



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CA Gléas ホワイトペーパー

～Cisco Secure ACS～

Cisco Secure ACS（802.1x EAP-TLS）連携設定手順

Ver.0.1

2011年9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。

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS (802.1x EAP-TLS) 連携設定手順

目次

1. はじめに.....	4
1.1. 本書について.....	4
1.2. 本書における環境.....	4
2. ACS の設定	5
2.1. デフォルトのネットワーク デバイス設定.....	5
2.2. CA 証明書の設定.....	6
2.3. 証明書認証プロファイルの設定.....	7
2.4. アクセスポリシーを設定.....	7
3. Gléas の管理者設定 (PC)	8
3.1. UA (ユーザ申込局) 設定	8
4. クライアント PC での証明書インポート・無線 LAN 設定	9
4.1. Gléas の UA からのインストール	9
4.2. 無線 LAN の設定 (Windows)	10
4.3. 【参考】グループポリシーを利用した設定.....	12
4.4. 【参考】コンピュータ証明書を利用した認証について.....	12
5. Gléas の管理者設定 (iPad)	13
5.1. UA (ユーザ申込局) 設定	13
6. iPad での構成プロファイル・証明書のインストール.....	14
6.1. Gléas の UA からのインストール	15
6.2. 無線 LAN の利用.....	17
7. Gléas の管理者設定 (Android)	18
7.1. UA (ユーザ申込局) 設定	18
8. Android での証明書のインストール・無線 LAN 設定	19
8.1. Gléas の UA からのインストール	19
8.2. 無線 LAN の設定 (Android)	23
9. 問い合わせ	25

1. はじめに

1.1. 本書について

本書では、プライベートCA Gléasで発行したクライアント証明書を利用してCisco Secure ACSを用いて無線LAN認証（802.1x EAP-TLS）を行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、9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。

- Cisco Secure ACS（バージョン5.1.0.44）
※以後、「ACS」と記載します
- JS3 プライベートCA Gléas（バージョン1.7）
※以後、「Gléas」と記載します
- Cisco Aironet 1140 Series Access Point（バージョン12.4(25d)JA）
※以後、「アクセスポイント」と記載します
※本書では、無線LANアクセスポイントが802.1xにおけるオーセンティケータとなります
- Microsoft Windows7 Ultimate SP1
※以後、「Windows」と記載します
※802.1xにおけるサブリカントは、Windows標準のものを利用します
- Apple iPad（iOS 4.3.5）
※以後、「iPad」と記載します
- HTC Aria（イー・モバイル S31HT、Android 2.2.1）
※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。

- ACSの基本的なセットアップ方法

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS (802.1x EAP-TLS) 連携設定手順

- アクセスポイントのセットアップ方法
- 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方法
- WindowsやiPad、Androidのネットワーク設定等の基本設定

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。

2. ACSの設定

2.1. デフォルトのネットワーク デバイス設定

Network Resources → Default Network Device において、デフォルトのネットワーク デバイス設定を実施します。

ACS はネットワーク デバイス リポジトリを検索して、その要求で示されている IP アドレスと一致する IP アドレスを持つネットワーク デバイスを見つけます。この検索で一致するアドレスが見つからなかった場合、ACS では、RADIUS 要求または TACACS+ 要求に対して、デフォルトのネットワーク デバイス定義を使用します。

- Default Network Device Status を Enabled に変更
- RADIUS にチェックを入れる
- Shared Secret に共通キーを入力

Network Resources > Default Network Device

Default Network Device
The default device definition can optionally be used in cases where no specific device definition is found that matches a device IP address.

