSEC SASPECIFICATION コマンドや CREATE ISAKMP POLICY コマンドでは、この番号で鍵を指定する

**TYPE**

鍵の種類。GENERAL は ISAKMP の事前共有鍵や認証用ハッシュ鍵として使う任意長の汎用鍵。DES は 56 ビット DES で使う暗号鍵

**VALUE**

鍵の値。汎用鍵の場合は任意の ASCII 文字列か 16 進数を指定する。DES 鍵の場合は 0x で始まる 64 ビット（パリティーを含む）の 16 進数を指定する

**例**

- ISAKMP の事前共有鍵（pre-shared key）を登録する。

```
CREATE ENCO KEY=1 TYPE=GENERAL VALUE="confidential"
```

- DES 暗号鍵（パリティーを含め 64 ビット）を登録する。

```
CREATE ENCO KEY=2 TYPE=DES VALUE=0xBB09BAC150913E82
```

- ハッシュ関数 MD5 用の認証鍵（16 バイト）を登録する。

```
CREATE ENCO KEY=3 TYPE=GENERAL VALUE="jogefogejogefoge"
```

## CREATE/SET IPSEC BUNDLESPECIFICATION

**構文**

**CREATE IPSEC BUNDLESPECIFICATION=*bspec-id* KEYMANAGEMENT={ISAKMP|MANUAL}**
**STRING="*bundle-string*"** [EXPIRYKBYTES=*1..2000000000*]
[EXPIRYSECONDS=*300..31449600*]

**SET IPSEC BUNDLESPECIFICATION=*bundle-id*** [EXPIRYKBYTES=*1..2000000000*]
[EXPIRYSECONDS=*300..31449600*]

**解説**

SA バンドルスペックを作成する。SA バンドルスペックは、IPsec 通信で使用する SA スペック（プロトコル等）の組み合わせを指定するもの。これにより、あるトラフィックには DES による暗号化（ESP）を施し、別のトラフィックには DES による暗号化（ESP）と MD5 による認証（AH）を適用するといった設定が可能になる。

**パラメーター**

**BUNDLESPECIFICATION**

SA バンドルスペック番号（0 ～ 255）

**KEYMANAGEMENT**

鍵管理方式。SA バンドルの作成を手動で行うか（MANUAL= 手動鍵管理）、ISAKMP/IKE のネゴシエーションによって自動的に行うか（ISAKMP= 自動鍵管理）を指定する

**STRING**

バンドルを構成する SA スペックの組み合わせ。SA スペック番号を AND、OR、カンマで区切って記述する。手動鍵管理の場合は、最大 2 個の SA スペックを AND で区切って指定する。各 SA スペックは、それぞれ別の IPsec プロトコル（ESP、AH）でなくてはならない。たとえば、SA スペック「1」（ESP）と「3」（AH）からなる SA バンドルは「1 AND 3」のように指定する。この場合、パケットに対して ESP、AH の順に処理が行われる。自動鍵管理の場合は、SA スペックの組み合わせをカンマ区切りで複数候補指定できる。実際にどのバンドル構成が使用されるかは、ISAKMP/IKE のネゴシエーションによって決まる。SA スペック「1」と「2」なら「1 AND 2」、「1」か「2」のどちらかのみなら「1 OR 2」、「1」と「2」が第一候補で「1」と「3」が第二候補なら、「1 AND 2, 1 AND 3」のように記述する。「AND」は併用するプロトコルを指定するものでそれぞれが異なるプロトコルでなくてはならない。「OR」はアルゴリズムの選択肢を示すもので同じプロトコルでなくてはならない。また、「AND」によるプロトコルの適用順序は、通常 ESP、AH の順とする。AT-VPN Client では IPComp は使えない

**例**

- 手動鍵管理用の SA バンドルスペック「1」を作成する。SA スペックは「1」と「2」を使用する。

```
CREATE IPSEC BUNDLE=1 KEYMAN=MANUAL STRING="1 AND 2"
```

- 自動鍵管理用の SA バンドルスペック「2」を作成する。SA スペックの組み合わせは、3 つの候補を指定する。

```
CREATE IPSEC BUNDLE=2 KEYMAN=ISAKMP STR="1 OR 2 AND 4, 1 OR 2, 3 AND 4"
```

