

# プライベート認証局Gléas ホワイトペーパー

VMware Identity Manager (vIDM)での

クライアント証明書認証設定

Ver. 1.0 2018 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.	はじょ	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.	留意事項	6
2.	シナ!	リオ1:vIDM の設定	7
	2.1.	信頼するルート認証局の設定	7
	2.2.	認証プロバイダの設定	7
	2.3.	認証ポリシーの設定	10
3.	シナ!	リオ1:Gléas の管理者設定	10
	3.1.	UA(ユーザ申込局)設定	10
4.	シナ!	リオ1:Windows PC での証明書インポート	11
	4.1.	Gléas の UA からのインストール	11
	4.2.	Office 365 へのアクセス認証	12
5.	シナ!	リオ 2:AirWatch の設定	14
	5.1.	証明書発行テンプレートの設定	14
	5.2.	プロファイルの設定	14
6.	シナ!	リオ 2:vIDM の設定	
	6.1.	認証プロバイダの設定	16
	6.2.	認証ポリシーの設定	17
7.	シナ!	リオ 2:iPad からの接続	18
	7.1.	クライアント証明書の配信	18
	7.2.	Office 365 へのアクセス認証	19
8.	問いる	合わせ	21

### 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、ヴイエムウェア社のデジタルワークスペース・プラットフォーム VMware Workspace ONEの一機能、「VMware Identity Manager」(IDaaS機能部 分)でのクライアント証明書による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。

また文中で触れられるモバイルデバイス管理「VMware AirWatch」も、VMware Workspace ONEの一機能となります。

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。

- ▶ ID管理サービス: VMware Identity Manager (Build 77a820c07daad39c49cab3eb8530cda86dee8b3b) ※以後、「vIDM」と記載します ※Active DirectoryとのID同期には、Enterprise System Connectorを使っています
- モバイルデバイス管理:VMware AirWatch 9.2.3.8
   ※以後、「AirWatch」と記載します
   ※Active DirectoryとのID同期には、Enterprise Systems Connectorを使っています
- ➤ SaaSサービス: Office 365 Enterprise E3
   ※以後、「Office 365」と記載します
   ※Active DirectoryとのID同期には、Azure Active Directory Connectを使っています
- プライベート認証局Gléas (バージョン1.15.4)
   ※以後、「Gléas」と記載します
- クライアント(PC): Windows 10 Pro / Office 2016 / Internet Explorer 11
   ※以後、「Windows PC」と記載します
- ▶ クライアント(タブレット):iPad Air 2 (iOS 11.2.6)/

VMware Workspace ONE 3.2 / Microsoft Excel 2.10.1

※以後、「iPad」と記載します

※本書の設定ではiOSのKerberos SSO機能を利用します。Microsoft Authenticatorアプリの インストールは不要となります

以下については、本書では説明を割愛します。

- AirWatchでの基本設定や、順守ポリシーの設定方法
- AirWatchと、Gléasとのクライアント証明書発行の連携設定
   ※AirWatchとGléasの証明書発行およびプッシュ配信に関する連携設定について、弊社では以下のURLでドキュメントを公開しています
   https://www.gleas.jp/news/whitepaper/airwatch
- vIDMにおける基本設定、Office 365とのフェデレーション(認証連携)設定
- ADと、Office 365・vIDM・AirWatchとのID同期設定
- 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・設定
- Windows PCやiPadの操作方法

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。

■シナリオ1



- 1. 宅内のADよりOffice365と、vIDMにユーザ情報が同期されている状態
- 2. ユーザはGléasよりWindows PCに証明書をインポートする
- 3. Office 365にアクセスする
- Office 365とvIDMとで認証連携がおこなわれ、ユーザはvIDMにリダイレクト される。vIDMはユーザにクライアント証明書をリクエストする →証明書(クラウドデプロイ)認証
- 5. 有効な証明書を提示すると、Office 365にログインする

■シナリオ2 (デバイスコンプライアンスチェック)



