Workspace ONE UEM 管理コンソールガイド(入門編)

Workspace ONE UEM 2011 WebUI ベース

2021 年 2 月 19 日
株式会社ウィザース

改訂履歴

ver.	発行日	改訂履歴
1.00	2013 年 11 月 20 日	初版発行
2.00	2014 年 2 月 26 日	第二版発行
3.00	2014 年 7 月 31 日	第三版発行
4.00	2014 年 12 月 31 日	第四版発行
5.00	2015 年 7 月 31 日	第五版発行
6.00	2016 年 1 月 20 日	第六版発行
6.01	2016 年 3 月 8 日	第六版更新
7.00	2016 年 7 月 19 日	第七版発行
8.00	2016 年 10 月 1 日	第八版発行
8.01	2016 年 11 月 16 日	第八版更新
9.00	2017 年 4 月 24 日	第九版発行
10.0	2018 年 6 月 20 日	第十版発行　AirWatch Ver9.2 対応
11.0	2018 年 8 月 21 日	第十一版発行　Workspace ONE UEM Ver9.5 対応
12.0	2019 年 1 月 18 日	第十二版発行　Workspace ONE UEM Ver18.11 対応
13.0	2019 年 11 月 1 日	第十二版発行　Workspace ONE UEM 1909 版
14.0	2020 年 7 月 7 日	第十二版発行　Workspace ONE UEM 1909 Web UI ベース版
15.0	2020 年 12 月 25 日	第十三版発行　Workspace ONE UEM 2011 Web UI ベース版

※ バージョン 9.4 より、コンソールの名称が " AirWatch Console " から " Workspace ONE UEM Console " に変更されました。

目　次

1 本書について

Workspace ONE UEM の SaaS を初めて操作される方を対象に、下記手順について説明しています。

・Workspace ONE UEM へのログイン
・ユーザー登録
・デバイスの状態確認とリモート操作

上記に無い SaaS の操作手順については、次の２つのガイドをご参照ください。

Workspace ONE UEM 管理コンソールガイド(初級編)
・ユーザー管理
・デバイス操作
・プロファイル

Workspace ONE UEM 管理コンソールガイド(機能編)
・機能別ガイドの概略
・システム設定
・アプリケーションの管理
・コンプライアンスの管理
・レポートの管理

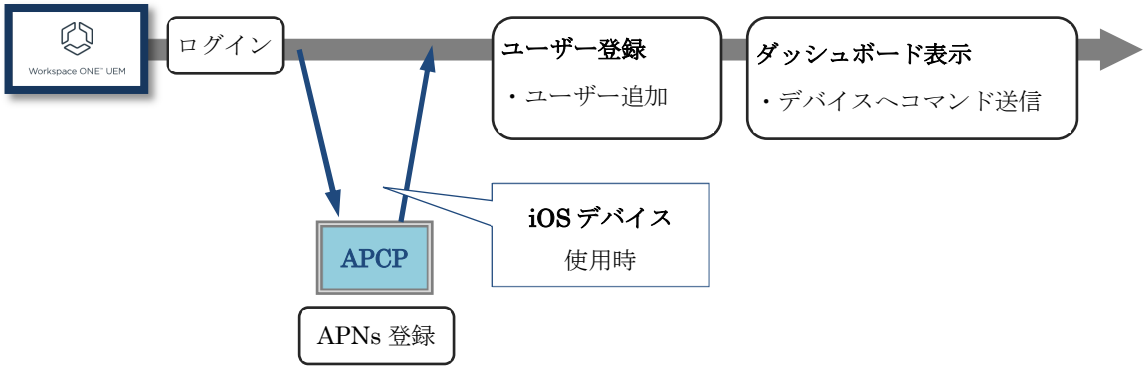
デバイス*の操作についてのガイドは、以下のようになっています。

かんたんセットアップガイド_Android 編
かんたんセットアップガイド_iOS 編

*デバイス： Android のスマートフォンとタブレット、iPhone、iPad、iPod touch
*iOS デバイス：iPhone、iPad、iPod touch

2 本書での操作の流れ

本書は下記図のように操作の流れを説明しております。



APCP：Apple Push Certificates Portal（Apple 社のサイト）

APNs：Apple Push Notification Service（iOS デバイスへ情報を送るサービス）

3 ご利用にあたっての準備

Workspace ONE UEM の利用開始にあたって、以下を準備してください。

✓ **Apple ID**

・既存アカウントの流用は避け、**Workspace ONE UEM 専用の Apple ID** をご用意ください。

・iOS 以外のデバイス使用時は、必要ありません。

✓ **VMware Workspace ONE SaaS 確認書**

・Workspace ONE UEM 管理コンソールの初回ログイン時やデバイスを Workspace ONE UEM (AirWatch)に加入させる時に必要な情報が記載されています。

✓ **Workspace ONE UEM 管理者アカウント アクティベーション メール**

・お申込みいただいた管理者様 E メールアドレスに件名「**Workspace ONE UEM 管理者アカウント アクティベーション**」のメールが届きます。管理者アカウントパスワード変更のリンク URL が記載されています。

✓ **Workspace ONE UEM 管理コンソール用 PC**

・以下の Web ブラウザ（いずれか）を利用して Workspace ONE UEM 管理コンソールを操作します。

Chrome
Firefox
Safari(Mac 版)

・最新バージョンの Web ブラウザのご使用を推奨しております。

・上記以外では、表示不良や操作が出来ない等の問題が発生する事があります。
特に IE は後述「5 APNs の登録」で問題となる為、使用しないでください。

✓ **管理対象デバイス**

・Workspace ONE UEM で管理予定のモバイルデバイスです。

・旧デバイスの場合、デバイスでご利用予定の Workspace ONE プロダクト(アプリケーション)より、以下の対応表で使用可否をご確認ください。

iOS & iPadOS 2021 年 2 月 19 日現在

Workspace ONE(AirWatch)プロダクト	サポート iOS Version
MDM 機能サポート	iOS 12
VMware Workspace ONE Intelligent Hub	iOS 12.2+※
VMware Workspace ONE Boxer	iOS 12.2+※
VMware Workspace ONE Web	iOS 12+※
VMware Workspace ONE Content	iOS 12+※
VMware Workspace ONE Tunnel	iOS 10.3+※

※ iOSバージョンがリリースされると、3世代前iOSバージョンのサポートは終了します。例、iOS 15 がリリースされると、VMware Workspace ONE アプリケーションの次のリリースバージョンではiOS 12のサポートが廃止される予定です。

※ 利用可能なバージョンのアプリは以前のiOSバージョンのデバイス上でこれまでどおり機能しますが、より新しいバージョンで導入された機能やバグ修正はご利用いただけません。

Android　　2021 年 2 月 19 日現在

Workspace ONE(AirWatch)プロダクト	サポート Android Version
VMware Workspace ONE Intelligent Hub	Android 4.4+
VMware Workspace ONE Boxer	Android 5.1+
VMware Workspace ONE Web	Android 5.0+
VMware Workspace ONE Content	Android 8+
VMware Workspace ONE Tunnel	Android 5.1+

