

IIJ ID サービスでのクライアント証明書認証

(Office 365 連携)

Ver.1.0 2021 年 10 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. はじ	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
2. IIJ ID	の設定	6
2.1.	Gléas のルート証明書の信頼設定	6
2.2.	ログインポリシーの設定	9
3. Gléa	s UA の管理者設定(Windows 向け)	10
4. クラ	イアントからのアクセス(Windows)	11
4.1.	クライアント証明書のインポート	
4.2.	Office 365 への接続(ブラウザ)	
4.3.	Office 365 への接続(Office デスクトップアプリ)	
5. Gléa	s の管理者設定(iPhone 向け)	
6. クラ	イアントからのアクセス(iPhone)	20
6.1.	クライアント証明書のインポート	20
6.2.	Office 365 へのアクセス	22
7. 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使って、株式会社インターネットイニシアティブが運営するクラウド型認証管理サービス「IIJ IDサービス」でMicrosoft CorporationのOffice 365の認証を行う環境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: IIJ IDサービス
 ※以後「IIJ ID」と記載します
- ➤ SaaS (SAML SP): Office 365 Enterprise E3 ※以後「Office 365」と記載します
- ▶ 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
 ◆ Azure AD Connect バージョン 1.4.18.0 (Office 365/Azure ADへのID同期)
 ◆ IIJ ID Service Directory Sync バージョン 3.0.1 (IIJ IDへのID同期)
- > JS3 プライベート認証局 Gléas (バージョン 2.2.8)
 ※以後「Gléas」と記載します
- ▶ クライアント: Windows 10 Pro (21H1) / Microsoft Edge 94.0.992.47 / Microsoft Excel for Microsoft 365 MSO バージョン2109 ※以後「Windows」と記載します
- > クライアント: iPhone 12 Pro (iOS 15.0.2) / Microsoft Authenticator 6.5.84 / Microsoft Outlook 4.2139.0

※以後「iPhone」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。

4 / 25

IIJ ID サービスでのクライアント証明書認証(Office 365 連携)

- IIJ IDの基本設定、およびADとのID同期方法
- IIJ IDとOffice 365とのフェデレーション設定
- Azure AD Connectを用いたOffice 365のユーザプロビジョニング
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作
- Windows、iPhoneでのネットワーク設定やアプリインストール方法

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. WindowsとiPhoneは、GléasのUAから証明書をインポートする
- Windowsでは、ブラウザおよびOfficeデスクトップアプリケーションからOffice 365 ヘアクセス試行する
- 3. 認証連携先のIIJ IDのログイン画面に画面遷移し、IIJ IDはパスワードとクライアント 証明書を要求し、認証成功するとOffice 365にログインした状態になる
- 4. iPhoneは、OutlookアプリでOffice 365へアクセス試行する
- 5. Microsoft Authenticatorアプリが呼びだされ、IIJ IDでのパスワードとクライアント 証明書認証を経て、Exchange Onlineに接続する

IIJ ID サービスでのクライアント証明書認証(Office 365 連携)

2. IIJ ID の設定

2.1. Gléas のルート証明書の信頼設定

Gléas より発行したクライアント証明書を IJID で認証できるようにするため、Gléas の 認証局証明書を IJID に設定します。

Gléas の管理画面(RA)の画面上部の[認証局]リンクをクリックし、発行局(IA)にある ルート認証局名をクリックします。証明書ダウンロードで[CA 証明書:PEM 形式]をクリ ックし、認証局証明書をダウンロードします。

発行局詳細	□一覧	に戻る
🚖 EVALUATION CA		
▲ 発行局情報	■更新依頼を作成	Â
▶この発行局の説明 EVALUATION CA		
★ 発行局証明書情報·····		
▶ EVALUATION CA(ルート証明書)	▶失効リスト ▶証明書	1
> 有効期限: 2021/03/30 10:27 から 2022/03/31 10:27 まで		
> 認証局番号:1		
> サブジェクト:/CN=EVALUATION CA/DC=com/DC=jcch-sss/O=JCCH Security Solution Systems Co.,	, Ltd.	
》発行局: /CN=EVALUATION CA/DC=com/DC=jcch-sss/O=JCCH Security Solution Systems Co., Ltd.		
» 発行局証明書のシリアル: f9:5c:c0:a0:5e:89:5d:db		
>管理権限: true		
>シリアル:649		
» CRL番号: 407		
> 損印: CE:8D:CF:48:6A:D3:35:C5:C2:2A:61:14:32:11:46:D9:F2:42:E1:D4		
> 証明書ダウンロード: CA証明書:PEM形式 CA証明書:DER形式 CRL		

