# NetAttest EPS 設定例

連携機器:

## Cisco ASA 5505

## Case: AnyConnect を利用した、

証明書とパスワードによるハイブリッド認証

Version 1.3

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  $\odot$  2017, Soliton Systems K.K. , All rights reserved.



## はじめに

#### 本書について

本書は、NetAttest EPS と Cisco Systems 社製 Cisco ASA 5505 との証明 書認証連携について記載した設定例です。

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 提に記述します。

#### 表記方法

表記方法	説明
ABCDabcd1234	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出力、
(normal)	コード例を示します。
ABCDabcd1234	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示しま
(bold)	す。
ABCDabcd1234	
(italic)	友奴で小しより。天际に使用する何足の石削または個し国ご換えます。

表記方法	説明
ſ J	参照するドキュメントを示します。
٢J	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。
[+-]	キーボード上のキーを表します。
[‡-1]+[‡- 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。
[filonamo]	[ ] 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
[filename]	いことを示しています。

## 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。
<u>.</u>	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 ASA 5505 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	
	1-1	構成図
2	NetA	ttest EPS の設定9
	2-1	システム初期設定ウィザードの実行10
	2-2	サービス初期設定ウィザードの実行11
	2-3	認証ユーザーの追加登録 12
	2-4	クライアント証明書の発行13
3	ASA	5505 の設定準備 14
	3-1	インターフェイスの設定15
	3-2	システム時刻の設定17
4	ASA	5505 の PKI 関連の設定18
	4-1	CSR の生成 (ASA 5505)19
	4-2	サーバー証明書署名要求 (NetAttest EPS) 22
	4-3	サーバー証明書の発行 (NetAttest EPS)
	4-4	サーバー証明書のダウンロード (NetAttest EPS)
	4-5	CA 証明書の取得 (NetAttest EPS)
	4-6	CA 証明書のインポート (ASA 5505)26
	4-7	サーバー証明書のインポート (ASA 5505)
5	ASA	5505 の接続設定 29
	5-1	IP アドレスプールの設定
	5-2	AAA サーバー(RADIUS サーバー)の設定
	5-3	AnyConnect VPN Connection Setup Wizard 33
6	Wind	lows版 AnyConnectの設定38
	6-1	PC へのデジタル証明書のインストール
	6-2	Windows 版 AnyConnect の設定 41
7	iOS 覑	反 AnyConnect の設定
	7-1	iPhone への VPN 用デジタル証明書のインストール
	7-2	iOS版 AnyConnectの設定44

- 5 -

## **Seliton**

8	Andro	oid OS版 AnyConnectの設定	45
	8-1	Android 端末への VPN 用デジタル証明書のインストール	46
	8-2	Android OS版 AnyConnect 設定	47
9	接続0	D確認	50
	9-1	PC における AnyConnect を利用した SSL-VPN 接続	50
	9-2	iPhone における AnyConnect を利用した SSL-VPN 接続	51
	9-3	Android 端末で AnyConnect を利用した SSL-VPN 接続	52



## 1 構成

#### 1-1 構成図



※NetAttest EPS の設定は、設定用の Windows 管理端末 と NetAttest EPS の管理ポート(LAN2) を直結して行います。



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)	ソリトンシステムズ	NetAttest EPS (EPS-ST05-A)	Ver. 4.10.0
RADIUS クライアント (SSL VPN 機器)	Cisco Systems	ASA 5505	Ver.8.4(1)
Client PC	Microsoft	Surface3 Pro	Windows 8.1
Client Smart Phone	Apple	iPhone X	iOS 11.1.2
Client Smart Phone	Huawei	Nexus 6P	Android 7.1.2
無線 AP	Allied	AT-TQ3400	_

#### 1-2-2 認証方式

#### デジタル証明書認証+ID・Password 認証

#### 1-2-3 ネットワーク設定

	EPS-ST05-A	ST05-A ASA 5505		Client Tablet	無線 AP
IP アドレス	192.168.1.2/24	192.168.1.1/24	DHCP (無線 AP から)	DHCP (無線 AP から)	192.168.2.110/24
RADIUS port (Authentication)	TCP 1812		-	_	
RADIUS port (Accounting)	TCP 1813		_	_	_
RADIUS Secret (Key)	secret		_	_	_



## 2 NetAttest EPS の設定

NetAttest EPS 設定の手順

- 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. クライアント証明書の発行



#### 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に従って、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
- ◆ メインネームサーバーの設定

🗲 🕘 📶 http://192.168.2.1 1161/	P・C 0 15275個地 noepo net. 0 15275個地 no	нера-мис	nee	
NetAttest EPS				
	「○」 加田改立ウィザ →・ システム →・ サービス →・ システム 単元 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	—————————————————————————————————————		
		初期設定ウィザード - 設定項	目の確認	
Copyright © 2004-2017, Soliton Systems K.K., Al	l rights reserved.	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	よ「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サーパー1	
			NTPサーバー2	
			NTPサーバー3	
			時刻同期する	無効
		ホスト名		naeps.example.com
		サービスインターフェイス		
			IPアドレス	192.168.1.2
			サブネットマスク	255.255.255.0

【ホスト名】 : naeps.example.com 【IP アドレス】: デフォルト (LAN1:192.168.1.2,LAN2:192.168.2.1) 【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。

本手順書では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)

CA種別選択		
CA種別選択	л-КСА 🗸	
CA秘密鍵		
● 内部で新しい鍵を生成する		
公開離方式	RSA 🗸	
鍵長	2048 🗸	
● 外部HSMデバイスの鍵を	使用する	
要求の署名		
要求署名アルゴリズム	SHA256 V	
CA情報		
CA名(必须)	EPS ROOT CA	
围名	日本 🗸	
都道府県名		
市区町村名		
会社名(組織名)		
部署名		
E-mailアドレス		
CA署名設定		
著名アルゴリズム	SHA256 V	
有効日敷	3650	

【CA 種別選択】
・ルート CA
【公開鍵方式】
・R S A
【鍵長】
・2048
【CA 名】
・EPS ROOT CA
【国名】
・日本
【著名アルゴリズム】
・SHA256

◆ 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

✓ このNAS/RADIUSクライアントを行う	有効にする		
モデル名	×		
タイプ	● NAS/RADIUSクライアント ● NASのみ ● RADIUSクライアントのみ		
此明		0	
P7FUZ*	192.168.1.1		
シークレット	•••••		P
ER + ZNAR /			

