



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

FortiGate SSL-VPNでのクライアント証明書認証

Ver. 1.0

2021年3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。

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. FortiGate の設定	6
2.1. 証明書設定画面の表示機能設定	6
2.2. サーバ証明書の登録	6
2.3. ルート証明書のインポート	7
2.4. SSL-VPN 設定	8
2.5. 失効リスト (CRL) の設定	8
3. Gléas の管理者設定 (Windows 用)	9
4. クライアントからのアクセス (Windows)	10
4.1. クライアント証明書のインポート	10
4.2. FortiClient からのアクセス (Windows)	12
5. Gléas の管理者設定 (iPhone / Android)	13
6. クライアントからのアクセス (iPhone)	15
6.1. ルート証明書のインポート	15
6.2. クライアント証明書のインポート	16
6.3. FortiClient での証明書のインポートと接続	18
7. クライアントからのアクセス (Android)	19
7.1. ルート証明書のインポート	19
7.2. クライアント証明書のインポート	21
7.3. FortiClient での証明書のインポートと接続	21
8. シナリオ 2 : LDAP-integrated certificate authentication	23
8.1. FortiGate の設定	23
8.2. FortiClient からの接続	24
9. 問い合わせ	25

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、フォーティネット社のUTMである FortiGate のSSL-VPN機能でクライアント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利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。

- VPNゲートウェイ：FortiGate 60E (ファームウェア v6.2.7 build1190 (GA))
※以後、「FortiGate」と記載します
- JS3 プライベート認証局 Gléas (バージョン2.2.2)
※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) /
FortiClient (バージョン 6.4.3.1608)
※以後、「Windows」と記載します
- クライアント：iPhone12 Pro (バージョン14.4) /
FortiClient VPN (バージョン 6.4.6.0539)
※以後、「iPhone」と記載します
- クライアント：Google Pixel 5 (Android バージョン11) /
FortiClient VPN (バージョン 6.4.4.0484)
※以後、「Android」と記載します

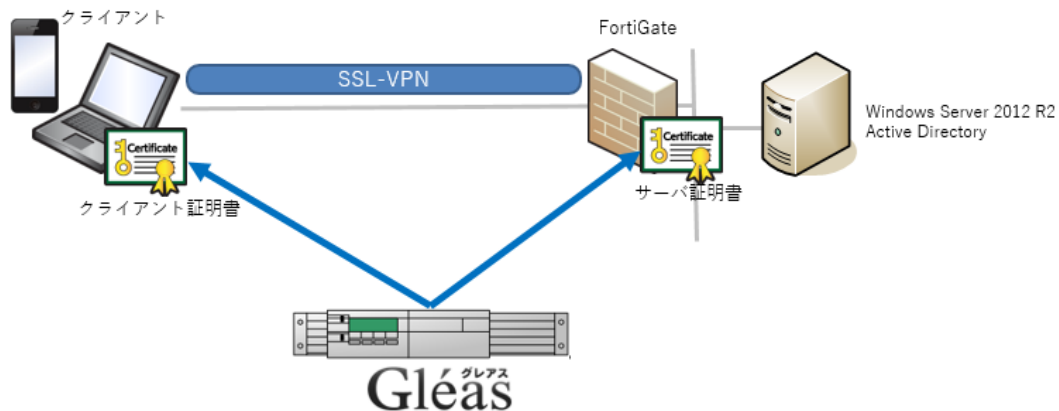
以下については、本書では説明を割愛します。

- FortiGate SSL-VPNの設定手順
※パスワード認証環境を構築可能な前提で本書は記載されています
- FortiGateでのActive Directoryとの連携
- Gléasでのサーバ・クライアント証明書の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、FortiGateに適用する。
2. Gléasはクライアント証明書を発行し、FortiClientが参照できる形式でクライアントデバイスに配布する。
3. 【シナリオ1】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。
4. 【シナリオ2】LDAP Integration Authentication を設定し、証明書に含まれるユーザプリンシパル名と、Active DirectoryのuserPrincipalName属性の一致をチェックするようにする

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については、クライアント証明書の取り込みに FortiClient 向けカスタマイズ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)。
- シナリオ2の場合は、クライアント証明書のサブジェクト代替名にユーザプリンシパル名 (ADのuserPrincipalName属性値) を含める必要があります。

