

# プライベート認証局Gléas ホワイトペーパー

Office 365 と

Active Directory フェデレーションサービス(AD FS)での クライアント証明書認証設定

(ブラウザ および Officeアプリ)

Ver.2.0 2020 年 1 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	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	6			
2. ドメ-	インコントローラでの設定	7			
2.1.	ルート証明書の NTauth ストアへのインポート	7			
3. ADFS	S サーバでの設定	10			
3.1.	SSL サーバ証明書のインポート	10			
3.2.	SSL サーバ証明書の適用	13			
3.3.	多要素認証(MFA)の設定	13			
4. WAP	サーバでの設定	14			
4.1.	SSL サーバ証明書のインポート	14			
4.2.	SSL サーバ証明書の適用	14			
5. Gléas	s の管理者設定(PC)	15			
6. クライ	イアント操作(PC)	15			
6.1.	クライアント証明書のインポート	15			
6.2.	Office 365 へのアクセス(ブラウザ)	17			
6.3.	Office 365 へのアクセス(Office アプリ)	18			
7. Gléa	s の管理者設定(iPhone)	20			
8. クライ	イアント操作(iPhone)	21			
8.1.	クライアント証明書のインポート	21			
8.2.	Office 365 へのアクセス	24			
9. 失効について					
10.CTL(Certificate Trust List)について					
11.お問い合わせ					

### 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」で発行したクライアント証明書 を利用して、Microsoft Corporationのクラウドサービス Office 365 と Windows Serverに含まれる Active Directory フェデレーションサービスで認証をおこな 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

▶ フェデレーションサーバ:

Windows Server 2016 Datacenter

/Active Directory フェデレーション サービス 4.0

※ 以後、「ADFSサーバ」と記載します

➤ AD FSプロキシサーバ:

Windows Server 2016 Datacenter

/ リモート管理(Web Application Proxy)

※ 以後、「WAPサーバ」と記載します

▶ JS3 プライベート認証局 Gléas (バージョン2.1.4)

※ 以後、「Gléas」と記載します

▶ SaaSサービス: Office 365 Enterprise E3

※ 以後、「Office 365」と記載します

クライアント: Windows 10 Pro / Internet Explorer 11 / Excel バージョン1902
 ※ 以後、「PC」と記載します

▶ クライアント: iPhone (iOS 13.3) /

Outlook 4.21.0 / Microsoft Authenticator 6.3.27

- ※ 以後、「iPhone」と記載します
- ※ iOSでは、Microsoft Authenticatorアプリが必要になるので事前にインストールしてお きます

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
- ADFSサーバや、WAPサーバのセットアップ
- Office 365の基本設定、ADFSとのフェデレーション設定
   本書では、Office 365とADFS/WAPとのフェデレーション設定が完了していることを前提にしています。
- 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
- PC、iPhone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。

ADFSではクライアント証明書認証にポート番号49443を利用します。このため、 クライアントデバイスからWAP向けのTCPポート49443の通信ができる必要があ ります。

Gléasでサーバアカウントを作成する際に、ホスト名に追加記述をすることでポート443での通信をすることもWindows Server 2016のADFSでは可能です。(代替 ホスト名バインド。1.4項参照)

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. Gléasでは、ADFSとWAPにSSL用サーバ証明書を、PC、iPhoneの利用者にク

ライアント証明書を発行する

- PC:クライアントはブラウザやOfficeアプリケーション(本書ではExcelを利用)でOffice 365にアクセスすると、認証先としてWAPにリダイレクトされる
- 3. iPhone:Officeモバイルアプリ(本書ではOutlookを利用)でOffice 365にア クセスすると、認証先としてWAPにリダイレクトされる
- ADFSでは二要素認証をおこなう(フォーム認証+クライアント証明書認証)。
   認証情報はOffice 365に連携される(フェデレーション)。
   有効な証明書を持つクライアントデバイスのみOffice 365に接続してOffice
   アプリを利用することができる。
- 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。

