



【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
(پ	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、
<u>.</u>	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。

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。

<u>Saliton</u>

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

Seliton 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



Spliton

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		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	UDP 1812	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	-	-

Seliton®

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

Seliton®

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

NetAttest EPS			
No Hindaria (a. 227 o) 7-± 227 Adt (a. Matrix	V−F Rames Rames S		
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!	かして下さい。		
ネットワーク時刻			
NTPサーバー1			
NTPサーバー2			
<u>NTPサ</u> 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	<u>第30</u>		
RADIUS 70 + 2	#X0		
Windowsトライン記念D連携	#50 年か		
	mox/ 新动		
	<u>無効</u>		
	一戻る「再起物」		

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	

<u>Seliton</u>

2. NetAttest EPSの設定

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

CA種別選択			
CA種別展択	1-►CA ¥		
CA秘密鍵			
● 内部で新しい鍵を生成する			
公開練方式	RSA 🗸		
鍵長	2048 🗸		
● 外部HSMデバイスの鍵を使	使用する		
要求の署名			
要求署名アルゴリズム	SHA256 🗸		
CA情報			
CA名(必須)	TestCA		
国名	日本	~	
都道府県名	Tokyo		
市区町村名	Shinjuku		
会社名(組織名)	Soliton Systems		
部署名			
E-mailアドレス			
CA署名設定			

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

NAS/RADIUSクライアンナ名・	RadiusClient01	^
☑ このNAS/RADIUSクライアント	を有効にする	
モデル名	×	
	● NAS/RADIUSクライアント ● NASのみ ● RADIUSクライアントのみ	
110) 1		
IP7FL/ス・	192.168.1.1	
シークレット	•••••	
所属するNASグループ	✓	

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

Spliton

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。

NetAttest EPS		ログオン中: admin
 naeps.example.com システム設定 システム管理 証明機関 DHCPサーバー IDACPサーバー 		
 LDAPサーバー RADIUSサーバー E起動/停止 RADIUSサーバー設定 RADIUSサーバー管理 EPS5ライセンス NAS/RADIUSクライアント VASCO DIGIPASS トークン一覧 DPXファイルインボート トークン一括管理 VASCOオブション 	転送キー インボート分数により数分かかる場合があります。 ▲ 回し完全する何報は更新できたさん。	

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。

NetAttest EPS					ログオン中: adm
 naeps.example.com ・ンステム設定 ・システム管理 ・証明機関 ・回明機関 		 ● 一部 ● 完全 状態 ダベで ¥ 200) 件まで 株本		
LDAPサーバー	トークンシリアルNo	トークンモデル	インボート日時	使用中のユーザーID	タスク
	279000001	DPGO6			リセット 変更 削除
■ 記載の「今止 ■ RADIUSサーバー設定 ■ RADIUSサーバー営理 ■ EP5ライセンス ■ NAS/RADUSクライアント ■ VASCO DIGIPASS ■ <u>トークンー気</u> ■ DPXフィルインボート ■ トークン一括管理	<u>VES0000001</u>				リセット 変更 削除

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。

Mat Attack FDG					ログ	オン中: admin
NetArtest EPS			・ トップペー	-ジ 🕒 🖁	锭保存)(0 ログオフ)
 naepsexample.com システム設定 システム管理 証明機関 DHCPサーバー LDAPサーバー RADIUSサーバー 	ユーザーー覧 ユーザー ユーザー ユーザー ユーザー ユーザー ユーザー ユーザー ユーザー ユージー ユー ユー	グルーナ 💙 📃 ユ	ーザーまで <mark>検索</mark> ユー	・ザー削除時	の証明書失	<u>追加</u> 対対ブション
= ユーザー	▲名施	<u>ユーザーID</u>	最終認証成功日時	証明書	夕	マク
■ <u>エーリー一頁</u> ■ エクスポート	test user	test		発行	変更	削除
■ インボート ■ ユーザーバスワードボリシー ■ デフォルトユーザーブロファイル ■ ゲスト						

