

# ***NetAttest EPS***

認証連携設定例

【連携機器】 NEC UNIVERGE IX2106

【Case】 ワンタイムパスワードを利用した PAP 認証

Rev1.0

株式会社ソリトンシステムズ

# はじめに



## 本書について

---

本書はオールインワン認証アプライアンス NetAttest EPS と、NEC 社製 VPN 対応高速アクセスルータ UNIVERGE IX シリーズのワンタイムパスワードを利用した PAP 認証での接続について、設定例を示したものです。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。

## 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あります。

## 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 UNIVERGE IX シリーズの操作方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。

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。

# 目次

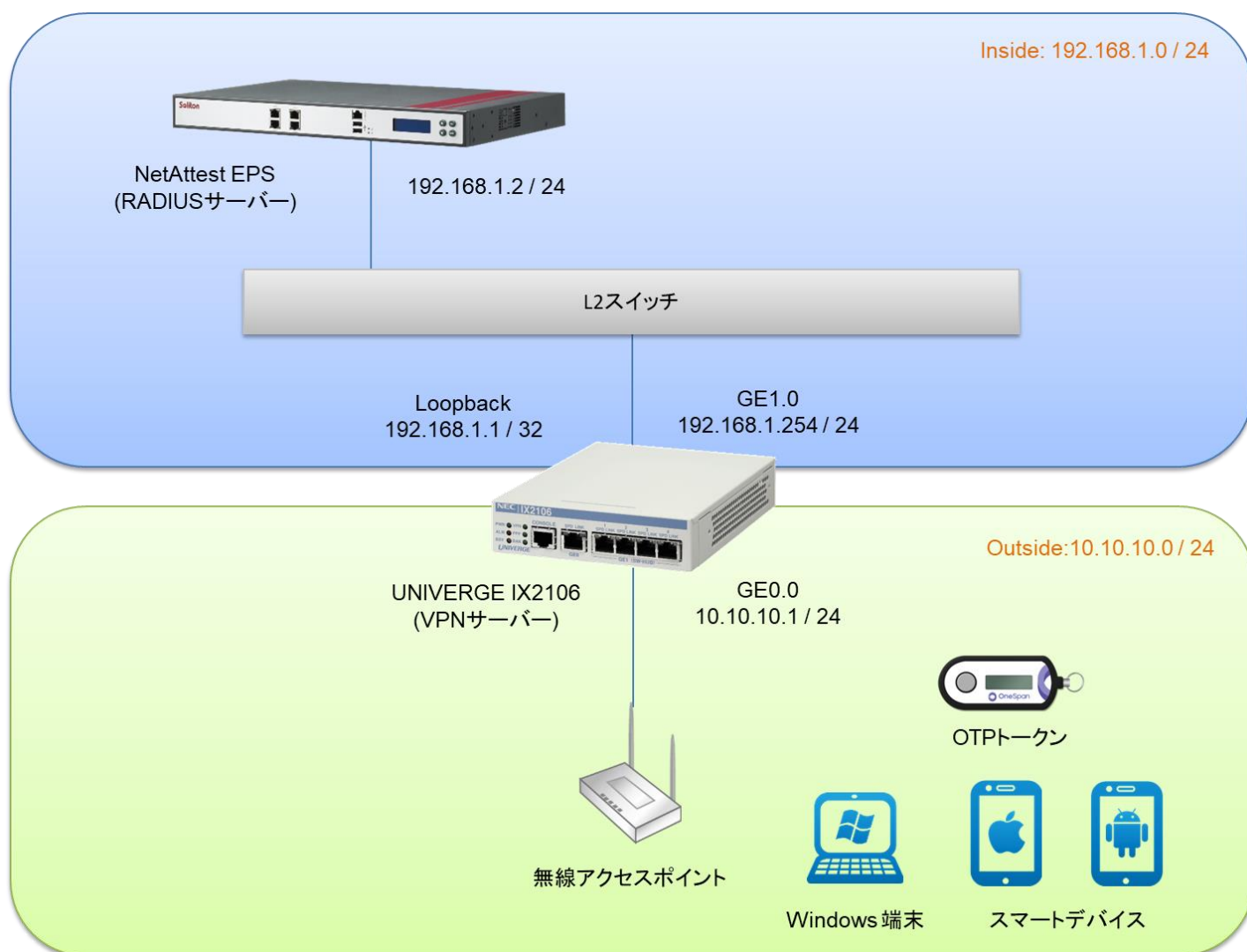
1. 構成	2
1-1 構成図	2
1-2 環境	3
1-2-1 機器	3
1-2-2 認証方式	3
1-2-3 ネットワーク設定	3
2. NetAttest EPS の設定	4
2-1 初期設定ウィザードの実行	4
2-2 システム初期設定ウィザードの実行	5
2-3 サービス初期設定ウィザードの実行	6
2-4 ワンタイムパスワードトークンの登録	7
2-5 ユーザーの登録とワンタイムパスワードトークンの紐付け	8
3. UNIVERGE IX シリーズの設定	10
4. クライアント端末の VPN 設定	12
4-1 Windows 10 の VPN 設定	12
4-1-1 VPN 設定	12
4-1-2 接続方法	14
4-2 iOS での VPN 設定	15
4-2-1 VPN 設定	15
4-2-2 接続方法	16
4-3 Android の VPN 設定	17
4-3-1 VPN 設定	17
4-3-2 接続方法	18
5. 動作確認結果	19
5-1 ワンタイムパスワード認証が成功した場合の EPS のログ表示例	19
5-2 UNIVERGE IX シリーズでのログ確認方法	19
5-2-1 表示コマンドでの確認方法(show interface tunnel0.0 detail)	19
5-2-2 装置ログでの確認方法	20

