

# プライベートCA Gléas ホワイトペーパー

PingFederateのクライアント証明書認証設定

(Office365 先進認証)

Ver. 1.0 2017 年 3 月

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

- 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l	ごめに	
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. Pin	gFederate の設定	6
2.1.	サーバ証明書の設定	6
2.2.	署名用証明書の設定	7
2.3.	ルート証明書の設定	
2.4.	証明書の失効確認設定	8
2.5.	X.509 Connector の設定	9
2.6.	サービスプロバイダの設定	
3. Off	ice365(Azure AD)の設定	15
4. Glé	eas の管理者設定(PC)	16
5. クラ	ライアント操作(PC)	17
5.1.	クライアント証明書のインポート	17
5.2.	Office365 へのアクセス(ブラウザ)	
5.3.	Office365 へのアクセス(Office アプリ)	
6. Glé	eas の管理者設定(iPhone)	21
7. クラ	ライアント操作(iPhone)	23
7.1.	クライアント証明書のインポート	23
7.2.	OTA エンロールメントを利用した証明書発行について	
7.3.	Office365 へのアクセス	25
8. 問い	い合わせ	27

## 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、Ping Identity社のSSOサーバ「PingFederate」経由でMicrosoft Corporationのクラウドサービス「Office 365」の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。

SAML IDP: Windows Server 2012 R2 Standard / PingFederate 8.2.2
 ※以後、「PingFederate」と記載します

※以下のコネクタを追加インストールしています

- ♦ Office365 Connector 2.0.2
- ♦ X.509 Integration Kit 1.2
- ➤ SaaSサービス: Office 365 Enterprise E3
   ※以後、「Office365」と記載します
   ※Office365をサービスプロバイダとして利用するには、ビジネスプランのサブスクリプションが必要になります
- ドメインコントローラ: Microsoft Windows Server 2012 R2 Standard
   ※以後、「AD」と記載します

※以下のツールをインストールしています

- ♦ Microsoft Online Services サインイン アシスタント
- ♦ Windows PowerShell用 Microsoft Azure Active Directory モジュール
- ♦ Azure AD Connect
- JS3 プライベートCA Gléas (バージョン1.14.6)
   ※以後、「Gléas」と記載します
- > クライアント: Windows 10 Pro / Internet Explorer 11 / Excel 2016

プライベート CA Gléas ホワイトペーパー PingFederate クライアント証明書認証設定 (Office365 先進認証) ※以後、「PC」と記載します > クライアント: iPhone 5c(iOS 10.2)/ Outlook 2.12.0 / Microsoft Authenticator 5.1.2 ※以後、「iPhone」と記載します ※iOSでは、Microsoft Authenticator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。

