

プライベート認証局Gléas ホワイトペーパー

Ivanti Connect Secure

クライアント証明書による認証設定

Ver.3.0 2022 年 6 月

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

- 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. はじる	ちに	4
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	5
2. Conn	ect Secure の設定	5
2.1.	信頼するルート認証局の設定	5
2.2.	サーバ証明書の設定	9
2.3.	認証サーバの設定1	3
2.4.	ロール(ユーザ権限)の作成1	3
2.5.	レルム(ユーザ認証)の作成1	4
2.6.	サインインポリシの設定1	6
3. Gléa	s の管理者設定(PC)1	7
4. PC て	の接続操作1	8
4.1.	クライアント証明書のインポート1	8
4.2.	クライアントからの VPN 接続(PC)1	9
5. Gléa	s の管理者設定(iPad)2	0
5.1.	UA(ユーザ申込局)設定2	1
6. iPad	での接続操作2	2
6.1.	Pulse Secure のインストール	2
6.2.	クライアント証明書のインポート2	3
6.3.	Pulse Secure から接続2	5
7. 問い1	合わせ2	7

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、Ivanti社のSSL-VPN装置「Ivanti 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。

- Ivanti Connect Secure (バージョン21.9R1 (build 421))
 ※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2.5.1)
 ※以後、「Gléas」と記載します
- クライアント: Windows 10 Pro / Pulse Secure (バージョン9.1.12 (10247) / Gléas CertImporter (バージョン 1.0.1)
 ※以後、「PC」と記載します
- クライアント: iPad Air 2 (iPadOS 15.4.1) / Pulse Secure (バージョン 9.11.0.89207)
 ※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操作
- PCのネットワーク設定等の基本設定、Pulse Secureクライアント、Gléas
 CertImporterアプリおよびブラウザ拡張機能のインストール方法
- iPad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

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Gléas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。

事前に 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。



管理者画面上部メニューより[System] > [Configuration] > [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。

Users	Users can be required to present valid client-side certificates to sign in(see the realm-specific Certificate Authentication Policy page). Specify trusted certificate authorities.					
Au	to-import options	Proxy Settings	Import CA Certificate	Delete		
10	✓ records per	page			Search:	
	Trusted Client CA		Trusted for client authentication?	Valid dates	Status checking	

[Import From:]のところで[Browse]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。



成功すると認証局の情報が表示されます。



Online Certificate Status Protocol (OCSP) 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、ページ下部の Client certificate status checking 項目で、 [Use CRLs (Certificate Revocation Lists)]を選択し、ここで一度[Save Changes] をクリックします。



ページ下部の OCSP Setting 項目で、[OCSP Options...]をクリックします。 OCSP Options ページで以下の設定をおこない、[Save Changes]をクリックしま す。

- [Use:]ドロップボックスでは、 [Responder(s) specified in the client certificates]を選択
 ※クライアント証明書の機関情報アクセス (AIA) フィールドが存在しない場合は [Manually configured responders]を選択し、OCSP レスポンダの URL を入力
- [Use Nonce]にチェック



	5P options to use during enduser	certificate verification.
Use	e: Responder(s) specified in the o	client certificates 🗸
	OCSP Responder URLs will be retrieve	ed during client authentication.
	OCSP responders	Last Used
✓ Options		
	ficate to sign the request : Do	not sign the request 、
Device Certi		
Device Certi Signature H	ash Algorithm: 🔘 SHA-1 💿 S	SHA-2

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、 ページ下部の Client certificate status checking 項目で、[Use CRLs (Certificate Revocation Lists)]を選択し、ここで一度[Save Changes]をクリックします。



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 ページで以下の設定をおこない、[Save Changes]をクリックします。

● [Use:]のドロップボックスでは、[CDP(s) specified in the client certificates] を選択

※クライアント証明書に CRL 配布ポイント(CDP)フィールドが存在しない場合は[Manually configured CDP]を選択し、CRL 配布ポイントの URL を入力

