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

Microsoft Exchange Serverでの
クライアント証明書マッピング認証を用いた認証設定
（Exchange ActiveSync / Outlook Web App）

Ver.1.0
2013 年 1 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Exchange 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 2008 R2 Standard
  ※以後、「ドメインコントローラ」と記載します
- Exchange Server：Microsoft Exchange Server 2010 / Windows Server2008 R2
  ※以後、「Exchangeサーバ」と記載します
- 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
- ActiveSyncクライアント：iPhone 5 （iOS 6.0.2）
  ※以後、「iPhone」と記載します
  ※以後、ActiveSyncは「EAS」と記載します
- Outlook Web Appクライアント:Microsoft Windows 8 Pro / Internet Explorer 10
  ※以後、「PC」と記載します
  ※以後、Outlook Web Appは「OWA」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。

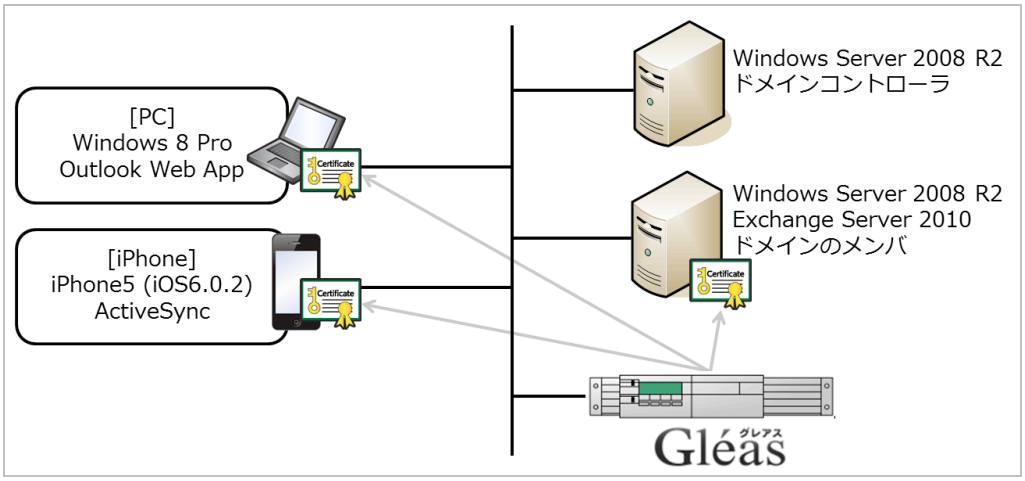
- ドメインコントローラのセットアップ
- Exchangeサーバのセットアップ（クライアントアクセスサーバ（EAS・OWA）設定を含む）
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定

- iPhoneやPC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. 有効なクライアント証明書を持つPCだけがOWAを利用することができる
2. 有効なクライアント証明書を持つiPhoneだけがEASを利用することができる
3. この時の認証はクライアント証明書のみによっておこなわれるものとし、ID・パスワードの入力は不要なものとする