#### 2-3 認証ユーザーの追加登録

NetAttest EPS の管理画面より、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。

← → M http://192.168.2.1:2181/sysadmin/Index.cgi	D - C 🚺 I-4-	一覧 [システム管理-n ×						<b>↑</b> ★♀
							ログオ	ナン中: admin
NetAttest EPS					● トップペー	·>) 🖸 🛚	定保存 🛛 🔁	<b>ロ</b> グオフ
■ naeps.example.com	8	<b>2</b> -						
■ システム設定	A 1-9	·n						
■ システム管理	ユーザー	● 一部 ● 完全	グループ 💙	ユーザーまで 検3	8			
■ 証明機関	詳細オプションの設定							
■ DHCPサーバー	エクスポート							
■ LDAPサーバー								追加
■ RADIUSサーバー					<u>–</u>	ザー削除時	の証明書失効	カオブション
■ ユーザー		名前	ユーザー	<u>-10</u>	終認証成功日時	証明書	タス・	2
□ ユーザー一覧		test user	test			*5	का	81 Kb
■ エクスポート						3611		111 102
■ インポート								
■ 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								
	<b>MR</b>			100	▼ 性/ページ 1件	由 1 1 任左	** <b>*</b> **	曲 水 带板
< >						1 1 1 1 2		
Copyright © 2004-2017, Soliton Systems K.K., All	rights reserved.							
http://192.168.2.1:2181/radius/naldapedit.cgi?CGIMODNAM	IE=LdapUserList&LdapServerN	lame=LocalLdap01&LdapOt	jectType=User				1	🔍 185% 🔻 🚽





#### 2-4 クライアント証明書の発行

NetAttest EPS の管理画面より、クライアント証明書の発行を行います。

「ユーザー」→「ユーザー一覧」から、該当するユーザーのクライアント証明書を発行します。(クライアント証明書は、user01\_01.p12 という名前で保存)





## 3 ASA 5505 の設定準備

### ASDM のセットアップと ASA 5505 の基本設定

- 1. インターフェイスの設定
- 2. システム時刻の設定

### 3-1 インターフェイスの設定

ASA 5505の設定は ASDM(Adaptive Security Device Manager)で行います。

本環境では、ASDM ver.7.1(7)を使用しています。

ASA 5505 のインターフェイスの設定は、下記の通りです。



#### [Ethernet0/0] inside

IP:192.168.1.1 255.255.255.0 · · · 社内 LAN に接続。管理 interface としても使用。

#### [Ethernet0/1] outside

IP:192.168.2.2 255.255.255.0 · · · AnyConnect による接続を受付ける interface。

♀♀ ASA 5505 のセットアップ方法は、 ASA 5500 シリーズのクイックセットアップガイドをご参照下さい。



また、 [Enable traffic between two or more interfaces which are configured with same security levels]を有効にします。

1						Cisco	ASDM 7.	1 for ASA - 3	192.168.1	1
Fil	e View Tools Wizards	Win	ndow	Help						
٢	Home % Configuration 📝	Monite	oring	🔜 Save 🔇 Refresh	🕒 Back	🖸 Forward	d 🦻 Help			
ti	Device Setup # 9	Con	figurat	tion > Device Setur	> Interfa	ices				
8	Startup Wizard	Inte	rfaces	Switch Ports						
Devi<	⊞*? Houting   Device Name/Passw ⊞© S∨stem Time	N	√ame	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow	VLAN
		in	side	Ethemet0/0, Ether	Yes	100	192.168.1.1	255.255.255.0		vlan1
			utsid	Ethemet0/1	Yes	100	192.168.2.2	255.255.255.0		vlan2
	< >									
	🔏 Device Setup		_							
	🕄 Firewall		C							
	Remote Access VPN		Enab	le traffic between two	or more in	nterfaces w	hich are confi	gured with same s	ecurity levels	
	Site-to-Site VPN		Enab	le traffic between two	or more h	osts conne	cted to the sa	ime interface		
	🛃 Device <u>M</u> anagement									

### 3-2 システム時刻の設定

NetAttest EPS と同じ時刻を設定します。

「Configuration」-「Device Setup」-「System Time」-「Clock」から設定します。

Home 🦓 Configuration 😥 Monit	toring	🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help
Device Setup 📼	ምዋ	Configuration > Device Setup > Startup Wizard
Startup Wizard Interfaces + 2 Routing		Configure the ASA date and clock
Pevice Name/Password ■		Time Zone: (GMT+09:00) Tokyo
		Data
		2017/12/22
		Time
		Time: 09 : 01 : 32 hh:mm:ss (24-hour)
		Update Displayed Time

#### [Time Zone]

• Tokyo



## 4 ASA 5505 の PKI 関連の設定

### 証明書の取得とインポートの手順

- 1. CSR の生成 (ASA 5505)
- 2. サーバー証明書署名要求 (NetAttest EPS)
- 3. サーバー証明書の発行 (NetAttest EPS)
- 4. サーバー証明書のダウンロード (NetAttest EPS)
- 5. CA 証明書の取得 (NetAttest EPS)
- 6. CA 証明書のインポート (ASA 5505)
- 7. サーバー証明書のインポート (ASA 5505)



#### 4-1 CSR の生成 (ASA 5505)

ASA 5505 で CSR(Certificate Signing Request)を生成します。

「Configuration」-「Device Management」-「Certificate Management」-「Ident ity Certificates」の画面で『Add』ボタンを選択します。

Fi	le View Tools Wizards Window	v Help					Type topic to search	
-	) Home 🖧 Configuration 📴 Monitoring	Save 💽 Refresh	🕒 Back 🜔 Forwar	d 🦓 Help				cisco
st	Device Management a 🕫 🕫	Configuration > De	evice Management	> Certificate Mana	ement > Identity Certificates			
99 10	Management Access	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
Devi	System Image/Configuration     Logging     Smart Call-Home							Show Details
	Gondit Collin Fibric							Delete
	- CA Certificates							Export
	■ P DHCP ■ DNS							Install
	🗄 🐯 Advanced	Eind:		Match Case				
		Public CA Enrollmen Get your Cisco A promotional price Using a previous!	t - A security appliance for certificates and tr y saved certificate sig	up and running quick ial certificates for tes ming request, <u>enroll w</u>	ly with an SSL Advantage digital or ting Erroll ASA SSL certificate with ith Entrust	ertificate from Ent	trust. Entrust offers Cisco cue	stomers a special





[Add Identity Certificate]画面で「Add a new identity certificate」を選択します。
①[Key Pair]の『New』ボタンをクリックし新しい Key Pair 名を作成した後、
②[Certificate Subject DN]を設定します。