 本書では、ADFSサーバ・WAPサーバのSSLサーバ証明書を入れ替える手順 を記述しますが、その場合ADFSの[フェデレーションサービス名]と、Gléas でのサーバアカウントを作成する際の[ホスト名]が一致している必要があり ます。

▶ アカウント情報	■ 上級#	向け設定		
>アカウント名 🚖				
▶初期グループ	tau			
	■ここをクリックしてユーザを参加させるグループを選択			
その他の設定	定 □ 証明書を発行する			
	□ 連続して登録を行う			
▶種類 ○ ユーザ ○ コンピ	ニュータ 🖲 サーバ 🔿 認証局 🔿 CSVファイルー括登録 🔿 LDAP			
> ホスト名 📩				
> ライセンスコード 📩	参照… ファイルが選択されていません。			
	1/15/5			

フェデレーションサービス名は、[ADFSの管理]より左ペインの[サービス] を右クリックし、[フェデレーションサービスのプロパティの編集(E)]をク リックすると表示される[フェデレーションサービスのプロパティ]画面で確 認できます。

フェデレーション サービスのプロパティ	×			
全般 組織 イベント フェデレーション サービスの表示名(E):				
JS3_win2016_adfs				
例: Fabrikam フェデレーション サービス				
フェデレーション サービス名(N):				
sts.				
例: fs.fabrikam.com				
フェデレーション サービスの識別子(1):				
http://sts. /adfs/services/trust				
例: http://fs.fabrikam.com/adfs/services/trust				
Web SSO の有効期間(分)(W): 480 🔤				

また1.2項で触れた通り、Windows Server 2016 以降では [ホスト名] に、"certauth.[フェデレーション サービス名]"も加えておくことで、ポート 49443の通信をしないようにできまです。 その場合の[ホスト名]欄の入力は以下の例のようにします。 例) sts.example.com;certauth.sts.example.com

- iOS 13以降より、サーバ証明書に対する要件が変更されており、証明書有効 期間は825日未満である必要があります。
- クライアント証明書には以下の属性を含める必要があります。
  - ✓ サブジェクトの別名:証明書利用ユーザのActive Directoryにおけるユー ザプリンシパル名(UPN)
  - ✔ CRL配布ポイント

### 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





正明書 全般 詳細  証明のパス	×		
表示(S): <すべて>	•		
フィールド	値		
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Digital Signature, Certificate Signing, Off-lin		
🐻 Netscape 証明書の種類	SSL CA, SMIME CA (06)		
🐻 Netscape コメント	Private CA Gleas		
🛛 \overline 🙀 基本制限	Subject Type=CA, Path Length Constraint=0		
■ 1月60アルゴリズム	sha1		
<b>画</b> 拇印	61 4a 68 c8 ae d8 9b 80 0d 1c b1 ed 57 c7 🚝		
4			
,			
61 4a 68 c8 ae d8 9b 80 0d 1c b1 ed 57 c7 03 b7 c8 44 5e 9b			
証明書の詳細について表示します。	_ ブロパティの編集(E)   ファイルにコピー(C)   -		
	OK		

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します

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。

<b>B</b>	役割と機能の追加ウィザード
機能の選択	選択したサーバーにインストールする機能を 1 つ以上選択します。
用ロック用に	10月11日 - 11日 - 110 - 11
インストールの程度	10AHS
サーバーの選択	□ リモート /シスタンス ^
サーバーの役割	▲ ■ リモート サーバー管理ツール (4/40 個をインストール済み)
機能	▷ □ 機能管理ツール
確認	⊿ ■ 役割管理ツール (4/28 個をインストール済み)
<b></b> 结理	▷ ■ AD DS および AD LDS ツール (3/5 個をインストール済み)
THE	▷ □ Hyper-V 管理ツール
	b Windows Server Update Services ツール
	▷ 🗌 リモート デスクトップ サービス ツール
	□ Active Directory Rights Management サービス ツール
	▲ ✔ Active Directory 証明書サービス ツール
	□ オンライン レスポンダー ツール
	☑ 証明機関管理ツール