ダウンロードした証明書ファイルは拡張子が ".pem" となり、それを ".cer" (或いは ".crt")に変更するとダブルクリックで証明書ウィンドウが開きます。開いたら[詳細]タブ をクリックし、ウィンドウ下部の[ファイルにコピー]をクリックすると、証明書のエクス ポートウィザードが開始されます。

表示(S): <すべて>	~	
フィールド	値	^
[] バージョン	V3	
📴 シリアル番号	00f95cc0a05e895ddb	
▶ 署名アルゴリズム	sha256RSA	
📴 署名ハッシュ アルゴリズム	sha256	
🛄 発行者	JCCH Security Solution Systems Co., Ltd., jo	6
📴 有効期間の開始	2021年3月30日 10:27:01	
📴 有効期間の終了	2022年3月31日 10:27:01	
<	>	
V3		
	プロパティの編集(E) ファイルにコピー(C)	

ウィザードを進めエクスポート形式では[Cryptographic ~]を選択し、エクスポートされる PKCS#7 証明書ファイルに名前を付けて保存します。

ェクスポートファイルの形式 さまざまなファイル形式で証明者をエクスボートできます。
使用する形式を選択してください。
O DER encoded binary X.509 (.CER)(D)
O Base 64 encoded X.509 (.CER)(S)
 Cryptographic Message Syntax Standard - PKCS #7 証明書 (.P7B)(C) 証明のパスにある証明書を可能であればすべて含む(I)
 Personal Information Exchange - PKCS #12 (.PFX)(P) 証明のパスにある証明書を可能であればすべて含む(U)
□ 正しくエクスポートされたときは秘密キーを削除する(K)
 すべての拡張プロパティをエクスポートする(A)
□ 証明書のプライバシーを有効にする(E)
○ Microsoft シリアル化された証明書ストア (.SST)(T)

※ OpenSSL コマンドが利用できる環境では、以下コマンドで PKCS#7 形式に変換可能で openssl crl2pkcs7 -nocrl -certfile ./ial.pem -out ./ial.p7b

IIJ ID の管理者画面の上部メニュー [システム] > [セキュリティの設定] > [デバイスの 制限]と進み、[外部 CA]を選択します。

IIJ ID サービスでのクライアント証明書認証(Office 365 連携)



その下の外部 CA の設定で、[CA 証明書チェーンを登録する]をクリックし、エクスポートした PKCS#7 形式の認証局証明書をアップロードします。

CA証明書チェーンの登録	l≱	
・CA証明書チェーンを登録できます。 ・対応する証明書はPKCS#7形式(鉱張子が.p	75や.ゆ7でなどのファイル)のみです。	
■ 名前 必須	Gleas	
■ CA証明書チェーン 必須	ia1.p7b	+ ファイルを選択
		ia1.p7b / 1.1 KB 🖉
	CA証明書チェーンを登録する	ia1.p7b / 1.1 KB Ø

登録成功すると認証局の情報が表示されます。次に、[証明書の失効設定]をクリックします。

とい。 2 ↓ 2 ↓ 2 ↓ 2 ↓ 2 ↓ 2 ↓ 2 ↓ 2 ↓ 2 ↓ 2 ↓
CA証明書チェーン数(現在/墨大): 1/10
CA証明書チェーンの表示 証明書の失効設定 フィルタリング設定 削除
,

OCSP 設定で以下設定を行います。

- [OCSP を有効にする]にチェック
- OCSP サーバ URL に、Gléas の OCSP レスポンダーの URL を入力 通常は右のような URL 形式になります: http://gleas.example.com:2560/ia1
- [Nonce を有効にする]にチェック

