



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

GlobalProtectでのクライアント証明書認証

Ver. 1.0

2021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・システムズの登録商標です。
- ・ 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  
GlobalProtectでのクライアント証明書認証

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. Gléas における留意事項 .....	5
2. PA-Firewall の設定 .....	6
2.1. サーバ証明書の登録 .....	6
2.2. ルート証明書、および OCSP 証明書のインポート .....	10
2.3. VPN クライアント証明書認証の設定 .....	11
3. Gléas UA の管理者設定 (Windows 用) .....	13
4. クライアントからのアクセス (Windows) .....	14
4.1. クライアント証明書のインポート .....	14
4.2. GlobalProtect から PA-Firewall への VPN アクセス .....	16
5. Gléas UA の管理者設定 (iPhone 用) .....	16
6. クライアントからのアクセス (iPhone) .....	18
6.1. クライアント証明書のインポート .....	18
6.2. PA-Firewall へのアクセス .....	20
7. 問い合わせ .....	21

## 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」で発行されたクライアント証明書を利用して、パロアルトネットワークス社のSSL-VPN「GlobalProtect」にて証明書認証をおこな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。

### 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。

- ▶ UTM(SSL-VPNゲートウェイ) : Palo Alto Firewall VM (PAN-OS 10.0.4)
  - ※ 以後、「PA-Firewall」と記載します
- ▶ JS3 プライベート認証局 Gléas (バージョン2.2.5)
  - ※ 以後、「Gléas」と記載します
- ▶ ディレクトリサービス : Windows Server 2012 R2 / Active Directory Domain Services
  - ※以後、「ドメインコントローラ」と記載します
- ▶ クライアント : Windows 10 Pro (バージョン20H2) /  
GlobalProtect (バージョン 5.2.6-87)
  - ※ 以後、「Windows」と記載します
- ▶ クライアント : iPhone 12 Pro (iOS 14.4.2) /  
GlobalProtect (バージョン 5.2.7-6)
  - ※ 以後、「iPhone」と記載します

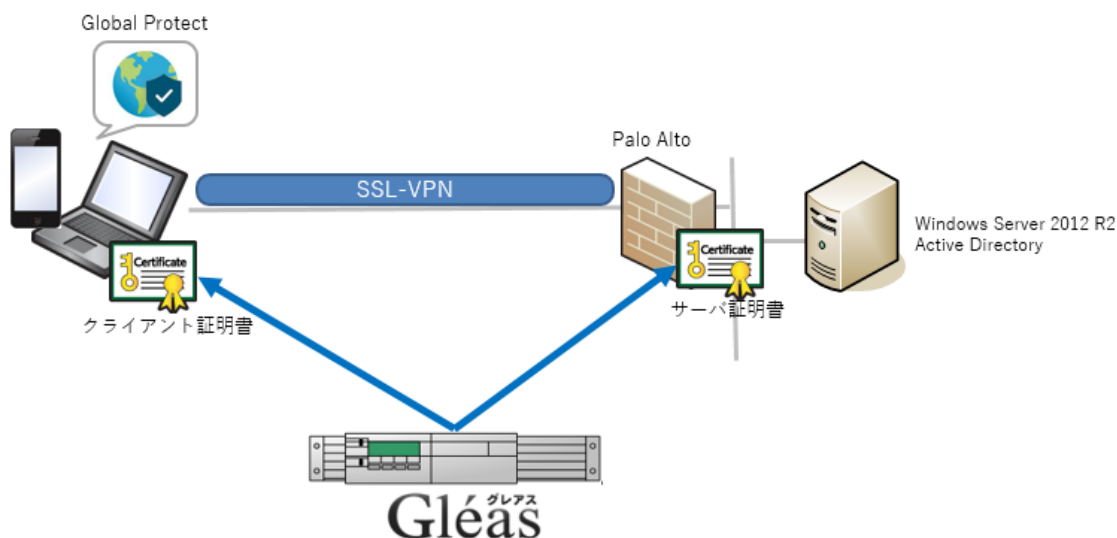
以下については、本書では説明を割愛します。

- PA-Firewallの一般的な設定 (ネットワーク的な設定、VPN設定、AD連携設定など)
  - ※ 本書はGlobalProtectからのADと連携したパスワード認証によるPA-FirewallへのSSL-VPN接続が可能なことを前提としています
- GlobalProtectのインストール方法
- Gléasでのアカウント登録やクライアント証明書発行などの基本操作