Default Network Device Status:

Network Device Groups

Location:

Device Type:

Authentication Options

▼ TACACS+

Shared Secret:

Single Connect Device

Legacy TACACS+ Single Connect Support

TACACS+ Draft Compliant Single Connect Support

▼ RADIUS

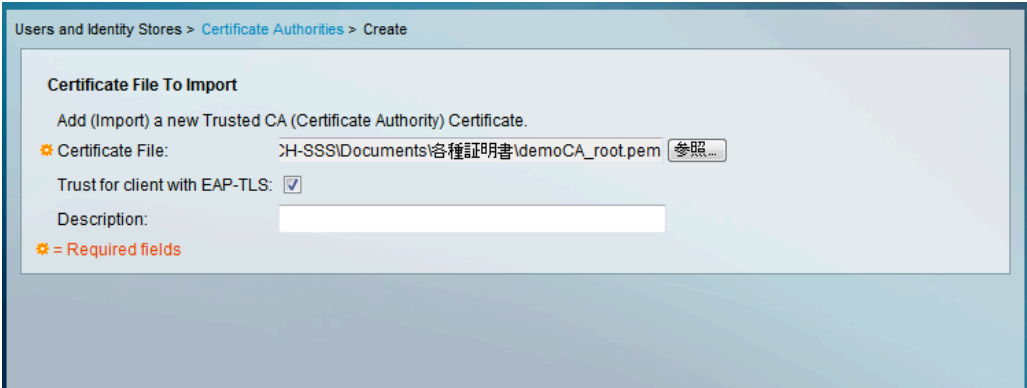
Shared Secret:

= 必須フィールド

2.2. CA 証明書の設定

Users and Identity Stores → Certificate Authorities の順にクリックして、「Add」ボタンをクリックして、以下の通り設定します。

- Certificate FileにCA証明書のファイルパスを指定する
- Trust for client with EAP-TLSのチェックを有効にする



Submitボタンをクリックすると、Certificate Authoritiesに追加されるので、Friendly Nameカラムの名前をクリックすると編集画面が表示されます。

証明書失効リスト（CRL）を利用する場合は、以下の設定を実施します。

項目	説明
Download CRL	CRLをダウンロードする場合に、このボックスをオンにします。
CRL Distribution URL	CRL配布URLを入力します。HTTPを使用するURLを指定できません。
Retrieve CRL	ACSは最初にCAからCRLをダウンロードしようとします。ACSがCAから新しいCRLを取得する時間設定を切り替えます。 <ul style="list-style-type: none">● Automatically：CRLファイルのNextUpdateを使用します。取得に失敗した場合、ACSは最初の失敗から定期的に、成功するまでCRLの取得を試みます。● Every：取得試行の頻度を指定します。時間間隔を入力します。
If Download Failed Wait	CRLの取得が失敗した場合に、次に取得を試行する時間を入力します。

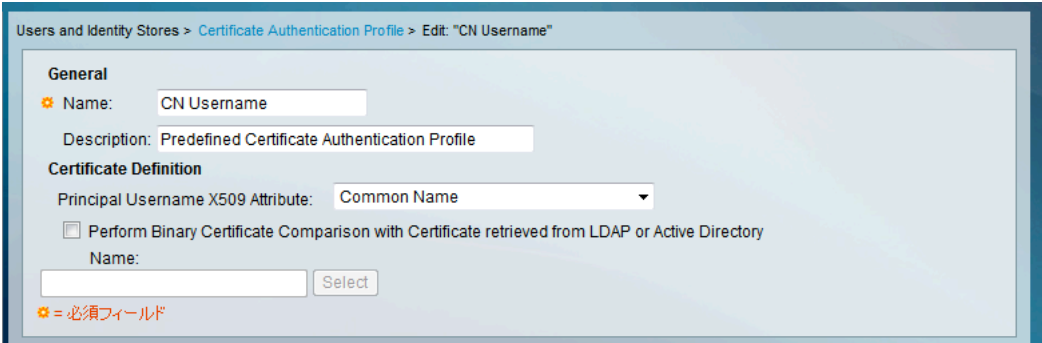
プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS（802.1x EAP-TLS）連携設定手順

