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

～Windows Server（ネットワークポリシーサーバー）～

## スマートデバイスでの802.1x EAP-TLS設定手順

**Ver.1.0**

**2012 年 8 月**

**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
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 ..... 5
2. ドメインコントローラでの設定 ..... 6
2.1. ルート証明書の NTauth ストアへのインポート ..... 6
2.2. グループポリシーの設定 ..... 7
2.3. Active Directory でのアカウント設定 ..... 7
3. NPS サーバでの設定 ..... 8
3.1. サーバ証明書のインポート ..... 8
3.2. NPS の Active Directory との連携 ..... 10
3.3. RADIUS クライアントの設定 ..... 11
3.4. 認証ポリシの設定 ..... 11
4. Gléas の管理者設定（iPad） ..... 14
4.1. UA（ユーザ申込局）設定 ..... 14
5. iPad での構成プロファイル・証明書のインストール ..... 16
5.1. Gléas の UA からのインストール ..... 16
5.2. OTA エンロールメントを利用した証明書発行について ..... 18
6. 無線 LAN の利用 ..... 19
7. Android でのクライアント証明書取得・EAP-TLS 設定 ..... 20
8. 問い合わせ ..... 20

# 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CA Gléas」で発行した電子証明書を利用して、Microsoft CorporationのWindows Serverにおける802.1x（EAP-TLS）認証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、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。

- 【ドメインコントローラ】Microsoft Windows Server 2008 R2 Standard SP1
  ※以後、「ドメインコントローラ」と記載します
- 【RADIUSサーバ】Microsoft Windows Server 2008 R2 Standard SP1
  ネットワークポリシーサーバー 6.1.7601.17514
  ※以後、「NPS」と記載します
- 【認証局】JS3 プライベートCA Gléas （バージョン1.10）
  ※以後、「Gléas」と記載します
- 【アクセスポイント】AirMac Extreme （バージョン7.6.1）
  ※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
- 【クライアント】iPad （iOS5.1.1）
  ※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。

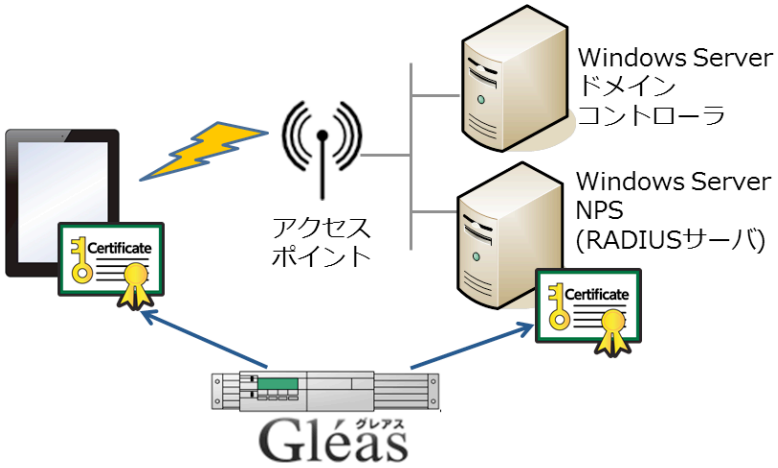
- Windows Server及びActive Directoryのセットアップ
  RADIUS認証用のユーザ及びグループは既に作成されているものとします
- 「ネットワークポリシーとアクセスサービス」のセットアップ
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作

- 各機器におけるネットワーク設定
- 無線LAN装置におけるRADIUSサーバの指定方法

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おります。




- スマートデバイス（iPad）からのWiFiアクセスをおこなう
- ユーザ認証にはEAP-TLSを利用する
- RADIUSサーバ証明書、及びクライアント証明書はGléasより発行されたものを利用する
- NPSはActive Directoryのグループ及びユーザ情報を参照して認証をおこなう（ログインユーザ情報はクライアント証明書のサブジェクトの別名に記載されているUPNを用いる）

## 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。

- クライアント証明書の発行には、「スマートカードログオン」テンプレートを用いて証明書を発行します。その際には、UPN（ユーザプリンシパル名。「username@Windowsドメイン名」の形式のもの）と、CRL配布ポイントを正しく設定する必要があります