※ 新しいOSバージョンでのみ使用可能なAPIに依存する可能性があるため、古いOSバージョンではすべての製品機能が使用できるわけではありません。さらに、一部の製品機能はサードパーティのライブラリに依存します。

4　Workspace ONE UEM 管理コンソールへログインする

PC で Web ブラウザを起動し、Workspace ONE UEM 管理コントールにログインします。

4.1. 初回ログイン

1) **Workspace ONE UEM 管理者アカウント アクティベーション メール**に記載されている**パスワードのリセットリンク**をクリックします。

重要
パスワードのリセット リンクの有効期限は 48 時間(2 日間)です。有効期限が過ぎた場合は、弊社サポートまでお問い合せください。

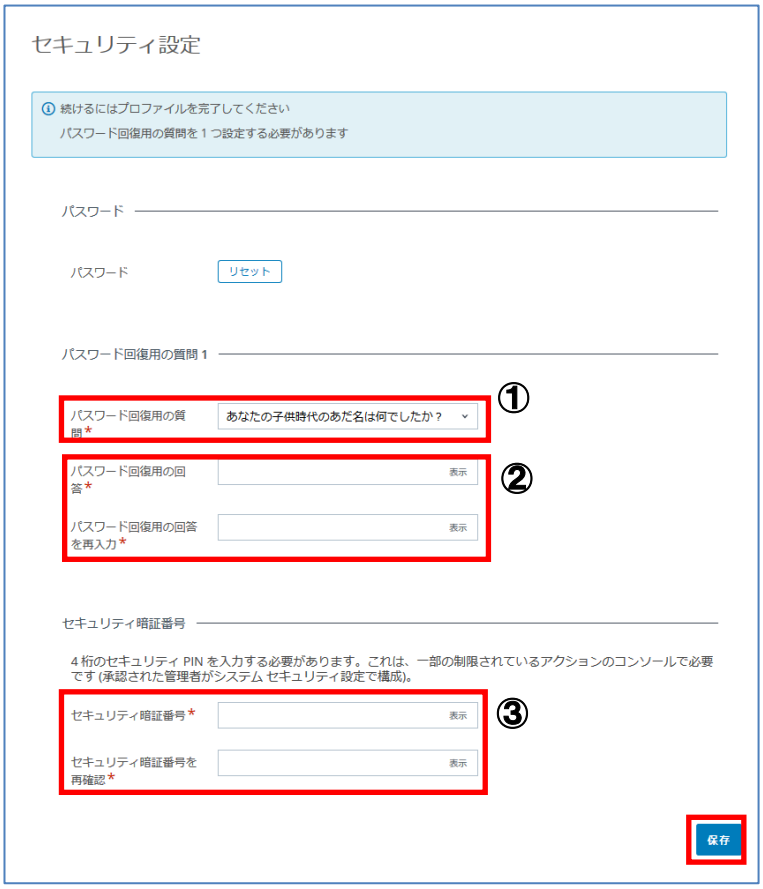
2) Workspace ONE UEM 管理コントールのパスワード変更の画面が表示されます。新しい**パスワード**を入力し、**送信**をクリックします。

3) Workspace ONE UEM 管理コントールのログイン画面が表示されます。画面のユーザー名とパスワードに対し、**VMware Workspace ONE SaaS 確認書**に記載の**アカウント**と設定した**パスワード**を入力し、ログインをクリックします。

4) **VMware Cloud Service 製品のサービス利用規約 (TOS)** が表示されます。[承諾] をクリックします。

5) **セキュリティ設定**の画面が表示されます。下記の必須項目①～③を設定し、[保存] をクリックします。項目名の後に＊がついているものは入力必須項目です。

重要
他の管理者アカウントからパスワードの変更が行えません。パスワード回復の質問と回答がわからなくなると、管理コンソールにログインが行えなくなりますので、ご注意ください。



必須項目		設定
①	パスワード回復用の質問	パスワード回復時に求められる質問を選択します。
②	パスワード回復用の回答	上記①で選択した質問に対する回答を設定します。
③	セキュリティ暗証番号	デバイスを Workspace ONE UEM へ加入する前の状態へ戻す”企業情報ワイプ”等の操作で入力を求められる 4 ケタの数字を設定します。

6)ログインが完了すると、**Workspace ONE UEM 管理コンソール画面**が表示されます。

4.2. 2 回目以降のログイン

2 回目以降は、上記「4.1 初回ログイン」の 3)のログイン画面になります。管理者アカウントとパスワードを入力すると、**Workspace ONE UEM 管理コンソール画面**が表示されます。

5 APNs の登録-iOS

iOS デバイスを管理するためには、**APNs** への事前登録が必要となります。
次の手順で証明書を作成し登録します。

① Workspace ONE UEM 管理コンソールから証明書要求をダウンロードする。
→ **5.1. 証明書要求をダウンロードする**

② APCP で証明書を作成する。
→ **5.2. APCP で証明書を作成する**

③ 作成した証明書を Workspace ONE UEM 管理コンソールで登録する。
→ **5.3. Workspace ONE UEM 管理コンソールで証明書を登録する**

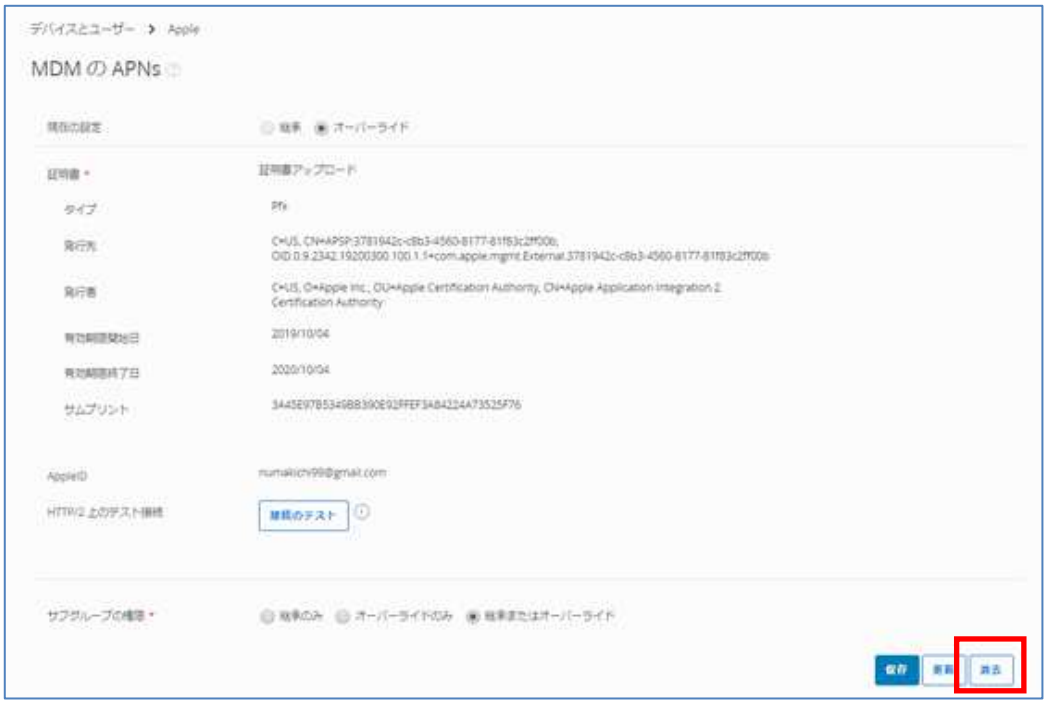
参考
iOS デバイスを利用しない場合、以降の操作（APNs の登録）は不要です。
次章の**ユーザー登録**へ進んでください。