• OCS • OCS • C	SPやCRLを用いて、認証時に証明書の失効が SPとCRLの両方を設定している場合はOCSP RLでの検証は、OCSPサーバへ正常に接続	WEを検証できます。詳しくは <u>0.ごちら</u> での検証が優先されます。 できない場合に利用されます。
OCSF	D設定	
0.0	NCSPを有効にしない	
	0.001 (213)/012 (0.001	
0	OCSPを有効にする	
•	OCSPを有効にする ■ OCSPサーバURL	http://
0	OCSPを有効にする ■ OCSPサーバURL ■ Nonce 1	http://:2560/ia1
•	OCSPを有効にする ■ OCSPサーバURL ■ Nonce ■ ■ 最新の検証ステータス	http:// Nonceを有効にする 成功 OCSPサーバ環境の検証

最新の検証ステータスの[OCSP サーバ接続の検証]を行うと、テスト接続をおこないま す。その際に HTTP ステータスが 200 で、OCSP ステータスが revoked (あるいは good) になっていれば OCSP レスポンダーとの通信に成功していると判断できます。

次に同じ画面の下部にある CRL 設定をおこないます。

- [CRL を有効にする]にチェック
- [CRL 配布ポイント URL]に、Gléas の CRL 配布ポイント URL を入力
 通常は右のような URL 形式になります: http://gleas.example.com/crl/ia1.crl
- [変更を適用する]をクリック(同時に CRL を取得します)
- [CRL を再取得する]をクリックすると、再度 CRL を取得します(失効の緊急反映時 などに利用可能)

● CRL配布ポイントのURLを指定する		
○ CRLファイルをアップロードする		
■ CRL配布ポイントURL	http://	つ CRLを再取得する
■登録されているCRL	登録されているCRLはありません	

なお、OCSP と CRL を両方設定した場合は、OCSP での検証確認が優先され、OCSP レスポンダーに正常に接続できない場合に CRL が利用されます(弊社未検証)。

2.2. ログインポリシーの設定

[システム] > [セキュリティの設定] > [ログインポリシー]と進みます。

IIJ ID サービスでのクライアント証明書認証(Office 365 連携)

※ 本検証ではデフォルト(Default) ポリシーを編集します

別途設定された信頼されたネットワーク(例:社内ネットワークセグメント)以外からの アクセスにクライアント証明書を要求するよう設定します。

【信頼するネットワーク外】

- [ログインを許可する]を選択
- 第1要素に[パスワード]、第2要素[デバイス証明書]を選択

領するネットワーク外			
) ログインを許可しない			
◉ ログインを許可する			
認証方式			
第1要素: パスワード			
第2要素: デバイス証明書			
第3要素: なし			
	第1要素	第2要素	第3要索
FID02	第1要素	第2要素	第3要素
FIDO2 パスワード	第1要素 □ ☑	第2要素	第3要素
FIDO2 バスワード 外部IdP	第1要素 □ 【】 □	第2要素	第3要素
FIDO2 パスワード 外部idP メールOTP	第1要素 口 【 【 【 【 【 【 【 【 【 】 【 】 【 】 】 】 】 】 】 】 】 】 】 】 】 】	第2要素	第3要素
FID02 パスワード 外部IdP メールOTP デバイス証明書	第1要素 口 で し し し し し し し し し し し し し	第2要素 □ □ □	第3要素

設定後、[更新]をクリックして保存します。

これで信頼されたネットワーク以外からの IIJ ID へのアクセスには Gléas より発行された有効なクライアント証明書が必須になります。

3. Gléas UAの管理者設定(Windows向け)

GléasのUA(申込局)より発行済み証明書をWindowsクライアント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おこな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。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します



申込局詳細画面が開くので、基本設定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

IIJ ID サービスでのクライアント証明書認証(Office 365 連携)

- 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

▶基本設定	日上級者向け
 トーケンへのインボート ✓ 証明書ストアへのインボート ダウンロードを許可 ダウンロード可能時間(分) 	 管理するトークン Gemalto.NETカード ✓ 証明書ストアの種類 ユーザストア ✓ インボートワンスを利用する 登録申請を行わない 登録泳済みデバイスのみインボート許可
保	7

