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

～Enterpras～

RADIUSサーバ（802.1x EAP-TLS）認証連携設定

Ver. 1.0
2017 年 8 月

目次

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。

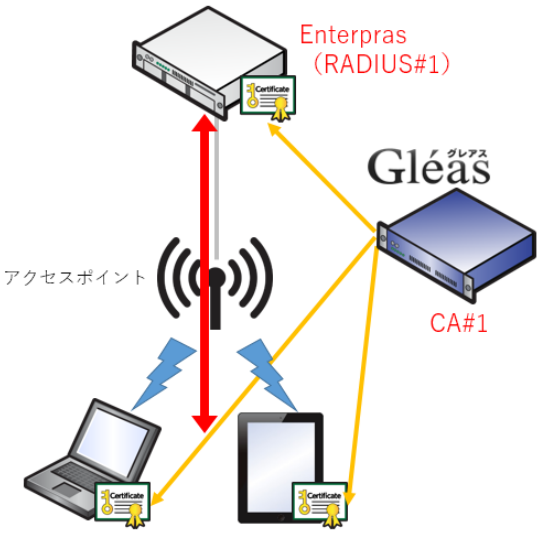
- Enterprasのインストールと基本的なRADIUS設定
- Gléasでのアカウント登録や各種証明書発行
- クライアントのセットアップ

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

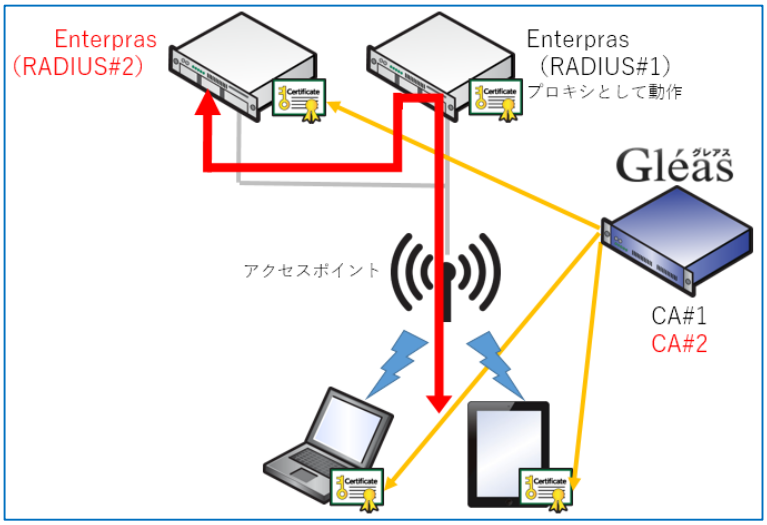
本書では、以下の構成で検証を行っています。

■シナリオ１



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）



1. 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。
2. 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

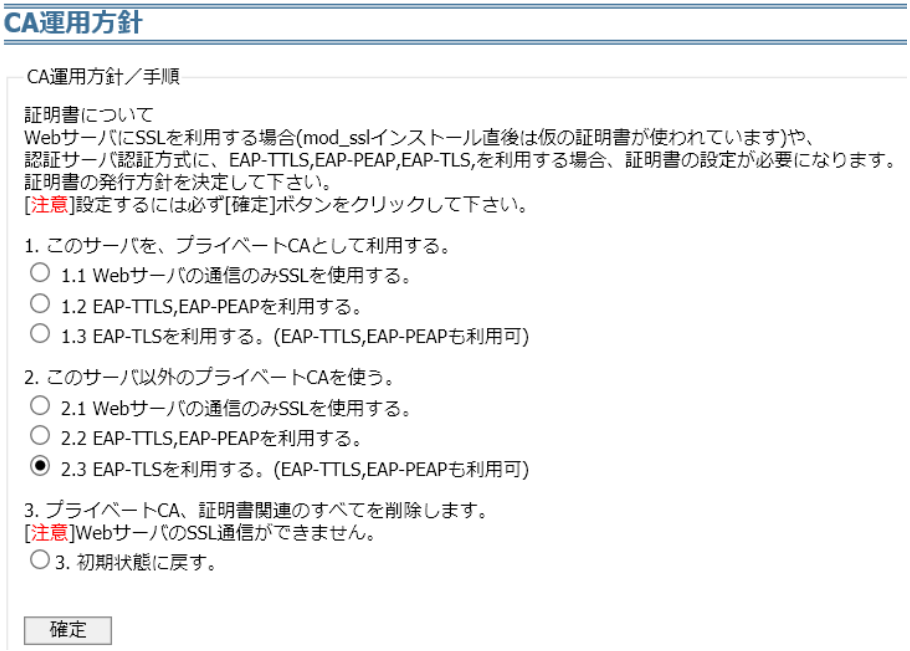
2. 【シナリオ１】Enterprasの設定

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



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)	Tokyo
市区町村(L)	Arakawa
会社名(O)	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