# 1. 構成

## 1-1 構成図

以下の環境を構成します。

- 無線 LAN へ接続するクライアント端末の IP アドレスは EPS で固定 IP を設定
- RADIUS クライアントの IP アドレスは Loopback の IP アドレスを使用する
- クライアント端末は UNIVERGE IX2106 の Outside に接続し、  
認証に成功すると Inside のネットワークとの通信が可能となる
- ワンタイムパスワードは OneSpan 社製ハードウェアトークンを使用して生成する  
トークンのボタンを押下するとディスプレイにワンタイムパスワードが表示される



## 1-2 環境

## 1-2-1 機器

製品名	メーカー	役割	バージョン
NetAttest EPS-ST05	ソリトンシステムズ	RADIUS サーバー	4.10.6
UNIVERGE IX2106	NEC	VPN サーバー	10.3.10
Surface Laptop	Microsoft	クライアント PC	Windows 10 64bit OS 標準 VPN クライアント
iPad Air 2	Apple	クライアントタブレット	iPad OS 13.5.1 OS 標準 VPN クライアント
Zenfone 6	ASUS	クライアントスマートフォン	Android 10 OS 標準 VPN クライアント
Digipass GO 6	OneSpan	ワンタイムパスワードトークン	-

## 1-2-2 認証方式

ワンタイムパスワードを利用した PAP 認証

## 1-2-3 ネットワーク設定

機器	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS-ST05	192.168.1.2/24	UDP 1812	secret
UNIVERGE IX2106	Inside: 192.168.1.254/24 Outside: 10.10.10.1/24 Loopback: 192.168.1.1/32 # Loopback を RADIUS クライアントの # IP アドレスとして使用		secret
クライアント PC	10.10.10.10	-	-
クライアントタブレット	10.10.10.20	-	-
クライアントスマートフォン	10.10.10.30	-	-

## 2. NetAttest EPS の設定

### 2-1 初期設定ウィザードの実行

---

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「<http://192.168.2.1:2181/>」にアクセスしてください。

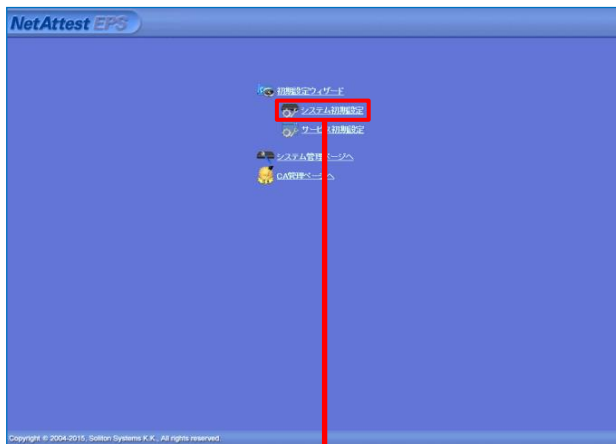
下記のような流れでセットアップを行います。

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. RADIUS クライアントの登録
4. ワンタイムパスワードトークンの登録
5. ユーザーの登録とワンタイムパスワードトークンの紐付け

## 2-2 システム初期設定ウィザードの実行

管理ページにアクセスしたら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イスの設定
- 管理インターフェイスの設定
- ドメインネームサーバーの設定



初期設定ウィザード - 設定項目の確認

設定内容を確認して下さい。  
この設定を保存・反映するには「再起動」ボタンをクリックして下さい。

ネットワーク時刻	
NTPサーバー1	
NTPサーバー2	
NTPサーバー3	
時刻同期する	無効

---

EPSライセンス	
最大ユーザー数	200
最大NAS/RADIUSクライアント数	20
外部サーバー証明書	無効
RADIUSプロキシ	無効
Windowsドメイン認証連携	無効
グループ	無効
MACアドレス認証	無効
ポート制御	無効

Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.

項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし



## 2-3 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。

- 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（EAP）
- 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

