Workspace ONE UEM 管理コンソールガイド

(Windows 10 初級編)

Workspace ONE UEM 2011 WebUI ベース

2021 年 1 月 4 日

株式会社ウィザース

改訂履歴

ver.	発行日	改訂履歴
1.00	2020 年 6 月 15 日	初版発行
2.00	2021 年 1 月 4 日	第二版発行

目　次

1 本書について

Workspace ONE UEM SaaS を利用して初めて **Windows 10** デバイスを管理される方を対象に、Windows 10 デバイス向けの手順について説明しています。

- Workspace ONE UEM へのログイン
- 組織グループの作成
- システム設定
- ユーザーの登録
- デバイスの加入
- 構成プロファイルの展開
- アプリケーションの展開

上記に無い **SaaS の操作手順**や**他のプラットフォーム**については、次の３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(入門編)

- Workspace ONE UEM へのログイン
- ユーザー登録

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)

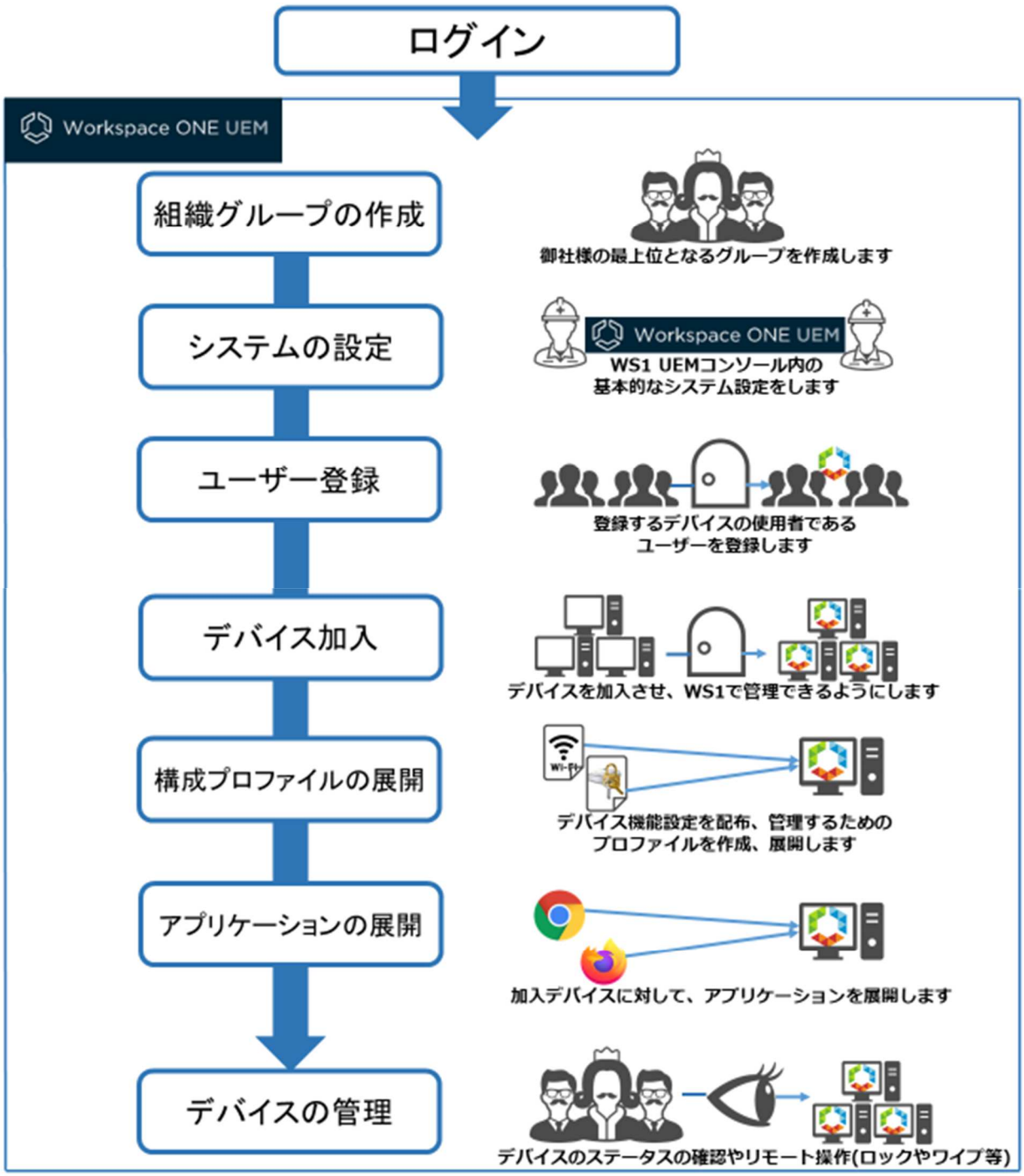
- 機能別ガイドの概略
- システム設定
- アプリケーションの管理
- コンプライアンスの管理
- レポートの管理

また、各パラメーターの詳細などについては、VMware 社のガイドをご参照ください。

https://docs.vmware.com/jp/VMware-Workspace-ONE-UEM/2001/Windows_Desktop_Device_Management/GUID-AWT-INTRO-WINMDM.html

2 本書での操作の流れ

本書は以下の流れで操作を説明しております。



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。

✓ **ウィザース発行ライセンス確認書（ウィザース提供環境のみ）**

・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 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の E メールアドレス宛に件名「**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。

✓ **管理対象デバイス**

・Workspace ONE UEM で管理予定の Windows 10 デバイスです。

・Workspace ONE UEM は、以下の OS を搭載するデバイスをサポートしています。

Windows 10 Pro
Windows 10 Enterprise
Windows 10 Education
Windows 10 Home
Windows 10 S

ご利用されるエディションによっては利用できない機能がございますので、ご注意ください。

Windows 10 エディションの機能比較については、VMware 社のガイドをご参照ください。

https://docs.vmware.com/jp/VMware-Workspace-ONE-UEM/2001/Windows_Desktop_Device_Management/GUID-AWT-MATRIX-WIN10.html

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 管理コンソ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。

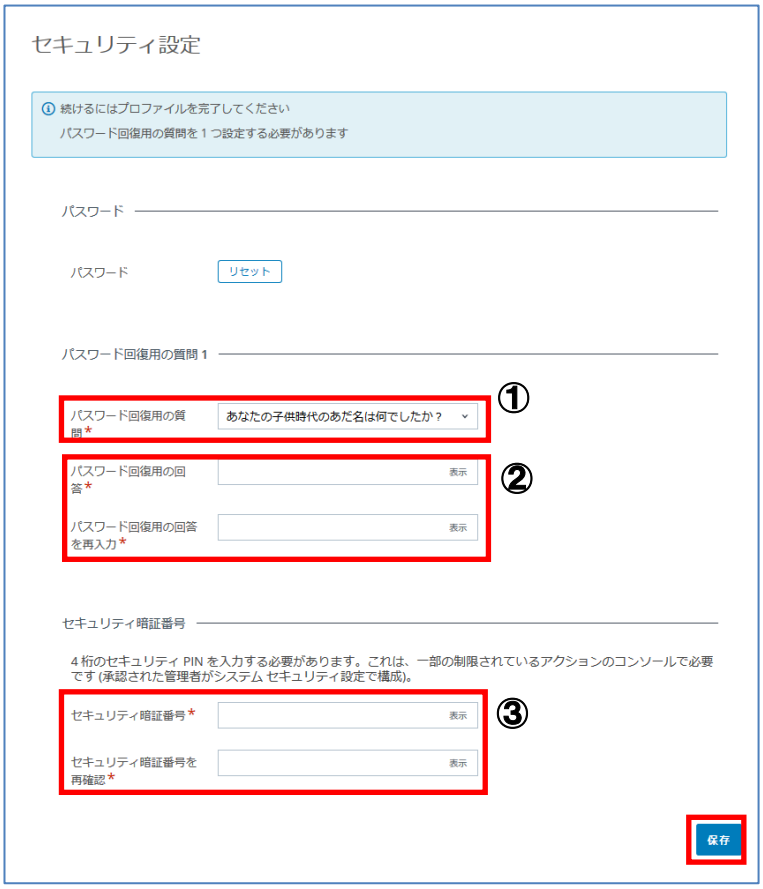
2) Workspace ONE UEM 管理コンソールのパスワード変更の画面が表示されます。新しい**パスワード**を入力し、**送信**をクリックします。