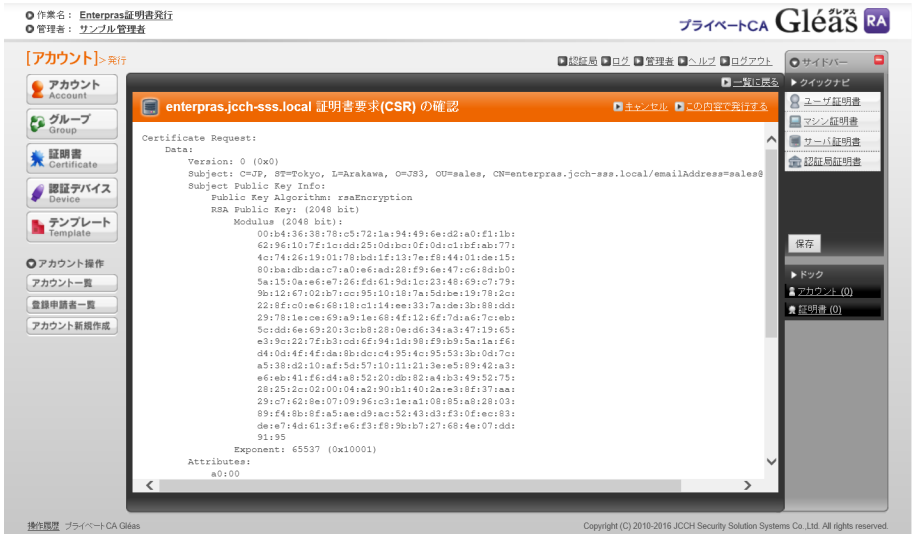
Gléas（RA）にログインし、該当のサーバアカウントのページへ移動します。
小メニューの[証明書発行]をクリックします。

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

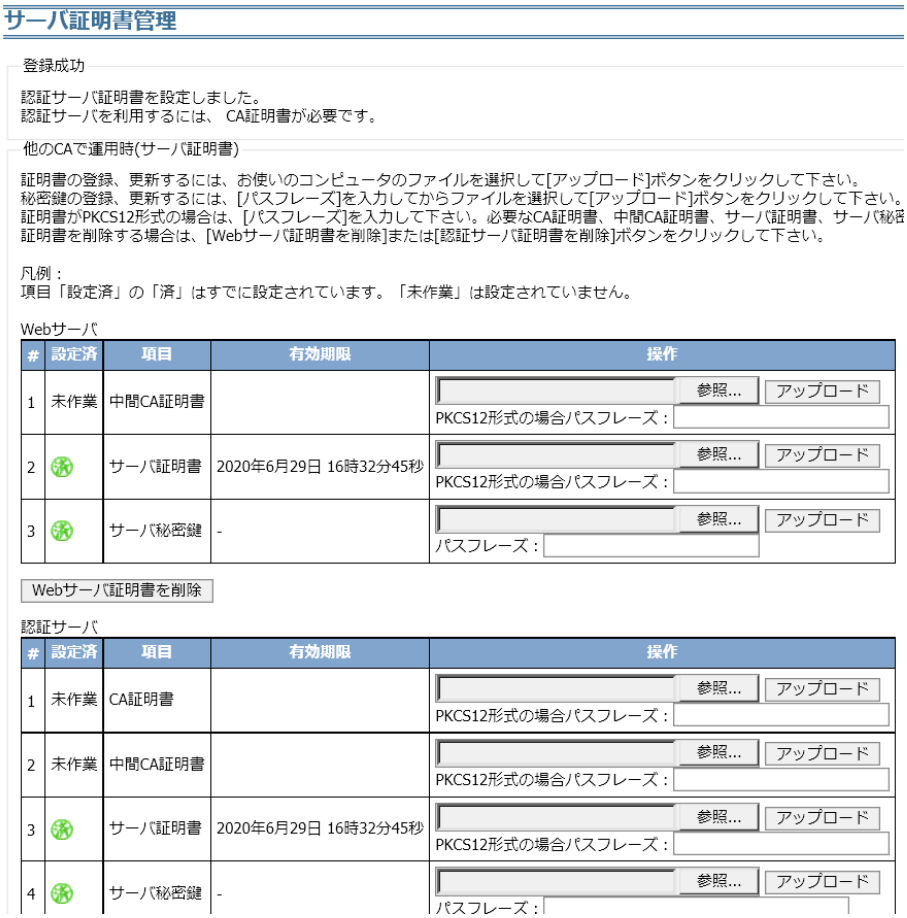
● [CSR ファイルの内容を確認する]にチェック
その後、[発行]ボタンをクリックします。