※CRL配布ポイントが含まれていない証明書を用いる場合は、NPSサーバで以下のレジストリエントリを設定すればクライアント証明書認証が可能となります

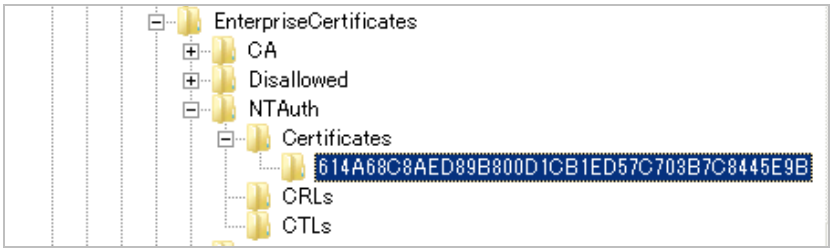
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥RasMan¥PPP¥EAP¥13
IgnoreNoRevocationCheck （存在しない場合は追加する）のDWARD値を 1 に設定する

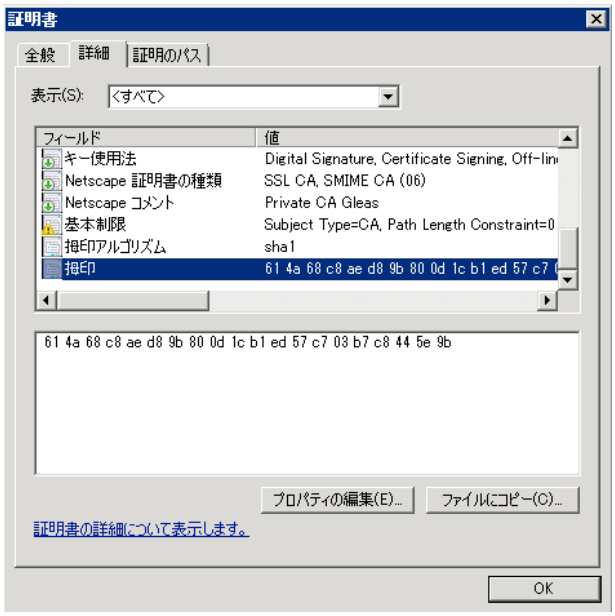
# 2. ドメインコントローラでの設定

## 2.1. ルート証明書の NTauth ストアへのインポート

ルート証明書を Gléas よりダウンロードし、Windows ドメインの NTauth ストアと呼ばれる格納領域にインポートします。
コマンドプロンプトを開き、以下のコマンドを入力します。
certutil -dspublish -f [*filename*] NTAuthCA
※[filename]には、エクスポートしたルート証明書を指定します。

コマンド実行後、以下のレジストリにルート証明書の拇印と同じ名前のレジストリキーが追加されます。
HKLM¥SOFTWARE¥Microsoft¥EnterpriseCertificates¥NTAuth¥Certificates
※追加されない場合は、gpupdate コマンドでポリシーの更新を行ってください。

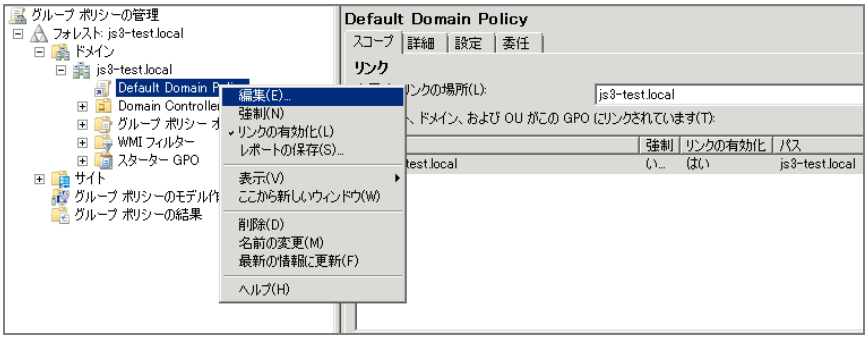


## 2.2. グループポリシーの設定

ドメインに参加しているコンピューターに対して信頼するルート認証機関を追加する設定を行います。

[スタートメニュー] > [管理ツール] > [グループポリシーの管理]を開き、対象となるグループポリシーオブジェクトを選択し右クリックし、[編集]をクリックします。
以下は Default Domain Policy を編集する場合の例です。