Bypass CRL Verification if CRL is not Received	オフの場合、選択したCAによって署名された証明書を使用するすべてのクライアント要求は、ACSによってCRLが受信されるまで拒否されます。オンの場合、クライアント要求はCRLが受信される前に受け入れられます。
Ignore CRL Expiration	期限切れのCRLに対して証明書をチェックする場合に、このボックスをオンにします。オンの場合、ACSは期限切れのCRLを使用し続け、CRLの内容に従ってEAP-TLS認証を許可または拒否します。オフの場合、ACSは、CRLファイルのNext Update フィールドでCRLの有効期限を調べます。CRLが期限切れの場合、選択したCAによって署名された証明書を使用するすべての認証は拒否されます。

2.3. 証明書認証プロファイルの設定

Users and Identity Stores → Certificate Authentication Profileにて、X.509認証に使用するプリンシパルユーザ名のアトリビュートを設定します。

ここでは、デフォルト設定されているCommon Nameを使用します。

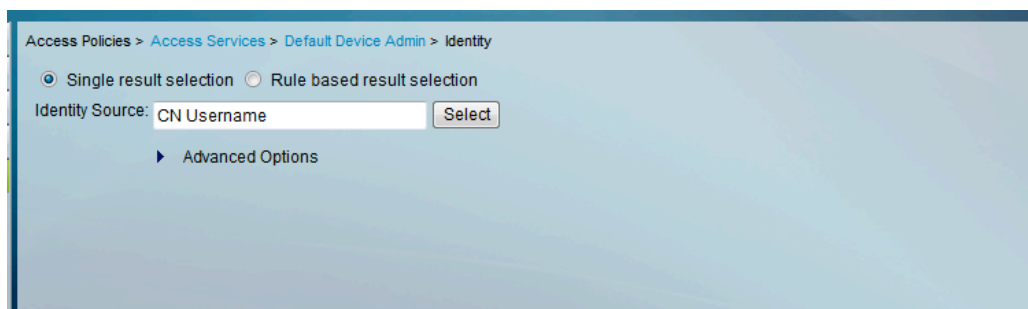


The screenshot shows the configuration page for a Certificate Authentication Profile. The breadcrumb is "Users and Identity Stores > Certificate Authentication Profile > Edit: 'CN Username'". Under the "General" section, the "Name" is "CN Username" and the "Description" is "Predefined Certificate Authentication Profile". Under the "Certificate Definition" section, the "Principal Username X509 Attribute" is set to "Common Name". There is a checkbox for "Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory" which is unchecked. Below it is a "Name:" field with a "Select" button. A legend at the bottom left indicates that a star icon (*) denotes a required field.

2.4. アクセスポリシーを設定

Access Policies → Access Services → Default Device Admin → Identity の Identity Source を「2.3 証明書認証プロファイルの設定」で確認した 「CN Username」に変更する。

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS（802.1x EAP-TLS）連携設定手順



以上で、ACS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クライアントPCにインポートできるように設定します。

※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。



上記の場合は、Gléasデフォルト申込局と記載のあるものをクリックします。

[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。

- [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



設定終了後、[保存]をクリックし設定を保存します。

各項目の入力が終わったら、[保存]をクリックします。

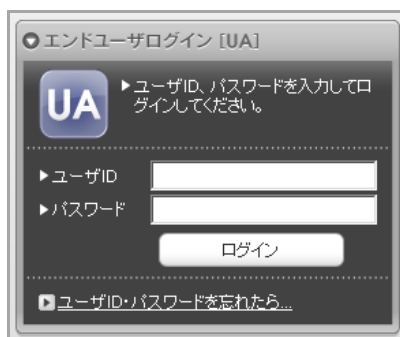
以上でGléasの設定は終了です。

4. クライアント 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、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てください。（インストールに必要な権限を持っている必要があります）