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。



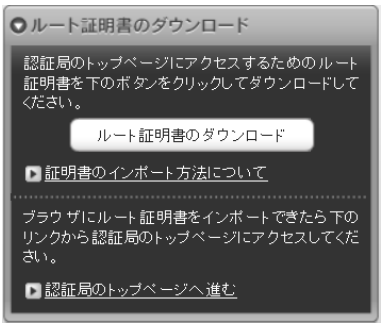
証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書：あり」を右クリックし、発行された証明書（download.crt）をダウンロードします。

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。

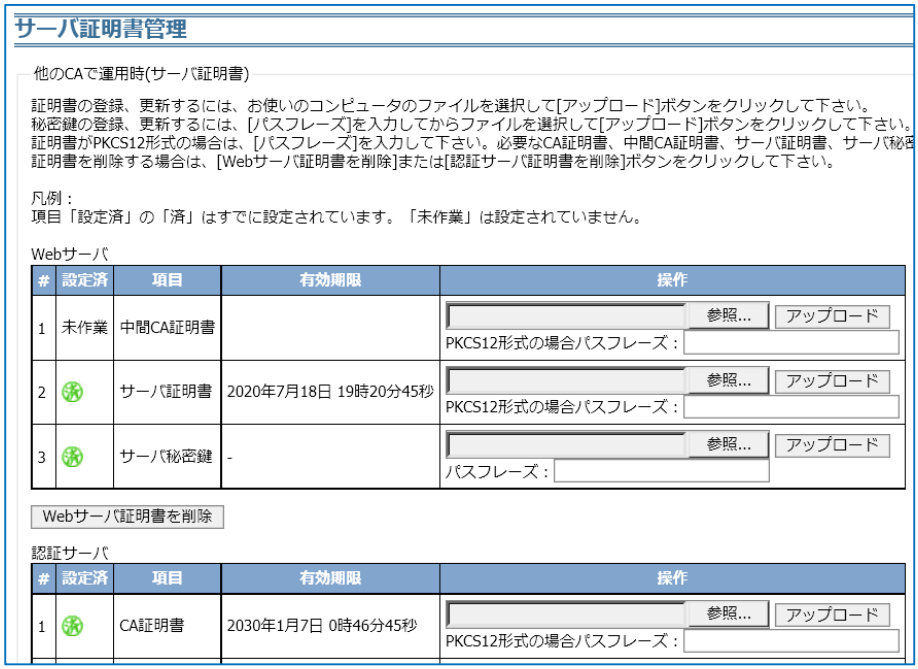


2.3. ルート証明書とクライアント証明書認証の設定

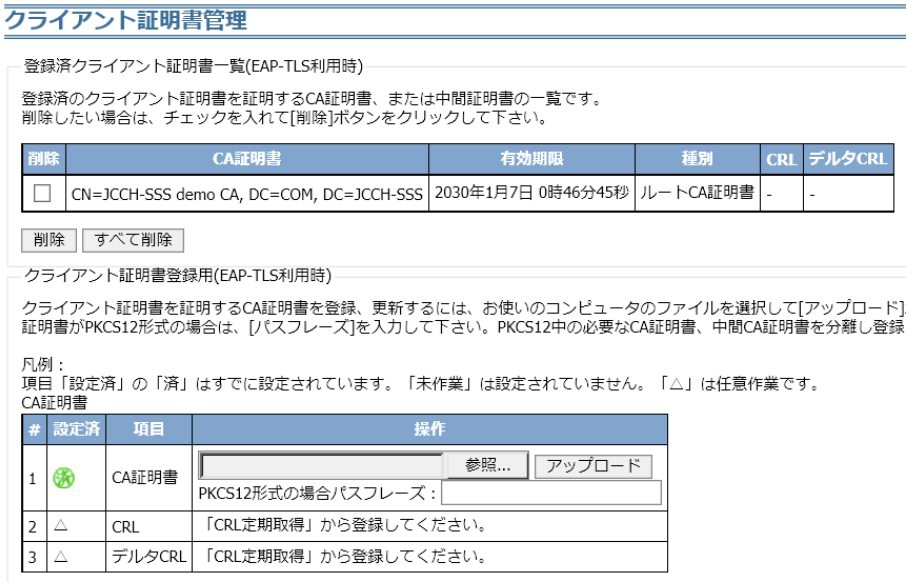
Gléasにhttpで接続するとルート証明書のダウンロードができるので、あらかじめダウンロードしておきます。



