

プライベート認証局Gléas ホワイトペーパー

Pulse Policy Secureでの802.1x EAP-TLS認証設定

Ver. 1.0 2018 年 2 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	ł
1.1.	本書について4	ł
1.2.	本書における環境	ł
1.3.	本書における構成	5
2. Polic	y 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	3
2.3.	User Realm 設定12	2
2.4.	Authentication Protocol Set 設定14	ł
2.5.	Sign-in Policy の設定15	5
2.6.	Location Group および RADIUS Attributes 設定15	5
3. Gléas	s の管理者設定(Windows PC)	,
3.1.	UA(ユーザ申込局)設定17	,
4. Wind	ows PC での証明書インポート・無線 LAN 設定18	;
4.1.	Gléas の UA からのインストール18	3
5. Gléas	s の管理者設定(iPad)19)
5.1.	UA(ユーザ申込局)設定19	J
6. iPad	での構成プロファイル・証明書のインストール 21	
6.1.	Gléas の UA からのインストール21	l
6.2.	OTA エンロールメントを利用した証明書発行について	ł
7. クラ・	イアントからの接続 24	ł
8. 問い1	合わせ	5

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、Pulse Secure社製ネットワークアクセス制御機器「Pulse Policy Secure」を利用しての802.1x EAP-TLS接続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。

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。

- ▶ Pulse Secure Policy Secure (バージョン5.4R1 (build 42499)) ※以後、「Policy Secure」と記載します
- プライベート認証局Gléas (バージョン1.14.6)
 ※以後、「Gléas」と記載します
- ▶ 無線LANアクセスポイント: AirMac Extreme (バージョン7.6.9)
- クライアント(PC): Windows 10 Pro
 ※以後、「Windows PC」と記載します
- クライアント(タブレット): iPad Air 2 (iOS10.3.2)
 ※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。

- Policy Secureでの基本的なネットワーク設定、RADIUSクライアント(無線 LANアクセスポイント)の追加方法
- 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・設定
- PC・iPadの操作方法

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。



- Gléasは、Policy Secureにサーバ証明書、Windows PCとiPadにクライアント 証明書を発行する。
- 2. 管理者はPolicy Secureにサーバ証明書を設定する。
- 3. ユーザは、Gléasの利用者Web画面(UA)より証明書をWindows PCとiPadに インポートする。同時に、無線LANの接続プロファイルもインポートする。
- 4. Windows PCとiPadからEAP-TLS認証による無線LANアクセスをおこなう。

2. Policy 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。 あらかじめ 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。



管理者画面左側のメニューより[Configuration] > [Certificates] > [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。

Configuration > Certificates > Trusted Client CAs								
Cor	onfigur _{tificates}	ation						
Pulse One	Security	Certificates	DMI Agent	Sensors	Client Types	Guest Ad	ccess	
Device Certif	icates Tr	usted Client CAs	Trusted Se	erver CAs 🕴	Client Auth Cert	ificates	Certific	ates Validi
Users can be required to present valid client-side certificates to sign in(see the realm-specific <u>Certifica</u> certificate authorities.								
Auto-imp	port optior	ns Prox	ky Settings.	Imp	ort CA Certifi	cate	Del	ete

[Import From:]のところで[参照]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。

Configuration > Certificates > Trusted Client CAs > Import Trusted Client CA					
Certificate file					
Import from: C:\temp\ia1.cer	参照				
Import Trusted Client CA?					
Import Certificat	е				

成功すると以下のような画面が現れます。

Configuration > Trusted Client CAs > Trusted Client CA					
Successfully imported T	rusted Client CA: JCCH-SSS demo CA				
Certificate					
Issued To:	JCCH-SSS demo CA				
Issued By:	JCCH-SSS demo CA				
Valid Dates:	Jan 11 15:46:45 2010 GMT - Jan 6 15:46:45 2030 GMT				
Details:	Other Certificate Details				
Renew Certificate					

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、 Client certificate status checking 項目で、[Use CRLs (Certificate Revocation Lists)]を選択します

Client cert	ificate status checking
0	None
0	Use OCSP (Online Certification Status Protocol)
۲	Use CRLs (Certificate Revocation Lists)
0	Use OCSP with CRL fallback
\bigcirc	Inherit from root CA

