

# 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

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. はじる	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. PA-F	īrewall 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	
2.3.	VPN クライアント証明書認証の設定	
3. Gléa	s 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	
4.2.	GlobalProtect から PA-Firewall への VPN アクセス	
5. Gléa	s 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)	
6.1.	クライアント証明書のインポート	
6.2.	PA-Firewall へのアクセス	20
7. 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、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 ( $\neg - \neg = 2$  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 ( $\neg - \neg = 2$  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。

4 / 21

#### 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。

証明書の生成  ⑦
証明書タイプ 🧿 ローカル 🔷 SCEP
証明書名 external-gateway
共通名 palo.
証明書に表記される IP または FQDN
老石者 External Authority (CSR) V
№3Ш/月 ✓ 秘密鍵のエクスポートをブロック
ー の証明書の秘密鍵のエクスポートを永続的にブロッ クするオプションです
OCSP レスポンダ
- ^ 暗号設定
アルゴリズム RSA V
ビット数 2048 🗸
ダイジェスト sha256 🗸
有効期限(日) 365
証明書の屋性
□ タイプ 値
(●追加) ○削除
生成キャンセル

※ 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している必要があります。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。

デバイス証明書 デフォルトの信頼された証明機関								
QC								
2 名	前		サブジェクト		発行者			
	external-gatewa	y	palo					
				1				
	<b>余</b> 無効化 更	新 売 インホー	- ト , 短成	占 証明	書のエクスボート			

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 その後、[発行]ボタンをクリックします。

<ul> <li>0作葉名: <u>タスク3826</u></li> <li>0管理者: システム管理</li> </ul>	2#3	プライベートCA	Gléå's 🖪
[アカウント]>証明	<b>非</b> 発行	記述局 0.05 0.管理者 0.ヘルブ 0.05アウト	O #⊀FM- □
アカウント	アカウント	D <u>一覧に戻る</u>	▶ クイックナビ
Account	🗐 palo.	▶ 詳細に戻る.	<u> 2 - ザ証明書</u>
ショ グループ			二マシン証明書
Group	★ 証明書発行	~	🗏 サーバ証明書
★ 証明書 Certificate	この画面では証明書要求の作成を行います。		☆ 認証局証明書
SEEデバイス Device	左側の「サブジェクト」と「屬性」の内容で証明書要求を作成します。 右側のテンプレートの中から必要なものを選択して「発行」を押してください。		
テンプレート	▶証明書発行	■上級者向け設定	
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		
アカウント一覧	> 証明書要求(CSR)ファイルをアップロードする: C:\temp\cert external-gal 参照	8	▶ ドック
●终由转来一覧	➤ CSRファイルの内容を確認する		■ <u>アカウント (0)</u>
東京ないの日本			★ ITel S (0)
	発行		
▶ 紅明眉死行			
	▶サラジェクト	Cいるテンプレート ■全て解除	
	> CN=palo > 必須デフ:		
	> 必須 サー	パ証明書	