- Pingの基本的な設定(データストア(Active Directory)の設定含む)、
   ConnectorやIntegration Kitのインストール なお本書では、PingFederateのhttpsのポート設定は以下の通りになっていることを前提 としています(<pf\_install\_directory>¥pingfederate¥bin¥run.properties で確認可能です) httpsプライマリポート(pf.https.port):9031
   httpsセカンダリポート(pf.secondary.https.port):9032
- Gléasでのアカウント登録や各種証明書発行
   今回は以下の証明書を発行する前提です
  - ➢ SSLサーバ証明書
  - ▶ SAMLアサーションの署名用証明書
  - ▶ クライアント証明書
- Windows ServerやWindowsドメインのセットアップ
- Azure AD Connectを用いたOffice365のユーザプロビジョニング
- 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。
```

#### 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。



プライベート CA Gléas ホワイトペーパー

PingFederate クライアント証明書認証設定 (Office365 先進認証)

- Gléasでは、PingFederate用にSSLサーバ証明書・アサーションの署名用証明
   書を、PC・iPad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 2016 を利用)でOffice365にアクセスすると、認証先としてPingFederateにリダイ レクトされる
- iOS:Officeモバイルアプリ(本書ではOutlookを利用)でOffice365にアクセ スすると、認証先としてPingFederateにリダイレクトされる
- PingFederateではクライアント証明書認証をおこなう。証明書に記載されているユーザアカウント情報に基づきADより必要な情報を取得し、Office365に送信しログインする。
- 1.4. 電子証明書の発行時における留意事項

本書の設定内容において、Gléasで電子証明書の発行操作をする際には以下の点に 留意する必要があります。

 クライアント証明書 サブジェクトの代替名(Subject Alt Name)に、ADのユーザ名 (userPrincipalName属性)と、有効なCRL配布ポイントが含まれるように しておきます。

# 2. PingFederateの設定

PingFederate の管理 Web 画面にログインし、以下の設定をおこないます。

#### 2.1. サーバ証明書の設定

事前にGléasでサーバ証明書を発行し、ダウンロードしておきます。

Server Configuration > CERTIFICATE MANAGEMENT > SSL Server Certificateと 進みます。

[Import]をクリックし、Gléasよりダウンロードしたサーバ証明書ファイルをアップ ロードします。PASSWORD欄にはGléasから証明書ファイルをダウンロードした際 に設定したバスワードを入力します。

	プライベート	CA Gléas ホワイ	トペーパー	
PingFederate	クライアント	·証明書認証設定	(Office365	先進認証)

Certificate Management   Import Certificate					
Import Certificate	Summary				
Please select the file co	ntaining the desired certificate.				
FILENAME	servercert.gleas.example.p12 Choose file				
PASSWORD					

[Next]をクリックするとサマリ画面が表示されます。 "MAKE THIS THE ACTIVE CERTIFICATE FOR THE RUNTIME SERVER"がチェッ クされていることを確認し、[Save]をクリックして保存します。

Certificate Management   Import Certificate
Import Certificate Summary
Summary information for your new certificate. Select the checkbox to make this new certificate the active certificate. Unselecting the checkbox preserves the current active certificate.
✓ MAKE THIS THE ACTIVE CERTIFICATE FOR THE RUNTIME SERVER
MAKE THIS THE ACTIVE CERTIFICATE FOR THE ADMIN CONSOLE

## 2.2. 署名用証明書の設定

事前にGléasで署名用の証明書を発行し、ダウンロードしておきます。

Server Configuration > CERTIFICATE MANAGEMENT > Signing & Decryption Keys & Certificatesと進みます。

[Import]をクリックし、Gléasよりダウンロードしたサーバ証明書ファイルをアップ ロードします。PASSWORD欄にはGléasから証明書ファイルをダウンロードした際 に設定したバスワードを入力します。

Certificate Management   Import Certificate							
Import Certificate	Summary						
Please select the file co	Please select the file containing the desired certificate.						
FILENAME	pf-sign.p12 Choose file						
PASSWORD	••••						

[Next]をクリックするとサマリ画面が表示されるので、内容を確認して[Save]をクリックして保存します。

### 2.3. ルート証明書の設定

事前に Gléas よりルート証明書をダウンロードしておきます。

※Gléas に http://hostname/(http であることに注意)でアクセスすると、ダウンロードが可能 です

・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
認証局のトップページにアクセスするための ルート証明書を下のボタンをクリックしてダウ ンロードしてください。
ルート証明書のダウンロード
▶ 証明書のインポート方法について
プラウザにルート証明書をインポートできたら 下のリンクから認証局のトップページにアクセ スしてください。
認証局のトップページへ進む

Server Configuration > CERTIFICATE MANAGEMENT > Trusted CAsと進みます。 [Import]をクリックし、Gléasよりダウンロードしたルート証明書ファイルをアップ ロードします

Certificate Management   Import Certificate						
