

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

- 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。

目次

1. はじる	めに	4
1.1.	本書について	4
1.2.	本書における環境	4
1.3.	本書における構成	5
1.4.	電子証明書の発行時における留意事項	5
2. ドメ・	インコントローラでの設定	5
2.1.	ルート証明書の NTauth ストアへのインポート	5
3. Shar	ePoint サーバでの設定	8
3.1.	SSL サーバ証明書のインポート	
3.2.	SSL ポートのバインド	10
3.3.	クライアント証明書要求の有効化	12
3.4.	クライアント証明書マッピング認証の設定	13
4. Gléa	s の管理者設定	14
4.1.	UA(ユーザ申込局)設定	14
5. iPad	での操作	16
5.1.	構成プロファイルのインストール	16
5.2.	SharePoint サーバへのアクセス	19
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	19
6. 問い	合わせ	20

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。



- 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
- 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)
- 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

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認証設定

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。



			証明書	
全般 2	詳細	証明のパス		
表示(<u>S</u>):	: <₫	t <t></t>	~	
フィール	۴		値	^
回サブシ 回機関: 回キー修 回Nets	シェクト キ キー職別 使用法 cape 調	⊧-識別子 別子 正明書の種類	ea 4a bd 49 b2 4a 97 b6 89 8d d6 f0 07 c2 cc 7 KeyID=ea 4a bd 49 b2 4a 97 b6 89 8d d6 f0 07 Digital Signature, Certificate Signing, Off-line Cf SSL CA, SMIME CA (06)	
 Nets 基本部 	cape ∃ 制限	メント	Private CA Gleas Subject Type=CA, Path Length Constraint=0	≡
□拇印:	アルゴリス	ズム	sha1	
圖拇印			61 4a 68 c8 ae d8 9b 80 0d 1c b1 ed 57 c7 03 t	V
01 44 (ae do 30 00	00 10 01 e0 57 07 05 07 00 44 5e 50	

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。

			ナップインの追加と削除	×
コンピューターで利用できるスナッス は、どの拡張を有効にするかを構成 利用できるスナップイン(S):	パインからこのコンソール 戎できます。	に使用す	スナップインを選択したり、選択したスナップインを構 選択されたスナップインイト):	成したりできます。拡張可能なスナップインで
Ztyデイン Ztyデイン INAP クライアントの構成 TPM 管理 Web アドレスへのリンク Windows Server / (シ WMI コントロール Iイント ピューアー インシト ピューアー インシーキュート インフォメー Tンターネット インフォメー Tンターオライズ PKT	ペンダー Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor		10(A) >	拡張の編集(公)… 削除(R) 上へ参勤(U) 下へ参勤(D)

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。

	AD コンテナーの管理		x
KRA コンテナー	証明機関コンテナー	登録サービス コンテナー	
NTAuthCertificates	AIA コンテナー	CDP コンテナー	
名前		状態	I
追加(A) 肖	除(R) 表示(V)		
L		0K +127/17	

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。

7	証明書を保護するための	のパスワードを入力してくたさい。	7=10-604
<u>tademo</u>	- バスワードの入力 -		シンイベーアレム 、 者 ロヘルブ ロログアウト
証明書 ■ JCCH-SSS de	パスワード	••••• ダウンロード キャンセル	 D 一覧に戻る D ビック
兼証明書情報···· ▶ <u>servercert.gleas.ex</u>	ample	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	▲ <u>ロード ■タイムライン</u> : 2017/04/03 12:26

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。

	証明書スナップイン	x	コンビューターの選択
20スナップインで管理する証明書: () ユーザーアカウント(<u>(t)</u> () サービス アカウント(<u>S</u>) (2) <u>ビンビューター アカウント(C)</u>			20スキップインて管理するコンピューターを選択して化さい、 20スキップインて管理するコンピューター: ③ (ローカルコンピューター(L): (20コンソールを実行しているコンピューター) ③ 別のコンピューター(A):
	< 戻る(B) 次へ(M) > キャンセ	JL	< 戻る(<u>B</u>) 完了 キャンセル