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。



PDDD/L-Ser       DEGR D-21 EBBE 0	<ul> <li>の作業名: <u>タスク3826</u></li> <li>の管理者: <u>システム管理者</u></li> </ul>	3	プライベートCA	Gléå 🖁 🖪
● Charlet       ● Charlet <th>[アカウント]&gt;発行</th> <th></th> <th>局 🛛 ログ 🗆 管理者 🗈 ヘルブ 🗈 ログアウト</th> <th><b>O</b>#4FM-</th>	[アカウント]>発行		局 🛛 ログ 🗆 管理者 🗈 ヘルブ 🗈 ログアウト	<b>O</b> #4FM-
A control         Image: Contro         Image: Contr	アカウント		□ <u>一覧に戻る</u>	▶クイックナビ
Participane                  Participane	Account	「「和中西太(CSP)の破到	■ キャンセット ■ 二の内容で発行する	♀ ユーザ証明書
Cartificate Report:         Wersion:	№ グループ			ロマン開発
↓ Cassimiliant         ↓ Cass	Group	Certificate Request:		
Wersion:         0 (90)           Wersion:	- EX BB SR	Data:	~	0
Subject:         Chepaio	Certificate	Version: 0 (0x0)		会 認証局証明書
Budgett Public My Info:           Device           Device <t< td=""><td></td><td>Subject: CN=palo</td><td></td><td></td></t<>		Subject: CN=palo		
Public Rey Algorithm: reakingption           Public Rey Algorithm: reakingptind<	🔬 認証デバイス	Subject Public Key Info:		
Pholic-Mey: (248 bit)           Modiania:           Properties           Pholic-Mey: (248 bit)           Modiania:           Pholic-Mey: (248 bit)           Modiania:           Pholic-Mey: (248 bit)	Device	Public Key Algorithm: rsaEncryption		
Boddular:         Boddular:         0:00:00:00:00:00:00:00:00:00:00:00:00:0		Public-Key: (2048 bit)		
Lampute         000000000000000000000000000000000000	- テンプレート	Modulus:		
C 2h2/17/06/01/40/06/21/76/01/40/17/26/01/40/10/20/10/20/10/20/00/10/20/00/10/20/00/10/20/00/10/20/00/2	Template	00:c5:08:69:ab:92:91:d6:d1:c0:24:3b:65:44:3a:		19.72
0 7 /h 20 /h Heft         0 7 /h 20 /h Heft         1 / 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1 /		62:D4:/C:e8:U4:U3:e2:5/:e8:I6:/C:U4:/9:C8:4I:		14:15
2/2022/E-E         12.42478424         12.4247842         12.4247842           2013/01.001         12.4247842         12.4247842         12.4247842           2013/01.001         12.4247842         12.4247842         12.4247842           2013/01.001         12.4247842         12.4247842         12.4247842           2013/01.001         12.124842         12.4247842         12.4247842         12.4247842           2013/01.001         12.124842         12.4247842         12.4247842         12.4247842         12.4247842           2013/01.001         12.124842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4247842         12.4447842         12.4447842         12.4447842         12.4447842         12.4447842         12.4447842         12.4447842         12.4447842         12.4447842         12.4447842         12.4447842         12.44478444444444444444444444444444444444	●アカウント操作	CB:a1:54:C5:51:da:36:CC:84:51:U6:9U:78:Te:Cd:		
プリントを当         このときょうのきもおねがらではおとかとうないがあくます。         まプリンントの           原田東面一         マリンともの         まプリンントの           アウントを当         マリントの         まプリンントの           アウントを当         マリントの         まプリンントの           アウントを当         マリントの         まプリンントの           アウントを取用の         ロシークショントの         まプリンントの           アウントを取用の         ロシークショントの         まプリントの           アウントの         まプリントの         まプリントの           アウントの         まプリントの         まプリントの           アウントの         まプリントの         まプリントの           アウントの         まプリントの         まプリントの           ロシントの         ロシントの         まプリントの           アウントの         ロシントの         まプリントの           ロシントの         ロシントの         ロシントの           ロシントの         <	(manahara) (m	AC:58:81:30:D/:0/:00:9D:D0:08:80:91:01:02:00:		▶ ドック
	アカウンドー覧			■ アカウント (0)
Chille and brid and Statistic 2011 of 501 - 601 - 441         A 2000-2010           77722 / ERRINE         05 - 641 - 641 - 551 - 621 - 641 - 551 - 661 - 441         A 2000-2010 - 551 - 64	帝终由结老——祭	27:12:54:b0:01:56:84:04:00:54:D0:10:20:12:04:D4:		- 1700 +
	ALL DO TO ANY DEL DO	c3+13+ea+bf+e3+e5+b2+53+4c+4c+71+9f+91+6b+44+		<u> ● 記記書(0)</u>