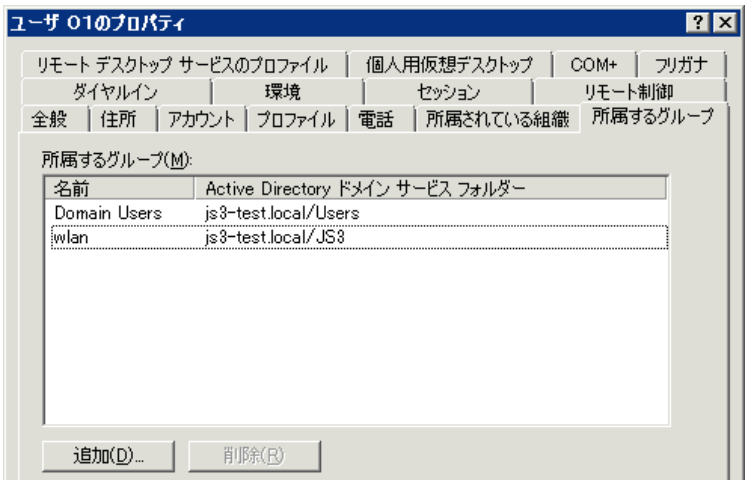

グループポリシー管理エディターが開きますので、左側ペインより[コンピューターの構成] > [ポリシー] > [Windows の設定] > [セキュリティの設定] > [公開キーのポリシー] > [信頼されたルート証明機関]を開きます。
次にメニューより[操作(A)] > [インポート(I)]を選択すると、証明書のインポートウィザードが起動するので、ルート証明書を登録します。

| ページ | 設定 |
|---|---|
| 証明書のインポートウィザードの開始 | [次へ(N)]をクリック |
| インポートする証明書ファイル | エクスポートしたルート証明書ファイルをを選択し、[次へ(N)]をクリック |
| 証明書ストア | [証明書をすべて次のストアへ配置する(P)]を選択し、[証明書ストア]で[信頼するルート認証機関]が選ばれていることを確認し、[次へ(N)]をクリック |
| 証明書インポートウィザードの終了 | [完了]をクリック |

## 2.3. Active Directory でのアカウント設定

[管理ツール]より[Active Directoryユーザーとコンピューター]を開始し、無線LANアクセスを許可するユーザアカウントのプロパティを開き、[所属するグループ]