# CREATE/SET IPSEC POLICY

**構文**

```
CREATE IPSEC POLICY=name INTERFACE=interface
      ACTION={DENY|IPSEC|PERMIT} [KEYMANAGEMENT={ISAKMP|MANUAL}]
      [BUNDLESPECIFICATION=bspec-id] [PEERADDRESS=ipadd]
      [LADDRESS={ANY|ipadd[-ipadd]}] [LMASK=ipadd] [LNAME={ANY|name}]
      [LPORT={ANY|port}] [RADDRESS={ANY|ipadd[-ipadd]}] [RMASK=ipadd]
      [RNAME={ANY|name}] [RPORT={ANY|port}]
      [TRANSPORTPROTOCOL={ANY|ESP|GRE|ICMP|OSPF|RSVP|TCP|UDP|protocol}]
      [GROUP={0|1|2}] [ISAKMPPOLICY=name] [UDPHEARTBEAT={TRUE|FALSE}]
      [UDPPORT=port] [UDPTUNNEL={TRUE|FALSE}] [USEPFSKEY={TRUE|FALSE}]

SET IPSEC POLICY=name [ACTION={DENY|IPSEC|PERMIT}]
      [BUNDLESPECIFICATION=bspec-id] [PEERADDRESS=ipadd]
      [LADDRESS={ANY|ipadd[-ipadd]}] [LMASK=ipadd] [LNAME={ANY|name}]
      [LPORT={ANY|port}] [RADDRESS={ANY|ipadd[-ipadd]}] [RMASK=ipadd]
      [RNAME={ANY|name}] [RPORT={ANY|port}]
      [TRANSPORTPROTOCOL={ANY|ESP|GRE|ICMP|OSPF|RSVP|TCP|UDP|protocol}]
      [GROUP={0|1|2}] [ISAKMPPOLICY=name] [UDPHEARTBEAT={TRUE|FALSE}]
      [UDPPORT=port] [UDPTUNNEL={TRUE|FALSE}] [USEPFSKEY={TRUE|FALSE}]
```

**解説**

IPsec ポリシーを作成する。IPsec ポリシーは、IP アドレス・IP プロトコル・ポートなどによって識別されるパケットに対し、どのような処理（IPsec 適用、通過、拒否）を施すかを指定する一種のフィルタールール。

AT-VPN Client では、Adapters メニューで選択したネットワークアダプターからパケットを送信するときと、同アダプターでパケットを受信したときにポリシーの検索が行われ、最初に条件に一致したポリシーのアクション（処理）が実行される。ポリシーの検索はセキュリティーポリシーファイル内での記述順にしたがって行われる。

1 つでもポリシーを作成すると、ポリシーリストの末尾にすべてのパケットを破棄（DENY）する暗黙のポリシーが作成されるので注意が必要。

**パラメーター**

**POLICY**

IPsec ポリシー名。ポリシーごとに異なる名前を付ける

**INTERFACE**

ポリシーを適用するインターフェース。IPsec ポリシーは、指定したインターフェースからパケットを送出するときと、同インターフェースでパケットを受信したときに処理される。AT-VPN Client では、すべての IPsec ポリシーが「Adapters」メニューで選択したネットワークアダプターに適用されるため、本パラメーターは実質的な意味を持たない。「ppp0」や「wan」など任意の文字列を指定する

**ACTION**

本ポリシーの条件（LADDRESS、LMASK、LNAME、LPORT、RADDRESS、RMASK、RNAME、RPORT、TRANSPORTPROTOCOL）に適合したパケットに対する処理を指定する。IPSEC（BUNDELSPECIFICATION パラメーターで指定した SA バンドルスペックによって処理する）、PERMIT（IPsec を使わない通常のパケット処理を行う）、DENY（パケットを破棄する）から選択する。IPSEC を指定した場合は、対向 IPsec 装置の IP アドレス（PEERADDRESS）、SA バンドルスペック（BUNDLESPECIFICATION）、鍵管理方式（KEYMANAGEMENT）も指定すること

**KEYMANAGEMENT**

SA バンドル作成時の鍵管理方式を指定する。手動（MANUAL）、自動（ISAKMP）から選択する。BUNDLESPECIFICATION パラメーターで指定した SA バンドルスペックと同じ鍵管理方式を指定すること。ACTION に IPSEC を指定した場合のみ有効（かつ必須）