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。



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。



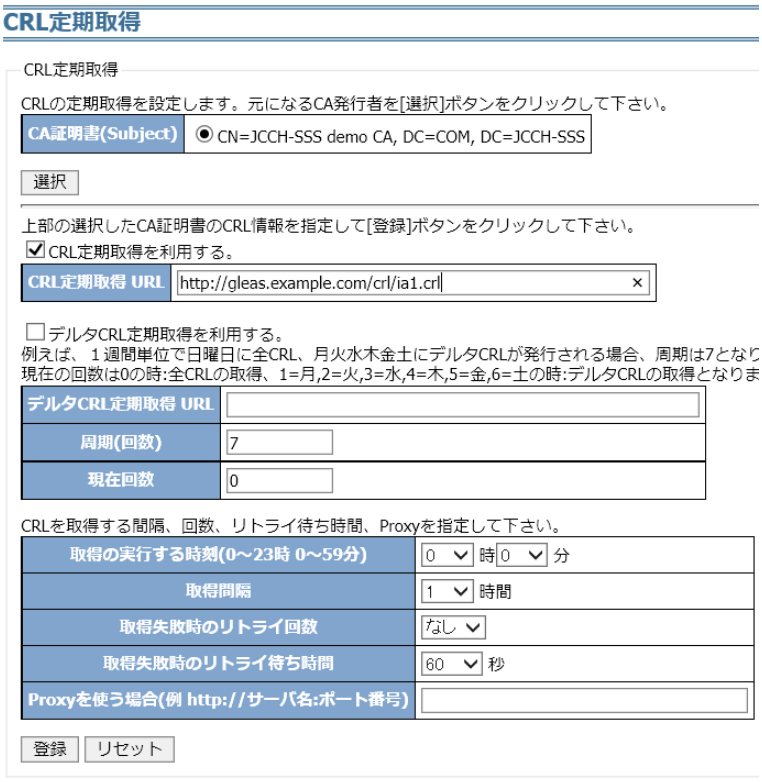
[CA運用管理] > [CRL定期取得]と進み、以下の設定をおこないます。

- [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。

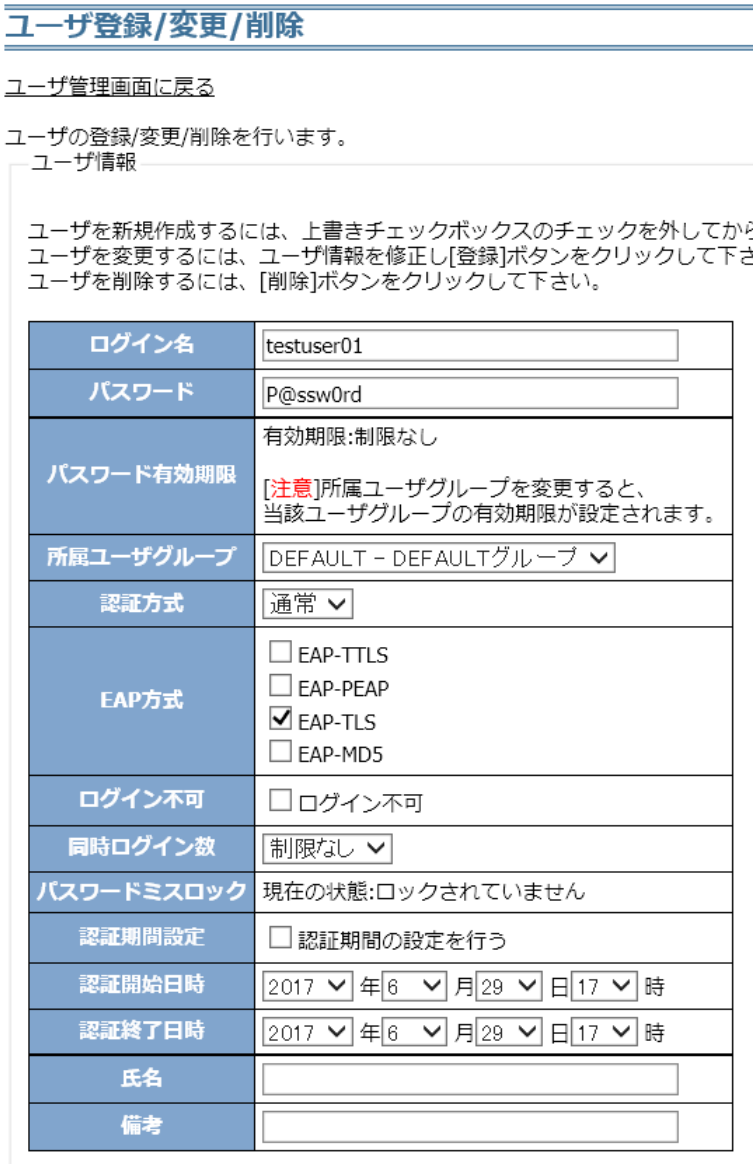


その後、[CRL取得　手動実行]をクリックするとCRL取得のテスト実行をします。
成功すると、以下のように表示されます。

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



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。