その後、[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。

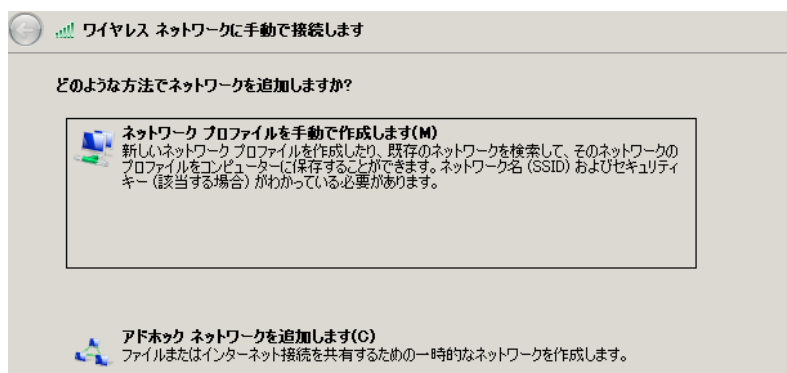
プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS (802.1x EAP-TLS) 連携設定手順



※「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

4.2. 無線 LAN の設定 (Windows)

[コントロール パネル]>[ネットワークとインターネット]>[ワイヤレス ネットワークの管理]を開き、[追加]をクリックします。
以下のウィザードが起動しますので、[ネットワークプロファイルを手動で作成します(M)]をクリックします。



無線LANの各種設定 (ESSID、認証方法、暗号化アルゴリズム等) を入力します。
なお、[セキュリティの種類(S)] (認証方法) は、[WPA - エンタープライズ]か[WPA2 - エンタープライズ]のどちらかに必ずなります。

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS (802.1x EAP-TLS) 連携設定手順

以下の画面では、[接続の設定を変更します(H)]をクリックします。

[ワイヤレスネットワークのプロパティ]ウィンドウが開きます。

[ネットワークの認証方法の選択(O)]で[Microsoft: スマートカードまたはその他の証明書]を選択し、[設定]をクリックします。

[スマートカードまたはその他の証明書のプロパティ]ウィンドウが開きます。

[接続のための認証方法]で[このコンピューターの証明書を使う(C)]を選択します。

※本書では触れておりませんが、クライアント証明書をICカードやUSBトークンに格納した場合は、[自分のスマートカードを使う(S)]を選択することで、認証に利用することが可能となります

認証サーバが正当なものであるかをクライアントで検証する場合は、[サーバーの証

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS（802.1x EAP-TLS）連携設定手順

明書を検証する(V)]にチェックを入れ、以下の項目を設定します。

- [次のサーバーに接続する]にチェックを入れ、RADIUSのホスト名を入力
※サーバ証明書はここで入力されるホスト名に対して発行されたものである必要があります。（入力されたホスト名とサーバ証明書の記述が異なるとなる場合、無線LAN接続時に警告が出現します）
- [信頼されたルート証明書]ではこのサーバ証明書のトラストアンカとなるルート証明書をチェック
（サーバ証明書にGléasの発行したものを利用する場合は、Gléasのルート証明書をチェック）



[OK]をクリックし、すべてのウィンドウをクローズします。

以上でEAP-TLSによる無線LAN接続が可能な状態となりますので、クライアント証明書によるセキュアな接続をお試しください。

4.3. 【参考】 グループポリシーを利用した設定

4.2項での設定は、Windowsドメイン環境ではグループポリシーで一括設定することも可能です。本書では割愛しますが、以下のポリシーを利用します（Windows Server 2008 R2の場合）。

[コンピュータの構成] > [ポリシー] > [Windowsの設定] > [セキュリティの設定] > [ワイヤレスネットワーク(IEEE802.11)ポリシー]

4.4. 【参考】 コンピュータ証明書を利用した認証について

Windowsでは「コンピュータ証明書」を利用して、ユーザがWindowsにログオンしていない状態で無線LAN接続を確立することが可能です。

詳細は9項に記載されている弊社お問合せ先までお問合せください

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、iPad用となるUA (申込局) をクリックします。

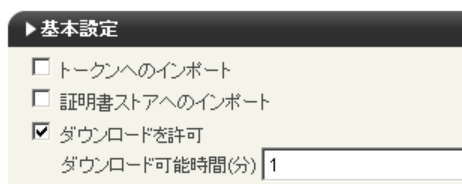


上記の場合は、iPad用UAと記載のあるものをクリックします。

[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な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]にチェックが入っていないことを確認
- iPhone OS 3を利用しているユーザがいる場合は[ログインパスワードで証明書

