

プライベート認証局Gléas ホワイトペーパー

Pulse Connect Secure

クライアント証明書による認証設定

Ver.2.1 2019 年 1 月

- JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式 会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキ ュリティ・ソリューション・システムズの商標です。
- その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

Copyright by JCCH Security Solution Systems Co., Ltd. All Rights reserved

目次

1. はじ	めに	
1.1.	本書について	4
1.2.	本書における環境	4
1.3.	本書における構成	5
1.4.	証明書発行時における留意事項	6
2. Conr	nect Secure の設定	6
2.1.	信頼するルート認証局の設定	6
2.2.	サーバ証明書の設定	8
2.3.	認証サーバの設定	
2.4.	ロール(ユーザ権限)の作成	
2.5.	レルム(ユーザ認証)の作成	
2.6.	サインインポリシの設定	
2.7.	Location Awareness の設定	
3. Gléa	s の管理者設定(PC)	17
4. PC 7	での接続操作	
4.1.	クライアント証明書のインポート	
4.2.	クライアントからの VPN 接続(PC)	
5. Gléa	s の管理者設定(iPad)	
5.1.	UA(ユーザ申込局)設定	
6. iPad	での接続操作	
6.1.	Pulse Secure のインストール	22
6.2.	クライアント証明書のインポート	23
6.3.	OTA エンロールメントを利用した証明書発行について	25
6.4.	Pulse Secure から接続	25
7. オン	ボーディングを利用した証明書配布	27
7.1.	Gléas での SCEP サーバの利用開始設定	
7.2.	Connect Secure での設定	27
8. 問い	合わせ	

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベート認証局Gléas」で発行したクライアント証明書 を利用して、Pulse Secure社のSSL-VPN装置「Pulse Connect Secure」を利用し てのトンネリング接続を行う環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あら ゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構 築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な 場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- Pulse Connect Secure (バージョン8.3R3 (build 59199))
 ※以後、「Connect Secure」と記載します
- JS3 プライベート認証局Gléas (バージョン1.16.9)
 ※以後、「Gléas」と記載します
- クライアント: Windows 10 Pro / Internet Explorer 11
 ※以後、「PC」と記載します
- ▶ クライアント: iPad Air2 (iOS 11.2.6) / Pulse Secure (バージョン6.5.2.74525)
 ※以後、「iPad」と記載します
 ※本書記載の内容は他のiPadシリーズやiPhone・iPod touchにも適用できます

以下については、本書では説明を割愛します。

- Connect Secureでのサーバ証明書設定やネットワーク設定、アクセス権限等の設定
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- PC・iPadでのネットワーク設定等の基本設定
- Pulse Secureクライアントのインストール方法

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



- Gléasは、Connect Secureにサーバ証明書を、PCとiPadにクライアント証明 書を発行する
- 2. Connect Secureに発行されたサーバ証明書を設定する
- 3. PCとiPadは、Gléas(UA)よりクライアント証明書をインポートする
- 4. Pulse Secureに、クライアント証明書を使ってVPNアクセスをする

2.7項では、Connect SecureのLocation Awareness機能を利用したPCでのVPN自 動接続について記載します。



※5.1項の[Pulse Secure SSL-VPNの設定]で、[オンデマンド接続先]を設定することによりiPadでもVPN自動接続を行うことが可能です

7項では、Connect Secureのデバイスオンボーディング機能を利用した証明書配 布について記載します。



1.4. 証明書発行時における留意事項

Gléasで電子証明書を発行する際に以下の点に留意する必要があります。

 本書2.2の方法でサーバ証明書を発行する場合は、事前にサーバアカウント を作成しておく必要があります。

2. Connect Secureの設定

2.1. 信頼するルート認証局の設定

今回利用するクライアント証明書のトラストアンカとなるルート認証局を設定しま す。

あらかじめ Gléas よりルート証明書をダウンロードしておきます。

Gléas に http://hostname/ (http であることに注意)でアクセスすると、ダウン ロードが可能です。



管理者画面左側のメニューより[Configuration] > [Certificates] > [Trusted Client CAs]と進み、右側に出現する[Import CA Certificate…]ボタンをクリックします。

Configuration Certificates							
Security Certificates	DMI Agent	NCP	Sensors	Client Types	Pulse		
Device Certificates Trusted	Client CAs Tru	isted Ser	ver CAs Co	de-signing Certifica	tes Cli		
Users can be required to	present valio	d client	-side certif	icates to sign ir	n(see th		
Auto-import options	Proxy Setting	6 I	mport CA Ce	ertificate De	elete		

[Import From:]のところで[参照]ボタンを押し、ローカルに保存してあるルート証 明書を選択し、[Import Certificate]ボタンをクリックします。

Certificate file		
	Import from: C:\Temp\ia1.cer	参照
Import Trusted Cl	ient CA?	

成功すると以下のような画面が現れます。



失効リスト (CRL) を利用したクライアント証明書の失効確認をおこなう場合は、 Client certificate status checking 項目で、[Use CRLs (Certificate Revocation Lists)]を選択します

Client	certificate status checking
	O None
	O Use OCSP (Online Certification Status Protocol)
	 Use CRLs (Certificate Revocation Lists)
	O Use OCSP with CRL fallback
	O Inherit from root CA

ここで一度[Save Setting]をクリックして、設定を保存します。

その後、画面最下部にある CRL Setting の項目で、[CRL Checking Options…]をクリックします。

CRL Checking Option の設定画面に移動しますので、以下の設定をおこないます。

- [Use:]のドロップボックスより[Manually Configured CDP]を選択
- Primary CDP の[CDP URL]に CRL 配布ポイントとなる URL を入力
 ※CRL 配布点が複数ある場合は、Backup CDP を設定します