これらについては、各製品・サービスのマニュアル・ヘルプをご参照いただくか、各製品を取り扱う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はサーバ証明書を発行し、PA-Firewallに適用する
2. Gléasはクライアント証明書を発行し、GlobalProtectがインストールされたクライアントデバイスはGléasのUAにアクセスし、発行された証明書をインポートする
3. クライアント証明書とパスワード認証によるSSL-VPN接続をおこなう

クライアント証明書の展開方法はGléasのUAを使用する以外にも、PA-FirewallとGléasをSCEP (Simple Certificate Enrollment Protocol)で連携させて、PA-Firewallのポータルよりクライアント証明書を配布するといった方法も可能です。

(本書ではこの手順は割愛します)

### 1.4. Gléas 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。

- Gléasで発行するサーバ証明書の有効期間は825日未満である必要があります。(macOS 10.15以降、およびiOS 13以降における制約)
- iPhoneについて、GlobalProtect向けにクライアント証明書 (VPN用構成プロファイル) のインポートをおこなうためにはGléasにオプションを適用する必要があります。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。

## 2. PA-Firewallの設定

### 2.1. サーバ証明書の登録

PA-Firewall で CSR（証明書署名要求）を作成します。

※ Gléas で証明書発行要求（CSR）を作成してサーバ証明書を発行することも可能です。本書ではその手順は割愛します

PA-Firewallの管理UIにログイン後、上部メニューより[DEVICE]をクリックし、左側のメニューより[証明書の管理] > [証明書]と進みます。メイン画面下部で [生成]をクリックし以下をおこなない証明書署名要求（CSR）データを生成します。

- 証明書タイプは、[ローカル]を選択
- 証明署名には、任意の識別名を入力
- 共通名には、クライアントから見たアクセス先となるPA-Firewallのホスト名を入力
- 署名者には、[External Authority (CSR)]を選択
- [秘密鍵のエクスポートをブロック]をチェック

以下はRSA 2048ビットの鍵長でCSRを作成する例です。[生成]をクリックするとCSRが作成されます。

プライベート認証局 Gléas ホワイトペーパー  
GlobalProtectでのクライアント証明書認証

※ 共通名（サーバホスト名）、暗号アルゴリズム、鍵長は、Gléas のサーバアカウントに適用されているテンプレート内容と一致する必要があります。一致しない場合、Gléas での証明書発行時にテンプレート不一致でのエラーとなります

CSRが追加されます。画面下部の[証明書のエクスポート]よりファイルダウンロードします。

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。

プライベート認証局 Gléas ホワイトペーパー  
GlobalProtectでのクライアント証明書認証



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。



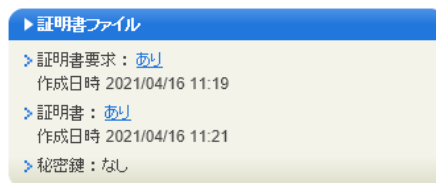
証明書の要求内容が表示されるので確認し、[▶この内容で発行する]をクリックし、証明書の発行をおこないます。



## プライベート認証局 Gléas ホワイトペーパー GlobalProtectでのクライアント証明書認証

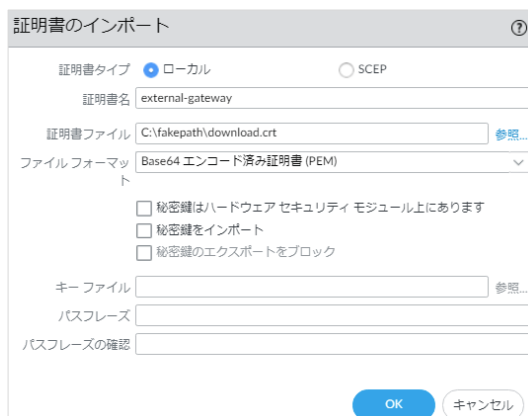


証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書：あり」をクリックし、発行された証明書をダウンロードします。



