

\sim Enterpras \sim

RADIUSサーバ(802.1x EAP-TLS)認証連携設定

Ver. 1.0 2017 年 8 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	4
1.1. 1.2.	本書について 本書における環境	4 4
1.3.	本書における構成	5
1.4.	電子証明書の発行時における留意事項	6
2. 【ショ	ナリオ1】Enterpras の設定	6
2.1.	CA の設定	6
2.2.	サーバ証明書の発行と適用	7
2.3.	ルート証明書と、クライアント証明書認証の設定	11
2.4.	ユーザの作成	13
3. Gléa	s の管理者設定(PC)	14
3.1.	UA(ユーザ申込局)設定	15
4. Wind	lows PC での証明書インポート・無線 LAN 設定	15
4.1.	Gléas の UA からのインストール	15
5. Gléa	s の管理者設定(iPad)	17
5.1.	UA(ユーザ申込局)設定	17
6. iPad	での構成プロファイル・証明書のインストール	19
6.1.	Gléas の UA からのインストール	19
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	21
7.【ショ	ナリオ2】Enterpras の設定	22
7.1.	RADIUS プロキシの設定	22
8. 【ショ	ナリオ2】Gléas の管理者設定	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」で発行したクライアント証明 書を利用して、株式会社ステラクラフトのRADIUSサーバ製品「Enterpras」でWiFi 認証(802.1x EAP-TLS)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。

- RADIUSサーバ: Enterpras Std 3.5
 ※以後、「Enterpras」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7.6.8)
- 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

以下については、本書では説明を割愛します。

- Enterprasのインストールと基本的なRADIUS設定
- Gléasでのアカウント登録や各種証明書発行
- クライアントのセットアップ

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。

■シナリオ1



- Gléasは、Enterpras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。Enterprasの信頼する認証局証明書として、CA#1のルート証明 書を設定する。
- 2. 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、WiFiの接続プロファイルもインポートする。
- 3. Windows PCとiPadからEAP-TLS認証によるWiFiアクセスをおこなう。

■シナリオ2 (RADIUSプロキシ検証)



- Gléas内に2つ目のルートCAを作成し(CA#2)、Enterprasサーバをもう一つ準備する(RADIUS#2)。 これらをシナリオ1とは異なる組織(認証レルム)の認証システムと仮定する。 Enterpras(RADIUS#2)の信頼する認証局証明書として、CA#2のルート証明書を設定する。
- GléasはCA#2を使って、RADIUS#2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。
- 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、WiFiの接続プロファイルもインポートする(同じア クセスポイントを利用する)。
- 4. Windows PCとiPadからEAP-TLS認証によるWiFiアクセスをおこなう。この時の認証はRADIUS#2でおこなう(RADIUS#1をプロキシとして利用)。

1.4. 電子証明書の発行時における留意事項

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。

シナリオ2においてGléasにアカウントを作成する際は「ユーザID@レルム名」
 である必要があります

2. 【シナリオ1】Enterprasの設定

Enterpras の管理画面に管理者ログインし、以下の設定をおこないます。

2.1. CA の設定

管理者画面のメニューより、[CA運用管理] > [CA運用方針]と進み、「CA運用方針/ 手順」にて以下の設定を行います。

● [2.3 EAP-TLS を利用する。(EAP-TTLS, EAP-PEAP も利用可)]を選択

CA運用方針

- CA運用方針/手順

証明書について WebサーバにSSLを利用する場合(mod_sslインストール直後は仮の証明書が使われています)や、 認証サーバ認証方式に、EAP-TTLS,EAP-PEAP,EAP-TLS,を利用する場合、証明書の設定が必要になります。 証明書の発行方針を決定して下さい。 [注意]設定するには必ず[確定]ボタンをクリックして下さい。
 このサーバを、プライベートCAとして利用する。 1.1 Webサーバの通信のみSSLを使用する。 1.2 EAP-TTLS,EAP-PEAPを利用する。 1.3 EAP-TLSを利用する。(EAP-TTLS,EAP-PEAPも利用可)
 このサーバ以外のブライベートCAを使う。 2.1 Webサーバの通信のみSSLを使用する。 2.2 EAP-TTLS,EAP-PEAPを利用する。 2.3 EAP-TLSを利用する。(EAP-TTLS,EAP-PEAPも利用可)
3. プライベートCA、証明書関連のすべてを削除します。 [注意]WebサーバのSSL通信ができません。 ○ 3. 初期状態に戻す。
確定

