JCCH・セキュリティ・ソリューション・システムズ

プライベート認証局Gléas ホワイトペーパー

BlackBerry WorkでのExchange ActiveSyncにおける クライアント証明書認証（BlackBerry UEM連携）

Ver. 1.0
2018 年 9 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品 プライベート認証局Gléas と、BlackBerry社の提供するモバイルデバイス管理サービス BlackBerry UEM、およびグループウェアのクライアントアプリである BlackBerry Work とを連携させて、Exchange ActiveSync 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

本書は、以下の環境で検証をおこなっております。

- Microsoft Exchange Server 2010 SP2 RU8
  ※以後、「Exchangeサーバ」と記載します
- モバイルデバイス管理：BlackBerry UEM 12.8.1
  ※以後、「BB UEM」と記載します
- 認証局：JS3 プライベート認証局Gléas（バージョン1.16.9）
  ※以後、「Gléas」と記載します
- クライアント：iPad Air2（iOS 11.4.1）/ BlackBerry Work 2.13.1.3713
  ※以後、「iPad」と記載します。またBlackBerry Work は以後、「BB Work」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。

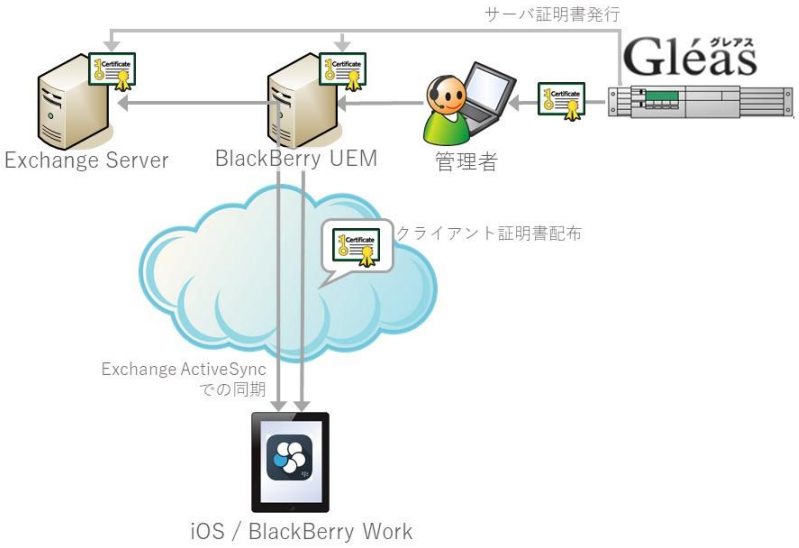
- Exchangeサーバの基本設定、およびクライアント証明書マッピング認証の設定方法
  ※クライアント証明書マッピング認証の設定について、弊社では以下のURLでホワイトペーパーを公開しています。本書では、事前にExchange Serverでクライアント証明書マッピング認証だけが有効にされていることを前提にしています
  https://www.gleas.jp/news/whitepaper/exchange-server
- BB UEMの導入、及びBB Workでパスワード認証によるExchange ActiveSyncをおこなうための設定

- Gléasの基本操作
- iPadの基本操作

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. ExchangeサーバおよびBB UEMに対しSSLサーバ証明書をGléasより発行し、設定する
   ※Exchangeサーバへの SSLサーバ証明書の設定方法は本書では説明を省略します。前項記載のホワイトペーパーをご参照ください
2. 管理者はGléasよりクライアント証明書（PKCS12ファイル）をダウンロードし、そのファイルをBB UEMにアップロードする
   （BB UEMのユーザアカウントに証明書を紐づける）
3. BB Workで初回ログインする際に、BB UEMよりその証明書が配布される
4. Exchangeサーバにクライアント証明書による認証を経てActiveSync接続をおこなう