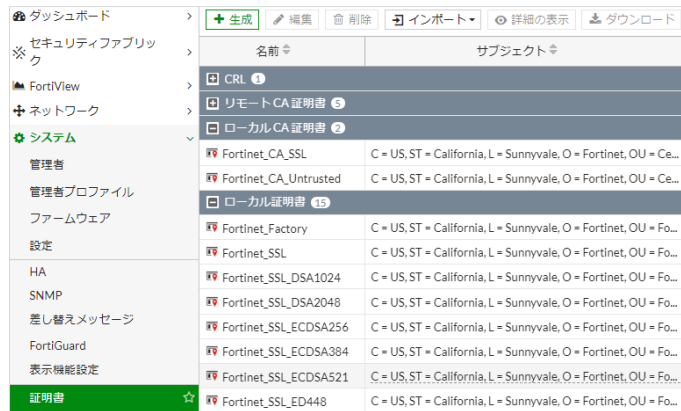
2. FortiGate の設定

2.1. 証明書設定画面の表示機能設定

デフォルトの状態では証明書の設定画面は表示されないため、表示設定を変更します。
管理画面のメニューから[システム] > [表示機能設定]をクリックし、[証明書]をオンにします。



証明書メニューが表示されます。



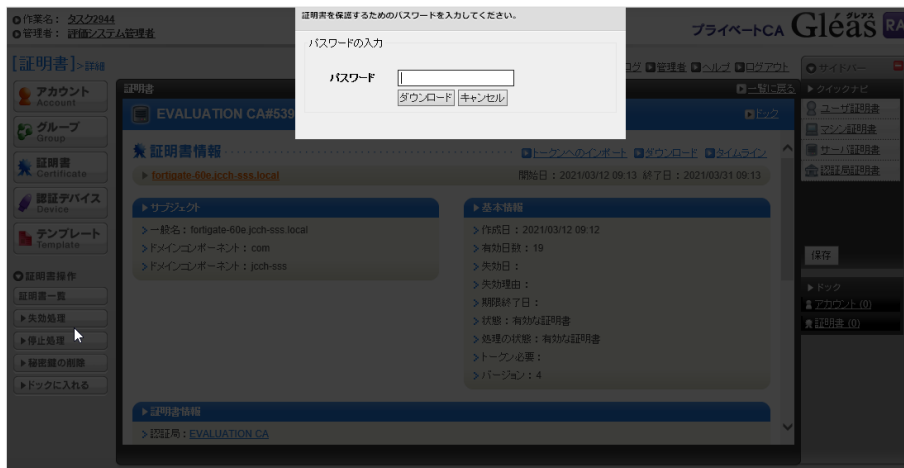
2.2. サーバ証明書の登録

あらかじめGléasで発行したサーバ証明書ファイル(拡張子が".p12"のもの)をローカルにダウンロードしておきます。

※ FortiGate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が、本書では割愛します

※ Gléasから証明書ファイルのダウンロード時に設定するパスワードは、FortiGateへのインポートに必要になります(以下)

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



管理画面のメニューから [システム] > [証明書] をクリックし、上部メニューから [インポート] > [ローカル証明書] をクリックします。インポート画面で以下の設定をおこないます。

- タイプ：PKCS12 証明書を選択
- キーファイルのある証明書：ローカルにダウンロードした証明書ファイルを選択
- パスワード：Gléas からダウンロードした際に設定したパスワードを入力
- 証明書名：任意の識別名称



登録したものが「ローカル証明書」として表示されます。

名前	サブジェクト	コメント	発行者	有効期限	ステータス	送信元	参照
ローカル証明書							
fortigate-60e.jcch-sss.local	CN = fortigate-60e.jcch-sss.local		JCCH Security Solution Systems ...	2022/03/01 ...	有効	ユーザ	0

2.3. ルート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をダウンロードしておきます。

デフォルト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.der>

管理画面のメニューから [システム] > [証明書] をクリックし、上部メニューから [インポート] > [CA 証明書] をクリックします。インポート画面で以下の設定をおこないます。

- タイプ：ファイルを選択

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

- アップロード：ローカルにダウンロードしたルート証明書ファイルを選択



登録したものが「リモート CA 証明書」として表示されます。

名前	サブジェクト	コメント	発行者	有効期限	ステータス	送信元	参照
リモート CA 証明書 (1/5)							
CA_Cert_1	CN = EVALUATION CA, DC = com, DC = jcc...		JCCH Security Solution Systems ...	2021/03/31 15:23:37	有効	ユーザ	0

