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

## SharePoint Serverでの

## クライアント証明書マッピング認証設定

**Ver.1.0**

**2014 年 7 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CA Gléas」で発行したクライアント証明書・を利用して、Microsoft CorporationのSharePoint Serverで認証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。

- ドメインコントローラ：Microsoft Windows Server 2012 R2 Standard
  ※以後、「ドメインコントローラ」と記載します
- SharePoint Server： SharePoint Server 2013 Enterprise SP1
  / Windows Server 2012 R2 Standard
  ※以後、「SharePointサーバ」と記載します
  ※スタンドアロンインストールをしています
- JS3 プライベートCA Gléas （バージョン1.11）
  ※以後、「Gléas」と記載します
- クライアント：iPad（第三世代、iOS 7.1.2）
  ※以後、「iPad」と記載します

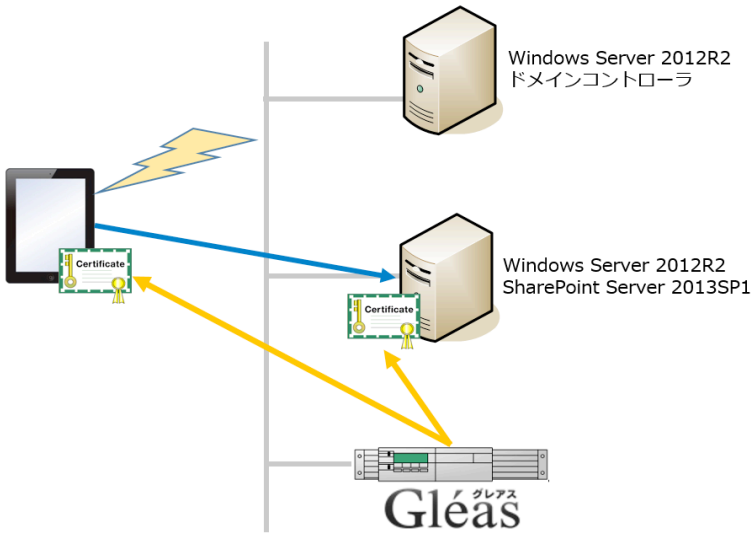
以下については、本書では説明を割愛します。

- Windows ServerやWindowsドメインのセットアップ
- SharePointサーバのセットアップ
