



JCCH・セキュリティ・ソリューション・システムズ

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

- ・ 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。

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

目次

1. はじめに	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. Connect 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	13
2.4. ロール（ユーザ権限）の作成.....	13
2.5. レルム（ユーザ認証）の作成.....	14
2.6. サインインポリシーの設定	16
3. Gléas の管理者設定（PC）	17
4. PC での接続操作	18
4.1. クライアント証明書のインポート	18
4.2. クライアントからの VPN 接続（PC）	19
5. Gléas の管理者設定（iPad）	20
5.1. UA（ユーザ申込局）設定.....	21
6. iPad での接続操作	22
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. Pulse Secure から接続	25
7. 問い合わせ	27

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」を利用する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。

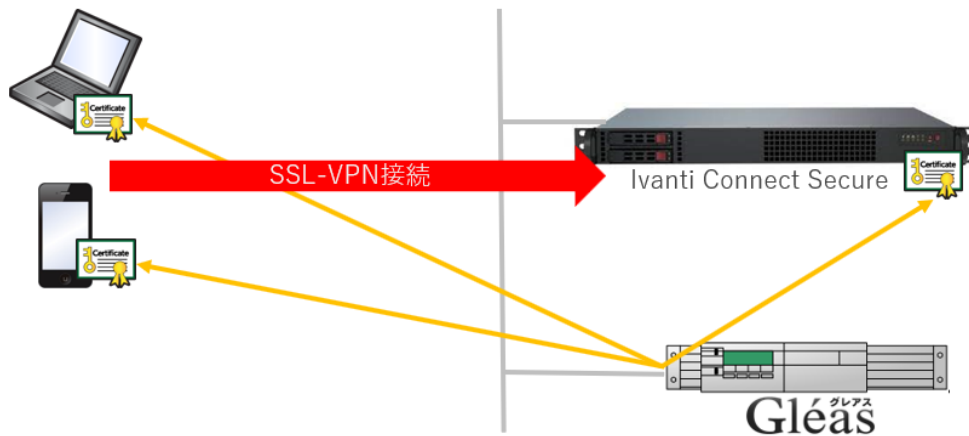
- Connect Secureでのサーバ証明書設定やネットワーク設定、アクセス権限等の設定
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作
- PCのネットワーク設定等の基本設定、Pulse Secureクライアント、Gléas CertImporterアプリおよびブラウザ拡張機能のインストール方法
- iPadのネットワーク設定等の基本設定、Pulse Secureクライアントのインス

ツール方法

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。



1. 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。

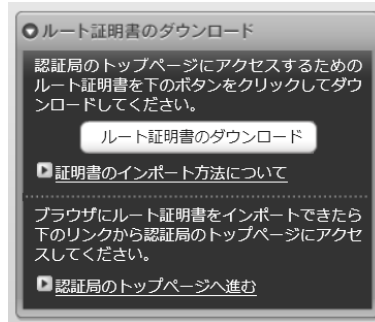
2. Connect Secureの設定

2.1. 信頼するルート認証局の設定

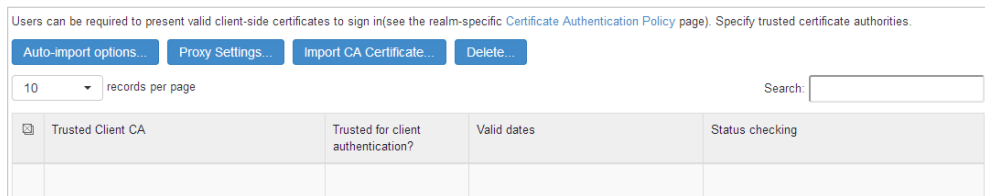
今回利用するクライアント証明書のトラストアンカとなるルート認証局を設定します。

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

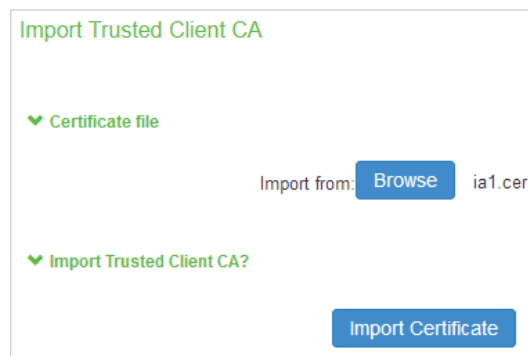
事前に Gléas よりルート証明書をダウンロードしておきます。
Gléas に `http://hostname/` (`http` であることに注意) でアクセスすると、ダウンロードが可能です。