 [CRL Download Frequency:]には、CRL をダウンロードする間隔を時間単位で 入力します。



Jse: CDP(s) speci	ied in client certificates	~
Certificates vary i	how they specify CDPs. If the clier	nt certificate does not specify a s
CDP Server:		If the server (and port) is not
CRL Attribute:		If the certificate only specifies
Admin DN:		If the server requires authenti
Password:		(LDAP only)
Options CRL Download Fr Dividate Serve	quency: 24 hours (1-9 r Certificate (LDAPS only)	999) Note that CRLs can also sp

また失効確認方法で[Use OCSP with CRL fallback]を利用することでこれらを併用 することが可能になります(CRL ファイルを Gléas 以外のサーバでも保存するな どの可用性を考慮した運用が前提)。



また、[Skip Revocation check when OCSP/CDP server is not available]を有効に すると、何らかの理由で OCSP レスポンダや CRL 配布ポイントにアクセスでき ず、失効確認がおこなえない場合でも証明書認証を継続することが可能です(弊社 未検証)。

2.2. サーバ証明書の設定

管理者画面上部メニューより[System] > [Configuration] > [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。 プライベート認証局 Gléas ホワイトペーパー

Ivanti Connect Secure クライアント証明書認証設定

New Certificate Signing Requestページでホスト名など、必要事項を入力し[Create CSR]をクリックするとCSRが作成されます。

以下は楕円曲線暗号P-384での鍵生成の設定でCSRを作成した例です。

© CSR created successfully: Your CSR was created successfully. See below for instructions on sending the CSR to a Certificate Authority. The certificate approval process may take several days. When you receive the signed certificate from the Certificate Authority, you will need to import the certificate to complete this process.
Configuration > Pending Certificate Signing Request
Pending Certificate Signing Request
CSR Details Common Name: Treated: 5/27/2022 16:16:10 Org. Name: JS3 Locality: Org. Unit Name: State: Email Address: Country: ECC Curve: secp304r1
Back to Device Certificates Step 1.Send CSR to Certificate Authority for signing To send the CSR to a Certificate Authority (CA), you need to copy the encoded text below, including the BEGIN and END lines, and submit it to the CA in one of the following ways: Save the text as a .cert file and attach it to an email message to the CA Paste the text into an email message to the CA Paste the text into a Web form provided by the CA Note: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed for each CSR.
BEGIN CERTIFICATE REQUEST MIIBY2CB60IBADAuMQwwCgYDVQQKDANKUzMxHjAcBgNVBA MMFWI2VW50aS5qY2No LXNzcy5sb2hhoB2NBA2IMBAGBygGSM49AgEGBSuBBAAIA2IABF8Z cF47JcLskAEGWhL3 ED/AAprKz6y78qQdq35gbk9NHPOdSNPFY5VsRgktbF ////

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。

 O作業名: <u>サーバ証明</u> O管理者: <u>システム管</u> 	<u>]書発行</u> 3理者			プライベートC	🗛 Gléäs̈́ 🖪
[アカウント]>詳細	8		 認証券 	□ ログ □ 管理者 □ ヘルブ □ ログアロ	2E •サイドバー •
💊 アカウント	アカウント			D <u>一覧に</u>	戻る ▶ クイックナビ
Account	🗐 ivanti.			E90	2 8 ユーザ証明書
Group					
👗 証明書	2 アカワント情報・・・・・・	■ 改訂履歴	ジ クループ情報・・・・・・		
Certificate	▶サーバ	登録日時:2022/05/27 16:28	▶ユーザグループ	□参加	1211/011011#
Service 認証デバイス	> ステータス:有効		> tal		
テンプレート	▶サーバ属性 最終]	E新:2022/05/27 16:28 <u>編集</u>	▶□ールグループ	日参加	
Template	> ホスト名:ivanti.		> 顧客評価用クライアント証明書	図削除	保存
●アカウント操作			> <u>サーバ証明書</u>	区直接	
アカウントー覧					▶ ドック ■ アカウトト (0)
登録申請者一覧	★ 証明書発行の履歴 ······				₹ 評明書 (0)
アカウント新規作成	►1 JCCH-SSS demo2 CA			- BB	
▶証明書発行	# シリアル 開始	有効期限 ステータス	失効日 暗号種別	秘密鍵 格納状況	
▶アカウント削除	▶ テンプレート持起				
▶ドックに入れる	■ リンソレート 情報				
	▶サフジェクト (600)		845-1-1 . L	// (() - 1) - 1	
	(型5) → 42-22 (CN)	ivanti		ロコンプレート	
	(R)(第2 (O))	ICCU Country Colution Cur	Nama Ca. 11d		
	TEATT-Ed(U)	Joon Security Solution Sys	aems cu., Liu.		
	ドメインコンボーネント(DC)	jcch-sss com			