PA-Firewall の管理 UI に戻り、[インポート]をクリックし Gléas からダウンロードした証明書ファイルをアップロードします。

- 証明書名には、CSR 作成時につけた名前を入力
- 証明書ファイルには、Gléas からダウンロードしたファイルを指定
- ファイルフォーマットには、[Base64 エンコード済み証明書 (PEM)]を選択



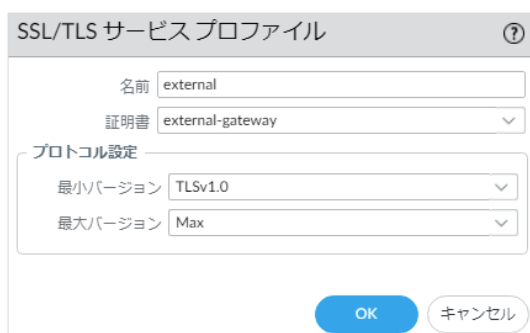
インポートされたサーバ証明書が一覧に表示されます。

プライベート認証局 Gléas ホワイトペーパー  
GlobalProtectでのクライアント証明書認証



名前	サブジェクト	発行者	CA	キー	有効期限	状態	アルゴリズム	用途
external-gateway	CN = palo	JCCH-SSS demo...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Apr 27...	有効	RSA	

[証明書の管理] > [SSL/TLS サービスプロファイル]を選択し、インポートしたサーバ証明書を含むプロファイルを作成します。



SSL/TLS サービスプロファイル

名前: external

証明書: external-gateway

プロトコル設定

最小バージョン: TLSv1.0

最大バージョン: Max

OK キャンセル

画面上部の[NETWORK]をクリックし、[GlobalProtect] > [ゲートウェイ]を選択し、対象のGlobalProtect ゲートウェイ設定を開きます。

左側の[認証]タブをクリックし、サーバー認証欄の[SSL/TLS サービスプロファイル]で作成したプロファイルを選択します。



GlobalProtect ゲートウェイ設定

全般

認証

サーバー認証

SSL/TLS サービスプロファイル: external

上記完了後に、設定の反映のためにコミットをおこないます。

## 2.2. ルート証明書、および OCSP 証明書のインポート

事前に Gléas よりルート証明書ファイルと、失効確認に用いる OCSP 証明書ファイルをダウンロードしておきます。

デフォルトの PEM 形式のルート証明書ダウンロード URL は以下の通りです。

<http://gleas.example.com/crl/ia1.pem>

ルート証明書のインポート手順は、サーバ証明書をインポートするときと同様です。

## プライベート認証局 Gléas ホワイトペーパー GlobalProtectでのクライアント証明書認証

証明書のインポート

証明書タイプ  ローカル  SCEP

証明書名

証明書ファイル  参照...

ファイルフォーマット

秘密鍵はハードウェアセキュリティ モジュール上にあります

秘密鍵をインポート

秘密鍵のエクスポートをブロック

キーファイル  参照...

パスフレーズ

パスフレーズの確認

OK キャンセル

OCSP 証明書は、Gléas の RA にログインして OCSP レスポンス署名に指定されている証明書をダウンロードして入手します。

※ 2.1 項と同様に証明書ファイルのみをダウンロードします。PKCS12 形式のファイル(拡張子が.p12 のもの)ではありません

OCSP 証明書のインポート手順もルート証明書の場合と同様です。  
インポートが完了すると、一覧に表示されます。

名前	サブジェクト	発行者	CA	キー	有効期限	状態	アルゴリズム	用途
gleas_ca	CN = EVALUATION CA...	CN = EVALUATION CA, ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Mar 31...	有効	RSA	
ocsp-sign	CN = ocsp-sign	CN = EVALUATION CA, ...	<input type="checkbox"/>	<input type="checkbox"/>	Mar 30...	有効	RSA	