2.4. SSL-VPN 設定

管理画面のメニューから[VPN] > [SSL-VPN]設定 を選択し、[サーバ証明書]を 2.2 項でインポートした証明書に変更します。

また、その下の[クライアント証明書を要求]をオンにします。



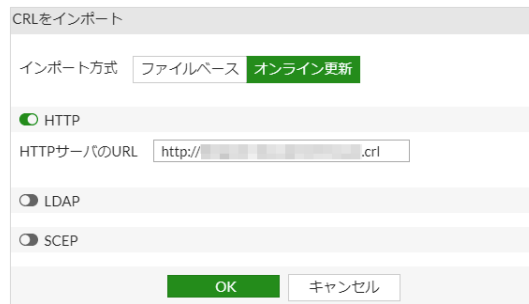
2.5. 失効リスト (CRL) の設定

管理画面のメニューから[システム] > [証明書]をクリックし、上部メニューから[インポート] > [CRL]をクリックします。インポート画面で以下の設定をおこないます。

- インポート方式：オンライン更新を選択
- HTTP：オン
- HTTP サーバの URL：Gléas の CRL 配布ポイント (URL) を指定
※ Gléas のデフォルト CA の CRL 配布ポイントは以下になります

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

http://gleas.example.com/crl/ia1.crl



登録したものが「CRL」として表示されます。



名前	サブジェクト	コメント	発行者	有効期限	ステータス	送信元	参照
CRL_1			JCCH Security Solution Systems Co., Ltd.		有効	ユーザ	0

オンライン更新では、CRL の有効期限を過ぎると再度 CRL 配布ポイントにアクセスして CRL を更新します。定期的に CRL をチェックしたい場合は、コマンドラインから設定可能です。以下は CRL の更新チェックの間隔を 1 時間(3600 秒)にする場合の例です。

```
FortiGate-60E # config vpn certificate crl
FortiGate-60E (crl) # edit CRL_1
FortiGate-60E (CRL_1) # set update-interval 3600
FortiGate-60E (CRL_1) # end
```

シナリオ 1 における FortiGate の設定は以上です。

3. Gléas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

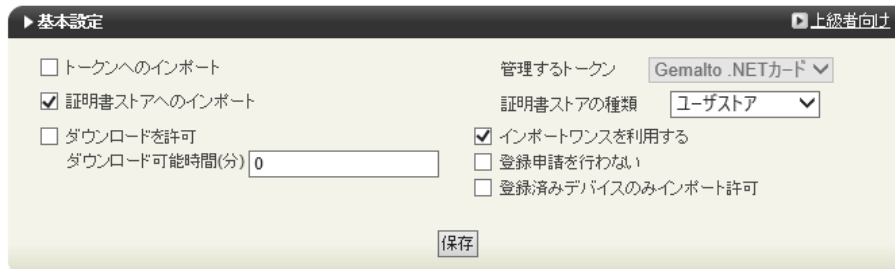
GléasのRA (登録局) にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA (申込局) をクリックします。

※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]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



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]

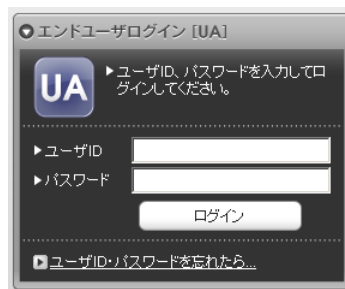
4. クライアントからのアクセス (Windows)

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。

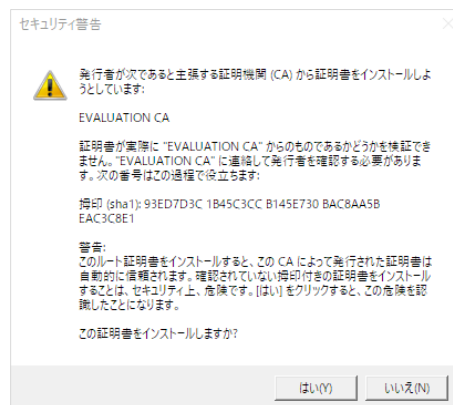
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。