③『Advanced』ボタンをクリックし、証明書のパラメータを設定します。

3	Add Identity Ce	ertificate				
Trustpoint Name:	ASDM_TrustPoint0					
O Import the identity certific	ate from a file (PKCS1	2 format with Certificate(s)	)+Private Key):			
Decryption Passphrase:						
File to Import From:		Browse		1	(Key Pair)	
<ul> <li>Add a new identity certific</li> </ul>	at <mark>e</mark> :			• •	\$45505 kev	
Key Pair:	ASA5505.key	Show	New	1 1	SASSOS. Rey	
Certificate Subject DIN:	CINEciscoasa	Select				
Act as local certi	ficate authority and iss	sue dynamic certificates to	TLS-Proxy			
			TEO TIONY			
		l	Advanced			
Add Certific	cate C 🔟		Certif cat	e Subject I	SN	
		DN Attribute to be Added	d		Attribute Value	-
		Attribute: — Select A	.ttribute — 🔻	Add>>	Company N Cisco Sy	
The state is a state	oct DN1	Value:		Delete	Country (C) US	
[Certificate Subj						
Certificate Subj						
Certificate Subj						
Certificate Subj • CN:Ciscoasa • O:Cisco Systems	s		DK	Cancel	Help	
<ul> <li>(Certificate Subj</li> <li>CN:Ciscoasa</li> <li>O:Cisco Systems</li> <li>C:US</li> </ul>	s		ок [	Cancel	Help	
<ul> <li>(Certificate Subj</li> <li>CN:Ciscoasa</li> <li>O:Cisco Systems</li> <li>C:US</li> </ul>	s		ок [	Cancel	Help	
(Certificate Subj ・ CN:Ciscoasa ・ O:Cisco System ・ C:US 証明書サブジェクト	s は必ず指定し <sup>-</sup>	て下さい。	DK	Cancel	Help	
(Certificate Subj ・ CN:Ciscoasa ・ O:Cisco System: ・ C:US 証明書サブジェクト	s は必ず指定し <sup>-</sup>	<u>て下さい。</u>		Cancel	Help	
(Certificate Subj ・ CN:Ciscoasa ・ O:Cisco System ・ C:US 証明書サブジェクト NetAttest EPS で(2)	s は必ず指定し <sup>-</sup> は、デフォルト	<u>て下さい。</u> 〜では CN が必須	िंट्रन. ੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑ	Cancel	Help	
(Certificate Subj ・ CN:Ciscoasa ・ O:Cisco System: ・ C:US 証明書サブジェクト NetAttest EPS では	s は必ず指定し <sup>-</sup> <u>は、デフォルト</u>	<u>て下さい。</u> <u>~では CN が必須</u>	ок 	Cancel	Help	
(Certificate Subj ・ CN:Ciscoasa ・ O:Cisco System ・ C:US 証明書サブジェクト NetAttest EPS で(	s は必ず指定し <sup>-</sup> <u>は、デフォルト</u>	て下さい。 <u>~では CN が必須</u>		Cancel	Help X	
<ul> <li>(Certificate Subjaction of the second stress of the secon</li></ul>	s は必ず指定し <sup></sup> は、デフォルト	て下さい。 <u>へでは CN が必須</u> rollment mode parameters and St ertificate Parameters <u>Enrollmen</u>	CEP challenge passw t Mode SCEP Challe	Cancel ptions ord are not availab	Help ke for self-signed certificates.	
<ul> <li>(Certificate Subject of Control of Contr</li></ul>	s は必ず指定し <sup>-</sup> <u>は、デフォルト</u>	て下さい。 へでは CN が必須 rollment mode parameters and St ertificate Parameters Eurollment FQDN: Ciscossa	OK です。 Advanced O CEP challenge passw t Mode SCEP Challe	Cancel ptions ord are not availab nge Password	Help We for self-signed certificates.	
<ul> <li>(Certificate Subjaction of the second structure)</li> <li>・ CN:Cisco Systems</li> <li>・ C:US</li> <li>証明書サブジェクト</li> <li>NetAttest EPS では</li> <li>③ [FQDN]</li> <li>・ Ciscoasa</li> </ul>	s は必ず指定し <sup></sup> は、デフォルト	て下さい。 へでは CN が必須 へでは CN が必須 rollment mode parameters and St ertificate Parameters Enrollment	DK	Dancel	Help Ne for self-signed certificates.	
<ul> <li>(Certificate Subjaction of the second secon</li></ul>	s (は必ず指定し <sup></sup> <u>は、デフォルト</u>	C下さい。 へではCNが必須 rollment mode parameters and St ertificate Parameters Enrollment FQDN: Ciscossa E-mail: PAddress: Include serial number of the of	CEP challenge passw t Mode SCEP Challe	Dancel	Help         Ke for self-signed certificates.	
<ul> <li>(Certificate Subjation of the second structure)</li> <li>・ CN:Cisco Systems</li> <li>・ C:US</li> <li>証明書サブジェクト</li> <li>NetAttest EPS では</li> <li>③ 【FQDN】</li> <li>・ Ciscoasa</li> </ul>	s (は必ず指定し <sup></sup> t、デフォルト	て下さい。 へでは CN が必須 へでは CN が必須 ertificate Parameters and SG ertificate Parameters Enrollment FQDN: Ciscossa E-mail: IP Address: Include serial number of the c	DK	Dancel	Help         Vector         Vector         Interview         In	
<ul> <li>(Certificate Subjaction of the second structure)</li> <li>・ C:US</li> <li>証明書サブジェクト</li> <li>NetAttest EPS でに</li> <li>③ 【FQDN】</li> <li>・ Ciscoasa</li> </ul>	s (は必ず指定し <sup></sup> <u>は、デフォルト</u> [ [ [	C下さい。 へではCNが必須 rollment mode parameters and Sd ertificate Parameters Enrollment FQDN: Ciscossa E-mail: IP Address: IP Address:	DK	Dancel	Help ×	
<ul> <li>(Certificate Subja · CN:Ciscoasa</li> <li>· O:Cisco Systems</li> <li>· C:US</li> <li>証明書サブジェクト</li> <li>NetAttest EPS で(a)</li> <li>③ 【FQDN】</li> <li>· Ciscoasa</li> </ul>	ti必ず指定し <sup>-</sup> <u>t、デフォルト</u>	て下さい。 へでは CN が必須 へでは CN が必須 Prollment mode parameters and St ertificate Parameters Enrollment FQDN: Ciscossa E-mail: IP Address: Include serial number of the co	Advanced O CEP challenge passw t Mode SCEP Challe device	Dancel	Help	



上記設定終了後、『Add Certificate』ボタンをクリックし次の画面に進み、CSR を保存

#### します。保存場所へのパスはすべて英語表記にする必要があります。

<b>(</b>	Identity Certifica	te Request	×		
To complete the request (CSR) ar	enrollment process, please nd send it to the CA.	save the PKCS10 enrollmer	it		
You will then nee clicking the Insta	ed to install the certificate t Il button in the Identity Cer	hat is returned from the CA tificates panel.	by		
Save CSR to File	e: C:¥Users¥soliton¥Deskto	p¥ciscoasacsr.txt Bro	wse		
	OK Cancel	Help			
Ir The CS	nformation 2 SR was saved successfully.	マ Cisco.asa.csr.: テキスト ドキュン 1 KB	xt わト		
File View Tools Wizards Windo	Cisco /	ASDM 7.1 for ASA - 192.168.1.1	T	Type topic to search	_ <b>⊟</b> ×
Home Configuration Device Monitorin	g 🛄 Save 💽 Refresh 🕥 Back 🔘 Forward				CISCO
Uevice Management ■ Management Access ■ System Image/Configuration ■ Logging ■ System Image/Configuration ■ Logging	Configuration > Device Management > (           Issued To         Issued By           [Ciscoasa]         Not Available	Expiry Date         Associated Trustpoints           Pending         ASDM_TrustPoint0	Usage Unknown	Public Key Type	Add Show Details
Bill Users/AAA     Certificate Management     Certificate Management     Sector Contribution     Contributii     Contrib					Delete Export Install
🗄 🗒 Advanced	Eind: © © M	atch Case			



#### 4-2 サーバー証明書署名要求 (NetAttest EPS)

ASA 5505 で生成した CSR を基に NetAttest EPS で ASA 5505 のサーバー証明書を 発行します。NetAttest EPS の管理者向け証明書サービスページ(http://192.168.2.1 /certsrva/)にアクセスし、証明書要求を行います。下記の手順で CSR をインポートし ます。