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>サーバ証明書発行</u> ○管理者: シ <u>ステム管理者</u>	プライベートCA	Gléås 🖪
【アカウント】> 証明書発行	■認証局 ■日グ ■管理者 ■ヘルブ ■日グアウト	O #1 K15- □
● アカウント アカウント	▶ <u>一間に戻る</u>	▶ クイックナビ
Account ivanti	■詳細に戻る	8 ユーザ証明書 ■マシン証明書
▲ Timl書発行		
★ 証明書 この画面では証明書要求の作成を行います。		
を他の「サブジュクト」と「儒性」の内容で証明書業求者作成します。 右側のテンプレートの中から必要なものを違釈して「発行」を押してください。		
▶ テンプレート ▶ 証明書発行		
Template > 下記の内容で証明書を発行します。よろしければ「発行」を押してください。		保存
●アカウント操作 > □発行済み証明書をすべて失効させる		
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:templivanti.csr 参照		▶ ドック
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。



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。

▶証明書ファイル		
▶証明書要求: <u>あり</u> 作成日時 2022/05/27 1	6:58	
▶証明書: <u>あり</u> 作成日時 2022/05/27 1	7:00	
> 秘密鍵:なし		

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。



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。

Devic	e Certificate					
Lic	ensing Security	Certificates	DMI Agent NCP C	lient Types Virtual Desktop	user Record Synchronization	IKEv2 SAML
Мо	bile VPN Tunneling	Telemetry	Advanced Client Configuration	Advanced Networking		
Device	Certificates Trusted Client CAs	Trusted Server CA	s Code-signing Certificates Client A	Auth Certificates Certificates Validity (Check	
Specify Impo	Specify the Device Certificate(s). 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.					
10	10 • records per page Search.					
	Certificate issued to Issued by Valid Dates Used by					
JCCH-SSS demo2 CA			JCCH-SSS demo2 CA	May 27 07:37:45 2022	GMT to Aug 27	

※複数のサーバ証明書が格納されている場合は、ポートに紐づけする必要があります。上の画面 で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



2.3. 認証サーバの設定

管理画面上部のメニューから[Authentication] > [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

New Certificate Se	rver	
*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

管理画面上部のメニューより[Users] > [User Roles] > [New 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
- [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



New Role	
Name:	VPNtest
Description:	11.
> Options	
✓ Access Features	
Check the features to enable for this	s user role, and specify any role-based options. Note that features disabled here
U Web	
Files, Windows	
Secure Application Mana	ager
O Windows version	Note: On Windows Mobile, Pulse Secure client is delivered via WSAM
 Java version 	
Terminal Services	
Virtual Desktops	
HTML5 Access	
🔽 VPN Tunneling	(includes IKEv2)

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。 ※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) については本書では説明を割愛します