「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。

₩ 果 刈 承: 新 723		
ユーザー情報 チェックアイテム		
基本情報		
姓	user01	
E-Mail		
詳細情報		0
認証情報		
ユーザーID*	user01	
	•••••	
パスワード(確認)。	••••••	
■ 一時利用停止		

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

🤰 ユーザー設定	
編集対象:新規	
ニューザー皆報 チェックアイテム リプラ	
標準のチェックアイテム	
認証タイプ	VASCO V
発信者番号	•
同時接続可能なセッション数	
接続可能な時間帯	
有効期限	❤ 年 ❤ 月 ❤ 日 ❤ 時 ❤ 分
任意のチェックアイテム	
アトリビュート	オペレーター 値
	OK キャンセル 適用

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。

##00/75/7754 Session Timeout 1800 VLAN ID 9/0 Filer ID 9/0 ##00/75/7764 9/0 TPUCa-h TAVL-9- ##00/75/7764 9/0 Service-Type 2 OK #+>>tw According Part 9/0 VASCO DIGIPASS 9/0 Protocool 9/0 OK #+>>tw 279000001 010	標準のリプライアイテム		アイテム				
Session Timeout 1800 VLAN ID 9/7 Filer ID Image: Image							
VLAX ID ダグ Filter ID (1) C&OUT5/77-7-L アリピュート オペレーター (1) Tramed-IP-Address (2) (1) (1) Service-Type (2) (1) (1) CK キャンセル (2) (1) (1) CK キャンセル (2) (1) (1) XASCO DIGIPASS (1) (1) (1) (1) トークンシリアア (1) (1) (1) (1) (1)	SessionTimeout	l (1800				
ihr tD 意のリブライアイテム アトリピュート オペレーター ramed-IP-Address 選訳 「 invice-Type 選訳 2 ok キャンセル 通用 CK キャンセル 通用 CK キャンセル 通用 CK 279000001 「 アンジリアノNA0 279000001 「	LAN ID	[タグ			
©UJ754747-A アトリビュート オペレーター 値 ramed-IP-Address 選択 = ✓ 192.168.1.10 ramed-Protocol 選択 = ✓ 2 OK キャンセル 通用 T - 5 倍報 チェックアイテム リブライアイテム OTP VASCO DIGIPASS トークンシリブアル№ 279000001 ■	ïilter ID				20		
ア・リビュート オ・レレーター 値 iramed-IP-Address 運訳 > PPP Service-Type 運訳 > 2 OK キャンセル 通用 2 OK キャンセル 2 Tramed-Protocol PPP 0K キャンセル 通用 2 Tramed-Protocol PPP 0K キャンセル 通用 2 Tramed-Protocol PPP 2 Tramed-Protocol PP 2 Tramed-Protocol PP 2 Tramed-Protocol PP 2 Tramed-Protocol P 2 Tramed-Protocol P 2 Tramed-Protocol P 2 Tramed-P Tramed-P 2 Tramed-P Tramed-P 2 Tramed-P Tramed-P 2 Tramed-P Tramed-P </th <th>意のリプライアイテム</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	意のリプライアイテム						
ramed-IP-Address 選択 = ✓ 192.168.1.10 ramed-Protocol 選択 = ✓ PPP ervice-Type 選択 = ✓ 2 OK キャンセル 適用 0K キャンセル 適用 2 192.168.1.10 Framed-IP-Address 192.168.1.10 Framed-IP-Address 192.168.1.10 Framed-Protocol PPP 2 ● ● ● ● 2 ● ● ● ● 2 ● ● ● ● ● 2 ● ● ● ● ● ● 2 ●<	アトリビュート		オペレータ	9— 値			
ramed-Protocol 速訳 ●	ramed-IP-Address	選択	= 🗸	192.168.1.10	+ -		
Service-1ype 速水 マ 2 メリロー 1 (1) 「Framed-IP-Address 192.168.1.10 Framed-Protocol PPP Service-Type 2 2 2 2 2	ramed-Protocol	選択	= 🗸	PPP	+ -	75	唐
Image: Contract of the second contr	ervice-Type	进伏	= •	2		現日	112
ОК *+>>tл. Эп ヴ- 情報 f== Framed-Protocol PPP Service-Type 2						Framed-IP-Address	192.168.1.10
OK キャンセル 適用 Service-Type 2 L-ヴー情報 チェックアイテム リプライアイテム OTP 2 2 ASCO DIGIPASS トーウンシリアルNo 279000001 ・ 1 1						Framed-Protocol	PPP
2-ザー情報 メュックアイテム リブライアイテム 0TP /ASCO DIGIPASS トークンシリアル№ 2790000001 ■				0K +++/++	適田	Service-Type	2
トークンシリアル№ 279000001 ···	VASCO DIGIPASS						
	トークンシリアルNo		27900000	001 + -			
項目						項目	値