設定完了後、[保存]をクリックし保存します。また、認証デバイス設定の以下項目にチェ ックがないことを確認します。

- iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]
- Android/Windows Phone の設定の、[Android / Windows Phone 用 UA を利用する]
- 証明書インポートアプリ連携の設定の、[証明書インポートアプリを利用する]

以上でGléasの設定は終了です。

4. クライアントからのアクセス (Windows)

4.1. クライアント証明書のインポート

IEモードが設定されたEdge、あるいは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。

※ UAのログイン認証をActive Directoryで行うことも可能です。詳細は最終項のお問い合わせ先ま でご連絡ください

●エンドユーザログイン [UA]
レム トユーザル、バスワードを入力して口 ダインしてください。
▶⊐-ザD
▶パスワード
ロダイン
■ユーザID・バスワードを忘れたら…

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。

🗖 🛛 ブライベートCA Glé	as テスト ユーザ1 × +						-		×
← → C [ø	https://	ua/login/info	1	. ()	ĩò	₹⁄≡	œ		
			プ	ライベー	-ԻCA	Gl	éå	Ŝ UA	
[テスト ユーザ1 さん	vのページ]							グアウト	
ユーザ情報				_	_	_	_		
🙎 テスト ユーザ1	さんのページ								
 ■ ユーザ情報・・・・ ■ ユーザ ● 姓: デスト 名: ユ > ユーザID: test01 > メールアドレス: > パスワード: ************************************	<u> 登</u> 録日時 : 2021/08/0 ー ザ 1	4 11:14						^	
★証明書情報···									
#	発行局		有効期限	í	証明書ス				
<u><u><u></u><u></u></u></u> <u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>	EVALUATION CA	#649	2021/10/22	(証明書	Юインボー	F		

※ 初回ログイン時には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ます

※ 証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印 を確認するなど正当性を確認してから[はい]をクリックします

(III ID利用においては必須ではないので [いいえ]を選択しても問題ありません)

セキュリテ・	(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:	
	EVALUATION CA	
	証明書が実際に "EVALUATION CA" からのものであるかどうかを検証できません。"EVALUATION 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): CE8DCF48 6AD335C5 C22A6114 321146D9 F242E1D4	
	警告: このルー証明書をイソストールすると、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。確認されていない毎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と になります。	
	この証明書をインストールしますか?	
	はいの しいいえ(N)	

インポートワンス機能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、再度ログインしてインポートをおこなうことはできません。

□ ブライベートCA Gléas ラ	-די די +				-	
→ C 🚺	ttps://	/ua/login/info		to	ć= @	
			プライ	~- Ի СА	Gléä	íŝ u
テスト ユーザ1 さんの	ページ]				0	ログアウト
ユーザ情報				_		
🙎 テスト ユーザ 1 さ	んのページ					
ユーザ情報 ・・・・・ トューザ	答錄日時:2021/08	3/04 11:14				^
>炸:テスト 名:ユーザ	H34Elot - 202100					
≥ユーザID : test01						
>メールアドレス:						
≥ ユーザID : test01 ≥ メールアドレス : ≥ バスワード : ***********	**					
★ 証明書情報 ·····						
▶発行済み証明書						
#	発行局	シリアル	有効期限	証明書:	ストアヘインボート	

4.2. Office 365 への接続(ブラウザ)

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



IIJ IDのサインイン画面でログインIDを入力します。

	ID	× +		-		×
$\leftarrow \rightarrow$	C Ô	https://www.auth.iij.jp/signin/id?config_code_hint= & & & & & & & & & & & & & & & & & & &	ē ζ≡	Ē	۲	
						-
						- 1
		סינוו 🎦				
		ID				- 1
		IDをメールアドレス形式で入力してください				- 1
						- 1
		次へ				
						- 1

