

# NetAttest EPS 設定例

連携機器：

AR-Router シリーズ

Case：ワンタイムパスワードでの認証

---

Version 1.0

株式会社ソリトンシステムズ

NetAttest®は、株式会社ソリトンシステムズの登録商標です。

その他、本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。

本文中に ™、®、©は明記していません。

Copyright © 2012, Soliton Systems K.K. , All rights reserved.

# はじめに

## 本書について

本書は CA 内蔵 RADIUS サーバーアプライアンス NetAttest EPS とアライドテレシス社製 AR560S との VPN によるワンタイムパスワード認証連携について、設定例を示したものです。

各機器の管理 IP アドレス設定など、基本設定は既に完了しているものとします。設定例は管理者アカウントでログインし、設定可能な状態になっていることを前提として記述します。

## 表記方法



表記方法	説明
ABCDabcd1234 (normal)	コマンド名、ファイル名、ディレクトリ名、画面上のコンピューター出力、コード例を示します。
<b>ABCDabcd1234</b> (bold)	ユーザーが入力する文字を、画面上のコンピューター出力と区別して示します。
<i>ABCDabcd1234</i> (italic)	変数を示します。実際に使用する特定の名前または値で置き換えます。

表記方法	説明
『 』	参照するドキュメントを示します。
「 」	参照する章、節、ボタンやメニュー名、強調する単語を示します。
[キー]	キーボード上のキーを表します。
[キー1]+[キー2]	[キー1]を押しながら[キー2]を押すことを表します。

## 表記方法(コマンドライン)

表記方法	説明
%, \$, >	一般ユーザーのプロンプトを表します。
#	特権ユーザーのプロンプトを表します。
[filename]	[ ] は省略可能な項目を示します。この例では、filename は省略してもよいことを示しています。

## アイコンについて

アイコン	説明
	利用の参考となる補足的な情報をまとめています。
	注意事項を説明しています。場合によっては、データの消失、機器の破損の可能性がります。

## 画面表示例について

このマニュアルで使用している画面(画面キャプチャ)やコマンド実行結果は、実機での表示と若干の違いがある場合があります。

## ご注意

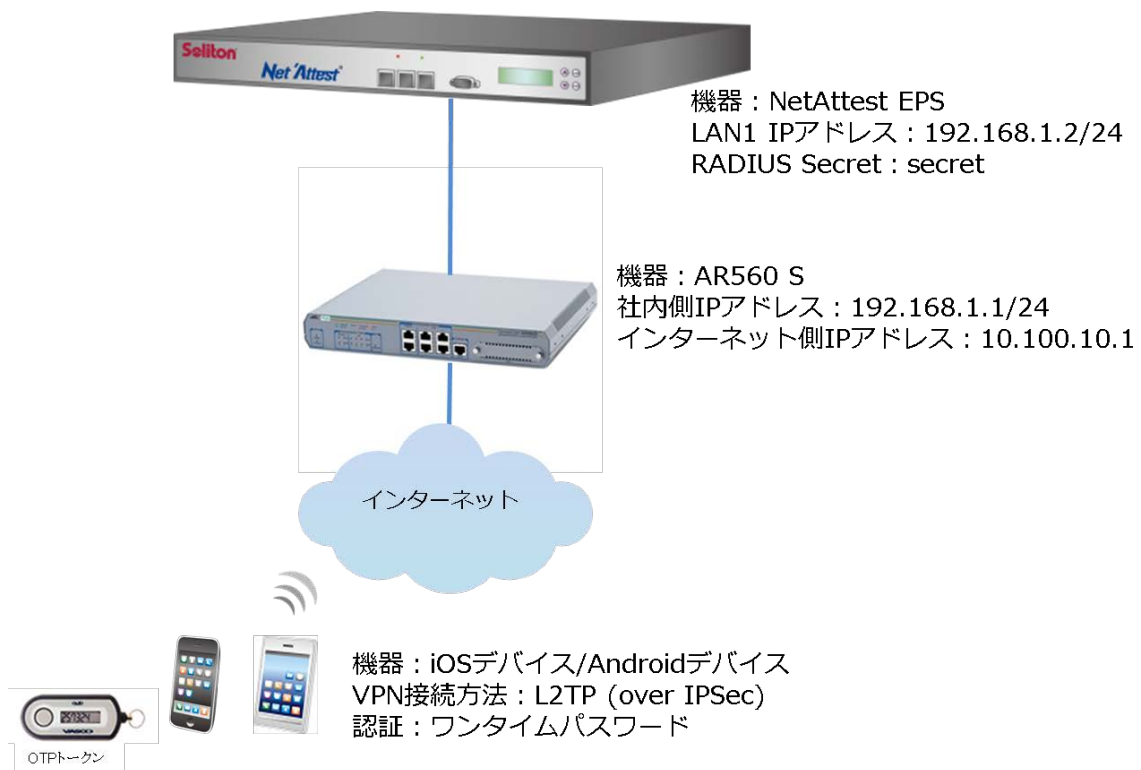
本書は、当社での検証に基づき、NetAttest EPS 及び AR560S の操作方法を記載したものです。すべての環境での動作を保証するものではありません。