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

2. ドメインコントローラでの設定

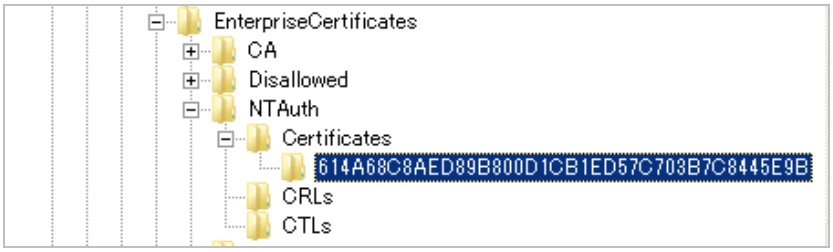
2.1. ルート証明書の NTauth ストアへのインポート

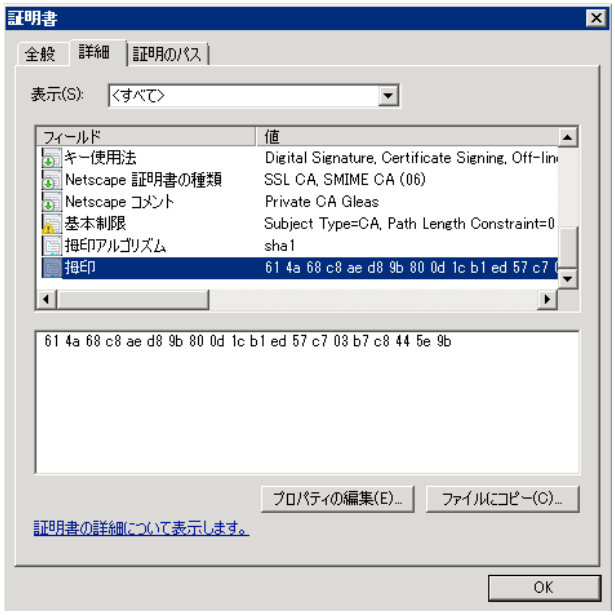
ルート証明書を Gléas よりダウンロードし、Windows ドメインの NTauth ストアと呼ばれる格納領域にインポートします。
コマンドプロンプトを開き、以下のコマンドを入力します。

```
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。



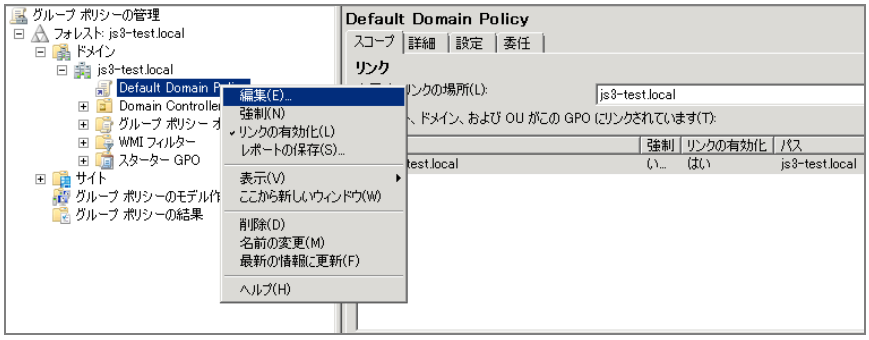


2.2. グループポリシーの設定

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。



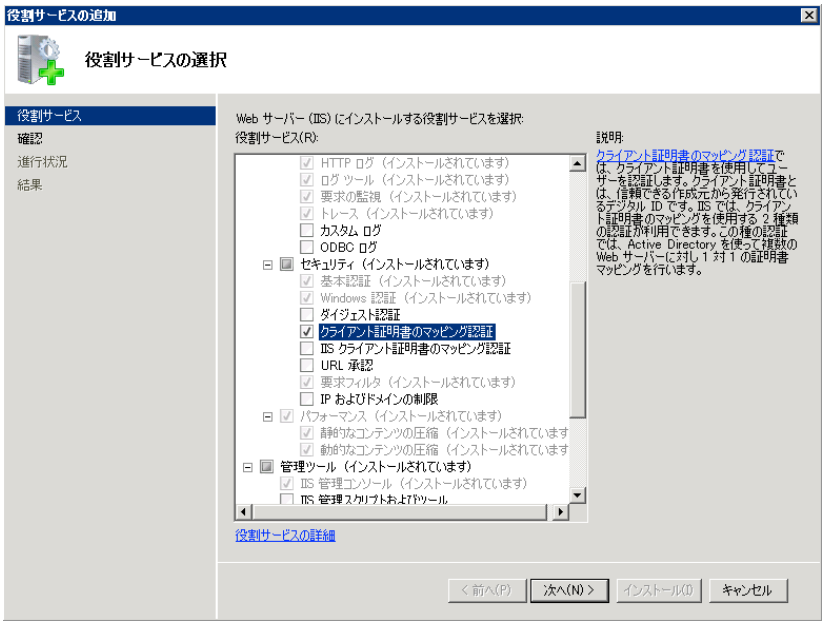
グループポリシー管理エディターが開きますので、左側ペインより[コンピューターの構成] > [ポリシー] > [Windows の設定] > [セキュリティの設定] > [公開キーのポリシー] > [信頼されたルート証明機関]を開きます。
次にメニューより[操作(A)] > [インポート(I)]を選択すると、証明書のインポートウィザードが起動するので、ルート証明書を登録します。

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

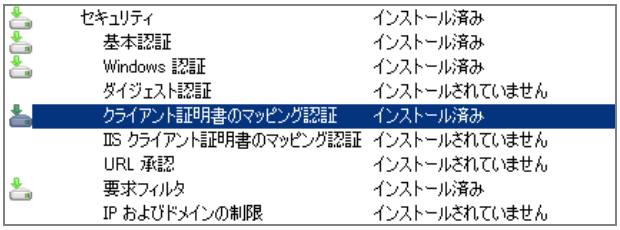
3. Exchangeサーバ（クライアントアクセスサーバ）の設定

3.1. インターネットインフォメーションサーバ（IIS）の役割追加

管理メニューの [サーバーマネージャ]を開き、左ペインの[役割]を展開します。
右ペインの[WEB サーバー（IIS）]欄で[役割サービスの追加]をクリックすると、[役割サービスの追加]ウィンドウが表示されるので、[クライアント証明書のマッピング認証]を選択し[次へ(N) >]をクリックし 、インストールします。



もとの画面で、クライアント証明書のマッピング認証がインストール済みであることを確認します。



スタートメニューより[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、他のものを全て無効にします。

3.2. SSL サーバ証明書の設定

「プライベート CA Gléas ホワイトペーパー ～IIS7.5 におけるクライアント証明書を利用したユーザ認証の設定手順～」の 2.1 項及び 2.2 項を参考に、IIS に SSL サ

ーバ証明書を設定します。

※上記ホワイトペーパーは以下 URL にて公開されています

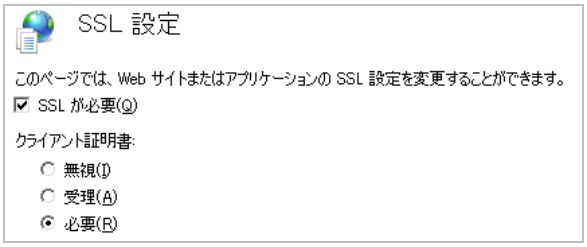
http://www.jcch-sss.com/service/support/2010/10/iis-ssl-client-auth

3.3. クライアント証明書認証の設定

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、左ペインで WEB サイトを [owa]ディレクトリまで展開します。

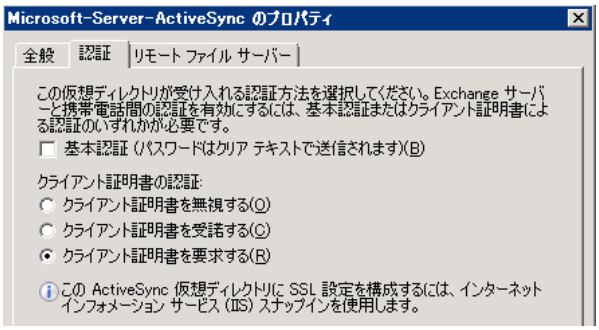
右ペイン（/owa ホーム）で[SSL 設定]を開き、以下を設定します。