Import Certificate	Summary					
Please select the file containing the desired certificate.						
FILENAME	ia1.cer Choose file					

[Next]をクリックするとサマリ画面が表示されるので、内容を確認して[Save]をクリックして保存します。

#### 2.4. 証明書の失効確認設定

Server Configuration > CERTIFICATE MANAGEMENT > Certificate Revocation Checkingと進み、以下の設定をおこないます。

- [Enable CRL Checking]をチェック
- [Verify CRL Signature]をチェック

プライベート CA Gléas ホワイトペーパー						
PingFederate クライアント証明書認証設定 (Offi	ce365 先進認証)					
Certificate Revocation Checking						
Specify the certificate validation mechanism. For OCSP-based validation, specify the se	ttings.					
ENABLE OCSP						
ENABLE CRL CHECKING						
TREAT UNRETRIEVABLE CRLS AS REVOKED						
NEXT RETRY ON RESOLUTION FAILURE (MIN)	1440					
NEXT RETRY ON NEXT UPDATE EXPIRATION (MIN)	60					

またこの状態で[Enable OCSP]をチェックし設定をおこなうことで、失効確認に OCSPとCRLを併用することも可能です(弊社未検証)。

## 2.5. X.509 Connector の設定

IDP Configuration > APPLICATION INTEGRATION > Adaptorsを選択します。 Manage IdP Adaptor Instancesで [Create New Instance]をクリックします。 その後、以下を設定します。

Typeタブで以下を設定します。

- INSTANCE NAME: 任意の名称
- INSTANCE ID: 任意の識別ID
- Type: [X.509 Certificate IdP Adaptor]を選択

Manage IdP Adapter Instances   Create Adapter Instance						
Type IdP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary		
Enter an Adapter Instance Name adapters currently installed on y	e and Id, select the Ada rour server.	pter Type, and a parent	f applicable. The Adapter Type is	limited to the		
INSTANCE NAME	CertAuth					
INSTANCE ID	CertAuth					
TYPE	X.509 Certificat	e IdP Adapter 1.2 🛛 🗸	Visit Pingldentity.com for a	additional types		
PARENT INSTANCE	None	~				

IdP Adaptorタブで以下を設定します。

- CLIENT AUTH PORT: 9032(セカンダリのポート番号) を入力
   Show Advance Fieldsを展開し、
- INCLUDE SUBJECT ALTERNATIVE NAME (SAN)をチェック

Manage IdP Adapter Instances   C	Create Adapter Ir	istance	
Type IdP Adapter Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary
Complete the configuration necessary to look up use	r security contexts in your	environment. This configuration	was designed into the adapter for use at your site.
X.509 Certificate IdP Adapter			
CONSTRAIN ACCEPTABLE ROOT ISSUERS (All trusted CAs of the Java Virtual Machine and the adapter. If issuers are specified in this table, then on	PingFederate server are u ly those issuers will be co	sed to validate the client certifica sidered valid for SSO purposes.]	te at the TLS layer. Optionally, you can use this table to designate a subset of those trusted CAs for end-user certificate authentication by the
ISSUER DN (An acceptable root CA issuer DN)			Action
Add a new row to 'Constrain Acceptable Root Issuer	s'		
Field Name	Field Value	C	Description
CLIENT AUTH PORT	9032	т	he PingFederate port configured to use client-certificate authentication.
CLIENT AUTH HOSTNAME		Т	he PingFederate hostname configured to use client-certificate authentication.
PARSE CLIENT CERT SUBJECT AND ISSUER DNS	•	lr o e	vdicates whether the client certificate Subject and Issuer DNs are parsed, treating their components as separate attributes. This allows you to add ommon attributes such as CR or UD to the Extended Adapter Contract and use for assertion mapping. Prefix have DN attributes with "Issuer,", for any project, issuer, CR to use the Subject OF "email attribute in the Core Contract, this too must be selected.