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- iPadで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。

## 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。




1. Gléasでは、SharePointサーバにSSL用サーバ証明書を、iPadにクライアント証明書を発行する
2. iPadはSharePointサーバにアクセスすると、クライアント証明書の提示が求められる（証明書を持たないクライアントは接続を拒否される）
3. SharePointサーバは、クライアント証明書に記載されたAcitve Directoryユーザ名（プリンシパル名）としてログイン認証をおこなう

## 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

# 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

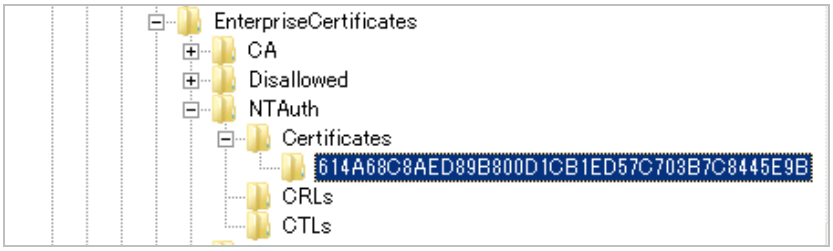
ルート証明書を Gléas よりダウンロードし、Windows ドメインの NTauth ストアと

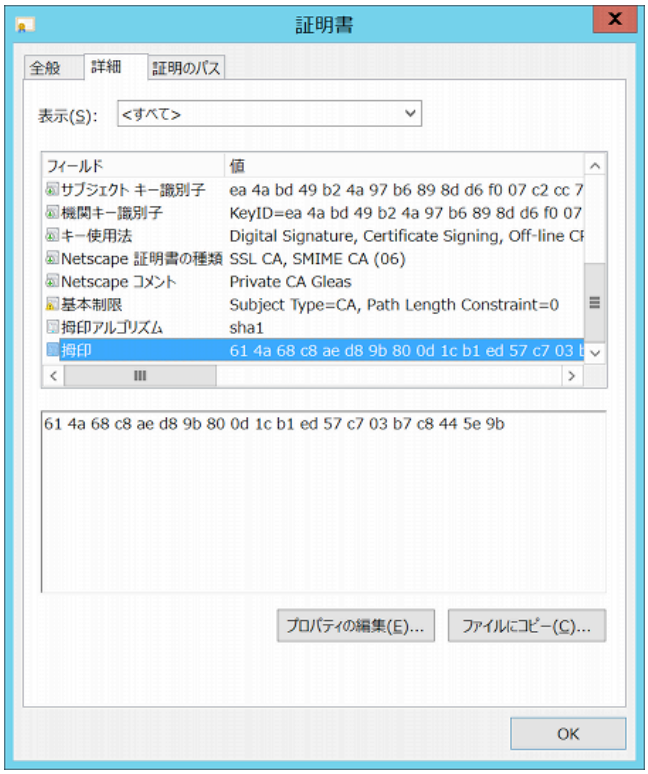
呼ばれる格納領域にインポートします。
コマンドプロンプトを開き、以下のコマンドを入力します。

```
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。

