

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

- 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

Copyright by JCCH Security Solution Systems Co., Ltd. All Rights reserved

目次

1. はじる	かに	
1.1.	本書について	
1.2.	本書における環境4	
1.3.	本書における構成	,
1.4.	留意事項5	,
2. Gléas	っからの証明書ダウンロード6	
2.1.	サーバ証明書・クライアント証明書6	j
2.2.	ルート証明書8	, ,
3. BB U	EM での設定8	
3.1.	SSL 関連設定8	5
3.2.	BB Work の設定)
3.3.	クライアントへの証明書配布設定11	
4. iPad	での操作13	
4.1.	BB Work の起動13	
5. 問い1	合わせ15	,

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。



iOS / BlackBerry Work

- 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。

6-65-1-1							6	
リワント」>詳細				▶ 認証局	09201	管理者 国ヘルズ 国口(17.01	•サイドバー
アカウント Account			_			_	_	<u>ت ا</u>
グループ	ser01@js3-test.loc	al						D
Group 👱 꾿	カウント情報・・・・・		•••• 🖸 改訂履歴	🚱 グル	レープ情報	暇		
証明書 Certificate トユー	ーザ	登録日時:20	018/08/10 17:00) -1-	ザグループ			▶参加
8証デバイス Device	9ス:有効			≯なし				
テンプレート	- ザ属性	最終更新:2018/08	3/10 17:00 <u>福集</u>	► □	レグループ			▶ 參加
emphate > 姓 > 名 > ソレー語	: user : 01 - ルアドレス :			> <u>70</u>	-バルグル-	<u>-7</u>		
	スワード:****************							
	^{スワード:************************************}							
	マワード:************************************	·····						
り フ ト ー 属	ローF: ************************************	開始	有効期限	ステータス	失効日		秘密鍵	格納状況
	ロード: 明書発行の履歴 ICCH-SSS demo CA シリアルレ 11571 (00:00:2d:33)	開始 2018/08/10	有効期限 2019/08/10	ステータス 有効	失効日	磁号種別 rsa2048(sha256)	秘密鍵 。	格納状況
	RワーF: 明書発行の履歴 ICCH-SSS demo CA シリアル 11571 (00.00.2d:33) ンブレート情報	時始 2018/08/10	有効期限 2019/08/10	ステータス 有効	失効日	暗号種別 rsa2048(sha256)	秘密鍵 。	格納状況
	R7-F: 明書発行の履歴・・・ ICCH-SSS demo CA シリアル 11571 (00.00.2d.33) ンプレート情報・・・ ジスク	開始 2018/08/10	有効期限 2019/08/10	ステータス 有効	失効日	曜号 種別 rsa2048(sha256)	秘密鍵	格納伏況
Pill and mathematical systems Pill and mathematical systems	RワーF: 明書発行の履歴・・・ ICCH-SSS demo CA シリアル 11571 (00.00.2d 33) ンプレート情報・・・ ジスク 権別	₩% 2018/08/10	有効期限 2019/08/10	ステータス 有効 必須テンプ	失効日	暗号 種別 rsa2048(sha256)	 秘密鍵 ○ 	格納伏況
	R7-F: 明書発行の履歴・・・ ICCH-SSS demo CA シリアル 11571 (00:00:2d33) ンプレート情報・・・ ジジェ外 産別 一般名(CN	M3%6 2018/08/10	有効期限 2019/08/10 user01@js	ステータス 有効 必須テンプ 3-test local	<u>失効日</u> レート	禮导種別 rsa2048(sha256)		
フトド編) 中国会一覧 中国会一覧 クト版版作成 単語会一覧 ・1 第 第 第 ・1 ・1 ・1 ・1	87-F:: 明書発行の履歴・・・ ICCH-SSS demo CA シリアル 11571 (00.00.2d.33) ンプレート情報・・・ ジェク・ 経知 一般名(CN ドメインコンボーキ:	► PASS 2018/08/10	有効期限 2019/08/10 user01@js CCM JCCH-SSS	ステータス 有効 必須テンプ 3-test local	失効日 レート	輕号 佳 別 rsa2048(sha256)	- 松密鍵 C C C C C C C C C C C C C C C C C C C	格納状況

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。

 ○ 作業名: <u>クライアント 証明書準備</u> ○ 管理者: <u>テスト 管理者</u> 	プライベートCA Gléäs RA
[証明書]>###	● 認証局 ● ログ ● 管理者 ● ヘルブ ● ログアウト ● サイドバー ● □ 二 知道民る
▲ Account ② JCCH-SSS demo CA#11571 ② Group ※ 証明書情報 ▶ user01@js3-test.local	
● 認証デバイス Device	最終更新:2018/08/10 17:07 <mark>攝集</mark>
 ▶ サブジェクト ▶ サブジェクト > 一般名: user01@js3-test local > ドメインコンボーネント: COM > ドメインコンボーネント: JCCH-SSS ▶ ドメインコンボーネント: JCCH-SSS ▶ ドックに入れる 	 ▶ 基本情報 * 作成日:2018/08/10 17:05 > 有効日数:365 > 失効日: > 失効理由:: > 朝現長了日: > 状態:有効な証明書 > 処型の状態:有効な証明書 > トークン必要: > パージョン:4
 ▶ 証明書情報 > 認証局: JCCH-SSS demo CA > 暗号アルゴリズム: rsa > ダイジェストアルゴリズム: sha256 > 鍵長: 2048 > 鍵用途: 電子署名 謎の暗号化 	~