[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

[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

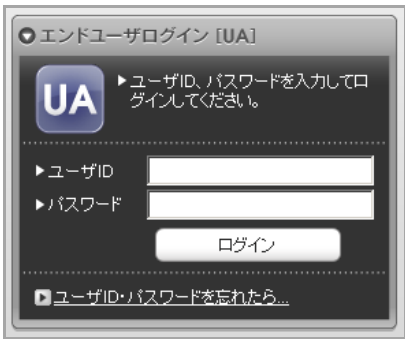
設定終了後、[保存]をクリックし設定を保存します。

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

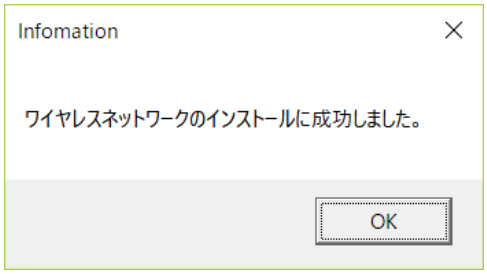
4.1. Gléas の UA からのインストール

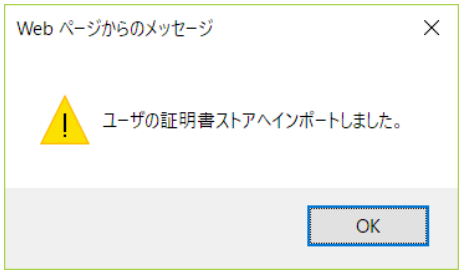
Internet ExplorerでGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、Gléasでのユーザ IDとパスワードを入力しログインします。