上記完了後に、設定の反映のためにコミットをおこないます。

### 2.3. VPN クライアント証明書認証の設定


PA-Firewall の管理 UI メニューから[証明書] > [証明書プロファイル]をクリックし、画面下部の[追加]をクリックし、クライアント証明書認証用のプロファイルを作成します。

- 名前には、任意の識別名称を入力
- ユーザー名フィールドには、[サブジェクト]を選択
- CA 証明書で、[追加]をクリックし、開いたウィンドウで以下を設定
  - CA 証明書には、前項でインポートしたルート証明書を選択
  - デフォルト OCSP URL には、Gléas の OCSP URL を入力
  - OCSP 検証証明書には、前項でインポートした OCSP 証明書を選択

※ Gléas のデフォルト CA の OCSP URL は以下の通りになります

<http://gleas.example.com:2560/ia1>

プライベート認証局 Gléas ホワイトペーパー  
GlobalProtectでのクライアント証明書認証



- [OCSP の使用]にチェック
  - ※ PA-Firewall では CRL による失効確認もサポートされています。CRL を使う場合はクライアント証明書に CRL 配布ポイントを付加するよう Gléas のテンプレートをセットする必要があります
  - ※ OCSP と CRL を両方有効にした場合は、OCSP が優先されそのフォールバックに CRL が利用されません（弊社未検証）
- [証明書状態が不明な場合にセッションをブロック]にチェック
- [タイムアウト時間内に証明書状態を取得できない場合にセッションをブロック]にチェック
  - ※ [証明書状態が不明な場合にセッションをブロック]、[タイムアウト時間内に証明書状態を取得できない場合にセッションをブロック]のチェックを外すことで、OCSP 通信の障害時にも認証を継続することが可能と思われます（弊社未検証）
- [証明書が認証側デバイスに発行されなかった場合セッションをブロック]は、チェックしない
- [期限切れ証明書のセッションをブロック]にチェック



作成した証明書プロファイルを GlobalProtect ゲートウェイに適用します。

管理 UI 上部から[NETWORK]タブを選択し、左側メニューから[GlobalProtect] > [ゲートウェイ]をクリックし、クライアント証明書認証をおこなう GlobalProtect ゲートウェイ設定を開きます。

認証タブを開き、[証明書プロファイル]に上記で設定した証明書プロファイルを選択します。

## プライベート認証局 Gléas ホワイトペーパー GlobalProtectでのクライアント証明書認証



上記完了後に、設定の反映のためにコミットをおこないます。  
PA-Firewall の設定は以上です。

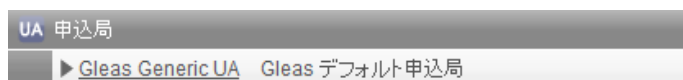
### 3. Gléas UAの管理者設定 (Windows用)

GléasのUA (申込局) より発行済み証明書をWindowsクライアントにインポートできるように設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

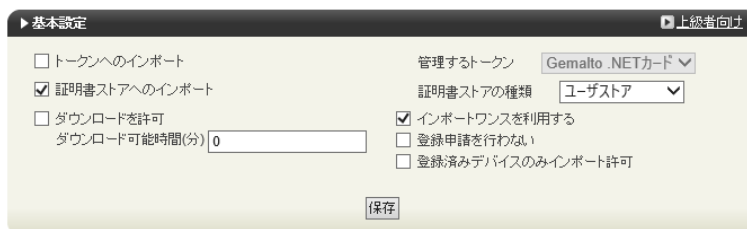
GléasのRA (登録局) にログインし、画面上部より[認証局]をクリックし認証局一覧画面に移動し、設定を行うUA (申込局) をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します



申込局詳細画面が開くので、基本設定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



設定終了後、[保存]をクリックし設定を保存します。また、認証デバイス設定の以下項目にチェックがないことを確認します。

- iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]
- Android/Windows Phone の設定の、[Android / Windows Phone 用 UA を利用する]
- 証明書インポートアプリ連携の設定の、[証明書インポートアプリを利用する]