項目	値
CA 種別選択	ルート CA
公開鍵方式	RSA
鍵長	2048
CA 名	TestCA

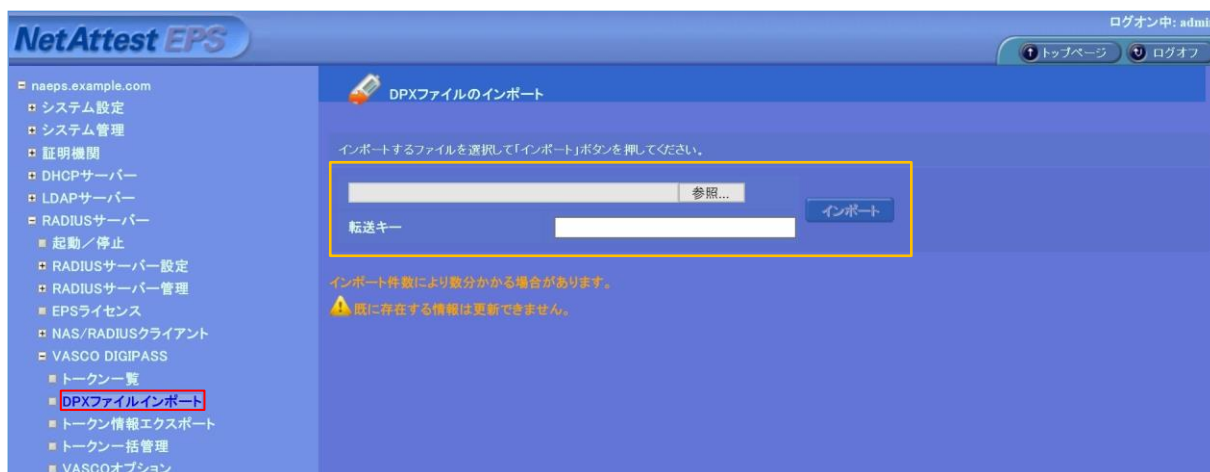
項目	値
NAS/RADIUS クライアント名	RadiusClient01
IP アドレス	192.168.1.1
シークレット	secret

## 2-4 ワンタイムパスワードトークンの登録

NetAttest EPS の管理画面より、ワンタイムパスワードトークンの登録を行います。

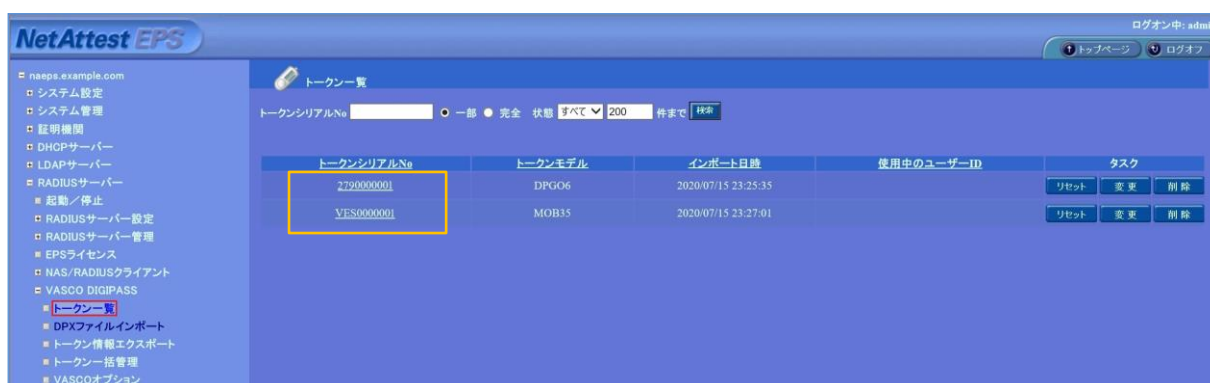
トークンを購入すると、トークンのシリアルナンバーが記載されたファイル(DPX ファイル)と、DPX ファイルをインポートするためのキーコード(転送キー)が提供されます。

[RADIUS サーバー]-[VASCO DIGIPASS]-[DPX ファイルインポート]にて DPX ファイルを指定し、転送キーを入力してインポートを行います。



登録したワンタイムパスワードトークン情報は「トークン一覧」画面にて確認できます。

表示されたトークンシリアル No. を各ユーザーに登録します。



1 行目のトークンモデル「DPGO6」はハードウェアトークン、

2 行目のトークンモデル「MOB35」はソフトウェアトークン(iOS/Android 用アプリ)です。

本資料では 1 行目のトークンシリアル「2790000001」を使用します。

## 2-5 ユーザーの登録とワンタイムパスワードトークンの紐付け

NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

[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。

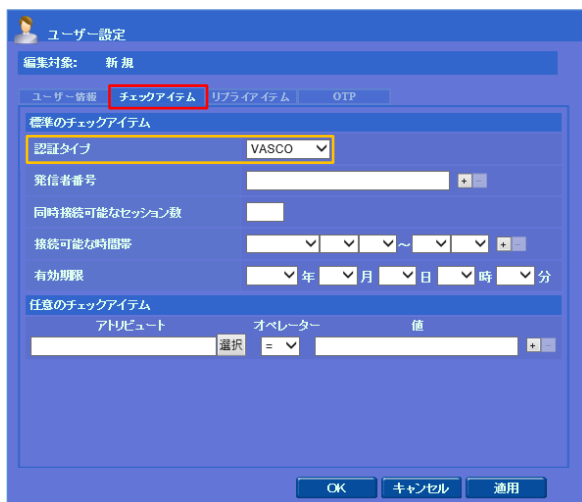


「ユーザー情報」タブにてユーザー情報を入力し、

「チェックアイテム」タブの認証タイプで「VASCO」を選択します。



項目	値
姓	user01
ユーザーID	user01
パスワード	password



項目	値
認証タイプ	VASCO

「リプライアイテム」タブの「任意のリプライアイテム」に右表の値を設定します。

「OTP」タブの「トークンシリアル No」にトークン一覧に表示されたシリアル No を設定します。

アトリビュート	オペレーター	値
Framed-IP-Address	選択 =	192.168.1.10
Framed-Protocol	選択 =	PPP
Service-Type	選択 =	2