- [SSL が必要(Q)]にチェックを入れる（入っていない場合）
- [クライアント証明書:]は、[必要(R)]を選択



[Microsoft-Server-ActiveSync]ディレクトリに対しても同じ設定をします。

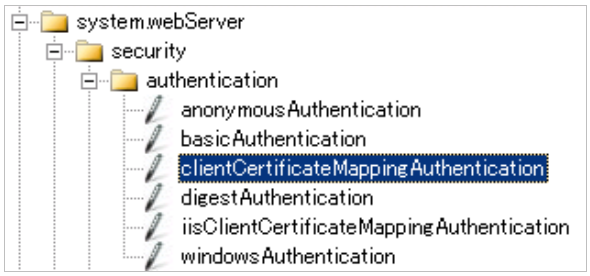
（EAS の場合は、Exchange 管理コンソール（[サーバの構成] > [クライアント アクセス] > [Exchange ActiveSync]タグ）からでも同様の設定が可能です）



3.4. 証明書マッピング認証の有効化

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、左ペインで WEB サイトを [owa]ディレクトリまで展開します。

右ペイン（/owa ホーム）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]を True にして[適用]をクリックします。



/owa ホームに戻り、[認証]をクリックします。
全ての認証方法を[無効]に設定します。

[Microsoft-Server-ActiveSync]ディレクトリに対しても同じ設定をします。

4. Gléasの管理者設定（OWA）

GléasのUA（申込局）より発行済み証明書を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

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。

- [証明書ストアへのインポート]をチェック

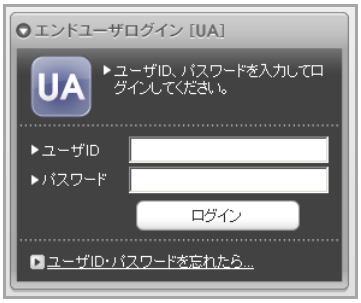
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

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。

5. PC での操作（OWA）

5.1. クライアント証明書のインストール

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。
[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。
※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。

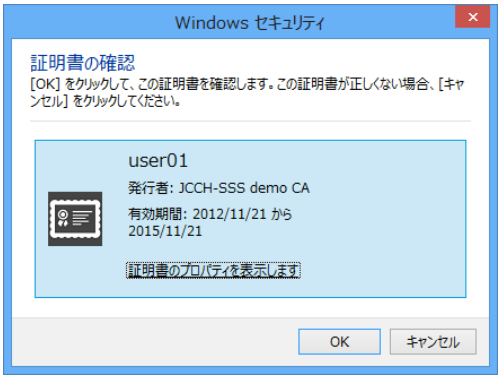
「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。

5.2. OWA へのアクセス

Internet ExplorerでOWAへアクセスします。

クライアント証明書の選択ダイアログが出現します。証明書を確認して[OK]をクリックします。

※IEの設定によっては、クライアント証明書の選択ダイアログが出ない場合もあります



その後、ActiveDirectoryのID・パスワードの入力を求められることなくOWAの画面が表示されます。

6. Gléasの管理者設定（EAS）

GléasのUA（申込局）より発行済み証明書をiPhone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

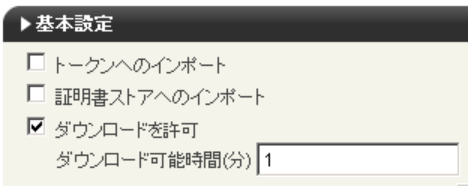
6.1. UA（ユーザ申込局）設定

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。