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

- ※ 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

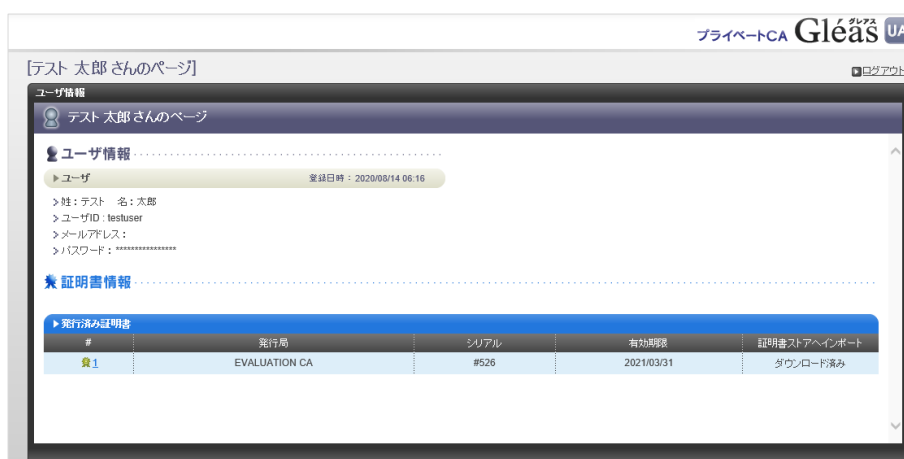


- ※ 証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を確認するなど正当性を確認してから[はい]をクリックします



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。

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



4.2. FortiClient からのアクセス (Windows)

FortiClientを起動し、新規VPN接続の設定をおこないます。

[クライアント証明書]のドロップダウンには4.1項でインポートした証明書が選択可能になっているので、それを選択します。



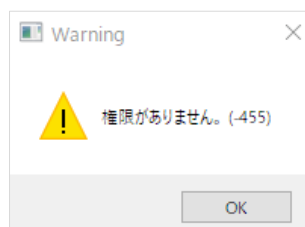
保存後、パスワードを入力し[接続]をクリックします。

クライアント証明書とパスワードによる認証が成功すると、VPN接続が完了します。

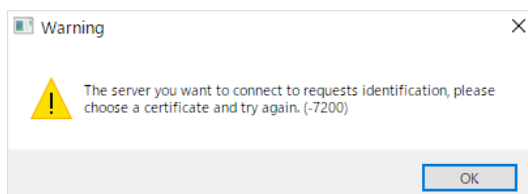
プライベート認証局 Gléas ホワイトペーパー
FortiGate SSL-VPN でのクライアント証明書認証



なお失効済みの証明書でアクセスをすると、以下のエラーで接続に失敗します。



またクライアント証明書がない場合は、以下のエラーで接続に失敗します。



5. Gléasの管理者設定 (iPhone / Android)

GléasのUA (申込局) より発行済み証明書をiPhoneやAndroid端末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行っている場合があります

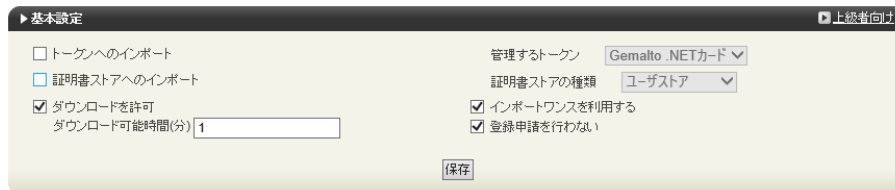
※iPhoneに関しては、GléasにiOS版FortiClient向けのカスタマイズがされている必要があります

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。

[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
- (任意項目) インポートロック

[インポートワンスを利用する]にチェックを入れ、かつ [ダウンロード可能時間(分)]の設定を行うと、証明書のダウンロードから指定分数を経過後は再度のダウンロードができなくなります。

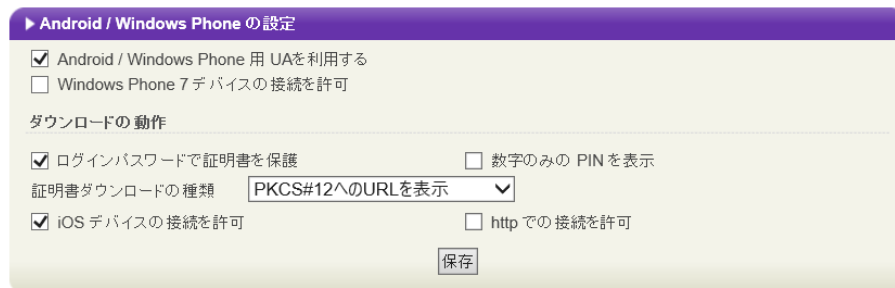


設定終了後、[保存]をクリックし設定を保存します。

[認証デバイス情報]の[Androidの設定]までスクロールし、[Android / Windows Phone用UAを利用する]をチェックし、以下の設定を行います。