項目	値
Framed-IP-Address	192.168.1.10
Framed-Protocol	PPP
Service-Type	2

項目	値
トークンシリアル No	2790000001

以上でユーザーの登録は完了です。

トークン一覧画面の「使用中のユーザーID」に、設定したユーザーIDが表示されていることを確認し、EPS の設定は終了です。

トークンシリアルNo	トークンモデル	インポート日時	使用中のユーザーID	タスク
2790000001	DPG06	2020/07/15 23:25:35	user01	リセット 変更 削除
VES0000001	MOB35	2020/07/15 23:27:01		リセット 変更 削除

## 3. UNIVERGE IX シリーズの設定

CLI を用いて UNIVERGE IX2106 の設定を行います。

本設定例では、IX ルーターに複数のプロポーザル(使用可能な暗号化方式・認証方式の組み合わせ)を設定し、端末が IX ルーターへ通知するプロポーザルで接続可能となることを想定しています。

VPN クライアントを NAT 環境で利用する構成も想定されるため、あらかじめ NAT トラバーサル機能を有効化しています。

IX ルーターでは L2TP(PPP)によるユーザー認証方式として「PAP」「CHAP」のいずれかを設定することができます。EPS を使用してワンタイムパスワード認証を行う場合に使用可能な認証方式は PAP のみのため、本設定例では PAP 認証を指定します。

```

logging subsystem all warn
logging timestamp datetime
logging buffered
!
aaa enable
aaa authentication ppp ppp-auth group radius
aaa authorization network ppp-author group radius
aaa accounting send stop-record authentication-failure
aaa accounting network acc-list1 start-stop local group radius
!
radius host ip 192.168.1.2 key 0 secret source Loopback0.0
!
ip route default 10.10.10.254
!
ip access-list sec-list permit ip src any dest any
!
ike nat-traversal
!
ike proposal ike-prop1 encryption aes-256 hash sha group 1024-bit
ike proposal ike-prop2 encryption aes hash sha group 1024-bit
ike proposal ike-prop3 encryption 3des hash sha group 1024-bit
!
ike policy ike-policy peer any key himitsu ike-prop1,ike-prop2,ike-prop3
!
ipsec autokey-proposal ipsec-prop1 esp-aes-256 esp-sha
ipsec autokey-proposal ipsec-prop2 esp-aes esp-sha
ipsec autokey-proposal ipsec-prop3 esp-3des esp-sha
!
ipsec dynamic-map ipsec-policy sec-list ipsec-prop1,ipsec-prop2,ipsec-prop3
!
ppp profile lns
accounting list acc-list1
authentication list ppp-auth
authentication request pap
authorization list ppp-author
lcp pfc
lcp acfc
ipcp ip-compression
!

```

RADIUS サーバーの指定コマンド IP アドレス「192.168.1.2」、シークレット「secret」を設定

ルーターのデフォルトルートの設定

IX ルーターと VPN クライアントの事前共有キー「himitsu」を設定  
RADIUS 設定のシークレットとは異なるため注意

```
interface GigaEthernet0.0
ip address 10.10.10.1/24
no shutdown
```

WAN インターフェイスの設定

```
interface GigaEthernet1.0
ip address 192.168.1.254/24
ip proxy-arp
no shutdown
```

LAN インターフェイスの設定

```
interface Loopback0.0
ipaddress 192.168.1.1/32
```

Loopback インターフェイスの設定

```
interface Tunnel0.0
ppp binding lns
tunnel mode l2tp-lns ipsec
ip unnumbered Loopback0.0
ip tcp adjust-mssauto
ipsec policy transport ipsec-policy
no shutdown
```

```
interface Tunnel1.0
ppp binding lns
tunnel mode l2tp-lns ipsec
ip unnumbered Loopback0.0
ip tcp adjust-mssauto
ipsec policy transport ipsec-policy
no shutdown
```

```
interface Tunnel2.0
ppp binding lns
tunnel mode l2tp-lns ipsec
ip unnumbered Loopback0.0
ip tcp adjust-mssauto
ipsec policy transport ipsec-policy
no shutdown
```

```
interface Tunnel3.0
ppp binding lns
tunnel mode l2tp-lns ipsec
ip unnumbered Loopback0.0
ip tcp adjust-mssauto
ipsec policy transport ipsec-policy
no shutdown
```

VPNのトンネルインターフェイスの設定

4端末の同時接続を想定し、tunnel0.0-tunnel3.0を使用

#同時接続端末数分のトンネル設定が必要

#Ver9.5以降、トンネル設定が共通の場合は省略可能

#10端末同時接続する場合の設定例

```
interface range Tunnel 0-3
tunnel mode l2tp-lns ipsec
ip unnumbered Loopback0.0
ip tcp adjust-mssauto
ipsec policy transport ipsec-policy
no shutdown
```