**BUNDLESPECIFICATION**

SA バンドルスペックを指定する。SA バンドルは、IPsec 処理に使用するセキュリティープロトコルやアルゴリズムの情報をひとまとめにしたもの。本パラメーターは、ACTION に IPSEC を指定した場合のみ有効（かつ必須）。なお、SA バンドルスペックの鍵管理方式が、本コマンドの KEYMANAGEMENT パラメーターと一致していること

**PEERADDRESS**

VPN ゲートウェイの IP アドレス。ACTION に IPSEC を指定したときだけ有効（かつ必須）

**LADDRESS**

パケット選択パラメーター（セレクター）の 1 つ。ポリシーの適用対象となるパケットのローカル側 IP アドレスを指定する。AT-VPN Client の IP アドレスが固定されている場合は、そのアドレスを指定する。アドレスが固定されていない場合は LNAME パラメーターで任意のシステム名（ただし、VPN ゲートウェイ側の RNAME パラメーターに指定してあるもの）を指定する。アドレスが不定でも内部 NAT を使う場合は、LADDRESS パラメーターに NAT 後のアドレスを指定する。省略時は ANY（すべて）

**LMASK**

セレクターの 1 つ。LADDRESS に対するネットマスクを指定する。省略時は 255.255.255.255

**LNAME**

セレクターの 1 つ。ローカル側システム名を指定する。本パラメーターは自アドレスが不定のときに指定するもので、ISAKMP のフェーズ 2 ID として対向システムに送信される。本パラメーターは UDP トンネリング時には使用できない。省略時は ANY（すべて）

**LPORT**

セレクターの 1 つ。ローカル側ポート番号。省略時は ANY（すべて）

**RADDRESS**

セレクターの 1 つ。ポリシーの適用対象となるパケットのリモート側 IP アドレス。RMASK と組み合わせてサブネットを指定したり、ハイフンでアドレスの範囲を指定することもできる。通常は VPN で通信したいネットワークのアドレス範囲（例：社内 LAN のサブネットアドレスなど）を指定する。省略時は ANY（すべて）

**RMASK**

セレクターの 1 つ。RADDRESS に対するネットマスク。省略時は 255.255.255.255

**RNAME**

セレクターの 1 つ。リモート側システム名。省略時は ANY（すべて）

**RPORT**

セレクターの 1 つ。リモート側ポート番号。省略時は ANY（すべて）

**TRANSPORTPROTOCOL**

セレクターの 1 つ。ポリシーの適用対象となるパケットの IP プロトコルタイプ。ALL、TCP のような定義済みの文字列かプロトコル番号で指定する。省略時は ANY（すべて）

**GROUP**

IKE フェーズ 2（Quick モード）での Diffie-Hellman 鍵交換に使用する Oakley グループ。PFS（Perfect Forward Secrecy）を有効にしている場合（USEPFSKEY パラメーターに TRUE を指定した場合）のみ有効。省略時はグループ 1

**ISAKMPPOLICY**

ISAKMP ポリシー名。ACTION に IPSEC を指定した場合のみ有効。通常指定する必要はないが、同じ PEERADDRESS を持つ ISAKMP ポリシーが複数存在するときに、この IPsec ポリシーで使用する ISAKMP ポリシーを明示的に指定したい場合に使う

**UDPHEARTBEAT**

UDP ハートビートを使用するかどうか。UDP ハートビートは、UDP トンネリング（ESP over UDP）使用時に、セッション情報が NAT 機器の変換テーブルから消えてしまうことを防ぐための機能。TRUE を指定した場合は、対向 IPsec 装置の UDP ポート 2746 番（UDPPORT パラメーターで変更可能）宛てに 30 秒間隔でハートビートパケットを送信する。このパケットはセッション維持だけを目的としているため、受信側での処理は行われない。省略時は FALSE

**UDPPORT**

UDP トンネリング（ESP over UDP）パケットの送信先 UDP ポート。デフォルトは 2746 番

**UDPTUNNEL**

UDP トンネリング（ESP over UDP）を使用するかどうか。TRUE を指定した場合は、IPsec（ESP）パケットを UDP でカプセル化して対向 IPsec 装置の 2746 番ポート（UDPPORT パラメーターで変更可能）宛てに送信する。これにより、VPN ゲートウェイと AT-VPN Client の間に NAT 装置がある環境でも IPsec を使用できるようになる。ただし、UDP トンネリング使用時は AH を利用できない。また、セレクターとして LNAME パラメーターを使用できない（NAT が必須。NAT 後の GBLIP を LADDRESS に指定する）。省略時は FALSE