以下は Gléas が http で公開している CRL を取得する場合の設定例となります。

L Distribution Points (C	DP)
Use: Manually cor	ifigured CDP
Specify a HTT enter the app	or LDAP-based CDP, and an optional backup CDP if the primary CDP is not accessible. If the CDP requires authentication, ropriate ordentials as well.
Primary Cl	q
CDP URL:	http://
	HTTP example: http://server.domain.com/839/domaincaserver.cd/ LDAP example: Idap.//Idap.domain.com/6000/CN=Idap.CN=CDP.CN=Public Key Services,CN=Services,CN=Configuration,DC=domain,DC=com7 certificateRevocationListYbase/Sobjectdass=CAIDistributionPoint
Admin DN:	(LDAP only)
Password:	(LDAP only)

また CRL の取得間隔を指定したい場合は、Options 項目で[CRL Download Frequency]を指定することにより可能です。

以下は CRL の有効期限に関係なく、24 時間毎に CRL を取得する場合の設定例です。

opuons			
CRL	Download Frequency:	24	hours (1-9999)

設定終了後、[Save Setting]をクリックして設定を保存してします。 遷移した画面の CRL Setting の Status 欄に Enabled と表示されます。

CR Cert enal	L Settings ificate revocation lists (CRL) are used to verify the ongoing validity of client-side or ple CRL checking, click CRL Checking Options, and specify the options.	ertificates, ar	nd are obtained from CRL d	istribution points (CDP). To
	CRL Checking Options Update Now Enable Disable			
	CRL distribution points	Status	Last Updated	Next Update
	http://demo.jcch-sss.com/crl/ia1.crl Last result: Success, new CRL	Enabled; ok: 9KB, 189	2016/01/11 11:31:52 [Save CRL]	2016/02/10 00:50:43

2.2. サーバ証明書の設定

管理者画面左側のメニューより[Configuration] > [Certificates] > [Device Certificates]と進みます。その後、[New CSR...]をクリックし証明書署名要求(CSR) を発行します。

New CSR	Delete
Certificate	Signing Requests

ホスト名など、必要事項を入力し[Create CSR]をクリックします。 以下はRSA2048ビットの鍵長でCSRを作成する例です。 ※1024ビットは現在推奨されない鍵長となるので、それ以上の鍵長にすることを推奨します ※Gléasでは、3072ビットの鍵長はサポートされないため2048を選択します

Configuration > New Certificate Signir	ng Request
Use this page to create a new	v Certificate Signing Request (CSR) to send to your Certificate Authority of choice
Common Name: (e.g., secure.company.com)	pulse-test.jcch-sss.local
Organization Name: (e.g., Company Inc.)	JS3
Org. Unit Name: (e.g., IT Group)	
Locality: (e.g., SomeCity)	
State (fully spelled out): (e.g., California)	
Country (2 letter code): (i.e., US)	
Email Address:	
Key Type:	● RSA ○ ECC
Key Length:	2048 🗸 bits
Please enter some random cl We recommend that you ent	naracters to augment the system's random key generator. er approximately twenty characters.
Random Data: (used for key generation)	••••••
	Croate CSP

CSRの生成がおこなわれます。

ur CSR was o	created su	ccessfully. S	ee below for in	structions on s	ending the C	SR to a Cert	ificate Autho	ority.
e certificate a thority, you	approval p will need t	rocess may o import the	take several da certificate to o	ays. When you complete this p	receive the s rocess.	signed certifi	icate from th	ne Certificate
guration >								
nding Cer	tificate	Signing R	lequest					
nding Cer CSR Detail	tificate Is	Signing R	lequest					
nding Cer CSR Detail	tificate Is e: pulse-test.	Signing R	lequest					
guration > nding Cer CSR Detail Common Name Created:	tificate ls :: pulse-test. 1/11/2016	Signing R	lequest					
CSR Detail Common Name Created:	tificate ls : pulse-test. 1/11/2016 153	Signing R jcch-sss.local 12:24:5	equest					
guration > nding Cer CSR Detail Common Name Created: Org. Name: Org. Linit Name	tificate ls : pulse-test. 1/11/2016 JS3	Signing R jcch-sss.local 12:24:5 Locality: State:	equest					
guration > nding Cer CSR Detail Common Name Created: Org. Name: Org. Unit Name Email Address:	tificate ls : pulse-test. 1/11/2016 JS3 e:	Signing R jcch-sss.local 12:24:5 Locality: State: Country:	lequest					

画面下部のテキストエリアにCSRが表示されます。 この内容をテキストファイルに保存します。



Gléas (RA) にログインし、該当のサーバアカウントのページへ移動します。 小メニューの[証明書発行]をクリックします。



上級者向け設定を展開し、以下の操作をおこないます。

- 証明書要求(CSR)ファイルをアップロードする:の[参照…]ボタンよりダウンロードした CSR ファイルを選択
- [CSR ファイルの内容を確認する]にチェック

その後、[発行]ボタンをクリックします。

○作業名: <u>サー/運明書発行デモ</u> ○管理者: <u>テスト管理者</u>	プライベートCA Gléäs RA
[アカウント]>認明書発行	□ 認証局 □ 日芝 □ 管理者 □ ヘルブ □ 日グアウト ○ サイドバー □
アカウント アカウント アカウント	□一切に戻る → クイックナビ ○ = 44770 年 → 24770 年 → 247700 年 → 24770 年 → 24770 → 247700 → 2477000 → 2477000 → 247700000000000000000000000000000000000
pulse-test.jcch-sss.local	
Croup ★ 証明書発行	
この画面では証明書要求の作成を行います。 この画面では証明書要求の作成を行います。	金 認証局証明 <u>書</u>
認証デバイス Device Allのテンブレートの中から必要なものを選択して「発行」を押	× メッ PUTください。
► テンプレート Tamplate	■上級者向け設定
> 下記の内容で証明書を発行します。よろしければ「発行」を	を押してください。 保存
 アカウント操作 単行済み証明書をすべて失効させる 	► Rm/2
アカウントー覧 > 証明書要求(CSR)ファイルをアップロードする: C:\temp\	pulse.csr 参照… アカウント(0)
登録申請者一覧	★ 証明書 (0)
アカウント新規作成	発行
▶証明書発行	
▶サデジェクト	▶ 選択されているテンプレート ■全工解除
> CN=pulse-test.jcch-sss.local	▶ 必須 デフォルト設定
> DC=COM, JCCH-SSS	> 必須 サーバ証明書
▶時佳	▶ 選択可能なテンプレート

