JCCH・セキュリティ・ソリューション・システムズ

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

- 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

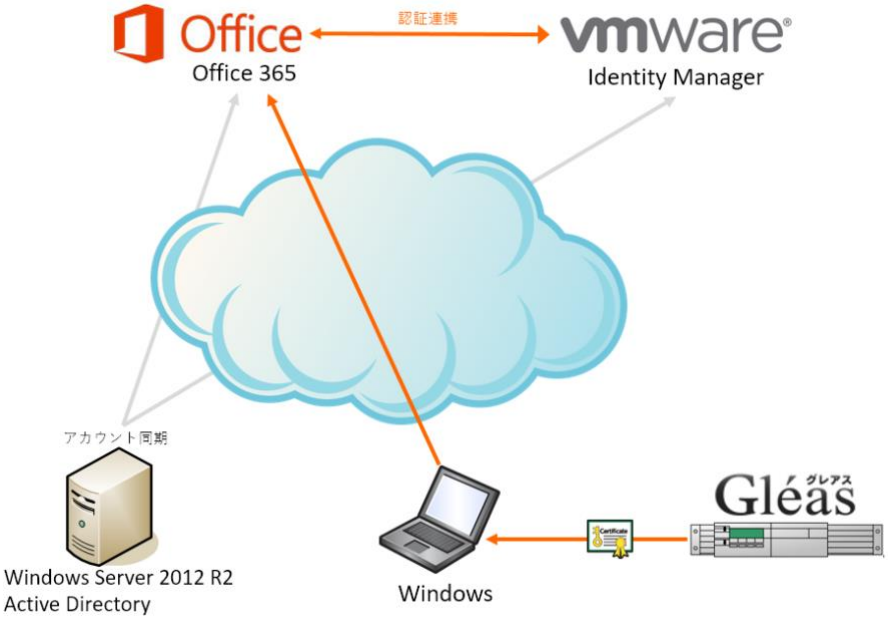
  https://www.gleas.jp/news/whitepaper/airwatch
- vIDMにおける基本設定、Office 365とのフェデレーション（認証連携）設定
- ADと、Office 365・vIDM・AirWatchとのID同期設定
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作・設定
- Windows PCやiPadの操作方法

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

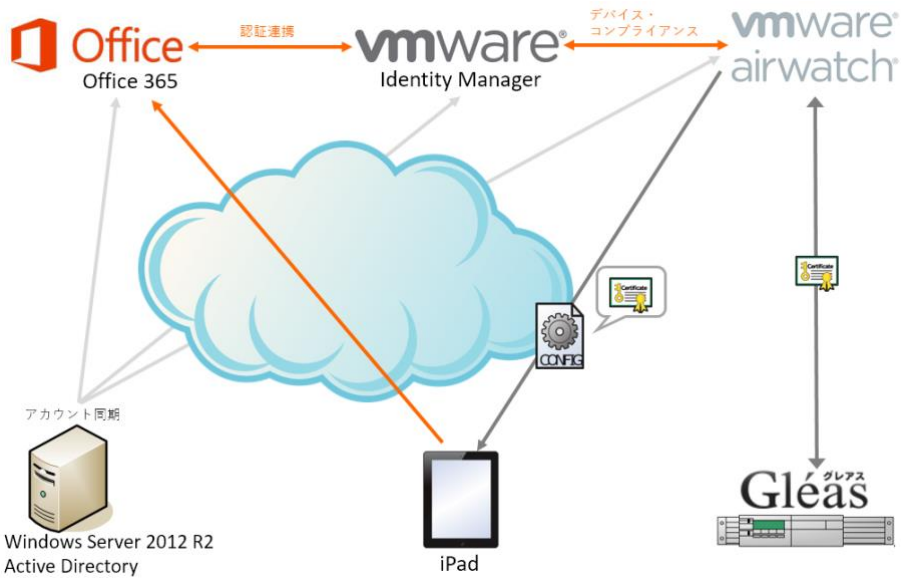
本書では、以下の構成で検証を行っています。

■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
4. 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）



1. 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
4. 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。

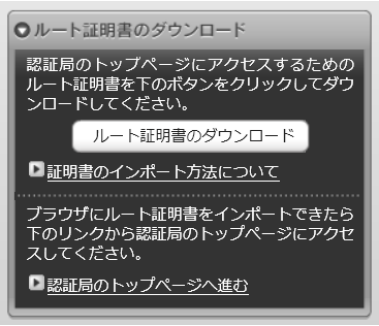
- 拡張鍵用途：PKINITクライアント認証
- ユーザプリンシパル名（AirWatchで管理する「ユーザプリンシパル名」）
  Gléasでは、別名(プリンシパル名)属性の「疑似定数（アカウント名のCN部分）」をテンプレートに含めるようにします。
- サブジェクトの別名：AirWatchが管理するデバイスID
  Gléasでは、別名(DNS)属性の「疑似定数（アカウント名のUDID部分）」をテンプレートに含めるようにします。

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

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


CertificateServiceAuthAdapter
証明書アダプタを有効にする
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 バランサはパ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できます
アップロードされた CA 証明書
CN=Evaluation CA
(25992A95C453176C0090A72799F63657F49014192FB2423C10B6E9596ED27EA0)
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 UID 値
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
OCSP の障害時に CRL を使用する
OCSP の障害時に CRL を使用するには、チェックボックスを選択します
OCSP Nonce を送信する
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 の URL
http://ocsp.example.com:2560
失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
証明書の 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 OCSP 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る
証明書認証を使用してログインする前に同意書ウィンドウを含めるには、チェックボックスを選択します
同意書の内容
表示する同意書の内容
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