Tert2 add 45 500 400 e01 la 7% act red 7 db 3d 32 12 1           a 73 51 75 31 72 45 e04 500 exet b61 df 77 45 44 44 e2           6 e10 b7 55 44 44 75 96 al terte f16 70 52 0 af f1           o bbb ars 2f 42 39 b1 11 e11 e16 b2 a2 do cor 54 60 b           b3 39 50 96 49 af ar e8 32 c4 437 13 b0 36 2 e db b           d db 37 55 0 56 49 af ar e8 32 c4 437 13 b0 36 2 e db b           d db 37 55 0 56 49 af ar e8 32 c4 437 13 b0 36 2 e db b           d db 37 55 0 56 49 af ar e8 32 c4 437 13 b0 36 2 e db b           d db 37 55 0 56 49 af ar e8 32 c4 437 13 b0 36 2 e db b           d db 37 55 0 56 49 af ar e8 32 c4 437 13 b0 16 2 e db b           d db 37 55 0 56 49 af ar e8 32 c4 437 13 b0 16 2 e db b           d db 36 76 19 a57 10 e b0 16 e db c1 31 51 a1 e e b           d db b5 3 df 76 350 00 1 as df 11 5 d3 16 e de f1 7 00 b           d b2 bb ab f1 e d5 37 (0 x10 00 1)           Artibuters:           d b2 00           D 100	アカウント新規作成	08:6d:62:12:5b:9c:f4:2e:97:58:ef:cf:96:f1:c4:		
a7:51:67:33:72:e9:df:00:edib61:d17:84:44:e0: 6:00:b7:55:44:47:39:00:edib61:d17:84:44:e0: 0:b0:b3:35:09:40:01:e0:e0:a2:edib51:00:00:45:40: b3:35:09:40:01:e0:63:22:edif50:00:00:45:40:00:00:00:00:00:00:00:00:00:00:00:00:		fe:f2:ad:45:50:60:e0:1a:7a:cf:ed:7d:3d:32:12:		
6e:00:b7:55:44:47:99:a1:ee:ec:16:70:92:0a:f1:         0:b3:a3:57:b2:95:41:1e:16:b3:22:0a:f2:         b3:33:50:95:49:a1:ee:83:22:44:73:b5:35:62:ed:0:         f:d0:a5:57:b6:55:56:e6:e6:e6:e6:f7:80:         b2:bb:ab:f1:a5:76:37:b0:b5:b6:a3:44:41:cb:b2:c0:         d7:be:d0:b5:d7:b5:03:a5:11:s5:d3:84:a1:cb:b2:c0:         d7:bb:d0:b5:d1:76:30:01:a5:f1:f5:d3:84:a1:cb:b2:c0:         d7:b2:b5:77:e6:55:56:00:11:a5:f1:f5:d3:84:a1:cb:b2:c0:         d7:b2:b5:77:e6:55:65:80:11:a5:f1:f5:d3:84:a1:cb:b2:c0:         d7:b2:b5:77:e6:55:65:80:11:a5:f1:f5:d3:84:a1:cb:b2:c0:         d7:b2:b5:77:e6:55:65:80:11:a5:f1:f5:d3:84:a1:cb:b2:c0:         d7:b2:b5:77:e6:55:65:80:11:a5:f1:f5:d3:84:a1:cb:b2:c0:         d7:b2:b5:77:e6:55:65:80:11:a5:f1:f5:d3:84:a1:cb:b2:c0:         d7:b2:b5:77:e6:55:65:80:11:a5:f1:f5:d3:84:a1:cb:b2:c0:         d7:b2:b5:77:e6:75:80:70:e6:77:80:90:12:         d5:b0:11:20:20:20:20:20:20:20:20:20:20:20:20:20:		a7:91:67:38:72:e9:df:80:ed:b6:1d:78:a4:4d:e2:		
cbbbsai2fd13951d111e1565a2cd5cc5466;           b5139505944941ctas           cbbbs3575be494541ctas           cbbbs3575be494541ctas           cbbbs3575be494541ctas           cbbbs3575be494541ctas           cbbbs3575be494541ctas           cbbbs3575be494541ctas           cbbbs3575be49541ctas           cbbb5755be49541ctas           cbb5755555555be49541ctas           cbb575555555555555555555555555555555555		6e:08:b7:55:44:47:98:a1:ee:ef:16:70:92:0a:fa:		
b31395019649491af1ac68220447315050562ctdb: fd10a55707e655565665e71800 b21bb3abf2b45781395cb566543034411cb511c8 d71be4dbb531d72501395cb56b3343411cb511c8 f137 Egyptometr: 6537 (0x10001) Attributestor 40100 Format abs2501252000000 Format abs2501250000000 Format abs2501250000000 Format abs25012500000000 Format abs25012500000000 Format abs250125000000000000000000000000000000000		c0:b8:aa:2f:82:39:1d:11:e1:6b:a2:cd:cc:54:6b:		
fd:0a:59:7D:ee:b5:66:44:df:15:a1:e6:6e:f7:80: b2:bb:a1:bb:a1:c6:58:30:ec:b8:33:44:df:c5:81:c6: df:be:dd:b5:dd:76:30:1a:5f1:f5:d3:8e:2a:1c: ef:87 Exponent: 65537 (0x1001) Attributes: a0:00		b3:39:50:96:49:af:ae:88:2c:4a:73:b8:36:2e:db:		
blzbbrahffalds78:39:00beth3134011cbt31:00 d7:betadbbc531d7:50:01asyf1155d3:8e:2a:lo: £187 Atzribussonent: 6537 (0x10001) Atzribussonent: 6537 (0x10001) d1:00 D0000000000000000000000000000000000		fd:0a:59:7b:e6:b5:66:4d:d7:15:a1:e6:6e:f7:80:		
d7:be:ddibb:5did7:63:01:65:f1:f5:d3:8e:2a:1c: ef:87 Exponent: 65537 (0x1001) Attributes: a0:00		b2:bb:ab:fb:45:78:39:cb:6b:3d:34:d1:cb:81:c8:		
efi87 Exponent: 6537 (0x1001) Attributes: 2000 - 2012 - 20		d7:be:dd:bc:5d:d7:63:01:a9:f1:f5:d3:8e:2a:1c:		
Exponent: 6537 (0x1001) Attributes: attoo Economic langthe, abs250(abs252aoung/ac		ef:87		
Attributes: a0:00 Stanuary Jungthan abs257(ab)22Ensympton		Exponent: 65537 (0x10001)		
80:00 Signature ligawithet shale SUITHERE averaging		Attributes:		
Signature llgericky, shale SichDSDE seguration		a0:00	~	
		Cimptume Magnithm, shall ClithDChEnonumtion		