以上でGléasの設定は終了です。

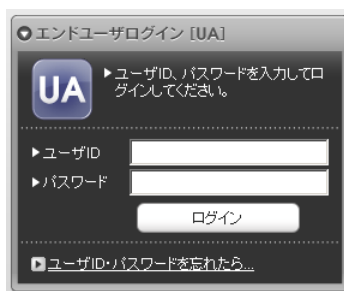
## 4. クライアントからのアクセス (Windows)

### 4.1. クライアント証明書のインポート

Internet Explorer (IE) 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、GléasでのユーザIDとパスワードを入力しログインします。

※ UAのログイン認証をActive Directoryで行うことも可能です。詳細は最終項のお問い合わせ先までご連絡ください

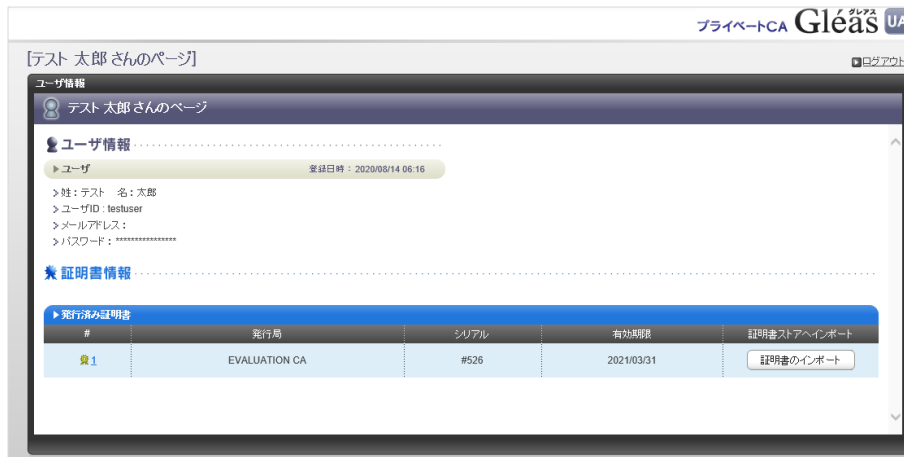


ログインすると、ユーザ専用ページが表示されます。

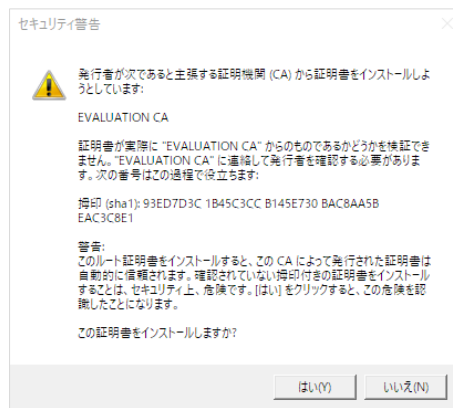
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。

※ 初回ログイン時には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ます

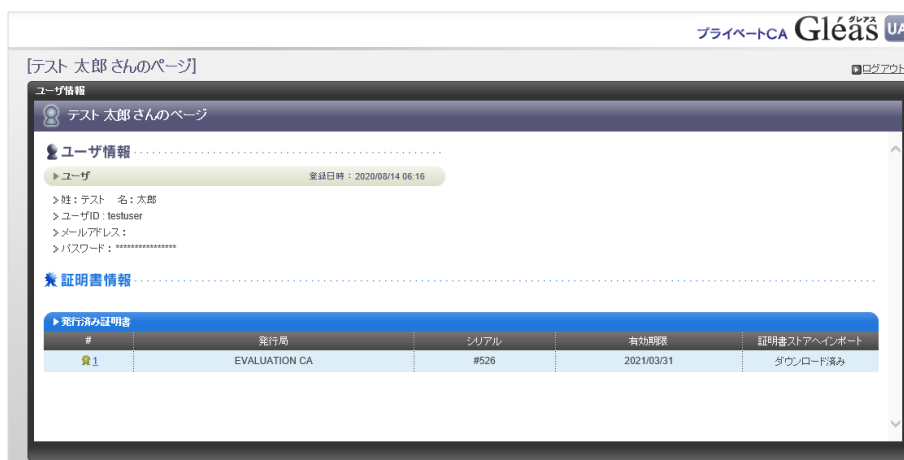
プライベート認証局 Gléas ホワイトペーパー  
GlobalProtectでのクライアント証明書認証