証明書の要求内容が表示されるので確認し、[▶この内容で発行する]をクリック し、証明書の発行をおこないます。

 ○作業名: <u>サーバ証明書発行</u> ○管理者: <u>テスト管理者</u> 	充		プライベートCA	Gléås 🖪
[アカウント]>発行	 深江岛 () 	3 <u>日グ</u> 11管理者	: ■ヘルズ ■ログアウト	0 #4FM-
アカウント				▶ クイックナビ
デ グループ Group Ce) pulse-test.jcch-sss.local 証明書要求(CSR) の確認	<u> きょンセル</u>	 この内容で発行する。 	 ■ マジン証明書 ■ マジン証明書 ■ サーバ証明書
★ 証明書 Certificate	Data: Version: 0 (0x0) Subject: 0=JS3, CN=pulse-test.jcch-sss.local Subject Public Key Info: Dible Key Info:		- 1	
Device Device テンプレート Template	RSA Public Key: (2048 bit) Modulus (2048 bit): 00:af:bf:34:2b:4e:48:58:d5:53:59:5e:7f:5a:42 47:61:bb:43:a5:2a:61:52:ce:16:01:18:44:d9:46	2:		保存
 アカウント操作 アカウント一覧 	4a:08:c1:d4:db:f4:5a:30:28:28:82:92:6c:10:24 70:37:e8:89:eb:b3:ab:3b:9e:6d:03:0d:83:82:51 2f:15:51:93:46'72:f0:ed:2c:a1:33:64:27:d0:cb 2d:5d:54:00:61:83:af:29:1f:ac:95:ae:ae:1a:0c	1: L: D:		▶ ドック ■ アカウント (0)
登録申請者一覧 アカウント新規作成	ec:bb:15:16:f8:66:5f:cf:03:a6:1d:64:66:99:f7 4c:fa:54:a4:1a:1d:9e:94:84:40:77:68:83:6b:b7 51:94:f0:f3:3e:32:41:b8:760:03:0a:a7:51:09:86 ca:27:ff:00:bc:ff:co:21:f6:cb:b2:10:65:bc:21:f6:0b:b2:f5:co:21:f6:b2:f5:co:21:f6:b2:f5:co:21:f6:b2:f5:f5:co:21:f6:b2:f5:co:21:f6:b2:f5:co:21:f6:b2:f5:co:21:f6:b2:f5:co:21:f6:b2:f5:f5:f5:f5:f5:f5:f5:f5:f5:f5:f5:f5:f5:	7: 7: 5:		★ <u>178月書 (0)</u>
	f0:b0:6b:ad:15:1a:8e:ba:c7:d2:64:34:e7:1f:e6 df:4a:f7:09:2b:ea:df:34:cf:e6:7e:19:75:f6:af 37:f8:f0:41:e8:7e:4a:70:71:a7:c0:6b:95:7d:4a	5: 5: 5:		
	4f:5f:43:b8:04:ca:9e:fd:b3:32:a0:0f:a2:3e:df 39:c5:2b:40:25:de:6a:e0:2d:87:78:f3:07:6d:82 76:d8:d9:72:7c:21:8a:44:0c:ad:dd:66:88:97:c7	E: 2: 7:		
	41:40:10:/4:95:74:69:29:86:03:68:79:b5:61:b3 65:bf Exponent: 65537 (0x10001)	3:	~	
操作問題 ブライベート CA Gléas	Copyr	right (C)2010-2015	JCCH Security Solution Syste	ms Co.,Ltd. All rights reserved.

証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書:<u>あり</u>」をクリ ックし、発行された証明書をダウンロードします。

COURSE Dista COURSE Dista COURSE	O作業名: <u>サーバ証明書</u> の管理者: <u>テスト管理者</u>	in 7 t	プライベートCA	Gléås 🖪
● Index designed as a local MixEll : 2016001/14 18.37 187日 : 201801/14 18.37 ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local as a local ● Index designed as a local ● Index designed as a local ● Index designed as a local as a local	[証明書]>詳編 2 アカウント Account ぼ Group	明書 ICCH-SSS demo2 CA#4 全面明書 信義	·전포동 이유선 이번 전 이유선 이유가 전 · 프립모프 · 단선 · · · · · · · · · · · · · · · · · · ·	 ●サイドバー ● タイックナビ ◎ ユーザ証明度 ◎ オンン証明度 ◎ サーバ証明度
・ 計画: ・ 指案::93 ・ かだは::006 > かたび::006	* 証明書 Certificate	▶ <u>pulse-test.jcch-sss.local</u> ▶ サーデンェクト	開始日:2016/01/14 18:37 終了日:2019/01/14 18:37 ▶ 基本估報	
EVER 5: 400H 1000 CA EVER 5: 400H 20A EVER 5: 400H EV	 F2ンプレート Template び庭明書操作 庭明酒一覧 大允処返還 や庄処還 ドックに入れる 	> 桂原:JS3 >一赴它:pulse-test.jcch-sss.local) 作成日:201600114 18:36 > 対応日波:1006 > 大約日: > 大約頃田: > 大約頃田: > 周期時/7日: > 1(成:= 約が成辺明書) > 後頃の(成:= 約が成辺明書) > トージン・必要: > バージョン:4 	(保存 ▶ ドック <u>ま アカウント (0)</u> ★ 詳単時 <u>後 (0)</u>
1210月274月2 1210月274月2 1210月274月2 1210月274月2 1210月274月2 1210月274月2 1210月274月2 1210月274月21 1210月274月21 1210月274月21 1210月274月21 1210月274月21 1210月274月21 1210月274月21 1210月274月21		▶ 2日初告結1 ↓ 22日為 12日本 14日アルージズム: tra シダイシェルトアルージズム: sha256 シダイシェルトアルージズム: sha256 シダイシェルトアルージズム: sha256 シダイシェルトアルージズム: sha256 シダ用金: 堂子玉名: 建ジェビライアンド校22 > 松松県明治: SSLサージの21: SSLワライアンド校22 > 松杉県町治: SSLサージの21: SSLサージの21: SSLワライアンド校22 > 松杉県町治: SSLサージの21: SSLサージの21: SSLワライアンド校22 > 松杉県町治: SSLサージの21: SSLサージの21: SSLワライアンド校22 > 松杉県町: SSLサージの21: SSLサーザージの21: SSLサージの21: SSLサージャージの21: SSLサージの21: SSLサージの21: SSLサージの21: SSLサージの21: SSLサージの21: SSLサージの21: SSLサージの21: SSLサージの21: SSLサージャージャージャージャージャージャージャージャージャージャージャージャージャー		
サール証明書 デフルル設定		- エンタン・パン 3日時東京: 参上 (YACUB 201601/14 18:36 3日時東: 参上 「YACUB 201601/14 18:38 > 紀密線: 42L - シンプレート情報 - ジンゴレート情報		
		サーバ課明後、デフォルト設定	、	