タブを開き、無線LANを利用するグループに所属していることを確認します。
（本書では「wlan」セキュリティグループとします）

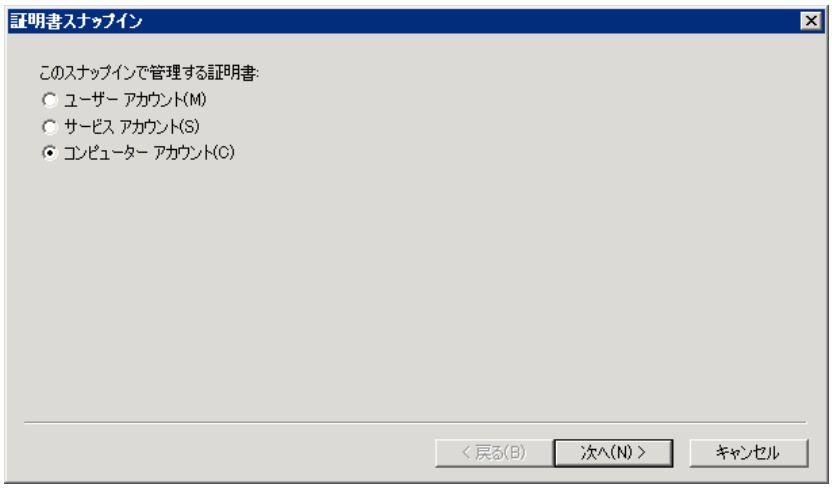


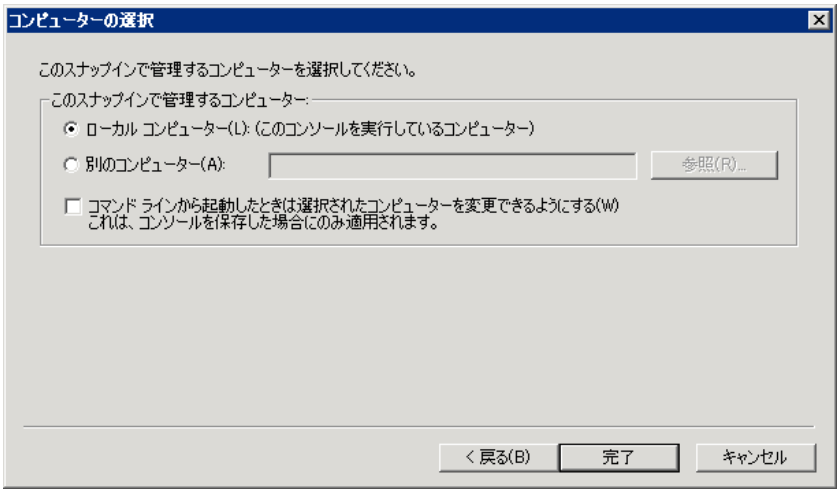

# 3. NPS サーバでの設定

## 3.1. サーバ証明書のインポート

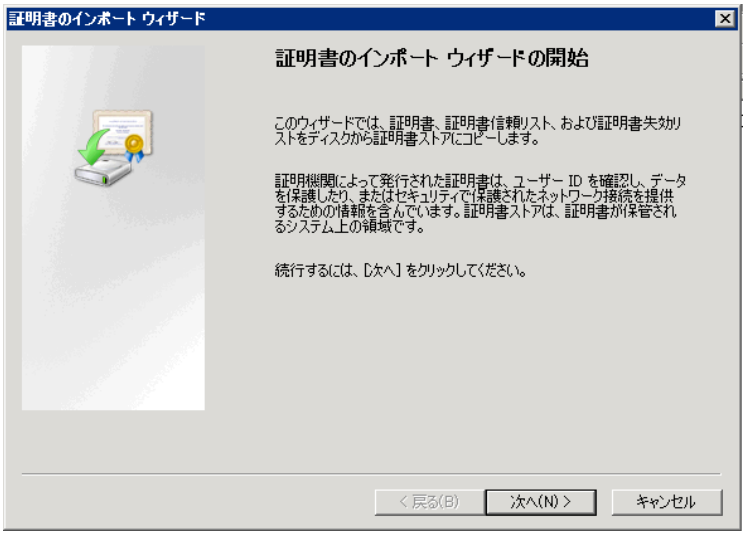
NPS を動かしているサーバ上で MMC（Microsoft Management Console）を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明書]を追加します。

「証明書のスナップイン」では、[コンピューター アカウント(C)]を選択し、次の「コンピューターの選択」では、[ローカルコンピューター(L)]を選択し、[完了]をクリックします。





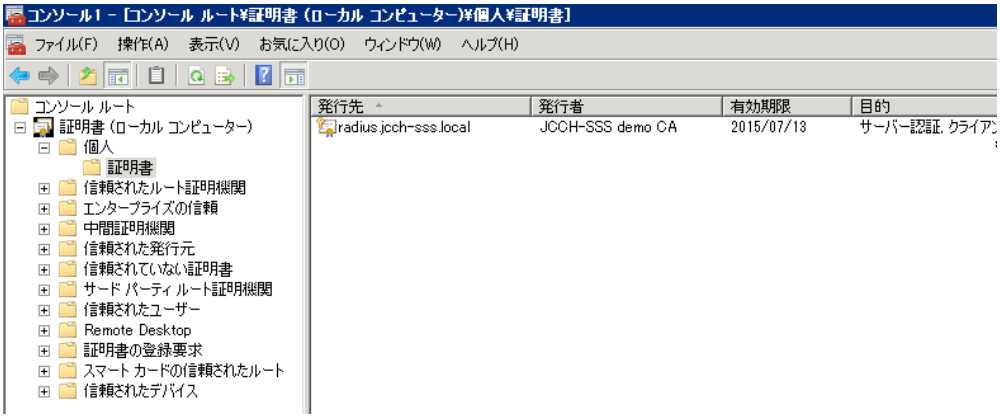

スナップインが追加されたら左側のペインより[証明書] > [個人]と展開し、右側のペインで右クリックして、[すべてのタスク(K)] > [インポート(I)]をクリックします。「証明書のインポートウィザード」が開始されるので、サーバ証明書とルート証明書をインポートします。




| ページ | 設定 |
|---|---|
| 証明書のインポートウィザードの開始 | [次へ(N)]をクリック |
| インポートする証明書ファイル | Gléas よりダウンロードした PKCS#12 ファイル（拡張子：p12）を指定して、[次へ(N)]をクリック |
| パスワード | Gléas から PKCS#12 ファイルをダウンロードする際に設定したパスワードを入力して、[次へ(N)] |