- 宅内のADよりOffice365とvIDM、AirWatchにユーザアカウント情報が同期されている状態
- 2. Gléasと連携しているAirWatchからクライアント証明書がプッシュ配信される
- 3. Office 365にアクセスする
- Office 365とvIDMとで認証連携がおこなわれ、ユーザはvIDMにリダイレクト される。vIDMはユーザにクライアント証明書をリクエストする →モバイルSSO(iOS)認証
- 5. デバイス識別番号を含む有効な証明書を提示すると、AirWatchに設定されてい る当該デバイスのポリシーの順守状態をチェックし、順守されていればOffice 365にログインする
- 1.4. 留意事項

シナリオ1では、クライアント証明書に以下の属性を含める必要があります。

- CRL配布点
- OCSP (Authority Information Access)
- ユーザプリンシパル名(Active DirectoryのuserPrincipalName)

シナリオ2では、上記の失効関連の属性(CRL配布点、OCSP)に加えて以下の 属性をクライアント証明書に含める必要があります。

- 拡張鍵用途:PKINITクライアント認証
- ユーザプリンシパル名(AirWatchで管理する「ユーザプリンシパル名」)
   Gléasでは、別名(プリンシパル名)属性の「疑似定数(アカウント名のCN部分)」をテンプレートに含めるようにします。
- サブジェクトの別名: AirWatchが管理するデバイスID
   Gléasでは、別名(DNS)属性の「疑似定数(アカウント名のUDID部分)」を
   テンプレートに含めるようにします。

また、Gléas内部(或いは外部サーバ)でOCSPレスポンダが適切に動作してい る必要があります。

# 2. シナリオ1:vIDMの設定

#### 2.1. 信頼するルート認証局の設定

今回利用するクライアント証明書のトラストアンカとなるルート CA の証明書をダウンロードします。

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。



2.2. 認証プロバイダの設定

Workspace ONE の管理者サイトにログインし、画面上部の[ID とアクセス管理]タ

プライベート認証局 Gléas ホワイトペーパー

VMware Identity Manager (vIDM) でのクライアント証明書認証設定

ブを選択し、[認証方法]>[証明書(クラウドデプロイ)]と進み、∞(構成)をクリ ックします。

以下を設定します。

- [証明書アダプタを有効にする]をチェック
- [ルート及び中間 CA 証明書]に、2.1 項でダウンロードしたルート証明書をアッ プロード
- [ユーザーID の検索順序]に、"UPN"を選択
- [証明書の失効を有効にする]をチェック
- [証明書の CRL を使用する]をチェック
- [OCSP の失効を有効にする]をチェック
- [OCSP の障害時に CRL を使用する]をチェック
- [OCSP Nonce を送信する]をチェック
- [OCSP の URL]に、Gléas、或いは外部の OCSP レスポンダの URL を設定
   ※以下の[証明書の OCSP の URL を使用する]では、失効ステータスの確認が正常にできないケースが見受けられたため、ここにも URL を設定しフォールバックできるようにしています
- [証明書の OCSP の URL を使用する]をチェック
- [OCSP レスポンダの署名証明書]に、Gléas で設定された OCSP 署名用証明書
   をアップロード