設定完了後、[確認]をクリックして設定を保存します。

2.2. サーバ証明書の発行と適用

[CA運用管理] > [自サーバCSR発行]と進み、以下のサーバ証明書の発行リクエスト ファイル作成に必要な情報の入力をします。

- 鍵長: 2048を選択
- パスフレーズ: 秘密鍵に付与するパスフレーズになります。
 任意のパスフレーズを入力します
- 国名(C): JPを入力
- 都道府県(ST)、市区町村(L)、会社名(O)、部署名(OU)、Eメールアドレス:
 環境にあわせ、適宜入力(認証には影響しません)
- サーバ名(CN): サーバホスト名を入力
 ※Gléasにも同名のサーバアカウントが存在する必要があります

入力完了後、[CSR作成]をクリックするとCSR(証明書署名要求)が生成されます。 その後[CSRダウンロード]をクリックすると、newcsr.pemという名前のファイルが ダウンロードされるので適当な場所に保存します。

自サーバCSR発行

自サーバのCSRを作成します。 CSR作成すると、自動的に「サーバ秘密鍵」、「サーバ秘密鍵のパスフレーズ」が上書きされます。 [注意]すでにCSR作成は作成されています。再作成する場合のみ「CSR作成」をクリックして下さい。

鍵長(ビット)	○ 1024 ● 2048 ※CA局の運用に合わせて選択してください。
パスフレーズ	
パスフレーズ(確認)	
国名(C)	JP
都道府県(ST)	Токуо
市区町村(L)	Arakawa
会社名(0)	JS3
部 署名(OU)	sales
サーバ名(CN)	enterpras.jcch-sss.local
Emailアドレス	sales@jcch-sss.com
チャレンジパスワード(省略可能)	
協力会社名(省略可能)	

CSR作成 リセット

CSRダウンロード

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。

1			► <u>12</u>	15日 10日ク 10日2211日日 10日21日日	29E 0#4FM-
アカウント Account	アカウント			0-1	111 戻る ▶ クイックナビ
のグループ	enterpras.jcch-sss.local				<u> </u>
Group	● アカウント情報・・・・・・・		ち グループ情報		··· へ ■ サーバ証明書
★ 証明書 Certificate	トサーバ 谷級日	Bh:2017/06/29 16:25	・ユーザグループ	D & ta	★ 認証局証明書
認証デバイス Device	▶ステータス:有効		>なし		
テンプレート	▶サーバ属性 最終更新:20	17/06/29 16:25 <u>援集</u>	▶ロールグループ	▶参加	
Template	▶ホスト名: enterpras.jcch-sss.local		> グローバルグループ		保存
●アカウント操作					
アカウント一覧	★ 証明書発行の履歴 ······				► ドック ■ アカウント (0)
登錄申請者一覧	Þ1				<u>₹証明書(0)</u>
アカウント新規作成	# シリアル 開始	有効期限 ス・	テータス 失効日	暗号種別 トークン	
▶証明書発行		証明書は発行。	されていません。 		
▶アカウント削除	▶ テンプレート情報 ······				
▶ドックに入れる	・サブジェクト				
	種別		必須テンプレート	任意テンプレート	
	一艘名(CN)	enterpras.jcch-	-sss.local		
	ドメインコンボーネント(DC)	COM JCCH-SSS			

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 (newcsr.pem) 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。

「リリント」> 証明	書発行	■認証局 ■日夕 ■管理者 ■	<u>ヘルブ ■ログアウト</u> ●サイドバー
アカウント	アカウント		□ 一覧に戻る
Account	enterpras.jcch-sss.local		▶ 詳細に戻る 8 ユーザ証明書
グループ Group			マシン証明書
野田書	★ 証明書発行		▲ ■ <u>サーバ証明書</u>
Certificate	この画面では証明書要求の作成を行います。		金 認証局証明書
認証デバイス Device	左側の「ワフシェクト」と「周日」の内容で証明音要求で下別します。 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」を押してび	Eð N.	
テンプレート	▶証明書発行		級者向于設定
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
カウント操作	▶ □ 発行済み証明書をすべて失効させる		
カウントー覧	> 証明書要求(CSR)ファイルをアップロードする: C∴temp\newcs	r.pem 参照	► ドック ■ マカウン(ト (0)
绿申請者一覧	> ☑ CSRファイルの内容を確認する		(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
カウント新規作成		祭 行	A SECTOR (C)
正明書発行			
	▶サブジェクト	▶ 選択されているテンプレート	<u>全て解除</u>
	> CN=enterpras.jcch-sss.local	> 必須 デフォルト設定	
	> DC=COM, JCCH-SSS		
		▶ 選択可能なテンプレート	
	▶属性	>/al	
	▶ 発行局: JCCH-SSS demo CA		_