3) Workspace ONE UEM 管理コンソ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、**AirWatch 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) **エンドユーザーライセンス同意書（EULA）**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。

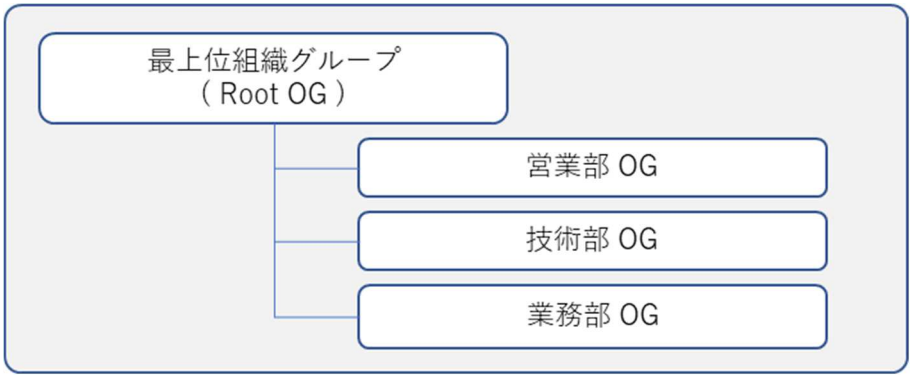
4.2.　2 回目以降のログイン

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。

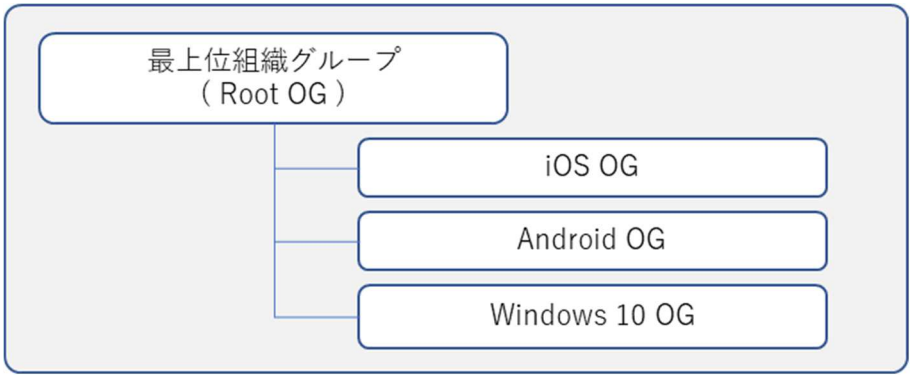
5 組織グループ

組織グループとは、各ユーザーアカウント及び全デバイスを、組織別、機能別、地域別、役割別にまとめて管理するためのグループです。ユーザーアカウント及びデバイスを登録するため、対象となる組織グループの作成が必要となります。ルートの組織グループ（ひとつの組織グループ）だけでも運用は可能ですが、組織グループを分けることにより、デバイスの管理の運用や新規機能の追加設定が行いやすくなります。組織グループを作成する前に、お客様が運用を行う上でデバイスの管理が行いやすいようにグループ構造を決めてください。
下記にグループ構造の一例をご紹介いたします。
※組織グループの略：OG