### 4-3 サーバー証明書の発行 (NetAttest EPS)

サーバー証明書要求の承認・発行を行います。

CA 管理ページ(http://192.168.2.1:2181/caadmin/)にアクセスし、【保留】 状態のサ ーバー証明書を承認(発行)します。

要	求リス	ŀ					
状趙	態 保 細オブ	留のみ表示 ションの設定	▶ 更新				
	状態	受付日時	送信元	プロファイル/証明書目的	<u>申請者</u>	クライアント	
	保留	2017/12/18 14:45:34	CAadm: admin :Mozil	WEBサーバー証明書 (unknown)	unstructuredName=Ciscoa		確認
	拒否	削除	発行	● デフォルト 365 日 2018 ✔ 12 ✔ 18 ✔	14 💙 46 💙 18 💙 🕫	e	

•

VPN 接続を IP アドレスで行う際は、ASA のサブジェクト別名に使用する IP を 追加する必要があります。サブジェクト別名に IP アドレスが記載されてない場合、 SSL 通信が正常に行われません。



### 4-4 サーバー証明書のダウンロード (NetAttest EPS)

サーバー証明書をダウンロードするために再度、管理者向け証明書サービスページにア クセスします。証明書の確認を選択すると状態が【発行】になっていますので、サーバ ー証明書(nausercert-pem.cer)をダウンロードします。

NetAttest EPS	
■ 証明書サービス - EPS ROOT CA ■ CA情報	
■ ダウンロード	
□ 証明書要求	
57 00 db 74 57	
■要求一覧■	
状態 単請日 プロファイル 証明書目的 申請者	927
発行 2017/1 14:45:34 WEBサー (unknown) unstructuredName=	. インストール ダウンロード 削除
	•
	nausercert-pem.cer セキュリティ証明書 1.73 KB

### 4-5 CA 証明書の取得 (NetAttest EPS)

管理者向け証明書サービスページから、NetAttest EPS の CA 証明書をダウンロードします。CA 証明書は、PEM 形式(nacacert-pem.cer)を選択します。

NetAttest EPS		ロ <b>グオン中:</b> admin <b>・</b> トップページ <b>1</b> 閉じる
<ul> <li>証明書サービス - EPS ROOT CA</li> <li>CA情報</li> <li>ダウンロード</li> <li>証明書要求</li> <li>証明書確認</li> </ul>	<mark>ダウンロード</mark> CA証明書ダウンロード <u>PEM DER</u> <u>CA証明書インストール</u> CRLダウンロード <u>PEM DER</u>	▲ 199 - 9 - 199 - 1

### 4-6 CA 証明書のインポート (ASA 5505)

NetAttest EPS からダウンロードした CA 証明書(nacacert-pem.cer)を ASA 5505 に インポートします。

「Configuration」-「Device Management」-「Certificate Management」-「CA Certificates」の画面からインポートを行います。

<b>(</b>		Cisco	ASDM 7.1 for A	SA - 192.168.1.1		_ 8 ×
File View Tools Wizards Window	<u>H</u> elp				Type topic to search	Go altala
Home 🔏 Configuration 📴 Monitoring	GRefresh	Back 🕐 Forward	🦓 Help			CISCO
Device Management 2 9	<u>Configuration &gt; D</u>	evice Management >	Certificate Managem	nent > <u>CA Certificates</u>		
B B Licensing	I. IT	1 10	5 1 D 1	A	11	Add
▲ B Logging B Smart Call-Home	VeriSign Class 3	Issued By Se cn=VenSign Class	3 23:59:59 UTC Feb	Associated Trustpoints	General Purpose No	Flit
Users/AAA						Show Details
						Pogra + CPI
	Eind:		latch Case			<b>v</b>
		100		Install Certifi	cate	×
				Instan Ceran	cutc	
		Trustpoint	Name: ASI	DM_TrustPoint1		
		<ul> <li>Install</li> </ul>	from a file: C·¥	Users¥soliton¥Desktop¥nar	ace Browse	
				4.5		
		OPaste	certificate in PEN	A format:		
🛃 Device Setup						
🐔 Firewall						
Remote Access VPN						
Ste-to-Site VPN						
SO Device Management						
		Use SC	EP:			
		SCEF	URL: http://			
		Retry	Period: 1		minutes	
[Install From a f	filo]	Patra	Count		(Line O to indicate	(unlimited untrian)
(Instan From a l		Retry	Court: 0		(Use V to Indicate	uninnited retries)
<ul> <li>nacacert-nei</li> </ul>	m cer					
						More Options
			Install Cout	if anto	Hala	
			Install Cert	Cancel	Пеір	

次に、インポートした CA 証明書を選択し、CRL の設定をします。

Configuration > Device Management >	Certificate Management > CA Cert	ificates				
Issued To Issue	d By Expiry Da	te Associat	ed Trustpoints	Usage	Active	Add
EPS ROOT OA on EFF Ven Sign Class 3 Secure Server on PV	-5 ROOT OA, c=, P 052315 ( prSign Class 3 Public Prim 235959 (	JTC Pec 16 2027 ASDM T JTC Feb 7 2020 SmartC	ustPoint1 JIIHome_ServerCA	(General Purpose General Purpose	Yes No	Edit Show Jetails Request CRL Deste
		Edit O	ntions for CA Car	tificate		×
	Revocation Check CRL F Do not check certific Check certificates fo Revocation Methods Specify the meth method will be us OCSP	Retrieval Policy CRL Re rates for revocation r revocation s ods used for revocation ed only if the first one r	checking and their order etums error. Add> CRL CRL CRL CRL CRL CRL CRL CRL CRL CRL	ules Advanced	selected, the second Move Up Move Down	
		ОК	Cancel	Help		



## 4-7 サーバー証明書のインポート (ASA 5505)

NetAttest EPS で発行したサーバー証明書をインポートします。

「Configuration」-「Device Management」-「Certificate Management」-「Ident ity Certificates」の画面からインポートします。

			Cisc	co ASDM 7.1 for	r ASA - 192.168.1.1			- 🖻 ×
Ei	le <u>V</u> iew <u>T</u> ools Wi <u>z</u> ards <u>W</u> indov	v <u>H</u> elp					Type topic to search	<u>60</u>
đ	Home 🦓 Configuration 📴 Monitoring	Save 🚱 Refresh	🕒 Back 🔘 Forw	ard 🦻 Help				CISCO
st	Device Management	Configuration > De	evice Management	<u>t &gt; Certificate Mana</u>	gement > Identity Certificates			
8	Licensing	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
Devi	System Image/Configuration     Logging     Sweet Cell-Heree	[Ciscoasa]	Not Available	Pending	ASDM_TrustPoint0	Unknow	m	Show Details
	Users/AAA							Delete
	Gentity Certificates							Export
								Install
	Advanced	Find	00	Match Case				
		- Di ten						
		Public CA Enrollmen	t A cocurity coroliano	o up and pupping quick	ly with an SSL Advantage digital o	ortificato from En	taust Entrust offers Cisco a	rtomore a crocel
		promotional price	for certificates and	trial certificates for te	sting.		ulast. Entrast offers ofsoord	
					Enroll ASA SSL certificate with	Entrust		
		Using a previously	y saved certificate s	signing request, <u>enroll v</u>	vith Entrust.			
								↓ _ I
			_					
			3		Install Identit	y certifi	cate	×
						,		
			Identity Cert	tificate ——				
			Inetall	from a file:	VI. leare Vealitars VDaald		aut-nom cor	Bimuno
	💑 Device Setup		Instan	iroma nie.	-=Osers=sontori=Deski	op≢nausero	ert penn.cer	Drowse
	Firewall		🔵 Paste	the certificate	data in base-64 forma	it:		
	Cite=te=Site VDN							
	Device Management							
	S povice management							
_								
				Install Cert	tificate Cano	el	Help	
								<b>J</b>
					<b>F</b>	In	formation	×
						Conti	fianta import ouccou	-ded
						/ Certi	ncate import succee	aca.
						_		
							OK	
							UN	