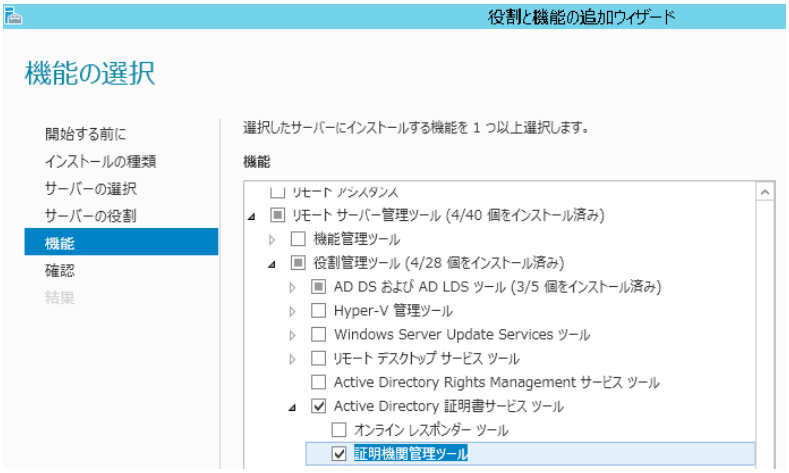


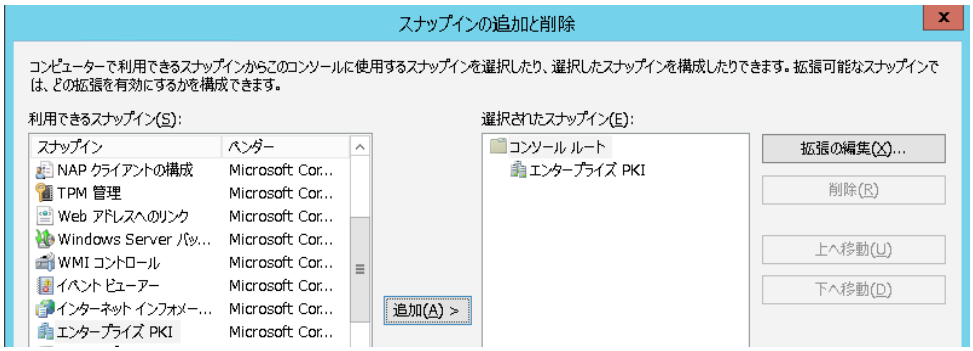

ADFS サーバでも同様にレジストリエントリに追加されているか確認します。
※追加されない場合は、gpupdate コマンドでポリシーの更新を行ってください。

なお、NTauth ストアへの証明書インポートは、GUI でおこなうことも可能です。

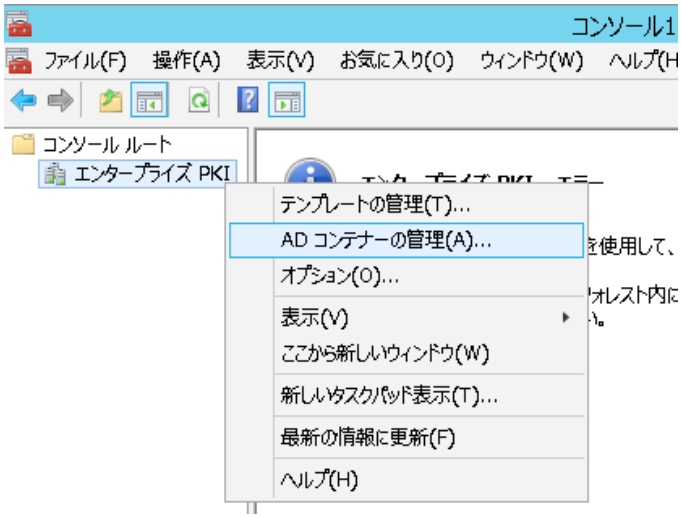
サーバーマネージャで、[役割と機能の追加]をおこない、[証明機関管理ツール]を追加します。



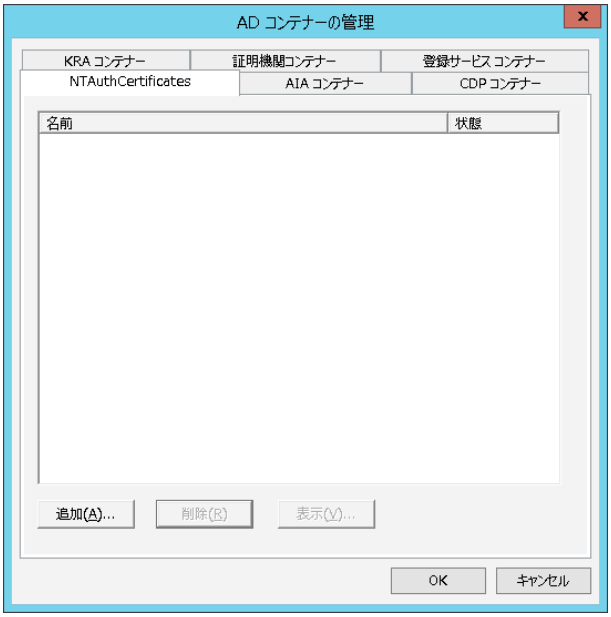

その後、MMC（マイクロソフト管理コンソール）を開き、[エンタープライズ PKI]スナップインを追加します。




エンタープライズ PKI 上で右クリックをし、[AD コンテナーの管理(A)...]を選択します。



[NTAuthCetificates]タブで[追加(A)…]をクリックし、ルート証明書ファイルを選択することで NTauth ストアにルート証明書を追加します。



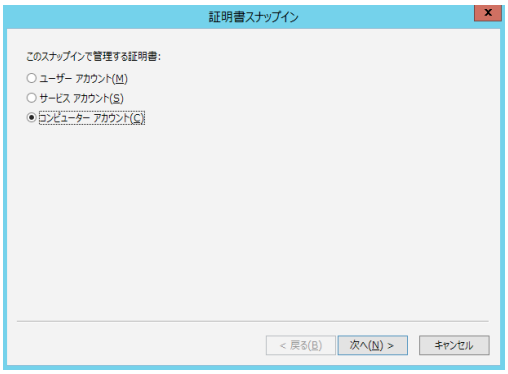

# 3. SharePointサーバでの設定

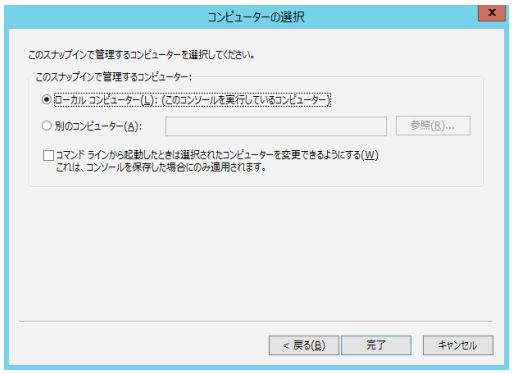
## 3.1. SSL サーバ証明書のインポート

本手順開始前に、Gléas の管理者画面よりサーバ証明書ファイル（PKCS#12 ファイル）をダウンロードします。
ダウンロードする際に保護パスワードの入力を求められますので、入力してからダウンロードし、ADFS サーバにそのファイルをコピーします。