5.1. 証明書要求をダウンロードする

1) [デバイス] > [デバイス設定] > [デバイスとユーザー] > [Apple] > [MDM の APNs]をクリックします。

2) [新しい証明書を作成] をクリックします。

[MDM 用の APNs] をクリック後に、次の画面が表示される場合があります。この場合は、[消去] をクリックし、[セキュリティ暗証番号] を入力すると、上記と同じ画面が表示されます。



3) [MDM_APNsRequest.plist] をクリックして、**AirWatch 証明書要求** をダウンロードします。

ご利用のブラウザのファイルダウンロードの操作で、MDM_APNsRequest.plist を（任意のフォルダへ）保存します。

5.2. APCP で証明書を作成する

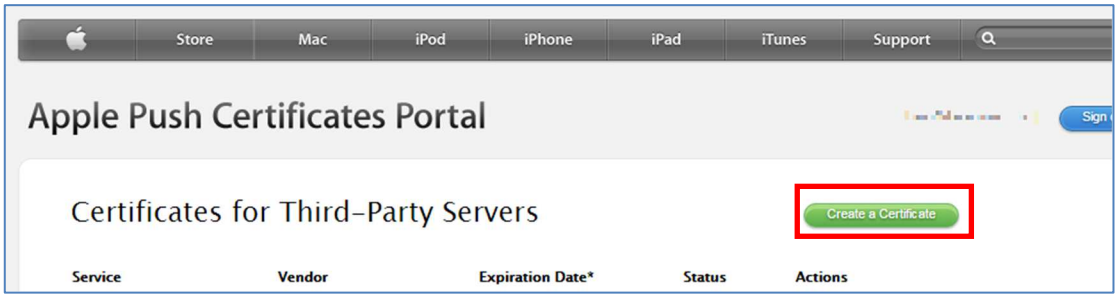
1) [Apple のサイトを開く] をクリックすると、Apple サインインの画面が表示されます。

重要
APCP を表示する際、Internet Explorer は使用しないでください！問題が生じることがあります。
APCP を表示する際、管理コンソールの画面は閉じないでください。管理コンソールの画面を閉じた場合は、APNs の登録に失敗するケースがあります。

2) Apple ID の資格情報(パスワード, 二要素認証)を利用して [サインイン] を行います。

参考
上記画面が表示されない場合（エラー、その他のメッセージが表示される）は、時間をおいて再度お試しください。エラーが続く場合、下記いずれかへご連絡ください。
・弊社サポート
・Apple 社サポート

3) ログイン後、[Create a Certificate] をクリックします。

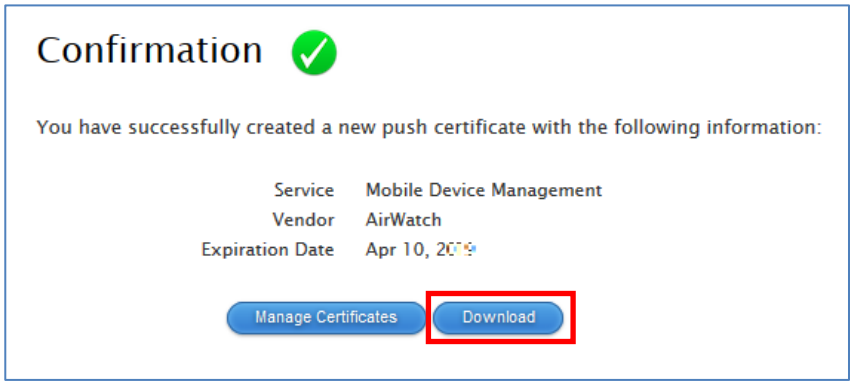


4) 内容を確認の上、同意の**チェック**をして[Accept] をクリックします。

5) [参照...] をクリックして、「5.1. 証明書要求をダウンロードする」のステップ 3 で保存した**証明書要求**のファイル（MDM_APNsRequest.plist）を選択します。

6) [Upload] をクリックして、**証明書要求**のファイルをアップロードします。

7) 要求が承認されると、確認画面が表示され[Download] をクリックします。



ご利用のブラウザのファイルダウンロードの操作で、MDM_AirWatch_Certificate.pem を（任意のフォルダへ）保存します。

Workspace ONE UEM 管理コンソールへ戻ります。

参考

クリック後にエラーで保存ができなかった場合

Apple のサイトに行く際、Workspace ONE UEM の管理コンソールを閉じてしまった場合は、

再度「5.1.証明書要求をダウンロードする」からやり直してください。

5.3. Workspace ONE UEM 管理コンソールで証明書を登録する

1) Workspace ONE UEM 管理コンソールに戻り、[次へ] をクリックします。

2) [アップロード] をクリックして「5.2. APCP で証明書を作成する」でダウンロード（保存）した MDM_ AirWatch_Certificate.pem をアップロードします。

[参照] をクリックしてファイルを指定し、[保存] をクリックします。

3) APCP で指定した Apple ID を入力して、[保存] をクリックします。

4) 4 桁の[セキュリティ暗証番号] を入力します。
セキュリティ暗証番号とは、「4.1 初回ログイン」5)で設定した 4 桁の数字です。

5) 正常に保存が行われると以下の画面表示になりますので、[サブグループの権限] が [継承またはオーバーライド] になっていることを確認します。

重要
証明書をアップロードして保存後、サブグループの許可がオーバーライドのみにチェックされている場合があります。この場合、下位の組織グループは APNs が継承されません。
下位の組織グループに所属する iOS デバイスがある場合は、必ず継承またはオーバーライドで保存してください。

6 デバイスの所有形態

Workspace ONE UEM では、デバイスの所有形態を指定することにより、構成プロファイルの配布やアプリケーションの展開を柔軟に行う事ができます。また、デバイスの情報収集やデバイスに対するコマンド実行の可否を設定するプライバシー設定と密接に関係しています。デバイス加入時にデバイスの所有形態を指定しない場合は、[未定義]のデバイスとして加入することとなり、プライバシー設定によっては意図しない動作になる場合があります。この為、デバイス加入時にデバイスの所有形態が自動的に[企業 – 専用]などになる設定を予め行う事を推奨しております。

