

# 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

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。

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.	Gléas における留意事項	5
2. Fort	iGate 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. Gléa	as の管理者設定(Windows 用)	9
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	
4.2.	FortiClient からのアクセス(Windows)	
5. Gléa	as の管理者設定(iPhone / Android)	
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	
6.2.	クライアント証明書のインポート	
6.3.	FortiClient での証明書のインポートと接続	
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	
7.2.	クライアント証明書のインポート	
7.3.	FortiClient での証明書のインポートと接続	
8. シナ	リオ 2:LDAP-integrated certificate authentication	23
8.1.	FortiGate の設定	
8.2.	FortiClient からの接続	
9. 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。

- > 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 ( $\mathcal{N} - \mathcal{V} \equiv \mathcal{V}$  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 ( $\neg - \neg = 2$  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ので、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。

🚯 ダッシュボード	> ^	表示機能設定
セキュリティファブリ ※ ック	>	◯ マルチキャストポリシー
🛋 FortiView	>	ג<קזוא-ם
♣ ネットワーク	>	
☆ システム	~	1
管理者	- 1	● 脅威ウェイトトラッキング
管理者プロファイル	- 1	
ファームウェア	- 1	○ 差し替えメッセージグループ
設定	. 1	● 証明書 ■
HA		SSLインスペクション、SSLロードパラン
SNMP	- 1	シング、SSL-VPN、IPsec VPNと認証に使 Photo z Fugata たの声 (ます、方の)(す)
差し替えメッセージ	- 1	「おされてお皿が音を支更します。"有効になっている場合は、システム > 証明書 から
FortiGuard	- 1	証明書の管理を行います。有効になって
表示機能設定	☆	いない場合、デフォルトのFortiGate証明 書がこれらの機能のために使用されま
ポリシー&オブジェク		■パーロンジの機能が20012.8013とうであ 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)

●作業名: <u>タスク2944</u>	証明書を保護するための	D/(スワードを入力してください。	プライベートCA	Gléäs	RA
O E HE : HEYATA E HE	バスワードの入力		551 + TCA +	Gieus	
[証明書]>詳細	1/20. F		■グ ■管理者 ■ヘルブ ■ログアウト		
Pカウント Account	////	ダウンロード キャンセル	D <u>一覧に戻る</u>	▶クイックナビ	
	9		■E±2		
Group 兼証明書情報······			<u> </u>	サーバ証明書	
★ 証明書 Certificate ► fortigate-60e.icch-sss.local					
● 認証デバイス Device トリブジェクト					
>一般名: fortigate-60e.jcch-sss.					
→ remplate >ドメインコンボーネント: com >ドメインコンボーネント: jcch-sss					
〇証明書操作		> 失効理由:			
		> 期限終了日:			
▶ 停止势理 ▲		> 47.88: 有効な証明書 > 処理の状態: 有効な証明書			
▶ 秘密鍵の削除		>トーケン必要:			
トドックに入れる					
▶記明書情報					
> 認証局: EVALUATION CA					

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

証明書をインポート				×
タイプ	ローカル証明書	PKCS12 証明書	証明書	
キーファイルのある証明書	fortigate-60	e.jcch-sss.local.p12		
パスワード	••••		۲	
証明書名	fortigate-60e.jcc	h-sss.local		
	ОК	キャンセル		

登録したものが「ローカル証明書」として表示されます。

+ 生成     ● 網除     ヨインポート・     ● 詳細の表示     ▲ ダウンロード     検索     Q				2			
名前 🕈 🛛 🔻 🕇	サブジェクト≑	コメントキ	発行者 🗢	有効期限 🗘	ステータス 🗢	送信元 🗢	参照 🗢
目 ローカル証明書 1							
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

● 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

CA証明書をイン	ポート
タイプ	オンラインSCEP ファイル
アップロード	• ia1.der
	OK キャンセル

登録したものが「リモート CA 証明書」として表示されます。

+ 生成 🥒 編	集 前 削除 3 インポート ● 詳細の	の表示 🕹 ダウ	ンロード 検索		Q		
名前 ≑ 🛛 🔻	サブジェクト≑	コメントキ	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)						
R 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。