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。





「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。

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

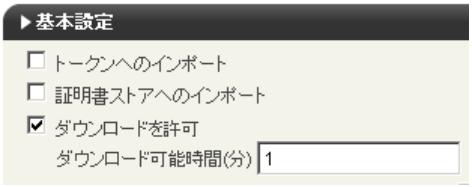
5.1. UA（ユーザ申込局）設定

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。

[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）

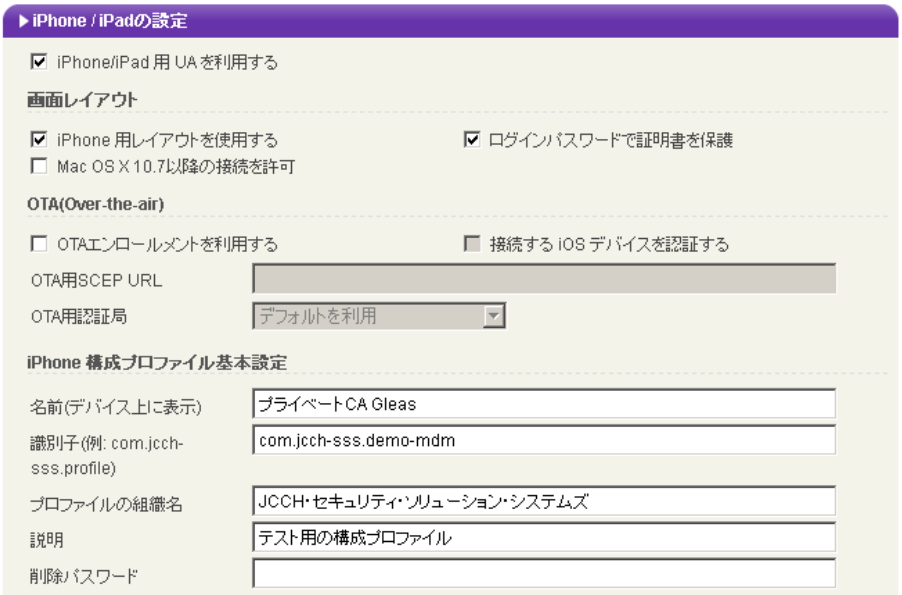
を経過した後に、構成プロファイルのダウンロードが不可能になります（「インポートロック」機能）。このインポートロックにより複数台のiPadへの構成プロファイルのインストールを制限することができます。



[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。

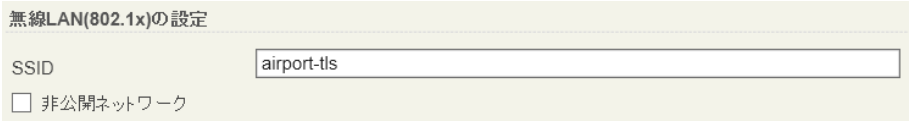
構成プロファイル生成に必要となる情報を入力する画面が展開されるので、以下設定を行います。

- [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）



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



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

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。

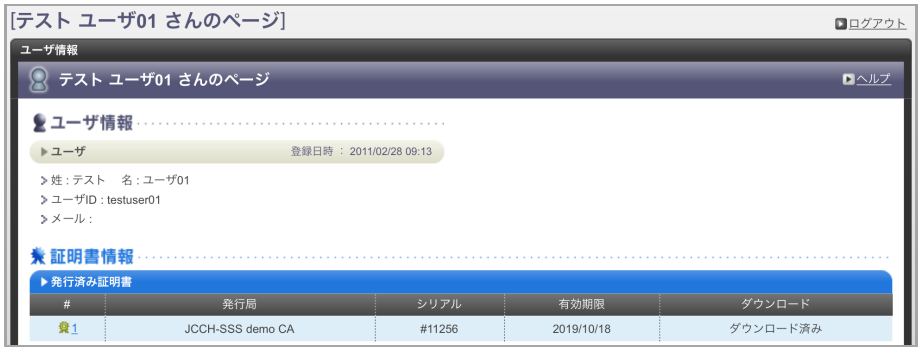
パスコードロックを有効にしている場合（或いは構成プロファイルでパスコードロックを強制する場合）はパスコードを入力します。
その後、以下のようなルート証明書追加の警告画面が現れますので、[インストール]をクリックして続行してください。
※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります

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。

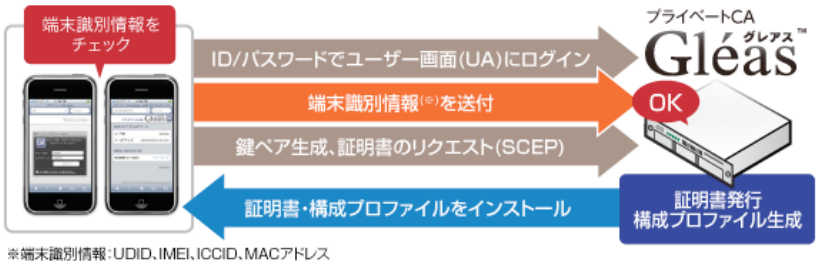
WiFiプロファイルとクライアント証明書がインポートされた端末では、SSIDを選択するだけで自動的にWiFi接続をすることが可能です。