「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。

		▶証明書情報	L
		 > 認証局: JCCH-SSS demo CA > 暗号アルゴリズム:rsa > ダイジェストアルゴリズム:sha256 > 離長: 2048 	
	demo.jcch	ss.com から user01@js3-test.local.p12 (3.80 KB) を開くか、または保存しますか? ×	l
<u>操作履歴</u> フ		ファイルを開く(Q) 保存(S) ▼ キャンセル(C) eserve	d.

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。

Exchange Ac	iveSyncサーノ	(の信頼を追)	加		
手順1/3:メールサーバ メールサーバ証明書を	E明書をエクスポートし (509形式(* cer. * der	します)でエクスポートしま	ة .		
		,,			
手順2/3:証明書を格釈 管理コンソールから3	ノます クヤスできろネットロ	ークトの場所に証明書	を格納します。		
手順3/3:メールサーパ	正明書をアップロードし	します アにインポートします			
ノアイルの場所を影響	し、証明書をキースト	7121 211-1089	0		
説明					
説明 Gleas CA					
説明 Gleas CA					
武明 Gleas CA					
説明 Gleas CA 証明書ファイル(.cer、	er)*				
説明 Gleas CA 証明書ファイル(.cer、 ia1.cer	er)*	参照	削除		
説明 Gleas CA 証明書ファイル(.cer、 ia1.cer	er)*	参照	削除	•	
説明 Gleas CA 証明書ファイル(.cer、 ia1.cer	er)*	参照	削除		

•	有効期限の日付 1月 07,2030	
H.	說明 Gleas CA	
	ステータス 有効	
	キーストア名 CACERTS	
	エイリアス mail_server_ae2fd999-1721-4369-b5b0-8da773c34307	
	サブジェクト DC=JCCH-SSS,DC=COM,CN=JCCH-SSS demo CA	
	発行者 DC=JCCH-SSS, DC=COM, CN=JCCH-SSS demo CA	
	削除	
	詳細を非表示	

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)

有効にするにはサー八の再起動か必要 説明			
Issued by Gleas			$\hat{}$
証明書ファイル(.pfx or .p12)*			
bbuem.js3-test.local.p12		参照	削除
バスワード			
••••	۲		
再起動日*			

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。



	BlackBerry Dynamicsサーバの証明書
Ŷ	説明
	Issued by Gleas
	有効期限
	2030年1月6日 12:04:45
	ステータス
	有効
	エイリアス
	ssl
	サブジェクト
	DC=JCCH-SSS, DC=COM, CN=bbuem.js3-test.local
	サブジェクトの別名
	DNSName=bbuem.js3-test.local,DNSName=192.168.20.198
	発行者
	DC=JCCH-SSS, DC=COM, CN=JCCH-SSS demo CA
	証明書を置き換える
	デフォルトに戻す
	詳細を閉す

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。

ユーザ延期書 ② BlackBerry Dynamicsアプリがユーザ証明書を使用することを許可する						
	キャンセル	保存				

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

•	Book	Interoperability	Docs and Attachments	Classification	Basic Configuration	Advanced C 🕨
	Basi	c Configuration				
	Belo	ow basic configura	tion is also available with	Application Cor	nfig JSON. In order for	below settings to ta
	Sec	urity Settings				
		isable SSL Certificate	Checking			
	Disa	bles SSL certificate ver	ification for ActiveSync / Exchan	nge Web Services in	test and POC environments	
	<u> </u>	lse Kerberos Constrain	ed Delegation in place of login/	password		
	If en auth	abled, Kerberos Constr entication will be used.	ained Delegation will be used fo	or logging into Exchai	nge, otherwise NTLM / Basic	3
	v 1	lse client certificate in p	place of login/password			
	lf en: certif	abled, clients must hav icates will be used for I	e individual login certificates (St ogin in place of basic credential	SL) uploaded in Blacl Is (login / password).	Berry Control Console. The	se

10 / 15

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

12.01				
demoCA				
説明				
証明書ファイル(.der、.cer、.k	ey, .pem, .crt) *	44.000	11100	
ia1.cer		参照	削除	
証明書のサブジェクト				
1200 (0)				
利益40万円70月70月10日 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)				
BlackBerry	i0\$	macOS	Android	Windows
適用先:				
適用先: *CA証明書をBlackBerryデバイ	スに送信するには、これら	のオプションが1つ以上	こ必要です。	
適用先: *CA証明書をBlackBerryデバイ. □ ブラウザー証明書ストア	スに送信するには、これら 7	のオプションが1つ以上	上必要です。	
道 用先: *CA証明書をBlackBenyデバイ. □ ブラウザー証明書ストア □ VPN証明書ストア	スに送信するには、これら 7	のオプションが1つ以上	心要です。	

