



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

～FirePass連携～

iPhoneでクライアント証明書を利用した

Microsoft Exchange ActiveSync連携設定手順

Ver.0.9

2010年8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
iPhone でクライアント証明書を利用した Microsoft Exchange ActiveSync 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. FIREPASS 側の設定	5
2.1. 電子証明書に関する設定	5
2.2. ランディング URI の設定	6
2.3. マスターグループの作成	6
2.4. マスタグループ用のパターンベースバイパスの指定	8
2.5. ダイナミックグループマッピング	9
3. GLÉAS の管理者設定	10
3.1. UA (ユーザ申込局) 設定	10
4. IPHONE での構成プロファイル・証明書のインストール	12
4.1. GLÉAS の UA からのインストール	12
4.2. EXCHANGE ACTIVESYNC の利用	14
5. 問い合わせ	16

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で生成したiPhone用の構成プロファイルを利用して、クライアント証明書認証により、F5 Networks社製FirePassを経由してMicrosoft Exchange ActiveSyncを行う環境を構築するための設定例を記載します。

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。

- F5 Networks FirePass Virtual Edition (バージョン7.0.0)
※以後、「FirePass」と記載します
- JS3 プライベートCA Gléas (バージョン1.7 ベータ版)
※以後、「Gléas」と記載します
- Microsoft Windows Server 2008 R2 Standard / Exchange Server 2010
- iPhone 3GS (iOS 4.0)
※以後、「iPhone」と記載します
※Microsoft Exchange ActiveSyncは以後、「Exchange ActiveSync」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。

- Microsoft Windows Server 2008 R2、Active Directoryのセットアップ
- Exchange Server 2010のセットアップ (ActiveSync設定を含む)
- FirePassのネットワーク設定やリソース設定等の基本設定
- 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

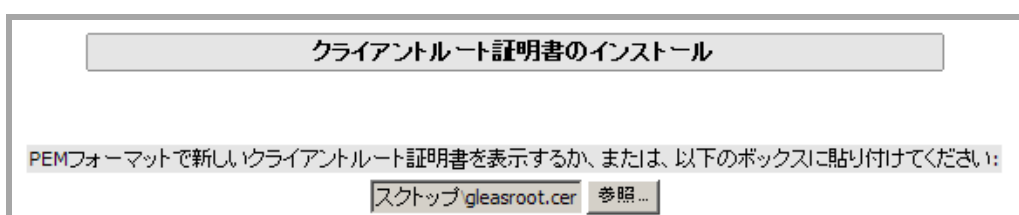
これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