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 2021/04/16 11:19	
> 証明書: <u>あり</u> 作成日時 2021/04/16 11:21	
>秘密鍵:なし	

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

証明書のインポ	- <b>h</b>	?
証明書タイプ	• □-カル ○ SCEP	
証明書名	external-gateway	
証明書ファイル	C:\fakepath\download.crt	参照
ファイルフォーマッ	Base64 エンコード済み証明書 (PEM)	$\sim$
	<ul> <li>□ 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</li> <li>□ 秘密鍵をインボート</li> <li>□ 秘密鍵のエクスボートをブロック</li> </ul>	
キー ファイル		参照
パスフレーズ		
パスフレーズの確認		
	ОК ‡7>	עש

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

デバイス証明書 デフォルトの信頼された証明機関									
Q	Q(2 @の項目s)→×								
	名前	サプジェクト	発行者	CA	<b>#</b>	有効期 限	状態	アルゴ リズム	用途
	Dexternal-gateway	CN = palo	JCCH-SSS demo			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。

名前	external	
証明書	external-gateway	~
- プロトコル設定		
最小バージョン	/ TLSv1.0	$\sim$
最大バージョン	Max	~

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	サーバー認証						
認証	SSL/TLS サービスプロファ external						
	-170						

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。



証明書のインポ	-ト	?
証明書タイプ	● ローカル O SCEP	
証明書名	gleas_ca	
証明書ファイル	C:\fakepath\ia1.pem	参照
ファイル フォーマッ	Base64 エンコード済み証明書 (PEM)	$\sim$
	<ul> <li>□ 秘密鍵はハードウェア セギュリティ モジュール上にあります</li> <li>□ 秘密鍵をインボート</li> <li>□ 秘密鍵のエクスボートをブロック</li> </ul>	
キーファイル		参照
パスフレーズ		
パスフレーズの確認		
	ОК =тр>	tul)

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。

デノ	デパイス証明書 デフォルトの信頼された証明機関								
Q(									$\rightarrow \times$
	名前	サプジェクト 🗸 🗸	発行者	CA	<b>‡</b>	有効期限	状態	アルゴリズム	用途
	∨ 🔊 gleas_ca	CN = EVALUATION CA,	CN = EVALUATION CA,	<ul> <li>Image: A second s</li></ul>		Mar 31	有効	RSA	
	📰 ocsp-sign	CN = ocsp-sign	CN = EVALUATION CA,			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

	CA 証明書	gleas_ca	~
デフォルト	OCSP URL	http:// :2560/ia1	
OCSP	検証証明書	ocsp-sign	$\sim$
テンプレ	ート名/OID		

- [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 す(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