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。

< ユーザ 0 1 ▶				00	/ 0	Û
VENR FACA						
ユーザの戦変 ユーザの詳細	 ITポリシーおよびプロファイル 					
アクティブ化されたデバイス なし	割り当てられたプロファイル		創り当て	ステータス		+
0/10テバイスをアクティブ化	Default ITポリシー	Aannay	SCEP	7/12		
アクティペーションパスワードを設定	O Default	AirPrint	VPN	デバイスSR世作		
	アクティベーション	BlackBerry 2FA	Webコンテンツフィルター	ネットワーク使用		
	Cefault エンタープライズ接続	BlackBerry Dynamics	Wi-Fi	プロキシ		
BlackBerry 2FA この機能を有効とするには、BlackBerry 2FA	Default	BlackBerry Dynamics接続	Windows Information Protection	ホーム画面レイアウト		
プロファイルを割り当てます。		CalDAV	アクティベーション	メール		
	BlackBerry Dynamics	CardDAV	アプリごとの通知	ユーザ資後情報		
	Default BlackBarry Dynamics2848	CALEME	アプリロックモード	ユーザ証明書		
		CRL	エンタープライズ接続	位置協戦サービス		
	Enterprise Management Agent	Enterprise Management Agent	カスタムペイロード	龙芒不可		
	 アプリ a 	імар/рорзж—л	ゲートキービング	管理ドメイン		

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。

CA証明書ブロファイルを割り当て	8	
CA証明書プロファイル・ demoCA マ		
- 選択 -		
demoCA 割り当て		

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。

く ユーザ 0 1 ▶					0 1
1 All users					
+					
★課社会 デパイス ENTERPRISE IDENTITY					
ユーザの概要					
1ーザの詳細	 ITポリシーおよびプロファイル 				
クティブ化されたデバイス	割り当てられたプロファイル		割り当て	ステータス	
い 10デバイスをアクティブ化	Default	AirPlay	SCEP	デバイス	
man of a state state.	III ITポリシー	AirPrint	VPN	デバイスSR要件	
アクティハーションバスワードを設定	Default アクティペーション	BlackBerry 2FA	Webコンテンツフィルター	ネットワーク使用	
	Default	BlackBerry Dynamics	WS-Fi	プロキシ	
ackBerry 2FA		BlackBerry Dynamics接続	Windows Information Protection	ホーム画商レイアウト	
のWeiを行わこう Solid、DeckDelly ZFA ロファイルを割り当てます。	コンプライアンス	CalDAV	アクティベーション	メール	
	BlackBerry Dynamics	CardDAV	アプリごとの遊知	ユーザ資格情報	
			771104/75-5	コーザ研究者	
	Default	CARMS	77907761		
	Default BlackBerry Dynamics狠扺	CRL	エンタープライズ接続	位置情報サービス	

「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。

▼ ITポリシーおよびプロファ	イル				
11/100 008-0000000	170				
割り当てられたプロファイル			割り当て	ステータス	+
Default πポリシー			◎ デフォルト		
Default アクティベーション			◎ デフォルト		
Cefault Cefault エンタープライズ接続			◎ デフォルト		
Default コンプライアンス			◎ デフォルト		
BlackBerry Dynamics			◎ デフォルト		
Default BlackBerry Dynamics接続			◎ デフォルト		
Default Enterprise Management Agent			◎ デフォルト		
emoCA CA証明書			1 ユーザ		×
user01 user certificate 1 ユーザ証明書			೨ ⊐−ザ		×
▼ アプリ ₀					
割り当てられた ▲ OS	種別	アプリごとのVPN	アプリ設定	割り当て基準	+
		割り当てなし			
▼ ユーザ証明書					
名前	デバイス	用途	デプロイされたアプリ	有効期限 更新	削除
user01 user certificate 1					×

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。

SlackBerry	
	通信を保護しています
	通信が保護されました
	ポリシーを取得しています
エンタ-	ープライズアクティベーション完了
	資格を確認しています

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。

*** Black	Berry
	クライアント証明書 user01@js3-test.local.p12 管理者が提供したパスワードを入力してください。
	••••
	キャンセル OK

成功すると以下のメッセージが表示されます。

₩ Bla	ckBei	<i>m</i> y
	*	クライアント証明書 user01@js3-test.local.p12 管理者が提供したパスワードを入力してください。
	•••	•
		キャンセル OK
		成功 個人証明書は正常にインポートされ ました。
		ОК
		ок

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。

☰ 受信箱		⊘	←	\sim	\sim	12	Î	+	+
Q. 検索	日付順	¢≡	0	ユー 宛先:	ザ 0 2 ユーザ 詳	細			
ユーザ 0 2 EAS検証 受信できていれば社	検証成功です	17:17 す。	EAS材 2018年 受信で	€証 ≅8月14 きていね	日 17:17 れば検証成	成功です。			

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

三 受信箱 📀	
Q. 検索 日付順 ↓=	ユーザ 02 宛先: ユーザ 詳細
ユーザ02 火曜日 EAS検証 受信できていれば検証成功です。	EAS検証 2018年8月14日 17:17
	受信できていれば検証成功です。
72	7セスが開止されています。 OK

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