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。

Pカウント]>発行		■認証局 ■ログ ■管理者 ■ヘルブ ■ログアウト ●サイドバー
アカウント		▶ 一覧に戻る ▶ クイックナビ
Account	·····································	
All -7	enterpras.jccn-sss.iocal 証明音要求(CSK) の確認	B 15/C/L B LUNACHITE G
Group		■ マシン証明書
Ce	rtificate Request:	∧ ■ サーバ証明書
証明書	Data:	
Certificate	Version: 0 (0x0)	m 認証局証明書
	Subject: C=JP, ST=Tokyo, L=Arakawa, O=JS3, OU=sales, CN=ente	erpras.jcch-sss.local/emailAddress=sales@
認証デバイス	Subject Public Key Info:	
Device	Public Key Algorithm: rsaEncryption	
	RSA Public Key: (2048 bit)	
テンプレート	Modulus (2048 bit):	
Template	UU:D4:36:38:78:65:72:1a:94:49:66:62:a0:E1:1b:	(27)
	62196101/11101001231001001001001001001001001	10.12
アカウント操作	40:/4:20:15:01:/0:Dd:11:15:/0:10:44:01:140:15:	
	50.15.00.06.07.26.64.61.94.10.27.40.69.07.70.	▶ ドック
パリントー覧	9b:12:67:02:b7:cc:95:10:18:7a:5d:be:19:78:2c:	まアカウント (0)
经申請去一覧	22:8f:c0:e6:68:18:c1:14:ee:33:7a:de:3b:88:dd:	+ MOT T (0)
	29:78:1e:ce:69:a9:1e:68:4f:12:6f:7d:a6:7c:eb:	<u>★ 計算時間 [0]</u>
カウント新規作成	5c:dd:6e:69:20:3c:b8:28:0e:d6:34:a3:47:19:65:	
	e3:9c:22:7f:b3:cd:6f:94:1d:98:f9:b9:5a:1a:f6:	
	d4:0d:4f:4f:da:8b:dc:c4:95:4c:95:53:3b:0d:7c:	
	a5:38:d2:10:af:5d:57:10:11:21:3e:e5:89:42:a3:	
	e6:eb:41:f6:d4:a8:52:20:db:82:a4:b3:49:52:75:	
	28:25:2c:02:00:04:a2:90:b1:40:2a:e3:8f:37:aa:	
	29:c7:62:8e:07:09:96:c3:1e:a1:08:85:a8:28:03:	
	89:f4:8b:8f:a5:ae:d9:ac:52:43:d3:f3:0f:ec:83:	
	de:e7:4d:61:3f:e6:f3:f8:9b:b7:27:68:4e:07:dd:	
	91:95	
	Exponent: 65537 (0x10001)	
	Attributes:	\checkmark
	a0:00	

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>」を右ク リックし、発行された証明書(download.crt)をダウンロードします。



Enterprasの管理画面に戻り、[CA運用管理]>[サーバ証明書管理]と進み、Webサー バのサーバ証明書と、認証サーバのサーバ証明書にGléasよりダウンロードしたファ イル (download.crt) をアップロードします。