# 目次

1 構成 .....	6
1-1 構成.....	6
1-2 環境.....	7
2 NetAttest EPS の設定.....	8
2-1 システム初期設定ウィザードの実行.....	9
2-2 サービス初期設定ウィザードの実行.....	10
2-3 認証ユーザーの登録 .....	11
2-4 ワンタイムパスワード設定.....	11
3 AR560S の設定.....	14
3-1 IP アドレスおよび Security Officer レベルユーザの作成 .....	15
3-2 PPP インターフェース及びスタティックルートの設定 .....	16
3-3 RADIUS サーバー及び IP アドレスプールの設定 .....	17
3-4 L2TP プロトコル並びに PPP TEMPLATE の設定.....	18
3-5 DNS リレーの設定.....	19
3-6 DHCP Server の設定.....	20
3-7 Firewall の設定.....	21
3-8 ISAKMP の設定.....	24
3-9 IPsec の設定 .....	25
4 スマートデバイスの設定.....	28
4-1 iOS 設定例.....	28
4-2 Android の設定例 .....	31
5 付録.....	34

# 1 構成

## 1-1 構成



## 1-2 環境

### 1-2-1 機器

役割	メーカー	製品名	SW バージョン
Authentication Server (認証サーバー)	Soliton Systems	NetAttest EPS-ST04	Ver. 4.4.0
RADIUS クライアント (VPN ルーター)	Allied-telesis	AR560S	2.9.2-07
Client	Apple/samsung	iPhone 3GS/Galaxy Tab	iOS 4.2/Android 2.2
ワンタイムパスワードトークン	VASCO	Digipass GO6	

### 1-2-2 認証方式

- ・ ID・パスワード(ワンタイムパスワード)

### 1-2-3 ネットワーク設定

	EPS-ST04	AR560S	Client PC	Client Tablet
IP アドレス	192.168.1.2/24	10.100.10.1/24	IPCP (AR560S から)	IPCP (AR560S から)
RADIUS port (Authentication)	UDP 1812		-	-
RADIUS port (Accounting)	UDP 1813		-	-
RADIUS Secret (Key)	secret		-	-

## 2 NetAttest EPS の設定

### NetAttest EPS の設定手順

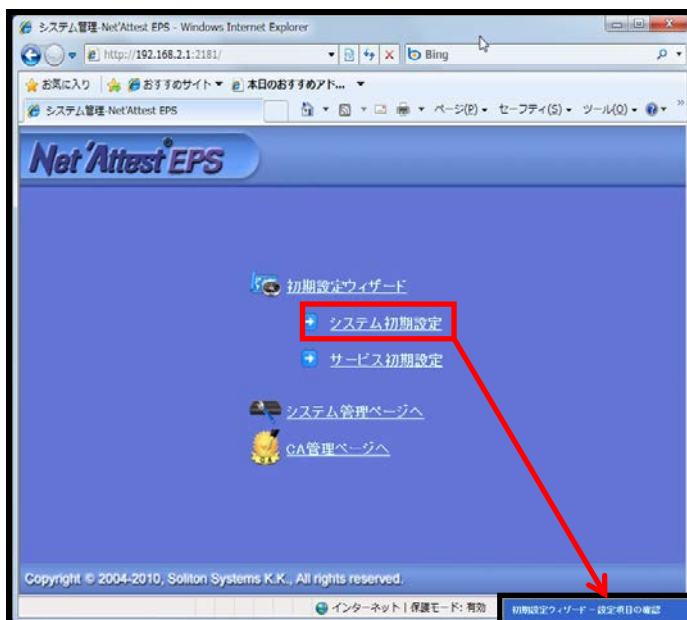
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. 認証ユーザーの追加登録
4. ワンタイムパスワード設定



## 2-1 システム初期設定ウィザードの実行

システム初期設定ウィザードを使用し、以下の項目を設定します。

- ◆ タイムゾーンと日付・時刻の設定
- ◆ ホスト名の設定
- ◆ サービスインターフェースの設定
- ◆ 管理インターフェースの設定
- ◆ メインネームサーバーの設定