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。

NetAttest EPS					ログオン中: admin
= naeps.example.com ロ システム設定 ロ システム管理	トークン一覧 トークンシリアルNo	● 一部 ● 完全 伏態 すべて ✔ 200	件までは本		
□ 証明機関 □ DHCPサーパー □ LDAPサーパー ■ RADIUSサーパー	<u>トークンシリアルNo</u> <u>2790000001</u>	<u>トークンモデル</u> DPG06	<u>インポート日時</u> 2020/07/15 23:25:35	<u>使用中のユーザーID</u> user01	タスク リセット 変更 削除
 記動ノ停止 RADIUSサーバー設定 RADIUSサーバー管理 EPSライセンス NAS/RADIUSクライアント VASCO DIGIPASS トークンー気 DPXファイルインボート トークン「報知エクスボート トークンー括管理 					91:91 变更 削除

<u>Seliton</u>

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 !	RADUIS サーバーの指 IP アドレス「192.168	定コマンド 3.1.2」、
radius host ip 192.168.1.2 key 0 secret source Loopback0.0	シークレット「secret	」を設定
ip route default 10.10.10.254 ip access-list sec-list permit ip src any dest any	ルーターのデフォルト	ルートの設定
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	IX ルーターと VPN ク 事前共有キー「himitsu RADIUS 設定のシーク	ライアントの 」を設定 レットとは
ike policy ike-policy peer any key himitsu ike-prop1,ike-prop2,ike-prop3	異なるため注意	
i 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-pro !	pp3	
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 !		



interface GigaEthernet0.0 ip address 10.10.10.1/24 no shutdown interface GigaEthernet1.0 ip address 192.168.1.254/24 ip proxy-arp	WAN インターフェイスの設定
no shutdown	LAN 1 ノダーノ11 入の設定
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 Ins tunnel mode l2tp-Ins ipsec ip unnumbered Loopback0.0 ip tcp adjust-mssauto ipsec policy transport ipsec-policy no shutdown ! interface Tunnel1.0 ppp binding Ins tunnel mode l2tp-Ins ipsec ip unnumbered Loopback0.0 ip tcp adjust-mssauto ipsec policy transport ipsec-policy no shutdown	
interface Tunnel2.0 ppp binding Ins tunnel mode l2tp-Ins ipsec ip unnumbered Loopback0.0 ip tcp adjust-mssauto ipsec policy transport ipsec-policy no shutdown ! interface Tunnel3.0 ppp binding Ins tunnel mode l2tp-Ins 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、tunnnel0.0-tunnnel3.0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-Ins 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



Seliton 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。

← 設定 - □ ×	VPN接続を追加
命 VPN	VPN プロパイダー
↓ VPN 接続を追加する	Windows (ビルトイン) 〜
	接続名
詳細オプション	IX2106
従量制課金接続経由での VPN を許可	サーバー名またはアドレス
() オン	10.10.10.1
ローミング中の VPN を許可	VPN の種類
	事前共有キーを使った L2TP/IPsec V
	with the second
関連設定	
アダプターのオブションを変更する	
共有の詳細オプションを変更する	サインイン情報の種類
ネットワークと共有センター	
Windows ファイアウォール	ユーザー名 (オプション)
	user01
	ולק ח_ג (גל ליביא)
2 フィートハックの送信	
	□ サインイン情報を保存する
	保存 キャンセル