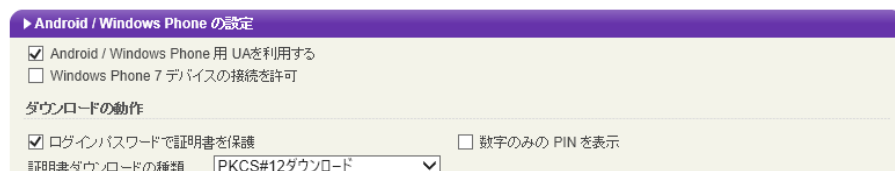
※iPhoneに関しても、GléasのAndroid向け機能を利用するためこのようにします

- iPhone用の設定：



証明書ダウンロードの種類を [PKCS#12へのURLを表示]にして、[iOSデバイスの接続を許可]をチェック。その状態でいったん保存し、証明書ダウンロードの種類を [PKCS#12ダウンロード]に変更します。

- Android用の設定：



証明書ダウンロードの種類を、[PKCS#12ダウンロード]にします。

- 証明書ダウンロード時の保護パスワードの設定

[ログインパスワードで証明書を保護]にチェックすると、UAログイン時のパスワードを証明書保護パスワードとして利用します。

設定終了後、下部の[保存]をクリックし設定を保存します。

6. クライアントからのアクセス (iPhone)

6.1. ルート証明書のインポート

Gléasが発行したサーバ証明書を信頼するため、そのルート証明書をインポート(信頼)します。

Safariブラウザで、GléasのUAに対しhttp接続すると[ルート証明書のダウンロード]ボタンが表示されます。

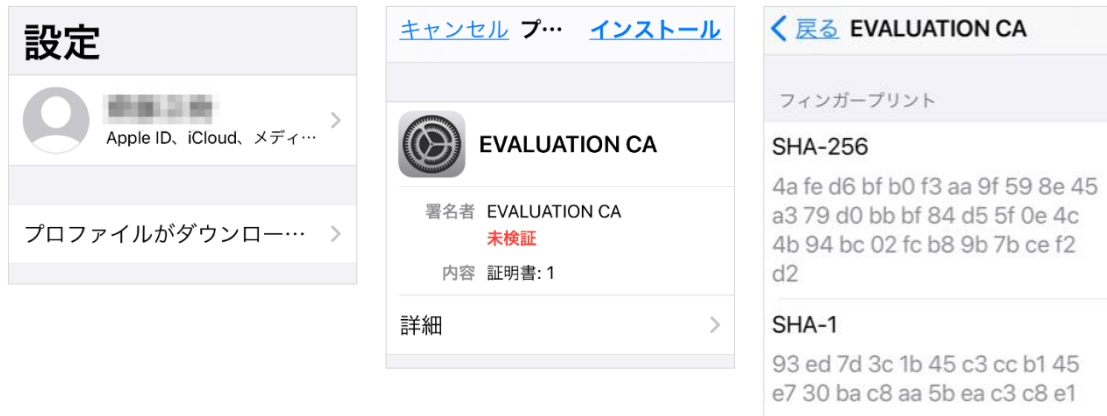


そのボタンをクリックすると認証局証明書のダウンロードページに遷移し、ローカルにダウンロードすると設定アプリを開くよう促されます。



設定アプリからインストールを進めます。[詳細]からルート証明書の拇印を確認することが可能です。

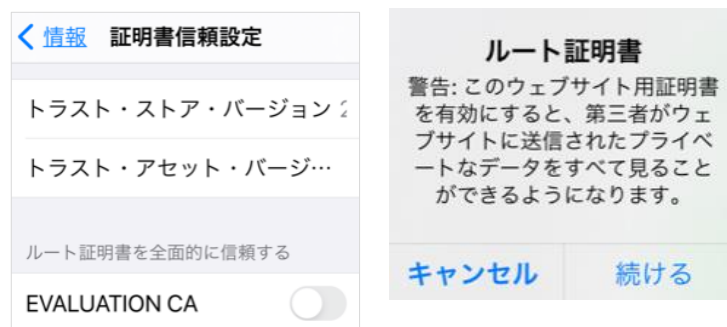
プライベート認証局 Gléas ホワイトペーパー
FortiGate SSL-VPN でのクライアント証明書認証