2.5. レルム(ユーザ認証)の作成

管理画面上部のメニューより[Users] > [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 Realm	
* Name:	VPNuser
Description:	li.
	□ When editing, start on the Role Mapping page
✓ Servers	
Specify the servers to use for authenticati	on and authorization. To create or manage servers, see the Servers page.
Authentication:	Gleas 🗸
User Directory/Attribute:	None ~
Accounting:	None ~
Device Attributes:	None 🗸

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「VPNtest」というロールにマ ッピングする例です。

Role M	apping Rule					
Rule bas	ed on: Usernan	ne	•	Update		
* Name:	VPNrule					
▼ Rule:	f username					
is		•	*		If more than o	one username
				/	li.	
✓ then a	assign these role	es				
Availab	ole Roles:			Selected Ro	oles:	
Users		^	Add -> Remove	VPNtest	^	
		~			~	
□ St	op processing ru	ules v	vhen this rule	e matches		
To mana	ige roles, see the F	loles c	configuration pa	ige.		

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

管理画面上部のメニューから[Authentication] > [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



 Authentication re 	alm				
Specify how to sel	ect an authenticat	tion realm when signing	in.		
O User types th	e realm name				
The user must ty	pe the name of one o	f the available authentication	realms.		
👩 User picks fro	om a list of authe	entication realms			
The user must ch realms, see the U Available realm	noose one of the follo Jser Authentication pa ns:	wing selected authentication age or the Administrator Auth Selected realm	realms when they sign in. If only one tentication page.		
Users	Add	d -> VPNuser	Move Up		
Remove 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。

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>pc</u>	PC用UA

[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

▶基本設定	
□ トークンへのインポート	管理するトークン Gemalto .NETカード 🗸
✔ 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 く
」ダウンロードを許可 ダウンロードを許可	✓ インボートワンスを利用する ○ 分級申請券行われ)
	 □ 登録済みデバイスのみインポート許可
 CA証明書を含めない 	
	1747

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

※以下は、Gléas CertImporter を使う場合の例となります。事前に Gléas CertImporter のインストールが必要です。



※他の方法として、Edge ブラウザの IE モードを使ってのインポートも可能です(この場合は事前のアプリインストールは不要)

Edge(あるいは Chrome)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。

	ユーザの証明#	書ストアヘインポートしました。		Crews
テスト 太郎 さ	んのページ]		0/	D <u>0</u> 2
ユーザ情報			OK	
🙎 テスト 太郎	\$ さんのページ			
●コーザ情報	6			
トユーザ	▲ 登録日時:2	020/08/14 15:46		
≥姓:テスト 4	4:太郎			
>ユーザID:test	user			
> マールマドレフ				

※初回インポート時には、Windows OS によりルート証明書確認のセキュリティ警告が表示され ます。拇印(フィンガープリント)を確認したうえでインストールするなどの運用が必要です(管理 者設定でルート証明書をインポートさせないようにすることも可能)

セキュリティ	整 <i>件</i> 三 日	
	発行者が次であると主張する証明機関 (CA) から証明書をインストールしようと しています:	
	JCCH-SSS demo2 CA	
	証明書が実際に "JCCH-SSS demo2 CA* からのものであるかどうかを検証でき ません。"JCCH-SSS demo2 CA* に連絡して発行者を確認する必要がありま す。次の番号はこの過程で役立ちます:	
	握印 (sha1): B96112E5 C0F29BA8 8FAB66EE 92FA7161 C6A0B417	
	警告: このルート証明者をイソストールすると、この CA によって発行された証明者は自 動的に信頼されます。確認されていない妈印付きの証明者をイソストールすること は、セキュリティ上、危険です。(はい)をクリックすると、この危険を認識したことに なります。	
	この証明書をインストールしますか?	
	はい(Y) しいえ(N)	

インポートワンス機能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。

		プライベ	K-FCA Gléäs
- スト 太郎 さんの^	ページ]		■ <u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>
ユーザ情報			
🙎 テスト 太郎 さん	のページ		
2ユーザ情報			
▶ ユーザ	登錄日時: 2020/08/14 15:46		
≥姓:テスト 名:太郎			
>ユーザID : testuser			
≥メールアドレス:			