プライバシー設定については「**11.1 デバイスワイプの設定**」をご参照ください。

6.1. 既定のデバイス所有形態を設定する

1) [グループと設定] > [すべての設定] > [デバイスとユーザー] > [全般] > [加入] をクリックします。

2) [グループ化]タブをクリックし、[現在の設定]を [オーバーライド]に変更します。

3)　[既定のデバイス所有形態]の欄をクリック(プルダウン)してデバイスの所有形態を選択します。

[企業 – 専用]　：会社支給の個人利用のデバイス
[企業 – 共有]　：会社支給の共用のデバイス
[従業員所有]　　：従業員が所有するデバイス（BYOD）

画面下 [保存] をクリックして設定を保存します。

7 ユーザー登録

デバイスを管理するために、**デバイスの使用者であるユーザー**をデバイスより先に登録する必要があります。

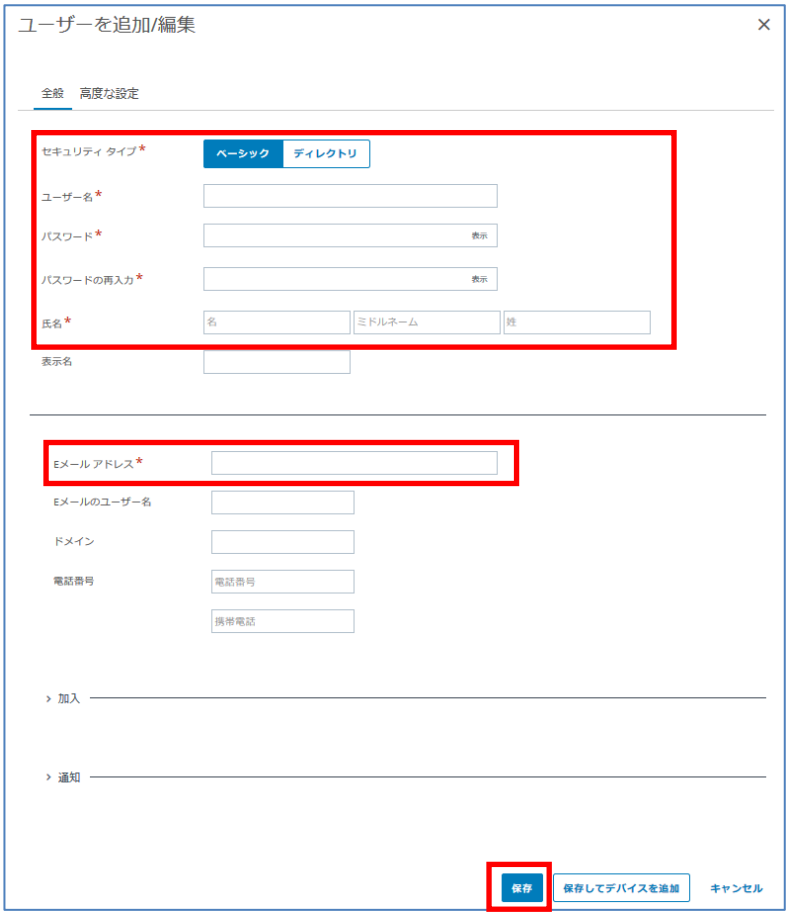
7.1. ユーザーを追加

1) [アカウント] > [リスト表示]をクリックします。

2) マウスポインタを[追加] に移動してサブメニューを表示し、[ユーザーを追加] をクリックします。

ユーザーを追加/編集の画面が表示されます。

3)　必須項目を入力して[保存] をクリックします。
項目名の後に「＊」がついているものは必須項目です。



[加入]、[通知] をクリックすると各設定内容が展開されますので、必要であれば設定を変更します。

4)　リスト表示でユーザが追加されている事を確認します。

8 Workspace ONE SDK プロファイルの設定-iOS

以下の Workspace ONE アプリケーションを iOS デバイスで使用する場合、Workspace ONE SDK プロファイル（アプリケーションプロファイル）の設定が必要になります。

Workspace ONE Intelligent Hub

Workspace ONE UEM のデバイス管理機能、Hub サービス機能、および、デバイス加入アシストに対応するアプリケーション

Workspace ONE Web

Workspace ONE UEM の管理・セキュリティ機能に対応するブラウザ

Workspace ONE Content

Workspace ONE UEM のコンテンツ管理機能に対応するコンテンツ参照アプリケーション

iOS デバイスを使用する場合、以下の画面で設定するセキュリティポリシーは、以下の項の記載の Workspace ONE SDK プロファイルの設定を行う事で、これらアプリケーションに適用されるようになります。

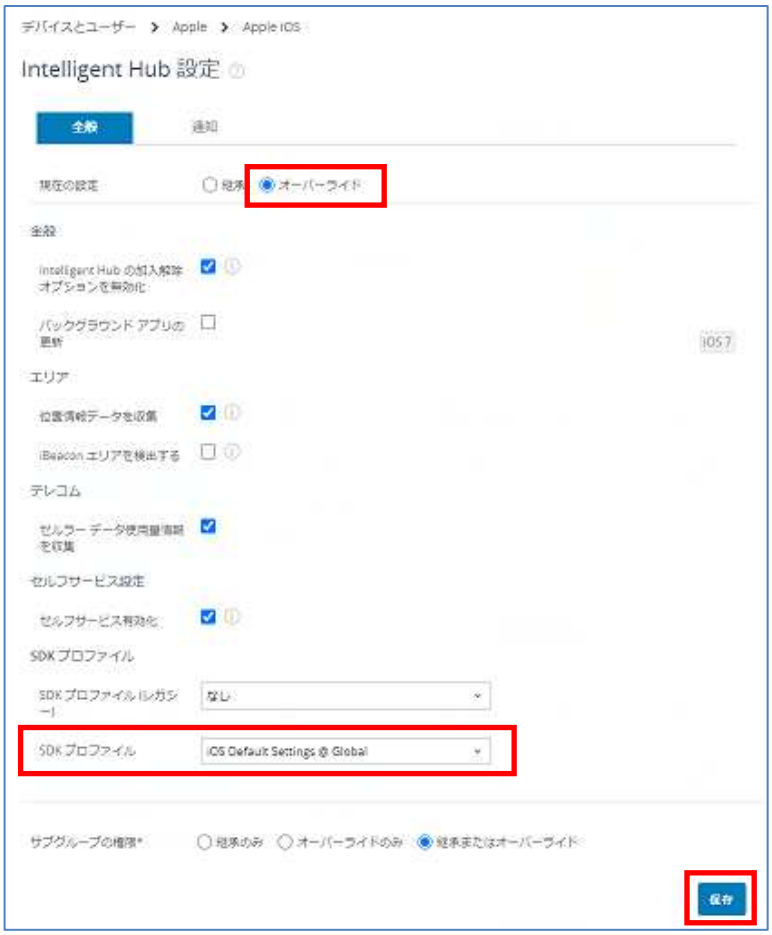
[グループと設定] > [すべての設定] > [アプリ] > [設定とポリシー] > [セキュリティポリシー]