ここで一度[Save Setting]をクリックして、設定を保存します。

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 の設定画面に移動しますので、以下の設定をおこないます。

- [Use:]のドロップボックスより[Manually Configured CDP]を選択
- Primary CDP の[CDP URL]に CRL 配布ポイントとなる URL を入力
 ※CRL 配布点が複数ある場合は、Backup CDP を設定します

以下は Gléas が http で公開している CRL を取得する場合の設定例となります。

Configuration > True CRL Check	ted Client CAs > ICCH-SSS demo CA > ing Options
Specify the CRL d	stribution point(s) from which to download the CRL, as well as how often to download.
Use: Manual	y configured CDP
Specify a H	ITP or LDAP-based CDP, and an optional backup CDP if the primary CDP is not accessible. If the CDP requires authentication, enter the appropriate credentials as well.
Primary	CDP
CDP UR	L: http:// /crl/ia1.crl
	HTTP example: http://server.domain.com:839/domaincaserver.crl LDAP example: ldap://ldap.domain.com:6000/CN=ldap.CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=domain,DC=com?certificateRevocationList?base? objectclass=COlbstitututionPoint
Admin I	N: (LDAP only)
Passwo	d: (LDAP only)
Backup	CDP
CDP UR	L:

また CRL の取得間隔を指定したい場合は、Options 項目で[CRL Download Frequency]を指定することにより可能です。

以下は CRL の有効期限に関係なく、24 時間毎に CRL を取得する場合の設定例となります。

Options		
CRL Download Frequency:	24	hours (1-9999)

設定終了後、[Save Setting]をクリックして設定を保存してします。

遷移した画面の CRL Setting の Status 欄に Enabled と表示されます。

CRI Cert (CD	CRL Settings Certificate revocation lists (CRL) are used to verify the ongoing validity of user certificates, and are obtained from CRL distribution points (CDP). To enable CRL checking, click CRL Checking Options, and specify the options.							
	CRL Checking Options Update Now Enable Disable							
	CRL distribution points	Status	Last Updated	Next Update				
	http://demo.jcch-sss.com/crl/ia1.crl Last result: Success, new CRL	Enabled; OK: 8KB, 162 revocations	2018/01/19 16:35:49 [Save CRL]	2018/02/17 20:30:36				

2.2. サーバ証明書の設定

管理者画面左側のメニューより[Configuration] > [Certificates] > [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。

New CSR Delete	
Certificate Signing Requests	

ホスト名など、必要事項を入力し[Create CSR]をクリックします。 以下はRSA2048ビットの鍵長でCSRを作成する例です。

Configuration > Certificates >	. .
New Certificate Signi	ng Request
Use this page to create a new	v Certificate Signing Request (CSR) to send to your Certificate Authority of choice
Common Name: (e.g., secure.company.com)	pulse-test.js3-test12.loca
Organization Name: (e.g., Company Inc.)	JS3
Org. Unit Name: (e.g., IT Group)	
Locality: (<i>e.g.</i> , SomeCity)	
State (fully spelled out): (e.g., California)	
Country (2 letter code): (i.e., US)	
Email Address:	
Key Type:	● RSA ○ ECC
Key Length:	2048 V bits
Please enter some random c We recommend that you ent	haracters to augment the system's random key generator. er approximately twenty characters.
Random Data: (used for key generation)	•••••
	Create CSR

CSRの生成がおこなわれます。

CSR created su	ccessfully					
our CSR was crea	ated succes	fully. See below f	for instructions on sending the CSR to a Certificate Authority.			
The certificate approval process may take several days. When you receive the signed certificate from the Certificate Authority, you will need to import the certificate to complete this process.						
afiguration >						
nfiguration > ending Ce CSR Details	ertificat	e Signing	Request			
nfiguration > ending Ce CSR Details Common Name: Created:	pulse-test.js 1/19/2018 1	e Signing ^{3-test12.local} 7:18:55	Request			
nfiguration > ending Ce CSR Details Common Name: Created: Org. Name: Org. Unit Name: Email Address:	pulse-test.js 1/19/2018 1 JS3	e Signing a-test12.local 7:18:55 Locality: State: Country:	Request			