サ-	サーバ証明書管理			
	绿成Tカ			
認認	証サーバ	証明書を設定しま	ました。	
認	証サーバネ	を利用するには、	、 CA証明書が必要です。	
一他	のCAで運	用時(サーバ証明	月書)	
証(秘) 証(証)	明書の登録 密鍵の登録 明書がPK 明書を削り	禄、更新するに(禄、更新するに(CS12形式の場合 除する場合は、[は、お使いのコンピュータのフ; は、[パスフレーズ]を入力してか (は、[パスフレーズ]を入力して) (Webサーバ証明書を削除]またに	ァイルを選択して[アップロード]ボタンをクリックして下さい。 からファイルを選択して[アップロード]ボタンをクリックして下さい。 下さい。必要なCA証明書、中間CA証明書、サーパ証明書、サーパ秘密 ±[認証サーパ証明書を削除]ボタンをクリックして下さい。
凡/ 項	列: 目「設定〉	斉」の「済」は"	すでに設定されています。「未ん	乍業」は設定されていません。
We	bサーバ			
#	設定済	項目	有効期限	操作
1	未作業	中間CA証明書		参照… アップロード PKCS12形式の場合パスフレーズ:
2	3	サーバ証明書	2020年6月29日 16時32分45秒	参照 アップロード
Ĺ	w		2020-00 125 [] 10000200 1010	PKCS12形式の場合パスフレーズ:
3	B	サーバ秘密鍵	-	参照 アップロード
	⊥ Vebサー/	「証明書を削除	1	
認	証サーバ		1	
#	設定済	項目	有効期限	操作
1	未作業	CA証明書		を照… アップロード PKCS12形式の場合パスフレーズ:
2	未作業	中間CA証明書		を照… アップロード PKCS12形式の場合パスフレーズ:
3	B	サーバ証明書	2020年6月29日 16時32分45秒	参照 アップロード PKCS12形式の場合パスフレーズ:

4 🛞

サーバ秘密鍵 -

Γ

パスフレーズ:

参照... アップロード

2.3. ルート証明書とクライアント証明書認証の設定

Gléasにhttpで接続するとルート証明書のダウンロードができるので、あらかじめ ダウンロードしておきます。



Enterprasの管理画面で、[CA運用管理]>[サーバ証明書管理]と進み、認証サーバの CA証明書にルート証明書をアップロードします。

サ					
	他のCAで運用時(サーバ証明書)				
ting and ting store	証明書の登録、更新するには、お使いのコンピュータのファイルを選択して[アップロード]ボタンをクリックして下さい。 秘密鍵の登録、更新するには、[パスフレーズ]を入力してからファイルを選択して[アップロード]ボタンをクリックして下さい。 証明書がPKCS12形式の場合は、[パスフレーズ]を入力して下さい。必要なCA証明書、中間CA証明書、サーバ証明書、サーバ秘密 証明書を削除する場合は、[Webサーバ証明書を削除]または[認証サーバ証明書を削除]ボタンをクリックして下さい。				
) I	凡仍 項目]:] 「設定〉	斉」の「済」は [.]	すでに設定されています。「未作	作業」は設定されていません。
ľ	Wel	サーバ	TAL	右効期限	t쿄/F
	1	未作業	中間CA証明書	XMISKIN ET	
	2	B	サーバ証明書	2020年7月18日 19時20分45秒	参照 アップロード PKCS12形式の場合パスフレーズ:
	3	B	サーバ秘密鍵	-	参照 アップロード パスフレーズ :
[
1	忍言	Eサーバ			
	#	設定済	項目	有効期限	操作
	1	B	CA証明書	2030年1月7日 0時46分45秒	参照 アップロード PKCS12形式の場合パスフレーズ:

次に、[CA運用管理]>[クライアント証明書管理]と進み、[クライアント証明書登録 用(EAP-TLS利用時)]のCA証明書にもルート証明書をアップロードします。

פי	ライアント証明書管理						
登録済クライアント証明書一覧(EAP-TLS利用時) 登録済のクライアント証明書を証明するCA証明書、または中間証明書の一覧です。 削除したい場合は、チェックを入れて[削除]ボタンをクリックして下さい。							
削	除		CA証明書	有効期限	種別	CRL	デルタCRL
] CN=	JCCH-SSS de	mo CA, DC=COM, DC=JCCH-SSS	2030年1月7日 0時46分45秒	ルートCA証明書	-	-
 ・ワライアント証明書登録用(EAP-TLS利用時) クライアント証明書を証明するCA証明書を登録、更新するには、お使いのコンピュータのファイルを選択して[アップロード], 証明書がPKCS12形式の場合は、[パスフレーズ]を入力して下さい。PKCS12中の必要なCA証明書、中間CA証明書を分離し登録 へ例: 項目「設定済」の「済」はすでに設定されています。「未作業」は設定されていません。「△」は任意作業です。							
#	設定済	項目	採	۴F			
1	B	CA証明書	PKCS12形式の場合パスフレーズ	参照 アップロート :	8/		
2	Δ	CRL	「CRL定期取得」から登録してく	ださい。			
З	Δ	デルタCRL	「CRI 定期取得」から登録してく	ださい。			