### 【ホスト名】

・ naeps.local

### 【IP アドレス】

・ デフォルト

### 【ライセンス】

・ なし

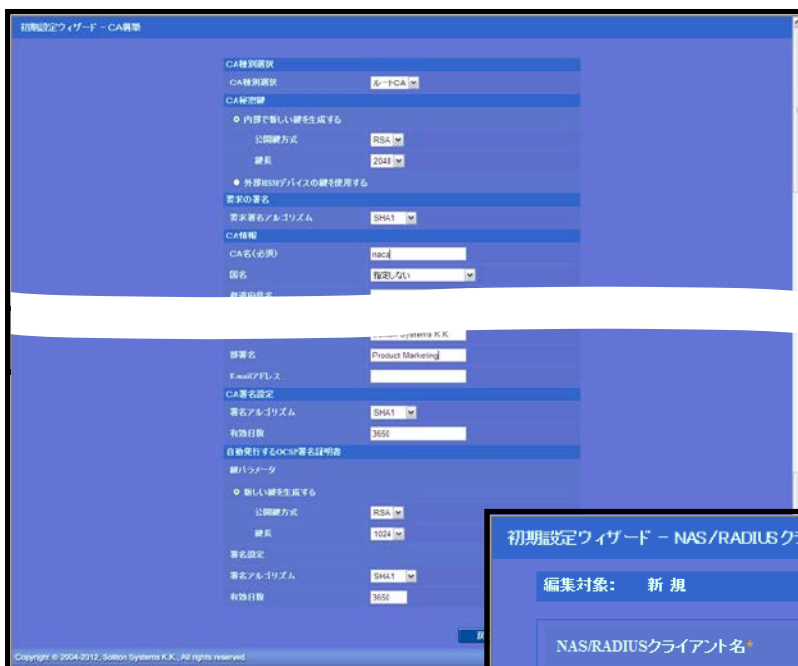


## 2-2 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

値を記載しているもの以外はすべてデフォルト設定で行いました。

- ◆ CA 構築
- ◆ LDAP データベースの設定
- ◆ RADIUS サーバーの基本設定（全般）
- ◆ RADIUS サーバーの基本設定（証明書検証）
- ◆ NAS/RADIUS クライアント設定