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

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。

O作業名: <u>サーパ証明書</u> O管理者: <u>テスト管理者</u>	第5元 プライベートCA	Gléå's 🖪
 ○「茶菜: エノン型考査 ○「お子: エノン型考査 「アカウント]->茶ド ② たらのはす ③ Cartificate ③ EdaPyrifa ③ EdaPyrifa ● State ● State	建築記録 プライベートCA 「登録法 ローム」 ロジン ロッシューム 「登録法 ローム」 ロジン ロッシューム 「日本記』を Puise-test.jcch-ass.local 語明書要求(CSR)の確認 ロームンロット Data: Variation 50 (DSD) Subject: 0-SSD, Clippelae-test.jcch-ass.local Subject: 0-SSD, Cli	● サイドハー ● ● サイドハー ● ● クイックアビ ● ● ユージ正形法 ● ■ ユージ正形法 ● ■ ユージ正形法 ● ● ビニリ形法 ● ● ビニリ形法 ● ● ビニリ形法 ● ● ビニリジボホー ● ■ コージェアのホー ● ● ビニリジェー ● ●<
アカウントー覧 登録中単素一覧 アカウント新聞作成	2 f:15:51:93:46:77:10:e4:2r:13:04:47:40:cb: 24:55:44:00:61:83:a6:27:16:e4:07:66:35:66:17: 40:f5:84:40:16:85:65:76:17:03:a6:11:64:66:99:f7: 40:f5:84:44:11:14:59:84:44:40:77:65:86:86:b5: 51:94:f5:19:96:96:67:00:11:76:62:b5:14:46:87:e6: 40:95:97:96:96:67:00:11:76:62:b5:14:46:87:e6: 40:95:97:96:96:86:14:14:19:89:84:19:76:15:64:14: 41:82:77:95:90:26:e6:14:95:16:64:14:97:15:e6: 41:82:77:95:90:26:e6:14:95:16:64:15:97:15:64:15: 41:15:f4:31:b5:19:16:14:05:19:16:14:15:15:64:15: 31:05:15:04:05:25:e6:16:20:04:16:77:15:16:45: 31:05:15:04:05:25:e6:16:20:04:16:77:16:16:12: 76:06:10:95:26:16:20:04:07:16:16:10:12: 76:06:10:95:26:16:20:06:17:95:15:10:75:06:12: 76:06:10:95:26:16:20:06:17:95:15:10:14:15: 55:bf Exponent: 65:37 (0x10001)	ま <u>7772-1-10)</u> ● 証明度 (0)

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。

 O作業名: サーバ証明 O管理者: テスト管理者 	R <u>第行デモ</u>	プライベートCA	Gléå 🕏 🛤
[証明書]>詳細		■ 認証局 ■ログ ■管理者 ■ ヘルブ ■ログアウト	0 #4FM-
アカウント Account グループ Group	証明書 同 JCCH-SSS demo2 CA#4 余 証明書情報	0 _ 11月現 ● 552 ● <u>24/3-0</u> 2	 ▶ クイックナビ <u>ユーザ証明書</u> <u>マンン証明書</u> サーバ証明書
★ LE明書 Certificate	pulse-test.icch-sss.local	開始日:2016/01/14 18:37 終了日:2019/01/14 18:37	金 認証局証明書
Service 認証デバイス	৾৾৾৸৸৵৾৴৴৵	▶基本情報	
 テンプレート Template び間書操作 サ会効処理 ・失効処理 ・快加処理 ・ドックに入れる 	>4週:253 >——配名:pulse-test,icch-sss.local) 作成日:204601/14 10:36 > 有功日数:1096 > 火功日数:1096 > 火功用数:1 >> 規関体介日: >> 大核型:有効な証明着 >> 达型の状態:有効な証明者 >> トーンンの層: >> パージョン:4 	(保存 ► ドック <u> ま プカウント (0)</u> 身 証明 <u>書 (0)</u>
	 王田市本部 ご目立ち、北〇に15855 (1988-02, CA) 第テアルニリンズは、1 ra メラインコンアルビリンズは、1 ra メラインコンアルビリンズは、1 ra メデルビリンズは、1 ra シボルビリンゴン(1 ra) シボルビリン(1 ra)		
操作履歴 プライベートCA Gié	25	Copyright (C)2010-2015 JCCH Security Solution Syst	tems Co.,Ltd. All rights reserved.