SSL-VPN設定		
接続設定 🜖		
リッスンするインターフェース	🖮 wan1 +	×
リッスンするポート	20443	
	₩ebモードアクセスをリッン https://192.168.20.233:204	スンするポート: <u>43</u>
HTTPをSSL-VPNにリダイレクトする 🔾	)	
アクセスを制限	任意のホストからアクセス許可	特定ホストヘアクセス制限
アイドルログアウト	)	
非アクティブ	300	秒
サーバ証明書	📭 fortigate-60e.jcch-sss.local	•
クライアント証明書を要求	)	

# 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

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

CRLをインボート
インポート方式 ファイルベース オンライン更新
C HTTP
HTTPサーパのURL http:// .crl
❑ LDAP
SCEP
OK キャンセル

#### 登録したものが「CRL」として表示されます。

+ 生成 🥒 編集 🛛	俞 削除	ヨ インポート・ 💿 詩	細の表示 🛃 ダ	ウンロード 検索		Q		
名前 🗣	•	サブジェクト≑	コメントキ	発行者 ♥	有効期限 🗘	ステータス 🕏	送信元 🗢	参照 🗘
CRL 1								۲
S 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

▶基本設定	
<ul> <li>トーケンへのインボート</li> <li>✓ 証明書ストアへのインボート</li> <li>ダウンロードを許可 ダウンロード可能時間(分)</li> </ul>	<ul> <li>管理するトークン Gemalto.NETカード ∨</li> <li>証明書ストアの種類 ユーザストア ∨</li> <li>インボートワンスを利用する</li> <li>登録申請を行わない</li> <li>登録済みデバイスのみインポート許可</li> </ul>
	保存

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

●エンドユーザログイン [UA]
●ユーザル、パスワード巻入力してロ ダインしてください。
▶ユーザID
▶パスワード
ログイン
□ <u>ユーザID・パスワードを忘れたら</u>

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CA Gléäs
テスト 太郎 さんの/	ページ]			
ユーザ情報				
🖉 テスト 太郎 さん	のページ			
▶ユーザ情報				
▶ ユーザ	登録日時: 2020/08/14	06:16		
<ul> <li>&gt; ユーザル: testuser</li> <li>&gt; メールアドレス:</li> <li>&gt; パスワード:</li> </ul>				
#	発行局	シリアル	有効期限	証明書ストアヘインボート
<b>\$1</b>	EVALUATION CA	#526	2021/03/31	証明書のインボート

※ 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

セキュリティ	管告	
<u> </u>	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:	
	EVALUATION CA	
	証明書が実際に"EVALUATION CA"からのものであるかどうかを検証でき ません。"EVALUATION 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Zの過程で役立ちます:	
	拇印 (sha1): 93ED7D3C 1B45C3CC B145E730 BAC8AA5B EAC3C8E1	
	警告: このルト証明書をインストールすると、この CA によって発行された証明書は 自動的に信頼されます。確認されていない時印付きの証明書をインストール 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 職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	м-ьса Gléäs
テスト 太郎 さんのぺ	-ジ]			1 <u>115</u>
2ーザ情報				
🙎 テスト 太郎 さんぬ	ウベージ			
▶ ユーザ情報 ·····				
▶ユーザ	登録日時: 2020/08/1	4 06:16		
> gt: アスパ 名: 太郎 > ユーザID: testuser > メールアドレス: > パスワード: ************************************				
▶ 発行済み証明書				
# <u>\$1</u>	第行局 EVALUATION CA	シリアル #526	有効期限 2021/03/31	証明書ストアヘインボート ダウンロード済み

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。

	新規VPN接続		
K	VPN	SSL-VPN IPsec VPN	XML
	接続名	JS3	
	説明		
X ZERO TRUST TELEMETRY	リモートGW	fortigate-60e.jcch-sss.local	×
品 リモートアクセス		<ul> <li>◆リモートケートワェイを追加</li> <li>✓ ポートの編集 20443</li> </ul>	
		Enable Single Sign On (SSO) for VPN Tu	innel
	クライアント証明書	testuser/EVALUATION CA	•
<b>Q</b> 設定	168		○ 無効
🗊 情報		一 無効なリーへ証明者の言古を非衣示	
		キャンセル 保存	