[CA運用管理] > [CRL定期取得]と進み、以下の設定をおこないます。

- [CRL定期取得を利用する。]にチェック
- [CRL定期取得URL]には、GléasのCRL公開URLを入力 ※デフォルトCAのCRL公開URLは以下の通りです http://hostname.example.com/crl/ia1.crl
- CRLを取得する間隔、回数、リトライ待ち時間、Proxyについては、環境に応じ て設定

設定後、[登録]ボタンをクリックし設定を保存します。

CPI 京期而得			
CKLLE规模			
CRL定期取得			
CRLの定期取得を設定します。元になるCA発行者を	[選択]ボタンをクリックして下さい。		
CA証明書(Subject)	DC=COM, DC=JCCH-SSS		
選択			
上部の選択したCA証明書のCRL情報を指定して[登録 ☑ CRL定期取得を利用する。	りボタンをクリックして下さい。		
CRL定期取得 URL http://gleas.example.com/crl/i	a1.crl ×		
□ デルタCRL定期取得を利用する。 例えば、1週間単位で日曜日に全CRL、月火水木金土にデルタCRLが発行される場合、周期は7となり 現在の回数は0の時:全CRLの取得、1=月,2=火,3=水,4=木,5=金,6=土の時:デルタCRLの取得となりま			
デルタCRL定期取得 URL			
周期(回数) 7			
現在回数 0			
CRLを取得する間隔、回数、リトライ待ち時間、Prc	xyを指定して下さい。		
取得の実行する時刻(0~23時 0~59分)	0 🗸 時0 🗸 分		
取得間隔	1 🗸 時間		
取得失敗時のリトライ回数	なし 🗸		
取得失敗時のリトライ待ち時間	60 🗸 秒		
Proxyを使う場合(例 http://サーバ名:ポート番号			
登録 リセット			

その後、[CRL取得 手動実行]をクリックするとCRL取得のテスト実行をします。 成功すると、以下のように表示されます。

CRL定期取得				
登録成功				
クライアント用 CRLを設定しました。				

2.4. ユーザの作成

Enterprasの管理画面で[ユーザ設定] > [ユーザ管理]と進み、新規ユーザの追加をします。

- [ログイン名]は、Gléasのアカウント名と同じにします
- [パスワード]は、EAP-TLSでは利用しませんがEnterprasの仕様上必須項目なので任意のパスワードを入力します
- [EAP方式]では、EAP-TLSのみ選択します(他のEAP認証方式を不可にします)
- 他の部分は必要に応じ設定

ユーザ登録/変更/削除

<u>ユーザ管理画面に戻る</u>

ユーザの登録/変更/削除を行います。 __ユーザ情報

ユーザを新規作成するには、上書きチェックボックスのチェックを外してから ユーザを変更するには、ユーザ情報を修正し[登録]ボタンをクリックして下さ ユーザを削除するには、[削除]ボタンをクリックして下さい。

ログイン名	testuser01		
パスワード	P@ssw0rd		
パスワード有効期限	有効期限:制限なし [<u>注意]</u> 所属ユーザグループを変更すると、		
	当該ユーザグルーブの有効期限が設定されます。		
所属ユーザグループ	DEFAULT - DEFAULTグループ 🗸		
認証方式	通常 🗸		
EAP方式	 □ EAP-TTLS □ EAP-PEAP ☑ EAP-TLS □ EAP-MD5 		
ログイン不可	□ログイン不可		
同時ログイン数	制限なし ~		
パスワードミスロック	現在の状態:ロックされていません		
認証期間設定	□ 認証期間の設定を行う		
認証開始日時	2017 🗸 年6 🖌 月29 🖌 日17 🗸 時		
認証終了日時	2017 🗸 年6 🖌 月29 🖌 日17 🗸 時		
氏名			
備考			

設定完了後、[登録]をクリックし保存します。

以上で、Enterprasの設定は終了です。

3. Gléasの管理者設定 (PC)

GléasのUA(申込局)より発行済み証明書を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、PC用となるUA(申込局)をクリックします。

UA 申込			
▶ <u>G</u>	eas Generic UA	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]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ボート	証明書ストアの種類 ユーザストフ	7 💌
□ 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