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS (802.1x EAP-TLS) 連携設定手順

を保護]をチェック

iPhone OS 3では構成プロファイルのインストール時に証明書のインポート用パスワードを求められますが、ここをチェックすることにより、UAへのログインパスワードを利用できます。

- [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、iPad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（iPad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）

認証デバイス情報

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する ログインパスワードで証明書を保護

iPhone 構成プロファイル基本設定

名前(デバイス上に表示)	JS3 Profile
識別子(例: com.jcch-sss.profile)	com.jcch-sss.profile
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
説明	JS3
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には無線LANアクセスポイントのSSIDを入力

無線LAN(802.1x)の設定

SSID eap-tls-a

非公開ネットワーク

※ SSIDをブロードキャストしていない場合は、[非公開ネットワーク]をチェックします。

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

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS (802.1x EAP-TLS) 連携設定手順

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



ダウンロードが終了すると、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。

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～

Cisco ACS (802.1x EAP-TLS) 連携設定手順



インストール途中に、以下のようなルート証明書のインストール確認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。

※iPhone OS 3の場合は、この前にクライアント証明書の保護パスワードを要求される画面が出現するので、UAログインに利用したパスワードを入力してください



インストール完了画面になりますので、[完了]をタップしてください。

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～

Cisco ACS (802.1x EAP-TLS) 連携設定手順



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。

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. 無線 LAN の利用

インストールした構成プロファイルにより、アクセスポイントの設定や、EAP-TLS 認証に利用するクライアント証明書は既にiPadにインストールされているので、接続したいワイヤレスネットワークを選択する等で、クライアント証明書によるセキ

ユーアな接続をお試しください。

7. Gléasの管理者設定 (Android)

Gléas で、発行済みのクライアント証明書を Android 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

7.1. 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、Android用となるUA (申込局) をクリックします。

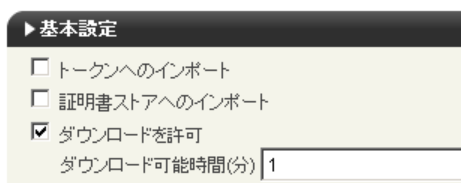


上記の場合は、Android用UAと記載のあるものをクリックします。

[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Android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。

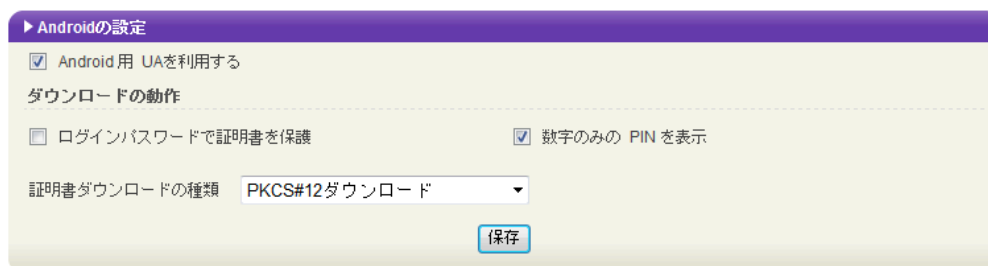


[認証デバイス情報]の[Androidの設定]までスクロールし、[Android 用 UAを利用する]をチェックします。

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS（802.1x EAP-TLS）連携設定手順

Android用の設定を入力する画面が展開されるので、以下設定を行います。

- [ログインパスワードで証明書を保護]にチェックを入れると、証明書をAndroidにインポートする際に入力するパスフレーズをUAへログインする際のパスワードと同一にします。チェックを入れないと、UA画面上にパスフレーズが表示されます。本書では、
- [数字のみの PIN を表示]にチェックを入れると、UA画面上に表示するパスフレーズが数字のみになります。
- [証明書ダウンロードの種類]では、PKCS#12ダウンロードを選択してください。