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。

ス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プインからこのコンソールに使用するスナップインを選択したり、選択したスナップインを構成したりできます。拡張可能なスナップインで は、どの拡張を有効にするかを構成できます。					
利用できるスナップイン <u>(S</u> ):			選択されたスナップイン(E):		
スナップイン	ペンダー	^	<b>ニ</b> コンソール ルート	拡張の編集(∑)	
🔬 NAP クライアントの構成	Microsoft Cor	1	動 エンタープライズ PKI		
📲 TPM 管理	Microsoft Cor			削除(R)	
📄 Web アドレスへのリンク	Microsoft Cor				
🐌 Windows Server パッ	Microsoft Cor			トへ移動(11)	
שאכב WMI ש>רם−וג	Microsoft Cor	=		T. ((2)	
🛃 イベント ビューアー	Microsoft Cor			下へ移動(D)	
🧊 インターネット インフォメー	Microsoft Cor		追加(A) >		
💼 エンタープライズ PKI	Microsoft Cor				

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。

			_	コンソール1
🚠 ファイル(F) 操作(A)	表示(V)	お気に入り(0)	ウィンドウ <b>(</b> W)	) へいプ(H
🧢 🄿 🖄 🖬 🙆	?			
□ンソール ルート 論 エンタープライズ PKI			/	=
	テンプ	レートの管理(T)		
	AD E	レンテナーの管理 <b>(</b> A	)	を使用して、
	オプシ	a> <b>(</b> 0 <b>)</b>		I-FL-7 Krbie
	表示(	M	•	- ADALASK 16
	ここか	ら新しいウィンドウ <b>(</b>	W)	
	新しい	ゆスクパッド表示(1	r <b>)</b>	
	最新	の情報に更新(F)		
	N17	(́Н)		
-				

[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 NTAuthCertificates	証明機関コンテナー AIA コンテナー	登録サービス コンテナー CDP コンテナー	
名前		状態	
追加( <u>A</u> ) 削	除( <u>R)</u> 表示( <u>V</u> )		
		0K +т>ти	ŀ

### 3. ADFS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	のパスワードを入力してください。,	J= AN-LOA
<u>#demo</u>	「バスワードの入力」		JUNICA
	パマワード	••••	査 ■ヘルブ ■ログアウト
証明書	////	ダウンロード キャンセル	▶一覧に戻る
JCCH-SSS de			■Ev2
★ 証明書情報 …			
servercert.gleas.ex		開始日:2014/04/03 12:26 終了日	: 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	× コンビューターの速	R ×
このスナップインで登録する証明書: () ユーザーブガウンドΔ0 () サーゼス アカウンド(S) (®) <u>ロンゼニーターブガウンド(S</u> )	לערגסט לערגסט וות-ם® בסופ עיצר ניאנ	で巻載するコンピューターを選択してください。 フマ管理するコンピューター: コンピューター(j):(Cのコンソン-Jを実行しているコンピューター) ピューター(d): 参照(t) ラインからお私したとさば選択されたコンピューターを安更できるようにする( <u>W</u> ) コンソールを保存した場合にのか通用されます。
< 戻る(8)	次へ( <u>N</u> ) > キャンセル	< 戻る(8) 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 ウィサ	「-ドの開始			
このウィザ します。	- ドでは、証明書、証明	書信頼リスト、および	証明書失効リストも	ディスクから証明書スト	7636-
証明機関 されたネッ 上の領域	によって発行された証明 トワーク接続を提供する です。	<b>1</b> 雪は、ユーザー ID をす ための情報を含んでい	確認し、デ−タを保証 います。証明書ストン	養したり、またはセキュリ・ アは、証明書が保管され	ティで保護 れるシステ
保存場	ħ				
○現	生のユーザー( <u>C</u> )				
۰ ۵	カル コンピューター( <u>L</u> )				
	こは、[次へ] をクリックし	てください。			
続行する					
続行する					