セキュリティポリシーは、上記アプリ利用時に利用者に求める認証の方法や各アプリの機能制約を集めた設定です。

8.1. Workspace ONE Intelligent Hub

1) [デバイス] > [デバイス設定] をクリックし、表示された設定画面右側に表示される [デバイスとユーザー] > [Apple] > [Apple iOS] > [Intelligent Hub 設定] をクリックします。

2) [SDK プロファイル] が iOS Default Settings@Global で設定されている事を確認します。
設定されてない場合、[現在の設定] を[オーバーライド] に変更して、[SDK プロファイル] を iOS Default Settings@Global にし、[保存] をクリックします。



8.2. Workspace ONE Web

1) [グループと設定] > [すべての設定] をクリックし、表示された設定画面右側に表示される [アプリ] > [Workspace ONE Web] をクリックします。

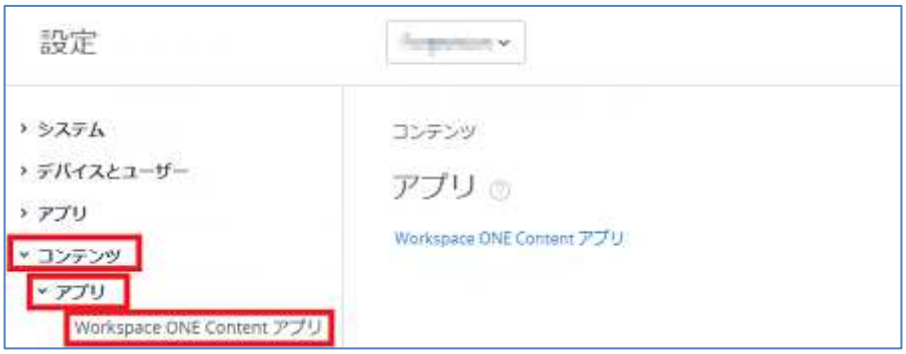
2) [Workspace ONE Web の設定] をクリックし、[アプリのプロファイル] が[既定] である事を確認します。
この設定でない場合、[現在の設定] を[オーバーライド] に変更後、[アプリのプロファイル] を[既定] に変更し、[保存] をクリックします。

3)　[通知] をクリックし、[アプリケーション名] が VMware Browser@Global である事を確認します。

この設定でない場合、[現在の設定] を[オーバーライド] に変更後、[アプリケーション名]を VMware Browser@Global に変更し、[保存] をクリックします。

8.3. Workspace ONE Content

1)　[グループと設定] > [すべての設定] をクリックし、表示された設定画面右側に表示される [コンテンツ] > [アプリケーション] > [Workspace ONE Content アプリ]をクリックします。



2) 以下の設定である事を確認します。

[設定とポリシー] – [アプリのプロファイル]： [既定]

[通知] – [アプリケーション名]： VMware Content Locker@Global

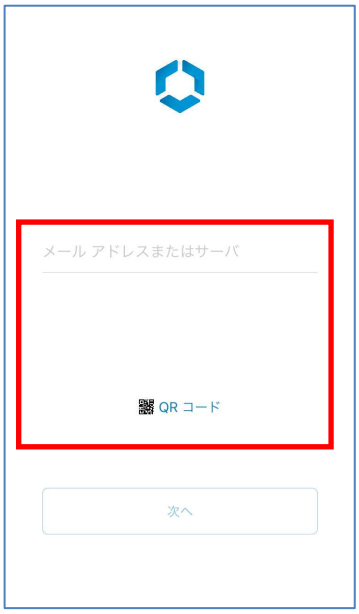
上記設定でない場合、[現在の設定] を[オーバーライド] に変更後、上記設定に変更し、[保存] をクリックします。

9 デバイスで加入処理を実行

デバイスから Workspace ONE UEM への加入処理を行い、このデバイスを Workspace ONE UEM で管理できるようにします。

1) 加入処理は、Workspace ONE Intelligent Hub アプリを利用し、以下からインストールします。
   - iOS: App Store
   - Android: Google play

2) **Workspace ONE Intelligent Hub** を起動します。
   本書では、iOS の加入処理方法を説明させていただきます。
   未加入時は、以下のように「メールアドレス」または「サーバアドレス」を入力する欄と、「QR コード」が表示されます。
   加入時認証方法によって、以下のように入力します。
   Eメールアドレス…[メール アドレスまたはサーバ]欄に入力
   サーバアドレス…[メール アドレスまたはサーバ]欄に入力
   QR コード…「QR コード」をタップし QR コードを読込



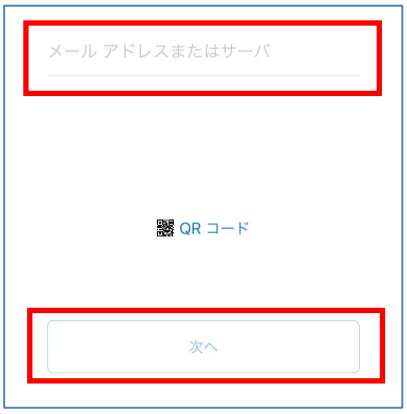
3) 各認証方法による操作は、以下で説明します。
   サーバ詳細
   7.1 サーバ詳細情報の入力から加入を行う
   QR コード
   7.2. QR コード付きのメール送信から加入を行う
   また、上記の操作は iOS デバイスの例で説明します。

E メールアドレスについては、別紙「メールアドレスを利用したデバイス登録方法について」をご参照ください。

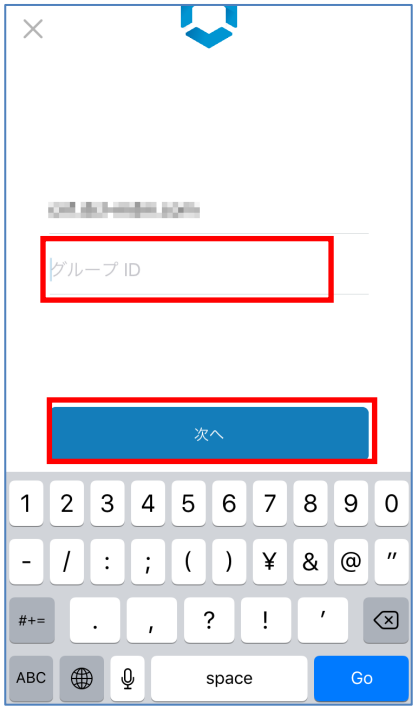
9.1. サーバ詳細情報の入力から加入を行う

認証に必要な情報を全て手入力で行い、加入を行う方法です。

1) [メール アドレスまたはサーバ] に VMware Workspace ONE SaaS 確認書に記載のデバイスサービス URL を入力して、[次へ]をタップします。