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。



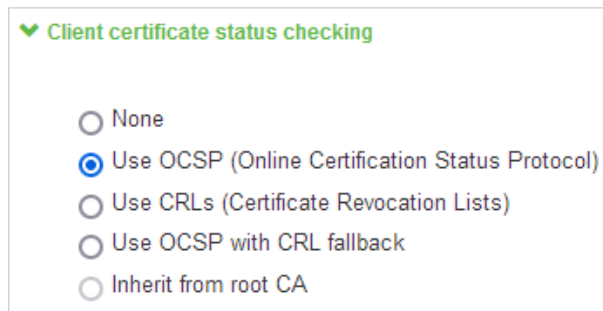
[Import From:]のところで[Browse]ボタンを押し、ローカルに保存してあるルート証明書を選択し、[Import Certificate]ボタンをクリックします。



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

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

Configuration > Trusted Client CAs > JCH-SSS demo2 CA >
OCSP Options

Specify the OCSP options to use during enduser certificate verification.

Use: Responder(s) specified in the client certificates ▾
OCSP Responder URLs will be retrieved during client authentication.

OCSP responders	Last Used

▼ Options

Device Certificate to sign the request : -- Do not sign the request -- ▾

Signature Hash Algorithm: SHA-1 SHA-2

Use Nonce

Save Changes

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。

▼ Client certificate status checking

None

Use OCSP (Online Certification Status Protocol)

Use CRLs (Certificate Revocation Lists)

Use OCSP with CRL fallback

Inherit from root CA

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。

Configuration > Trusted Client CAs > JCH-SSS demo2 CA >
CRL Checking Options
Specify the CRL distribution point(s) from which to download the CRL, as well

Use:

Certificates vary in how they specify CDPs. If the client 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 Frequency: hours (1-9999) Note that CRLs can also sp

Validate Server Certificate (LDAPS only)

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）。

▼ Client certificate status checking

None

Use OCSP (Online Certification Status Protocol)

Use CRLs (Certificate Revocation Lists)