2. FirePass側の設定

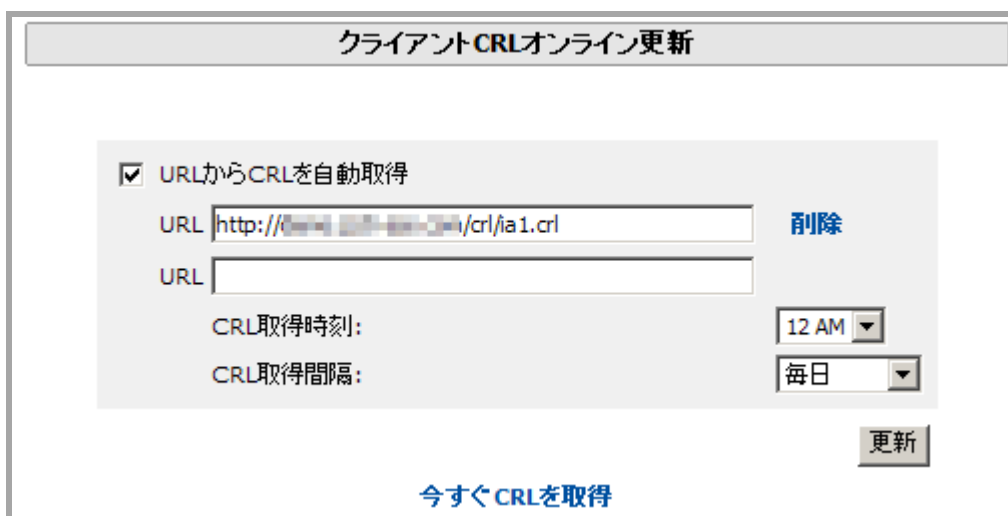
2.1. 電子証明書に関する設定

メニューより[デバイス管理]、[セキュリティ]、[証明書]と進み、右側の[クライアントルート証明書と CRL のインストール]中の[クライアントルート証明書]をクリックします。

[クライアントルート証明書のインストール]にプライベート CA Gléas よりダウンロードしたルート証明書ファイル（PEM フォーマット）を選択し、最下部の[証明書のインストール]ボタンをクリックし、ルート証明書をインポートします。



失効リストを参照する場合は、[証明書]の画面まで戻り、[クライアント CRL オンライン更新]に CRL 配布ポイントを記載します。

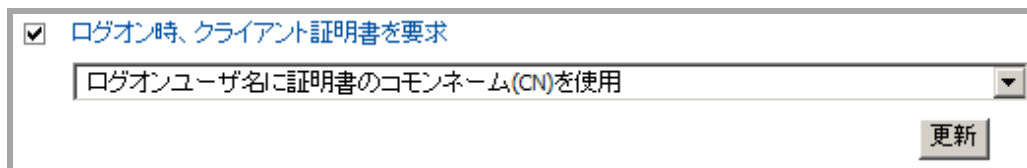


上記は CRL 配布ポイントとして設定された URL から、毎日 0 時に CRL を取得する設定例です。

また、iPhone のアクセス時に FirePass よりクライアント証明書を要求させるために以下の設定が必要となります。

[証明書]の画面で、[ログオン時、クライアント証明書を要求]をチェックし、[ログオンユーザ名に証明書のコモンネーム (CN) を使用]を選択し、[更新]をクリックしま

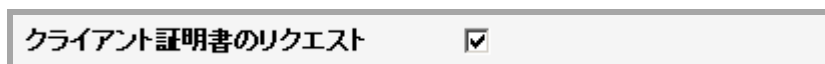
す。



ログオン時、クライアント証明書を要求
ログオンユーザ名に証明書の共通名前(CN)を使用
更新

右側のメニューより[デバイス管理]、[設定]、[ネットワーク設定]と進み、右側のタブで[ウェブサービス]タブを選択します。[WEB サーバ設定]でクライアント証明書認証を必要とさせるサイトの[設定(Configure)]をクリックし、次の画面で以下の設定を行います。

- [クライアント証明書のリクエスト]をチェック



クライアント証明書のリクエスト

2.2. ランディング URI の設定

メニューから[デバイス管理]、[カスタマイズ]と進み、右側のタブで[URIベースカスタマイズ]を選択し以下の設定を行います。

- [ランディングURIの作成]テキストボックスに以下を入力
Microsoft-Server-ActiveSync
- [ActiveSync認証]オプションを選択し、[適用]をクリック



新しいランディングURI:
ランディングURIを作成: Microsoft-Server-ActiveSync
 フォームベース認証
 ActiveSync認証
適用

2.3. マスターグループの作成

メニューから[ユーザ]、[グループ]、[マスターグループ]と進み、右側で[新しいグループを作成]をクリックし、以下の設定を行います。

- [新しいグループ名]テキストボックスに任意のグループ名を入力
- [グループのユーザ]は[外部]を選択

※[ローカル]にする場合はFirePass内部にユーザを作成する必要があります

- [認証方法]は[クライアント証明書(パスワード無し)]を選択

グループ管理

新しいグループを作成

新しいグループ名:	<input style="width: 90%;" type="text" value="sample"/>
グループのユーザ:	<input style="width: 90%;" type="text" value="外部"/>
認証方法:	<input style="width: 90%;" type="text" value="クライアント証明書(パスワード無し)"/>
ルーティングテーブル:	<input style="width: 90%;" type="text" value="main"/>
以下から設定をコピー:	<input style="width: 90%;" type="text" value="コピーしない"/>