Connect Secure に戻り、ダウンロードした証明書を指定し、[Import]をクリック しアップロードします。

Step 2.	. Import signed certificate		
	When you receive the signed certificate certificate and remove this pending CSP	ile from the CA, select it below and click Import. This will add the si	gned
	Signed certificate: C:\temp\download.crt	参照	
	Import		

プライベート認証局 Gléas ホワイトペーパー

Pulse Connect Secure クライアント証明書認証設定

以上でサーバ証明書の登録が完了です。

Device Certificates にアップロードした証明書が表示されます。

Configuration					
Security Certificates DMI Agent NCP	Sensors Client Types Pulse Collabora	ation Virtual Desktops User Record Sync	nronization IKEv2 SAML Mobile		
Device Certificates Trusted Client CAs Trusted Serve	er CAs Code-signing Certificates Client Auth Ce	rtificates			
specify the Device Certificate(a). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom Intermediate CAs.					
Certificate issued to Issued by Valid Dates Used by					
pulse-test.jcch-sss.local	JCCH-SSS demo2 CA	Jan 14 09:37:45 2016 GMT to Jan 14 09:37:45 2019 GMT			

※複数のサーバ証明書が格納されている場合は、クライアントからのアクセスを受け付けるポートを指定する必要があります。上の画面の証明書名のリンクをクリックすることでその設定がお こなえます

Present certificate on these ports	
Select the internal and	external virtual ports that will present this certificate:
Internal Virtual Ports:	Selected Virtual Ports:
<internal port=""></internal>	Add -> Remove
External Virtual Ports:	Selected Virtual Ports:
<external port=""></external>	Add-> Remove
Vlan Ports:	Selected Vlan Ports:
Add -> Remove	
Management Port	
Management Port	

2.3. 認証サーバの設定

左側のメニューから[Auth. Server]をクリックし、右側の画面の[New:]のドロップダ ウンより[Certificate Server]を選択し、[New Server…]をクリックします。 認証サーバの設定画面に移動するので、以下の設定を行います。

- [Name:]には、一意の認証サーバ名称を入力
- [User Name Template:]にはConnect SecureでユーザIDとして扱う属性を指定
 ※クライアント証明書のサブジェクトCN (Common Name)を利用するケースでは、デフォ ルトで入っている <certDN.CN> のままにしておきます

Auth Servers > New Certificate Se	erver	
* Name:	Gleas	Label to reference this server.
User Name Template:	<certdn.cn></certdn.cn>	Template for constructing user names from certificate attributes.

設定終了後、[Save Change]をクリックして設定を保存してください。

2.4. ロール(ユーザ権限)の作成

左側のメニューより[User Roles] > [New User Role]をクリックします。 ロールの作成画面に移動しますので、以下の設定を行います。

- [Name:]に一意のロール名称を入力
- [Options]の欄で、[Pulse Secure Client]にチェック
- [Access features]の欄で、[VPN Tunneling]にチェック
- 必要に応じその他の項目を設定

Roles > New R	ole	
Name:	VPN Test	
VPN Tunneling	(includes IKEv2)	at to Windows and MAC OSY users

設定終了後、[Save Change]をクリックして設定を保存してください。

画面上部の[VPN Tunneling]タブを選択し、トンネリングに関する設定を行います。 ※ここではクライアントへのIPアドレス割当設定のみを記載します。その他各種設定(アクセス コントロール、接続プロファイル、スプリットトンネル、帯域幅の管理等)については説明を割愛 します。ネットワーク環境やポリシーに応じて設定を行ってください

画面最下部の[Connection Profiles]リンクをクリックします。

See also VPN Tunneling policies that apply to this role:	
Access control	<u>Connection profiles</u>
Split tunneling networks	Bandwidth Management

Network Connect Connection Profiles画面に移動します。[New Profiles]ボタンを クリックし、プロファイルの作成画面に移動しますので以下の設定を行います。

- [Name:]には、一意のルール名称を入力
- IP address assignmentの項目に、クライアントに対するIPアドレスの配布方法
 を選択(既存のDHCPサーバを利用か、管理者が割り当てるIPアドレスレンジ
 を設定)
- 必要に応じその他の項目を設定

以下はクライアントに対し、10.0.0.1から10.0.0.10までのアドレスを割り当てる設

定例となります。

۲	IPv4 address pool Specify the assignable IPv4 address ranges f Note: Please refer to Admin Guide for details	for this	profile, one per line.
	10.0.0.1-10.0.0.10	< >	Examples: 10.10.1.1-10.10.5.200 10.10.10.10-100 10.10.10.50

設定終了後、[Save Change]をクリックして設定を保存してください。

2.5. レルム(ユーザ認証)の作成

左側のメニューより[User Realms] > [New User Realm]をクリックします。 Realm の作成画面に移動しますので、以下の設定を行います。

- [Name:]には、一意のレルム名称を入力
- [Authentication:]には、2.3項で設定した認証サーバを選択
- 必要に応じその他の項目を設定

New Authentication Real	m	
* Name: Description:	VPN User	Label to reference this realm
	When editing, start on the start of the s	he Role Mapping page
Servers		
Specify the servers to use for authentication	and authorization. To create or manage serv	vers, see the <u>Servers</u> page.
Authentication:	Gleas	Specify the server to use for authenticating users.
User Directory/Attribute:	None V	Specify the server to use for authorization.
Accounting:	None V	Specify the server to use for Radius accounting.
Device Attributes:	None 🗸	Specify the server to use for device authorization.