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
	リック
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

#### プライベート認証局 Gléas ホワイトペーパー

Office 365 と ADFS でのクライアント証明書認証設定

証明書インポートウィザードの終了	[完了]をクリック
------------------	-----------

ルート証明書も同時にインポートされるため、Windows OS が警告を表示します。 正しい拇印を持った証明書であることを確認し、[はい]をクリックします。

セキュリラ	1警告	$\times$					
	発行者が次であると主張する証明機関 (CA) から証明書をインストールしようとし ています:						
	JCCH-SSS demo2 CA						
	証明書が実際に "JCCH-SSS demo2 CA" からのものであるかどうかを検証できま せん。"JCCH-SSS demo2 CA" に連絡して発行者を確認する必要があります。次 の番号はこの過程で役立ちます:						
	拇印 (sha1): B96112E5 C0F29BA8 8FAB66EE 92FA7161 C6A0B417						
	警告: このルート証明書をインストールすると、この CA によって発行された証明書は自動 的に信頼されます。確認されていない提印付きの証明書をインストールすること は、セキュリティ上、危険です。[はい]をクリックすると、この危険を認識したことに なります。						
	この証明書をインストールしますか?						
	はい(2) いいえ(2)						

なお、Gléas 上でルート証明書の拇印を確認するには、管理画面右上の[▶認証局]か ら該当する発行局情報をクリックし、拇印の欄を参照します。



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。

	k (11		1-00-1			
····································						
🥁 ファイル(E) 操作(A) 表示(V) お気に入り(D) ウィンドウ(W) ヘルプ(E)						
🗢 🔿 🙍 🔂 🖬 🗎 🙆 😽	? 🖬	1				
אין אראכב 🛄	^	発行先 ^	発行者	有効期限	操作	
◇ 🙀 証明書 (ローカル コンピューター)		🖏 sts.js3-test12.local	JCCH-SSS demo2 CA	2020/12/13	証明書	<b>^</b>
◇ □ 個人					他の操作	•
> 🔛 信頼されたルート証明機関					sts.is3-test12.local	
> 📔 エンタープライズの信頼					()- の 把 (+	
> 🦳 中間証明機関					他以操作	,
> 📔 信頼された発行元						
> 🧮 信頼されていない証明書	~					
< >	>	<		>		
個人 ストアには1個の証明書があります。						

またルート証明書も同時にインポートされていることを確認します。

<ul> <li>□ンソール1 - (コンソール ルート¥証明</li> <li>ファイル(E) 操作(A) 表示(Y)</li> <li>◆ ◆ 2 (2)</li> </ul>	書 (ロー) お気に   2    5	カル コンピューター)¥信頼された。 入り( <u>Q) ウ</u> ィンドウ( <u>W)</u> へJ 	ルート証明機関¥証明書] レプ(出)			_	- 5 x
<ul> <li>コンソール ルート</li> <li>マ 緑 証明書 (ローカル コンピューター)</li> </ul>	^	発行先 PLICCH SSS domo2.CA	発行者	有効期限 2029/12/21	^	操作	
> 🧾 個人 🖌 🧰 信頼されたルート証明機関		Microsoft Authenti	Microsoft Authent Microsoft Root Au	2000/01/01 2020/12/31		証明音 他の操作	•
□ 証明書		Microsoft Root Cert	Microsoft Root Ce	2021/05/10		JCCH-SSS demo2 CA	
> · 中間証明機関 > · 信頼された発行元	~	Microsoft Root Cert	Microsoft Root Ce Microsoft Root Ce	2035/06/24 2036/03/23	~	他の操作	۲.
<	>	<		>			
信頼されたルート証明機関 ストアには 21	個の証明	明書があります。					