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[認証局一

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。

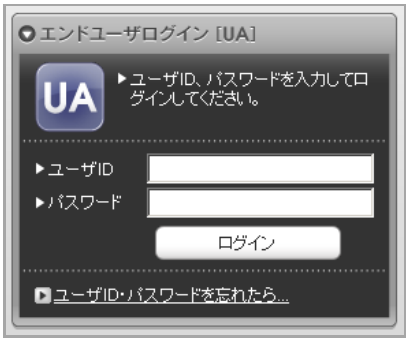
- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

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

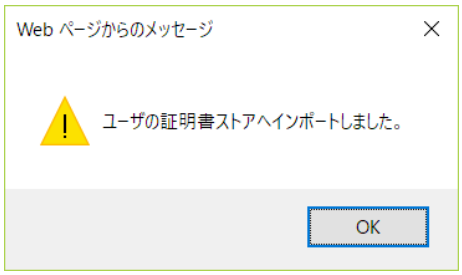
4.1. Gléas の UA からのインストール

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。

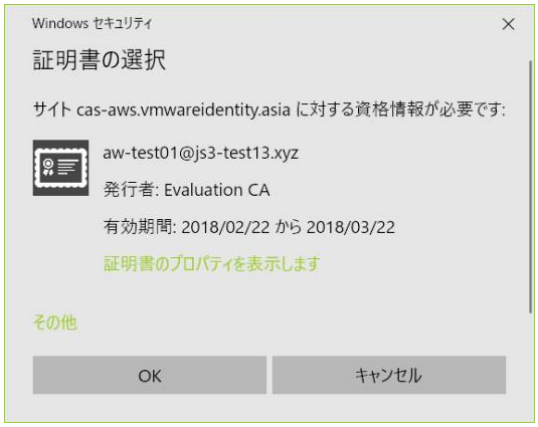


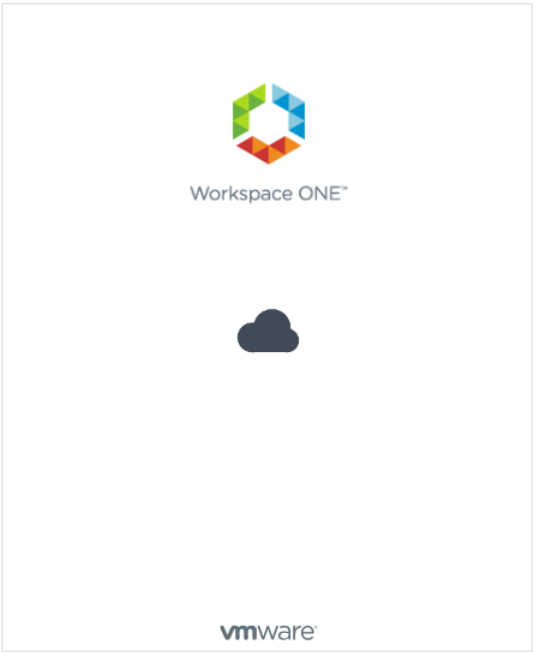
「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。

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。





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。

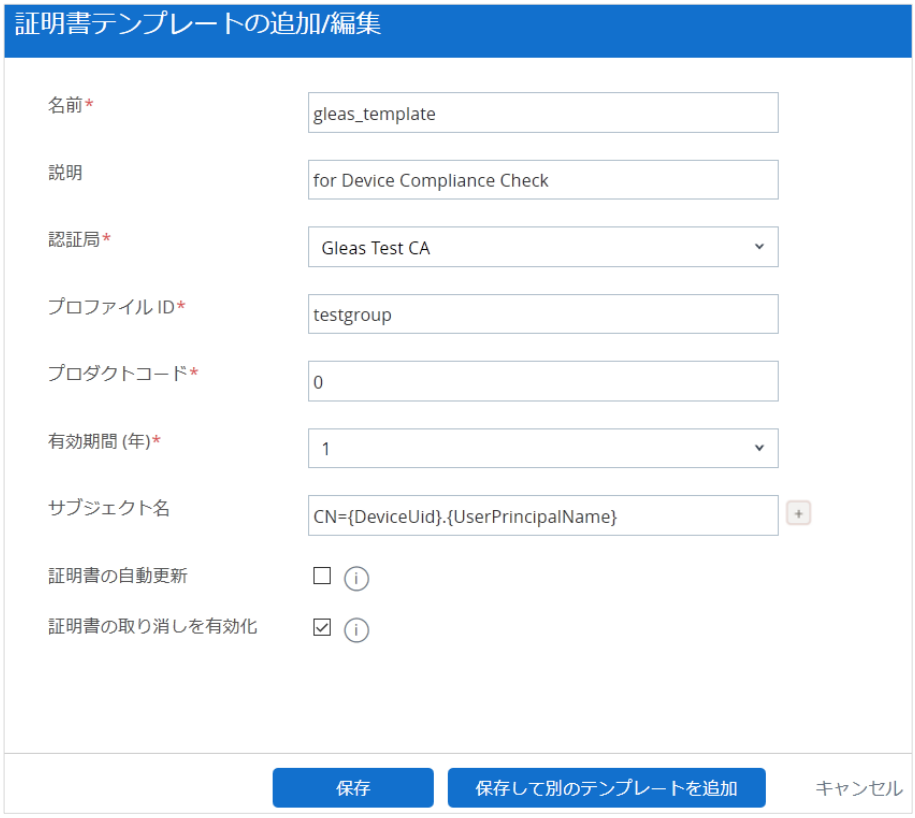
5. シナリオ2：AirWatchの設定

※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}



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、

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

【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）

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

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

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

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