設定終了後、[Save Change]をクリックして設定を保存してください。その後、Role Mapping設定画面に移動しますので、[New Rule…]をクリックします。 Role Mapping Rule画面に移動しますので、以下の設定を行います。

- [Rule based on:]には、ドロップダウンメニューより[Username]を選択し、
 ※[Certificate]を選択した場合、証明書サブジェクトOU等による制御が可能
- [Name:]には、一意のルール名称を入力
- [Rule: If username...]項目にはこのロールを適用するユーザ名を入力
 ※ワイルドカード "*"の利用も可能
- [...then assign these roles]項目には、2.4項で作成したロールを選択
- 必要に応じその他の項目を設定

以下は、有効なクライアント証明書が提示された場合、証明書のサブジェクトCN (2.3項でユーザIDとして設定済み)が何であろうと「VPN Test」というロールにマッピングする例です。

14 / 30



User Authentication Reals Role Mapping	ns > VPN User > Rule	
Rule based on: Us	ername V Update	
* Name: VPN Rule		
* Rule: If username		
then assign these ro	You can use * wildcards.	er line
Auglishin Delesero		
Available Roles:	Add -> VPN Test	

設定終了後、[Save Change]をクリックして設定を保存してください。

2.6. サインインポリシの設定

左側のメニューから[Signing-in] > [Sign-in Policies]をクリックし、右側の画面の User URLsの[*/](ユーザ用のデフォルトページ)をクリックします。 その後、当該ログインページの設定画面に移動するので、[Authentication realm]の 項目で以下を設定します。

- [User picks from a list of authentication realms]を選択
- [Available Realm]ボックスにある2.5で作成したレルムを、[Selected Realm]ボックスに移動

Specify how to select an au	thentication realm wi	hen signing in.
O User types the realm	name	
The user must type the name o	f one of the available authe	ntication realms.
• User picks from a list	of authentication r	realms
The user must choose one of th sign in. If only one realm is sele display the list). To create or m <u>Administrator Authentication</u> pa	e following selected autheni acted, it is automatically use anage realms, see the <u>User</u> ge.	tication realms when they d (the sign-in page will n <u>Authentication</u> page or th
Available realms:	Selected rea	ılms:
A	vdd -> VPN User	Move Up
P	emove	Move Down

設定終了後、[Save Change]をクリックして設定を保存してください。

2.7. Location Awareness の設定

※本項は、1.3項で言及したLocation Awareness機能を利用したPCでのVPN自動接続をおこなう

場合にのみ必要な設定なります

左側のメニューから[Users] > [Pulse Secure Client] > [Connections]を選択し、右 側の画面で Default をクリックします。

その次の画面の Connections にて SA をクリックします。

Description
Default server connection

Location awareness rules: より自動接続させるルールを設定するため。[New...]を クリックします。

Location awar	eness rules:		
Automatic awareness	connections ar rules are evalu	e attempted Jated when	d when the conditio the user activates
New	Duplicate	Delete]

自動接続の条件を設定します。

以下は、「物理ネットワークインターフェースで、test-server.js3-test12.localが 192.168.0.1に解決される」ことを設定した例です。

Name: Action:	sample-rule Resolve address:	~		
Conditio	on:			on interface:
test-ser	⊪e: ver.js3-test12.local			
Specify 1 192.10	che IP address range,	one per line:	Examples: 10.10.10.50	 Physical Pulse Secure Any

設定後、[Save Changes]をクリックして保存します。

Location awareness rules:で以下の通り設定します。

- Require:の部分に、[Custom...]を選択
- Accepted:の部分に、[NOT sample-rule]とします。

ocation awareness rules:	
Automatic connections are attem disconnected when the conditions when the user activates a connec no longer true. New Duplicate Delete	oted when the conditions specified in the location awareness rules and are no longer true. For a manual connection, location awareness ru tion. Manual connections are disconnected when the location awareness.
Name	Description
1. sample-rule	When address(s) test-server.js3-test12.local can be resolved 192.168.20.100 on physical interface
Require: All of the above rules Any of the above rules Custom	Accepted: (), AND, OR, NOT Example: DNS-Rule AND NOT (IP-1 OR IP-2) NOT sample-rule

これにより「物理ネットワークインターフェースで、test-server.js3-test12.localが 192.168.0.1に解決されない場合にVPN自動接続」となります。

また、PC側のクライアントソフトウェア(Pulse Secure Client)へこの設定を反映 させるため以下をおこないます。

[Users] > [Pulse Secure Client] > [Connections]を選択し、対象の設定をチェック して[Update Clients]をクリックして、その後確認画面が表示されるので[Update] をクリックします。

Pulse Secure Client > Pulse Secure Clie	ent Connections	
Connections Compo	nents	
A Pulse Secure connect	tion set determines client settings and provi Duplicate Assume Ownership Up	des a listing of available connect vdate Clients
Name Name	Description	Owner
☑ 1. <u>Default</u>	Default Pulse Secure client connection set	pulse-test.jcch- sss.local

※Location AwarenessルールがPCに反映されるのは、次回のPulse Secure ClientでのVPN接続後 となります

3. Gléas の管理者設定 (PC)

GléasのUA(申込局)より発行済み証明書をPCにインポートできるよう設定します。 ※下記設定は、Gléasの納品時に弊社で設定をおこなっている場合があります

GléasのRA(登録局)にログインし、画面上部より[認証局]をクリックし[認証局一 覧]画面に移動し、設定を行うUAをクリックします。

UA 申込局		
► <u>Gleas Generic</u>	<u>: UA</u> Gleas デフォルト申込局	

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

▶ 証明書ストアへのインポート	証明書ストアの種類	ユーザストア	•
□ ダウンロードを許可	✓ インボートワンスを利用す	3	

設定終了後、[保存]をクリックし設定を保存します。

4. PC での接続操作

4.1. クライアント証明書のインポート

Internet Explorer で Gléas の UA にアクセスします。 ログイン画面が表示されるので、ユーザ ID とパスワードを入力しログインします。