Use OCSP with CRL fallback

Inherit from root CA

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)。

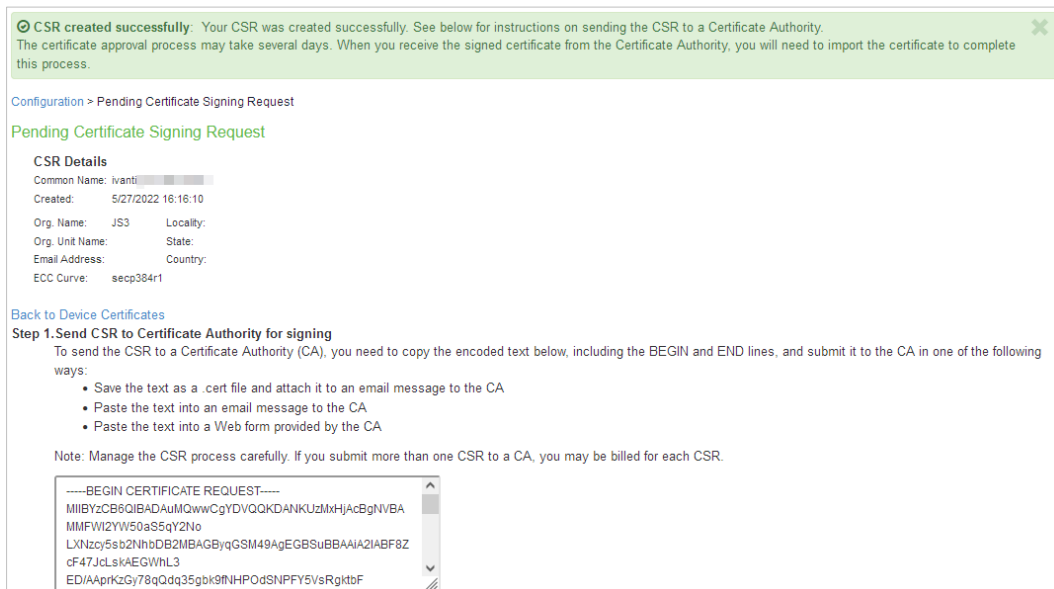
2.2. サーバ証明書の設定

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。



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。

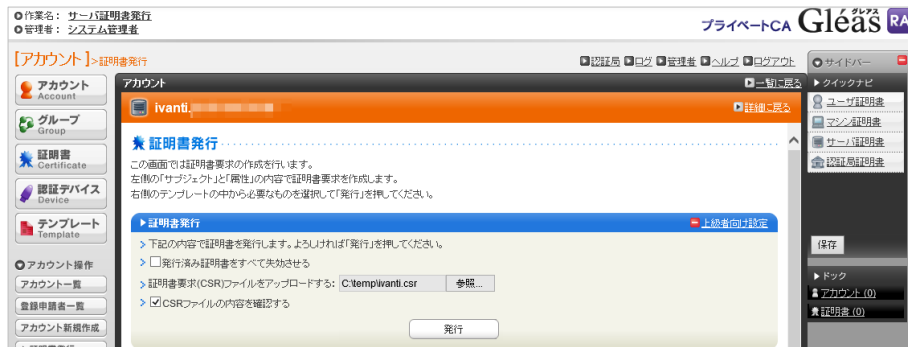


上級者向け設定を展開し、以下の操作をおこないます。

- 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

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

その後、[発行]ボタンをクリックします。



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。

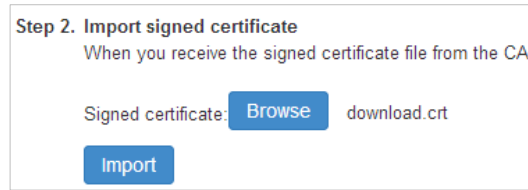


証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書：あり」をクリックし、発行された証明書をダウンロードします。

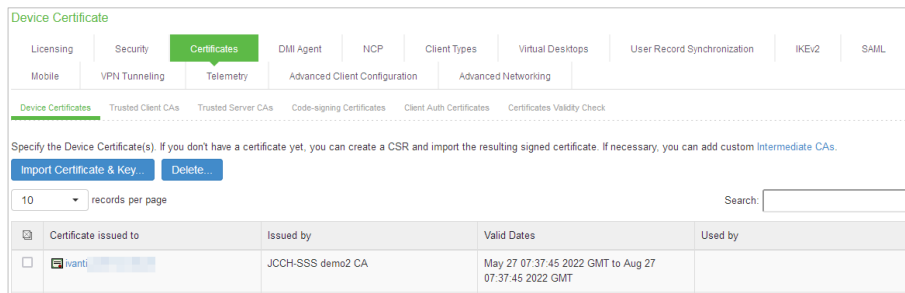


Connect Secure に戻り、ダウンロードした証明書を指定し、[Import]をクリックしアップロードします。

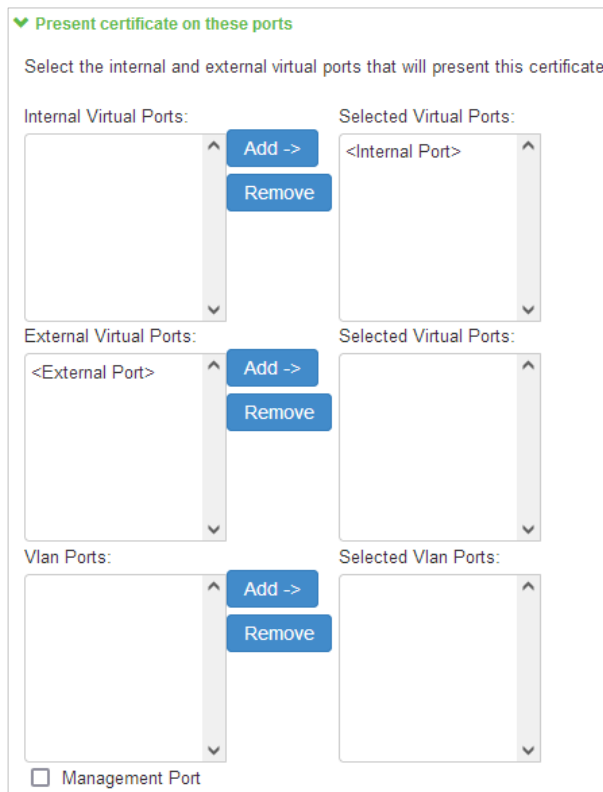
プライベート認証局 Gléas ホワイトペーパー
Ivanti Connect Secure クライアント証明書認証設定



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。



※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 Server

*Name: Label to reference this server.