【CA 名】

・ naca

【NAS/RADIUS クライアント名】

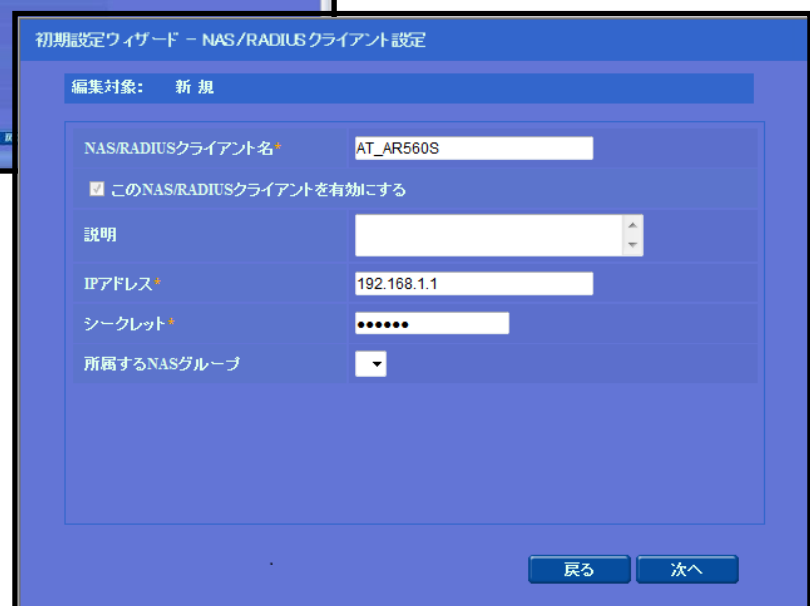
・ AT\_AR560S

【IP アドレス(Authenticator)】

・ 192.168.1.1

【シークレット】

・ secret



## 2-3 認証ユーザーの登録

NetAttest EPS 管理画面より、ユーザー登録を行います。

「ユーザー」→「ユーザー一覧」から、『追加』ボタンでユーザー登録を行います。



【姓】

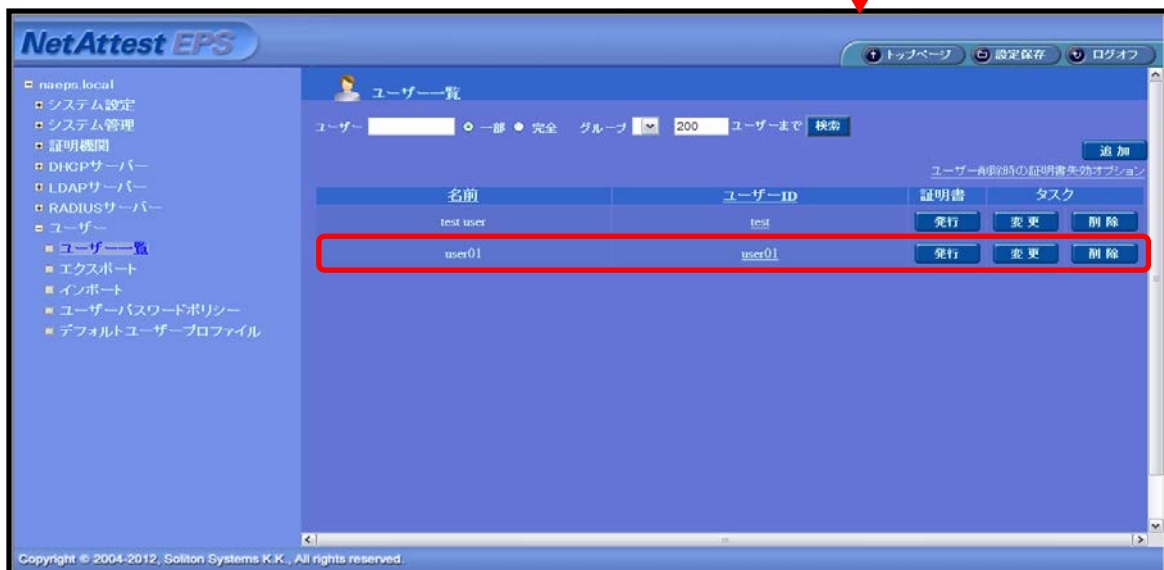
・ user01

【ユーザーID】

・ user01

【パスワード】

・ password





ユーザーとワンタイムパスワードトークンを紐付けます。

ユーザーの「変更」ボタンをクリックしてください。「標準属性」タブの「チェックアイテム」→「認証タイプ」から「VASCO」を選択してください。

「OTP」タブに進み、トークンのシリアル No を入力し、「OK」ボタンをクリックしてください。なお、認証タイプが「自動認証」では「ワンタイムパスワード」で認証できません。

The first screenshot shows the 'ユーザー一覧' (User List) interface. The left sidebar has 'ユーザー一覧' selected. The main area shows a table with columns '名前' (Name), 'ユーザーID' (User ID), '証明書' (Certificate), and 'タスク' (Tasks). The first row is 'test user' with ID 'test'. The '変更' (Change) button in the 'タスク' column is highlighted with a red box. A red arrow points from this button to the second screenshot.

The second screenshot shows the 'ユーザー設定' (User Settings) interface for 'user01'. The '標準属性' (Standard Properties) tab is selected. Under 'チェックアイテム' (Check Items), the '認証タイプ' (Authentication Type) dropdown is set to 'VASCO'. A red box highlights the dropdown. A red arrow points from this dropdown to the third screenshot.

The third screenshot shows the 'ユーザー設定' (User Settings) interface for 'user01'. The 'OTP' tab is selected. Under 'VASCO DIGIPASS', the 'トークンシリアルNo' (Token Serial No) field contains '0091234582'. A red box highlights the input field. A red box also highlights the 'OK' button at the bottom of the form.

## 3 AR560S の設定

### AR560S の設定手順

1. IP アドレスおよび Security Officer レベルユーザの作成
2. PPP インターフェースおよびスタティックルートの設定
3. RADIUS サーバーおよび IP アドレスプールの設定
4. L2TP プロトコルならびに PPP TEMPLATE の設定
5. DNS リレーの設定
6. DHCP Server の設定
7. Firewall の設定
8. ISAKMP の設定
9. IPsec の設定



設定はすべて CLI から行います。ID/パスワードは以下の通りです。

ID : manager

パスワード:friend

なお、各設定画面のパラメーター詳細についてはユーザーマニュアルや設定例をご参照  
下さい

<http://www.allied-telesis.co.jp/support/list/router/ar560s/docs/index.html>

<http://www.allied-telesis.co.jp/support/list/router/ar560s/docs/cfg-197.html>

---

## 3-1 IP アドレスおよび Security Officer レベルユーザの作成

---

1. IP モジュールを有効にします。

```
ENABLE IP
```

2. ルーターへログイン後、LAN 側のインターフェースへ IP アドレスを設定します

```
ADD IP INT=VLAN1 IP=192.168.1.1 MASK=255.255.255.0
```

3. セキュリティモードで各種設定を行うことのできる Security Officer レベルのユーザー「secoff」を作成します。パスワードは「secoff」とします。※セキュリティモードを使用しないと IPsec 機能で用いる鍵情報がルーターの再起動時に消去されます。

```
ADD USER=secoff PASSWORD=secoff PRIVILEGE=SECURITYOFFICER ↓
```

## 3-2 PPP インターフェース及びスタティックルートの設定

1. WAN 側 Ethernet インターフェース (eth0) 上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、ISP から通知された PPPoE の「サービス名」を記述します。ISP から指定がない場合は、どのサービス名タグでも受け入れられるよう、「ANY」を設定します。

```
CREATE PPP=0 OVER=eth0-ANY
```

2. ISP から通知された PPP ユーザー名とパスワードを指定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

```
SET PPP=0 OVER=eth0-ANY USER=user@isp PASSWORD=isppasswd LQR=OFF BAP=OFF ECHO=ON
```

3. WAN 側 (ppp0) インターフェースに IP アドレス「10.100.10.1」を設定します。

```
ADD IP INT=ppp0 IP=10.100.10.1 MASK=255.255.255.255
```

4. デフォルトルートを設定します。

```
ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
```



---

### 3-3 RADIUS サーバー及び IP アドレスプールの設定

---

1. RADIUS サーバーを登録します。

```
ADD RADIUS SERVER=192.168.1.2 SECRET="PASSWORD" PORT=1812
```

2. IP アドレスプール「VPNC」を作成し、接続してきた VPN クライアントに割り当てるアドレスの範囲を指定します。ここでは 100 台分のモバイル端末のアドレスプールを用意しています。

```
CREATE IP POOL=VPNC IP=192.168.2.1-192.168.2.100
```