※ ルート証明書については、以下のグループポリシ(GPO)により複数マシンに対して同様の設定を一括しておこなうことが可能です。
[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]

### 3.2. SSL サーバ証明書の適用

Windows Powershell を起動して、以下のコマンドを入力します。 Set-AdfsSslCertificate -Thumbprint [証明書の拇印]

代替ホスト名バインドを使う場合は、Set-AdfsSslCertificateの代わりに以下コマンドを入力します。

Set-AdfsAlternateTlsClientBinding -Thumbprint [証明書の拇印]

なお、3.1 項でインポートした証明書の拇印は以下のコマンドで確認できます。 Get-ChildItem Cert:¥LocalMachine¥My

なお、適用されたサーバ証明書は以下で確認できます。 Get-AdfsSslCertificate

### 3.3. 多要素認証(MFA)の設定

スタートメニューより[AD FS の管理]を起動し、左側ペインの[サービス]>[認証方法]を選択し、中央ペインの[多要素認証方法]の[編集]をクリックします。 [認証方法編集]ウィンドウが開くので、[多要素]タブで[証明書認証]をチェックしま す。



認証方法	の編集						×
プライマリ	多要素						
追加の認 必要があ	証方法を ります( <u>S</u> ):	選択する。 MFA	を有効にする(;	は、次の方注	から少なくとも	1つを選択する	
☑ 証明 □ Azur	書認証 e MFA						٦
多要素	2証の概要						

次に、左ペインで[証明書利用者信頼]を選択し、中央ペインで"Microsoft Office 365 Identity Platform"を選択、右ペインよりアクセス制御ポリシーの編集をクリックします。

アクセス制御ポリシーの編集ウィンドウで、[すべてのユーザーを許可し、エクス トラネット アクセスで MFA を要求]を選択し、[適用(P)]ボタンをクリックしま す。

Microsoft Office 365 Identity Platform のアクセス制御ポリシーの編集	×
アクセス制御ポリシー	
アクセス制御ボリシーを選択してください:	
名前         説明           特定のグループを許可         指定した           すべてのユーザーを許可し、認証されていないデバイスから MFA を要求         オペてのユ すべてのユーザーを許可し、特定のグループに MFA を要求           すべてのユーザーを許可し、特定のグループに MFA を要求         イントラネ           すべてのユーザーを許可し、MFA を要求         オペアのコ すべてのユーザーを許可し、MFA を要求           すべてのユーザーを許可し、MFA を要求         オペアのコ すべてのユ すべてのユーザーを許可           すべてのユーザーを許可         オペアのコ すべてのコ すべてのコーザーを許可	
ポリシー	
次の場合にユーザーを許可する イントラネットネットワークから 次の場合にユーザーを許可する インターネットネットワークから および Multi-Factor Authentication を要求する	
OK キャンセル 通	用(P)

## 4. WAPサーバでの設定

4.1. SSL サーバ証明書のインポート

3.1 項と同じ手順でサーバ証明書とルート証明書を WAP サーバにインポートします。

### 4.2. SSL サーバ証明書の適用

Windows Powershell を起動して、以下のコマンドを入力します。 Set-WebApplicationProxySslCertificate -Thumbprint [証明書の拇印]

なお、4.1 項でインポートした証明書の拇印は以下のコマンドで確認できます。 Get-ChildItem Cert:¥LocalMachine¥My

設定された証明書は以下のコマンドで確認できます。 Get-WebApplicationProxySslCertificate

# 5. Gléasの管理者設定 (PC)

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

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。

> UA 申込局 ▶<u>Gleas Generic UA</u> Gleas デフォルト申込局

[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

▶ 証明書ストアへのインボート	証明書ストアの種類	ユーザストア	-
🗖 ダウンロードを許可	☑ インボートワンスを利用す	-3	

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。

# 6. クライアント操作 (PC)

6.1. クライアント証明書のインポート

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。

				プライベートCA Gléäs
スト 四郎 さんの^	ページ]			<b>1</b> 22
ーザ情報				
🧕 テスト 四郎さん	のページ			►_⊥
2 ユーザ情報				
▶ユーザ	登録日時: 2019/10/02 04:55			
> ユーザID : testuser4@ > メールアドレス : > パスワード : ********** * 証明書情報 ·····				
▶ 発行済み証明書 #	举行局	シリアル	有thmmB	証明書ストアヘインボート
<u>\$1</u>	JCCH-SSS demo2 CA	#170	2020/10/02	証明書のインボート