インストールを完了させます。



その後、[設定] > [一般] > [情報] > [証明書信頼設定]と進み、インポートした証明書をオンにします。



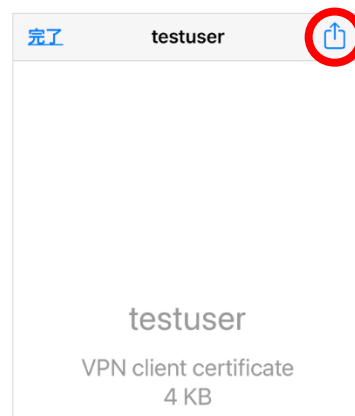
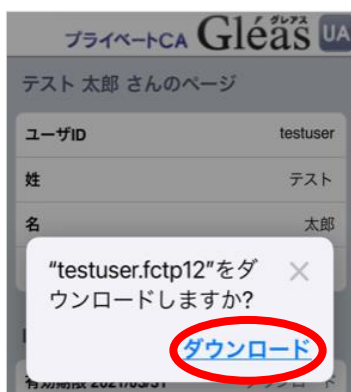
6.2. クライアント証明書のインポート

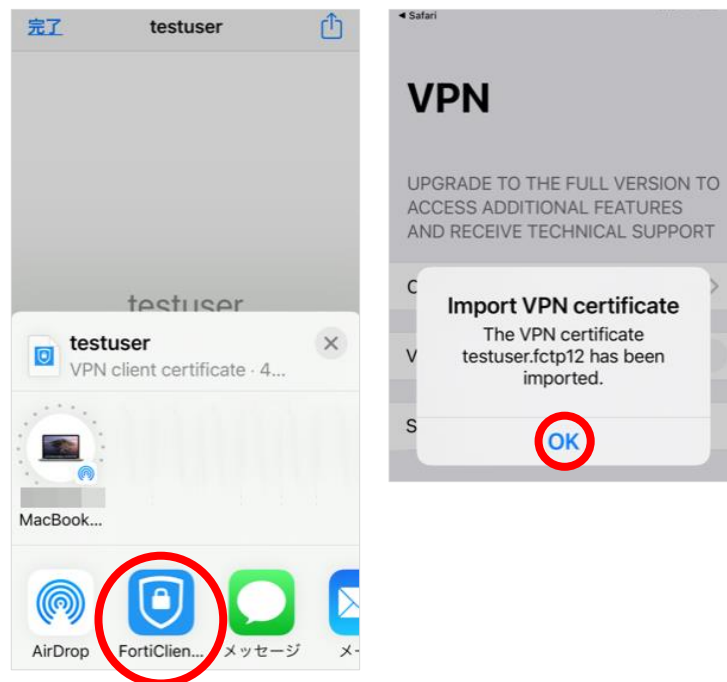
Safariブラウザで、iOS用に設定されたUAのURLにアクセスします。ユーザIDとパスワードを入力しログインすると、ユーザ専用ページが表示されます。

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



[ダウンロード]リンクをタップすると、クライアント証明書ファイル（拡張子が".fctp12"のファイル）がローカルにダウンロードされるので、FortiClientに証明書を送ってインポートします。