## 5 ASA 5505の接続設定

### ASA 5505 の接続に関する設定の流れ

- 1. IP アドレスプールの設定
- 2. AAA サーバー(RADIUS サーバー)の設定
- 3. AnyConnect VPN Connection Setup Wizard



#### 5-1 IP アドレスプールの設定

AnyConnect を用いて SSL-VPN 接続に成功した VPN クライアントに対して、割り当てる IP アドレスプールを設定します。

「Configuration」-「Remote Access VPN」-「Network (Client) Access」-「Addr ess Assignment」の「Address Pools」で『Add』をクリックします。

[Add IP Pool]で割り当てる範囲の IP アドレスを指定します。





### 5-2 AAA サーバー(RADIUS サーバー)の設定

NetAttest EPS に問合わせる際のプロトコル等を指定します。

「Configuration」-「Remote Access VPN」-「AAA/Local Users」-「AAA Server Groups」の[AAA Server Groups]から設定します。

	Cisco ASDM 7.1	for ASA - 192.168.1.1		_ 6 ×
File View Tools Wizards Window	v <u>H</u> elp		Type topic to search	Go altalta
Home Configuration Monitoring	Save 🔇 Refresh 🔾 Back 💭 Forward 🤶 Help			cisco
Hemote Access VPN	Configuration > Remote Access VPN > AAA/Local L	Jsers > AAA Server Groups		
Information of Access     Information of Access     Information Science S	AAA Server Groups Server Group Protocol Accounting Mode Reacti LOCAL LOCAL End © © Match Case Servers in the Selected Group Server Name or IP Address Interface Timeout	vation Mode Dead Time Max Faik	d Attempts	Add Ed t Del te Del te Ed t Ed t Del te Move Down Tert
CAA Carter Content Co	End End DAP Attribute Map A Server Group] haeps(任意) counting Mode] Single	Add AAA Server Group: Protocol: Accounting Mode: Reactivation Mode: Dead Time: Max Failed Attempts Enable interim acc Enable Active Di VPN3K Compatibilit	AAA Server Group	
			Vancel Help	





次に、[Servers in the Selected Group]で RADIUS サーバーとして NetAttest EPS を指定します。

Cisco	D ASDM 7.1 for ASA - 192.168.1.1	_ 8 ×
File View Tools Wizards Window Help	Type topic to search	Go ululu
Home Configuration Monitoring Save C Refresh C Back Forwar	rd ? Help	cisco
Introduction     AAA Server Groups	/ MAY LOGILOBOIS / MAY OF VOLUTION	
Generitess SSL VFN Access     Generitess Server Group Protocol Accountin     AAA/Local Vers	ng Mode Reactivation Mode Dead Time Max Failed Attempts	Add
Add Sanver Groups     Course     Course	Depletion [10 ]3	Eait Delete
Eind 🛛 🛇 👄 🗌	Match Case	
Servers in the Selected Group		
Server Name or IP Address Interface	e Timeout	Add
	Match Case Apoly Reset Kadmin> 15   @ Mai   @	Ec t Del te Move Up Move lown Te t
		<u> </u>
	C Add AAA Server	×
[Interface Name]	Server Group: naeps	
• inside	Interface Name: inside 🗸	
[Server name or IP Address]	Server Name or IP Address: 192.168.1.2	
	Timeout: <u>10</u> seconds	
· 192.168.1.2	RADIUS Parameters	
[Server Authentication Port]	Server Authentication Port: 1812	
· 1812	Retry Interval: 10 seconds	

[Server Accounting Port]

· 1813

[Server Secret Key]

 $\cdot$  secret

Interface Name:	nside 🗸
Server Name or IP Address: 1	92.168.1.2
Timeout:	10 seconds
RADIUS Parameters	
Server Authentication Port:	1812
Server Accounting Port:	1813
Retry Interval:	10 seconds 🗸 🗸
Server Secret Key:	•••••
Common Password:	•••••
ACL Netmask Convert:	Standard 🗸
Microsoft CHAPv2 Capable:	
SDI Messages	
Message Table	۲
ОК	Cancel Help
	次ページへ



### 5-3 AnyConnect VPN Connection Setup Wizard

AnyConnect(SSL-VPN)の接続プロファイルを作成します。

「AnyConnect VPN Wizard」を利用し、プロファイルを作成します。

<b>11</b>		Cisco ASDM 7.1 for ASA - 192 168 1 1	_ <b>_</b> ×
File View Tools Wizard	ts Window Help		Type topic to search Go
Home Configu Sta	rtup Wizard	Forward ? Help	CISCO
Remote Access V VPI	V Wizards	Site-to-site VPN Wizard	
Introduction	h Availability and Scalability Wizard	AnyConnect VPN Wizard	
Clientless SS	fied Communication Wizard	Clientles: SSL VPN Wizard	ed Attempts Add
	ket Capture Wizard	IPsec (Ik Ev1) Remote Access VPN Wizard	Edit
- A LDAP Attribute Ma	ap naeps RADIUS Sin	gle  Depletion  10  3	Delete
Host Scan Image	ager		
🗄 🖽 Certificate Managem 😼 Language Localizatio	ent n		
DHCP Server			
		↓	
	AnyConnect VPN Connec	tion Setup Wizard	
VPN Wizard	Introduction		
Branch			
	Use this wizard to configure the AS/ Am/Connect VPN Client The conne	to accept VPIN connections from the ctions will be protected using either the IPsec	
EST ISP	or the SSL protocol. The ASA will a	utomatically upload the AnyConnect VPN	
	Client to the end user's device when	a VPN connection is established.	
Home		/PN Remote Access	
Corporate Network	Local	Remote	
rectifier ve			
TITA	1		
1 I III	1		
E C			
	< Back Next >	取消 Help	
			-
<b>[</b> ]	AnyConnect VPN Connect	ion Setup Wizard	
Steps	Connection Profile Identification		1
2. Connectio 🔥	This step allows you to configure a C	connection Profile Name and the Interface the	
Profile	remote access users will access for	VPN connections.	
	Connection Profile Name: soliton ar	voonnect	
3. VHN Protoc	control of the field of the fie	g ees a re eq	
4. Client Image	VPN Access Interface: outside	$\checkmark$	
5. Authenticat Methods			
6. Client Addre			[Connection Profile Name]
Assignment			· soliton anyconnect
7. Network Na Resolution			jointon_anyconnect
Servers			[VDN Accoss Interface]
8. NAT Exemp			TVFIN ACCESS INTELLACE
9. AnyConnec			
Client Deplc 🗸			·outside
	< <u>B</u> ack <u>N</u> ext>	取消  Help	