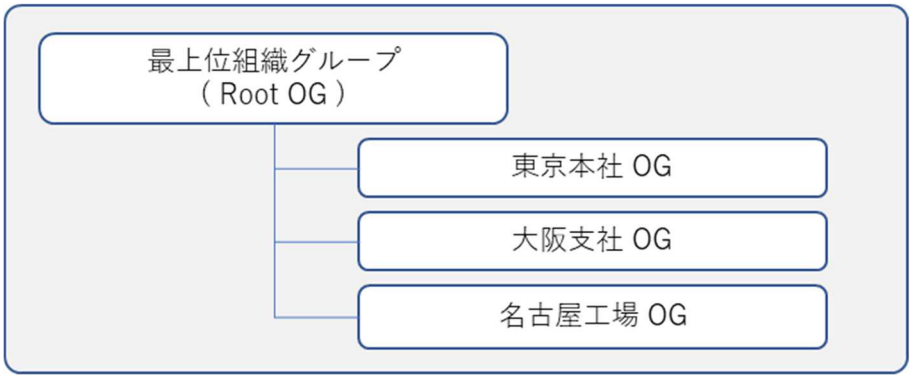
➢ 組織別グループ構造の一例



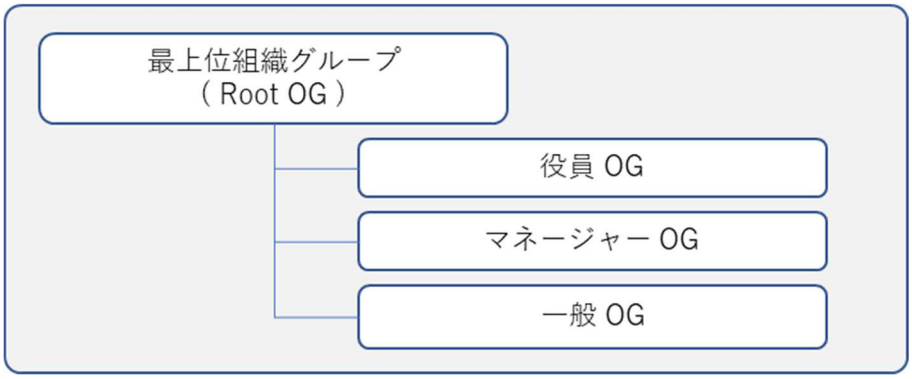
➢ プラットフォーム機能別グループ構造の一例



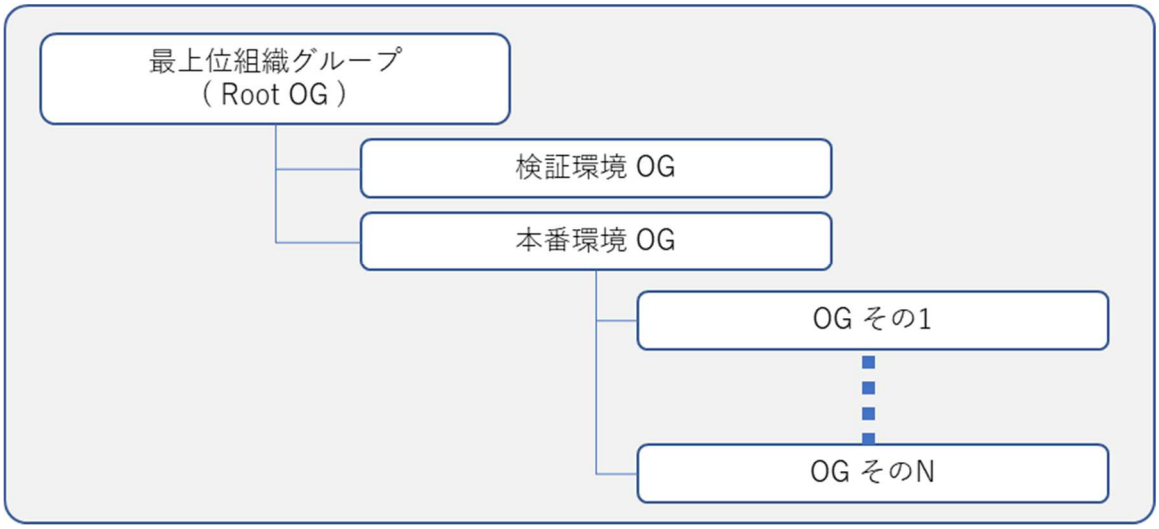
➢ 地域別グループ構造の一例



➢ 役割別グループ構造の一例



➢ 推奨される組織グループの構成



参考
本番環境と検証環境の組織グループを作成することにより、本番環境に影響を与えることなく新規機能の設定追加や問題点の洗い出しが可能となります。

5.1. 組織グループの作成

下記の画像は、まだ組織が下位にない状態です。

デフォルトでは**１つの組織グループ**のみ存在します。これは、**ルートの組織グループ**で、お客様の組織名になっています。
組織グループの追加を行います。

1) [グループと設定] > [グループ] > [組織グループ] > [詳細]をクリックし、
[サブ組織グループの追加]をクリックします。

2) [サブ組織グループの追加] タブの画面で、必要事項を設定します。
項目名の後に「＊」がついているものは必須項目です。

項目（＊必須）	設定する値
名前＊	組織グループ名。コンソール画面に表示されます。
グループ ID	半角英数 20 文字以内で入力します。 デバイスを加入させる場合は必ず設定してください。 デバイス加入時、ユーザーはグループ ID が必要です。 ユーザー未登録時は、設定する必要はありません。
タイプ＊	リストボックスから選択します。
国＊	リストボックスから選択します。
ロケール＊	リストボックスから選択します。
タイムゾーン＊	リストボックスから選択します。

3)　必要な値を設定後、[保存]をクリックします。

同様に他の組織グループも必要に応じて追加してください。

6 基本的なシステム設定

Workspace ONE UEM には、管理コンソールのカスタマイズや、エンタープライズ統合の設定、Workspace ONE アプリの設定など、さまざまなシステム設定があります。このシステム設定はデフォルト値を持っており、お客様が期待する動作の設定ではない場合がございます。この章では、Windows 10 デバイスを管理する上で最低限のシステム設定の方法について説明しています。また、このシステム設定を実施する組織グループは一番上位の組織グループで設定を行い、下位の組織グループは上位の組織グループから設定を「継承」とすることを前提に説明しています。

6.1. 既定のデバイス所有形態を設定する

Workspace ONE UEM へデバイスを加入した際、自動的にデバイス所有形態を設定する設定項目となります。デフォルトはデバイス所有形態が「なし/未設定」となります。

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。

[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。

6.2. プライバシーを設定する

デバイスの所有形態により、デバイスの情報収集、デバイスに対する操作(ロックやワイプなどのコマンド)を制限することができます。

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] > [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)　各情報収集項目および各コマンドのデバイス所有形態に対するプライバシー設定内容の確認を行います。画面内の丸（ ● ｜ ○ ）にマウスカーソルを合わせることにより設定変更が可能です。必要に応じて設定の変更を行ってください。

情報収集項目

コマンド

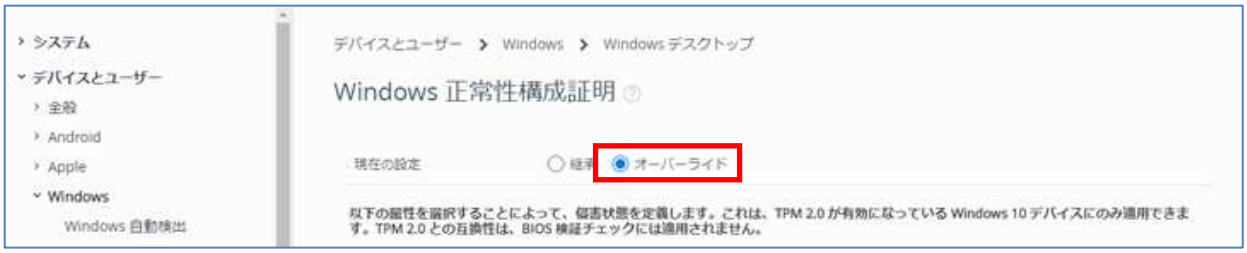
4)　画面一番下にある [保存] をクリックして設定を保存します。

6.3. Windows 正常性構成証明を設定する

管理している Windows 10 デバイスの状態によりデバイスの侵害状態を定義します。この機能は TPM 2.0 が有効になっている Windows 10 デバイスにのみ適用されます。

1) [グループと設定] > [すべての設定] > [デバイスとユーザー] > [Windows] > [Windows デスクトップ] > [Windows 正常性構成証明] をクリックします。

2) [現在の設定]を [オーバーライド]に変更します。



3) 必要に応じて[侵害状態の定義]を変更します。デフォルトでは[セキュア ブート無効化済み]と[BitLocker 無効化済み]にチェックが付いており有効となっています。デフォルトの設定の状態で、BitLocker が無効の Windows 10 デバイスを加入させると**侵害状態**として検知します。

4) 画面一番下にある [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ーが追加されている事を確認します。

8 Windows 10 デバイスの加入

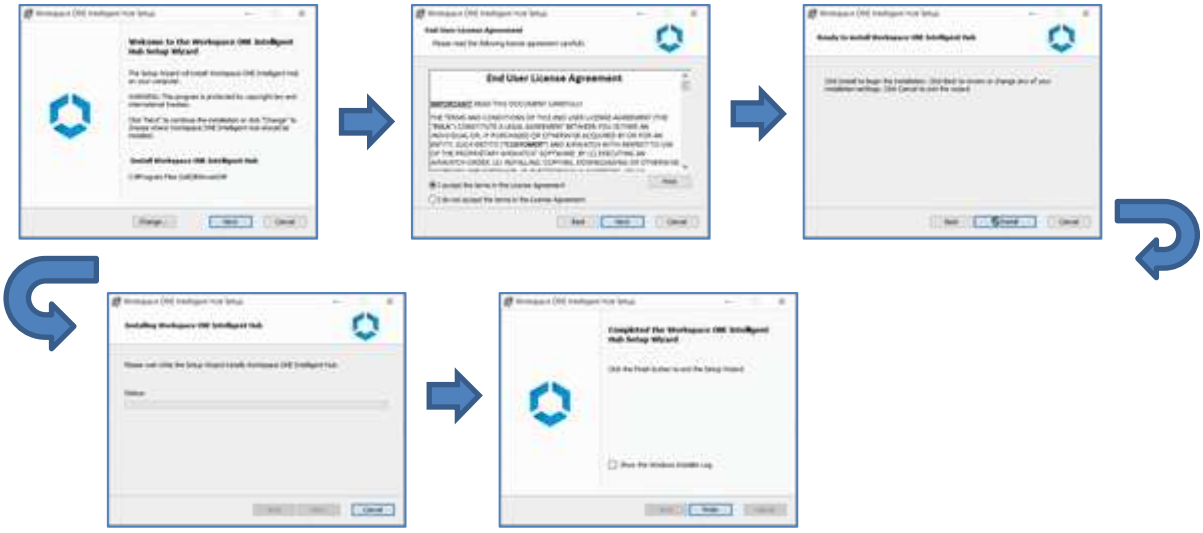
デバイスを Workspace ONE UEM へ加入させることにより、加入したデバイスが Workspace ONE UEM で管理できるようにします。Windows 10 デバイスにおける Workspace ONE UEM への加入方法は何通りか用意されておりますが、この章では、**Workspace ONE Intelligent Hub アプリ**を利用した加入方法を説明しています。