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。

証明書のインボート ウィザードの開始
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保 譲されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシス テム上の領域です。
保存場所 ○ 現在のユーザー(<u>C</u>) ④ ローカル コンピューター(<u>L</u>)
持行するには、[次へ] をクリックしてください。

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
	2
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。

a	בעכב] - עכב	ル ルート¥証明書 (ロ−	・カル コンピュー	-ター)¥個人¥
骗 ファイル(F) 操作(A) 表示(V) お気	に入り(O) ウィンドウ(W) ヘル	プ(H)		
🗢 🔿 🙍 🗊 📋 🧟 🛃				
📔 コンソール ルート	発行先 💧	発行者	有効期限	目的
⊿ 🙀 証明書 (ローカル コンピューター)	😨 servercert.gleas.examp	le JCCH-SSS demo CA	2017/07/05	サーバー認証
⊿ 📔 個人				
🧰 証明書				

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。

			ታイト バイ	インド	? X
種類	ホスト名	ポート	IP アドレス	バインド情報	追加(<u>A</u>)
inttp		80			編集(E)
					削除(<u>R</u>)
					参照(<u>B</u>)
					閉じる(<u>C</u>)

[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

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認証設定

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。

	サイト バインド	*の追加 ? X
種類(<u>T</u>): https	IP アドレス(I): 未使用の IP アドレスすべて	ポート(<u>0</u>): ✓ 443
ホスト名(日):		
□ サーバー名表示を要	求する(<u>N</u>)	
SSL 証明書(<u>F</u>):		
servercert.gleas.ex	ample	✓ 選択(上) 表示(⊻)
		OK キャンヤル

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。

SharePoint - 80 $\pi - h$	操作
	▶ エクスプローラー
フィルター: ▼ 蒙 検索(G)	アクセス計可の構実
ASP.NET	サイトの編集
۵	バインド
.NET グローバリゼ .NET コンパイル	アプリケーションの表示
-537	仮想ディレクトリの表示
404	Web サイトの管理
.NET のエラー ペー .NET の承認規則	💈 再起動
۶ ۶	▶ 開始
	■ 停止
	Web サイトの参照
.NET の役割 .NET プロファイル	💿 :80 (http) 参照
	💽 *:443 (https) 参照
🏢 機能ビュー 🕼 コンテンツ ビュー	詳細設定

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。

接続 Q, + 🔜 Ž 分。	Share	ePoint - 80 ホーム
	フィルター:	
SharePoint Web Services	IIS HTTP リダイレクト び ISAPI フィルター	HTTP 応答ヘッダー IP アドレスおよびドメ インの制限 MIME の種類

[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。

SSL 設定	操作
このページでは、Web サイトまたはアプリケーションの SSL 設定を変更することができます。 ✔ SSL が必要(Q)	■▼ 週用 ■★ キャンセル
クライアント証明書:	
○ 無視(<u>I</u>)	
○ 受理(A)	
● 必要(<u>R</u>)	

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。

Б.	サーバーマネージャー			
@ @• :	ナーバー マネージャー・	IIS • ② 🏲 管理(M) ッ-,	μ(I) 表示(Y) ヘルプ(出)	
 	役割と機能 すべての役割と機能 合計: 39 フィルター 名前 Windows 認証 ダイジェスト認証 クライアント証明書マッピング認証 IIS クライアント証明書マッピング認証 URL 承認 トレース く		タスク ▼ (マ) (マ) (マ) (ア) (ア)	