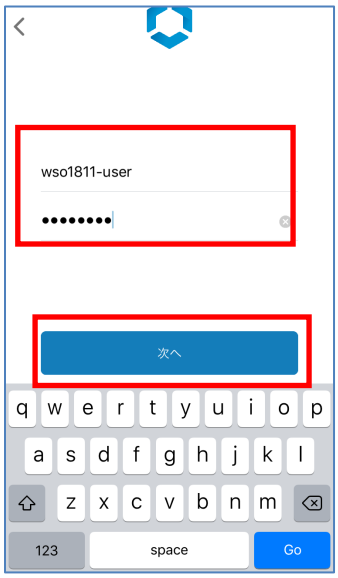
2) [グループ ID] にグループ ID を入力して、[次へ]をタップします。



参考

グループ ID は組織グループを識別する為の ID です。Workspace ONE UEM 管理コンソール画面右上の組織グループ表示にマウスポインタを重ねるとグループ ID を確認する事が出来ます。

3) **6．ユーザー登録**で設定したユーザー名とパスワードを入力して、[次へ] をタップします。



4) 加入後の機能説明が表示されます [次へ] をタップします。タップすると Safari に遷移します。

5) 構成プロファイルダウンロード許可のポップアップに対して[許可] をタップします。構成プロファイルダウンロード後、[閉じる] をタップします。

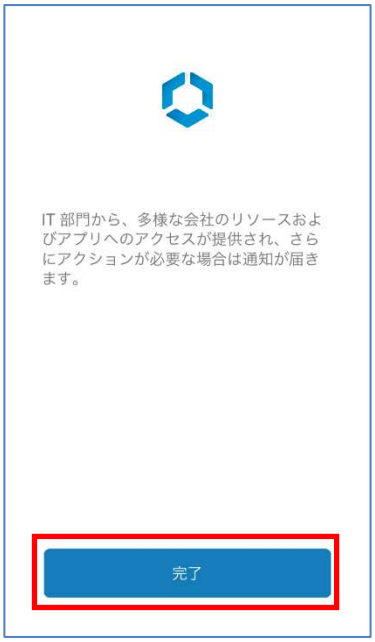
6) 手動で iOS デバイスの[設定]を開きます。[プロファイルがダウンロードされました]をタップすると、ダウンロードした構成プロファイルが表示されます。[インストール] をタップします。

7) デバイスにパスコードが設定されている場合、インストール実行前にパスコード入力を求められます。[インストール] をタップします。

8) モバイルデバイス管理になる警告表示に対し[インストール] をタップし、続けて表示されるポップアップに対し[信頼] をタップします。

9) プロファイルのイントール完了の画面の[完了] をタップし、続けて表示される画面のポップアップに対し、[開く] をタップします。

10) 手動で Workspace ONE Intelligent Hub アプリを開きます。加入完了の画面が表示されますので、[完了] をタップします。



11）**プライバシー**の同意画面で[理解しました]を選択し、次の**データ共有**の同意画面で [同意します] または[今はしない]を選択します。

データ共有の同意は任意です。どちらを選択しても問題ありません。

【認証設定あり】 Workspace ONE Intelligent Hub アプリの利用に対する認証画面が表示され、認証に必要な情報を正しく入力すると、プライバシーの同意画面が表示されます。

上記左画面は、セキュリティポリシーの設定にある[**認証タイプ**] が[**パスコード**] の場合の例です。[**認証タイプ**] が[**無効**] の場合は、表示されません。

9.2. QR コード付きのメール送信から加入を行う

Workspace ONE Intelligent Hub の加入処理で最初に行うサーバ詳細情報の入力を QR コードで行う方法です。

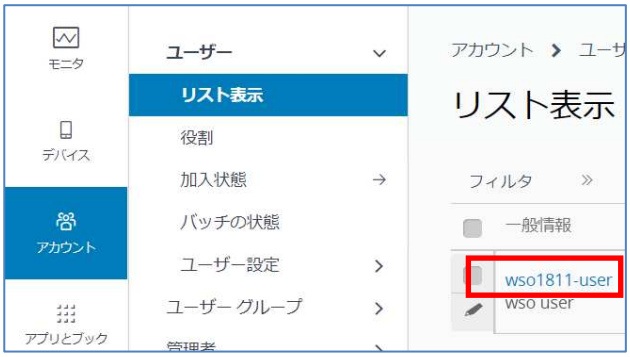
これ以降の手順は **7.1 サーバ詳細情報の入力から加入を行う**と同じです。

QR コードは、管理コントールから送信される以下の「**Workspace ONE UEM デバイスアクティブ化**」のメール本文に貼りつけられています。

9.2.1. デバイスの追加を E メールで通知する

管理コンソールの操作で、デバイス利用者にメール「**Workspace ONE UEM デバイスアクティブ化**」を送信します。

1) [アカウント] > [ユーザー] > [リスト表示] で該当ユーザーをクリックします。



2) 画面右上の[デバイスを追加] をクリックします。

3) [メッセージタイプ] を[E メール] に設定し、デバイス利用者宛の E メールアドレスを[宛先アドレス] に設定し、[保存] をクリックします。

保存が正常に行われると、デバイス利用者にメール「Workspace ONE UEM デバイスアクティブ化」が送られます。

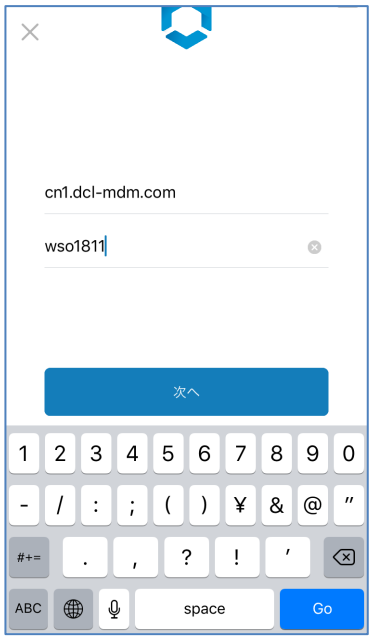
9.2.2. QR コードを読み取り加入をする

メール「**Workspace ONE UEM デバイスアクティブ化**」にある QR コードを準備（PC に画面表示、印刷）し、加入するデバイスで **Workspace ONE Intelligent Hub** アプリを起動し以下を行います。

1) [QR コード] をタップします。

2) デバイスでカメラが起動し、QR コードの読み取りが開始されるので、メール「**Workspace ONE UEM デバイスアクティブ化**」にある QR コードを読み取らせます。

4) QR コードの読み取りに成功すると、ユーザー資格情報の入力を求める画面が表示されます。
これ以降は「**8.1. サーバ詳細情報の入力から加入を行う**」3)～12) と同じ操作で、加入を行います。