# プライベート認証局 Gléas ホワイトペーパー

### VMware Identity Manager (vIDM) でのクライアント証明書認証設定

CertificateServiceAut	thAdapter
証明書アタフタを有効にす る	<ul> <li></li> </ul>
	有効にすると、ロード バランサ上で SSL を終了できなくなります (ロード バランサはバススルーとして設定 する必要があります)。
ルートおよび中間 CA 証明 ま*	ファイルを選択
8	連結 PEM ファイルを含む DER および PEM 形式の複数のルートおよび中間 CA 証明書をアップロードできま す
マップロードさわた CA 証	2 CN=Evaluation CA
明書	(25992A95C453176C0090A72799F63657F49014192FB2423C10B6E9596ED27EA0) X
ユーザー ID の検索順序	UPN ~
	証明書内のユーザー ID の検索順序を選択します。UPN: Subject Alternative Names (SAN) の UserPrincipalName 値、E メール: Subject Alternative Names (SAN) のメール アドレス、サブジェクト: サブ ジェクトの UPD 使
UPN フォーマットを検証	
	 UserPrincipalName フィールドのフォーマットを検証
要求のタイムアウト	0
	- 応答待機のタイムアウト(秒)。値0を指定すると、タイムアウトなしで待機します。
承認された証明書ポリシー	
	別の値を追加
	証明書ポリシー拡張で承認されたオブジェクト識別子 (OID) リスト
証明書の失効を有効にする	
	失効チェックを有効にするには、チェックボックスを選択します
証明書の CRL を使用する	
	証明書の CRL 配布ポイント拡張を使用するには、チェックボックスを選択します
CRL の場所	
	失効チェックで使用する CRL の場所 (例: http://crlurl.crl or file:///crlFile.crl)
OCSP の失効を有効にする	$\checkmark$
OC SP の障害時に CRL を	
使用する	0000 の管字時に 001 も体田オフには、ゴーックゼックフを図ね」 ナオ
OCSP Nonce を送信する	してきたいないのでは、デエッジパックスを選びしよう
OCSP NOTICE -Z.MAP S	▼ OCSP 要求に nonce を含めるには、チェックボックスを選択します
OCSP Ø URL	http://ocsp.avampla.com/2560
	大効チェックで使用する OCSP の URL (例: http://ocspurl.com)。
証明書の OCSP の URL を	
使用する	
	証明音の OCSP の URL を優先します。利用できない場合は、構成済み OCSP の URL にフォールバックします。
OCSP レスポンダの署名証 明書	ファイルを選択
	複数の DER および PEM でエンコードされた OCSP レスポンダの証明書をアップロードできます
アップロードされた OC SP 署名証明書	O=JCCH Security Solution Systems, CN=ocsp_sign (D3791F1A46C2003C55F1E9AFAC322721BC080D336EC28FC8923254BAB4F622DB) ¥
認証前に同意書を有効にす	
<u>බ</u>	
日卒事。中的	証明實総証を使用してロクインする則に同意書ウインドウを含めるには、チェックボックスを選択します
同息者の内容	
	表示する同意習の内容
	キャンセル 保存

2.3. 認証ポリシーの設定

Workspace ONE の管理者サイトで、画面上部の[ID とアクセス管理]タブを選択し、 [ポリシー]と進み、Office 365 の認証ポリシーを選択します。 ポリシールールを追加する場合は、[+]ボタンをクリックし以下を設定します

- 「ユーザーのネットワーク範囲が次の場合…]に、"すべての範囲"を選択
- [およびユーザーのコンテンツアクセス元が次の場合...]に、"Windows 10"を選 択
- [次に、以下の方法を使用して認証することができます]に、"証明書(クラウドデ プロイ)"を選択

ポリシー ルールの編集	
ユーザーのネットワーク範囲が次の場合	すべての範囲~
およびユーザーのコンテンツ アクセス元が次の場合	Windows 10 ~
また、ユーザーが次のグループに属する場合	グループが選択されていませんでした。 このポリシー ルールは すべてのユーザーに適用されます。
	グループを編集
次に、以下の方法を使用して認証することができます	
証明書 (クラウド デプロイ)	
先行する認証方法が失敗するか適用できない場合は、以下を実行します	3
-認証方法の選択	
	キャンセル OK

また、default\_access\_policy\_set も同様に"証明書(クラウドデプロイ)"に変更し ておきます。 ※Windows の Office アプリケーションでの認証(先進認証)はデフォルトのポリシー設定が適用 されるため

vIDM 側の設定は以上です。

# 3. シナリオ1:Gléasの管理者設定

※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

3.1. 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-

覧]画面に移動し、Windows PC用となるUA(申込局)をクリックします。



[申込局詳細]画面が開くので、以下の設定をおこないます。

- [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	5	

設定終了後、[保存]をクリックし設定を保存します。 以上でGléasの設定は終了です。

### 4. シナリオ1: Windows PC での証明書インポート

4.1. Gléas の UA からのインストール

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。 ※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ます