**USEPFSKEY**

PFS（Perfect Forward Secrecy）の有効・無効。PFS とは、ある鍵の解読が他の鍵の解読の手がかりにならないような性質を言う。PFS を有効にすると、IPsec SA 鍵の生成・更新時に Diffie-Hellman アルゴリズムを再実行するようになる。自動鍵管理（KEYMANAGEMENT=ISAKMP）のときのみ有効。省略時は FALSE

**例**

- ISAKMP パケット（始点・終点ポートともに 500 番の UDP パケット）を素通しさせる IPsec ポリシー「isa」を作成する。

```
CREATE IPSEC POLICY=isa INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500
   TRANSPORT=UDP
```

- IPsec ポリシー「vpn」を定義し、サブネット 192.168.10.0/24 との通信に IPsec を使うよう設定する。この例では自アドレスが不定のため、LNAME パラメーターで名前「user1」を指定している。VPN ゲートウェイのアドレスは 200.100.10.1、使用する SA バンドルスペックは「1」。

```
CREATE IPSEC POLICY=vpn INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
   PEER=200.100.10.1

SET IPSEC POLICY=vpn LNAME=user1 RAD=192.168.10.0 RMASK=255.255.255.0
```

- 他の IPsec ポリシーにマッチしなかったパケットをすべて素通し(平文通信)させる IPsec ポリシー「inet」を作成する。特定のサイトとは IPsec で通信し、その他のサイトとは平文で通信したい場合は、最後のポリシーとして「すべて許可」のポリシーを設定する必要がある(RAD などの条件を指定しなかった場合は「すべて」の意味になる)。

```
CREATE IPSEC POLICY=inet INT=ppp0 ACTION=PERMIT
```

## CREATE/SET IPSEC SASPECIFICATION

**構文**

```
CREATE IPSEC SASPECIFICATION=spec-id KEYMANAGEMENT={ISAKMP|MANUAL}
     PROTOCOL={AH|ESP} [MODE={TRANSPORT|TUNNEL}] [ENCALG={DES|NULL}]
     [ENCKEY=key-id] [HASHALG={DESMAC|MD5|NULL|SHA}] [HASHKEY=key-id]
     [INSPI=spi] [OUTSPI=spi]

SET IPSEC SASPECIFICATION=spec-id [MODE={TRANSPORT|TUNNEL}]
     [ENCALG={DES|NULL}] [ENCKEY=key-id]
     [HASHALG={DESMAC|MD5|NULL|SHA}] [HASHKEY=key-id] [INSPI=spi]
     [OUTSPI=spi]
```

**解説**

SA スペックを作成する。SA スペックは IPsec 通信の仕様(パケットに適用する処理)を定義するもので、SA の動作モード(トンネル、トランスポート)、鍵管理方式(手動、自動)、処理 / プロトコル(暗号化・認証 /ESP、認証 /AH)、使用アルゴリズム(DES、MD5、SHA など)、SPI(手動設定の場合)などのパラメーターを設定する。

**パラメーター**

**SASPECIFICATION**

SA スペック番号

**KEYMANAGEMENT**

鍵管理方式。手動設定(MANUAL)か自動設定(ISAKMP)から選択する

**PROTOCOL**

IPsec プロトコル。ESP(暗号化と認証)、AH(認証)から選択する。個々の SA スペックでは 1 つしかプロトコルを指定できないが、実際に IPsec 通信の設定を行うときは、SA スペックの組み合わせを「SA バンドルスペック」として指定する。なお、UDP トンネリング使用時は AH 使用不可

**MODE**

SA の動作モード。TUNNEL(トンネルモード)と TRANSPORT(トランスポートモード)がある。省略時は TUNNEL

**ENCALGORITHM**

暗号化アルゴリズム。PROTOCOL に ESP を指定した場合の必須パラメーター。通常は DES(56 ビット DES)を指定する。NULL(NULL 暗号化アルゴリズム)は、ESP の認証機能だけを使いたいときやデバッグを行うときに指定する。ENCALGORITHM と HASHALGORITHM の両方に NULL を指定することはできない