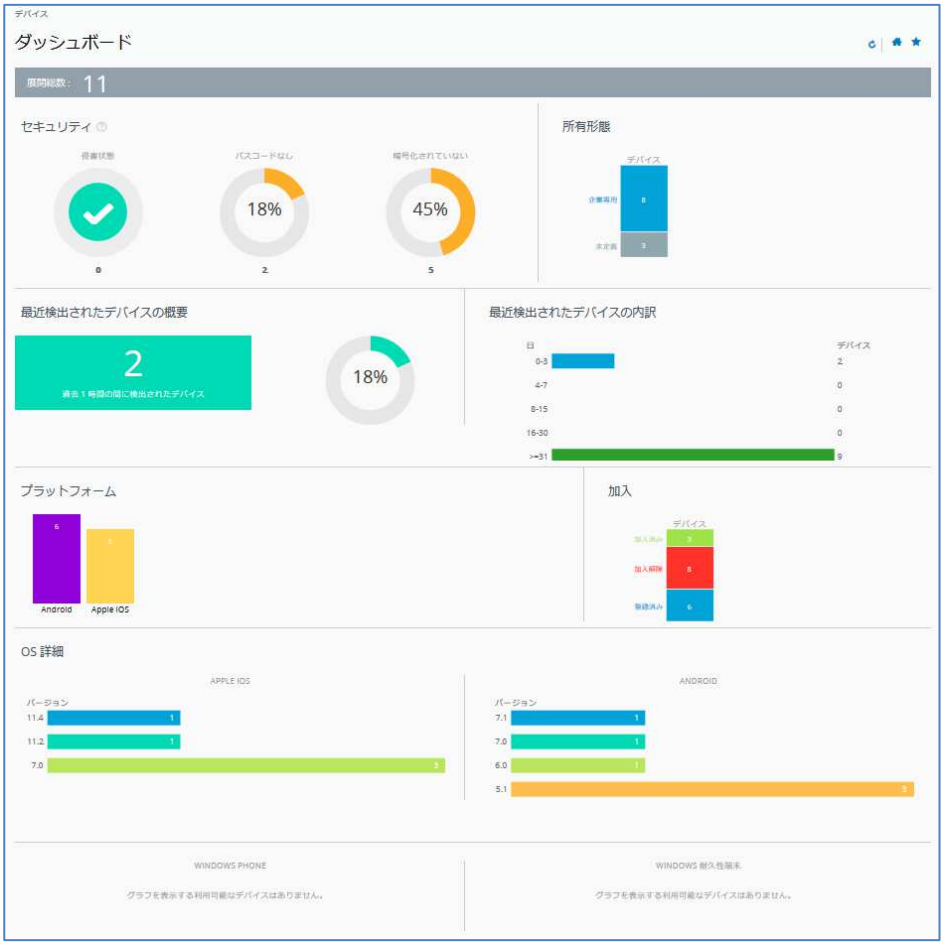


10デバイスの状態確認とリモート操作

デバイスを加入すると、**Workspace ONE UEM 管理コンソール**から加入デバイスに対し、以降の項で記載するデバイスのステータス確認、リモート操作が可能になります。

10.1. ダッシュボード　－　デバイスの加入状況を確認する

[デバイス] > [ダッシュボード] をクリックすると、加入済みデバイスのセキュリティや所有形態、プラットフォーム内訳などの統計が視覚的に確認できます。



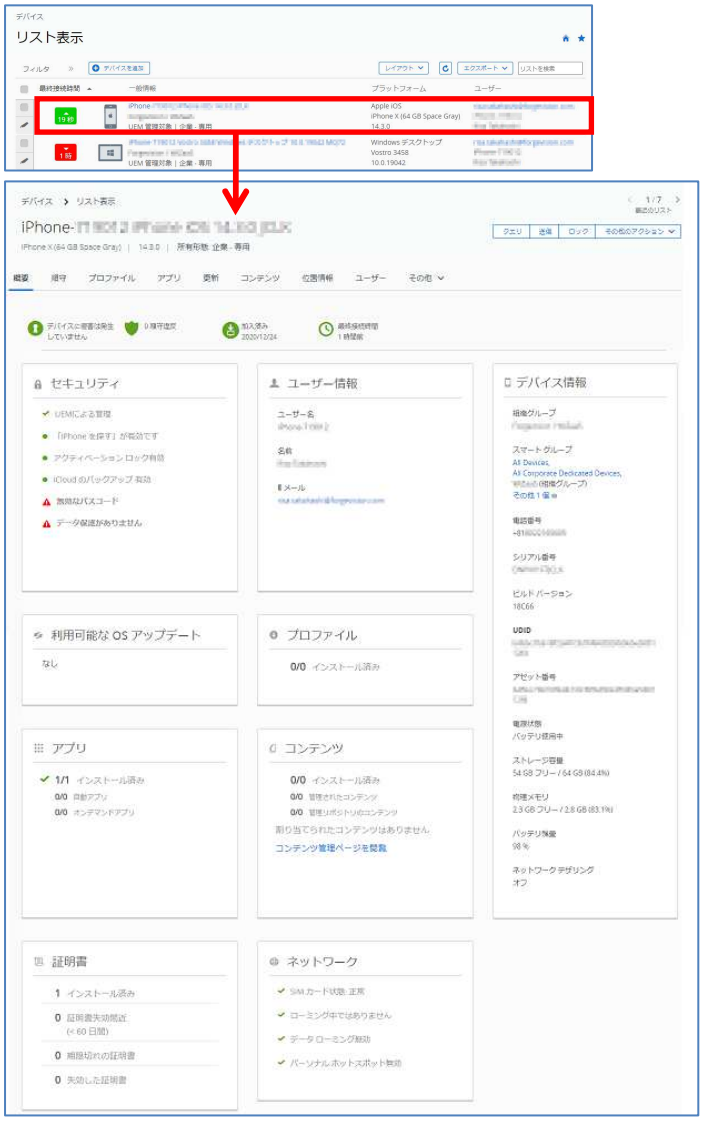
表示対象は、画面で選択されている組織グループ（以下）と配下のサブ組織グループに加入しているデバイスです。