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。



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。

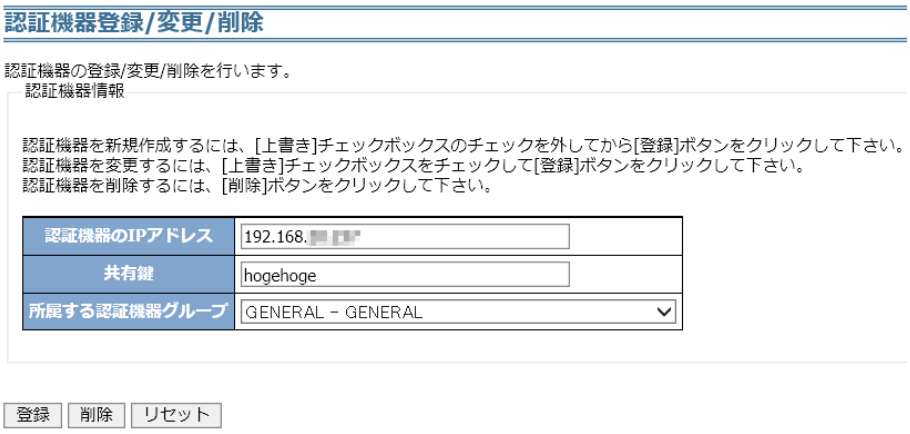
7. 【シナリオ２】Enterprasの設定

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



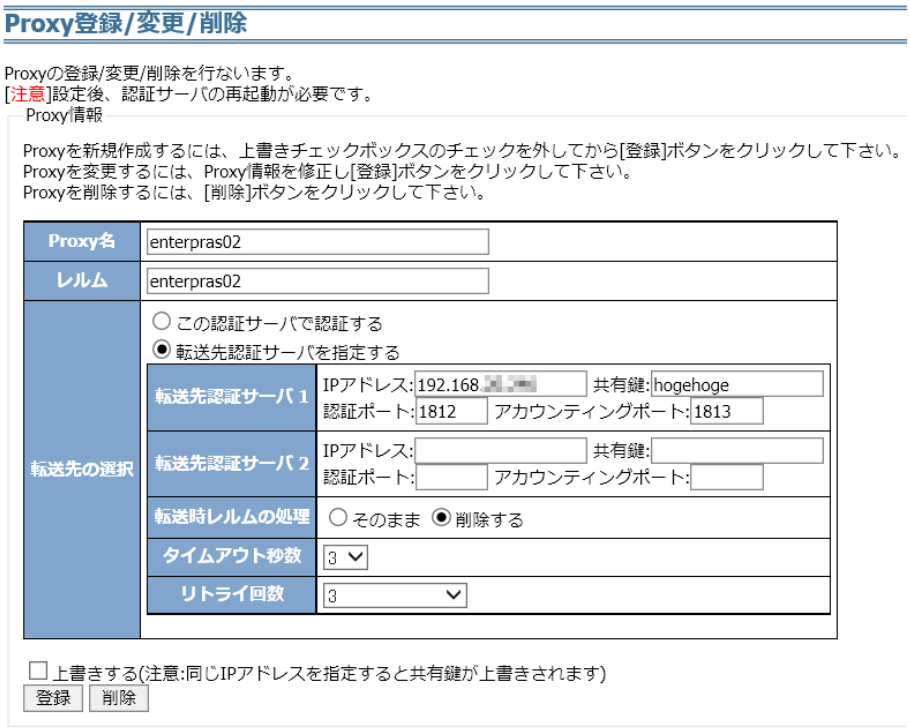
RADIUSプロキシとなるEnterpras（RADIUS#1）に管理者ログインし、管理者画面

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。

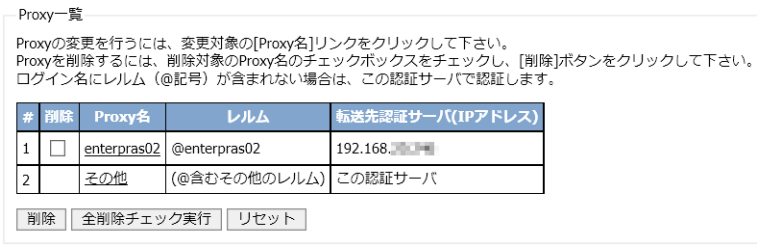
- [Proxyの使用]は、「使用する」にチェック
- [レルムの大文字小文字]は、「無視する」を選択

[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。

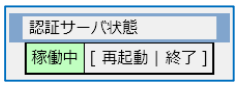
- [Proxy名]に、任意の名称を入力
- [レルム]に、任意の領域名を入力（WiFiログイン「ユーザID@...」のアットマークの後ろの部分）
- [転送先の選択]には、[転送先認証サーバを指定する]を選択し、認証サーバ（RADIUS#2）のIPアドレスやポート、共有鍵を入力



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。



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