「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。

			プライ・	x-fca Gléäs	<b>U</b> A
[テスト 四郎 さんのページ]					<u> 5701</u>
ユーザ情報		_			
🙎 テスト 四郎さんのページ	7			Þa	ルゴ
2ーザ情報					^
▶ユーザ	登録日時:2019/10/02 04:55				
>姓: テスト 名: 回惑 >ユーザロ: testuser4@ >メールアドス: >パスワード: ************************************					
#	発行局	シリアル	有効期限	証明書ストアヘインボート	
<u>\$1</u>	JCCH-SSS demo2 CA	#170	2020/10/02	ダウンロード済み	
					V
プライベートCA Gléas			Copyright (C) 2010-2019 JCCH Securi	ty Solution Systems Co.,Ltd. All rights	reserved.

6.2. Office 365 へのアクセス(ブラウザ)

ブラウザでOffice 365へアクセスし、ドメイン名を含むユーザIDを入力すると、 ADFSのログオン画面にリダイレクトされます。

🚦 アカウントにサインイン	׼
<mark>●●</mark> Microsoft 組織のサイ	ンイン ページに移動します。
キャンセル	

ADFSのサインイン画面でパスワードを入力します。

<i>員</i> サインイン	× 📑	
JS3_wi	in2016_adfs	
組織アカウン	ントを使用してサインインしてください	
testuser4@j		
パスワード	2	
サインイ		

- その後、クライアント証明書を提示するよう求められます。
- ※ WAPサーバがローカルイントラネットゾーンに設定されている場合など、IEの設定によっては 以下の「Windows セキュリティ」画面は表示されない場合もあります

◯ sts.js3-test12.local の特機中 × □	Windows 証明書	<sup>セキュリティ</sup> 『の選択		×
JS3_win2016_adfs	サイト cer 유문	tauth.sts.js3-test12.local   testuser4@ 発行者: JCCH-SSS demo	に対する資格情報が必要です: 	
セキュリティ上の理由により、アカウント (testuser4@) を検証するための追加情報が必要です	7 m 04	有効期間: 2019/10/02 か 証明書のプロパティを表示(	ッら 2020/10/02 します	
認証に使用する証明書を選択してください。操作を取り消す 場合は、ブラウザーを終了して、再度実行してください。	20118	ОК	キャンセル	ľ

認証が完了すると、Office 365のポータル画面が表示されます。



Microsoft Office 7	т-4 ×							
Office 365					، م	) ()	?	Q
こんにちは	t				Office ගැ	(ンストー)	۷ ×	
+	0	-	w	x	P	N	i,	
新規作成 ~	Outlook	OneDrive	Word	Excel	PowerPoint	OneNe	ote	
4	<b>uji</b>	-	$\rightarrow$					
SharePoint	Teams	Yammer	すべてのアプ リ					
最近使ったファ	イルピン	留め 自分と	共有 注目度	の高いファー	()L		₹	
			<b>1</b> 70					
		2	<u> </u>	•				
	最	近使ったの	ffice のオン	ラインド:	±	フィードバ	ック	