上記設定後、[作成]ボタンをクリックし、遷移した [全体]タブ画面で以下の設定を行います。

- [ダイナミックマスタグループマッピングを使用して、このマスタグループにユーザがアサインされることを許可]をチェック

その後、[認証]タブを選択し、以下設定を行います

- [クライアント証明書が提示されたとき、自動的にログイン]をチェック
- [必要なクライアント証明書発行者]で、2.1項でインポートしたルート証明書を選択

ここまでの設定でクライアント証明書認証が有効になりますが、Active Directory (AD) 連携において追加チェックを設定することができます (オプション)。

以下は、クライアント証明書のCN (プライベートCA Gléasにおけるアカウント名) がAD内のユーザとして実在するか否かをチェックする設定例となります。

- [クライアント証明書に対して追加のチェックを行う]の項目を[アクティブディレクトリ]に設定
- [比較に使用するクライアント証明書のサブジェクトフィールド]に[クライアント証明書の共通名 (CN)]に設定
- [検証方法]を[アクティブディレクトリにて検出されたユーザ]に設定
- [検証に使用するアクティブディレクトリ属性]に「sAMAccountName」 (Windows 2000以前の互換ログオン名) を入力
- [アクティブディレクトリ設定]にドメインコントローラにアクセスするための情報を入力

クライアント証明書パスワード無しの認証

[認証方法の変更 >>](#)

クライアント証明書が提示されたとき、自動的にログイン

クライアント証明書 common name (CN) フィールドをログオンユーザ名に対して確認

必要なクライアント証明書発行者:

クライアント証明書に対して追加のチェックを行う

比較に使用するクライアント証明書のサブジェクトフィールド

検証方法

検証に使用するアクティブディレクトリ属性

(例: sAMAccountName, displayName, mail)

アクティブディレクトリ設定

ドメイン名:	<input type="text" value="example.local"/>
フォレストモード:	<input type="checkbox"/>
Kerberosサーバ名 (オプション):	<input type="text"/>
WINSサーバIPアドレス(オプション):	<input type="text"/>
ドメイン管理者名:	<input type="text" value="administrator"/>
ドメイン管理者パスワード:	<input type="password" value="....."/>

2.4. マスタグループ用のパターンベースバイパスの指定

メニューから[ポータルアクセス]、[Webアプリケーション]、[マスタグループ設定]と進み、右側で2.3項で作成したマスタグループを選択し、[最小限のコンテンツ書き換えバイパス]まで移動し、以下の設定を行います。

- [パターンの、コンマ区切りリスト]の左側のテキストボックスに、以下を入力
/Microsoft-Server-ActiveSync*

- 右側のテキストボックスには、Exchangeサーバのアドレスを指定
- [追加]ボタンをクリック

最小限のコンテンツ書き換えバイパス

代替ホスト/ポートベース
バイパスWebサービスが設定されていません。
[ここをクリックして設定](#)

パターンベース

パターンの、コンマ区切りリスト http[s]://<IP Address/Name>[:Port]

/Microsoft-Server-ActiveSync*	%	https://[redacted].local	%	追加
-------------------------------	---	--------------------------	---	----

2.5. ダイナミックグループマッピング

メニューから[ユーザ]、[グループ]、[ダイナミックグループマッピング]と進み、右側で[グループマッピングシーケンス]タグを選択します。

[マスターグループマッピングシーケンス]のところの[マスタグループマッピングテーブル]を使用してユーザのマスタグループを動的に決定]をチェックします。

その後、[マスターグループマッピングテーブル]タグを選択し、[マッピング方法]で[クライアント証明書]を選択し、[追加]ボタンをクリックします。

[属性]欄にマッピングを行いたいクライアント証明書の属性を選択し、[値]欄にマッピングを行う証明書属性を入力し、[FirePassグループ]に先ほど作成したマスターグループを設定します。