<b>(</b>	AnyConnect VPN Connection Setup Wizard	1
Steps Jeenunicauo 3. VPN Proto 4. Client Image 5. Authenticat Methods 6. Client Addre Assignment 7. Network Na Resolution Servers 8. NAT Exemp 9. AnyConnec Client Depk	VPN Protocols         AnyConnect can use either the IPsec or SSL protocol to protect the data traffic.         Please select which protocol or protocols you would like this connection profile to support.         IPsec         Device Certificate         Device Certificate identifies the ASA to the remote access clients. Certain AnyCon features (Always-On, IPsec/IKEv2) require that valid device certificate be available the ASA.         Device Certificate:       None         Mar	【VPN Protocols】 ・SSL 【Device Certificate】 ・インポートした サーバー証明書を選択
10. Summary 🗸	ASDM_TrustPoint0 hostname=Ciscoasa, cr=Ciscoasa, TrustPoint: ASDM_TrustPoint0     < ASDM_TrustPoint0   Issued To: hostname=Ciscoasa, or Sister Ciscoasa, cr=Ciscoasa, cr=C	n=Ciscoasa, o=Cisco Systems, c=US
Steps Derrance au 3. VPN Protoc 4. Client Ima 5. Authenticat Methods 6. Client Addre Assignment 7. Network Na Resolution Servers 8. NAT Exemp 9. AnyConnec Client Depk 10. Summary	AnyConnect VPN Connection Setup Wizard Client Images ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network. A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.  Add I Replace Delete t  Regular expression to match user-agent Gisk0/anyconnect_win=42 01035-49  You can download AnyConnect Client packages from Clisco by searching 'AnyConnect VPN Client' or click here.  Explant Replace Delete the Regular expression to match user-agent	【Add】ボタンから、クライアントイ メージ[Any Connect pkg ファイル] を選択
	pkg ファイル(クライアント用 AnyConnect トしなければ、AnyConnect を受付ける Inte ージョンを取得するには cisco.com でダウン	ソフトウェアイメージ)をインポー erface が有効になりません。 最新バ ロードして下さい。
C Steps	AnyConnect VPN Connection Setup Wizard	



【AAA Server Group】 ・作成済みの[naeps]を指定



	AnyConnect VPN Connection Sotup Wizard X	1
Steps Jeenuncaue 3. VPN Protoc 4. Client Image 5. Authenticat Methods 6. Client Adc Assignmer 7. Network Na Resolution Servers 8. NAT Exemp 9. AnyConnec Client Depk 10. Summary	Client Address Assignment         This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect.         IPv6 address pool is only supported for SSL connection.         IPv4 Address Pool IPv6 Address Pool         Address Pool: pool-sample         New         Details of the selected address pool         Starting IP Address:         192.168.1.200         Subnet Mask:         255.255.255.0	【IPv4 Address Pool】 作成済みの IP アドレスプー ルを指定
	〈Back Next〉 取消 Help	
Steps Juernuncauu 3. VPN Protoc 4. Client Image 5. Authenticat Methods 6. Client Addre Assignment 7. Network N Resolution Servers 8. NAT Exemp 9. AnyConnec Client Deple 10. Summary	AnyConnect VPN Connection Setup Wizard       ×         Network Name Resolution Servers       This step lets you specify how domain names are resolved for the remote user when accessing the internal network.         DNS Servers:       192.168.1.20         WINS Servers:       Domain Name:         Domain Name:       example.local	【DNS Servers】 ・DNS のアドレスを指定
Steps Juernumcauo 3. VPN Protoc 4. Client Image 5. Authenticat Methods 6. Client Addre Assignment 7. Network Na Resolution	AnyConnect VPN Connection Setup Wizard × NAT Exempt If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation. Exempt VPN traffic from network address translation	IVAT Exempt] ・チェックなし
8. NAT Exem 9. AnyConnec Client Depk 10. Summary ↓	< Back Next > 取消 Help	



	AnyConnect VPN Conne	ection Setup Wizard
Steps	AnyConnect Client Deployment	
3. VPN Protoc	AnyConnect client program can b following two methods:	e installed to a client device by one of the
4. Client Image 5. Authenticat Mathada	1) Web launch - On accessing the client package will be automatica	ASA using a Web Browser, the AnyConnect Ily installed;
6. Client Addre Assignment	2) Pre-deployment - Manually ins	tall the AnyConnect client package.
7. Network Na Resolution Servers		
8. NAT Exemp		
9. AnyConne Client Deploymer		
10. Summary 🗸		
	< Back Next >	取消  Help
VPN Wizard	AnyConnect VPN Conne	ction Setup Wizard
Branch	Summary Here is the summary of the configu	uration.
ISP ISP	Name	Value
Corporate	Summary Name/Alias of the Connection . VPN Access Interface	soliton_anyconnect
Network	Device Digital Certificate	ASDM_TrustPoint0:hostname=Ciscoasa,
A DOTATION	VPN Protocols Enabled	SSL only
	AnyConnect Client Images	1 package
Tall	Authentication Server Group	naeps 1921681150 - 1921681200
TH	DNS	Server: Domain Name:
6	Network Address Translation	The protected traffic can be subjected to network address translation





作成された[Connection Profiles]を『edit』から編集します。

[AAA Server Group]には、先程作成した[AAA Server Group]を選択します。

	Cisco ASDM 7.1 for ASA - 192.168.1.1		- 8 ×
File View Tools Wizards Window Help	K S Forward ? Help	I ype topic to search	CISCO
Remote Access VPN # Configuration > Remote A	cess VPN > Network (Client) Access > AnyConnect Connection Profiles		0
<ul> <li>The security accelerates and accelerates and accelerates and accelerates acc</li></ul>	Initial digelogs the Cisco AnyConnect VFN Client to remote users upon connection. The initial client deployment requires end-user administra Li turnel with Datagram Transport Layer Security (DTL5) turneling options. et VFN Client access on the interfaces selected in the table below all fyou allow AnyConnect client to be launched from a torware (Meb Launch). Piece (IREV) Access insteh DT	Group Policy OfficiePolicy DifficiePolicy DifficiePolicy Childrefolicy C	zend
Edit AnyCon	nect Connection Profile: soliton_anyconnect		
Name: Advanced Name: Aliases: Automistic Method: AAA Server Group: Client Address Assignm DHOP Servers: Client Address Pools Client IPv6 Address I Default Group Policy Group Policy (Following field is an : ♥ Enable IPsed(II DNS Servers: Domain Name: e	soliton_anyconnect soliton_anyconnect AAA Certificate EctH naeps V Manage Use LOCAL if Server Group fails ant None OHCP Link OHCP Subnet pool-sample Select IPV6 address pool is only supported for SSL GroupPolicy_soliton_anyconnect V Manage ttribute of the group policy selected above.) N client protocol EV2) client protocol 22.1681.20 xample.local	I be used (Method) • Both (AAA Server ( • naeps	2/18601-44 UTO
	OK Cancel Help		