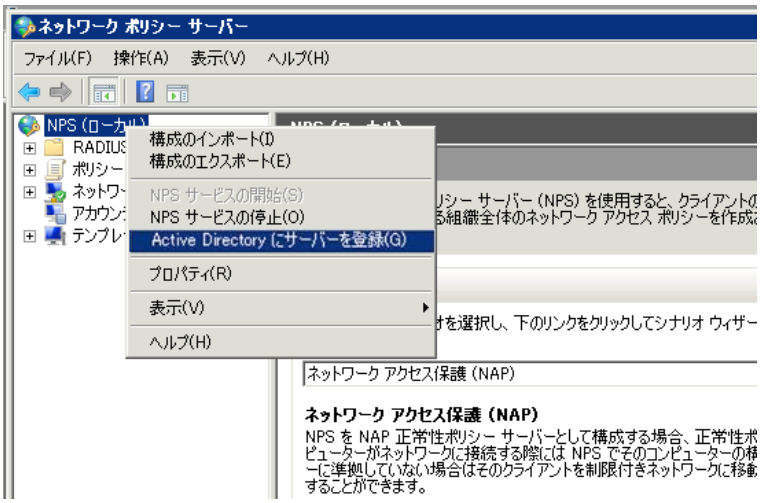
| | |
|---|---|
| | をクリック |
| 証明書ストア | [証明書の種類に基づいて、自動的に証明書ストアを選択する(U)]を選択し、[次へ(N)]をクリック |
| 証明書インポートウィザードの終了 | [完了]をクリック |

完了後、[個人]に Gléas よりダウンロードした RADIUS サーバ用の証明書がインポートされていることを確認します。




## 3.2. NPS の Active Directory との連携

[管理ツール]から[ネットワーク ポリシー サーバー]を開きます。
左ペインの[NPS（ローカル）]を右クリックして、[Active Directory にサーバーを登録(G)]をクリックします。



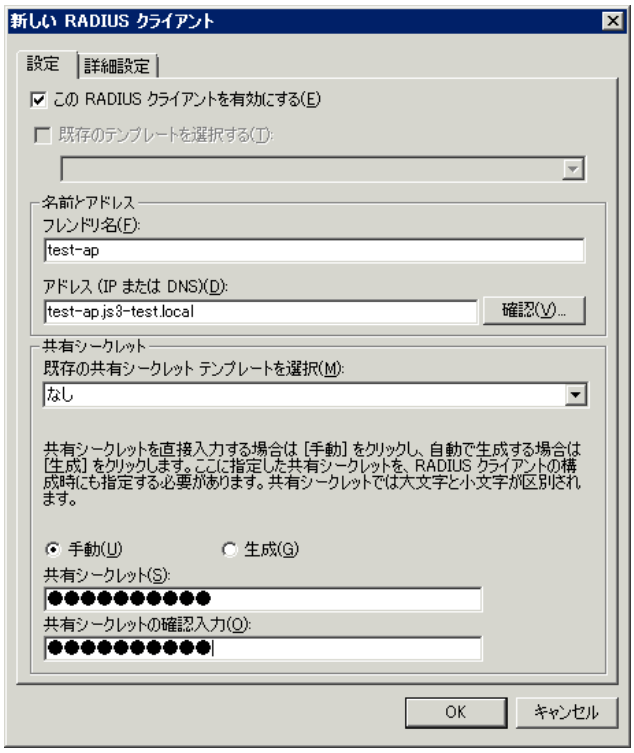

その後、確認メッセージが表示されるので[OK]をクリックします。

## 3.3. RADIUS クライアントの設定

[ネットワーク ポリシー サーバー]の左ペインから[NPS（ローカル）] > [RADIUSクライアントとサーバー] > [RADIUSクライアント]を展開し右クリックし、[新規]を選択します。

[新しいRADIUSクライアント]画面にて、本件章においてのRADIUSクライアントとなるアクセスポイントの情報を入力します。

- [フレンドリ名(F):]には、任意の名称を入力
- [アドレス（IPまたはDNS）(D):]には、アクセスポイントのIPアドレスか、ホスト名を入力（名前解決できるようになっている必要があります）
- [共有シークレット(S):]には、アクセスポイントとの通信に利用するパスワード（シークレット）を入力