Policy 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。

Step 2.	Import signed certificate When you receive the signed certificate file from the CA, select it I						
	Signed certificate:	C:\temp\download.crt	参照				
	Import						

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。

Configuration > Certificates > Device Certificate								
Pulse One Security Certificates	OMI Agent Sensors	Client Types	Guest Access					
Device Certificates Trusted Client CAs	Trusted Server CAs	Client Auth Cer	tificates 🕴 Certificates Validity Check					
Specify the Device Certificate(s). If you you can add custom Intermediate CAS.	u don't have a certifica	te yet, you car	n create a CSR and import the resu	ilting signed certificate. If necessary,				
Certificate issued to	Issued by		Valid Dates	Used by				
pulse-test.jcch-sss.local	JCCH-SSS demo CA		Jan 19 08:35:45 2018 GMT to Fe 19 08:35:45 2018 GMT	b				

複数のサーバ証明書が格納されている場合は、クライアントからのアクセスを受け 付けるポートを指定する必要があります。上の画面の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。以下は内部ポートに割り当てる例となりま す。

Certificate Details
Certificate
Issued To: pulse-test.jcch-sss.local Issued By: JCCH-SSS Valid: Jan 19 08:35:45 2018 GMT to Feb 19 08:35:45 2018 GMT Details: Other Certificate Details Download
Present certificate on these ports
Select the internal and external virtual ports that will present this certificate: Internal Virtual Ports: Add -> Remove
External Virtual Ports: Selected Virtual Ports: <external port=""> Add -> Remove </external>
Vlan Ports: Selected Vlan Ports: Add -> Remove

2.3. User Realm 設定

管理者画面左側のメニューより[User Realms] > [User Realms]と進みます。 レルム一覧が表示されるので、デフォルトで作られている[Cert Auth]をクリックし ます。

Authenticationに、[Certificate Authentication]が選択されていることを確認します。

※或いは、新たにUser Realmを作成します

User Realms > Cert Auth > General		
General Authentication	Policy Role Mapping	
* Name: Description:	Cert Auth System created authentication realm for When editing, start on the Role	Label to reference this realm Mapping page
Servers		
Specify the servers to use for Authentication: User Directory/Attribute: Accounting: Device Attributes:	authentication and authorization. To creat Certificate Authentication None None None None	te or manage servers, see the <u>Servers</u> page. Specify the server to use for authenticating users. Specify the server to use for authorization. Specify the server to use for Radius accounting. Specify the server to use for device authorization.
Dynamic policy evaluation		
Enable dynamic policy	v evaluation	
Session Migration		
Other Settings		
Authentication Policy: Role Mapping:		Certificate restrictions Password restrictions 1 Rule

Authenticationの選択肢にCertificate Authenticationがない場合は、右側のメニューの[Auth. Servers]で、Server TypeにCertificate Serverを指定した認証サーバ設定をおこなう必要があります。

以下にその場合の手順を記します。

Authentication Servers	
New: (Select server type) V New Server	Delete
Authentication/Authorization Servers	Туре
Administrators	Local Authentication
Certificate Authentication	Certificate Server
Guest Authentication	Local Authentication
MacAuth	MAC Address Authentication
System Local	Local Authentication

[New:]のドロップダウンより[Certificate Server]を選択し、[New Server...]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、ユーザIDとする証明書内の属性を入力 ※証明書サブジェクト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

Auth Servers > New Certificat	e Server	
* Name:	Gleas	Label to reference this server.
User Name Template:	<certdn.cn></certdn.cn>	Template for constructing user names from certificate attributes.

設定したレルムには、認証成功後にマッピングされるロールを設定しておきます。 以下は、証明書サブジェクトのCNにどのような値があろうとUsersロールを割り当 てる場合の例となります(以下記載の[Auth. Servers]設定の[User Name Template] で <certDN.CN> を指定していること)。

User Realms > Cert Auth > Role Mapping		
General Authentication Policy Role Mapping		
Specify how to assign roles to users when they sign in. Users t	hat are not assigned a role will not be able to sign ir	1.
New Rule Duplicate Delete]	Save Changes
When users meet these conditions	assign these roles	Rule Name Stop
1. <u>username is</u> "*"		all_cn
When more than one role is assigned to a user:		
Merge settings for all assigned roles		
 User must select from among assigned roles 		
 User must select the sets of merged roles assigned by each 	ch rule	
Note: Users that do not meet any of the above rules will not be able to	sign into this realm.	