なお、失効した証明書でアクセスをすると、エラー表示となります。



6.3. Office 365 へのアクセス(Office アプリ)

Excelを起動しタイトルバーにある[サインイン]をクリックします。

Book1 - Excel	サインイン 困	— (	
---------------	---------	-----	--

Office 365ログイン用のユーザIDを入力します。

Microsoft	
サインイン	
testuser4@	
アカウントがない場合 アカウントを作成しましょう	

ADFSのログイン画面でパスワードを入力します。

	;	×
JS3_win2016_adfs		
組織アカウントを使用してサインインしてください		
testuser4@		
サインイン		

その後、ブラウザでのアクセスと同様にクライアント証明書の提示を求められます。



認証に成功するとログインユーザが表示されるようになります。

}	≠ Excel	<u>テストューザ4 団 ー ロ X</u>
	テスト ユーザ4 testuser4@	
€.	<u>プロファイル</u> アカウント設定	設定・セル編集
	アカウントの切り替え	·



同時にOneDriveやSharePoint Onlineにもログインするので、オンラインストレージ を透過的に利用できます。

また一度ログインした情報はキャッシュされるので、他のOfficeアプリケーション を開いてもログインした状態になります。

## 7. Gléas の管理者設定(iPhone)

Gléas で、発行済みのクライアント証明書を iPhone にインポートするための設定を 記載します。

※ 下記設定は、Gléasの納品時に弊社で設定を既にしている場合があります

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・[インポートワンスを利用する]にチェック この設定を行うと、GléasのUAからインポートから指定した時間(分)を経過し た後は、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)。これにより複数台のデバイス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。

🗹 ダウンロードを許可		🗹 インボートワンスを利用する
ダウンロード可能時間(分)	1	☑ 登録申請を行わない

設定終了後、[保存]をクリックし設定を保存します。

[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。

プライベート認証局 Gléas ホワイトペーパー

Office 365 と ADFS でのクライアント証明書認証設定

🦸 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

画面レイアウト

✓ iPhone 用レイアウトを使用する	✔ ログインバスワードで証明書を保護
Mac OS X 10.7以降の接続を許可	

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)	JS3 demo profile	
識別子(例: com.jcch-	com.jcch-sss.demo-profile	
sss.profile)		
ブ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	
i 兑8月	Office365接続プロファイル	
削除バスワード		

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。

# 8. クライアント操作(iPhone)

#### 8.1. クライアント証明書のインポート

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おこないます。

※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



画面の表示にしたがい設定を開くと、プロファイルがダウンロードされた旨が表示 されるので、インストールをおこないます。



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できま す。必要に応じて確認してください。





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、内容を確認し [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。



インストール完了画面になりますので、[完了]をタップして終了します。



その後、設定より[情報] > [証明書信頼設定] と進み、インポートしたルート証明 書を信頼するよう設定をおこないます。

く情報	証明書信賴設定
- 20 - 10 - 10	
トラストス	ストアバージョン 2018121
トラスト	・アセット・バージョン 7
ルート証明書	書を全面的に信頼する
JCCH-SS	S demo2 CA

Safariに戻り、[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。

プライベ-	-pca Gléãs 🛯
テスト 四郎 さんのぺ	ージ
ユーザロ	testuser4@
姓	テスト
名	四郎
メール	
JCCH-SSS demo2 C	A
有効期限 2020/10/02	ダウンロード済み
	ログアウト
Copyright (C) 2010-2019 JCCH Security	Solution Systems Co.,Ltd. All rights reserved.

### 8.2. Office 365へのアクセス

Outlook アプリを起動してアカウントの追加をおこないます。

$\langle$	アカウントの追加
	職場または個人のメール アドレ
	スを入力してください
	testuaer4@
	<u>アカウントの追加</u>
	<u> プライバシーと Cookie</u>