無線LAN の基本設定	
✔ WiFiブ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。



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]			■ ログアウト
ユーザ情報			
🗕 テスト ユーザ 01 さんのページ	_	_	D <u>ヘルブ</u>
▶ ユーザ情報 · · · · · · · · · · · · · · · · · · ·			\sim
▶ユーザ 登録日時:2011/02/2	8 09:13		
 > 姓:テスト 名:ユーザ01 > ユーザID:testuser01 > メールアドレス: > パスワード:************************************			
秦 証明書情報 · · · · · · · · · · · · · · · · · · ·			
▶ 発行済み証明書	: .		
#	#11256	有 幼期限 2019/10/18	証明書のインボート
			~
Infomation	×	Web ページからのメ	vセ-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。	<u>!</u> ユーザの	証明書ストアヘインポートしました。
0	К		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]				<u> ブアウト</u>
ユーザ情報		_			
גד 🙎	トユーザ 01 さんのページ			D <u>^</u>	ルプ
2 ⊐-t	だ情報 ・・・・・				^
▶ ユーザ	登録日時:2011/02/28 09	013			
> 姓: テフ > ユーザII > メールア > パスワー * 証明書	スト 名:ユーザ01 D:testuser01 ドレス: -F:***********************************				
▶ 発行済。	み証明書				
# <u>?</u> 1	発行局 JCCH-SSS demo CA	シリアル #11256	有効期限 2019/10/18	証明書ストアヘインボート ダウンロード済み	
					\rightarrow

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WiFi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 WiFi 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。

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]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
□ トークンへのインポート
🗖 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 用レイアウトを使用 ■ Mac OS X 10.7以降の接続	する 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	T
iPhone 構成ブロファイル基本	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.demo-mdm	n
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
記印	テスト用の構成プロファイル	,
削除パスワード		

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

114	無線LAN(802.1x)の設定	
	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。



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

テスト ユーザ01 さんのページ] に								
ユーザ情報	2.一ザ情報							
8 FZF	・ユーザ01 さんのページ			▶ <u>ヘルプ</u>				
2 ユーザ	情報							
▶ユーザ	登録日時:	2011/02/28 09:13						
> 姓 : テスト	ト 名:ユーザ01							
> ユーザID > メール:	: testuser01							
	42.40							
末 証明書	情							
▶発行済み	▶ 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-SSS demo CA	#11256	2019/10/18	構成プロファイルのダウンロード				

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

キャンセル	警告	インストール
管理対象外ルート証明書		
証明書"JCCH-SSS demo できる証明書のリストに追 まで、この証明書はWebt	2 CA"をインストール 追加されます。"証明書 ナイト用には信頼され	すると、iPadにある信頼 信頼設定"で有効にする ません。

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。

WiFi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]			■ ログアウ		
ユーザ情報						
8 7 78	ユーザ01 さんのページ			▶ <u>ヘルプ</u>		
🖢 ユーザ情	∮報 · · · · · · · · · · · · · · · · · · ·					
▶ユーザ	登録日時 : 2011	/02/28 09:13				
≥ 姓 : テスト ≥ ユーザID : t ≥ メール :	> 姓: デスト 名: ユーザ01 > ユーザD: testuser01 > メール:					
★ 証明書情報						
▶ 死行済み証	明書 発行局	シリアル	有効期限	ダウンロード		
<u>*</u>	JCCH-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。



※端末識別情報:UDID、IMEI、ICCID、MACアドレス

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. 【シナリオ2】Enterprasの設定

2 項と同様の手順で、もう一台 Enterpras(RADIUS#2)を EAP-TLS 認証をおこな えるようにセットアップしておきます。

この際に、サーバ証明書やクライアント証明書を発行する CA はシナリオ1とは異 なるもの(CA#2)にしておきます。また、アクセスポイントに認証サーバとして RADIUS#2 を設定する必要はありません。

7.1. RADIUS プロキシの設定

新しく構築したEnterpras (RADIUS#2) に管理者ログインし、管理者メニューより [認証機器/グループ設定] > [認証機器管理]と進み、[新規作成]をクリックします。 以下の設定をおこないます。