マスタグループマッピングテーブル

クライアント証明書属性をFirePassグループにマップ

属性	同一名をマップ	値	FirePassグループ
Subject Distinguished Name (DN) substring ▼	<input type="checkbox"/>	OU=sample	sample ▼

上記では、クライアントより提示された証明書のサブジェクトに「OU=sample」という項目があれば、FirePassの「sample」マスターグループに割り当てられる設定例になります。

以上でFirePassの設定は終了です。

3. Gléas の管理者設定

Gléas で、発行済みのクライアント証明書を含む Exchange ActiveSync 設定（構成プロファイル）を iPhone にインポートするための設定を本章では記載します。

※なお、画面は 2010 年 8 月現在開発中のものであり、実際のものとは異なる可能性があります

※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、iPhone用となるUA（申込局）をクリックします。

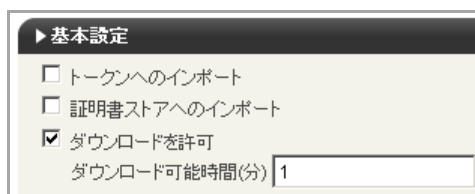


上記の場合は、iPhone用UAと記載のあるものをクリックします。

[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。



[トークン情報]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

プライベート CA Gléas ホワイトペーパー
iPhone でクライアント証明書を利用した Microsoft Exchange ActiveSync 連携設定手順

定を行います。

- [iPhone用レイアウトを利用する]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、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）
- [Exchangeホスト名]にアクセス先となるFirePassのホスト名（FQDN）を入力
- [署名用証明書]に構成プロファイルに署名するための署名用証明書（PKCS#12ファイルのパス、及び保護パスワード）を入力

The screenshot shows the 'iPhone/iPad の設定' (iPhone/iPad Settings) screen. It is divided into several sections:

- iPhone/iPad 用 UA を利用する**: A checkbox is checked.
- 画面レイアウト**: A checkbox for 'iPhone 用レイアウトを使用する' is checked.
- iPhone 構成プロファイル基本設定**:
 - 名前(デバイス上に表示): プライベートCA Gléas
 - 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: iPhone 用の構成プロファイル
 - 削除パスワード: (empty)
- Microsoft Exchange(ActiveSync)の設定**:
 - Exchange ホスト名: firepass-name.example.com
- 署名用証明書**:
 - 証明書ファイル(PKCS#12): (empty) with a '参照...' (Browse...) button.
 - PKCS#12 のパスワード: (empty)

A '保存' (Save) button is located at the bottom center of the screen.

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。

設定を反映させるために、UAのアプリケーションサーバの再起動を行ってください。

4. iPhone での構成プロファイル・証明書のインストール

4.1. 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



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

プライベート CA Gléas ホワイトペーパー
iPhone でクライアント証明書を利用した Microsoft Exchange ActiveSync 連携設定手順

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。

※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 iPhone でクライアント証明書を利用した Microsoft Exchange ActiveSync 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、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能となります。



4.2. Exchange ActiveSync 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FirePassの設定や、認証に

プライベート CA Gléas ホワイトペーパー
iPhone でクライアント証明書を利用した Microsoft Exchange ActiveSync 連携設定手順

利用するクライアント証明書やユーザID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Exchange ActiveSyncによるアクセスが可能となっています。

クライアント証明書によるセキュアな接続をお試してください。

5. 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。

■FirePassに関するお問い合わせ先

F5ネットワークスジャパン株式会社

Tel: 03-5114-3210

URL : <http://www.f5networks.co.jp/fc>

(上記URLのお問い合わせフォームよりご連絡ください。)

■Gléasに関するお問い合わせ先

株式会社JCCH・セキュリティ・ソリューション・システムズ

Tel: 03-5615-1020

Mail: support@jcch-sss.com