RETURN SUCCESS ON SLO	~	R	teturns an automatic success message on a single-logout event. Note that SLO is not supported for this adapter, and the user's session is not eminated. This option is provided solely to prevent SLO failure at other sites that may be involved in the same logout request.
AUTHENTICATION CONTEXT	Default     Policy OID     Custom	Ţ	he value used to populate the "Authentication Context" field in a SAML token. By selecting "Default", the value is set to "TLSClient", by selecting Policy OD', the identifier for the policy populates the field, and "Custom" allows for a specified static value.
CUSTOM AUTHENTICATION CONTEXT		S	tatic value for specifying a custom Authentication Context value in your SAML tokens.
INCLUDE SUBJECT ALTERNATIVE NAME (SAN)	×	ł	clude the decoded SAN attributes from the certificate to make them available in the attribute contract.
Hide Advanced Fields			

Extend Contractタブで以下を設定します。

• Extend the Contractに、"cn"と"userPrincipalName"を追加

Manage IdP Adapt	er Instances   C	reate Adapter In	istance	
Type IdP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary
This adapter type supports th Adapter Contract may be use persistent name identifier whi	e creation of an Extended d to fulfill the Attribute Co ich uniquely identifies the	d Adapter Contract after i ontract, look up additiona e user passed to your SP	nitial deployment of the adapter i I attributes from a local data store partners.	nstance. This e, or create a
Core Contract				
ClientCertificateChain				
email				
IssuerDN				
SubjectDN				
Extend the Contract	Action			
cn	Edit I Delete			
userPrincipalName	Edit I Delete			
	Add			

Adaptor Attributesタブで、以下を設定します。

● userPrincipalNameのPseudonymをチェック

Summaryタブで設定を確認し[Done] > [Save]とクリックして設定を保存します。

Manage IdP Adapter Instances Create Adapter Instance						
Туре	ldP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary	
IdP adapter	instance summar	y information.				
Create A	dapter Instanc	e				
Туре						
Instance Na	ame		CertAuth			
Instance Id			CertAuth			
Туре			X.509 Certificate	IdP Adapter 1.2		
Class Name	2		com.pingidentity.	adapters.idp.clientcert.ClientCertl	dpAuthnAdapter	
Parent Insta	ance Name		None			
ldP Adapt	ter					
Client Auth	Port		9032			
Client Auth	Hostname					
Parse Clien	t Cert Subject an	d Issuer DNs	true			
Return Suc	cess On SLO		true			
Authenticat	ion Context		Default			
Custom Au	thentication Cont	ext				
Include Sub	ject Alternative N	Name (SAN)	false			
Extended	Contract					
Attribute			IssuerDN			
Attribute			SubjectDN			
Attribute			email			
Attribute			ClientCertificate	Chain		
Attribute			cn			
Attribute			userPrincipalNan	1e		
Adapter A	Attributes					
Mask all O	GNL expression lo	og values	false			
Pseudonyn	1		userPrincipalNan	1e		
Adapter (	Contract Mapp	olng				
Attribute	Sources & Use	er Lookup				
Data Sourc	es		(None)			
Adapter (	Contract Fulfillr	ment				
IssuerDN			IssuerDN (Adapte	ər)		
cn			cn (Adapter)			
SubjectDN			SubjectDN (Adap	iter)		
email			email (Adapter)			
userPrincip	alName		userPrincipalNan	ne (Adapter)		
ClientCertif	icateChain		ClientCertificate	Chain (Adapter)		
Issuance Criteria						
Criterion			(None)			

# 2.6. サービスプロバイダの設定

IDP Configuration > SP CONNECTIONSと進み、[Create New]ボタンをクリックし 以下の設定をおこないます。

SP Connections > Connection Templateタブ

- USE A TEMPLATE FOR THIS CONNECTIONを選択
- CONNECTION TEMPLATEは、Office 365 Connector を選択