画面の指示にしたがい、Microsoft Authenticator を開きます。



ADFSのログイン画面に遷移するので、パスワードを入力します。

<u>キャンセル</u>
JS3_win2016_adfs
組織アカウントを使用してサインインしてください testuser4@
パスワード
サインイン

その後、証明書認証がバックグラウンドでおこなわれ(提示できる証明書が複数あ る場合は選択ダイアログが出現します)、ログインが完了しメール閲覧が可能となり ます。

この状態で[設定]をタップすると Office 365 や OneDrive にログインしていること がわかります。





また Microsoft Authenticator を見ると、Azure AD にログインできたことが記録されています。

(Microsoft Authenticator を認証に使う他 Office モバイルアプリもこの認証結果 情報を参照します)



なお、有効な証明書がない場合や、失効した証明書でログインを試行するとログインに失敗します。



# 9. 失効について

証明書失効によるアクセス拒否時には、ADFSサーバのadminログに以下のログエ

# プライベート認証局 Gléas ホワイトペーパー

Office 365 と ADFS でのクライアント証明書認証設定

ントリが発生します。

```
説明:
トークンの検証に失敗しました。
追加データ
トークンの種類:
http://schemas.microsoft.com/ws/2006/05/identitymodel/tokens/X509Certificate
%エラー メッセージ:
ID4070: X.509 証明書 'CN=testuser4@example.com' チェーンの構築に失敗しました。使
用された証明書には、検証できない信頼チェーンが存在します。証明書を交換するか、
certificateValidationMode を変更してください。' 証明書が失効しています。
```

Windows Serverは失効リスト (CRL) を取得するとその有効期限までキャッシュ します。以下コマンドをADFSを動かしているサーバ上で実行することで、CRLの キャッシュ終了時間を即時にクリアできます。 certutil -urlcache crl delete certutil -setreg chain¥ChainCacheResyncFiletime "@now" net stop cryptsvc net start cryptsvc

# **10.** CTL (Certificate Trust List) について

CTLを使うことで、Gléasから発行したクライアント証明書だけをクライアントに提示させることが可能となります。 CTLの設定は、今回の環境ではWAPサーバにて以下の手順でおこないます。

CTLを作成する
 certutil -f -addstore [証明書ストア名] [ルート証明書ファイル]
 MMCで証明書ストアを見ると (certlm.msc)、ストアが作成されているのが分かります。
 例) certutil -f -addstore adfs\_client\_trust ial.cer





この画面で信頼するルート証明書を追加インポートすることも可能です。

● ポート49443 (証明書認証サイト)のSSLバインドを解除する

netshコマンドを使って設定します。

```
> netsh
```

netsh>http

netsh http>delete sslcert hostnameport=[フェデレーションサービス名]:49443 ※ 代替ホスト名バインドの利用時は、「hostnameport=certauth.[フェデレーションサービ ス名]:443」とします(以下同じ)

正常に終了すると、「SSL 証明書を正常に削除しました」と表示されます

作成したCTLを指定し、ポート49443に対してSSLバインドを再度設定する
 netsh http>add sslcert hostnameport=[フェデレーションサービス名]:49443
 certhash=[サーバ証明書の拇印] appid={5d89a20c-beab-4389-9447-324788eb944a}
 certstorename=MY sslctlstorename=[証明書ストア名]

正常に終了すると、「SSL 証明書を正常に追加しました」と表示されます

```
    実施した結果を確認
```

netsh http>show sslcert

SSL 証明書のバインド: ホスト名∶ポート 証明書ハッシュ : [フェデレーションサービス名]:49443 : e98585ee1f032b7fd7f94f2bb57de2bc7d6e9e0f 証明<del>古</del>ハッシー アプリケーション ID : {5d89a20c-beab-4389-9447-324788eb944a} 証明書ストア名 : MY クライアント証明書の失効状態の検証: Enabled キャッシュされたクライアント証明書のみを使用した失効状態の検証: Disabled 使用法のチェック : Enabled 失効リストの更新を確認する間隔:0 URL 取得のタイムアウト : 0 Ctl 識別子 : (null) Ctl ストア名 : adfs\_client\_trust DS マッパーの使用法 : Disabled クライアント証明書のネゴシエート: Disabled

# 11. お問い合わせ

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