1) 加入処理は、**Workspace ONE Intelligent Hub アプリ**を利用します。以下サイトから **Workspace ONE Intelligent Hub アプリ**のインストーラーをダウンロードします。
https://getwsone.com

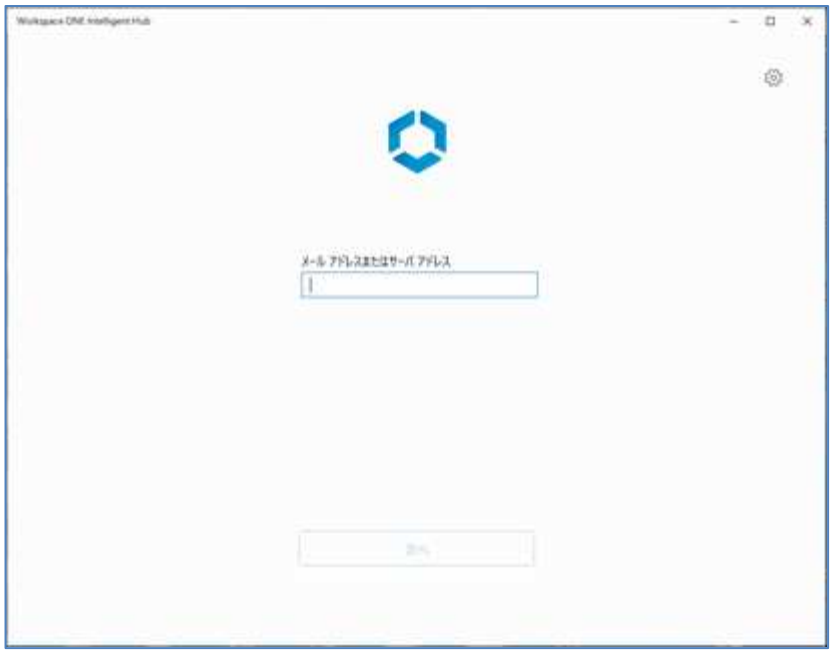
参考

上記 URL からダウンロードしたタイミングで、その時リリースされている最新バージョンの Workspace ONE Intelligent Hub アプリがダウンロードされます。過去利用した Workspace ONE Intelligent Hub アプリは利用せず、都度 Workspace ONE Intelligent Hub アプリのダウンロードを行う事をお勧めします。

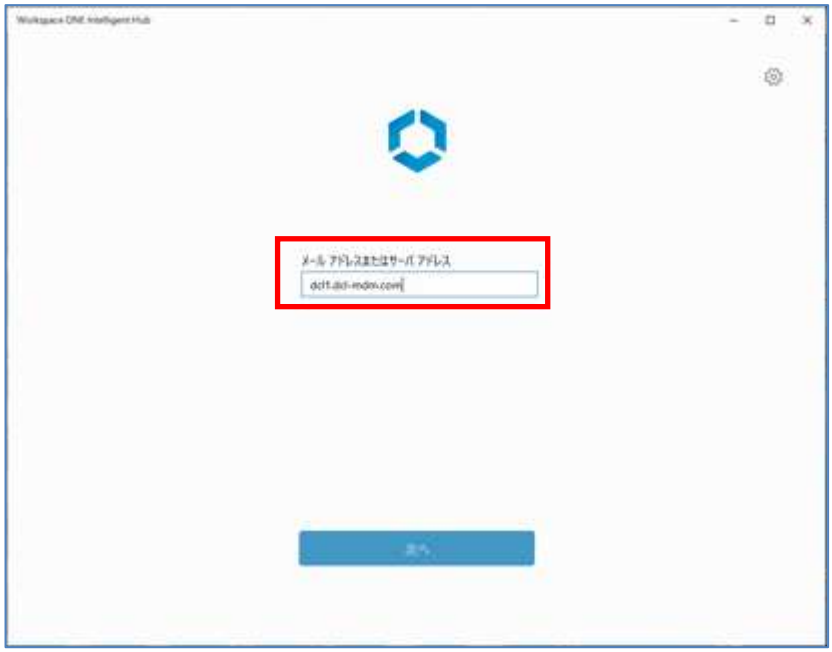
2) ダウンロードしたインストーラーは MSI 形式の一般的な Windows インストーラーです。インストーラーを起動しインストールウィザードに従い **Workspace ONE Intelligent Hub アプリ**のインストールを完了させます。



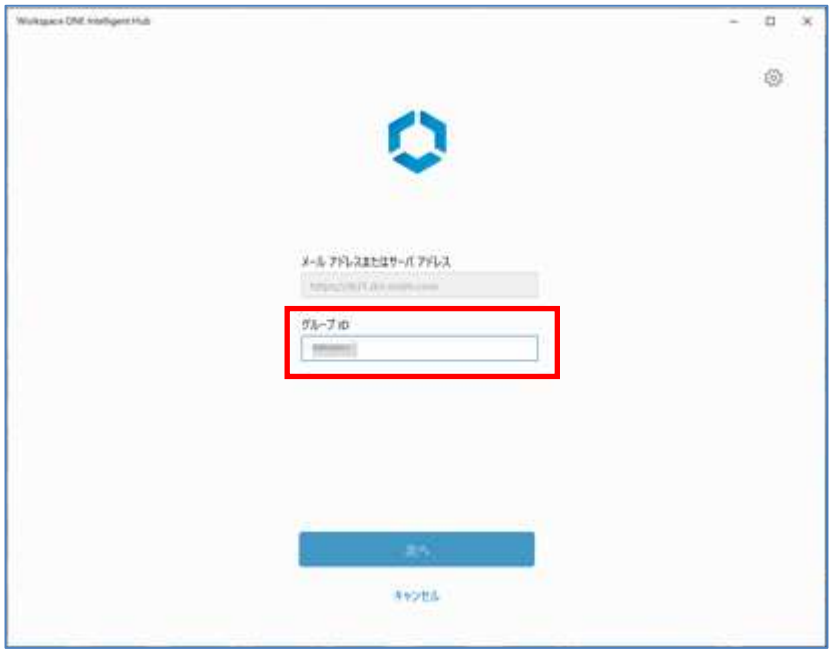
3) インストール終了後、自動的に Workspace ONE Intelligent Hub アプリが起動します。



4) [メール アドレスまたはサーバ] に Workspace ONE UEM 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。