注意:コマンド有効化のために設定保存と再起動が必要

## 4. クライアント端末の VPN 設定

### 4-1 Windows 10 の VPN 設定

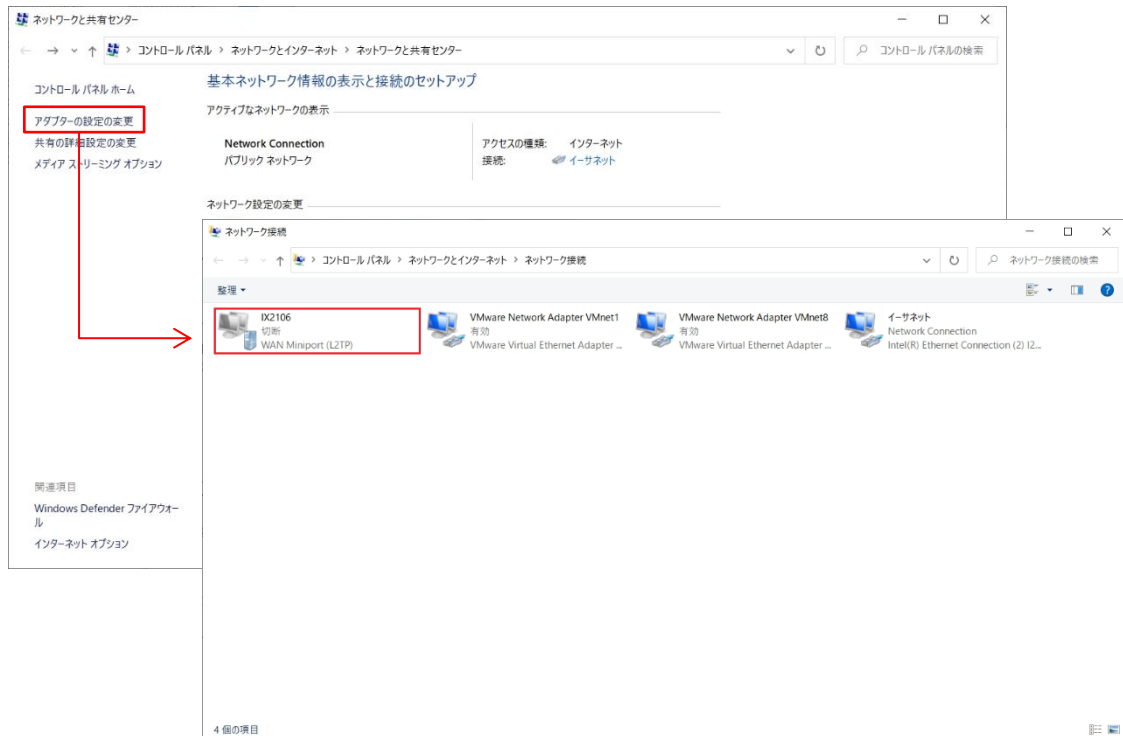
#### 4-1-1 VPN 設定

[Windows の設定]-[ネットワークとインターネット]-[VPN]を開き、「VPN 接続を追加する」をクリックし、下記の値を設定します。

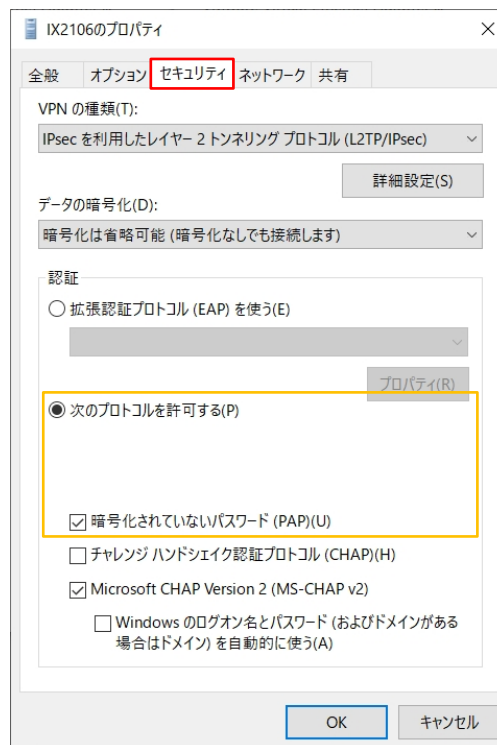


項目	値
VPN プロバイダー	Windows(ビルトイン)
接続名	IX2106
サーバー名またはアドレス	10.10.10.1
VPN の種類	事前共有キーを使った L2TP/IPsec
事前共有キー	himitsu
サインイン情報の種類	ユーザー名とパスワード
ユーザー名(オプション)	user01
パスワード(オプション)	(空欄)