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。

8	VPN接続済み	UNLICENSED
🔆 ZERO TRUST TELEMETRY		
<u> リ</u> モートアクセス		
! お知らせ		VPN名称 JS3
➡ 設定	IP	アドレス 10.212.134.200
T		ユーザ名 testuser
🗊 情報		期間 00:00:12
	· · · · · · · · · · · · · · · · · · ·	信バイト 4.75 KB
	送	信パイト 37.27 KB
		切断

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 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。

▶基本設定	
□ トーケンへのインボート	管理するトークン Gemalto .NETカード V
□ 証明書ストアへのインボート	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	<ul> <li>✓ インボートワンスを利用する</li> <li>✓ 登録申請を行わない</li> </ul>
	[条存]

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:

▶ Android / Windows Phone の設定	
✓ Android / Windows Phone 用 UAを利用する ○ Windows Phone 7 デバイスの 接続を許可	
ダウンロードの 動作	
✔ ログインバスワードで証明書を保護	<ul> <li>数字のみの PIN を表示</li> </ul>
証明書ダウンロードの種類 PKCS#12へのU	JRLを表示 V
☑ iOS デバイスの接続を許可	□ http での接続を許可
	保存

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:

▶ Android / Windows Phone の設定	
✓ Android / Windows Phone 用 UAを利用する ○ Windows Phone 7 デバイスの接続を許可	
ダウンロードの動作	
✓ ログインバスワードで証明書を保護 証明書ダウンロードの種類	<ul> <li>□ 数字のみの PIN を表示</li> </ul>

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。

設定	<u>キャンセル</u> プ… インストール	く 戻る EVALUATION CA
		フィンガープリント
Apple ID、iCloud、メディ…	EVALUATION CA	SHA-256
プロファイルがダウンロー… >	署名者 EVALUATION CA <mark>未検証</mark> 內容 証明書: 1	4a fe d6 bf b0 f3 aa 9f 59 8e 45 a3 79 d0 bb bf 84 d5 5f 0e 4c 4b 94 bc 02 fc b8 9b 7b ce f2 d2
	詳細 >	SHA-1 93 ed 7d 3c 1b 45 c3 cc b1 45
		e7 30 ba c8 aa 5b ea c3 c8 e1

インストールを完了させます。

	イノストール元」 元」
管理対象外ルート証明書	EVALUATION CA
証明書"EVALUATION CA"をイン ストールすると、iPhoneにある信 頼できる証明書のリストに追加さ	署名者 EVALUATION CA
れます。"証明書信頼設定"で有効 にするまで、この証明書はWebサ イト用には信頼されません。	検証済み ✓ 内容 証明書:1

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。

く <u>情報</u> 証明書信頼設定	ルート証明書	
トラスト・ストア・バージョン	警告: このウェブサイト用証明書 を有効にすると、第三者がウェ ブサイトに送信されたプライベ ートなデータをすべて見ること ができるようになります。	
トラスト・アセット・バージ…		
ルート証明書を全面的に信頼する		
EVALUATION CA	キャンセル 続ける	

# 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CA	Gléå 🖾
テスト 太郎 さんのペー	ージ
ユーザロ	testuser
姓	テスト
名	太郎
メール	
EVALUATION CA	
有効期限 2021/03/31	ダウンロード
	ログアウト

[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。

JETA-FCA Glé	as UA 35	•	0 0	<u>完了</u>	testuser	
テスト 太郎 さんのページ		ダウンロード	消去 🗛			
ユーザロ	testuser	-				
姓	<del>7</del> 21	4 KB	Q			
名	太郎姓		テスト			
"testuser.fctp12"をダ	×					
ワンロートしますか?					testuser	
אוואנאנג בטבווטאטן				VPN	client certificate 4 KB	)



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。

Cancel Add/Edit VPN Port	<u>Save</u> 20443	< Add/Edit VPN		Cancel Add/Edit	VPN <u>Save</u> 2044
User	testuser	FILE NAME		User	testuse
SERVER CERTIFICATE		testuser.fctp12	~	SERVER CERTIFICATI	E
Hide invalid certificate warni				Hide invalid certificat	e warni
CLIENT CERTIFICATE				C Summ	ary er
Use Certificate				ι ΟΚ	)
				File Name t	estuser.fctp12 >
				Passphrase	