### 3-4 L2TP プロトコル並びに PPP TEMPLATE の設定

1. L2TP 経由で VPN クライアントが PPP 接続してきたときに動的に作成する PPP インターフェースのテンプレート「1」を作成します。接続時の認証には PAP を使い、CHAP の再認証は OFF にし、VJ 圧縮を有効にします。また、アドレス割り当てには IP アドレスプール「VPNC」を使うようにします。

```
CREATE PPP TEMPLATE=1 IPPOOL=VPNC AUTHENTICATION=PAP BAP=OFF ECHO=30  
RECHALLENGE=OFF VJC=ON
```

2. L2TP モジュールを有効にします。

```
ENABLE L2TP
```

3. L2TP サーバーを BOTH モードで起動します。

```
ENABLE L2TP SERVER=BOTH
```

4. L2TP 経由で VPN クライアントが接続してきたときに使用する PPP テンプレートを指定します。ここではクライアントのアドレスが不定なので、どのアドレスからでも接続を受け入れるように設定します。

```
ADD L2TP IP=0.0.0.0-255.255.255.255 PPPTEMPLATE=1
```

---

## 3-5 DNS リレーの設定

---

1. DNS リレー機能を有効にします。

```
ENABLE IP DNSRELAY
```

2. 接続確立まで ISP の DNS サーバーアドレスが不明なため、DNS リクエストの転送先として、IPCP ネゴシエーションを行うインターフェース名「ppp0」を指定します。

```
SET IP DNSRELAY INT=ppp0
```

## 3-6 DHCP Server の設定

1. DHCP サーバー機能を有効にします。

```
ENABLE DHCP
```

2. DHCP ポリシー「DHCP」を作成します。IP アドレスの使用期限は 3,600 秒（1 時間）とします。

```
CREATE DHCP POLI="DHCP" LEASE=3600
```

3. クライアントに提供する情報を設定します。ここでは、DNS サーバーアドレスとして、ルーターの LAN 側インターフェースの IP アドレスを指定しています。ここへ送られた DNS リクエストは、DNS リレー機能により ISP の DNS サーバーに転送されます。

```
ADD DHCP POLICY="DHCP" SUBNET=255.255.255.0 ROUTER=192.168.1.1 DNSSERVER=192.168.1.1
```

4. クライアントに提供する IP アドレスの範囲を設定します。ここでは、192.168.1.128～192.168.1.144 の 16 個を指定しています。

```
CREATE DHCP RAN="CLIENT" POLI="DHCP" IP=192.168.1.128 NUM=16
```

## 3-7 Firewall の設定

1. ファイアウォール機能を有効にします。

```
ENABLE FIREWALL
```

2. ファイアウォールの動作を規定するファイアウォールポリシーを作成します。

```
CREATE FIREWALL POLICY=net
```

3. ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。デフォルト設定では、ICMP はファイアウォールを通過できません。

```
ENABLE FIREWALL POLICY=net ICMP_F=UNRE,PING
```

4. ルーターの ident プロキシ機能を無効にし、外部のメール (SMTP) サーバーなどからの ident 要求に対して、ただちに TCP RST を返すよう設定します。

```
DISABLE FIREWALL POLICY=net IDENTPROXY
```

5. VPN クライアントが L2TP 経由で接続してきたときに動的に作成される PPP インターフェイス用のファイアウォール設定を行います。最初に、ダイナミックインターフェイステンプレート「vpnif」を作成します。名前は自由です。

```
CREATE FIREWALL POLICY=net DYNAMIC=vpnif
```

6. 次に、ダイナミックインターフェーステンプレート「vpnif」の対象ユーザーを指定します。USER パラメーターで指定したユーザーが接続してきたときに動的作成される PPP インターフェースは、ADD FIREWALL POLICY INTERFACE コマンドで「DYN-templatename」として参照できます（templatename はテンプレート名）。ここでは対象ユーザーとして「ANY」を指定しています。これは、PPP の認証をパスしたすべてのユーザーが対象であることを示します。

```
ADD FIREWALL POLICY=net DYNAMIC=vpnif USER=ANY
```

7. ファイアウォールポリシーの適用対象となるインターフェースを指定します。LAN 側インターフェース（vlan1）を PRIVATE（内部）に設定します。

```
ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
```

- WAN 側インターフェース（ppp0）を PUBLIC（外部）に設定します。

```
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
```

- L2TP 経由でユーザーが接続してきたときに動的作成される PPP インターフェース（vpnif）を PRIVATE（内部）に設定します。

```
ADD FIREWALL POLICY=net INT=DYN-vpnif TYPE=PRIVATE
```

8. LAN 側ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるように設定します。グローバルアドレスには、ppp0 の IP アドレスを使用します。

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
```

9. VPN クライアントが ENAT 機能を使用できるように設定します。グローバルアドレスには、IP アドレスを使用します。

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=DYN-vpnif GBLINT=ppp0
```