その後、 [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 インポートがおこなわれます。

			:	Jəan-dea Gléas 🛛
[AW テスト さんの	のページ]			■ ログアウト
ユーザ情報				
🙎 AW テスト a	さんのページ			▶ <u>ヘルブ</u>
🖢 ユーザ情報				~
▶ユーザ	登録日時:20	018/02/22 18:32		
>メールアドレス: >パスワード:***** ★ 証明書情報 > 発行済み証明書			4 405B	
#	来(T向		有 如果的	
	Web ページt	からのメッセージ ユーザの証明書ストア・	ヘインポートしました。	X
			ОК	

「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-rca Gléäs
W テスト さん	のページ]			▶□グアウ
ーザ情報				
AW テスト	さんのページ	_	_	▶ <u>ヘルブ</u>
2 ユーザ情報				,
▶ユーザ	登録日時:20	18/02/22 18:32		
》 姓:AW 名: > ユーザID:aw-t > メールアドレス: > バスワード:***	テスト est01@js3-test13.xyz			
<b>桊</b> 証明書情報				
▶発行済み証明書	ł			
#	発行局	シリアル	有効期限	証明書ストアヘインポート
-				

4.2. Office 365 へのアクセス認証

クライアント証明書がインポートされたWindows PCのブラウザや、Word・Excel

といったOfficeアプリケーションでOffice 365にアクセスすると、Office 365から 認証連携されたvIDMへリダイレクトされ、クライアント証明書の選択ダイアログ が表示されます。

Windows セキュリティ		×	
証明書の選択		1	
サイト cas-aws.vmwareidentity.as	ia に対する資格情報が必要で	<b>J</b> :	Workspace ONE
aw-test01@js3-test13.	xyz		
発行者: Evaluation CA			
有効期間: 2018/02/22	から 2018/03/22		
証明書のプロパティを表示	えします		
その他			
ОК	キャンセル		
			vmware

証明書認証が成功するとOffice 365にログインします。

クライアント証明書がない場合や、失効された証明書でアクセスするとエラーになります。



# 5. シナリオ2:AirWatchの設定

※1.2 項に記載の通り、AirWatch と Gléas での証明書発行の連携設定がすでにおこなわれていることを前提 とします

### 5.1. 証明書発行テンプレートの設定

AirWatch管理コンソールにログインし、[デバイス] > [証明書] > [認証局]と進みま す。[要求テンプレート]タブをクリックし、該当のテンプレートを編集します。

- [プロファイルID]は、Gléasにあらかじめ作成してあるグループIDを指定 ここで指定するグループには1.4項に記載されたとおりのテンプレートが適用されている必 要があります
- [サブジェクト名]は、以下の通りに設定 CN={DeviceUid}.{UserPrincipalName}

証明書テンプレートの追	5加/編集	
名前*	gleas_template	
説明	for Device Compliance Check	]
認証局*	Gleas Test CA ×	]
プロファイル ID*	testgroup	]
プロダクトコード*	0	
有効期間 (年)*	1 ~	]
サブジェクト名	CN={DeviceUid}.{UserPrincipalName}	+
証明書の自動更新		
証明書の取り消しを有効化	(j)	
	保存 保存 保存して別のテンプレートを追加	キャンセル

### 5.2. プロファイルの設定

AirWatch 管理コンソールより、 [デバイス] > [プロファイルとリソース] > [プロフ ァイル]と進みます。[追加] > [プロファイルを追加] > [Apple iOS]をクリックし、 プライベート認証局 Gléas ホワイトペーパー