その後、SSL-VPN接続が可能となります。

VPN	VPN
A A Username and password	UPGRADE TO THE FULL VERSION TO ACCESS ADDITIONAL FEATURES AND RECEIVE TECHNICAL SUPPORT
C testuser >	Connections JS3 >
V Cancel OK	VPN
Save Password	Save Password
Status Connecting	Status Connected
	IP 10.212.134.200
	<b>Duration</b> 00:00:05
	<b>Sent</b> 443
	Received 128

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。

	Error
In: Plea	sufficient credential(s).
1	client certificate, etc.
	OK

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

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。

CA Certificates]
◇◇ 認証局証明書のダウンロード
認証局証明書のダウンロード
► EVALUATION CA
> <u>認証局証明書</u> > <u>完全CRL</u>

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。

÷	信頼できる	認証情報
	システム	ユーザー
JCC Co., EVAL	H Security Solu Ltd. UATION CA	tion Systems

# 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。

プライベートC	A Gléås 🛛
テスト 太郎 さんのページ	
ユーザID	testuser
姓	テスト
名	太郎
メール	
EVALUATION CA	
有効期限 2021/03/31	ダウンロード
	ログアウト

[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)。

証明書を抽出		
証明書を抽出するため す。	のパスワードを入	力しま
	キャンセル	ОК

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。

FortiClient VPN	≡
VPN追加	
js3	
VPNタイプ ● SSL VPN ● IPsec VPN	
作成	

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。

FortiClient VPN	≡	≡ ダウンロード	Q :		_
SSL VPN設定		ダウンロード		パスワード	
トンネル名 <sup>js3</sup>		□ 画像	נ×ב≠א 🚺		
サーバ	>	[ダウンロード] 内のファイル	E		キャンセル OK
ポート <sup>20443</sup>	>	•		tootucor	
ユーザ名 testuser	>	Ĩ.			
<b>証明書</b> PKCS12フォーマットのX.509証明書	>	👼 testuser.p12			
Prompt User Credentials <sup>有効</sup>	>	3.97 KB 11:14			
サーバ証明書をチェック <sup>有効</sup>	>				
VPN削除					
VPNトンネルプロファイル削 このVPN設定を削除し、VPNトンネルリストが 去します。	<b>余</b> いら消				

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。

FortiClient VPN	≡
SSL VPN設定	
トンネル名 js3	
サーバ	>
ポート 20443	>
ユーザ名 testuser	>
証明書 DC=jcch-sss,DC=com,CN=testuser	>

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。

3	<mark>接続失敗</mark> 接続できませんでした。 "Js3". エラー: Daemon failure: SSLCONNFAILED	)
	キャンセル リトライ	

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。

ľ	認証失敗 js3			
L	testuser			
L	パスワード		۲	
2				
3		キャンセル	ログイン	
	バスワード	の保存		11

# 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。

Ø ダッシュボード	> ^	LDAPサーバの編集		
セキュリティファブリ ※ ック	>	名前	js3-test12	
FortiView	>	サーバIP/名前	192.168.20.235	
♣ ネットワーク	· · ·	サーバポート	636	
	Ń	コモンネーム識別子	sAMAccountName	
✿ システム	745	識別名	DC=js3-test12,DC=local	ブラウズ
▶ ポリシー&オブジェク	>	バインドタイプ	シンプル 匿名 レギュラー	
		ユーザ名	CN=Administrator,CN=Users,DC	⊆js3-t
▲ セキュリティプロファ	>	パスワード	変	更する
- <i>ส</i> ม		セキュアな接続		
L VPN	>	プロトコル	STARTTLS LDAPS	
🛓 ユーザ&デバイス	~	証明書		•
ユーザ定義		接続ステータス	⊘ 成功	
ユーザグループ		接続をテスト		
ゲストマネジメント		ユーザクレデンシャルをテスト		
デバイスインベントリ				
LDAPサーバ	☆			

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

🛔 ユーザ&デバイス 💦 🗸 📩	PKIユーザの編集		
ユーザ定義 ユーザグループ ゲストマネジメント	名前 testuser3 サブジェクト testuser3@js3-test12.local CA CA_Cert_1 ・		
デバイスインベントリ	● 二要素認証		
LDAPサーバ RADIUSサーバ 認証設定	- パスワード ••••••• パスワード確認 •••••••		
FortiToken	OK キャンセル		
РКІ 🏠			

### 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