1.4. 留意事項

Gléasで発行する証明書には以下が含まれなければならず、その通りに証明書発行テンプレートが構成されている必要があります。

【サーバ証明書（BlackBerry Dynamicsサーバ証明書）】

- ホスト名（サブジェクトのCN、およびサブジェクトの代替名（DNS名）フィールド）

【クライアント証明書】

- Active Directoryのユーザプリンシパル名(サブジェクトの代替名フィールド)
- CRL（失効リスト）配布ポイント

2. Gléas からの証明書ダウンロード

2.1. サーバ証明書・クライアント証明書

Gléas の管理画面（RA）にログインし、あらかじめ発行したサーバ証明書とクライアント証明書をダウンロードします。

※以下のスクリーンショットはクライアント証明書の例となりますが、サーバ証明書でも同じ手順です

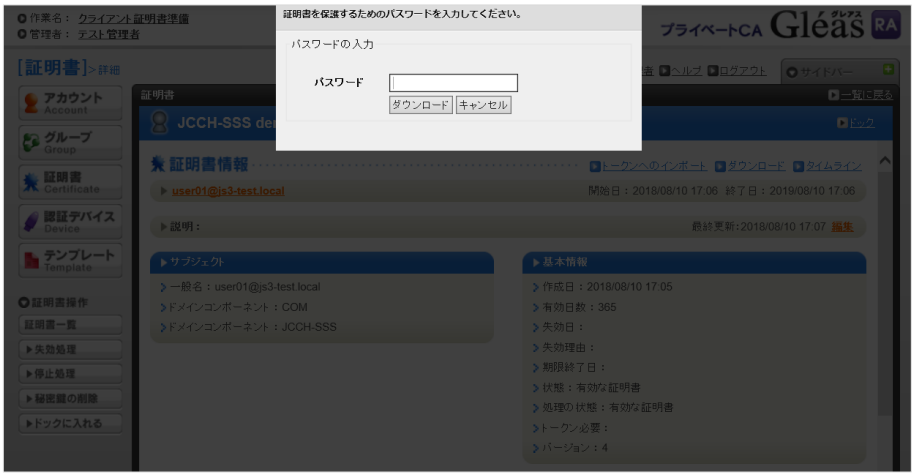
大メニュー[アカウント]から該当のアカウントを検索します。(検索ボックスを使うと便利です)

「証明書発行の履歴」から発行済みの証明書をクリックします。

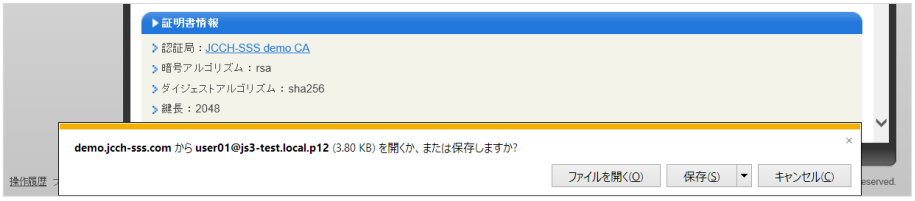
証明書の詳細ページに遷移するので、[ダウンロード]リンクをクリックします。

「証明書を保護するためのパスワードを入力してください」と表示されますので、パスワードを設定します。

※クライアント証明書の場合は、このパスワードを iPad の利用ユーザに通知します

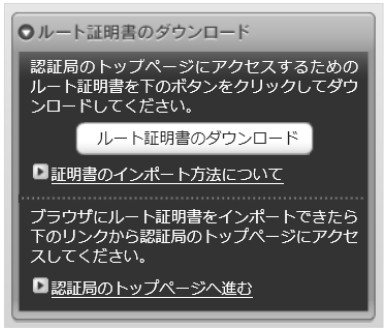


パスワード設定後にファイルのダウンロードが始まるので適当な場所に保存します。



2.2. ルート証明書

Gléas に http://hostname/ （http であることに注意）でアクセスすると、ルート証明書のダウンロードが可能です。
BB UEM 側の設定で必要になるのでダウンロードしておきます。



Gléas での操作は以上です。

3. BB UEM での設定

3.1. SSL関連設定

BB UEM が Exchange Server に対し SSL アクセスする際に必要となるルート証明書を設定します。

BB UEMのWeb管理コンソールにログインし、[設定] > [外部統合] > [信頼された証明書]と進み、[Exchange ActiveSyncサーバの信頼]の右側にある[+]をクリックし、[証明書ファイル(.cer、.der)]に2.2項で保存しているルート証明書をアップロードします。

アップロードが完了すると、以下の通り表示されます。

次に、BB WorkがBB UEMに対しSSLアクセスする際のサーバ証明書をデフォルトのものからGléasで発行したものに変更します。

Web管理コンソールにて、[設定] > [インフラストラクチャ] > [サーバ証明書] > [BlackBerry Dynamics証明書]タブに進み、[SSL/TLS証明書]の[BlackBerry Dynamicsサーバの証明書]の[詳細を見る]をクリックして表示を展開させ、[証明書を置き換える]をクリックし以下を設定します。

- [証明書ファイル(.pfx or .p12)]には、2.1項でダウンロードしたサーバ証明書ファイルを指定
- [パスワード]は、2.2項でダウンロードの際に設定したパスワードを入力
- [再起動日]は、サービス再起動する日時を指定（入れ替える証明書を有効にするにはサービスの再起動が必要）