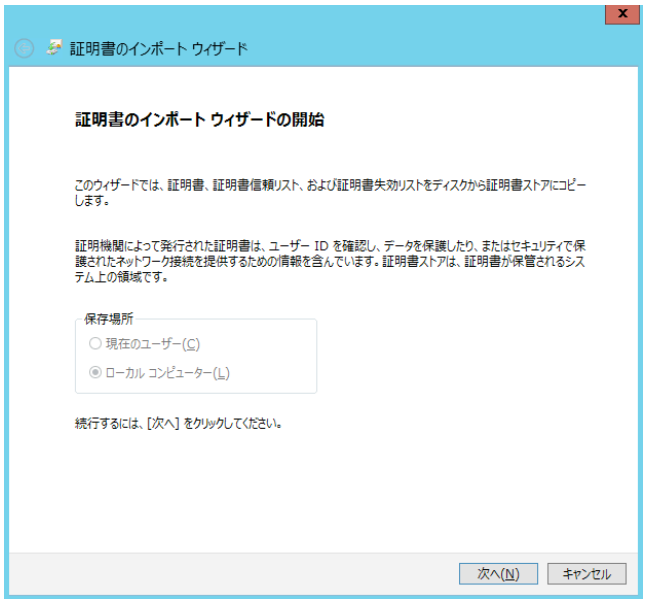

MMC を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明書]を追加します。

「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。



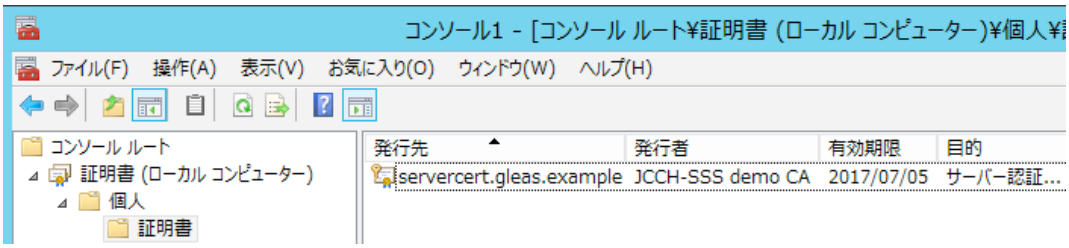

スナップインが追加されたら左側のペインより[証明書] > [個人]と展開し、右側のペインで右クリックして、[すべてのタスク(K)] > [インポート(I)]をクリックします。「証明書のインポートウィザード」が開始されるので、サーバ証明書をインポートします。




| 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、サーバ証明書がインポートされていることを確認します。

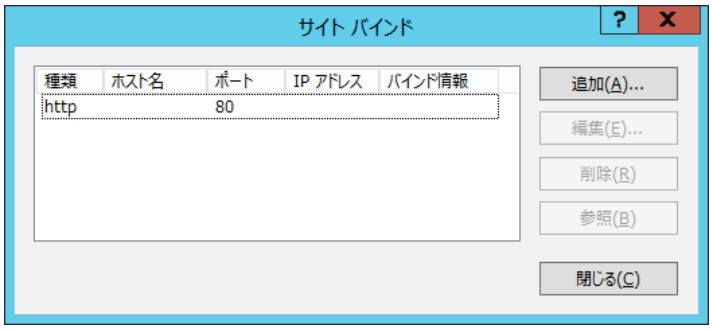



またこの際に、ルート証明書が[信頼されたルート証明機関]に追加されているのを確認します。

## 3.2. SSL ポートのバインド

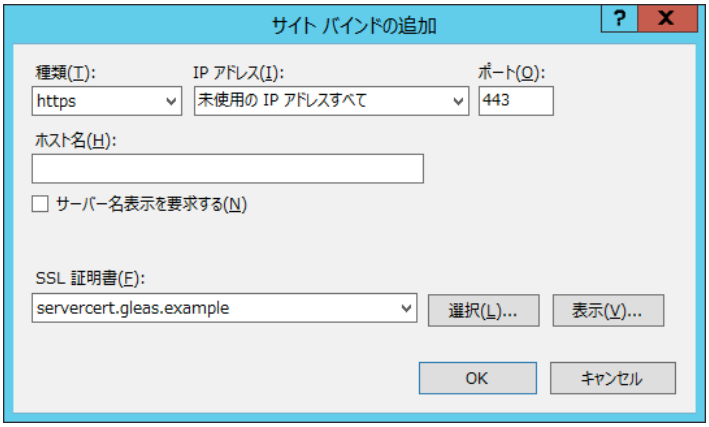
スタートメニュー > [管理ツール]より[インターネット インフォメーション サービス（IIS）マネージャー]を開き、左ペインより対象となる Web サイト（本検証ではデフォルトで作成される[SharePoint - 80]）を選択し、右ペインの[バインド...]をクリックします。