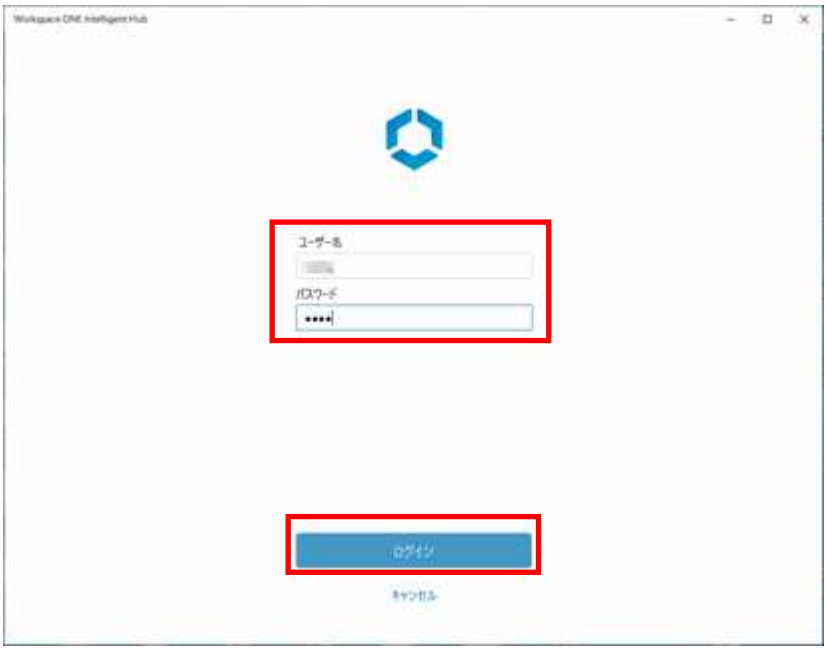
5) [グループ ID] にグループ ID を入力して、[次へ]をタップします。



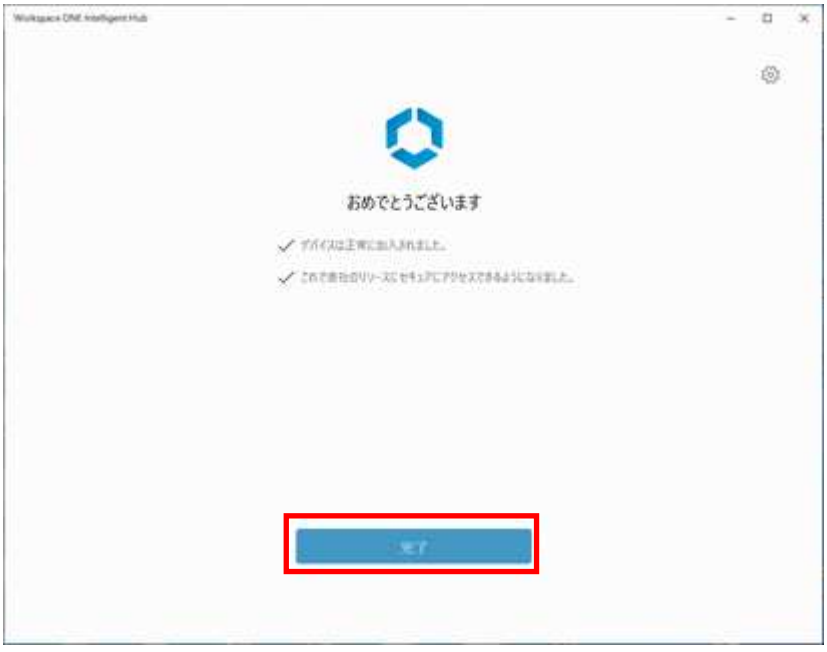
参考

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 を確認する事ができます。

6) **[7. ユーザー登録] の章**で設定したユーザー名とパスワードを入力して、[ログイン] をクリックします。



7) 加入が完了したメッセージが表示されます。[完了] をクリックします。



8)　加入後の基本ステータスが表示されます。[✕] をクリックしてウィンドウを閉じます。

9 構成プロファイルの展開

9.1. Windows 10 構成プロファイル

構成プロファイルとは、管理しているデバイスのパスコードや制限事項などのセキュリティ設定、または、 WiFi、VPN などのデバイス機能設定を配布・管理するためのプロファイルです。Windows 10 デバイス向け構成プロファイルは、ユーザー証明書などのユーザー固有の設定となるユーザーベースプロファイルとデバイス全体に適用されるデバイスベースプロファイルの二種類があります。

9.2. 構成プロファイルの作成と配布

本章では参考として、[制限事項:カメラを許可しない] デバイスベースプロファイルの作成について説明します。

1) [デバイス] > [プロファイルとリソース] > [リスト表示]をクリックします。
2) [追加] をクリック後、表示された[プロファイルを追加]をクリックします。