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、証明書認証がバックグラウンドでおこなわれたのちに接続します。



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。

Secure −×	
ファイル(F) ヘルプ(H)	
接続 + ノ ×	
▼ Ivanti 生取しました	Signature Desktop Client →
サーバー URL: ivanti	Pulse Secure 接続に失敗しました。
ステータス: 矢取しました 詳細: クライアント証明書が失効されました。	接続: Ivanti 理由・クライアント証明書が失効されました
コンプライアンス:	詳細についてはここをクリックしてください。

証明書のない状態でアクセスすると以下のエラーが表示されます。



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。 ※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。

[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	□上級者向上
□ トークンへのインボート	管理するトークン Gemalto .NETカード 🗸
□ 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 ダウンロード可能時間(分) 1	 ✓ インボートワンスを利用する ✓ 登録申請を行わない ● 登録済みデバイスのみインボート許可
□ CA証明書を含めない	_
	(\$77)

[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、[名前]、 [識別子]、[プロファイルの組織名]、[説明]の項目を入力します。

🦸 認証デバイス情報		
▶ iPhone / iPadの設定		
🔽 iPhone/iPad 用 UA を利用	する	
画面レイアウト		
✓ iPhone 用レイアウトを使用 ● Mac OS X 10.7以降の接続	する 徳許可	✔ ログインパスワードで証明書を保護
OTA(Over-the-air)		
 OTAエンロールメントを利用 	ける	□ 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	設定	
名前(デバイス上に表示)	JS3 Demo Profile	
識別子(例: com.jcch-	com.jcch-sss.profile	
sss.profile)		
ブロファイルの組織名	JS3	
記印	テストプロファイル	

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-VPNの設定			
SSL-VPN 接続名	lvantiテスト		
SSL-VPN ホスト名	ivanti		
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

				JETA-PCA Gléas		
テスト 太郎	阝さんのページ]			■ <u>ログア</u>		
ユーザ情報		_	_			
8 7 75	太郎 さんのページ					
오그-ザ	青報 · · · · · · · · · · · · · · · · · · ·					
▶ ユーザ	£	録日時 : 2020/08/14 15:46				
> 姓 : テスト	名:太郎					
> ユーザID : testuser						
> X − /L :						
秉 証明書	青報・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・					
▶発行済み	証明書					
#	発行局	シリアル	有効期限	ダウンロード		
\$ 1	JCCH-SSS demo2 CA	#453	2022/08/30	構成プロファイルのダウンロード		

プロファイルのダウンロードが完了すると、設定アプリからインストールするよう 促されます。





設定アプリからプロファイルのインストールを行います。



[詳細]をタップすると、プロファイルの内容を確認することができます。



画面の指示に従い、インストールを完了させます。





Safariに戻り UA画面の[ログアウト]をタップしてログアウトします。

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 「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。

				プライベートCA Gléäs UA
[テスト 太郎 さんの	0ページ]			■ ログアウト
ユーザ情報		_		
🙎 テスト 太郎 さん	のページ			
2 ユーザ情報				
▶ ユーザ	登録日時 : 2020/	08/14 15:46		
≫姓:テスト 名:太郎				
> X-JL :				
★ 証明書情報 ·····				
▶発行済み証明書				
#	発行局	シリアル	有効期限	ダウンロード
<u>\$1</u>	JCCH-SSS demo2 CA	#453	2022/08/30	ダウンロード済み

6.3. 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接続先は設定された状態となります。

	Pulse Secure	
接続		
● Ivantiテスト ivan		•••
	接続	

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。

0.44 1878(6)	Pulse Secure	🗢 আল 72% 💽
接続		
● Ivantiテスト https://ivanti.		•••
イントラネット		>
	切断	
💲 testuser		00:59:44

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。





7. 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。

■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