次にパスワードを入力します。

ai ui 🖬	× +			-	×
\leftarrow \rightarrow C \textcircled{b} https;	//www.auth.iij.jp/signin/password?config_code_hint=klocale=ja	ô	£≡	Ē	
	Gilli 💶				
	ID.				
	Seduced Septo-Aurit23.vyE				
	■ パスワード				
	パスワードを入力してください				
	次へ				
	●パスワードを忘れた場合				
	別のアカウントでログインする				

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。

	×	+	-	×
$\leftarrow \rightarrow \mathbf{x}$	https://www.auth	.iij.jp/signin/password?config_code_hint= 🔧 🗞 🏠 🏠	Ē	
	 ID ノ(ス ・・・ 別のア: 	認証用の証明集の選択 × サイト certauthuiju/43 では資格倍級が必要です: ・ ・		

D 🚺 Microsoft	Office #-LA × +				-		×
$\leftarrow \ \ \rightarrow \ \ G$	ttps://www.office.com/?auth=2	₿	τô	£≡	œ		
Office 365	▶ 検索			5	۵¢	?	8
	こんにちは	Office	のイン	ルストー	ル ~		
•	すべて 最近使用したアイテム 共有 お気に入り 入力してリストをフィルター	一処瑁	7 7	マップロ	1-K		
x	・ ・ アクティビ	ティ 〜					
1							
4	コンテンツ アクティビティなし 他のユーザーと共有して共同作業を行います。新しいドキュメ ントを作成したり、アップロードして開き、作業を開始しま す。						
ab	↑ アップロードして開く 新規作成						

認証が完了すると、Office 365のポータル画面が表示されます。

IIJ ID管理画面の上部メニュー[レポート] > [ログイン履歴]を見ると、二要素(パスワード・クライアント証明書)によるログインに成功したことが分かります。

■ ログイン履歴				Ν		
• 最新のものから最大10 • ログをCSVファイルで	0件のログを表示して ダウンロードすること	います。 かできます。		r3		
■ ログイン履歴の保	持期間	7日		0 編集		
					▲ CSVファイ	いのダウンロード
ログイン日時・	ID ¢	IPアドレス ≑	認証要素	デバイス	FIDO2セキュリティキー	証明書UUID
2021/10/15 17:09:30	maanarjan Milan	31.2012.2	デバイス証明書 (OCSP)	Microsoft Edge 94.0.992.47 (W indows 10 64-bit) fingerprint: b63fe95d87f4a2e7da8bef39bfc 2a4db		3b13ca47-6 538-4417-8c 36-16c3d7df 7674
2021/10/15 17:09:25	105.001.002.0	34136303	パスワード認証	Microsoft Edge 94.0.992.47 (W indows 10 64-bit)		

なお、クライアント証明書がない状態でアクセスをすると、「登録されていないデバイス からのアクセス」と表示されます。



失効された証明書でアクセスしても同様の表示に加え、提示した証明書情報が表示されます。



4.3. Office 365 への接続(Office デスクトップアプリ)

Officeデスクトップアプリ(ここではExcelを使用)を起動して、画面上部の[サインイン] をクリックします。

⊟ 9 · C · % · →	Book1 - Excel	サインイン	厨 −	o x
ファイル ホーム 挿入 描画 ページレイアウト	数式 データ	校閲 表示 ヘルプ	♀ 操作ア:	۶ 🖻
$ \begin{array}{c c} & & & \\ & & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & $	% ■ 条件作 数値 × 図 セルの:			
クリップボード 15 フォント 15		スタイル		^
D1 • : × ✓ fx				*
A B C D	E F	G H	I	J
1				
2				

サインイン画面でドメイン名を含むユーザIDを入力すると、IIJ IDのログオン画面にリダ イレクトされます。

Microsoft	
サインイン	
メール、電話番号、または Skype	
アカウントがない場合 アカウントを作成しましょう	

ユーザIDとパスワードを入力します。





証明書認証がバックグラウンドでおこなわれ(証明書が複数ある場合は選択ダイアログが出現します)、ログインに成功するとOfficeデスクトップアプリケーションにログイン した状態になり、そのユーザに割り当てられたOfficeライセンスやファイル共有システム(OneDrive、SharePoint)が利用可能な状態になっています。