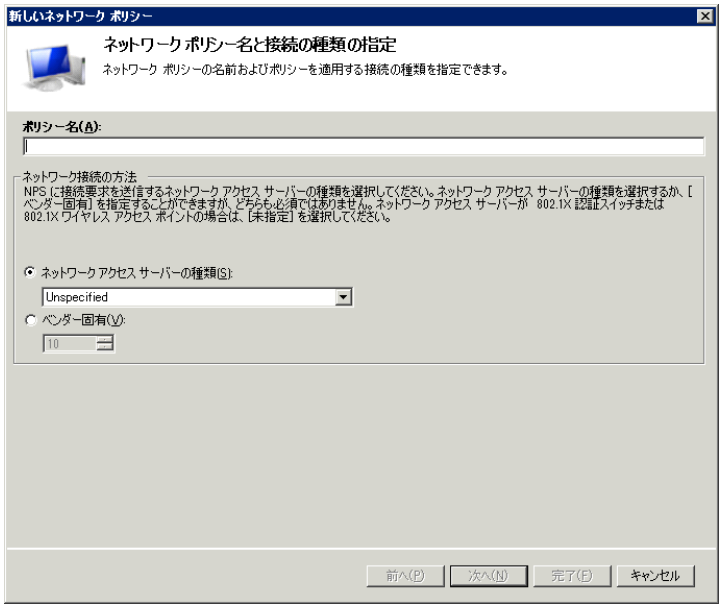


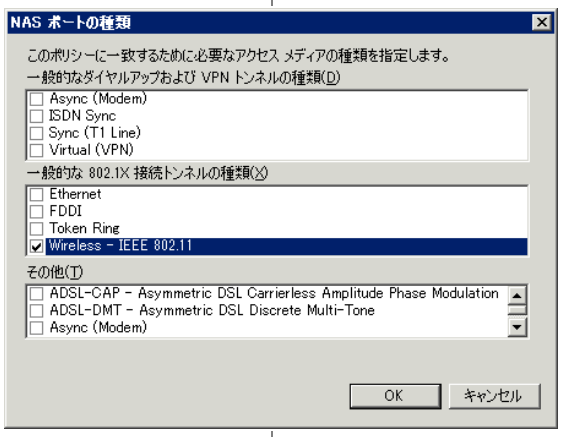

以上を設定したら[OK]をクリックします。

## 3.4. 認証ポリシの設定

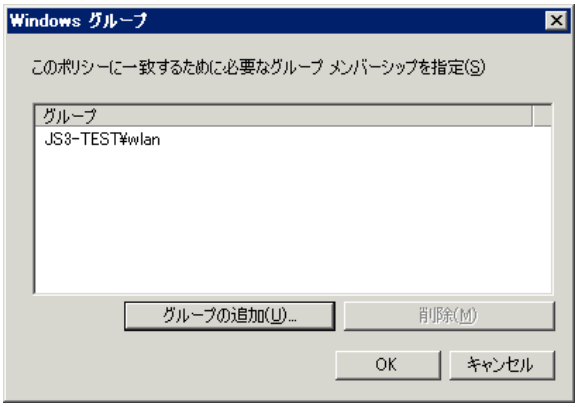
[ネットワーク ポリシー サーバー]の左ペインから[NPS（ローカル）] > [ポリシー] > [ネットワーク ポリシー]を展開し右クリックし、[新規]を選択します。