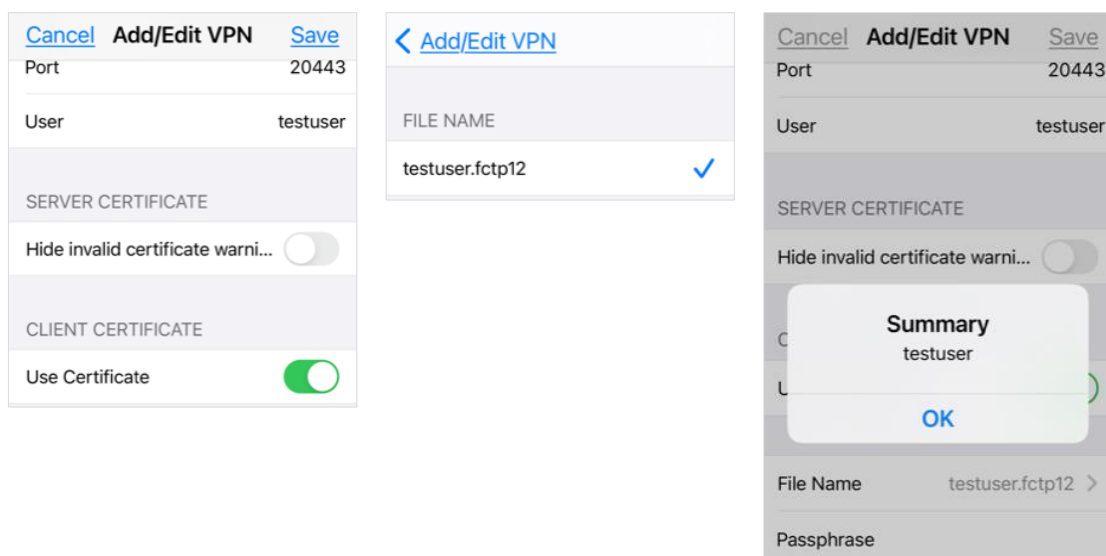




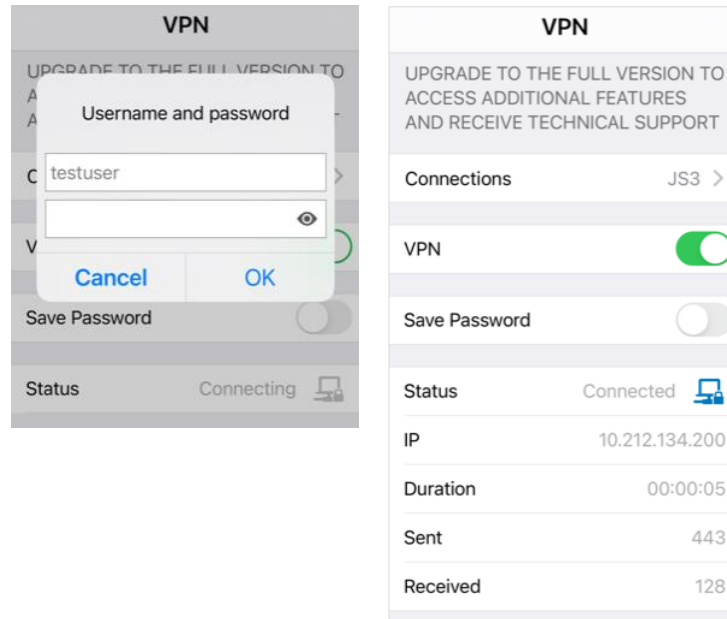
6.3. FortiClient での証明書のインポートと接続

FortiClientアプリで、SSL-VPN接続設定をおこないます。

接続設定画面のCLIENT CERTIFICATEで[Use Certificate]をオンにして、[File Name]に6.2項でインポートした証明書を選択し、[Passphrase]にはUAログインパスワードを入力します。インポートに成功すると[Summary]にクライアント証明書情報が表示されます。



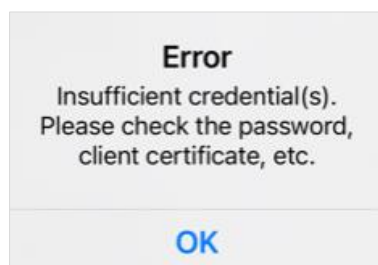
その後、SSL-VPN接続が可能となります。



失効済みの証明書でアクセスすると以下のエラーとなります。



クライアント証明書を設定せずにアクセスした場合は以下のエラーになります。



7. クライアントからのアクセス (Android)

7.1. ルート証明書のインポート

Gléasが発行したサーバ証明書を信頼するため、そのルート証明書をインポート(信頼)しま

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

す。

Chromeブラウザで、GléasのUAに対しhttp接続するとルート証明書のダウンロードボタンが表示されます。



ボタンをクリックすると認証局証明書のダウンロードページに遷移するので、ローカルにファイルダウンロードします。

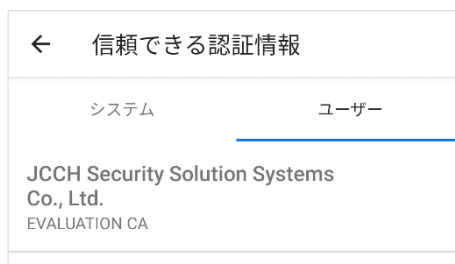


設定アプリから、[セキュリティ] > [暗号化と認証情報] > [証明書のインストール] > [CA 証明書]と進み、ダウンロードしたルート証明書をインポートします。



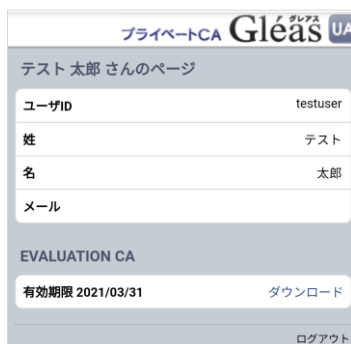
[セキュリティ] > [暗号化と認証情報] > [信頼できる認証情報] > [ユーザー]と進むことでイ