- METADATA FILEは、Office 365のメタデータをアップロード

※Office365のメタデータは、2017年2月現在以下のURLで公開されています

https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml

SP C	onnection					
Con	nection Template	Conne	ction Type	Connection Options	Import Metadata	General Info
Brow	vser SSO Cr	edentials	Activation	& Summary		
PingFeo applical	lerate provides qu ble, please select	uick-configur a template f	ation template or this connec	es, available separately w tion; otherwise, continue	th SaaS Connectors, for to the next screen for m	specific Service Providers. If ore options.
	DO NOT USE	A TEMPLATI	E FOR THIS C	ONNECTION		
۲	USE A TEMPL	ATE FOR TH	IS CONNECTI	ON		
	CONNECTION TEMPLATE	ł	Office 36	5 Connector 🗸 🗸		
			Click Browse Directory:	e below to locate the SAN	IL 2.0 metadata file expo	orted from Azure Active
	METADATA FI	ILE	federationm	etadata.xml Cho	ose file	

Browser SSOタブで、[Configure Browser SSO]ボタンをクリックします。 SP Connection | Browser SSO > Assertion Creationタブで、[Configure Assertion Creation]ボタンをクリックします。

SP Connection | Browser SSO | Assertion Creation > Authentication Source Mappingタブで[Map New Adaptor Instance]ボタンをクリックします。

SP Connection | Browser SSO | Assertion Creation | IdP Adaptor Mapping > Adaptor Instanceタブで以下を設定します。

● ADAPTOR INSTANCEで、2.5項で設定したインスタンスを選択

Mapping Methodタブで以下を設定します。

 "RETRIVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING"を選択



SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Adapter Instance	Mapping Method	Attribute Sources & User Lookup	Attribute Contract Fulfillment
Issuance Criteria	Summary		
You can choose to fulfi Adapter 1.2" adapter, o	ll the Attribute Contract r you can use these valu	with your partner using either the value ues plus additional attributes retrieved fi	s provided by the "X.509 Certificate IdF rom local data stores.
Adapter Contract			
ClientCertificateChain			
cn			
email			
IssuerDN			
SubjectDN			
userPrincipalName			
RETRIEVE ADDIT	IONAL ATTRIBUTES FR	OM MULTIPLE DATA STORES USING C	INE MAPPING
O RETRIEVE ADDIT	IONAL ATTRIBUTES FR ATE DATA STORES ANI	OM A DATA STORE INCLUDES OPTIC D/OR A FAILSAFE MAPPING	ONS
USE ONLY THE	DAPTER CONTRACT V	ALUES IN THE SAML ASSERTION	

Attribute Sources & User Lookupタブでは、[Add Attribute Source]ボタンをクリックします。

SP Connection | Browser SSO | Assertion Creation | IdP Adaptor Mapping | Attribute Sources & User Lookup > Data Storeタブでは、設定済みのデータストア (Active Directory)を指定します。

LDAP Directory Searchタブでは、LDAPの検索条件を設定します。ここでAttribute to return from searchに、"ObjectGUID"と"userPrincipalName"を追加します。

SP Connec Adapter M	ctions   SP Connect apping   Attribute S	tion   E Source	Browser SSO   A s & User Looku	Assertic p	n Creatio	n IdP
Data Store	LDAP Directory Search	LDAP E	linary Attribute Encodin	ig Types	LDAP Filter	Summary
Please configure contract.	your directory search. This in	formation,	along with the attribute	s supplied i	n the contract, w	ill be used to fulfill the
BASE DN			CN=Users,dc=exan	nple,dc=loc	al	
SEARCH SCOPE	-		Subtree	~		
Attributes to ret	urn from search					
ROOT OBJECT	CLASS		ATTRIBUTE		Ac	tion
			Subject DN			
			objectGUID		Re	move
			userPrincipalName		Re	move
<show all="" att<="" td=""><td>ributes&gt;</td><td>~</td><td>Enabled</td><td></td><td>~</td><td>Add Attribute</td></show>	ributes>	~	Enabled		~	Add Attribute
View Attribute C	Contract					