**ENCKEY**

暗号鍵番号。PROTOCOL に ESP を指定し、KEYMANAGEMENT に MANUAL を指定した場合にのみ有効(かつ必須)

**HASHALGORITHM**

メッセージ認証用のハッシュアルゴリズム。必須パラメーター。NULL は ESP の暗号化機能だけを用い、認証機能を使わない場合に指定する。ENCALGORITHM と HASHALGORITHM の両方に NULL を指定することはできない

**HASHKEY**

認証鍵番号。KEYMANAGEMENT に MANUAL を指定した場合にのみ有効（かつ必須）

**INSPI**

内向きトラフィックの SPI (Security Parameter Index) 値。KEYMANAGEMENT に MANUAL を指定した場合にのみ有効（かつ必須）

**OUTSPI**

外向きトラフィックの SPI (Security Parameter Index) 値。KEYMANAGEMENT に MANUAL を指定した場合にのみ有効（かつ必須）

**例**

- 自動鍵管理用の SA スペック「1」を作成する。この SA では、トンネルモード ESP による暗号化と認証を行う。暗号化アルゴリズムには DES を、認証用のハッシュアルゴリズムには SHA を用いる。暗号・認証鍵と SPI 値は、ISAKMP/IKE のネゴシエーションによって自動的に管理するため指定しない

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
```

## CREATE/SET ISAKMP POLICY

**構文**

```
CREATE ISAKMP POLICY=name PEER={ipadd|ANY} [KEY=0..65535]
      [MODE={MAIN|AGGRESSIVE}] [LOCALID=id] [REMOTEID=id] [ENCALG=DES]
      [HASHALG={SHA|MD5}] [GROUP={0|1|2}] [DHEXPONENTLENGTH=160..1023]
      [SENDDELETES={TRUE|FALSE}] [SENDNOTIFY={TRUE|FALSE}]
      [SETCOMMITBIT={TRUE|FALSE}] [EXPIRYKBYTES=1..1000]
      [EXPIRYSECONDS=600..31449600] [PRENEGOTIATE={TRUE|FALSE}]
      [HEARTBEATMODE={BOTH|NONE|RECEIVE|SEND}] [XAUTH={CLIENT|NONE}]
      [XAUTHNAME=username] [XAUTHPASSWORD=password]