[サイト バインド]ウィンドウが表示されるので、[追加(A)...]をクリックします。

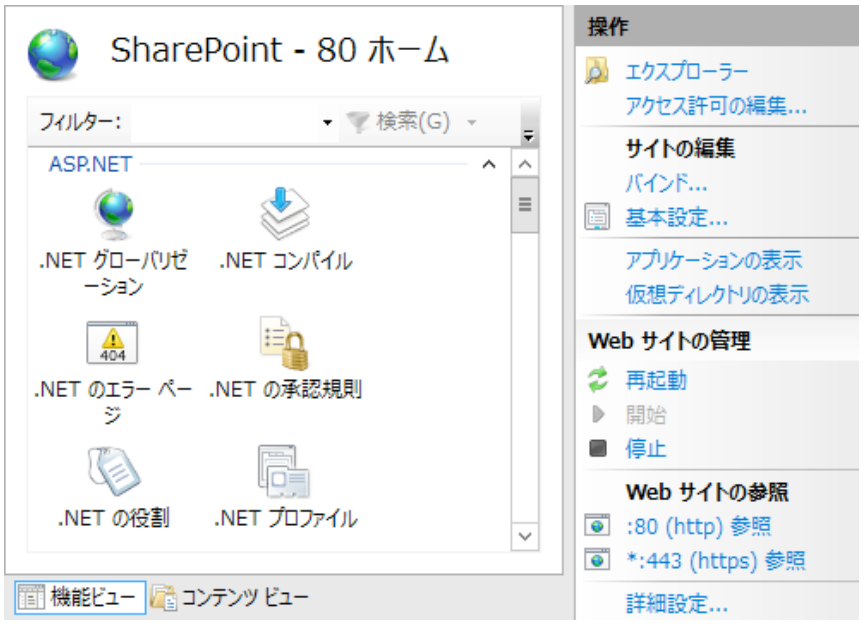



[サイト バインドの追加]ウィンドウが表示されるので、[種類(T):]を https にします。
[SSL 証明書(S):]で、3.1 項でインポートしたサーバ証明書が選択可能になっているので、それを選びます。
また、サービスを公開する IP アドレスやポート番号を限定する場合は、[IP アドレ

ス(I):]、[ポート(O):]を変更します。
設定変更後、「OK」ボタンをクリックします。

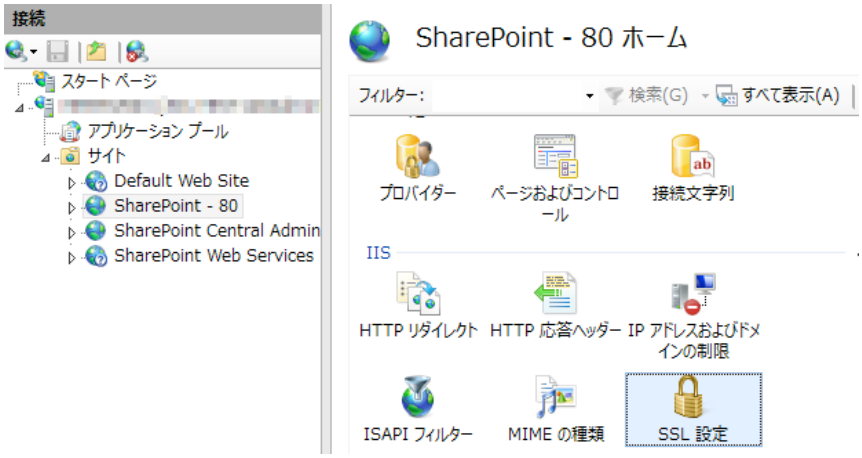



右ペインの「Web サイトの管理」に[*.443(https) 参照]が追加されていれば、バインドの設定は完了です。

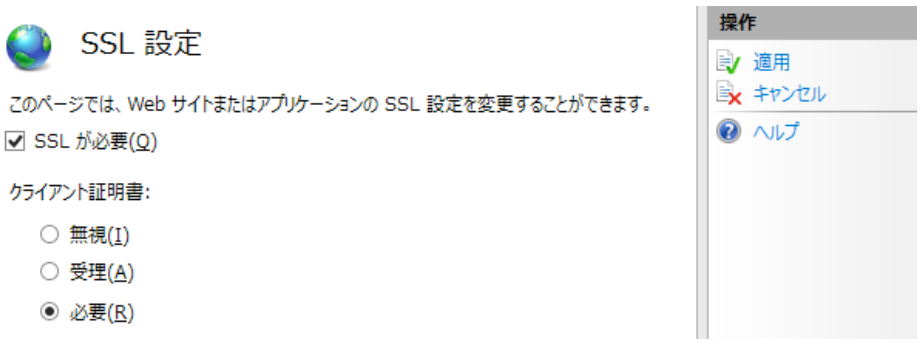



## 3.3. クライアント証明書要求の有効化

左ペインの対象のWebサイト選択された状態で、中ペインの[SSL設定]アイコンをクリックします。

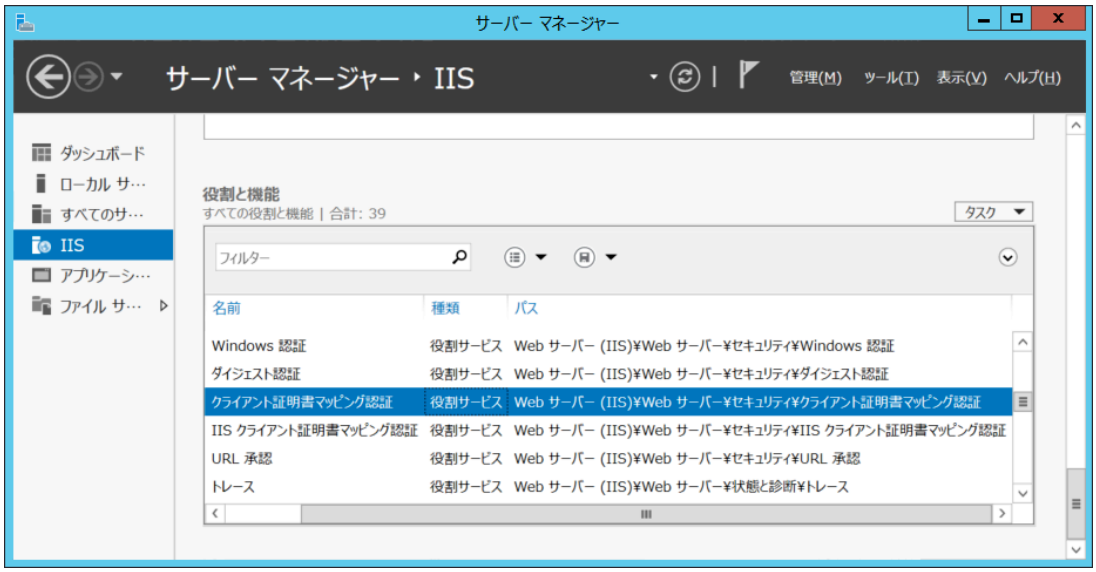



[SSLが必要]のチェックボックスを有効にし、クライアント証明書の[必要(R)]を選択し有効化します。
右ペインの[適用]をクリックすると、SSL設定の変更が反映されます。

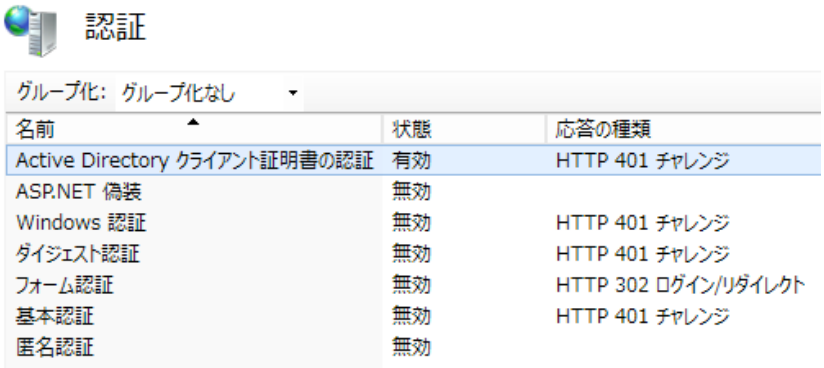



## 3.4. クライアント証明書マッピング認証の設定

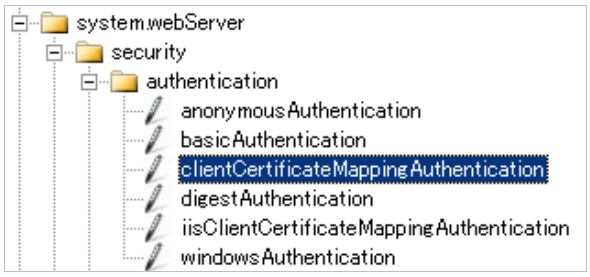