## 6 Windows 版 AnyConnect の設定

## AnyConnect VPN クライアントの設定

- 1. PC へのデジタル証明書のインストール
- 2. Windows版 AnyConnectの設定



#### 6-1 PC へのデジタル証明書のインストール

PC にクライアント証明書をインポートします。

ダウンロードしておいたクライアント証明書(user01\_01.p12)をダブルクリックする と、証明書インポートウィザードが実行されます。

user01_01.p12	
$\checkmark$	
× ◎ 参 証明書のインボート ウィザード	
証明書のインボート ウィザードの開始	
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。	【現在のユーザー】を選択
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護されたやトワーウ接続を提供するための情報を含んでいます。証明書人アは、証明書が保護されるシステム上の領域です。	
<ul> <li>● 現在のユーザー(C)</li> <li>○ ローカル コンピューター(L)</li> </ul>	
統行するには、[次へ]をクリックしてください。	
次へ(N) キャンセル	
•	
× C 参 証明書のインポート ウィザード	
インボートする証明書ファイル インボートするファイルを指定してください。	
ファイル名(F):	
C:¥UsersYsoliton¥DesktopYuser01_01.p12 注意:次の形式を使うと1つのファイルに複数の証明書を保管できます:	
Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)	
Microsoft シリアルルとされた証明書ストア (.SST)	
次へ(N) キャンセル	

## Seliton





#### 6-2 Windows版 AnyConnectの設定

Cisco AnyConnect VPN クライアントを Cisco.com もしくは ASA ユーザーサービス ページからダウンロードし、インストールします。ASA ユーザーサービスからダウンロ ードする場合は、本環境では http://192.168.2.2/にアクセスして下さい。 AnyConnect をインストールすると[タスクトレイ]に アイコンが表示されます。 クリックすると以下の画面が表示されますので、接続先の ASA を指定します。 AnyConnect のバージョンによって表示される画面構成は異なる場合があります。

🕒 Cisco Any	Connect Secure Mobility Client 🗕 🗖	×
	YPN: Ready to connect.	
_	192.168.2.2 V Connect	
<b>\$</b> (i)		cisco



## 7 iOS 版 AnyConnect の設定

## AnyConnect VPN クライアントの設定

- 1. iPhone へのデジタル証明書のインストール
- 2. iOS版 AnyConnectの設定



#### 7-1 iPhone への VPN 用デジタル証明書のインストール

NetAttest EPS から発行した VPN 用デジタル証明書を iOS デバイスにインストールする方法として、下記 4 つの方法などがあります。

1)NetAttest EPS-ap を使い、SCEP で取得する方法

2)Apple Configurator2(構成プロファイル)を使う方法

3) デジタル証明書をメールに添付し iOS デバイスに送り、インストールする方法

4)HTTP アクセス可能なサーバーに証明書をアップロードして、インストールする方法

上記いずれかの方法で CA 証明書とユーザー証明書をインストールします。

本手順では証明書のインポート方法については割愛いたします。

▶ iOS 10 以降の OS 仕様上 ROOT 証明書をインポートする場合、 手動でインポートした証明書を信頼させる必要があります。

証明書をメール添付して iOS デバイスに送りインストールする方法は、 Legacy AnyConnect にのみ適用されます。 (Legacy AnyConnect は iOS12 以降 では利用できません。)

新しい AnyConnect の場合は以下の様な方法があります。

- Web サーバーに証明書をアップロードし、 ダウンロード URL を用いてインポー トを行う方法
- メール添付等で iOS デバイスに送った証明書を iOS の「システム共有機能」を 利用しインポートを行う方法
- EPS-ap で証明書配布時に、VPN プロファイルも配布する方法

VPN 設定	
_	
	VPN
接続名	VPN 構成
VPNサーバー	
接続のタイプ	Cisco AnyConnect
グループ	IPSec (Cisco)
	Cisco AnyConnect (Legacy) Cisco AnyConnect
*	Juniper SSL Pulse Secure
該当するドメインまたはホス	F5 SSL SonicWALL Mobile Connect
	常に確立 ▼    追加

EPS-ap プロファイル管理ページの[プロファイル]-[VPN]-[接続タイプ]



### 7-2 iOS 版 AnyConnect の設定

Cisco AnyConnect VPN クライアントを Apple App Store からインストールします。 インストール後アプリを起動し、AnyConnect の設定を行います。 下記のように接続先と認証に使うデジタル証明書をインポートし、 VPN の設定を行います。

(本手順書は CiscoAnyConnect for iOS V4.0.0 を基準で作成されています。)

#### 7-2-1.AnyConnect VPN の基本設定



1. AnyConnect 起動 【接続】タップ。

▲ AnyConnect VPN接続	16:44			<b>?</b> 🔳
VPN接続の追加	AnyConr	nect VPN	接続	
VPN接続の追加				
A A CI O	VPN接	続の追加		
A A D				
A A D				
<b>^ \</b>				
<b>^ \</b>				
<b>^ * 0 0</b>				
<b>^  • • •</b>				
n 🔅 🖸 O				
A & D 0				
<b>^</b> * 🖸 O				
			_	-
	<b>而</b> ホーム	RR.	1917	1/1-ジョン情報

 2.【VPN 接続の追加】を タップ。

キャンセル       VPN接続の追加       保存         説明       CiscoASA       ・         サーバ       192.168.2.2       ・         詳細       ・       ・         1       2       3       4       5       6       7       8       9       C         (@       &       %       ?       ,       =       [       1         #+=        :       -       +       <          ABC       (()       ,       /       jp       Done	16:45				. ? •
説明 CiscoASA サーバ 192.168.2.2 ・ の 詳細 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	キャンセル	VPN接線	の追加		保存
サーパ       192.168.2.2       ●         詳細       →       →         1       2       3       4       5       6       7       8       9       C         @       &       %       ?       ,       =       [       1         #**        :       -       +       <	説明	CiscoA	SA		
詳細 1 2 3 4 5 6 7 8 9 C ② & % ? , = [ ] #++ : - + 交 ABC 健 . / jp Done	サーバ	192.16	8.2.2		$\odot$
1 2 3 4 5 6 7 8 9 C @ & % ? , = [ ] #*= _ : - + ≪ ABC ∰ . / jp Done	詳細				>
1 2 3 4 5 6 7 8 9 C @ & % ? , = [ ] #+= _ : - + ≪ ABC ∰ . / jp Done					
1 2 3 4 5 6 7 8 9 0 @ & % ? , = [ ] #** _ : - + ≪ ABC ∰ . / jp Done					
1     2     3     4     5     6     7     8     9     C       @     &     %     ?     ,     =     [     1       #+     _     :     -     +     <					
1     2     3     4     5     6     7     8     9     C       @     &     %     ?     ,     =     []     ]       #+=     _     :     -     +     <					
1     2     3     4     5     6     7     8     9     C       @     &     %     ?     ,     =     [     ]       #+*     _     :     ·     +     <       ABC     ⊕     .     /     .jp     Done					
@ & % ?     , =     []       #+=     _     :     -     +     <					
#+= _ : - + <∑ ABC ⊕ . / jp Done	123	4 5	67	8	9 0
ABC	123	45%?	67	8	90
	123	45 %?	67,	8 = [ +	90
	1 2 3 @ & #+=	4 5 % ? :	67	8 = [ +	9 0 ] 