SET ISAKMP POLICY=name [KEY=0..65535] [MODE={MAIN|AGGRESSIVE}]
      [LOCALID=id] [REMOTEID=id] [ENCALG=DES] [HASHALG={SHA|MD5}]
      [GROUP={0|1|2}] [DHEXPONENTLENGTH=160..1023]
      [SENDDELETES={TRUE|FALSE}] [SENDNOTIFY={TRUE|FALSE}]
      [SETCOMMITBIT={TRUE|FALSE}] [EXPIRYKBYTES=1..1000]
      [EXPIRYSECONDS=600..31449600] [PRENEGOTIATE={TRUE|FALSE}]
      [HEARTBEATMODE={BOTH|NONE|RECEIVE|SEND}] [XAUTH={CLIENT|NONE}]
      [XAUTHNAME=username] [XAUTHPASSWORD=password]
```

**解説**

ISAKMP ポリシーを作成する。ISAKMP ポリシーでは、ISAKMP メッセージの交換相手（ISAKMP ピア）や使用する鍵・認証アルゴリズムなど、ISAKMP/IKE に関する各種設定パラメーターを定義する。

**パラメーター**

**POLICY**

ISAKMP ポリシー名

**PEER**

ISAKMP の通信相手（ISAKMP ピア）の IP アドレスを指定する。ANY を指定した場合は、どの相手からでも接続要求を受け入れる

**KEY**

ISAKMP ピアの認証に用いる事前共有鍵（GENERAL 鍵）の番号を指定する

**MODE**

ISAKMP フェーズ 1 で使用する IKE 交換モード。ID 情報が保護される MAIN モードと ID 情報が保護されない AGGRESSIVE モードがある。相手認証に事前共有鍵（PRESHARED）方式を使い、なおかつ、AT-VPN Client のアドレスが不定な場合は AGGRESSIVE モードを使う必要がある。それ以外の場合は通常 MAIN モードを使う。省略時は MAIN モード

**LOCALID**

ISAKMP フェーズ 1 において、相手に送信する ID ペイロードの内容（自分の ID 情報）を指定する。IP アドレス（例：172.16.10.5）、ドメイン名（例：bar.mydomain.net）、ユーザー名付きドメイン名（例：joger@bar.mydomain.net）の 3 形式が使用できる。本パラメーター省略時は、Adapters メニューで選択したアダプターの IP アドレスが ID として使われる。このパラメーターは、おもに AT-VPN Client の IP アドレスが不定な場合に使う

**REMOTEID**

ISAKMP フェーズ 1 において、相手から受け取ることを期待する ID ペイロードの内容（相手の ID 情報）を指定する。IP アドレス（例：172.16.10.5）、ドメイン名（例：bar.mydomain.net）、ユーザー名付きドメイン名（例：joger@bar.mydomain.net）の 3 形式が使用できる。デフォルトでは、相手から受け取った ISAKMP メッセージの始点 IP アドレスを ID 値として期待する。このパラメーターは、おもに相手の IP アドレスが不定な場合に使う

**ENCALG**

ISAKMP メッセージの暗号化アルゴリズム。DES のみサポート。省略時は DES

**HASHALG**

ISAKMP メッセージの認証用ハッシュアルゴリズム。省略時は SHA

**GROUP**

鍵交換時に用いる Diffie-Hellman（Oakley）グループを指定する。グループ 0（512 ビット MODP）、グループ 1（768 ビット MODP）、グループ 2（1024 ビット MODP）から選択する。省略時はグループ 1

**DHEXPONENTLENGTH**

Diffie-Hellman 鍵交換アルゴリズムにおいて、各当事者が生成する乱数（$g^a$ mod p における a）の長さ（ビット）。値が大きいほど生成した鍵の安全性が高まるが、鍵の交換に時間がかかるようになる。Oakley グループ 0、1、2 いずれの場合も最小値は 160 ビット。最大値はグループによって異なり、グループ 0 は 511 ビット、グループ 1 は 767 ビット、グループ 2 は 1023 ビット。省略時は 160 ビット

**SENDDELETES**

SA の削除を通知する Delete ペイロードを送信するかどうか。TRUE を指定した場合は、ローカル側で SA 情報が削除された場合に該当 SA がもはや有効でないことを相手に通知する。省略時は FALSE

**SENDNOTIFY**

IKE のステータスやエラー情報を通知する Notify ペイロードを送信するかどうか。省略時は FALSE

**SETCOMMITBIT**

ISAKMP SA のネゴシエーション時に ISAKMP ヘッダーの Commit ビットをオンにするかどうか。省略時は FALSE

**EXPIRYKBYTES**

ISAKMP SA の有効期限（Kbyte）。通信データ量が指定量に達すると、ISAKMP SA は再ネゴシエートされる。省略時は NONE（無期限）

**EXPIRYSECONDS**

ISAKMP SA の有効期限（秒）。SA 作成後、指定時間が経過すると、ISAKMP SA は再ネゴシエートされる。省略時は 86400（24 時間）

**PRENEGOTIATE**

起動時に IKE フェーズ 1 のネゴシエーションを行っておくかどうか（ISAKMP SA を確立しておくかどうか）を指定する。省略時は FALSE

**HEARTBEATMODE**

ISAKMP ハートビートを使用するかどうか。ISAKMP ハートビートは、VPN ゲートウェイ・AT-VPN Client 間の通信が途絶えたときに古い SA 情報が残らないようにする独自機能。SEND を指定した場合は、20 秒間隔でハートビートメッセージを送信する。RECEIVE を指定した場合は、ハートビートメッセージの受信だけを行う。受信側は、3 回連続してハートビートを受信できなかった場合は通信が不可能になったものとみなして、対向 IPsec 装置との間に張られた SA をすべて削除する。BOTH を指定したときは送信と受信の両方を行う。NONE はハートビートメッセージを使用しないことを示す。省略時は NONE

**XAUTH**

ISAKMP フェーズ 1 終了後に拡張認証（XAUTH）を受けるかどうか（AT-VPN Client はクライアントモードのみサポート）。CLIENT を指定した場合は XAUTH クライアント（認証を受ける側）として動作する。NONE は XAUTH を使わない。省略時は NONE

**XAUTHNAME**

XAUTH ユーザー名

**XAUTHPASSWORD**

XAUTH パスワード

**例**

- VPN ゲートウェイ 1.2.3.4 との間でネゴシエーションを行う ISAKMP ポリシー「ix」を作成する。事前共有鍵は「1」。フェーズ 1 完了後に XAUTH 認証を受ける。XAUTH ユーザー名は「user1」、パスワードは「passwd1」