サーバーマネージャーを起動し、IIS の役割と機能で[クライアント証明書マッピング認証]が有効にされていることを確認します。




[インターネット インフォメーション サービス（IIS）マネージャー]を開き、左ペインからホスト名を選択し、右ペインより[認証]オプションを開きます。[Active Directory クライアント証明書の認証]を有効にします。

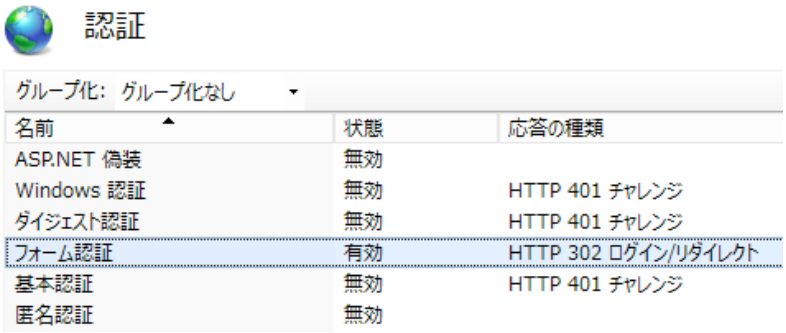


左ペインで対象の Web サイトをクリックし、中央ペインで[構成エディター]を開き、セクション system.webServer > security > authentication > clientCertificateMappingAuthentication に移動して、[enabled]が「True」になっていることを確認します。





再度、左ペインで対象の Web サイトをクリックし [認証]をクリックします。
[フォーム認証]のみ有効に設定し、他の認証方法をすべて無効にします。




# 4. Gléasの管理者設定

GléasのUA（申込局）より発行済み証明書をiPad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

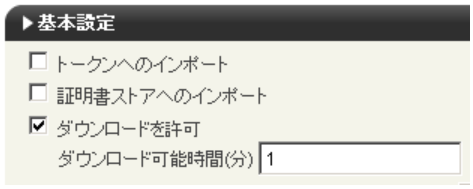
## 4.1. UA（ユーザ申込局）設定

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[認証局ー

覧]画面に移動し、設定を行う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iPhone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。