- [認証機器のIPアドレス]は、RADIUSプロキシのIPアドレスを入力
- [共有鍵]は、RADIUSプロキシとの共有鍵(同じパスワード)を入力

認証機器登録/変更/削除							
認証機器の登録/変更/削除を行います。 認証機器情報							
認証機器を新規作成するには、[上書き]チェックボックスのチェックを外してから[登録]ボタンをクリックして下さい。 認証機器を変更するには、[上書き]チェックボックスをチェックして[登録]ボタンをクリックして下さい。 認証機器を削除するには、[削除]ボタンをクリックして下さい。							
認証機器のIPアドレス	192.168.]					
共有鍵	hogehoge]					
所属する認証機器グループ	GENERAL - GENERAL	~					
登録 削除 リセット							

RADIUSプロキシとなるEnterpras (RADIUS#1) に管理者ログインし、管理者画面

のメニューより、[Proxy設定] > [Proxy設定]と進み、以下の設定を行います。

- [Proxyの使用]は、「使用する」にチェック
- [レルムの大文字小文字]は、「無視する」を選択

Proxv彀定				
Proxyの動作設定を行ないます。各種設定値を設定して、[設定]ボタンをクリックして下さい。 [注意]設定後、認証サーバの再起動が必要です。				
Proxyの使用				
Proxyを使用するかしないかを選択します。 初期値:使用しない				
Proxyの使用 使用する。				
レルムの大文字小文字				
レルムの大文字小文字を無視するかどうかを指定します。 初期値:無視しない				
レルムの大文字小文字 無視する				
設定				

[設定]をクリックし保存し、その後[Proxy管理]メニューに進み [新規作成]をクリックし以下の設定をおこないます。

- [Proxy名]に、任意の名称を入力
- [レルム]に、任意の領域名を入力(WiFiログイン「ユーザID@…」のアットマー クの後ろの部分)
- [転送先の選択]には、[転送先認証サーバを指定する]を選択し、認証サーバ (RADIUS#2)のIPアドレスやポート、共有鍵を入力

Pr	Proxy 豆 録 / 役 史 / 削 际 Proxyの 登録 / 変更 / 削除を行ないます。							
2	[注意]設定後、認証サーバの再起動が必要です。 │ Proxy情報							
	Proxyを新規作成するには、上書きチェックボックスのチェックを外してから[登録]ボタンをクリックして下さい。 Proxyを変更するには、Proxy情報を修正し[登録]ボタンをクリックして下さい。 Proxyを削除するには、[削除]ボタンをクリックして下さい。							
	Proxy名	enterpras02						
	レルム	enterpras02						
		 ○ この認証サーバで ● 転送先認証サーバ 	認証する を指定する					
		転送先認証サーバ 1	IPアドレス: 192.168 共有鍵: hogehoge 認証ポート: 1812 アカウンティングポート: 1813					
	転送先の選択	転送先認証サーバ 2	IPアドレス: 共有鍵: 認証ポート: アカウンティングポート:					
		転送時レルムの処理	○ そのまま ● 削除する					
		タイムアウト秒数	3 🗸					
		リトライ回数	3 ~					
	□ 上書きする(注意:同じIPアドレスを指定すると共有鍵が上書きされます) 登録 削除							

設定後、「登録」をクリックし設定を保存します。[Proxy管理]画面で以下のように 表示されます。

	Pro	xy一覧	l					
	Proxyの変更を行うには、変更対象の[Proxy名]リンクをクリックして下さい。 Proxyを削除するには、削除対象のProxy名のチェックボックスをチェックし、[削除]ボタンをクリックして下さい ログイン名にレルム(@記号)が含まれない場合は、この認証サーバで認証します。							
	#	削除	Proxy名	レルム	転送先認証サーバ(IPアドレス)			
	1		enterpras02	@enterpras02	192.168.			
	2		<u>その他</u>	(@含むその他のレルム)	この認証サーバ			
削除 全削除チェック実行 リセット								

Proxy設定後は認証サーバの再起動が必要となるので、[再起動]をクリックします。



以上でEnterpras (RADIUS#2)の設定は終了です。

8. 【シナリオ2】Gléasの管理者設定

シナリオ1と同じですが、Gléasでのアカウントは"ユーザID@enterpras2(7.1項で設定 したレルム)"にします。

これによりRADIUS#2で認証されるようになります。

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。

■Enterprasに関するお問い合わせ先

株式会社ステラクラフト 企画営業部

Tel: 03-5289-3911

Mail: sales@stellar.co.jp

■Gléasや本検証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