10. VPN クライアントから受信した IKE パケット (UDP500 番) と NAT-T パケット (UDP4500 番) がファイアウォールを通過できるように設定します。

```
ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0 PROT=UDP GBLPORT=500  
GBLIP=10.100.10.1
```

```
ADD FIREWALL POLICY=net RULE=2 AC=ALLOW INT=ppp0 PROT=UDP GBLPORT=4500  
GBLIP=10.100.10.1
```

11. 基本ルールのままでは IPsec パケットまで遮断されてしまうので、これらのパケットを通過させるためのルールを設定します。「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケットを取り出したあとでこのルールを適用することを示します。よって、以下のコマンドは、「取り出したパケットが UDP で終点ポートが 1701 番 (L2TP パケット) ならば許可する」の意味になります。

```
ADD FIREWALL POLICY=net RULE=3 AC=ALLOW INT=ppp0 PROT=UDP GBLPORT=1701  
GBLIP=10.100.10.1 PORT=1701 IP=10.100.10.1 ENCAP=IPSEC ↓
```

## 3-8 ISAKMP の設定

1. ISAKMP 用の事前共有鍵 (pre-shared key) を作成します。ここでは鍵番号を「1」番とし、鍵の値は「secret」という文字列で指定します (VPN クライアントにも同じ値を設定)。

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



**CREATE ENCO KEY** コマンドは、コンソール上でログインしている場合のみ有効なコマンドです。そのため、EDIT コマンド (内蔵スクリーンエディター) などで設定スクリプトファイル (.CFG) にこのコマンドを記述しても無効になりますのでご注意ください

2. VPN クライアントからの IKE ネゴシエーション要求を受け入れる ISAKMP ポリシー「i」を作成します。

ISAKMP メッセージの暗号化には「3DES」、認証には「SHA」アルゴリズム、Oakley グループは「2」を使用し、VPN クライアントとの認証には前の手順で作成した事前共有鍵 (鍵番号「1」) を使います。さらに、クライアントの IP アドレスが不定なため PEER に ANY を指定し、NAT-Traversal を有効にしています。

```
CREATE ISAKMP POLICY="i" PEER=ANY KEY=1 SENDN=TRUE NATTRAVERSAL=TRUE
```

```
SET ISAKMP POLICY="i" ENCALG=3DESOUTER HASHALG=SHA GROUP=2
```

3. ISAKMP SA の有効期限を 600 秒 (10 分) に設定し Responder Rekey Extension 機能を有効にします。

```
SET ISAKMP POLICY="i" EXPIRYSECOND=600 REKEY=true
```



## 3-9 IPsec の設定

1. IPsec 通信の仕様を定義する SA スペック「1」を作成します。鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「AES256bit」、認証方式「SHA」に設定します。この例では L2TP によってトンネリングを行うため、デフォルトのトンネルモードは使用せずに、トランスポートモードを使用します。UDP1701 番ポートを使って送受信される L2TP パケットだけを暗号化する形になります。

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=AES256 HASHALG=SHA  
MODE=TRANSPORT
```

2. 同様に IPsec 通信の仕様を定義する SA スペック「2」を作成します。鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「AES128bit」、認証方式「SHA」に設定します。

```
CREATE IPSEC SASPEC=2 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=AES128 HASHALG=SHA  
MODE=TRANSPORT
```

3. 同様に IPsec 通信の仕様を定義する SA スペック「3」を作成します。鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「3DES」、認証方式「SHA」に設定します。

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=AES256 HASHALG=SHA  
MODE=TRANSPORT ↓
```

4. SA スペック「1」、「2」、「3」からなる SA バンドルスペック「1」を作成します。鍵管理方式は「ISAKMP」を指定します。

```
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1 or 2 or 3"
```

5. IKE パケット (UDP500 番) と NAT-T パケット (UDP4500 番) を素通しさせる IPsec ポリシー「isa」「nat」を作成します。

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

```
CREATE IPSEC POLICY=nat INT=ppp0 ACTION=PERMIT LPORT=4500 TRANSPORT=UDP
```



**NAT-Traversal** を使用する場合は、必ず IKE と NAT-T のパケットが通過できるような設定を行ってください。

「IPsec ポリシー」は設定順に検索され、最初にマッチしたものが適用されるため、設定順序には注意が必要です。検索順は **SHOW IPSEC POLICY** コマンドで確認できます。また、検索順を変更するには、**SET IPSEC POLICY** コマンドの **POSITION** パラメーターを使用します。

6. L2TP パケットを暗号化する IPsec ポリシー「L2」を PPP インターフェース「0」に対して作成します。鍵管理方式には「ISAKMP」を指定します。VPN クライアントの IP アドレスが不定なため、PEER には ISAKMP の認証をパスした相手という意味の「DYNAMIC」を、BUNDLE には前の手順で作成した SA バンドルスペース「1」を指定します。また、LPORT と TRANSPORT で対象となるパケットの条件（ここでは L2TP パケット）を指定します。

```
CREATE IPSEC POLICY=L2 INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1  
PEER=DYNAMIC
```

```
SET IPSEC POLICY=L2 LPORT=1701 TRANSPORT=UDP
```