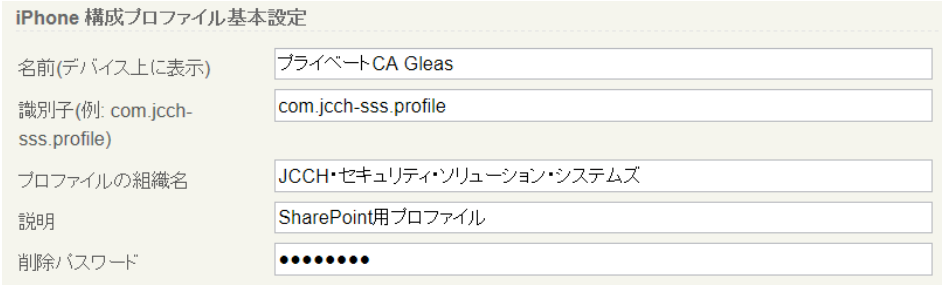
画面レイアウト

- [iPhone用レイアウトを利用する]をチェック
- [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

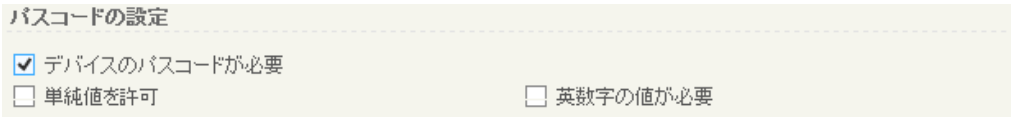
- [名前]、[識別子]に任意の文字を入力（必須項目）
- [削除パスワード]を設定すると、iPhoneユーザが設定プロファイルを削除する際に管理者が定めたパスワードが必要となります（iPhoneユーザの誤操作等によ

る構成プロファイルの削除を防止できます）




設定が終わったら、 [保存]をクリックします。

クライアント証明書マッピング認証をおこなう場合、パスワード認証なしでSharePointサーバへのアクセスが可能となるので、デバイスパスコードを設定しておくことが推奨されますが、構成プロファイルでパスコードを強制させることも可能です。




# 5. iPad での操作

## 5.1. 構成プロファイルのインストール

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。


インストール途中に、以下のような確認画面が現れますので、その説明内容を確認したうえで[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Gléasのルート認証局証明書になります。