名前gle	asAuth			
3フィ <b>サ</b> :	ブジェクト	✓ common	i-name	
ルド				
7				
~				
明書	名前	デフォルト OCSP URL	OCSP 検証証明書	テンプレート名/OID
•	gleas_ca 追加 ○ 削除 ↑」	http://2560/ia1	ocsp-sign	
■	gleas_ca 注意加 ○ 削除 ↑ 」 ォルト OCSP URL (http:// i	http:// 2560/ia1 とへ ↓ 下へ または https://で開始する必要あり)	ocsp-sign	
€ 77	gleas_ca 追加 〇 削除 个」 ポルト OCSP URL (http:// 2 CRL の使用	http:// 2550/61 たい → 下へ または http://で開始する必要あり) CRL 受信の有効相限 (約)	ocsp-sign	唐伏板が不明な場合にセッション ク
<ul> <li>✓</li> <li>✓</li></ul>	gleas_ca 追加 ○ 削除 ↑ 」 オルト OCSP URL (http://] CRL の使用 OCSP の使用 より OCSP を優先	http:// 2550/61 または http://で開始する必要あり) CRL 受信の有効用限 (例) OCSP 受信の有効用限 (例)	ocsp-sign ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	■状態が不明な場合にセッション ク ムアウト時間内に証明書状態を取
<ul> <li>✓</li> <li>デフ</li> <li>✓</li> <li>CRL</li> </ul>	gleas_ca 追加 ○ 削除 ↑ 」 ポルト OCSP URL [http://] CRL の使用 OCSP の使用 より OCSP を優先	thtp:// 2500/61     2500/61     CRL 受信の有効期限 (8) [         CCSP 受信の有効期限 (8) [         E時間の有効期限 (8) [         E時間の有効]         E時間の有効期間 (8) [         E時間の有効]         E時間の有効期間 (8) [         E時間の有効]         E         E         E	ocsp-sign 2 証明 2 分 2 分 2 分 2 分 2 分 2 分 2 分 2 分 2 月 2 日 2 日 2 日 2 日 2 日 2 日 2 日 2 日 2 日 2 日	書状数が不明な場合にセッション ムアウト時間内に証明書状数を取 い場合にセッションをプロック ページマーマーマーマー
<ul> <li>✓</li> <li>✓</li></ul>	gleas_ca 1追加 ○ 削除 ↑ 」 オルト OCSP URL [http://] CRL の使用 OCSP の使用 より OCSP を優先	http:// 2550/s1 をたはhttps:/ で開始する必要あり) CRL 受信の有効期間 (約) 証明者の有効期間 (約)	ccsp-sign     こ    こ    こ    こ    こ    に    い    に    い    こ    い    こ    ジ     こ     こ    ジ    こ    ・    ご    ジ    ジ	書状版が不明な場合にセッション ク ムアウト時間内に証明書状版を考 い場合にセッションをブロック 書か認識研デバイスに発行された 合センションをブロック

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。



全般	サー	サーバー認証								
8証	SSL	SSL/TLS サービス プロファ external								
Eージェント ナテライト	25	イアント認証	-170							
		名前	OS	認証プロファイ ル	バスコードを自 動取得	ユーザー名のラ ベル	パスワードラベ ル	認証メッセージ	ユーザー資格 報またはクラ- アント証明書 使用した認証 許可	
		ADauth	Any	Auth-Profile01		Username	Password	Enter login credentials	いいえ	
	+	追加 ⊝ 剛剛	k @22-	↑ 上へ ↓ 下へ						
		証明書プロファイル [glessAuth								
			R	難されたデバイスのロ	グインをブロック					

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 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

UA 申込局 ▶<u>Gleas Generic UA</u> Gleas デフォルト申込局

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

▶基本設定	日上級者向上
<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</li> <li>ダウンロード可能時間(分)</li> </ul>	<ul> <li>管理するトークン</li> <li>Gemalto.NETカード </li> <li>証明書ストアの種類</li> <li>ユーザストア</li> <li>インボートワンスを利用する</li> <li></li></ul>
1	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]

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

			-	1774-rca Gléäs 🛛
テスト 太郎 さんのべ	ページ]			■ <i>₽<i>७7</i>5</i>
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		
> 姓:テスト 名:太郎 > ユーザID:testuser > メールアドレス: > パスワード:************************************	****			
★ 証明書情報 ····· ◆ 発行済み証明書				
#	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