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。

は ネットワークと共有センター				- 🗆 ×	
← → × ↑ 💆 > או-חאכב	《ネル > ネットワークとインターネット > ネットワーク	7と共有センター	~ O	, クロントロール パネルの検索	
コントロール パネル ホーム	基本ネットワーク情報の表示と接続	たのセットアップ			
アダプターの設定の変更 共有の詳細設定の変更 メディアストリーミング オプション	Network Connection パブリック ネットワーク	アクセスの種類: インターネット 接続: <i>御</i> イーサネット			
	ネットワーク設定の変更				
	🌺 ネットワーク接続				- 🗆 ×
	🔶 א א א א א א א א א א א א א א א א א א א	> ネットワークとインターネット > ネットワーク接続		~ U 🔎	ネットワーク接続の検索
	整理 ▼				Ē • 🔟 🕜
	ViAN Miniport (L2TP)	VMware Virtual Ethernet Adapter VMware Virtual	e Virtual Ethernet Adapter	Intel(R) Ethernet Connectio	n (2) I2
開連項目					
Windows Defender ファイアウオー ル					
インターネット オプション					
	_				

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。

■ IX2106のプロパティ	×
全般 オプション セキュリティ ネットワーク 共有	
VPN の種類(T):	
IPsec を利用したレイヤー 2 トンネリング プロトコル (L2TP/IPsec)	\sim
詳細設定(S)	
データの暗号化(D):	
暗号化は省略可能 (暗号化なしでも接続します)	\sim
認証	
○ 拡張認証プロトコル (EAP) を使う(E)	
~	11
ゴロ パテ ノノ の	11
● 次のプロトコルを許可する(P)	٦.
☑ 暗号化されていないパスワード (PAP)(U)	
□ チャレンジ ハンドシェイク認証プロトコル (CHAP)(H)	
Microsoft CHAP Version 2 (MS-CHAP v2)	
── Windows のログオン名とパスワード (およびドメインがある 場合はドメイン)を自動的に使う(A)	
ОК ++v>t	211



4-1-2 接続方法

Spliton

[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。

Seliton

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。

14:13	7月10日(金)		@ 88%	14:13	7月10日(金)				@ 87% ()
		一般				<-	一般	VPN	
=0	. 	情報	>	=0.	-				
設	定	ソフトウェア・アップデート	>	設	定		/PN構成を追加…		
Q	検索			Q	検索				
	ソリトン大郎	AirDrop	>		いリトン大郎				
	Apple ID、iCloud、iTunes Storeと	AirPlay & Handoff			Apple ID, iCloud, iTunes Store	٤			
		An ay changer							
⊳	機内モード	iPadストレージ	>	P	機内モード				
?	Wi-Fi 未接続	Appのバックグラウンド更新	>	?	Wi-Fi 未打	医統			
*	Bluetooth オフ			*	Bluetooth	17			
		日付と時刻	>						
	通知	キーボード	>		通知				
(۱)	サウンド	フォント	>	•10	サウンド				
C	おやすみモード	言語と地域	>	C	おやすみモード				
X	スクリーンタイム	辞書	>	X	スクリーンタイム				
Ø	一般	VPN *	接続 >	0	一般				
8	コントロールセンター	プロファイル etail heD 10 ge-	848.>	2	コントロールセンター				
AA	画面表示と明るさ			AA	画面表示と明るさ				
	ホーム画面とDock	法律に基づく情報および認証	>		ホーム画面とDock				
()	アクセシビリティ			٢	アクセシビリティ				
-	壁紙	リセット	>	۲	壁紙				
	Siriと検索	システム終了			Siriと検索				
6	Touch IDとパスコード				TouchIDとパフコード		-		

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

		V		
キャンセル				完了
タイプ				L2TP >
説明	IX2106			
サーバ	10.10.10.1			
アカウント	user01			
RSA Securl	C			\bigcirc
パスワード	毎回確認			
シークレット	•••••			
すべての信号	号を送信			
プロキシ				
7477				
77		手動	自動	