「ネットワークと共有センター」を開き、「アダプターの設定の変更」をクリックします。



追加された VPN 設定「IX2106」のプロパティを開き、「セキュリティ」タブにて PAP 認証の許可を行います。

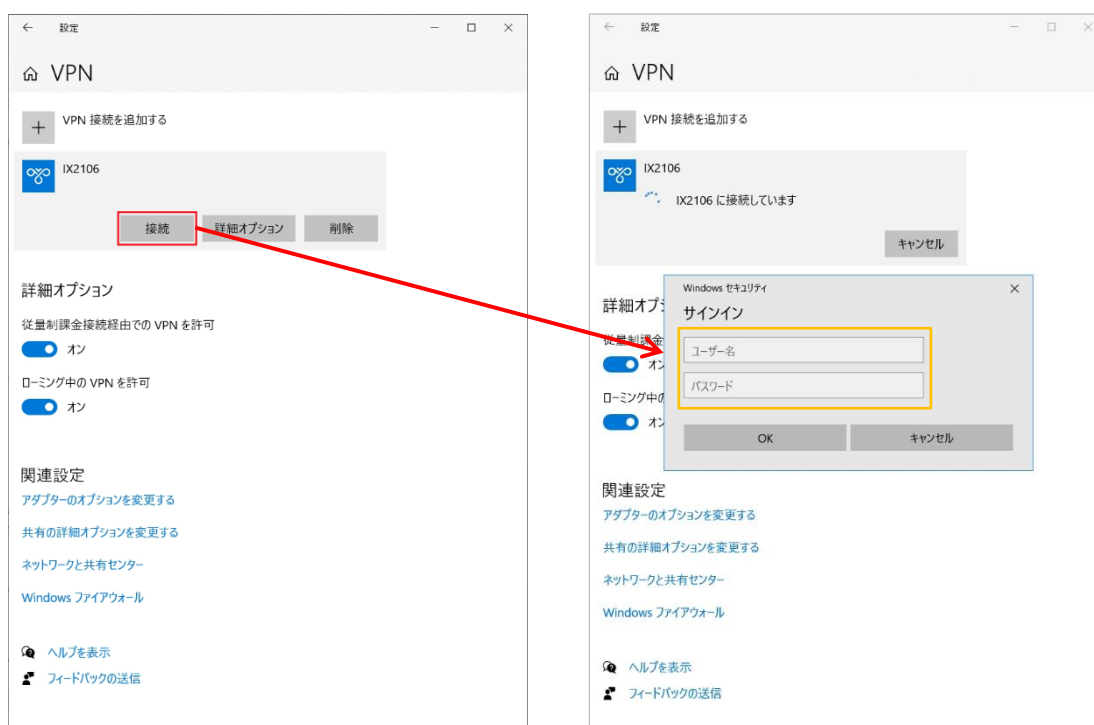




### 4-1-2 接続方法

[Windows の設定]-[ネットワークとインターネット]-[VPN]を開き、追加した「IX2106」の接続ボタンをクリックします。

サインイン画面でユーザー名とワンタイムパスワードを入力し、接続します。



#### 補足

リモートユーザー宅内のブロードバンドルーター等、Windows 端末と IX ルーターの間に NAT ルーターが存在する場合、Windows 端末のレジストリ設定で NAT トラバーサル機能を有効にする必要があります。

以下の URL に記載されている手順に従い、NAT トラバーサル機能を有効にしてください。

<http://support.microsoft.com/kb/926179/ja> (外部リンク)

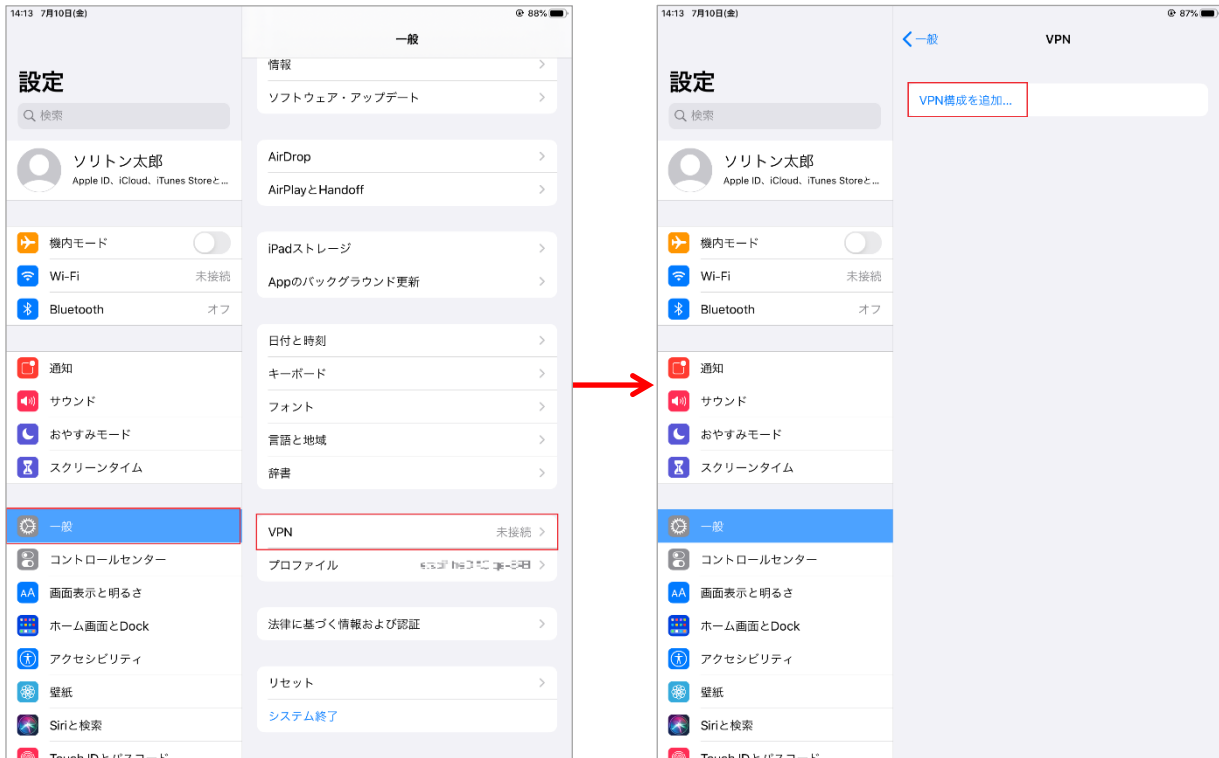
**AssumeUDPEncapsulationContextOnSendRule** の値は「2」を設定してください。