ログインすると、ユーザ専用ページが表示されます。

[証明書のインポート]ボタンをクリックすると、クライアント証明書が証明書スト アにインポートされます。

※初回ログインの際は、ActiveX コントロールのインストールを求められるので、画面の指示に従 いインストールを完了してください。

				プライベートCA Gléas	JA
[サンプル ニ	1ーザ さんのページ]			■ <u>□グアウ</u>	뇬
ユーザ情報					
2 サン	プル ユーザ さんのページ			D <u>へルブ</u>	
2 ユーサ	「情報			,	
▶ ユーザ	登録日時 : 2011/	07/19 13:48			
> メール7 > パスワー ★ 証明書	?ドレス : -ド : ***********************************				
#	発行局	シリアル	有効期限	証明書ストアヘインポート	
\$1	JCCH-SSS demo CA	#11167	2018/10/29	証明書のインポート	
					~

「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログ アウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、 再度のインポートを行うことはできません。

			プライ	K-FCA Gléäs	UA
[サンプル ユー	-ザ さんのページ]			Ľ <u>□</u> /	アウト
ユーザ情報					
🙎 サンプル	レユーザ さんのページ				レブ
2 ユーザ情	5 幸夜 · · · · · · · · · · · · · · · · · · ·				\sim
▶ユーザ	登録日時 : 2011/07/19	13:48			
 > 姓: ワン。 > ユーザロ:u > メールアド > パスワード * 証明書報 	パレ 名:ユーサ iser01 レス: : ************************************				
#	発行局	シリアル	有効期限	証明書ストアヘインポート	
\$1	JCCH-SSS demo CA	#11167	2018/10/29	ダウンロード済み	
					~

4.2. クライアントからのVPN接続 (PC)

2.6項で設定したConnect Secureのサインインページに、Pulse Secure クライアントから接続すると、証明書認証がおこなわれたのちに接続します。 (証明書が一枚しかない場合は、それがバックグラウンドで自動的に選択されます)



失効された証明書でアクセスすると以下のエラーが表示されます。

S Pulse Secure
接統先: pulse-test.jcch-sss.local
接続に失敗しました。
● 接続エラー クライアント証明書が失効されました。(エラー:1389)
クライアント証明書が失効されました。有効なクライアント証明書で再 試行してください。
(再試行(R)) (キャンセル(A)

Location Awarenessが設定されている場合は、事前設定した条件が満たされる場合に自動的にVPN接続がおこなわれます。

VPN接続がバックグラウンドでおこなわれると、タスクバーに以下のメッセージが 表示されます。



5. Gléasの管理者設定(iPad)

Gléas で、発行済みのクライアント証明書を含む Pulse Secure 接続設定(構成プロ ファイル)を iPad にインポートするための設定を本章では記載します。 プライベート認証局 Gléas ホワイトペーパー

Pulse Connect Secure クライアント証明書認証設定

※下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります ※Pulse Secure 用の構成プロファイル生成機能は Gléas ではオプションとなります。詳細は最終 項の問合せ先までお問い合わせください

5.1. UA(ユーザ申込局)設定

GléasのRA(登録局)にログインし、画面上部より[認証局]をクリックし[認証局一 覧]画面に移動し、設定を行うUAをクリックします。

UA	申込局	
	▶ Gleas Generic UA	Gleas デフォルト申込局

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定 この設定を行うと、GléasのUAからダウンロードしてから、指定した時間(分) を経過した後に、構成プロファイルのダウンロードが不可能になります(「イン ポートロック」機能)。このインポートロックにより複数台のiPadへの構成プロ ファイルのインストールを制限することができます。

▶基本設定
□ トークンへのインボート
□ 証明書ストアへのインボート
☑ ダウンロードを許可
ダウンロード可能時間(分) 1

[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UA を利用する]をチェックします。

🦸 認証デバイス情報			 	
▶iPhone / iPadの設定				
🗖 iPhone/iPad 用 UAを利	用する			
		保存		

構成プロファイル生成に必要となる情報を入力する画面が展開されるので、各項目 を入力します。

- [名前]、[識別子]、[プロファイルの組織名]、[説明]は必須
- [削除パスワード]を設定すると、利用者が設定プロファイルを削除する際に管理者が定めたパスワードが必要となり、利用者の誤操作等による構成プロファイルの削除を防止できます。
 ※ここでパスワードを設定した場合でも、Pulse Secureアプリから接続設定を削除することはできてしまうため注意が必要

🦸 認証デバイス情報	
▶ iPhone / iPadの設定	
🖌 iPhone/iPad 用 UA を利	用する
画面レイアウト	
✓ iPhone 用レイアウトを使 Mac OS X 10.7以降の接	用する ログインパスワードで証明書を保護 続き許可
OTA(Over-the-air)	
OTAエンロールパントを利	I用する () 接続する iOS デバイスを認証する
OTA用SCEP URL	
OTA用認証局	デフォルトを利用
iPhone 構成プロファイル基本	本設定
名前(デバイス上に表示)	JS3 demo profile
識別子(例: com.jcch- sss.profile)	com.jcch-sss.demo-profile
プロファイルの組織名	JCCH・セキュリティ・ソリューション・システムズ
II兑8月	JS3のデモ用プロファイル(Pulse Secure)
削除パスワード	

さらに[Pulse Secure SSL-VPNの設定]項目に以下を設定します。

- [SSL-VPN 接続名]に、任意の接続名を入力(必須)
- [SSL-VPN ホスト名]に、接続先のConnect Secureのホスト名(或いはIPアドレス)を入力(必須)
- [オンデマンド接続先]に、自動VPN接続のトリガとなる文字列(ドメイン名など)
 を入力(オプション)

※ここで指定された接続先(後方一致)が、名前解決できない場合に自動的にVPN接続を開始 します(アプリケーションがオンデマンドVPNに対応している必要があります)