[新しいネットワーク ポリシー]ウィザードが開始されますので、以下の通り設定をおこないます。

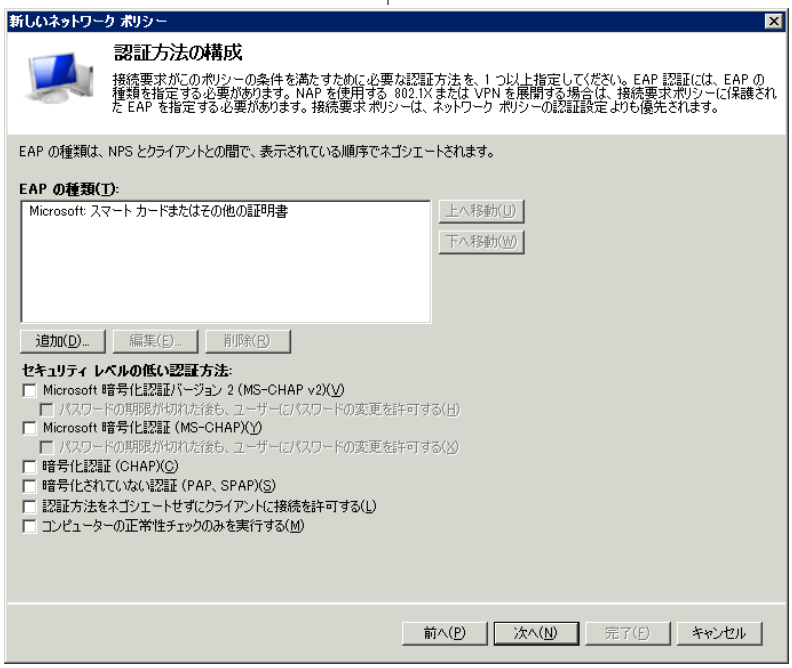


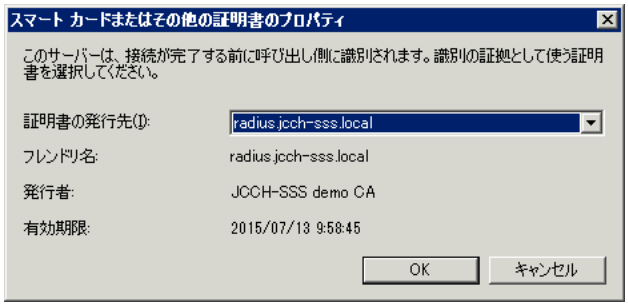

| ページ | 設定 |
|---|---|
| ネットワークポリシー名と接続の種類の指定 | [ポリシー名(A)]に任意の名称を入力 |
| 条件の指定 | 1. [追加(D)]をクリック<br>2. [条件の選択]画面で、[NAS ポートの種類]を選択し、[追加(D)]をクリック<br>3. [NAS ポートの種類]画面で、[一般的な 802.1X 接続トンネルの種類(X)]より[Wireless - IEEE802.11]をチェックし OK をクリック<br>  <br>4. 元の画面まで戻り、再度[追加(D)]をクリック<br>5. [条件の選択]画面で、[Windows グループ]を選択し、[追加(D)]をクリック<br>6. [ユーザグループ]画面にて、[グループの追加(U)]をクリックし、該当のグループ(本検証で |

| | |
|---|---|
| | は wlan)を選択<br>7. [OK]をクリックし元の画面まで戻り、[次へ(P)]をクリック |




| | |
|---|---|
| | 7. [OK]をクリックし元の画面まで戻り、[次へ(N)]をクリック |
| アクセス許可の指定 | [アクセスを許可する(A)]を選択し、[次へ(N)]をクリック |
| 認証方法の構成 | 1. [EAP の種類(T)]にて、[追加(D)]をクリック<br>2. [EAP の追加]画面で、[Microsoft:スマートカードまたはその他の証明書]を選択し[OK]をクリック<br>3. [セキュリティレベルの低い認証方法]のチェックをすべて外す |



| | |
|---|---|
| | 4. 追加した[Microsoft:スマートカードまたはその他の証明書]を選択し[編集]をクリック<br>5. [スマートカードまたはその他の証明書プロパティ]画面にて、[証明書の発行先]に 3.1 項でインポートしたサーバ証明書が選択されていることを確認して[OK]をクリック<br>  <br><br>6. [次へ(N)]をクリック |
| 制約の構成 | 追加の制約条件などを必要に応じ設定し、[次へ(N)]をクリック |
| 設定の構成 | RADIUS 属性(VLAN　ID など)を必要に応じ設定し、[次へ(N)]をクリック |
| 新しいネットワークポリシーの完了 | [完了(F)]をクリック |