5<1100 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。

16:25 7月21日(火)	중 ⑥ 充電していません ■)	
	<一般 VPN	
設定	VONIBLE	
	VPN编成 状况 未培練	
ソリトン太郎 Apple ID、iCloud、iTunes Storeと	✓ <mark>IX2106</mark> (j)	
機内モード	VPN構成を追加	
Soliton-01		
Bluetooth オフ	16:24 7月21日(火) 😔 🗢 ④ 充電していません	•
VPN VPN	<一般 VPN	
_	設定 VPN構成	
通知	Q 検索 状況 接続しています	
◀ サウンド		
▶ おやすみモード	Apple ID, iCloud, iTunes Storeと V IX2106 (1)	
🔀 スクリーンタイム	VPN接続	
🔘 一般	マ Wi-Fi Sol パスワードを入力してください:	
🕄 コントロールセンター	Bluetooth キャンセル OK	
AA 画面表示と明るさ	VPN VPNに接続中	
📰 ホーム画面とDock		
(アクセシビリティ	日 通知	
●●● 壁紙	뒔 サウンド	
Siriと始表	おやすみモード	
	☑ スクリーンタイム	
	5 7 B	
	qwertyui op <)
	a s d f g h j k l ← .	
	.?123 🌐 👰 abc 📖	



Seliton

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。

← ネットワークとイン	ンターネット	Q	÷	VPN			۹ -
Wi-Fi OFF							
モバイル ネットワーク NTT DOCOMO		\rightarrow					
デュアルSIMカード設定							
通話							
モバイルプラン このサービスはネットワークキャリ	アが提供します						
アクセス ポイントとテザリング OFF	Ĵ			VPN プロフ ; ^{タ前}	ァイルの編集		
機内モード				石町 IX2106 タイプ			_
データセーバー OFF				ション L2TP/IPSec PS サーバー アドレス	К		•
VPN なし				10.10.10.1			_
プライベート DNS 自動				(未使用) 			_
				········ (未使用) IPSec事前共有鍵			_
				••••••• □ 詳細オプシ	·ョンを表示する		—
項目	値			ユーザー名			
名前	IX2106			user01			—
タイプ	L2TP/IPSec PSK		Ĺ				
サーバーアドレス	10.10.10.1		L				
IPSec 事前共有鍵	himitsu			 二 吊 吋 按 続 V 常 時 接続 VPN に(PN はDNS サーバーを指定	してください	
ユーザー名	user01						
パスワード	(空欄)						

Seliton

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。

	VPN		م	
ଙ୍କ	IX2106			(\$)

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。

ユーザー名					
user01					
パスワード					
アカウント情報を係					
□ 常時接続 VPN 常時接続 VPN には DNS サーバーを指定してください					

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)

	クライアントとの VPN 接続状確認
Router(config)# show interfaces Tunnel0.0 detail	UP:接続 DOWN:未接続
Fundamental MTU is 1400 octets Current bandwidth 1G b/s, QoS is disabled Datalink header cache type is none: 0/0 (standby/dy IPv4 subsystem disconnected, physical layer is up, 0 Dialer auto-connect is enabled Inbound call is enabled Outbound call is enabled Dial on demand restraint is disabled, 0 disconnect	ynamic)):00:32
【中略】	NetAttest EPS との認証状態確認
PAP statistics: 2 packets rcvd 38 octets	auth acks:認証広答
2 auth reqs, 0 auth acks, 0 auth naks 0 errors, 0 unknowns 2 packets sent, 52 octets	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
【中略】	
Encapsulation TUNNEL: Tunnel mode is ipsec (l2tp-Ins ip) Destination address is not configured Interface MTU is 1424 Path MTU is 1500 L2TP information:	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
Tunnel is idle Statistics: 45 packets input, 3956 bytes, 0 errors 45 packets output, 4856 bytes, 0 errors Received ICMP messages:	VPN 接続状態が UP だったにも関わらず送受信 カウント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
0 errors 0 network unreachable 0 host unreachable 0 protocol unreachable 0 fragmentation needed	

Seliton®

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 \rightarrow 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

<u>Seliton</u>

改訂履歴

日付	版	改訂内容
2020/09/09	1.0	初版作成