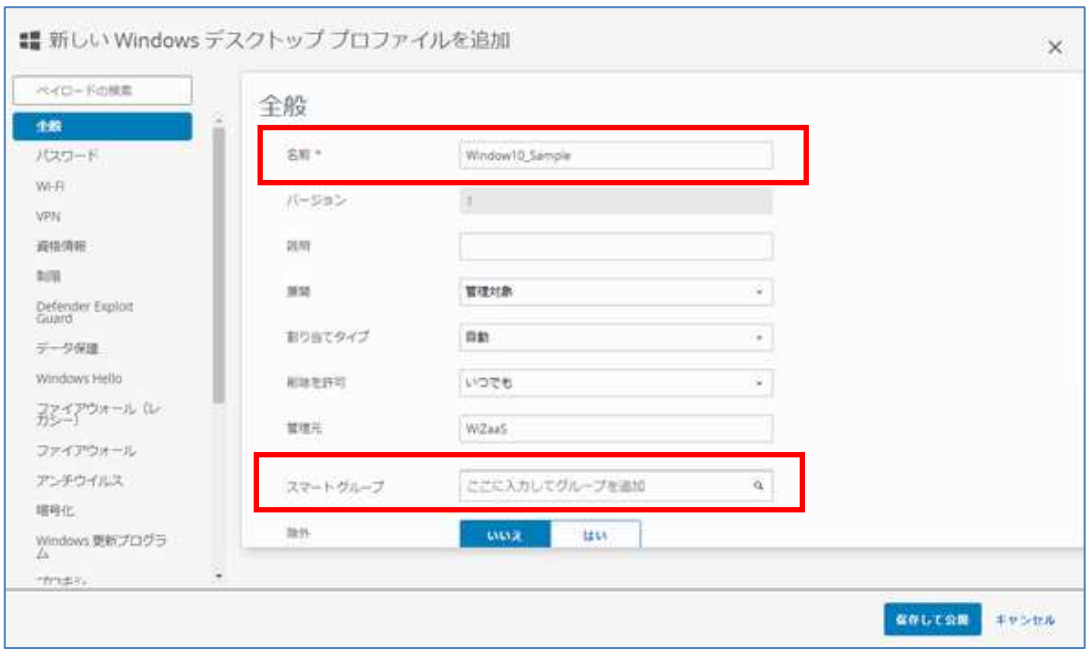
3) プロファイルを追加の画面で、[Windows]をクリックします。

4)　デバイスタイプを選択の画面で、[Windows デスクトップ]をクリックします。

5)　コンテキストを選択の画面で、[デバイス プロファイル]をクリックします。

4)　[全般]に対し必要な項目を入力します。

[名前＊]と[スマートグループ]を設定します。

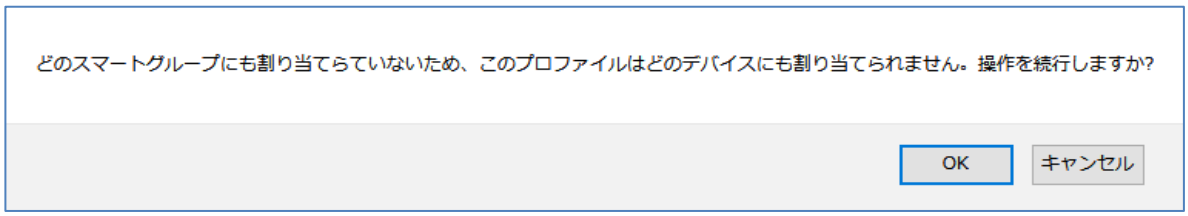


項目（＊必須）	設定する値
名前＊	任意のプロファイル名称
バージョン	システムが自動的に割り当て
説明	備考
展開	管理対象／手動
割り当てタイプ	自動／オプショナル／順守
削除を許可	いつでも/要承認/なし
管理元	クリックによりリストされる組織グループから選択
割り当てるグループ	割り当てるデバイスを組織グループまたはスマートグループ※1で指定
除外	割り当てるグループから除外したいデバイスがある場合“はい”を選択し、除外するグループに除外する組織グループまたはスマートグループを指定
スケジュールを有効にし、選択した時間帯のみインストール	特定の時間帯に割り当てる場合、チェックを入れて割り当てるスケジュールにスケジュール※2を指定
削除日	デバイスから削除する日付です

※1　スマートグループについては、別紙「AW 設定事例_026_「スマートグループ」の作成方法について」をご参照ください。

※2　[デバイス] > [プロファイルとリソース] > [プロファイル設定] > [タイムスケジュール]で、スケジュールを作成します。

重要
全般の割り当てるグループに対し指定がない場合、下記のメッセージが表示されます。
[OK]をクリックすると構成プロファイルはデバイスに配布されず、インストール状態が”割り当てなし”で作成されますので、ご注意ください。



5) [制限]の項目をクリック、[構成]をクリックします。

6) 制限の設定項目が表示されます。（下へスクロールして）カメラ [許可しない] をクリックします。[保存して公開] をクリックします。

7) [公開] をクリックします。
表示されているデバイスに構成プロファイルが配布されます。

8) プロファイルの状況を確認します。
リアルタイムで状況を確認したい場合は、 (更新) をクリックします。
デバイスへの配布が終了しますと、「インストール状態」の上段の数字（緑）に割り当てられている台数が表示されます。

9) Windows 10 デバイスの[設定]から構成プロファイルが反映されたことを確認します。
下図はカメラが許可されていない(カメラが使用できない)制限が反映された状態です。
[変更]ボタンは操作不可となっています。

9.3. 構成プロファイルの管理

プロファイルのリスト表示から構成プロファイルの管理が行えます。

項目		概要
①	選択ボタン	選択ボタンをクリックするとメニューが各種表示されます。 選択したプロファイルの操作が行えます。
②	編集ボタン	構成プロファイルの編集が行えます。
③	デバイス	選択したプロファイルに割り当てられたデバイスが表示されます。
④	</>XML	プロファイルを XML 形式で表示します。表示後、エクスポートなどが行えます。
⑤	その他のアクション	[コピー] 選択したプロファイルをコピーします。 [アクティブ化]/[非アクティブ化] 選択したプロファイルをアクティブ化/非アクティブ化に切り替えをおこないます。 [削除] 選択したプロファイルを削除します。選択したプロファイルをインストールしているデバイスが 1 台以上あると、プロファイルは削除されません。デバイスにインストールされているプロファイルが削除され、選択したプロファイルは非アクティブ化になります。
⑥	インストール状態	上段：インストール済み台数 中断：未インストールデバイス台数 下段：割り当てデバイス台数

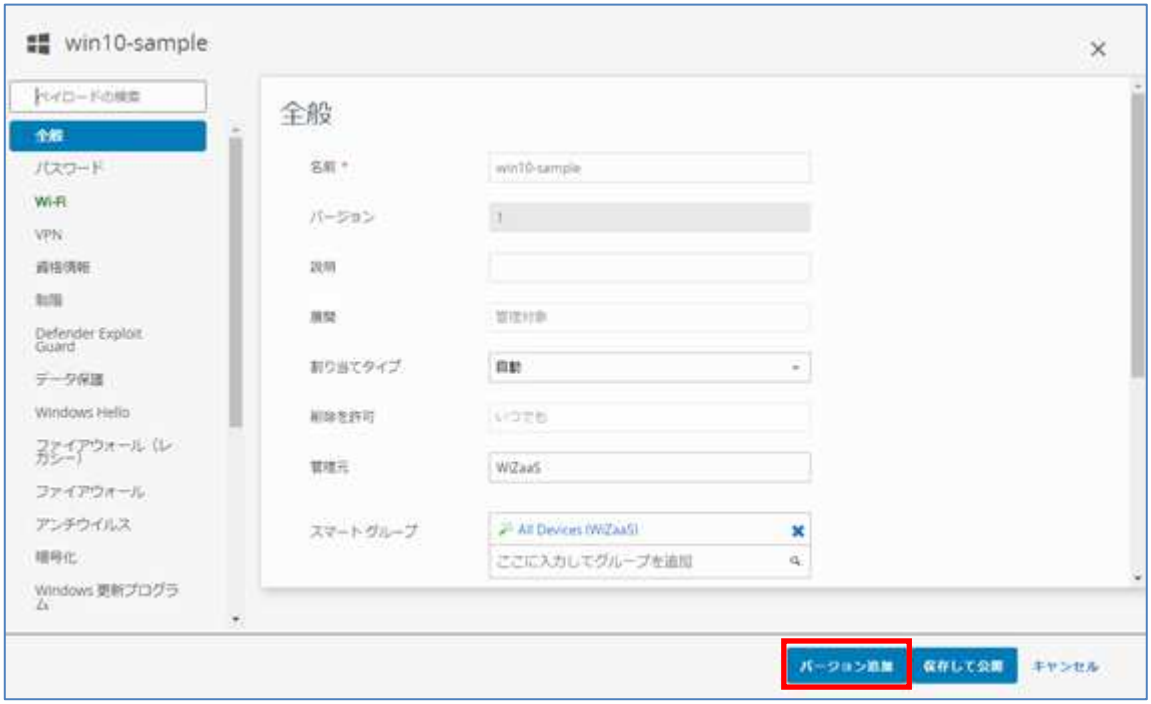
9.4. 構成プロファイルの変更

プロファイルの全般を設定後、任意の項目を設定します。

1) [デバイス] > [プロファイルとリソース] > [プロファイル]をクリックします。

2) 変更したいプロファイルの（編集）をクリックしプロファイル画面を開きます。

3) [バージョン追加] をクリックする。



重要

[全般]以外の編集は、[バージョンを追加]をクリックする必要があります。

4) 変更したい項目をクリックして選択し、設定内容を変更します。

5) 編集を行ったら、[保存して公開]をクリックし、デバイス割り当て表示の画面で割り当てデバイスを確認して[公開] をクリックします。
構成プロファイルは保存され、デバイスに配布されます。