# 4. 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

## 4.1. 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。

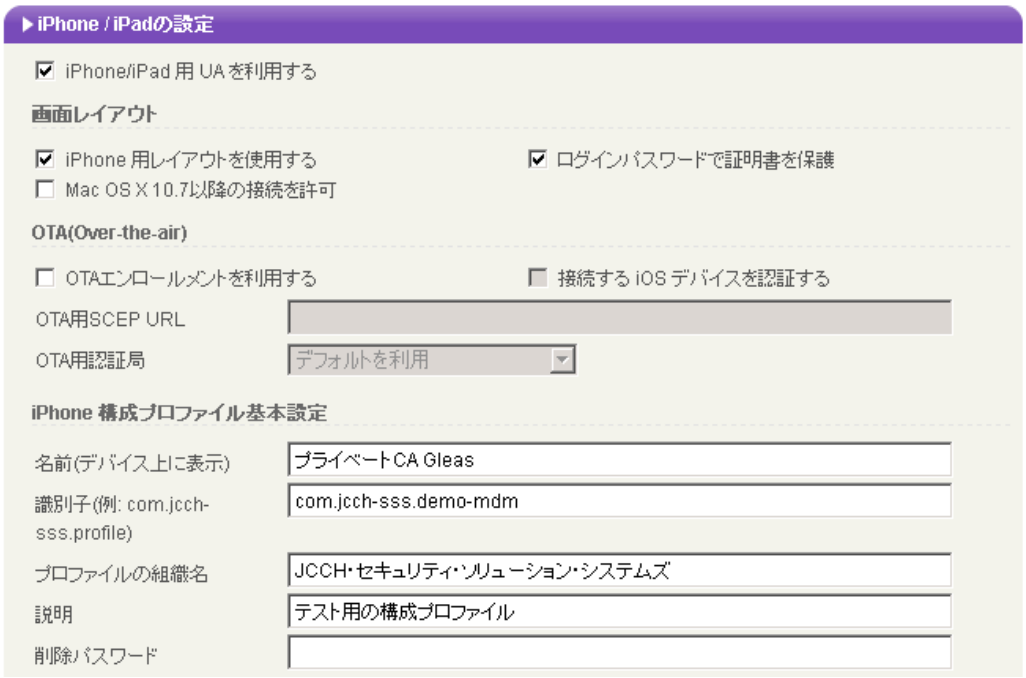
- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定

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
- [OTA(Over-The-Air)]を利用する場合はチェック（下述参照）
- [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）



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、無線LAN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は、[非公開ネットワーク]をチェック


他項目の設定も終了したら、[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。

# 5. 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）

## 5.1. 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。


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

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、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。

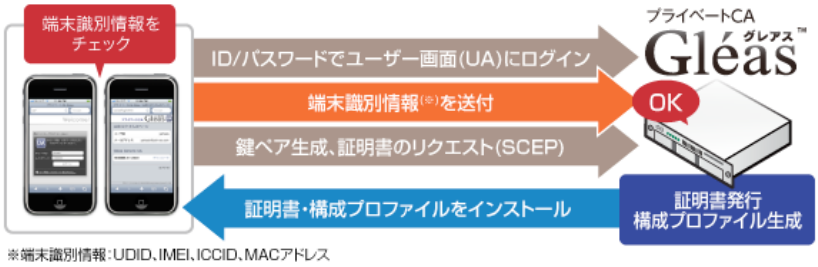

元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトしてください。
以上で、iPadでの構成プロファイルのインストールは終了です。

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。


## 5.2. 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7項のお問い合わせ先までお問い合わせください。

# 6. 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ュアな接続をお試しください。

無線LANアクセス成功時には、Windows Serverのセキュリティログに以下のメッセージが表示されます（一部の抜粋）。

*イベント ID:　6272*
*タスクのカテゴリ:　ネットワーク ポリシー サーバー*
*レベル:　情報*
*キーワード:　成功の監査*
*説明:　ネットワーク ポリシー サーバーがユーザーにアクセスを許可しました。*
*認証の詳細:*
*認証の種類:　EAP*
*EAP の種類:　Microsoft: スマート カードまたはその他の証明書*

失効済みの証明書を利用すると、アクセスに失敗しWindows Serverのセキュリティログに以下のメッセージが表示されます（一部の抜粋）。
※失効情報がNPSに伝播されている必要があります
*イベント ID:　6273*
*タスクのカテゴリ:　ネットワーク ポリシー サーバー*
*レベル:　情報*
*キーワード:　失敗の監査*
*説明 :　ネットワーク ポリシー サーバーがユーザーのアクセスを拒否しました。*

*詳細については、ネットワーク ポリシー サーバーの管理者に問い合わせてください。*

*認証の詳細:*

| | |
|---|---|
| *認証の種類:* | *EAP* |
| *EAP の種類:* | *Microsoft: スマート カードまたはその他の証明* |
| *理由コード:* | *256* |
| *理由:* | *この証明書は失効しています。* |

# 7. Android でのクライアント証明書取得・EAP-TLS 設定

弊社ホワイトペーパー「Android での無線LAN （802.1X EAP-TLS）設定」をご参照ください。公開URLは以下の通りとなります。

http://www.jcch-sss.com/service/support/2011/06/wifi-eap-tls-android

# 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。

**■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