ンポートしたルート証明書情報を見ることが可能です。必要に応じ、拇印などを確認します。



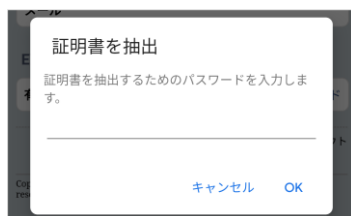
7.2. クライアント証明書のインポート

Chromeブラウザで、Android用に設定されたUAのURLにChromeでアクセスします。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すると、ユーザ専用ページが表示されます。



[ダウンロード]リンクをタップすると、クライアント証明書がローカルにダウンロードされます。

以下の画面が表示される場合は[キャンセル]をクリックします（OSのストア領域にインポートするための表示ですが、今回はFortiClientアプリにインポートするため）。



7.3. FortiClient での証明書のインポートと接続

FortiClientアプリを起動して、SSL-VPN接続設定をおこないます。

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



接続設定画面で[証明書]をタップし、ダウンロードした証明書をインポートします。
パスワードを求められるので、UAのログインパスワードを入力します。



インポートが完了すると、クライアント証明書のサブジェクトが表示されます。



SSL-VPN接続が可能となります。

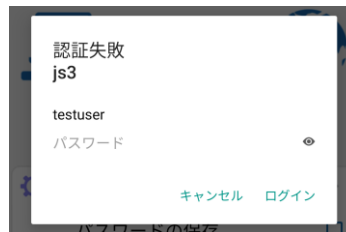
プライベート認証局 Gléas ホワイトペーパー
FortiGate SSL-VPN でのクライアント証明書認証



失効済みの証明書でアクセスすると以下のエラーとなります。



クライアント証明書を設定せずにアクセスした場合は以下のエラーになります。



8. シナリオ2：LDAP-integrated certificate authentication

FortiGateの”LDAP-integrated certificate authentication”を使うことにより、クライアント証明書とユーザIDを紐づけることが可能となります。

8.1. FortiGate の設定

あらかじめLDAPサーバ（Active Directory）へのアクセス設定をしておきます。
本書では詳細な説明は割愛します。

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

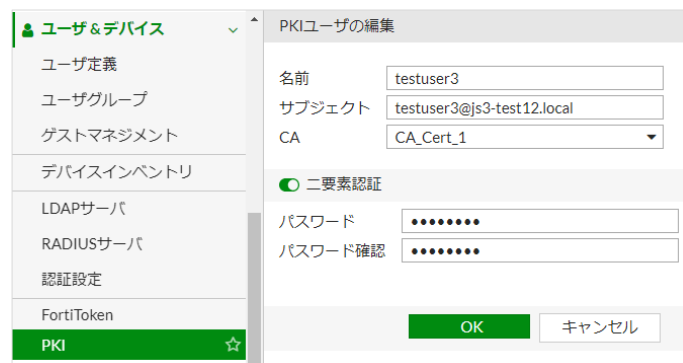


その後、CLI にログインし PKI ユーザを作成します。

```
FortiGate-60E # config user peer
FortiGate-60E (peer) # edit testuser3
new entry 'testuser3' added
FortiGate-60E (testuser3) # set ca CA_Cert_1
FortiGate-60E (testuser3) # set ldap-server "js3-test12"
FortiGate-60E (testuser3) # set ldap-mode principal-name
FortiGate-60E (testuser3) # end
```

管理者画面のメニューのユーザ&デバイスの下に PKI が追加され、CLI で追加したユーザが見えるようになっています。そのユーザを編集します。

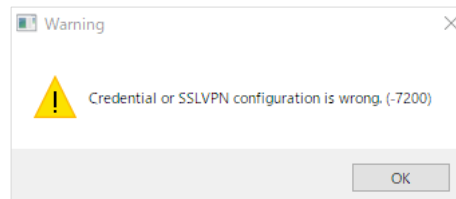
- [サブジェクト]に、証明書に記載されるユーザプリンシパル名を入力
- パスワード認証を併用する場合は、[二要素認証]をオンにして、[パスワード]を入力
- 設定後、SSL-VPN 利用可能なユーザグループに PKI ユーザを参加させる



8.2. FortiClient からの接続

クライアント証明書のサブジェクト代替名に、PKI ユーザの ID に対応するユーザプリンシパル名がある場合は VPN 接続に成功します。

一致しない場合は以下のエラーを表示し（Windows の場合）、VPN 接続に失敗します。



9. 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