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。

(テスト 太郎 さんのページ) マーザ毎報 ● フーザ 伝報 さんのページ ■ ユーザ情報 ● ユーザ 伝報 ※目目時: 202000/14 06:16 > 目: テスト 名: 太郎 > ユーザの: testuser > メーリロ: testuser > メーリアレス: > バスワード: ************************************				プライ	«-hea Gleas
z - 57年程	テスト 太郎 さんのぺ	ージ]			1 <u>9</u> 2
<ul> <li>○ テスト 太郎 さんのページ</li> <li>シューザ情報</li> <li>シューザ 登録日時: 202005/14/06:16</li> <li>&gt; 独: テスト 名: 太郎 シューザロ: testuser</li> <li>シューザロ: testuser</li> <li>シューリアに又: ショーレアに又:</li> <li>&gt;&gt; パスワード: ************************************</li></ul>	ユーザ情報		_		_
	🖉 テスト 太郎 さんの	)ページ			
▶ ユーザ 全組日時:202000/14/06:16     > 対: 方沢: 名: 太郎     > ユーザ[D: lestuser     > ノールアレス:     > ノバンアしス:     > パスワード: ************************************	▶ユーザ情報 ·····				
> 姓: テスト 名: 太郎 > ユーザD: Itsituser >> パルアレス: >> パスワード: ************************************	▶ ユーザ	登録日時: 2020/08/14 06:	16		
▶ 第行済み互明書	>班: テスト 名: 太郎 > ユーザID: testuser > メールアドレス: > パスワード: ************************************				
# 発行局 シリアル 有効期限 証明書ストアヘイ	▶ 発行済み証明書				
	#	発行局	シリアル	有効期限	証明書ストアヘインボート
発1 EVALUATION CA #526 2021/03/31 ダウレロード	<u>\$1</u>	EVALUATION CA	#526	2021/03/31	ダウンロード済み

#### 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。

GlobalProtect	GlobalProtect
サインイン 認証失敗. Enter login credentials	Core a
Portal(ボータル): palo	
•••••	
サインイン	接続済み 企業ネットリークに安全に接続され
キャンセル	ました

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

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
□ トークンへのインボート
□ 証明書ストアへのインボート
▶ 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となる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

する				
する 	☑ ログインバスワードで証明書を保護			
する	□ 接続する iOS デバイスを認証する			
デフォルトを利用 🗸 🗸				
受定				
プライベート CA Gleas				
識別子 (例: com.jcch-sss.profile				
JCCHセキュリティ・ソリューション	ハシステムズ			
プライベート CA Gleas で作成し	た構成プロファイル			
	する する 法法中可 する 「 デフォルトを利用 マ 第定 「 フライベート CA Gleas Com Jcch-sss.profile JCCHセキュリティ・ソリューション 「 フライベート CA Gleas で作成し:			

PaloAlto GlobalProtectの設定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PA-Firewallのホスト名 (或いはIPアドレス)を入力 (必 須)

PaloAlto GlobalProtect	院
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。



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CA	Gléås 🔼	プライベート	ca Glé	as ua	プライベート(	🗛 Gléås 🛂
テスト ユーザ2 さんの	のページ	テスト ユーザ2 さ	きんのページ	P	テスト ユーザ2 さ	きんのページ
ユーザロ	testuser2	ユーザロ		testuser2	ユーザID	testuser2
姓	テスト	姓		テスト	姓	テスト
名	ユーザ2	名		ユーザ2	*	- **2
メール		このWebサイト イルをダウンロ	トは構成プロ コードしよう。 ・ますか?	ファ として	70771/	レがダウンロード 済み ンストールするには"設
EVALUATION CA			/ of y /J · :		E 定"Appで再始	自認してくたさい。
有効期限 2021/06/10	ダウンロード		無視	計型 ·	7	162

画面の表示にしたが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Gléas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。



く 情報 証明書信頼設定
トラスト・ストア・バージョン 2020
トラスト・アセット・バージョン 12
ルート証明書を全面的に信頼する
EVALUATION CA

## 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。

<u> </u>	Enter login credentials	GlobalProtect
GlobalProtect に接続 してネットワーク接続 を保護してください	Username testuser2	
e print of the con-	Password 表示	
	<u> </u>	
タップして接続		接続済み

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