[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。

		■ 意刻日本
-	In	中心声肚

グループ化:グループ化なし 🔹		
名前 🔷	状態	応答の種類
Active Directory クライアント証明書の認証	有効	HTTP 401 チャレンジ
ASP.NET 偽装	無効	
Windows 認証	無効	HTTP 401 チャレンジ
ダイジェスト認証	無効	HTTP 401 チャレンジ
フォーム認証	無効	HTTP 302 ログイン/リダイレクト
基本認証	無効	HTTP 401 チャレンジ
匿名認証	無効	

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。

() 認証		
グループ化:グループ化なし・		
名前 ^	状態	応答の種類
ASP.NET 偽装	無効	
Windows 認証	無効	HTTP 401 チャレンジ
ダイジェスト認証	無効	HTTP 401 チャレンジ
フォーム認証	有効	HTTP 302 ログイン/リダイレクト
基本認証	無効	HTTP 401 チャレンジ
匿名認証	無効	

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-

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認証設定

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。

▶基本設定
□ トークンへのインポート
🗖 証明書ストアへのインポート
▼ ダウンロードを許可
ダウンロード可能時間(分) 1

[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。

認証デバイス情報 ○ □
▶iPhone / iPadの設定
□ iPhone/iPad 用 UAを利用する
保存

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)

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 Gleas			
識別子(例: com.jcch-	com.jcch-sss.profile			
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	SharePoint用プロファイル			
削除バスワード	••••••			

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。

パスコードの設定	
✓ デバイスのバスコードが必要	
単純値を許可	📃 英数字の値が必要

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

う フライベートCA Gléas ユーザ 0 1 さんのページ				
				JEAN-PCA Gléas UA
[ユーザ 0	1 さんのページ]			■ ログアウト
ユーザ情報		_	_	
🛛 🛛 ユーザ	・01 さんのページ			
2 ユーザ	青報			
▶ ユーザ	登録日時:	2011/07/19 13:48		
> 姓 : ユーザ > ユーザID : > メール :	* 名:0] user01			
★ 証明書	情報			
▶発行済み証	E明書			
#	発行局	シリアル	有効期限	ダウンロード
<u>\$1</u>	JCCH-SSS demo CA	#10969	2017/07/05	構成プロファイルのダウンロード

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。

キャンセル	警告	インストール
ロックされたプロファイル	,	
このプロファイルをイ が必要となります。	ンストールすると、	削除するには認証
ルート証明書		
証明書"JCCH-SSS de にある信頼できる証明	mo CA"をインスト]書のリストに追加さ	ールすると、iPad されます。

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。

\otimes	プライベートCA Gléas ユーザ 0 1 さんのページ				
				プライベートCA Gléäs UA	
[ユーザ 0 1	さんのページ]			■ ログアウト	
ユーザ情報					
🙎 ユーザ	01 さんのページ				
2 ユーザ情	与報 ····				
▶ ユーザ	登録日時 : 2011	/07/19 13:48			
≫ 姓 : ユーザ ≫ ユーザID : u ≫ メール :	名:0 1 user01				
★ 証明書情	青報 · · · · · · · · · · · · · · · · · · ·				
▶発行済み証	明書				
#	発行局	シリアル	有効期限	ダウンロード	
\$ 1	JCCH-SSS demo CA	#10969	2017/07/05	ダウンロード済み	

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。

\otimes		ホーム - ホーム						
SharePoint			ニュースフィード	OneDrive	サイト	ユーザ 01 🗸	ø	?
参照 ページ				7	☆ フォロー	🔓 同期 🖌	編集	
s 🔉	^{ホーム} 『 リンクの編集 ホーム			2	のサイト の	検索		Q
ホーム ドキュメント サイト コンテンツ * リンクの編集	サイトでの作業の開始 レストやライブラリ、 その他のアプリを追加	このパネルを表示しない						
	ニュースフィード 会話の開始 アクティビティがありません。も を開始してください。	っと多くの人をサイトに	: 招待するか、会話	ドキ:	ュ メント _{名前} っーにド:	キュメントはま	5りま	

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)

このWebには証明書が必要です 必要な証明書がインストールされてい ません。
了解

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