User Name Template: 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

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 Role

Name:

Description:

Options

Access Features

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here r

Web

Files, Windows

Secure Application Manager

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)

Secure Mail

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:

Description:

When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication:

User Directory/Attribute:

Accounting:

Device 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。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...]項目にはこのル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項で作成したルールを選択
- 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 Mapping Rule

Rule based on: Username Update

* Name: VPNrule

Rule:if username...

is * If more than one username

then assign these roles

Available Roles: Users Selected Roles: VPNtest

Add -> Remove

Stop processing rules when this rule matches

To manage roles, see the [Roles configuration page](#).

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. サインインポリシーの設定

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 realm

Specify how to select an authentication realm when signing in.

User types the realm name
The user must type the name of one of the available authentication realms.

User picks from a list of authentication realms
The user must choose one of the following selected authentication realms when they sign in. If only one realm, see the [User Authentication](#) page or the [Administrator Authentication](#) page.

Available realms: Selected realms:

Users Add -> Remove VPNUser Move Up 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に設定します。
※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。



[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 上級者向け

トークンへのインポート

証明書ストアへのインポート

ダウンロードを許可
ダウンロード可能時間(分) 0

CA証明書を含めない

管理するトークン Gemalto .NETカード ▼

証明書ストアの種類 ユーザストア ▼

インポ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ポート許可

保存

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

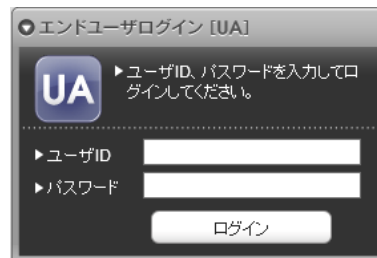
※以下は、Gléas CertImporter を使う場合の例となります。事前に Gléas CertImporter のインストールが必要です。



※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。



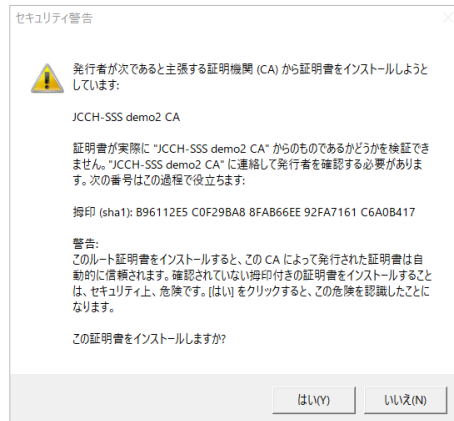
ログインすると、ユーザ専用ページが表示されます。

[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。



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

※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)



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。



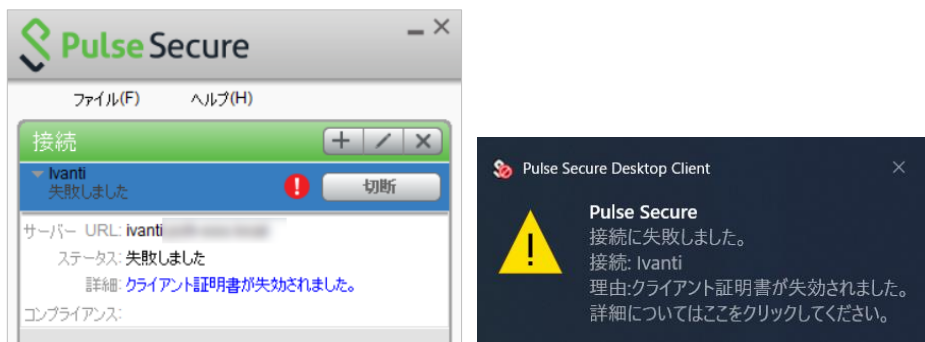
4.2. クライアントからのVPN接続 (PC)