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. Authentication Protocol Set 設定

Signing-in > Authentication Protocol Sets と進み、認証プロトコルセットに EAP-TLS が含まれるものを作成しておきます。

※Factory Default の状態で、Cert Auth というプロトロルセットが作成されています

<u>Signin</u> Aut	Staning In > Authentication Protocols								
Sign	-in Policies Sign-in Pages Sign-in Notifications Aut	hentication Protocol Sets							
Ne	w Authentication Protocol Duplicate	Delete Restore Fac	tory Default						
	Name	Authentication Protocol	PEAP	TTLS					
	1 802:1X System created default authentication protocol required for UAC agents	EAP-TTLS EAP-PEAP	EAP-JUAC EAP-MS-CHAP-V2	EAP-JUAC PAP MS-CHAP-V2 EAP-MS-CHAP-V2 EAP-GenericTokenCard					
	2 802.1X-Phones System created default authentication protocol for phones	EAP-MD5-Challenge EAP-TLS							
	3 Guest System created authentication protocol for guest users	PAP CHAP							
	4 <u>Cert Auth</u> System created authentication protocol for Certificate Authentication	EAP-TLS	EAP-JUAC EAP-TLS	EAP-JUAC EAP-GenericTokenCard					

2.5. Sign-in Policy の設定

管理者画面左側のメニューより[Signing-in] > [Sign-in Policies]と進みます。その後、 [New URL...]をクリックし以下の設定をおこないます。

- Sign-in URLには、サインイン用のURL(以下の例では */radius)を設定
- Authentication Realmには、2.3項で設定したレルムと2.4項で設定した認証プロト コルセットを設定

lew Sign-I	n Pol	icy						
User type:	Use	rs 🔿 Ad	ministrators					
Sign-in URL:	*/radiu	5				Format: <h< td=""><td>ost>/<path>/;</path></td><td>Use * as wildcard in the beginning of the host nam</td></h<>	ost>/ <path>/;</path>	Use * as wildcard in the beginning of the host nam
Description:	JS3 t	est WiF	i		0			
Sign-in page:	Defaul To create	t Sign-In F or manage p	Page ∨ ages, see <u>Sig</u>	n-In pages.				
Sign-in page:	Defaul To create	t Sign-In I or manage p	Page ✔ ages, see <u>Siq</u>	n-In pages.				
Sign-in page: uthentication realm	Defaul To create	t Sign-In F or manage p	Page V ages, see <u>Sia</u>	n-In pages.				
Sign-in page: uthentication realm	Defaul To create	t Sign-In F or manage p wailable wi	Page V ages, see <u>Sig</u> een signing i	<u>n-In pages</u> . n.	,			
Sign-in page: uthentication realm pecify what realms Delete	Defaul To create will be a	t Sign-In F or manage p wailable wh	Page V ages, see <u>Sig</u> een signing i	n-In pages. n.				
Sign-in page: uthentication realm pecify what realms Delete Available realm	Defaul To create will be a	t Sign-In F or manage p available wh	Page Pages, see Sig en signing i n protocol s	n-In pages. n.				
Sign-in page: uthentication realm pecify what realms Delete Available realm Cert Auth	vill be a more than a construction of the second se	t Sign-In I or manage p wailable wh uthentication Not appli	Page V ages, see <u>Sig</u> een signing i n protocol s cable - V	n-In pages- n. et				

2.6. Location Group および RADIUS Attributes 設定

管理者画面左側のメニューより[Network Access] > [Location Group]と進みます。 その後、[New Location Group...]をクリックします。 任意のロケーショングループ名と、2.5項で設定したサインイン用のURLを設定しま す。

Network Access > Location Group > New Location Group		
Location Group		
 * Name: Description: * Sign-in Policy: MAC Authentication Realm: 	802_1x_test	Label to reference this Location Group. To manage policies, see the <u>Sign-In Polcies</u> To manage realm, see the <u>MAC Address Realms</u>
Save changes		
Save Changes * indicates required field		

保存後、[RADIUS Attributes]タブを選択し、[New Policy...]をクリックします。 任意のポリシー名称と、本項上部で設定したロケーショングループを設定します。 またクライアントに適用するRADIUS属性を設定します。 今回は何の属性の割り当てもしないので、[Open port]を選択しています。