例:ここに ".js3-test12.local"を指定すると、safariで "http://www.js3-test12.local/" にア クセスすると後方一致の条件を満たすので自動的にVPN接続がおこなわれます

Pulse Secure SSL-VPN0	D設定
SSL-VPN 接続名	JS3 Remote Access
SSL-VPN ホスト名	pulse-test.jcch-sss.local
オンデマンド 接続先	

各項目の入力が終わったら、 [保存]をクリックします。 以上でGléasの設定は終了です。

6. iPad での接続操作

6.1. Pulse Secureのインストール

iPadでPulse Secureを利用する場合は、クライアントソフトウェアのダウンロード が必要です。App Store より事前にインストールを行ってください。 本書ではPulse Secureのインストール方法については割愛します。

6.2. クライアント証明書のインポート

iPadのブラウザ(Safari)でGléasのUAサイトにアクセスします。 ログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。



ログインすると、そのユーザ専用ページが表示されるので、[ダウンロード]をタッ プし、構成プロファイルのダウンロードを開始します。

※インポートロックを有効にしている場合は、この時点からカウントが開始されます

				JEAN-PCA Gleas	
[ユーザ 0 1 さんのページ] ロログアウト					
ローザ情報					
🙎 ユーザ 0) 1 さんのページ				
2ユーザ情	報				
▶ユーザ	登録日時	: 2011/07/19 13:48			
> 姓 : ユーザ 名 : 0 1 > ユーザ/D : usef01 > メール :					
美 証明書情	報 · · · · · · · · · · · · · · · · · · ·				
▶ 発行済み証明	*				
#	発行局	シリアル	有効期限	ダウンロード	
<u>\$1</u>	JCCH-SSS demo CA	#11139	2018/10/02	構成プロファイルのダウンロード	

自動的にプロファイル画面に遷移するので、構成プロファイルの表示を[許可]し、 その後に[インストール]をタップします。







※[詳細]をタップすると、インストールされる証明書情報を見ることが可能ですので、ルート証 明書のフィンガープリントなどを必要に応じ確認します

以下のプライベート認証局のルート証明書のインストール確認画面が現れますの で、[インストール]をクリックして続行します。



インストール完了画面になりますので、[完了]をタップします。



元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトします。

以上で、iPadでの構成プロファイルのインストールは終了です。 なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点 より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り プライベート認証局 Gléas ホワイトペーパー

Pulse Connect Secure クライアント証明書認証設定

「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可となり ます。



6.3. OTAエンロールメントを利用した証明書発行について

Gléasでは、iOSデバイスに対するOver The Air(OTA)エンロールメントを利用し た証明書の発行・構成プロファイルの配布も可能です。

OTAを利用すると事前に指定した端末識別番号を持つ端末だけに証明書の発行を限 定することも可能になります。



詳細は最終項のお問い合わせ先までお問い合わせください。

6.4. Pulse Secureから接続

インポートが完了すると、Connect Secureへの接続に利用するクライアント証明 書やVPN接続先が設定されています。

Pulse Secureを起動し[接続]ボタンをタップすると、バックグラウンドでクライア ント証明書を利用した認証を行いVPNの接続がおこなわれます。

※提示可能な証明書が複数ある場合は、選択ダイアログが表示されます

以下はPulse Secureから接続した画面です。



接続成功すると、通知エリアに VPN アイコンが表示されます。

Pad 🗢 VPN	20:19	🕑 76% 🗖
	Pulse Secure	
接続		
JS3 Remote Access https://pulse-test.jcch-sss.local		
	切断	
S user01		00:59:45

証明書を持っていない場合、失効された証明書を提示した場合(※)は接続失敗の 表示になります。以下は失効された証明書でアクセスした場合の表示となります。 ※該当する証明書の失効情報を含むCRLがConnect Secureに伝搬されている必要があります

pulse-test.jcch-sss.local	キャンセル
S Pulse Secure	
Pulse Connect Secure	
証明書が失効されています。	
Please sign in to begin your secure session.	
Sign In	

7. オンボーディングを利用した証明書配布

7.1. GléasでのSCEPサーバの利用開始設定

SCEP 通信には専用の電子署名用証明書が必要になるので、事前に Gléas より SCEP サーバに利用する証明書を発行し、ファイルダウンロードしておきます。

RA で上部の[認証局] > [デフォルト登録局]をクリックします。

認証局一覧
フィルタ 全て表示 🗸
💿 test.jcch-sss.com の認証局
RA 登録局
▶ <u>Gleas Generic RA</u> Gleas デフォルト登録局
14 発行局
► Evaluation CA Evaluation CA

登録局詳細の「▶SCEP の設定」で、以下設定をおこないます。

- SCEP 用の証明書をアップロードする
- [静的チャレンジを利用する]にチェックを入れ、チャレンジ値を入力する ※チャレンジ値は Connect Secure にも設定します
- [接続を許可するネットワーク]に、"ネットワークアドレス/ネットマスク"の形式で接続許可するネットワーク情報を入力します ※未入力の場合は、全てのアドレスからのアクセスを許可します

▶ SCEPの設定	
≫ SCEPサーバを利用中です。	
≫ SCEP用証明書: 🌻 scep-demo 🚺 <u>削除</u>	
≥ 有効期限:2021/04/11 09:03	
▶ 🗹 静的チャレンジを利用する	
≫ 静的チャレンジ jcch-sss-demo	
≫ 接続を許可するネットワーク 192.168.20.249/32	
保存	
保存	

設定が完了したら[保存]をクリックすることで SCEP サーバ機能が利用可能になります。

7.2. Connect Secureでの設定

管理者画面左側のメニューの[User Roles]より、Onboarding を利用するロールの設 定画面で[Enterprise Onboarding]をチェックします。

Enterpri	se Device Onboarding
	Check the 'Enterprise Onboarding' to enable for this user role, and specify any role-based options. assigned to the user.
	Secure Mail Options
	Enterprise Onboarding Options (VPN, Wifi and Certificate Profiles)

その後、[Save Changes]をクリックし、設定を保存します。

また、必要に応じオプションも設定します。

管理者画面左側のメニューの[Enterprise Onboarding] > [SCEP Configuration]と進み、[SCEP Configuration]タブで以下設定をおこないます。