証明書がない場合、失効された証明書でアクセスした場合の表示はブラウザのものと同じになります。

5. Gléas の管理者設定(iPhone 向け)

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。

IIJ ID サービスでのクライアント証明書認証(Office 365 連携)

[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		2 1	(ンポートワンスを利用する
ダウンロード可能時間(分)	1	2	診録申請を行わない

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。

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

構成プロファイルに必要となる情報の入力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)

┦ 認証デバイス情報 ────────────────────────────────────						
▶ iPhone / iPadの設定	▶iPhone / iPadの設定					
🔽 iPhone/iPad 用 UA 초利用	する					
画面レイアウト						
✓ iPhone 用レイアウトを使用 Mac OS X 10.7以降の接続	する を許可	☑ ログインパスワードで証明書を保護				
OTA(Over-the-air)						
 OTAエンロールメントを利用 	する	□ 接続する iOS デバイスを認証する				
OTA用SCEP URL						
OTA用認証局	デフォルトを利用 🖌					
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- sss.profile)	com.jcch-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	ICCHセキュリティ・ソリューション・システムズ				
記印	プライベートCA Gleas で作成した	-構成プロファイル				

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。

6. クライアントからのアクセス (iPhone)

6.1. 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。

プライベート	Gléås 🗤	プライベー	- ECA Gléäs UA	1	プライベートCA Gleas UA
テスト ユーザ1 さんのペー	-ジ	テスト ユーザ1 さんの	ページ	テスト ユーザ	1 さんのページ
ユーザID	test01	ユーザID	test01	ユーザID	test01
姓	テスト	姓	テスト	姓	テスト
名	ユーザ1	名	ユーザ1	名	ユーザ1
メール		メール		メール	
EVALUATION CA		このWebサイト	、は構成プロファ	EVAL	ファイルがダウンロ
有効期限 2021/10/22	ダウンロード	イルをタリンロています。許可	ートしょうとし しますか?	有効期	ード済み
Copyright (C) 2010-2021 JCCH Security Solu	ログアウト tion Systems Co.,Ltd. All rights reserved.	copyrigen to training search to car assuming	<u>無視</u> 許可	するに Copyrig	ンデートレビーン グアウト には"設定" Appで再確認 してください。
					問じる

※ 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。

設定	<u>キャンセル</u> プロファイ… インストール
Q 検索	
Apple ID、iCloud、メディアと購入	プライベート CA Gleas JCCHセキュリティ・ソリ…
プロファイルがダウンロード済み >	署名者 未署名 説明 プライベート CA Gleas で作成し た構成プロファイル 内容 証明書: 2
	詳細 >
	ダウンロード済みプロファイル…

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。

戻る	プライベート CA Gleas	
証明	書(2)	
0	test01 EVALUATION CA	>
0	EVALUATION CA 発行元: EVALUATION CA 有効期限: 2022年3月31日	>

インストール中にルート証明書のインストール確認画面が現れるので、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
管理対象外ルー	-卜証明書	
証明書"EVAL トールすると できる。"証明 ます。"証明 するまで、こ ト用には信頼	UATION 、iPhon のリスト 書信頼設 の証明書 きれませ	I CA"をインス neにある信頼 < に追加され 定"で有効に 書はWebサイ さん。

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。



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。

プライベートCA	Gléấs 🗠
テスト ユーザ1 さんのページ	3
ユーザID	test01
姓	テスト
名	ユーザ1
メール	
EVALUATION CA	
有効期限 2021/10/22	ダウンロード済み
	ログアウト

6.2. 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。

<	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	
te	estuser1@	
	<u>アカウントの追加</u>	
	新しいアカウントの作成	

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



IIJ IDのログイン画面に遷移するので、IDとパスワードを入力します。



その後、証明書認証がバックグラウンドでおこなわれ(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はログインに失敗します。



また、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。



7. 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。

■IIJ ID に関するお問い合わせ

株式会社インターネットイニシアティブ 担当営業までお問い合わせいただくか、以下よりご連絡をお願いいたします。 お問い合わせURL:https://biz.iij.jp/public/application/add/33

■Gléasや本検証内容、テスト用証明書の提供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