LDAP Binary Attribute Encoding Typeタブにて、objectGUIDのエンコーディングタイプを、"Base64"に設定します。

※LDAP Binary Attribute Encoding Typeタブが出現しない場合は、データストアのADの詳細設定 でobjectGUIDをバイナリ属性として設定する必要があります

LDAP Filterタブで、Filter欄に"userPrincipalName=\${userPrincipalName}"を入力 します。

ata Store	LDAP Directory Search	LDAP Binary Attribute Encoding Types	LDAP Filter	Summary
e enter a Fi	ter for extracting data from y	our directory.		
e enter a Fi ER	ter for extracting data from y	our directory.		

Summaryタブで設定内容を確認し[Done]をクリックします。

SP Connection | Browser SSO | Assertion Creation | IdP Adaptor Mapping > Attribute Contract Fulfillmentタブで以下を設定

• IDPEmail

Source:	Adaptor
Value:	userPrincipalName

- SAML\_NAME\_FORMAT
   Source: Text
   Value: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- SAML\_SUBJECT

Source: LDAP(データストア名)

Value: objectGUID

Adapter Instance	Mapping Method	Attribute Sou	rces & User Lookup	Attribute Contra	ct Fulfillment
Issuance Criteria	Summary				
ulfill your Attribute Co	ntract with values from	one or more data	stores, the authenticati	on adapter, or dyna	mic text values.
Attribute Contract	Source		Value		Actions
IDPEmail	Adapte	r v	userPrincipalNa	ime v	None availab
SAML_NAME_FORMA	T Text	~	ameid-format:pe	ersistent	None availab

Summaryタブで設定内容を確認し[Done]をクリックします。

SP Connection | Browser SSO | Assertion Creation > Summaryタブで設定内容を 確認し、[Done]をクリックします。

SP Connection | Browser SSO > Protocol Settingタブ・SAML Profilesタブの設定 等は環境にあわせておこない、Summaryタブで設定内容を確認し、[Done]をクリッ クします。

SP Connection > Credentialsタブで[Configure Credentials]をクリックし、SP Connection | Credentials > Digital Signature Settingsタブで以下の設定をおこないます。

- SIGNING CERTIFICATEは、2.2項で設定した署名用証明書を選択
- SIGNING ALGORITHMは、"RSA SHA256"を選択

Summaryタブで設定内容を確認し、[Done]をクリックします。

SP Connection > Activation & Summaryタブで、ACTIVEを選択し[Save]をクリッ クし設定を保存します。



PingFederateの設定は以上です。

# 3. Office365 (Azure AD) の設定

Office365 の認証をおこなう Azure Active Directory の設定変更のため、「Windows PowerShell 用 Windows Azure Active Directory モジュール」を起動します。

Windows PowerShell 用 Windows Azure Active Directory モジュール – – ×
PS C: ¥WINDOWS¥System32> Connect-MsolService

 Enter Credentials ? ×

 Please enter credentials
 ユーザー名心: 
 バスワード心:

 OK キャンセル

以下のコマンド入力し、Office365の管理者権限を持つアカウントでログインします。 Connect-MsolService

ログイン後に以下を入力し、対象ドメインをフェデレーションドメインに変更します。 \$domainName = "<Federated Domain Name>" \$pingfederate = "https://<Hostname>:9031" \$brandName = "PingFederate" \$issuer = "<PingFederate SAML 2 entity id>" \$spId = "urn:federation:MicrosoftOnline" \$activeLogOn = "\$pingfederate/idp/sts.wst" \$logOff="\$pingfederate/idp/SLO.saml2" \$metaData="\$pingfederate/pf/sts mex.ping?PartnerSpId=\$spId" \$passiveLogOnPF="\$pingfederate/idp/SSO.saml2" \$certData="<2.2 項で設定した署名用証明書(テキスト形式)> Set-MsolDomainAuthentication -DomainName "\$domainName" ` -FederationBrandName "\$brandName" -Authentication Federated ` -PassiveLogOnUri "\$passiveLogOnPF" -SigningCertificate "\$certData" ` -IssuerUri "\$issuer" -ActiveLogOnUri "\$activeLogOn" ` -LogOffUri "\$logOff" -MetadataExchangeUri "\$metaData" ` -PreferredAuthenticationProtocol SAMLP

※<PingFederate\_SAML\_2\_entity\_id>は、PingFederate の設定画面の以下項目に設定されているも のとなります Server Configuration > System Settings > Server Settings > Federation Info > SAML 2.0 Entity ID

以下のコマンドを実行することで設定内容の確認が可能です。 Get-MsolDomainFederationSettings -DomainName <DomainName>