参考
複数の機能をひとつの構成プロファイルにまとめて構成してデバイスへ公開することは可能ですが、**ひとつの機能**を**ひとつの構成プロファイル**で構成することをお勧めしています。

6) Windows 10 デバイスの[設定]から変更された構成プロファイルが反映されたことを確認します。

10アプリケーションの展開

10.1. Windows 10 向けアプリケーションの展開

Workspace ONE UEM では Windows 10 デバイスに対して、いくつかのアプリケーション展開方法を機能として有してきます。アプリケーションの展開にサポートされているインストーラーファイル形式は、MSI 形式、EXE 形式、および、ZIP 形式となっております。この章では、代表的な Win 32 アプリケーションの Google Chrome (MSI 形式) を例としてアプリケーションの展開方法について説明します。

10.2. アプリケーション展開に必要な情報

Workspace ONE UEM は、Win 32 アプリケーションを社内アプリとしてデバイスに展開します。展開および展開後の管理にあたり必要な情報を下記にまとめます。

- Windows 標準 MSI 形式のインストーラーで開発されていること
- デバイスに対してサイレントインストールが行えるインストーラーであること
- インストール後、インストール状況が確認できる情報を取得していること
  ※インストール後の終了コードやインストールパスなどの情報です。
- アンインストールコマンドの情報を取得していること

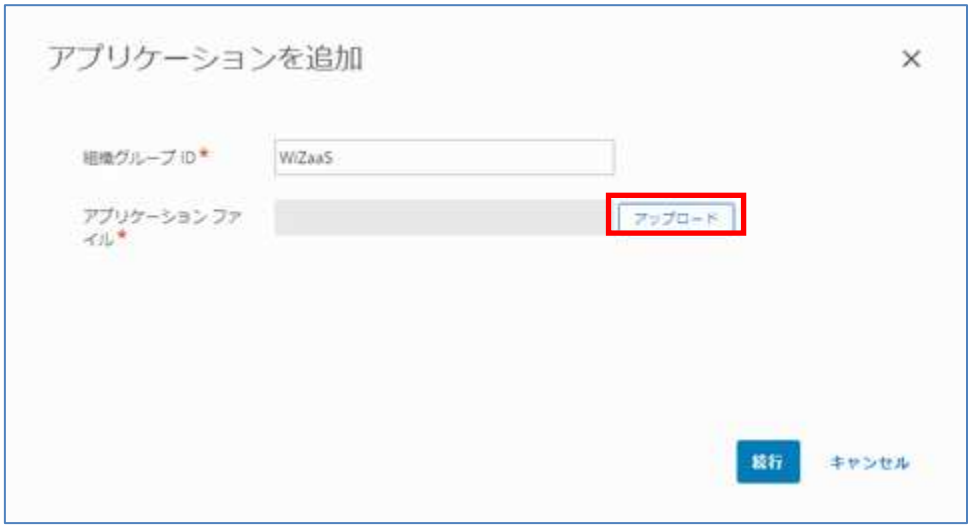
10.3. Win 32 アプリケーションの展開

本章では参考として、Google Chrome アプリケーションの展開設定を説明していますので、事前に Google Chrome インストーラーをダウンロードしてください。
https://www.google.com/chrome/

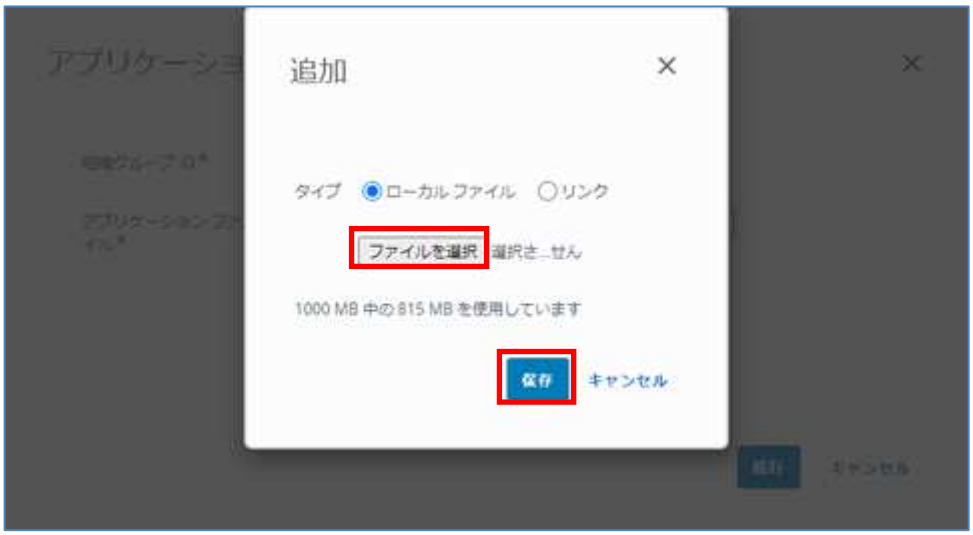
1) [アプリとブック] をクリックし、 [ネイティブ] - [社内]タブ が表示されます。

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、[アプリケーション ファイル] をクリックします。

3) 「アプリケーションを追加」の画面が表示されます。[アップロード] をクリックします。



4) 「追加」の画面が表示されます。[ファイルを選択] をクリックし、アプリケーションのインストーラーを指定して [保存] をクリックします。



参考
インストーラーを保存した際にファイルサイズに関するメッセージが表示されましたら、弊社サポートへお問い合わせください。

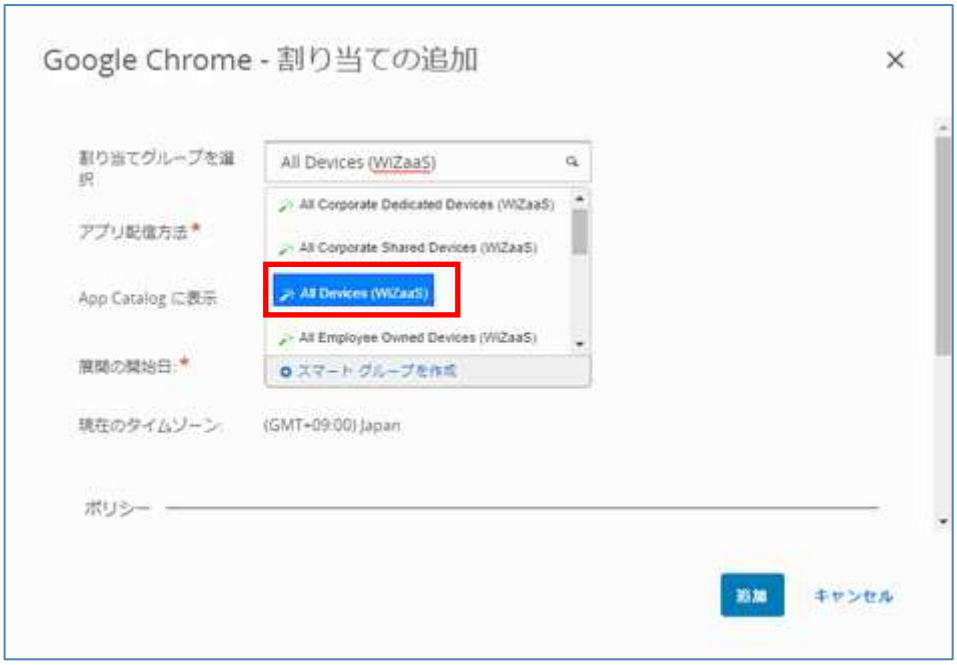
5)　「アプリケーションを追加」の画面に戻ります。[続行] をクリックします。

6)　「アプリケーションの編集」の画面になります。サポートされているプロセッサアーキテクチャの値を[64-bit] に変更し、[保存して割り当て] をクリックします。