※ 証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を確認するなど正当性を確認してから[はい]をクリックします



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、再度ログインしてインポートをおこなうことはできません。



## 4.2. GlobalProtect から PA-Firewall への VPN アクセス

GlobalProtectで接続するとバックグラウンドで証明書認証がおこなわれて、パスワードを入力することによりPA-Firewallに接続します。



証明書がない状態、もしくは失効された証明書でアクセスすると以下のメッセージが出現します。



## 5. Gléas UAの管理者設定 (iPhone用)

Gléas で、発行済みのクライアント証明書を含む GlobalProtect 接続設定 (構成プロファイル) を iPhone 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

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



プライベート認証局 Gléas ホワイトペーパー  
GlobalProtectでのクライアント証明書認証

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、基本設定で以下の設定をおこないます。

- [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)を経過した後は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iOSデバイス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) 1

次に、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な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。

- [iPhone用レイアウトを使用する]をチェック
- [ログインパスワードで証明書を保護]をチェック
- [名前]、[識別子]、[プロファイルの組織名]、[説明]に任意の文字を入力

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する  ログインパスワードで証明書を保護

Mac OS X 10.7以降の接続を許可

OTA(Over-the-air)

OTA Enrollment を利用する  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

iPhone 構成プロファイル基本設定

名前(デバイス上に表示) プライベートCA Gleas

識別子(例: com.jcch-sss.profile) com.jcch-sss.profile

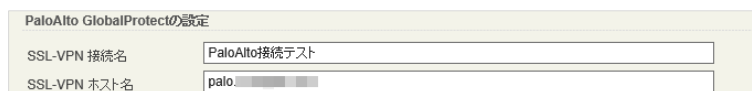
プロファイルの組織名 JCCHセキュリティソリューション・システムズ

説明 プライベートCA Gleas で作成した構成プロファイル

PaloAlto GlobalProtectの設定に以下を設定します。

プライベート認証局 Gléas ホワイトペーパー  
GlobalProtectでのクライアント証明書認証

- [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PA-Firewallのホスト名（或いはIPアドレス）を入力（必須）



PaloAlto GlobalProtectの設定	
SSL-VPN 接続名	PaloAlto接続テスト
SSL-VPN ホスト名	palo.....

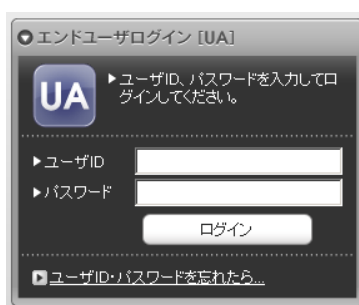
各項目の入力が終わったら、[保存]をクリックします。

以上でGléasの設定は終了です。

## 6. クライアントからのアクセス (iPhone)

### 6.1. クライアント証明書のインポート

iPhoneのブラウザ (Safari) でGléas UAのログイン画面にアクセスし、ユーザIDとパスワードを入力しログインします。



● エンドユーザログイン [UA]