構成プロファイルでデバイスのパスコード付与が強制されていて、かつiPadにデバイスパスコードが設定されていない場合は、パスコードの設定を促されます。


インストール完了となりますので、[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. SharePoint サーバへのアクセス

SafariでSharePointサーバへアクセスするとユーザIDやパスワードの入力を求められることなく、クライアント証明書に記載されているユーザプリンシパル名に基づくユーザ名でログインが完了します。

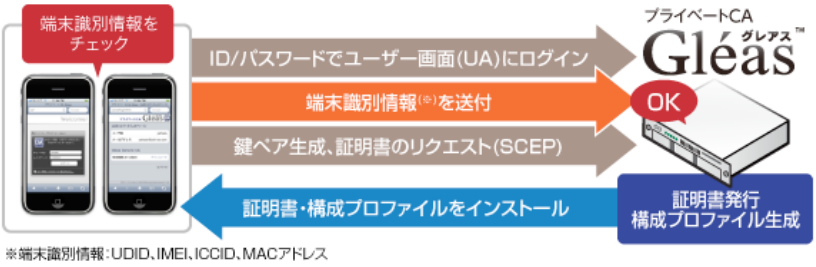

クライアント証明書が無い場合は先に進むことができなくなります。
ユーザプリンシパル名が記載されていないなど、必要要件を満たしていないクライアント証明書でアクセスすると、「401 UNAUTHORIZED」エラーとなります。

失効済みの証明書でアクセスをすると、以下のメッセージが出現し接続できません。
（失効情報がSharePointサーバに伝搬されている必要があります。IISのログには403エラーが記録されます）


## 5.3. 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。




詳細は最終項のお問い合わせ先までお問い合わせください。

## 6. 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。
（マイクロソフト製品に関するお問い合わせについては回答できないケースもありますので、あらかじめご了承ください）

**■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