7. インターネットへの平文通信を許可する IPsec ポリシー「inet」を PPP インターフェース「0」に対して作成します。

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



インターネットにもアクセスしたい場合は、必ず最後の IPsec ポリシーですべてのパケットを通過させる設定を行ってください。いずれの IPsec ポリシーにもマッチしなかったトラフィックはデフォルトで破棄されてしまうため、上記の設定がないと VPN 以外の通信ができなくなります。

8. IPsec モジュールを有効にします。

```
ENABLE IPSEC
```

9. ISAKMP モジュールを有効にします。

```
ENABLE ISAKMP
```

10. Security Officer レベルのユーザーでログインしなおします。

```
LOGIN secoff
```

11. 動作モードをセキュリティモードに切り替えます。

```
ENABLE SYSTEM SECURITY_MODE ↓
```



**セキュリティモードでは、Security Officer レベルでの Telnet ログインが原則として禁止されています。セキュリティモードにおいて、Security Officer レベルで Telnet ログインしたい場合は、あらかじめ RSO (Remote Security Officer) の設定を行っておいてください。**

12. 設定は以上です。設定内容をファイルに保存し、SET CONFIG コマンドで起動時設定ファイルに指定します。

```
CREATE CONFIG=router.cfg ↓
```

```
SET CONFIG=router.cfg ↓
```

## 4 スマートデバイスの設定

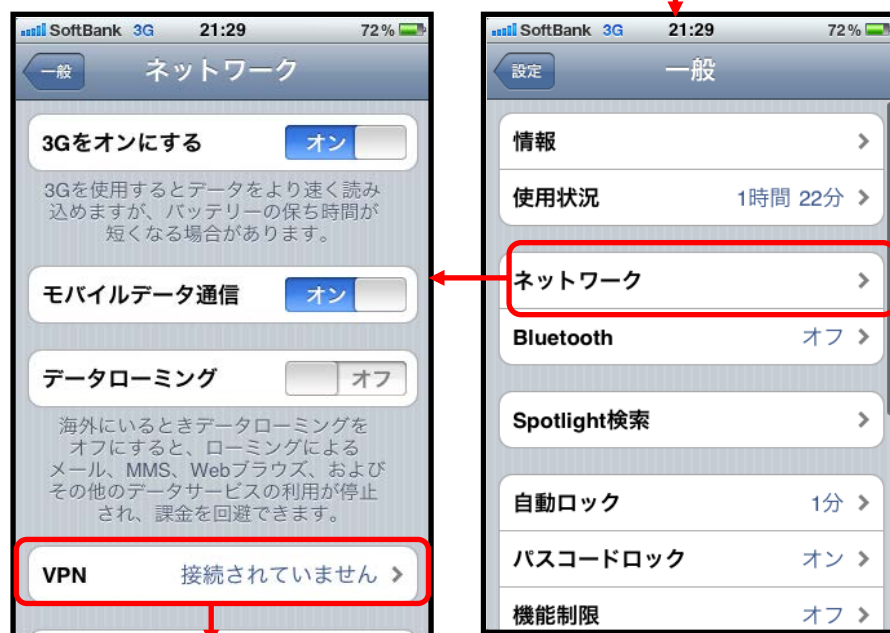
### 4-1 iOS 設定例

iOS 側の設定を行います。

ホーム画面より「設定」アイコンをタップし、「一般」をタップします。



「ネットワーク」→「VPN」と進んでください。



「VPN 構成を追加」をタップします。



「L2TP」をタップし、下記のように設定してください。



【説明】

・ AR\_VPN(任意の名称)

【サーバー】

・ 10.100.10.1

【アカウント】

・ (NetAttest EPS に設定したもの)

【RSA SecureID】

・ オフ

【パスワード】

・ 毎回確認(認証時には OTP トークンに表示されるパスワードを入力)

【シークレット】

・ secret

【すべての信号を送信】

・ オン

「プロキシ」の「オフ」をタップし、「保存」をタップしてください。  
その後、「AR-VPN」を選択し、VPN をオンにします。



画面上段右上に VPN アイコンが表示され、「状況」に接続中と表示されれば接続に成功です。



## 4-2 Android の設定例

Android 側の設定を行います。

ホーム画面で「メニュー」ボタンを押し、「設定」をタップします。



設定メニューの「無線とネットワーク」 - 「モバイルネットワーク」と進み、「VPN 設定」をタップします。



「VPN の追加」 → 「L2TP/IPsec PSK VPN を追加」と進みます。



各項目を下記のように設定します。



【説明】

・ AR\_VPN(任意の名称)

【VPN サーバー】

・ 10.100.10.1

【IPsec 事前共通鍵の設定】

・ secret

【L2TP セキュリティ保護を有効にします】

・ 無効

【DNS 検索ドメイン】

・ (未設定)



登録した「AR-VPN」をタップします。



ユーザーID とパスワードを入力する画面が出ますので、EPS に登録したユーザーID と VASCO の OTP トークンに表示されるパスワードを入力し、「接続」をタップしてください。