UA ▶ ユーザID、パスワードを入力してログインしてください。

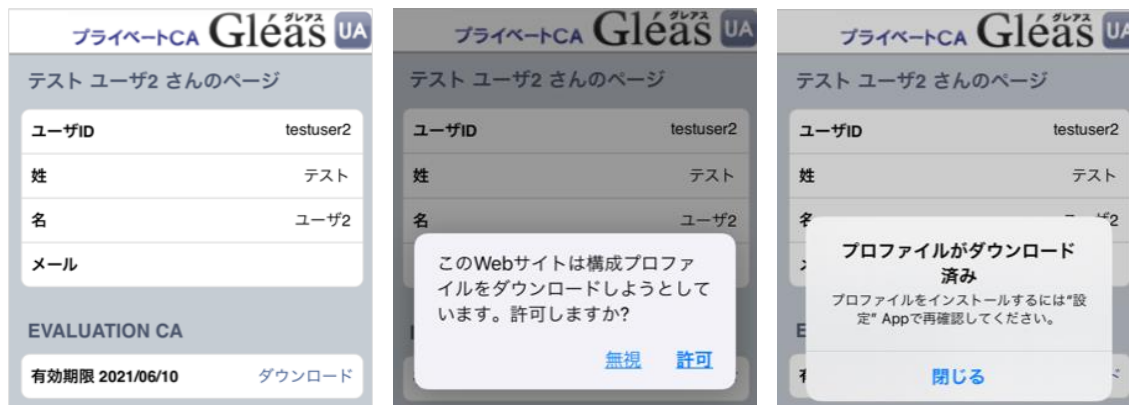
▶ ユーザID

▶ パスワード

ログイン

▶ ユーザID・パスワードを忘れたら...

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おこないます。



プライベート認証局 Gleas ホワイトペーパー  
GlobalProtectでのクライアント証明書認証

画面の表示にしたい設定アプリを開くと、プロファイルがダウンロードされた旨が表示されるので、インストールをおこないます。



なお、[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できます。必要に応じて確認してください。



Safariに戻り、[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、iPhoneでの構成プロファイルのインストールは終了です。

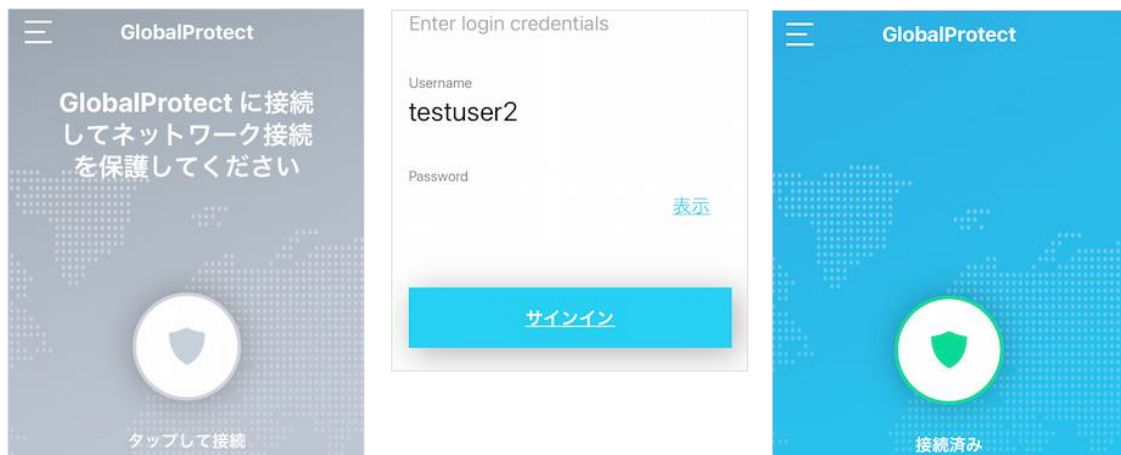
なお、本書のようにサーバ証明書をGleasで発行した場合は、設定アプリから[一般] > [情報] > [証明書信頼設定]と進み、インポートしたルート認証局を信頼するという手順が必要になります。

プライベート認証局 Gléas ホワイトペーパー  
GlobalProtectでのクライアント証明書認証



## 6.2. PA-Firewall へのアクセス

GlobalProtectアプリを起動するとすでに設定済みの状態になっています。  
接続試行時にパスワードを入力するとバックグラウンドで証明書認証をおこない、PA-FirewallにVPN接続します。



なお、証明書がない状態、もしくは失効された証明書でアクセスすると以下のメッセージが出現します。



## 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。

### ■本検証内容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  
営業本部

Tel: 050-3821-2195

Mail: sales@jcch-sss.com