※Exchange Online で先進認証を有効にするためには、以下の操作が必要です。 https://support.office.com/en-us/article/Enable-Exchange-Online-for-modern-authentication-58018196-f918-49cd-8238-56f57f38d662

# 4. 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。 プライベート CA Gléas ホワイトペーパー

PingFederate クライアント証明書認証設定 (Office365 先進認証)



[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る	

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。

# 5. クライアント操作 (PC)

#### 5.1. 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 Gléas ホワイトペーパー

PingFederate クライアント証明書認証設定 (Office365 先進認証)

			プ	∍イベートCA Gléås
テスト ユーザ2 さ	ふのページ]			■⊐ <sup>j</sup> 7
ユーザ情報				
🙎 テスト ユーキ	F2さんのページ			► <u>n</u> uđ
2 ユーザ情報				
▶ユーザ	登録日時:2016/09/1	5 10:06		
>メールアドレス: >パスワード: ****** ★証明書情報				
▶ 発行済み証明書				
▶ 発行済み証明書 #	発行局	シリアル	有効期限	証明書ストアヘインポート
▶ 発行済み証明書 # <u><b>発</b>1</u>	発行局 JCCH-SSS demo CA	ジリアル #11241	有効期限 2019/09/18	証明書ストアヘインボート 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・	rx-fca Gléäŝ
テスト ユーザ2 さ	んのページ]			<b>1</b> 957
ユーザ情報				
🖉 テスト ユーザ	2さんのページ			<u>مالد</u>
▶ユーザ情報				
▶ユーザ	登録日時:2016/09/15	10:06		
★証明書情報·				
★ 証明書情報・ ▶ 第行済み証明書	發行 昆	וקנג?	右拉斯限	
★ 証明書情報・ 第行済み証明書 # <u> 発行済み証明書</u>	発行局 JCCH-SSS demo CA	シリアル #11241	有幼期限 2019/09/18	証明書ストアヘインボート ダウンロード演み

## 5.2. Office365 へのアクセス(ブラウザ)

Internet ExplorerでOffice365へアクセスし、ドメイン名を含むユーザIDを入力しま す。その後、PingFederateに転送されクライアント証明書を求められます。 ※PingFederateのURL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



認証が完了すると、Office365のポータル画面が表示されます。

Contraction of the second seco	office.com/1/?auth=	2&home=1&fro 🔎	- 🔒 🖒 🚺 Mia	rosoft Office ホーム	×			- □ 合☆	× © ©
こんにちは							テストューザ2 tratuer2巻 自分について		
オンライン	ドキュメントを	検索		٩		アカウン サインス	ットの表示 2ウト		
オンライン	アプリの伎	使用							1
о х-л	····· 予定表	<b>上</b> "" 正称先	<b>Y</b> ≑ <sup>Yammer</sup>		OneDrive	SharePoint	<b>2</b> 929		
Delve	Video	Word	Encel	Pee	OneNote	Sway	ם גרק גרק	■ フィードバック	Ý

5.3. Office365 へのアクセス(Office アプリ)

Excel 2016をひらき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 団 - ロ ×

Office365ログイン用のユーザIDを入力します。

	×
サインイン	
Excel で使用したいアカウントのメール アドレスまたは電話番号	
を入力します。	
次へ	
プライバシーに関する声明	

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を提示するよう求められます。

Win	dows セキュ!	17-1 X	<
記 [0 セ)	E明書の確 K] をクリックし W] をクリックし	認 ズ、この証明書を確認します。この証明書が正しくない場合、[キャン ズください。	
		testuser2@	
	[]]	発行者: JCCH-SSS demo CA	
	%≡	有効期間: 2016/09/18 から 2019/09/18	
	_	証明書のプロパティを表示します	
		OK キャンセル	

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。

	Book1 - E	xcel	<del>ም</del> አዮ ፲-1	f2 团	-//	
ペ テン	ストユー	ザ2		開発	♀ 操作アミ	尽共有
test	testuser2@				り :保存	
: 文章 <u>プロファイル</u> アカウント 恐定			La 王 2 2 La 電子 >	(-)L		
				<b>本</b>		^
アカ	ワントの切り替え	-				*
D	E	F	G	Н	1	J 🔺

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 を透過的に利用することが可能です。



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。

証明書を提示しない場合は以下のメッセージが表示されます。



失効された証明書でアクセスすると、ログインに失敗します。 この時にPingFederateのserver.logには、以下のログが書き込まれます。 [com.pingidentity.crypto.RevocationCheckerImpl] Certificate issued to < 証明書サブジェクト> has been revoked as indicated by CRL found at <証明書CRL 配布ポイント>

※server.logファイルは <pf\_install\_directory>¥pingfederate¥log にあります

# 6. 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

プライベート CA Gléas ホワイトペーパー

PingFederate クライアント証明書認証設定 (Office365 先進認証)

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	諸を行わない

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。

🦸 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
    ○ Mac OS X 10.7以降の接続を許可
```