サービス再起動が完了すると、以下のように表示されます。

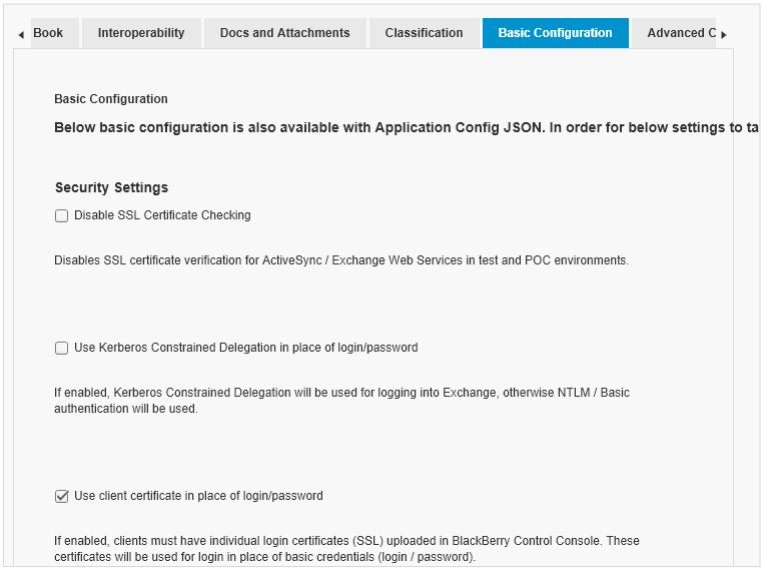
3.2. BB Workの設定

Web管理コンソールにて、[アプリ] > [アプリ] > [BlackBerry Work]をクリックします。

[設定]タブ ＞ [ユーザ証明書]の「BlackBerry Dynamicsアプリがユーザ証明書を使用することを許可する」をチェックします。

またそのページの[アプリ設定]のGood Default Policyをクリックし、アプリ設定の[Basic Configuration]タブで以下を設定します。

- [Security Settings]の「Use client certificate in place of login/password」にチェックを入れる



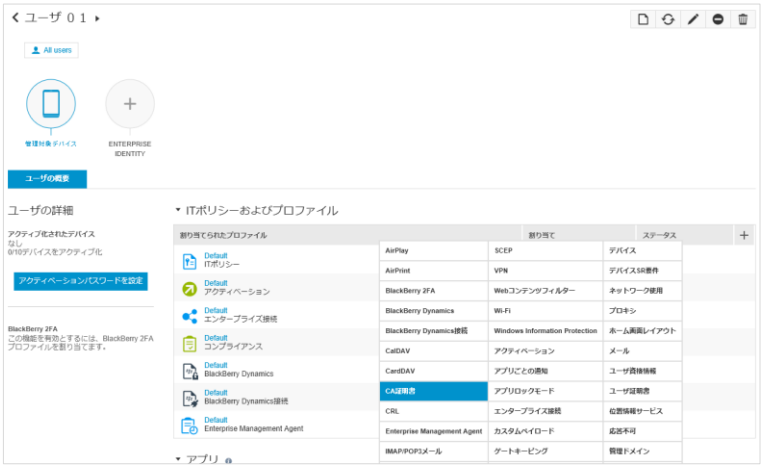
3.3. クライアントへの証明書配布設定

Web管理コンソールにて、[ポリシーとプロファイル] > [Managed devices] > [Certificates] > [CA Certificate]と進み、検索ボックスの右にある[+]をクリックし、以下を設定します。

- [名前]には、任意の識別名称を入力
- [証明書ファイル(.der、.cer、.key、.pem、.crl)]には、2.2項でダウンロードしたルート証明書を指定

設定完了後、[追加]をクリックします。

その後、[ユーザ] > [すべてのユーザ]と進み、クライアント証明書を設定するユーザアカウントを選択し、[ITポリシーおよびプロファイル]の表内にある[+]をクリックし、[CA証明書]をクリックします。



作成済みのCA証明書プロファイルを指定し、[割り当て]をクリックします。

次に、[ITポリシーおよびプロファイル]の表内にある[+]をクリックし、[ユーザ証明書]を選択します。

「ユーザ証明書を追加」ポップアップが表示されるので以下を設定し、[追加]をクリックします。

- [名前]には、任意の名称を入力
- [証明書を適用する]には、[BlackBerry Dynamics対応デバイス]
- [証明書ファイル(.pfx or .p12)]には、2.1項でダウンロードしたクライアント証明書ファイルを指定

元のページに戻りページ更新をすると、以下の通りルート証明書（CA証明書）とクライアント証明書（ユーザ証明書）が追加されたことが分かります。

BB UEMの設定は以上です。

4. iPad での操作

4.1. BB Workの起動

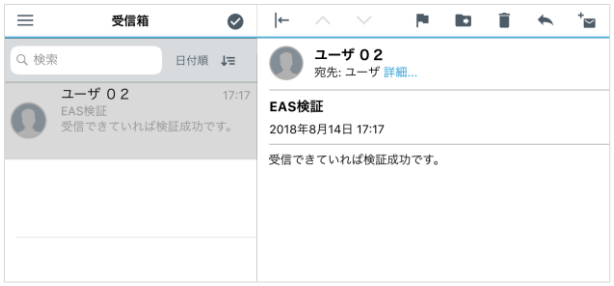
iPadでBB Workを起動します。

初回起動時に、BB UEMに登録されたメールアドレスとアクセスキーを入力し、アクティブベーションをおこないます。

アプリケーションのパスワード設定後に、クライアント証明書のインポートを促されますので、2.1項で設定した保護パスワードを入力します。

成功すると以下のメッセージが表示されます。

ランチャーが表示されれば、接続に成功しておりExchangeサーバ上のメールなどにアクセスがおこなえます。



クライアント証明書が失効されると、以下のような表示になります。
※失効情報がExchangeサーバに伝搬されている必要があります

5. 問い合わせ

■BlackBerry製品に関するお問い合わせ先
BlackBerry Japan株式会社
TEL：　03-6867-1799
URL：　https://jp.blackberry.com/

■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: 050-3821-2195
Mail: sales@jcch-sss.com