レジストリを誤って変更すると深刻な問題が発生することがありますので設定変更は慎重に実施してください。

## 4-2 iOS でのVPN 設定

## 4-2-1 VPN 設定

「設定」メニューの[一般]-[VPN]にて設定を行います。



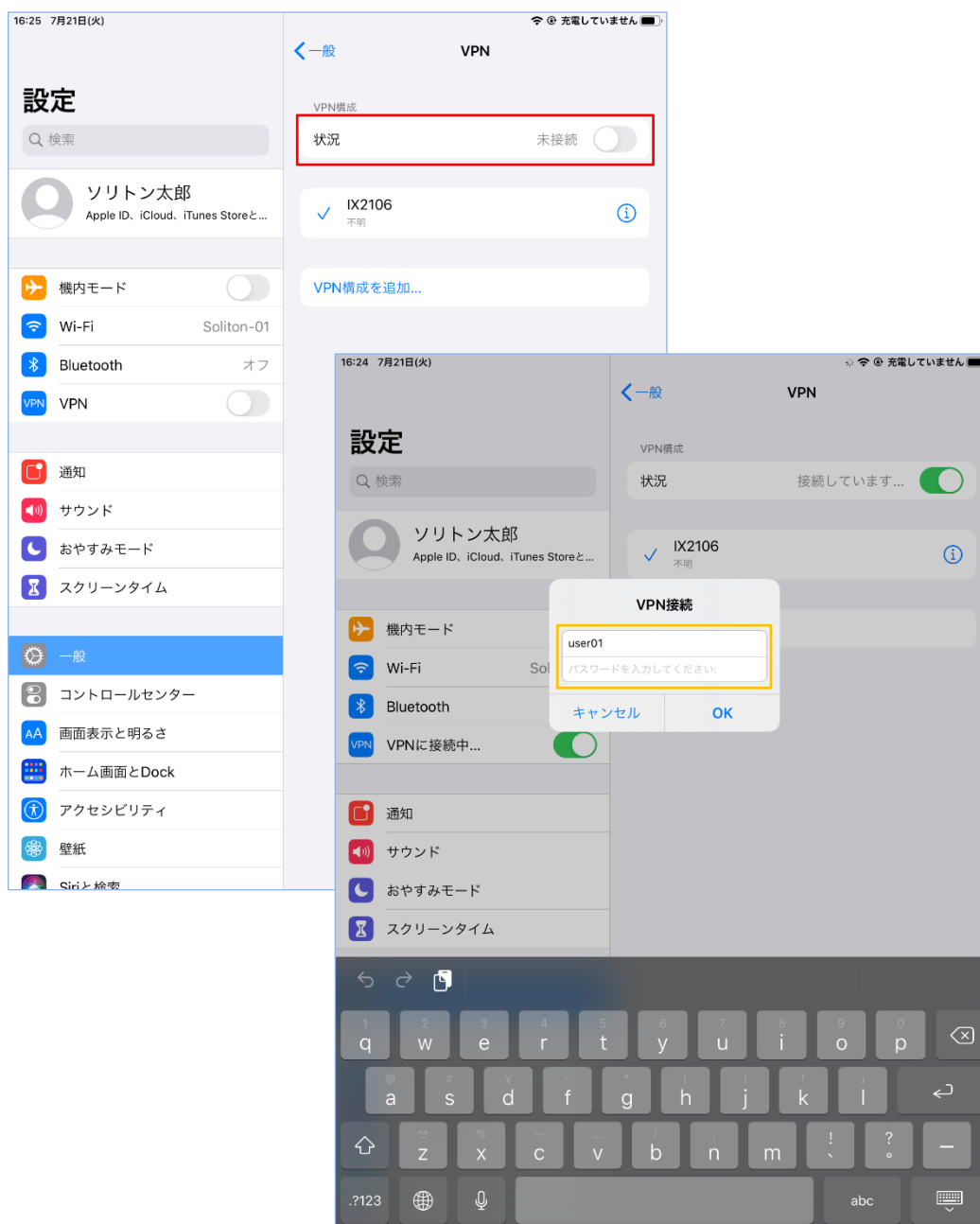
項目	値
タイプ	L2TP
説明	IX2106
サーバ	10.10.10.1
アカウント	user01
パスワード	(空欄)
シークレット	himitsu