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。

8. Android での証明書のインストール・無線 LAN 設定

AndroidからGléasのUAに接続し、発行済みのクライアント証明書のインポートを行います。クライアント証明書のインポート後、Android端末の無線LAN設定を行います。

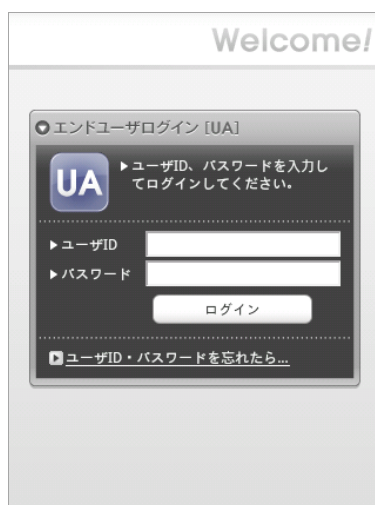
※本ケースではUAに接続するためのネットワーク接続が必要となります（3G回線や、証明書認証を必要としない無線LAN接続等）

8.1. Gléas の UA からのインストール

Androidの標準ブラウザで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。

プライベート CA Gleás ホワイトペーパー
～Cisco ACS～
Cisco ACS (802.1x EAP-TLS) 連携設定手順



ログインすると、ユーザ専用ページが表示されるので、[ダウンロード]をタップします。



画面に証明書のPINが表示されるので、[決定]をタップします。

プライベート CA Gleás ホワイトペーパー
～Cisco ACS～
Cisco ACS (802.1x EAP-TLS) 連携設定手順

[PKCS12キーストアから抽出]と表示されるので、先の画面に表示されたPINを入力します。

[証明書の名前を指定する]と表示されるので、任意の名前を指定します。

プライベート CA Gleas ホワイトペーパー
～Cisco ACS～
Cisco ACS（802.1x EAP-TLS）連携設定手順



初めて「認証情報ストレージ」（Androidのキーストア）にアクセスする場合は、認証情報ストレージをアクティベートするパスワードの設定を求められますので、画面の説明に従いパスワードを設定します。

※ここで設定するパスワードはAndroid起動後、認証情報ストレージへの初回アクセス時に入力を求められます



証明書の認証情報ストレージへのインポートが行われます。

プライベート CA Gleás ホワイトペーパー
～Cisco ACS～
Cisco ACS（802.1x EAP-TLS）連携設定手順



終了後、[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、Androidでの証明書インポートは終了です。

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」という表示に変わり、以後のダウンロードは一切不可能となります。



8.2. 無線 LAN の設定（Android）

Androidのホーム画面で[設定]>[無線とネットワーク]>[Wi-Fi]をタップし、無線LANをオンにします。その後、[Wi-Fi設定]をタップし、接続するアクセスポイント（SSID名）をタップし、以下の設定を行います。

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS（802.1x EAP-TLS）連携設定手順

- [EAP方式]には、[TLS]を設定
- [CA証明書]には、3.1でインポートしたルート証明書を選択
- [クライアント証明書]には、3.1でインポートしたクライアント証明書を選択
- [ID]には、RADIUSサーバに登録したユーザIDを入力。本書の設定では入力の必要はありません。
- [パスワード]には、RADIUSサーバに登録したパスワードを入力。本書の設定では入力の必要はありません。



※[Wi-Fi設定]画面にてSSID名の下に表示されているセキュリティの種類が「802.1x EAP で保護」となっていないと、上記EAP-TLSの設定が表示されません。「802.1x EAPで保護」となっていない場合は、アクセスポイントの設定をご確認ください。

以上で、設定は終了です。

正常に設定が行われている場合、無線LANに接続されます。

プライベート CA Gléas ホワイトペーパー
～Cisco ACS～
Cisco ACS（802.1x EAP-TLS）連携設定手順



9. お問い合わせ

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。

■ACSに関するお問い合わせ

■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

Tel: 050-3821-2195

Mail: sales@jcch-sss.com