**PIN コードありの OTP トークンの場合は PIN コード+OTP トークンのパスワードを入力してください。**



画面左上の鍵アイコンの表示、「AR-VPN」の下の「接続されています」の表示の2点を確認できれば接続成功です。



## 5 付録

### ・アライドテレシス社製スイッチ AR560S config

ENABLE IP ↓

ADD IP INT=VLAN1 IP=192.168.1.1 MASK=255.255.255.0 ↓

ADD USER=secoff PASSWORD=secoff PRIVILEGE=SECURITYOFFICER ↓

CREATE PPP=0 OVER=eth0-ANY ↓

SET PPP=0 OVER=eth0-ANY USER=user@isp PASSWORD=isppasswd LQR=OFF BAP=OFF ECHO=ON ↓

ADD IP INT=ppp0 IP=10.100.10.1 MASK=255.255.255.255 ↓

ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0 ↓

ADD RADIUS SERVER=192.168.1.2 SECRET="PASSWORD" PORT=1812 ↓

CREATE IP POOL=VPNC IP=192.168.2.1-192.168.2.100 ↓

CREATE PPP TEMPLATE=1 IPPOOL=VPNC AUTHENTICATION=PAP BAP=OFF ECHO=30

RECHALLENGE=OFF VJC=ON ↓

ENABLE L2TP ↓

ENABLE L2TP SERVER=BOTH ↓

ADD L2TP IP=0.0.0.0-255.255.255.255 PPPTEMPLATE=1 ↓

ENABLE IP DNSRELAY ↓

SET IP DNSRELAY INT=ppp0 ↓

ENABLE DHCP ↓

CREATE DHCP POLI="DHCP" LEASE=3600 ↓

ADD DHCP POLICY="DHCP" SUBNET=255.255.255.0 ROUTER=192.168.1.1 DNSSERVER=192.168.1.1 ↓

CREATE DHCP RAN="CLIENT" POLI="DHCP" IP=192.168.1.128 NUM=16 ↓

ENABLE FIREWALL ↓

CREATE FIREWALL POLICY=net ↓

ENABLE FIREWALL POLICY=net ICMP\_F=UNRE,PING ↓

DISABLE FIREWALL POLICY=net IDENTPROXY ↓

CREATE FIREWALL POLICY=net DYNAMIC=vpnif ↓

ADD FIREWALL POLICY=net DYNAMIC=vpnif USER=ANY ↓

ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE ↓

---

```
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC ↓
ADD FIREWALL POLICY=net INT=DYN-vpnif TYPE=PRIVATE ↓

ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0 ↓
ADD FIREWALL POLICY=net NAT=ENHANCED INT=DYN-vpnif GBLINT=ppp0ADD FIREWALL POLICY=net
RULE=1 AC=ALLOW INT=ppp0 PROT=UDP GBLPORT=500 GBLIP=10.100.10.1
PORT=500 IP=10.100.10.1 ↓
ADD FIREWALL POLICY=net RULE=2 AC=ALLOW INT=ppp0 PROT=UDP GBLPORT=4500
GBLIP=10.100.10.1
PORT=4500 IP=10.100.10.1 ↓
ADD FIREWALL POLICY=net RULE=3 AC=ALLOW INT=ppp0 PROT=UDP GBLPORT=1701
GBLIP=10.100.10.1 PORT=1701 IP=10.100.10.1 ENCAP=IPSEC ↓

CREATE ENCO KEY=1 TYPE=GENERAL VALUE="secret" ↓
CREATE ISAKMP POLICY="i" PEER=ANY KEY=1 SENDN=TRUE NATTRAVERSAL=TRUE ↓
SET ISAKMP POLICY="i" ENCALG=3DESOUTER HASHALG=SHA GROUP=2 ↓
SET ISAKMP POLICY="i" EXPIRYSECOND=600 REKEY=true ↓

CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=AES256 HASHALG=SHA
MODE=TRANSPORT ↓
CREATE IPSEC SASPEC=2 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=AES128 HASHALG=SHA
MODE=TRANSPORT ↓
CREATE IPSEC SASPEC=3 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=3DESOUTER HASHALG=SHA
MODE=TRANSPORT ↓
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1 or 2 or 3" ↓

CREATE IPSEC POLICY=isa INT=ppp0 ACTION=PERMIT LPORT=500 TRANSPORT=UDP ↓
CREATE IPSEC POLICY=nat INT=ppp0 ACTION=PERMIT LPORT=4500 TRANSPORT=UDP ↓
CREATE IPSEC POLICY=L2 INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=DYNAMIC ↓
SET IPSEC POLICY=L2 LPORT=1701 TRANSPORT=UDP ↓
CREATE IPSEC POLICY="inet" INT=ppp0 ACTION=PERMIT ↓
ENABLE IPSEC ↓
ENABLE ISAKMP ↓
LOGIN secoff ↓
ENABLE SYSTEM SECURITY_MODE ↓
CREATE CONFIG=router.cfg ↓
SET CONFIG=router.cfg ↓
```