- 3.VPN 接続の追加
  [説明]
  ・任意(CiscoASA)
  【サーバー】
  - ・ASA のアドレス(192.168.2.2) 【保存】ボタンで設定保存。

## 8 Android OS 版 AnyConnect の設定

## AnyConnect VPN クライアントの設定

- 1. Android 端末への VPN 用デジタル証明書のインストール
- 2. Android 版 AnyConnect の設定(基本設定、ユーザー証明書インポート)



#### 8-1 Android 端末への VPN 用デジタル証明書のインストール

NetAttest EPS から発行したデジタル VPN 用ユーザー証明書を Android デバイスに インストールする方法として、下記 3 つの方法などがあります。

1)NetAttest EPS-ap を使い、SCEP で取得する方法
 2)デジタル証明書をメールに添付し Android デバイスに送り、インストールする方法
 3)HTTP アクセス可能なサーバーに証明書をアップロードして、インストールする方法

上記いずれかの方法で Android OS の「VPN とアプリ」に CA 証明書とユーザー証明書 をインストールします。

本手順では証明書のインポート方法については割愛いたします。

Android 用の AnyConnect アプリの仕様で、ユーザー証明書を Android OS の「VPN とアプリ」にインストール後、AnyConnect 上で別途インポートする必要があります。



### 8-2 Android OS版 AnyConnect 設定

Cisco AnyConnect VPN クライアントを Google Play Store からインストールします。 インストール後、アプリを起動し、AnyConnect の設定を行います。

下記のように接続先と認証に使うデジタル証明書をインポートし、

VPN 設定を行います。

(本手順書は CiscoAnyConnect for Android V4.0.09039を基準で作成されています。)

#### 8-2-1. AnyConnect VPN の基本設定

■ × ▼ ▼	🖨 マ 🖹 🗎 15:09
S AnyConnect	1 ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (
AnyConnect VPN 接続解除済み	オフ
接続 接続なし	
詳細	
սիսիս	
cisco	

1.AnyConnect を起動。



2. [Add New VPN Connection]をタップ。

<ul> <li>☆ 接続エディタ</li> <li>説明 CISCO</li> </ul>	
説明 CISCO	
CISCO	
サーバ	
192.168.2.2	
Advanced Preferences	
正治自てノロドゴルの時間の	AE 'E (M, 3E
キャンセル	完了

3.接続エディタ
[説明]
・CISCO(任意)
[サーバー]
・ASA の IP を入力
【保存】ボタンで設定保存 。



## 8-2-2 AnyConnect にユーザー証明書のインポート

		$\phi \blacklozenge \mathbb{R}$	û 17:44
NHYCONNECT			1
🔒 パーチャルプライベート	ネットワーク		
AnyConnect VPN 接続解除済み		オフ	
接続 CISCO			
詳細			
il c	ı.ılı. Isco		
Φ	0		

1. AnyConnect を起動 【接続】をタップ。



4.下段の【Import】を タップ。



8-2-1 で作成した
 【CISCO】を長押しし、
 【接続を編集】ボタンを
 タップ。



- 3. 【証明書】をタップ。

5.【デバイスクレデンシャル ストレージ】 をタップ。



【証明書の選択】で
 8-1 でインストールした
 証明書を選択し、
 【許可】ボタンをタップ。



無効	証明書 user01
自動 user01 统行于 EBS PODT CA	IPsecを使って接続 接続にはSQIではなくIPsecが使用されます。IPsecパラ メータの詳細については、I評種皆細の下のメニューを 参照してたざい。
26.5% 有効期限: 12/18/2018	認証 EAP-AnyConnect
	IKE ID 未設定
証明書バンドルが正常にインポート	
import	キャンセル 完了
	< 0 □

タップ。

完了。



## 9 接続の確認

#### 9-1 PC における AnyConnect を利用した SSL-VPN 接続

Cisco AnyConnect VPN クライアントを利用し、VPN 接続を行います。

Cisco AnyConnect Secure Mobility Client –	[VPN] • 192.168.2.2
S Cisco AnyConnect   192.168.2.2	[Group]
Please enter your username and password.	Soliton_anyconnect
Group: soliton_anyconnect v	[username]
Username: user01	• user01
Password:	[password]
OK Cancel	• password
	<b>〕</b> 【Group】には Connection Profile Name を指定。

AnyConnect 接続が完了すると、タスクトレイのアイコンが表示され、 IP アドレスプールから IP アドレスが払い出されます。





#### 9-2 iPhone における AnyConnect を利用した SSL-VPN 接続

Cisco AnyConnect VPN クライアントを利用し、VPN 接続を行います。 AnyConnect アプリを起動し、「接続」で作成済みの接続プロファイルを選択し、「Any

Connect VPN」をONにします。



1. 【接続】 ·CiscoASA

15:24		<b>?</b> 🗖
キャンセル	認証	接続
ユーザ名と/	《スワードを入力します。	
グループ:	soliton_any	connect >
ユーザ名:	user01	
パスワード:	1	
		Ŷ
q w e	ertyu	i o p
a s	d f g h j	k I
φZ	x c v b n	m 🗵
.?123	space	Done

- 2. [Group]
  - soliton\_anyconnect
     [username]
  - user01
    - [password]
  - password



3. 【詳細】で IP 払い出し情報 確認可能。



#### 9-3 Android 端末で AnyConnect を利用した SSL-VPN 接続

Cisco AnyConnect VPN クライアントを利用し、VPN 接続を行います。

AnyConnect アプリを起動し、「接続」で作成済みの接続プロファイルを選択し、「Any Connect VPN」を ON にします。



1.【接続】 ·Cisco

	<u></u>		0 7	15:12
Any	Connect			
ユーザ: A グルー:	名とパスワー ブ:	ドを入力しま	!す。	
solite ユーザ:	on_anyconn 8:	ect		-4
c user パスワ・	01 - ド:			- 8
ま ・・・・・・・  パフロードを表示します				
			1002	-1
	キャンセル	_	按机	-
4	@/	ABC	DEF 3	×
۹	GHI 4	JKL 5	MNO 6	►
?123 😳	PQRS	TUV	WXYZ	
க்க	a⇔A	'":; 0	.,?!	e
		0		

- 2. [Group]
  - soliton\_anyconnect
     [username]
  - user01
  - [password]
  - password

		🖨 🗣 😭 🖹 🛔 15:13
AnyConnect		1
VIRTUAL PRIVATE	NETWORK	
AnyConnect VPN 接続済み		オン
接続 CISCO		
詳細		
	uluilu cisco	
$\triangleleft$	0	

3. 【詳細】で IP 払い出し情報 確認可能。



## 改訂履歴

日付	版	改訂内容
2012/03/30	1.0	初版作成
2013/08/13	1.1	誤表記修正
2018/1/22	1.2	設定内容を ASA 5505 にあわせて更新
2018/10/31	1.3	誤表記修正