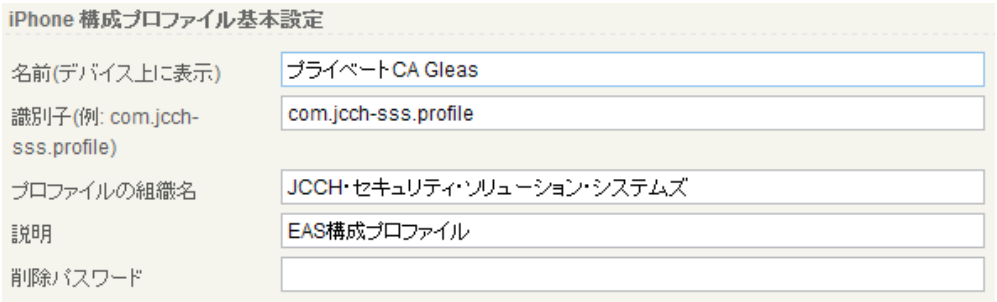
構成プロファイル生成に必要となる情報を入力する画面が展開されるので、以下設定を行います。

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）



Microsoft Exchange(ActiveSync)の設定

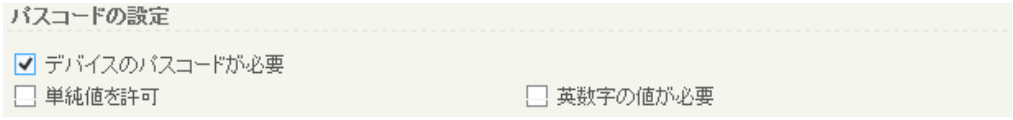
- [Exchangeホスト名]にアクセス先となるExchangeサーバのホスト名（FQDN）を入力
- [パスワードの入力方法]には、Exchange用パスワードの入力方法を以下より選択（今回はパスワードを利用しないので、いずれを選択しても問題ありません）
  - ✓ [ログインパスワードを利用] : UAへのログインパスワードを利用
  - ✓ [UAでパスワードを入力] : UA画面内でパスワードを入力
  - ✓ [パスワードを保存しない] : 構成プロファイルのインストール時にパスワードを

要求されるので入力

- [iOS4互換のフォーマットを試用しない]にチェック

設定が終わったら、 [保存]をクリックします。

パスワード認証なしでEAS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。



7. iPhone での操作（EAS）

7.1. Gléas の UA からのインストール

iPhone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、[ダウンロード]をタップし、構成プロファイルの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

※UAの設定で[UAでパスワードを入力]を選択した場合は、EASのパスワード入力を求められるので、適当な文字列を入力します（実際は利用しない）

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。

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。

※UAの設定で[パスワードを保存しない]を選択した場合は、EASのパスワード入力を求められるので、そのまま[次へ]をタップします

デバイスパスコードを設定している場合は、入力を求められます。
パスコード強制が構成プロファイルに含まれていて、デバイスにパスコードを設定していない場合は、以下の画面が出現しパスコードの設定を求められます。

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からログアウトします。
以上で、iPhoneでの構成プロファイルのインストールは終了です。

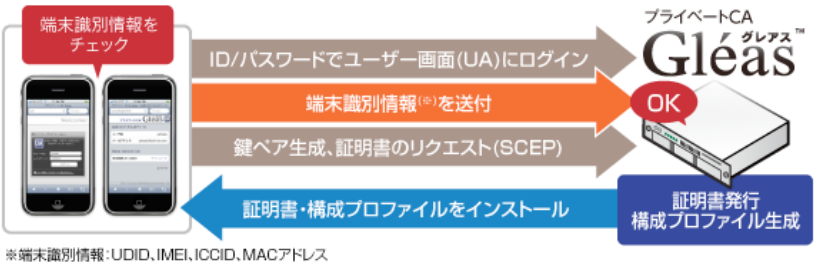
なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可となります。

7.2. EAS の利用

インストールした構成プロファイルにより、アクセス先の設定や、認証に利用するクライアント証明書は既にiPhoneにインストールされていますので、メールアプリケーションよりActiveSyncによるアクセスが可能となっています。

7.3. 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。

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