Network Access >	RADIUS Return Attributes Policies >
* Name: Description:	test_policy
Location Group	
Specify the Lo Available Lo Default Guest Cert Auth	Add -> Remove
RADIUS Attribut	es
✓ Open por ✓ VLAN:	t (1 - 4094)

3. Gléasの管理者設定(Windows PC)

GléasのUA(申込局)より発行済み証明書と無線LAN設定をWindows PC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

3.1. 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、Windows PC用となる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]の右側にある[▶上級者設定]をクリック し、設定項目を展開し以下の設定をおこないます。

- [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

▶ 証明書ストアへのインポート	証明書ストアの種類 ユーザストア
□ ダウンロードを許可	✓ インポートワンスを利用する

[無線LANの基本設定]で以下の設定をおこないます。

- [WiFiプロファイルを使用する]をチェック
- [WiFiプロファイルの SSID]に、対象のSSIDを入力 <u>無線LANの基本設定</u>

☑ WiFiプロファイルを使用する			
WiFiプロファイルの SSID	airport-tls		

設定終了後、[保存]をクリックし設定を保存します。

以上でGléasの設定は終了です。

4. Windows PC での証明書インポート・無線 LAN 設定

4.1. Gléas の UA からのインストール

Internet Explorer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。

●エンドユーザログイン [UA]	
●ユーザID、バスワードを入力してロ ダインしてください。	
▶ユーザID	1
▶パスワード	
ログイン	
■コーザID・パフロード友立わたら	
	_

ログインすると、ユーザ専用ページが表示されます。 ※初回ログインの際は、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

その後、 [証明書のインポート]ボタンをクリックすると、無線LANのプロファイルのインポートと、クライアント証明書のインポートが順次自動でおこなわれます。

[テスト ユ-	ーザ01 さんのページ]			٥	ログアウト
ユーザ情報					
8 FZ	トユーザ 01 さんのページ			D	ヘルブ
£ ⊐−1	げ情報 · · · · · · · · · · · · · · · · · · ·				~
▶ ユーザ	登録日時:2011/02/28	09:13			
> 姓: テン > ユーザI > メールァ > バスワー * 証明	スト 名:ユーザ01 D.testuser01 アドレス: ード:************ 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	
R 1	JCCH-SSS demo CA	#11256	2019/10/18	証明書のインポート	
					\sim

Infomation X	Web ページからのメッセージ	×
ワイヤレスネットワークのインストールに成功しました。	ユーザの証明書ストアヘインボートしました。	
ОК	ОК	

「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、再度のインポートを行うことはできません。

[テスト ユー	ザ01 さんのページ]				ジアウト
ユーザ情報		_			
🙎 テスト	ユーザ 01 さんのページ				ルプ
2 ユーザ	情報 · · · · · · · · · · · · · · · · · · ·				\sim
▶ ユーザ	登録日時:2011/02/28 0	9:13			
> 姓: テスト > ユーザID > メールアド > パスワード * 証明書	・名:ユーザ01 :testuser01 レス: ::************ 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	
21	JCCH-SSS demo CA	#11256	2019/10/18	ダウンロード済み	
					\sim

無線LANプロファイルとクライアント証明書がインポートされたWindows PCでは、SSIDを選択するだけで自動的に無線LAN接続をすることが可能です。

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無線 LAN 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

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、設定をおこなう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
- [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。

▶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

[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となる情報を入力する画面が展開されるので、以下設 定を行います。

- [iPhone用レイアウトを利用する]にチェック
- [ログインパスワードで証明書を保護]をチェック
- [iPhone構成プロファイル基本設定]の各項目を入力
 ※[名前]、[識別子]は必須項目となります
 ※[削除パスワード]を設定すると、ユーザが設定プロファイルを削除する際に管理者が定めたパスワードが必要となります(ユーザの誤操作等による構成プロファイルの削除を防止できます)

▶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 □ Mac OS X 10.7以降の持	用する 続を許可	▶ ログインバスワードで証明書を保護			
OTA(Over-the-air)					
OTAエンロールメントを利	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	デフォルトを利用	v			
iPhone 構成ブロファイル表	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.demo-m	ldm			
プロファイルの組織名	JCCH・セキュリティ・ソリ	リューション・システムズ			
記日月	テスト用の構成プロファー	テスト用の構成プロファイル			
削除バスワード					