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。

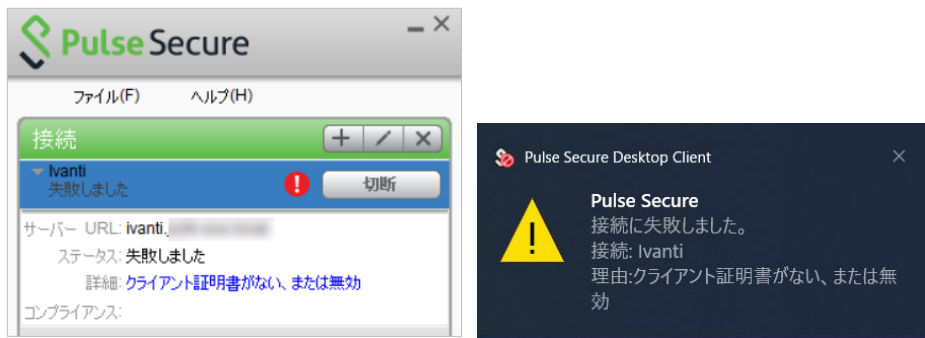
プライベート認証局 Gléas ホワイトペーパー
Ivanti Connect Secure クライアント 証明書認証設定



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。



証明書の無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

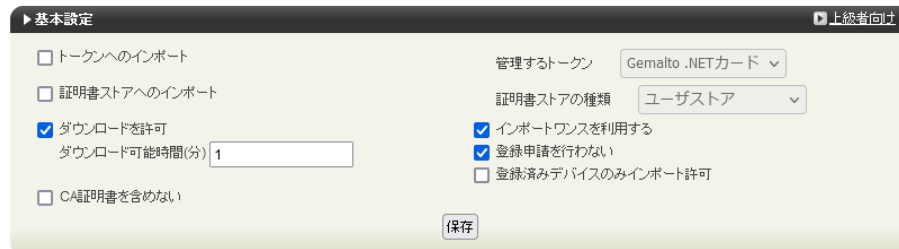
5.1. UA（ユーザ申込局）設定

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。



[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。



構成プロファイル生成に必要な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。

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

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

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

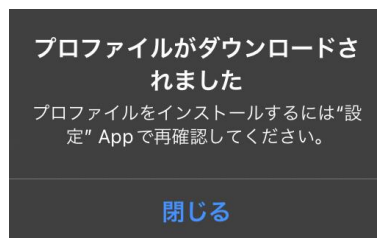


プロファイルのダウンロードが完了すると、設定アプリからインストールするよう促されます。

このWebサイトは構成プロファイルをダウンロードしようとしています。許可しますか？

無視 許可

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



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。

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



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。

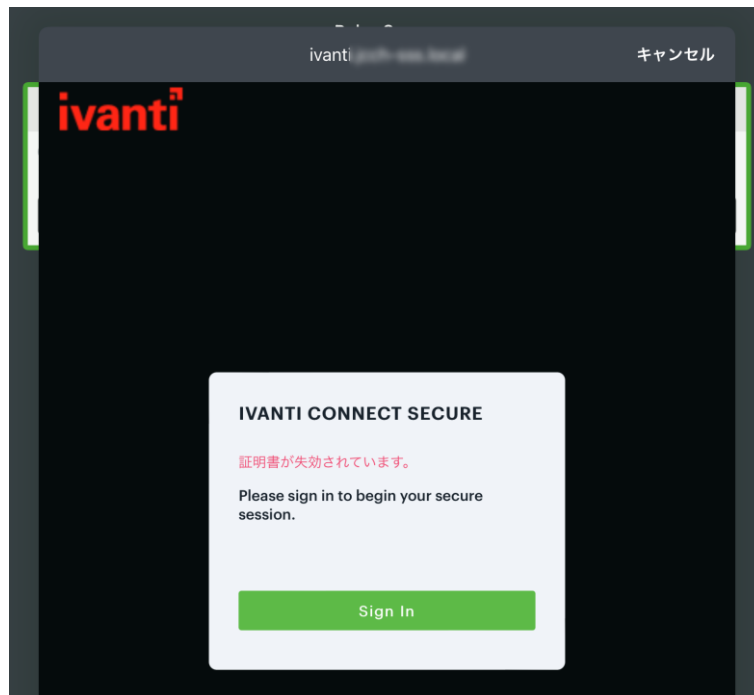


6.3. Pulse Secureから接続

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。



以下はPulse Secureから接続した画面です。



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