- [SCEP Server URL]には、Gléas の SCEP 用 URL を入力します ※URL は以下の形式で入力します。
 http(s)://[Gléas UA ホスト名]/scep/[認証局番号]
 例:デフォルトの認証局で発行する場合: http://ua.example.com/scep/1
- [Challenge]には、Gléas で設定したチャレンジ値を入力します
- [Upload Encryption Certificate:]には、Gléas にアップロードした SCEP 用の証 明書を設定します

※PKCS#12 ファイル(*.p12)ではなく、証明書ファイル(*.crt)を Gléas よりダウンロー ドしてここの設定をおこないます

Ent	erprise O	nboarding				
SCE	P Configurat	tion CSR Templat	es VPN Profile	es WiFi Profiles	Certificate Profiles	Secure Mail
*	SCEP Server URL:	Mig. Ann Arren (n. A.	/scep/1			Example: http:// <scep Server>/certsrv/mscep/msce for Microsoft Network Device Enrollment Service(NDES)</scep
	Challenge:	•••••				Shared secret for automatic enrollment
	Retries:	0				Number of retries when connection fails (0 - 10)
	Retry Delay:	0				Duration in seconds between successive retries (0 - 10)
	Upload Enc	ryption Certificate:		参照	Used to encrypt the requ	ests to SCEP Server
			Manually upload th upload it automatic	e encryption certificat	e or run Test Configuration	below with Test Enrollment
	Current Ce	rtificate:	Issued To:	scep-demo		
			Valid:	Dec 10 06:29:45	CA 2014 GMT - Dec 10 (06:29:45 2017 GMT
			Details:	Other Certificate	Details	
	Test Config	guration	✓ Test Conne □ Test Enrollr	ctivity nent		
	Save Char	nges				

設定後に、[Save Changes]をクリックし保存します。

[CSR Template]タブで[New CSR Template]をクリックし、CSR テンプレートの設 定をおこないます。

- [Name]には、任意の設定名を入力
- [Subject DN]には、証明書のサブジェクトになるものを入力

CN=<USERNAME>とすることで、Connect Secure のユーザ ID を証明書サブ ジェクト CN とすることができます。

また、Gléas には Connect Secure のユーザ ID と同一のアカウントが作成され ている必要があります (Gléas は未登録ユーザ ID への証明書発行を拒否しま す)。

<u>CSR T</u> Nev	_{emplates} > v Certificate Signin	g Request Template	
*	Name:	JS3test	Label to reference this CSR Template
*	Subject DN:	CN= <username>,OU=Employees,O=Com</username>	Example: CN= <username>,OU=Employees,O=Company</username>
	Email:		
	Subject Alternative Name Type:	None	
	Subject Alternative Name Value:		
	Key Size:	2048-bit 🗸	Ensure that the selected Key Size is enabled on the SCEP Server. An invalid Key Size will cause a certificate request failure.
	Save Changes		

設定後に、[Save Changes]をクリックし保存します。

[SCEP Configuration]タブに戻り、接続及び証明書発行のテストをおこないます。 ※Connect Secure の管理ユーザ ID と同一のアカウントを Gléas にあらかじめ作成しておく必要 があります

Test Configuration	✓ Test Connectivity
	Test Enrollment JS3test
	This will request a certificate on the SCEP server using the specified Certificate Signing Request (CSR) Template.
	The encryption certificate may be updated during the test if it is not already or correctly configured.

成功すると、以下のメッセージが表示されます。

Successfully received a test certificate from the server which will be discarded. More details are available in the Event Log.
SCEP configuration is saved.

[Certificate Profile]タブで、証明書の配布設定をおこないます。

- [Import and Use CA Certificate]にチェックを入れ、クライアントに送信するル ート証明書をアップロード
- [Generate per User Certificate]にチェックを入れ、設定したCSRテンプレート を選択

Name:	test		×		Label to reference this profi
Description:					
				0	
Apply to Client Types					
Apply to client Types:	105	🗹 Android	Mac OS X	✓ Windows	
☐ Import and Use Glol ✓ Import and Use CA (Unchecking this option will delet	oal Certifica Certificate e the uploaded C	n te CA certificate upon s	successfully saving cha	anges.	
☐ Import and Use Glol ✓ Import and Use CA (Unchecking this option will delet CA Certificate: On successful import, this profile Import from:	certificate Certificate e the uploaded C a will be auto sav	i te ^{CA} certificate upon s red. 参照	successfully saving cha	anges.	
☐ Import and Use Gloi ☐ Import and Use CA (Unchecking this option will delet CA Certificate: On successful import, this profile Import from: Import CA Certificate	certificate Certificate e the uploaded C e will be auto sav	n te A certificate upon s red. 参照	uccessfully saving cha	anges.	
☐ Import and Use Glol ☑ Import and Use CA (Unchecking this option will delet CA Certificate: On successful import, this profile Import from: Import CA Certificate Issued To: ▶ Evaluation	Dal Certifica Certificate e the uploaded C e will be auto sav	n te A certificate upon s red. 参照…	successfully saving cha	anges.	
☐ Import and Use Glol ✓ Import and Use CA (Unchecking this option will delet CA Certificate: On successful import, this profile Import from: Import CA Certificate Issued To: ▶ Evaluation Issued By: ▶ Evaluation	Dal Certifica Certificate e the uploaded of a will be auto save a CA	ite A certificate upon s red. 参照	successfully saving cha	anges.	

設定後、[Save Changes]をクリックして設定を保存します。

Onboarding機能がオンになった状態でWindowsからWebアクセスをおこなうと、 [オンボード]タブが表示されます。



画面表示にしたがい、オンボーディングを実行します。成功すると以下のダイアロ グが表示されます。



8. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Connect Secureに関するお問い合わせ先

パルスセキュアジャパン株式会社 Tel: 03-6809-6836 Mail: info_jp@pulsesecure.net

■Gléasや検証用の証明書に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ Tel: 050-3821-2195 Mail: sales@jcch-sss.com