10.2. デバイスリスト　－　デバイスの情報を確認する

1)　[デバイス] > [リスト表示] をクリックすると、各デバイスの概要情報がリスト表示されます。

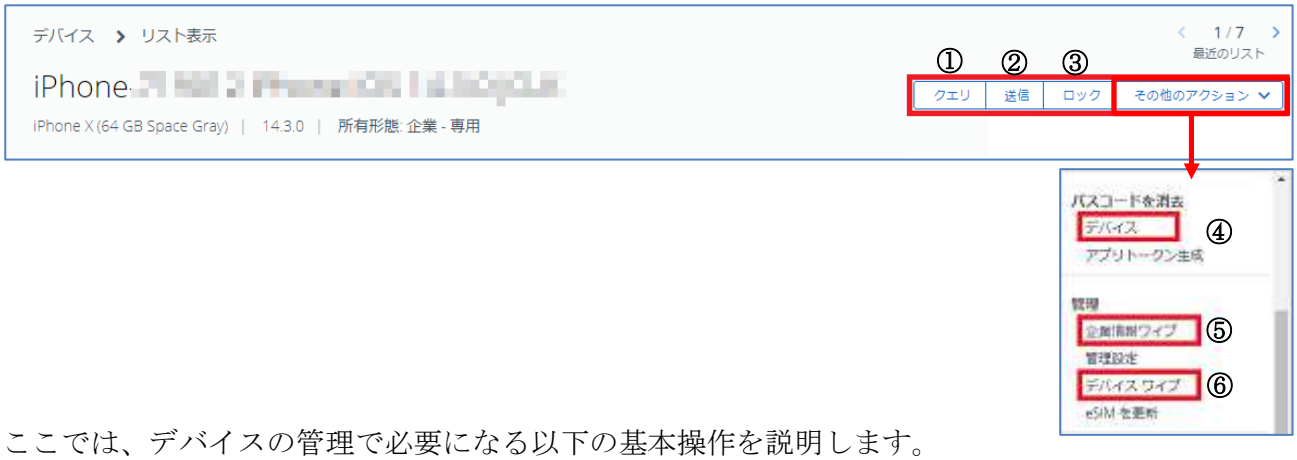
加入解除状態のデバイス（以前加入していたデバイス）も表示されます。

3)　更に、リストされているデバイス（行）をクリックすると、このデバイスの詳細が表示されます。



10.3. デバイスをリモート操作する

デバイスの詳細表示の右上にあるボタン（コマンド）で、デバイスに対してリモート操作をすることができます。



ここでは、デバイスの管理で必要になる以下の基本操作を説明します。

基本操作

操作		説明
①	[クエリ]	このデバイスに対し、Workspace ONE UEM SaaS へデバイス情報を送信するよう要求します。
②	[送信]	このデバイスに対し、メッセージを送信します。 [メッセージタイプ] は[E メール] または[プッシュ通知] を選択できます。（[SMS] は未対応）
③	[ロック]	このデバイスをロックします。 詳しくは「**9.3.1. デバイスをロックする**」をご参照ください。
④	[その他のアクション] > [パスワードを消去 – デバイス]	このデバイスのパスワードを消去します。
⑤	[その他のアクション] > [管理 – 企業情報情報ワイプ]	このデバイスを Workspace ONE UEM へ加入する前の状態へ戻します。 詳しくは「**9.3.2 企業情報情報ワイプ**」をご参照ください。
⑥	[その他のアクション] > [管理 – デバイスワイプ]	このデバイスを工場出荷状態に初期化します。 詳しくは「**9.3.3 デバイスワイプ**」をご参照ください。

参考

[ロック] [パスワードを消去 – デバイス] [管理 – デバイスワイプ] が表示されない場合は、「**10.1 コマンドの設定**」で記載の設定をご確認ください。

10.3.1. デバイスをロック

デバイス紛失の際に、ロックする事ができます。

1) [ロック] をクリックします。

2) iOS の場合は以下の画面が表示され、ロック画面にメッセージと電話番号（拾得時の連絡先）を表示させる事ができます。（[メッセージテンプレート] を[カスタムメッセージ]にした場合）

[送信] をクリックすると、以下の画面でロックされます。

3) Android の場合は、通常のロック画面でロックされます。
1)の[ロック] 後に表示される以下のダイアログに対し、[OK] をクリックすると、デバイスがロックされます。

10.3.2. 企業情報ワイプ

デバイスを加入する前の状態に戻します。これにより Workspace ONE UEM で設定したアプリケーションやプロファイルを含む全ての管理企業リソースが削除されます。

この操作を戻すためには、Workspace ONE(AirWatch)への再加入が必要になります。

1) **[その他のアクション] > [管理 – 企業情報ワイプ]** をクリックします。

2) 理由を選択し、初回ログインで登録したセキュリティ暗証番号を入力します。中止したい場合は、**[キャンセル]** をクリックします。

セキュリティ暗証番号を最大回数以上間違えると、ログアウトします。最大回数については「**10.2 制限事項の設定**」をご参照ください。

10.3.3.　デバイスワイプ

デバイスを初期化して工場出荷状態に戻します。

1)　[その他のアクション] > [管理 – デバイスワイプ] をクリックします。

参考
デバイスワイプのメニューが表示されない場合、プライバシー設定でデバイスへの操作が制限されている可能性があります。「**10.1 デバイスワイプの設定**」にて確認・設定変更の上ご利用ください。

2)　初回ログインで登録したセキュリティ暗証番号を入力するとデバイスワイプが実行されます。中止したい場合は、[キャンセル] をクリックします。

セキリティ暗証番号を最大回数以上間違えると、ログアウトします。最大回数については「**10.2 制限事項の設定**」をご参照ください。

11 システム構成

11.1. デバイスワイプの設定

デバイスの所有形態により、ロックやワイプなどのデバイスに対する操作を制限することができます。デバイスワイプの操作が行えない場合は、デバイスの所有形態と以下の設定をご確認ください。

1) [デバイス] > [デバイス設定] をクリックし、[設定] 画面の[デバイスとユーザー] > [全般] > [プライバシー] をクリックします。

2) [現在の設定] を[オーバーライド] にします。

3) [コマンド - デバイスワイプ]に設定されている、各デバイス所有形態に対する許可を確認します。
[〇許可しない]が設定されていると、デバイスに対する操作でコマンド未表示になります。
設定変更は、マウスポインタを各設定箇所に合せて設定ボタンを表示させます。

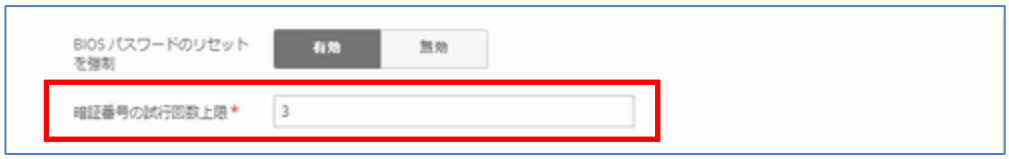
4) 設定変更した場合は、[保存]をクリックします。

11.2. 制限された操作の設定

デバイス削除やアカウント削除などの操作に、パスワードによる保護処理を適用することができます。

1) [デバイス] > [デバイス設定] をクリックし、[設定] 画面の[システム] > [セキュリティ] > [制限された操作] をクリックします。

2) [パスワード保護処理] の各項目に対し、 [有効] にすると、実行時にセキュリティ暗証番号の入力を求められるようになります。



また、セキュリティ暗号番号入力ミスによるログアウトまでの試行回数の設定も行えます。

3) [保存] をクリックします。

12弊社サポート

株式会社ウィザース Workspace ONE サポートデスク

E-Mail　wso-support@wizaas.co.jp

TEL　　03-3633-4833

重要

お問い合せの際、お客様へ発行させていただいた[VMware Workspace ONE SaaS 確認書]に記載のライセンス管理番号を確認させていただいております。

Workspace ONE UEM管理コンソールガイド(入門編)

Workspace ONE UEM 2011 Web UI ベース

ver.15.00　2021年2月19日

ご注意事項

- この文書に記載された製品の仕様ならびに動作に関しては、各社ともにこれらを予告なく改変する場合があります。
- 本文中にあるシステム名、製品名、およびロゴ等は各社の商標または登録商標です。