入力が終わったら、 [無線LAN(802.1x)の設定]項目まで移動し以下を設定します。

- [SSID]に、WiFiアクセスポイントのSSIDを入力
- (SSIDをブロードキャストしていない場合) [非公開ネットワーク]をチェック 無約 AN(802 1x)の設定

MUNCH AND OF LEASE	
SSID	airport-tls
· 非公開ネットワーク	

設定終了後、[保存]をクリックして設定を保存します。

以上でGléasの設定は終了です。

6. iPad での構成プロファイル・証明書のインストール

GléasのUAに接続し、発行済みのクライアント証明書・構成プロファイルのインポートを行います。 ※本ケースではUAに接続するためのネットワーク接続が必要となります(3G回線や、証明書認証を必要としない無線LAN接続等)

6.1. Gléas の UA からのインストール

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。

21 / 25



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、[構成プロファイルの ダウンロード]をタップし、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

自動的にプロファイル画面に遷移するので、[インストール]をタップします。 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可能で すので、必要に応じ確認してください。



パスコードロックを有効にしている場合(或いは構成プロファイルでパスコードロ ックを強制する場合)はパスコードを入力します。

その後、以下のようなルート証明書追加の警告画面が現れますので、[インストール]をクリックして続行してください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書に なります



インストール完了画面になりますので、[完了]をタップします。



元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトしてく ださい。

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。

無線LANプロファイルとクライアント証明書がインポートされた端末では、SSID を選択するだけで自動的にWiFi接続をすることが可能です。

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能とな ります。

テスト ユーザ01 さんのページ]					
ユーザ情報					
悤 テスト ユーザ01 さんのページ					
2 ユーザ情報					
▶ ユーザ	登録日時 : 2011/	02/28 09:13			
> 姓: デスト 名: ユーザ01 > ユーザD : testuser01 > メール :					
★ 証明書情報 · · · · · · · · · · · · · · · · · · ·					
▶ 発行済み証明書					
# 発行局 シリアル 有効期限 ダウンロード					
\$1 JCCH-S	SSS demo CA	#11256	2019/10/18	ダウンロード済み	

6.2. OTA エンロールメントを利用した証明書発行について

Gléasでは、iOSデバイスに対するOver The Air (OTA) エンロールメントを利用した証明書の発行・構成プロファイルの配布も可能です。

OTAを利用すると事前に指定した端末識別番号を持つ端末だけに証明書の発行を限 定することも可能になります。



詳細は最終章のお問い合わせ先までお問い合わせください。

7. クライアントからの接続

クライアントデバイスでは無線LANの接続設定はすでにおこなわれているので、対象のSSIDを選択すれば自動的にEAP-TLS認証をおこなって接続されます。

認証の成功時には、Policy SecureのUser Accessログに以下のログエントリが表示 されます。

Agent login succeeded for USER_NAME/USER_REALM from MAC_ADDRESS. Primary authentication successful for USER_NAME/Certificate Authentication from MAC_ADDRESS The X.509 certificate for 'CERT_SUBJECT' issued by CERT_ISSUER, successfully passed CRL checking CRL checking started for certificate 'CERT_SUBJECT' issued by CERT_ISSUER

失効済みの証明書でアクセスすると接続に失敗し、Policy SecureのUser Accessロ グには以下のログエントリが表示されます。

```
Login failed using auth server Certificate Authentication (Certificate Server). Reason:
Revoked Certificate
Primary authentication failed for USER_NAME/Certificate Authentication from MAC_ADDRESS
The X.509 certificate for 'CERT_SUBJECT' issued by CERT_ISSUER failed in CRL checking;
Status '23'; Detail: 'certificate revoked'
CRL checking started for certificate 'CERT_SUBJECT' issued by CERT_ISSUER
```

```
24 / 25
```

8. 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。

■Policy Secureに関するお問い合わせ先

マクニカネットワークス株式会社

Pulse Secure 製品担当

TEL: 045-476-1980

Mail: pulsesecure-sales@cs.macnica.net

■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 営業本部 Tel: 050-3821-2195

Mail: sales@jcch-sss.com