VMware Identity Manager (vIDM) でのクライアント証明書認証設定

以下を設定します。

※プロファイルの各項目の設定については、設定項目が多岐にわたることや本書の主旨と異なるので割愛します

【資格情報】

- 資格情報ソース:アップロードを選択
- 資格情報名:任意の名称
- 証明書:以下からダウンロードした証明書をアップロード
   Workspace ONE 管理者サイトにログインし、画面上部の[ID とアクセス管理]
   タブを選択し、[ID プロバイダ]から対象の ID プロバイダを選択し、[KDC 証明書のエクスポート]から"証明書のダウンロード"リンクをクリック

【資格情報 #2】

- 資格情報ソース:[定義済み認証局]を選択
- 認証局:あらかじめ設定した認証局を選択
- 証明書テンプレート:5.1 項で設定した証明書テンプレートを選択

資格情報		資格情報#2	
資格情報ソース	アップロード ・	資格情報ソース	定義済み認証局 🗸
資格情報名 *	DC=selfsigned, CN=kdc-CA-cert	認証局 *	Gleas Test CA
証明書 *	証明書アップロード 変更	証明書テンプレート *	gleas_template v
タイプ	Cert		
発行先	DC=selfsigned, CN=kdc-CA-cert		
発行者	DC=selfsigned, CN=kdc-CA-cert		
有効期限開始日	2015/12/10		
有効期限終了日	2025/12/07		
サムプリント	15E4E4CFFDDB2243C1D09850C7D6EC7DE93B094B		

【シングルサインオン】

- アカウント名:任意の管理名称
- Kerberos プリンシパル名:{EnrollmentUser}を選択
- レルム:VMWAREIDENTITY.ASIA (vIDM のドメイン名)
- 更新証明書:証明書 #2 を選択
- URL プレフィックス:https://<テナント名>.vmwareidentity.asia

アプリケーション

モバイル SSO の対象とするアプリケーションバンドル ID を記入 ※ 以下はバンドル ID の例となります(大文字小文字を区別します) com.apple.mobilesafari (モバイル Safari)

#### 15 / 21

com.air-watch.appcenter	(Workspace ONE アプリ)
com.microsoft.Office.Word	(Microsoft Word)
com.microsoft.Office.Excel	(Microsoft Excel)
com.microsoft.Office.Power	point (Microsoft PowerPoint)
com.microsoft.Office.Outloo	k (Microsoft Outlook) など