```
CREATE ISAKMP POLICY=ix PEER=1.2.3.4 KEY=1 XAUTH=CLIENT XAUTHNAME=user1
   XAUTHPASS=passwd1 SENDN=TRUE SETC=TRUE
```

- VPN ゲートウェイ 200.100.10.1 との間でネゴシエーションを行う ISAKMP ポリシー「ia」を作成する。Aggressive モードで自 ID として「user1」を送る。事前共有鍵は「1」

```
CREATE ISAKMP POLICY=ia PEER=200.100.10.1 KEY=1 MODE=AGGRESSIVE
   LOCALID="user1" SENDN=TRUE SETC=TRUE
```

## SET IPSEC UDPPORT

**構文** **SET IPSEC UDPPORT=*port***

**解説**　UDP トンネリング（ESP over UDP）パケットを送受信する（ローカル側）UDP ポートを変更する。デフォルトは 2746 番。

**パラメーター**　**UDPPORT**

UDP ポート番号（0 ～ 65535）。デフォルトは 2746

# A ユーザーサポート

障害回避などのユーザーサポートは、巻末の「調査依頼書」をコピーしたものに必要事項を記入し、下記のサポート先に FAX してください。できるだけ電話による直接の問い合わせは避けてください。FAX によって詳細な情報を送付していただくほうが、電話による問い合わせよりも遥かに早く問題を解決することができます。記入内容の詳細は、「調査依頼書のご記入にあたって」をご覧ください。なお、**お試し版をご利用のお客様のユーザーサポートは、お受けできません。**

**アライドテレシス株式会社　サポートセンター**

Tel: 0120-860-772
月～金（祝・祭日を除く）9:00 ～ 12:00、13:00 ～ 18:00

Fax: 0120-860-662
年中無休 24 時間受け付け

## 調査依頼書のご記入にあたって

本依頼書は、お客様の環境で発生した様々な障害の原因を突き止めるためにご記入いただくものです。ご提供いただく情報が不十分な場合には、障害の原因を突き止めることに時間がかかり、最悪の場合には障害の解消ができない場合もあります。迅速に障害の解消を行うためにも、担当者が障害の発生した環境を理解できるよう、以下の点にそってご記入ください。記入用紙で書き切れない場合には、プリントアウトなどを別途添付ください。なお、都合によりご連絡の遅れることもございますので予めご了承ください。

## ソフトウェアとハードウェア

1 AT-VPN Client のバージョンとシリアル番号をご記入ください。バージョンは、タスクトレイの「AT-VPN Client」アイコンを右クリックし、「バージョン情報」を選択することで確認できます。シリアル番号は「CentreNET AT-VPN Client」ライセンス同梱の「シリアル番号 / 認証キー」シールに印字（10、25、50 ユーザーライセンスの場合）（図 3.2.5）、または、同梱フロッピーディスク内の XXXXuser.csv ファイル（XXXX はユーザー数）に記載（100 ユーザー以上のライセンスの場合）（図 3.2.6）されています。

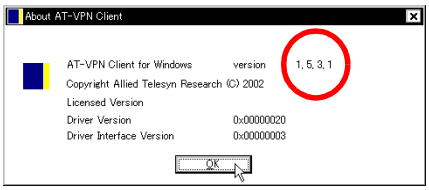


**図 A.0.1 バージョン情報**

2 AT-VPN Client を実行している Windows の種類、バージョンについてご記入ください。情報は、「コントロールパネル」→「システム」→「情報」で表示されます。

3 AT-VPN Client がインストールされているコンピューターについてご記入ください。

4 AT-VPN Client と VPN 通信をする AR ルーターの機種、シリアル番号、Rev. をご記入ください。

5 AR ルーターのファームウェアバージョンについてご記入ください。

## お問い合わせ内容について

1 どのような症状が発生するのか、それはどのような状況で発生するのかをできる限り具体的に（再現できるように）記入してください。

2 もし可能であれば、AT-VPN Client のセキュリティーポリシーファイル（.spl）、AR ルーターの設定ファイル（.cfg）のハードコピーをお送りください。その際、**認証に使用される文字列など、第三者に知られてはいけない情報はマーカーで塗りつぶすなどの措置をとってください。**