☑ ログインバスワードで証明書を保護

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.protile)	
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
記印	Office365接続プロファイル
削除パスワード	

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。

# 7. クライアント操作 (iPhone)

#### 7.1. 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。

<b>O</b> エンドユーザロ	コグイン [UA]
<sup>ב</sup> <b>UA</b>	ーザID、バスワードを入力して口 インしてください。
トユーザID	
▶パスワード	
	ロダイン
<u>□ザID・パ</u>	スワードを忘れたら

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

プライベートCA	Gléås 🔼
テスト ユーザ2 さんの	ページ
ユーザID testuser2	@
姓	テスト
名	ユーザ2
メール	
JCCH-SSS demo CA	
有効期限 2019/09/18	ダウンロード
	ログアウト

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。



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。

キャンセル	警告	インストール
ルート証明書		
証明書"JCC CA"をインス iPhoneにあ 書のリスト(	H-SSS くトール る信頼 <sup>-</sup> こ追加さ	demo いすると、 できる証明 されます。

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。

プライベートCA	Gléås ua
テスト ユーザ2 さん	のページ
ユーザID testuse	er2@
姓	テスト
名	ユーザ2
メール	
JCCH-SSS demo C	A
有効期限 2019/09/18	ダウンロード済み
	ログアウト

7.2. 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。

### 7.3. Office365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。



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



その後、証明書認証がバックグラウンドでおこなわれ、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 Outlook アプリの[設定]をタップすると、Office365 や OneDrive にログ インしていることがわかります。

	設定	
ヘル	<i>、</i> プとフィードバック	>
アカ	ウント	
1	testuser2@ Office 365	>
<b>(</b>	testuser2@ OneDrive for Business	>
	<u>アカウントの追加</u>	

有効な証明書を提示できない場合は、以下のようになります。



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)



# 8. 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。

#### ■PingFederateに関するお問い合わせ先

マクニカネットワークス株式会社

Mail: ping-sales@cs.macnica.net

プライベート CA Gléas ホワイトペーパー

PingFederate クライアント証明書認証設定 (Office365 先進認証)

#### ■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 営業本部

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