シングル サインオ	2			IOS 7
接続情報				
アカウント名	jcch-sss			
Kerberos プリンシパル名	{EnrollmentUser}		+	IOS 7
	VMWAREIDENTITY.ASIA			IOS 7
更新証明書	証明書 #2	v		IOS 8
URLプレフィックス				
このアカウントを HTTP 上の Kerbe	eros 認証で使用する際に一致さ	せなければならない、URL プレフ	フィックスの一覧。	
URL				
1				
nttps://jccn-security-solution-sys	tems.vmwareidentity.asia X			
nttps://jccn-security-solution-syst	tems.vmwareidentity.asia			
nttps://jccn-security-solution-syst	tems.vmwareidentity.asia			
nttps://jccn-security-solution-sys	tems.vmwareidentity.asia		マテルマゴリ語のマニ海田」	± *
nttps://jcch-security-solution-sys ② 追加 アプリケーション このログインの使用を許可されたア	terns.vmwareidentity.asia X プリ識別子の一覧。この項目か	「ない場合は、このログインはす	べてのアプリ識別子に適用し	ます。
nttps://jcch-security-solution-sys ② 追加 アプリケーション このログインの使用を許可されたア アプリケーション/ンドルD com.apple.mobilesafari	tems.vmwareidentity.asia X アプリ識別子の一覧。この項目か	「ない場合は、このログインはす	べてのアプリ識別子に適用し	ह <b>.</b> इ.
nttps://jcch-security-solution-sys ② 追加 アプリケーション このログインの使用を許可されたア アプリケーションバンドルロ com.apple.mobilesafari com.air-watch.appcenter	tems.vmwareidentity.asia アプリ識別子の一覧。この項目か	「ない場合は、このログインはす	べてのアプリ識別子に適用し	ます <b>.</b>
nttps://jcch-security-solution-sys つ 追加 アプリケーション このログインの使用を許可されたア アプリケーション/(ンドルD com.apple.mobilesafari com.air-watch.appcenter com.microsoft.azureauthenticate	tems.vmwareidentity.asia マブリ識別子の一覧。この項目カ ン ン or	「ない場合は、このログインはす	べてのアプリ識別子に適用し	ます。
nttps://jcch-security-solution-sys ② 追加 アプリケーション このログインの使用を許可されたア アプリケーション/ンドルD com.aprie.mobilesafari com.air-watch.appcenter com.microsoft.azureauthenticato com.microsoft.Office.Excel	terns.vmwareidentity.asia アプリ識別子の一覧。この項目か ン or	「ない場合は、このログインはす	べてのアプリ識別子に適用し	ŧŢ,
nttps://jcch-security-solution-sys う 追加 アプリケーション このログインの使用を許可されたア アプリケーション//ンドルD com.apple.mobilesafari com.air-watch.appcenter com.microsoft.azureauthenticato com.microsoft.Office.Excel com.microsoft.Office.Powerpoint	terns.vmwareidentity.asia アプリ識別子の一覧。この項目か ン or	5ない場合は、このログインはす	<てのアブリ識別子に適用し	ます。
nttps://jcch-security-solution-sys う 追加 アプリケーション このログインの使用を許可されたア アプリケーション/(ンド)レD com.apple.mobilesafari com.air-watch.appcenter com.microsoft.office.Excel com.microsoft.Office.Excel com.microsoft.Office.Powerpoint com.microsoft.Office.Powerpoint	terns.vmwareidentity.asia マプリ識別子の一覧。この項目か ン マ マ 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	「ない場合は、このログインはす	べてのアプリ識別子に適用し	ます。

# 6. シナリオ2:vIDMの設定

6.1. 認証プロバイダの設定

Workspace ONE の管理者サイトにログインし、画面上部の[ID とアクセス管理]タ ブを選択し、[認証方法] > [モバイル SSO(iOS 版)]と進み、◎(構成)をクリックし ます。

以下を設定します。

- [KDC 認証を有効にする]をチェック
- [ルート及び中間 CA 証明書]に、2.1 項でダウンロードしたルート証明書をアッ

プロード

- [OCSP を有効にする]をチェック
- [OCSP Nonce を送信する]をチェック
- [OCSP レスポンダの署名証明書]に、Gléas で設定された OCSP 署名用証明書
   をアップロード

KdcKerberosAuthAdapter			
KDC 認証を有効にする	$\checkmark$		
	Kerberos をサポートするデバイスを使用したユーザー ログインを有効にします。		
レルム	VMWAREIDENTITY.ASIA		
	このアダプタを使用した認証の実行に使用されるキー配布センター (KDC)の ID。		
ルートおよび中間 CA 証明 書	ファイルを選択		
	連結 PEM ファイルを含む DER および PEM 形式の複数のルートおよび中間 CA 証明書をアップロードしま す。		
アップロードされた CA 証 明書のサブジェクト DN	CN=Evaluation CA 🗶		
OC SP を有効にする	$\checkmark$		
	証明書のオンライン証明書ステータス プロトコル (OCSP) チェックを有効にします。AirWatch CA などの OCSP をサポートしない認証局には OCSP を選択しないでください。		
OCSP Nonce を送信する	$\checkmark$		
	各 OCSP 要求に Nonce を含めることで、レスポンス リプレイ攻撃から保護します。		
OCSP レスポンダの署名証 明書	ファイルを選択		
	OCSP レスポンスへの署名に使用する証明書をアップロードします。		
OC SP レスポンダの署名証 明書サブジェクト DN	O=JCCH Security Solution Systems, CN=ocsp_sign X		
キャンセル メッセージ			
	ユーザーの認証中に表示されるログイン メッセージをカスタマイズします。		
キャンセル リンクを有効に する			
	[キャンセル] を有効にすると、ユーザーはログイン ページで [キャンセル] をクリックして Kerberos 認証を停 止できるようになります。		
エンタープライズ デバイス 管理サーバの URL			
	キャンセル 保存		