3 障害などが発生する場合には、併用しているユーティリティ、アプリケーションの処理内容も記入してください。

4 エラーメッセージやエラーコードが表示される場合には、表示されるメッセージの内容のプリントアウトなどを必ず添付してください。

## ネットワーク構成について

運用形態がわかるようにネットワーク構成図を記入してください。

# 調査依頼書（CentreNET AT-VPN Client 1/2）　年　月　日

## 一般事項

**1.** 御社名：

部署名：　　ご担当：

ご連絡先住所：〒

TEL：　　(　　)　　FAX：　　(　　)

**2** ご購入先：　　ご購入年月日：

ご購入先担当者：　　ご連絡先 (TEL)：　　(　　)

## ハードウェアとソフトウェア

**1.** AT-VPN Client

バージョン：＿＿＿＿(＿＿＿＿)　シリアル番号：＿＿＿＿＿－＿＿＿＿＿－＿＿＿＿＿

**2** AT-VPN Client を実行しているコンピューターのオペレーティングシステム
☐ Windows 98　☐ Windows 98 Second Edition　☐ Windows Me (Millenium Edition)
☐ Windows 2000 Professional　(Service Pack ＿＿＿＿＿ )

**3** AT-VPN Client がインストールされているコンピューターの機種とメーカー名：

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

コンピューターに実装されているメモリー：＿＿＿＿＿MB
コンピューターのハードディスク容量：＿＿＿＿＿ MB
LAN アダプター機種とメーカー名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

**4** AR ルーター
機種名：CentreCOM AR＿＿＿＿＿＿＿＿


**5** AR ルーターのファームウェア（ソフトウェア）のバージョン
Rev（本体）：＿＿＿＿＿＿＿＿＿＿＿＿
Rev（暗号ボード、暗号・圧縮ボード）：＿＿＿＿＿＿＿＿＿＿＿＿
SoftwareVersion：＿＿＿＿＿＿＿＿＿＿＿＿
ReleaseVersion：＿＿＿＿＿＿＿＿＿＿＿＿
Patch file name：　☐なし　　☐あり（＿＿＿＿＿＿＿＿＿＿＿＿）

# 調査依頼書（CentreNET AT-VPN Client 2/2）　年　月　日

## お問い合わせ内容

□別紙あり　□別紙なし

□設置中に起こっている障害　□設置後、運用中に起こっている障害（どのくらい後：＿＿＿＿＿＿＿＿＿＿）

## ネットワーク構成図

□別紙あり　□別紙なし

簡単なもので結構ですからご記入をお願いします。

# ご注意

- 本マニュアルは、アライドテレシス株式会社が作成したもので、全ての権利をアライドテレシス株式会社が保有しています。アライドテレシス株式会社に無断で本書の一部または全部をコピーすることを禁じます。
- アライドテレシス株式会社は、予告なく本マニュアルの一部または全体を修正、変更することがありますのでご了承ください。
- アライドテレシス株式会社は、改良のため製品の仕様を予告なく変更、改良することがありますのでご了承ください。
- 本製品の内容またはその仕様に関して発生した結果についてはいかなる責任も負いかねますのでご了承ください。



# マニュアルバージョン

| | | |
|---|---|---|
| 2000 年 12 月 | Rev.A | Ver.1.1 |
| 2001 年 12 月 | Rev.B | Internal use only |
| 2002 年 4 月 | Rev.C | Ver.1.4 |
| 2002 年 11 月 | Rev.D | Ver.1.5 |
| 2003 年 6 月 | Rev.E | Ver.1.5（追記） |

# 商標について

CentreCOM、CentreNET はアライドテレシス株式会社の登録商標です。Windows、WindowsNT は米国 Microsoft Corporation の米国およびその他の国における登録商標です。その他、この文書に掲載されているソフトウェアおよび周辺機器の名称は各メーカーの商標または登録商標です。