## 4-2-2 接続方法

「VPN」設定画面にて、「状況」のトグルスイッチを有効にします。

パスワードの入力を求められるので、ワンタイムパスワードを入力し、「OK」をタップしてください。



## 4-3 Android の VPN 設定

## 4-3-1 VPN 設定

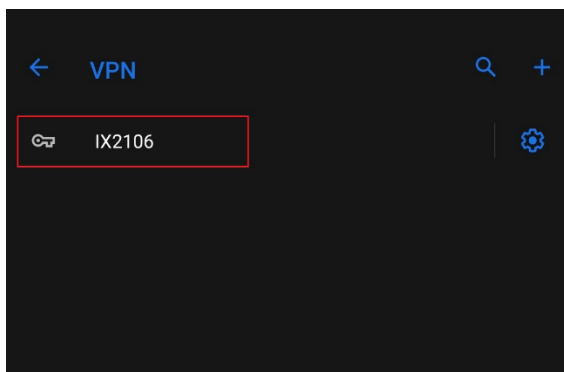
端末の設定メニューから VPN の設定を行います。



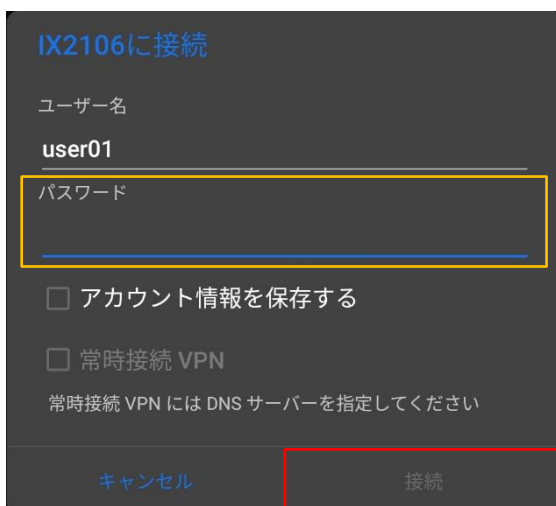
項目	値
名前	IX2106
タイプ	L2TP/IPSec PSK
サーバーアドレス	10.10.10.1
IPSec 事前共有鍵	himitsu
ユーザー名	user01
パスワード	(空欄)

### 4-3-2 接続方法

VPN 一覧画面にて、作成した VPN をタップします。



パスワードの入力を求められるので、ワンタイムパスワードを入力し、「接続」をタップします。



## 5. 動作確認結果

### 5-1 ワンタイムパスワード認証が成功した場合の EPS のログ表示例

```
Login OK: [user01](from client RadiusClient01 port 2147484450)
```

### 5-2 UNIVERGE IX シリーズでのログ確認方法

#### 5-2-1 表示コマンドでの確認方法(show interface tunnel0.0 detail)

<pre>Router(config)# show interfaces Tunnel0.0 detail Interface Tunnel0.0 is up Fundamental MTU is 1400 octets Current bandwidth 1G b/s, QoS is disabled Datalink header cache type is none: 0/0 (standby/dynamic) IPv4 subsystem disconnected, physical layer is up, 0:00:32 Dialer auto-connect is enabled Inbound call is enabled Outbound call is enabled Dial on demand restraint is disabled, 0 disconnect</pre>	<p>クライアントとの VPN 接続状態確認 UP:接続 DOWN:未接続</p>
<p>【中略】</p> <pre>PAP statistics:  2 packets rcvd, 38 octets  2 auth reqs, 0 auth acks, 0 auth naks  0 errors, 0 unknowns  2 packets sent, 52 octets  0 auth reqs, 2 auth acks, 0 auth naks</pre>	<p>NetAttest EPS との認証状態確認 auth reqs:認証要求 auth acks:認証応答</p> <p>auth reqs のカウントが上がっているにも関わらず auth acks のカウントが上がらない場合は、 NetAttest EPS もしくは IX の設定の誤りあり</p>
<p>【中略】</p> <pre>Encapsulation TUNNEL: Tunnel mode is ipsec (l2tp-lns ip) Destination address is not configured Interface MTU is 1424 Path MTU is 1500 L2TP information: Tunnel is idle Statistics:  45 packets input, 3956 bytes, 0 errors  45 packets output, 4856 bytes, 0 errors</pre>	<p>VPN 経由の通信状態の確認 packets input:受信カウンタ packets output :送信カウンタ</p> <p>VPN 接続状態が UP だったにも関わらず送受信 カウンタが上がらない場合は、今回の推奨設定 以外の経路設定などが誤っている可能性が高い</p>
<pre>Received ICMP messages:  0 errors  0 network unreachable  0 host unreachable  0 protocol unreachable  0 fragmentation needed</pre>	

## 5-2-2 装置ログでの確認方法

IX シリーズ認証成功時のログを確認する場合は、レベルの変更が必要になります。

logging subsystem all warn → logging subsystem aaainfo

確認コマンド(show logging)

■ 成功時(AAA.003 が出力)

AAA.003 AUTHEN\_TYPE authentication succeeded, user=USER\_NAME,  
addr=REMOTE\_ADDR, svr=AUTHEN\_SERVER

■ 失敗時(AAA.004 が出力)

AAA.004 AUTHEN\_TYPE authentication failed, user=USER\_NAME,  
addr=REMOTE\_ADDR, svr=AUTHEN\_SERVER