### 6.2. 認証ポリシーの設定

Workspace ONE の管理者サイトで、画面上部の[ID とアクセス管理]タブを選択し、 [ポリシー]と進み、Office 365 の認証ポリシーを選択します。 ポリシールールを追加する場合は、「+]ボタンをクリックし以下を設定します。

- [ユーザーのネットワーク範囲が次の場合…]に、"すべての範囲"を選択
- [およびユーザーのコンテンツアクセス元が次の場合...]に、"iOS"を選択
- [次に、以下の方法を使用して認証することができます]に、"モバイル SSO(iOS 版)"を選択。さらに[+]をクリックし"デバイスコンプライアンス (AirWatch)" を選択追加

ハリノールールの補朱			
ユーザーのネットワーク範囲が次の場合		すべての範囲	~
およびユーザーのコンテンツ アクセス元が次の場	合	OS	~
また、ユーザーが次のグループに属する場合	クす	ループが選択されていませ べてのユーザーに適用され グループを編集	もんでした。 このポリシー ルールは います。
次に、以下の方法を使用して認証することができ	<b>हे</b> जु		
モバイル SSO (IOS 版)	+ および デバイス	コンプライアンス (AirWatch	n) 🎽 🗙
<ul> <li>モバイル SSO (iOS 版) -</li> <li>先行する認証方法が失敗するか適用できない場合</li> </ul>	★ および デバイス : は、以下を実行します:	コンプライアンス (AirWatch	1) 🖌 🗶
モバイル SSO (iOS 版)     -       先行する認証方法が失敗するか適用できない場合       -認証方法の選択-	<ul> <li>▶ および デバイス :</li> <li>は、以下を実行します:</li> </ul>	コンプライアンス (AirWatcł	1) 🗠 🗙

また、default\_access\_policy\_set も同様に"モバイル SSO(iOS 版)"に変更しておきます。

※Workspace アプリでの認証のため

vIDM 側の設定は以上です。

# 7. シナリオ 2: iPad からの接続

### 7.1. クライアント証明書の配信

AirWatchの管理下になり5項で設定したプロファイルが適用されたiPadには AirWacthより自動的にクライアント証明書および各種設定がプッシュ配信されま す。

配信された設定内容は、[設定]アプリ > 一般 > プロファイルとデバイス管理 > モバイルデバイス管理 > デバイスマネージャーと進むことで確認することができます。



7.2. Office 365 へのアクセス認証

クライアント証明書がインポートされたiOSデバイスのブラウザやWorkspaceアプリ、各種OfficeアプリケーションでOffice 365にアクセスすると、Office 365から認証連携されたvIDMへリダイレクトされます。 その後、自動的に証明書認証がおこなわれOffice365にログインします。

以下はSafariやWorkspaceアプリでアクセスした場合の画面です。



以下はExcelアプリケーションでアクセスした場合(先進認証)です。



ログインしようとする端末がAirWatchで定められたポリシーを順守していない場 合は、ログインできません(デバイスコンプライアンス機能)。

以下はiOSバージョンが定められたポリシーにしたがっていない場合の画面表示で す。



証明書が失効されている場合や、シングルサインオン(Kerberos認証)の設定が 適切にされていない場合は、以下の画面が表示されます。



# 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。

■Workspace ONE(Airwatch/vIDM)に関するお問い合わせ先 ヴイエムウェア株式会社 URL: http://www.vmware.com/jp/company/contact.html

#### ■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