7) 「割り当てを更新」の画面になります。デバイスをグルーピングするスマートグループを利用して柔軟なアプリケーションの割り当て設定が行えますが、ここではすべてのデバイスを割り当てます。[割り当ての追加] をクリックします。

8) 「割り当てを追加」の画面になります。始めにアプリ配信方法を選択します。WS1 UEM SaaS からデバイスへ自動的に展開する場合は [自動] を選択します。デバイス側にあるアプリカタログからインストールする場合は [オンデマンド] を選択します。

9) 割り当てグループを選択 欄をクリックして割り当て可能なグループを表示し、[All Device] を選択します。次に割り当ての追加を終了するため、[追加] をクリックします。



10) 割り当てが追加されていることを確認してから、[保存して公開] をクリックします。

10) 「割り当てデバイスプレビュー」の画面になり、割り当てられるデバイスの一覧が表示されます。[公開] をクリックします。

10.4.　アプリケーションの管理

アプリケーションのリスト表示からアプリケーションの管理が行えます。

項目		概要
①	選択ボタン	選択ボタンをクリックするとメニューが各種表示されます。 選択したアプリケーションの操作が行えます。
②	編集ボタン	アプリケーションの編集が行えます。
③	割り当てボタン	アプリケーションの割り当ての編集が行えます。
④	削除ボタン	アプリケーションの削除が行えます。
⑤	{アプリ名称}	アプリケーションの名前をクリックすることにより、より詳細な情報が表示されます。
⑥	インストール状態	表示ボタンをクリックするとインストール状態の台数が表示されます。各インストール状態をクリックするとインストール状態のフィルタされた状態のデバイスのリストが表示されます。 上段：未インストールデバイスの台数 中断：インストール済みデバイスの台数 下段：割り当てデバイスの台数

※インストール状態［割り当て］をクリックしてデバイスのリストを表示した一例です。

10.5.　EXE 形式の配布設定

EXE 形式インストーラーは MSI 形式インストーラーと異なり、インストールコマンド、アンインストールコマンド、および、インストール完了時の確認方法の情報が必要となります。
この章では FireFox アプリケーションを例として説明します。

インストールコマンド:　　Firefox Installer.exe -ms
アンインストールコマンド:　　%ProgramFiles%¥Mozilla Firefox¥uninstall¥helper.exe /S
インストール完了時:　　ファイルが存在する [C:¥Program Files¥Mozilla Firefox¥firefox.exe]

参考
EXE 形式インストーラーの実装によっては Workspace ONE UEM から展開しても、アプリケーションが期待通りにインストールされない場合がありますので、ご注意ください。

1)　[10.3 Win 32 アプリケーションの展開] 1) - 5) の手順で FireFox アプリケーションインストーラーをアップロードします。

2)　「アプリケーションの編集」の「詳細」タブ画面が表示されます。サポートされているプロセッサアーキテクチャの値を[64-bit] に変更します。次に [ファイル] タブ をクリックします。

3) 「ファイル」タブ画面が表示されます。アンインストールコマンド欄に %ProgramFiles%¥Mozilla Firefox¥uninstall¥helper.exe /S を入力します。次に [展開オプション] タブ をクリックします。

4) 「展開オプション」タブ画面が表示されます。インストール欄に Firefox Installer.exe -ms を入力します。

5) アプリケーションの特定方法 [+追加] をクリックします。

6) 「条件」画面が表示されます。条件タイプに [ファイルが存在しています] を選択、パスに C:¥Program Files¥Mozilla Firefox¥firefox.exe 入力します。次に [追加] をクリックします。

7)　「展開オプション」タブ画面に戻ります。[10.3 Win 32 アプリケーションの展開] 7) - 10) の手順でデバイスへの展開設定を行います。

10.6.　設定事例サイト

Windows 10 デバイスにおける Win 32 アプリケーション展開の設定事例が下記サイトに記載されておりますので、ご参照ください。

https://techzone.vmware.com/deploying-win32-applications-vmware-workspace-one-operational-tutorial#283481

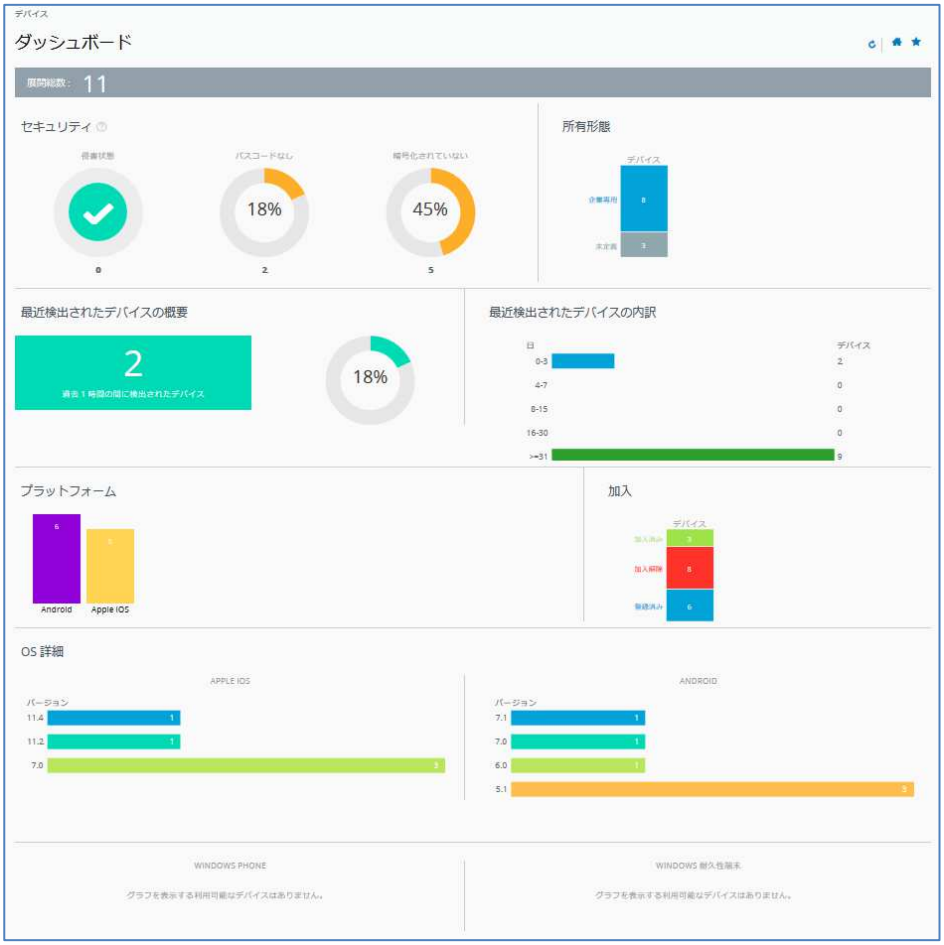
Deploying Win32 Applications: VMware Workspace ONE Operational Tutorial

11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、以降の項番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。

11.1. 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。



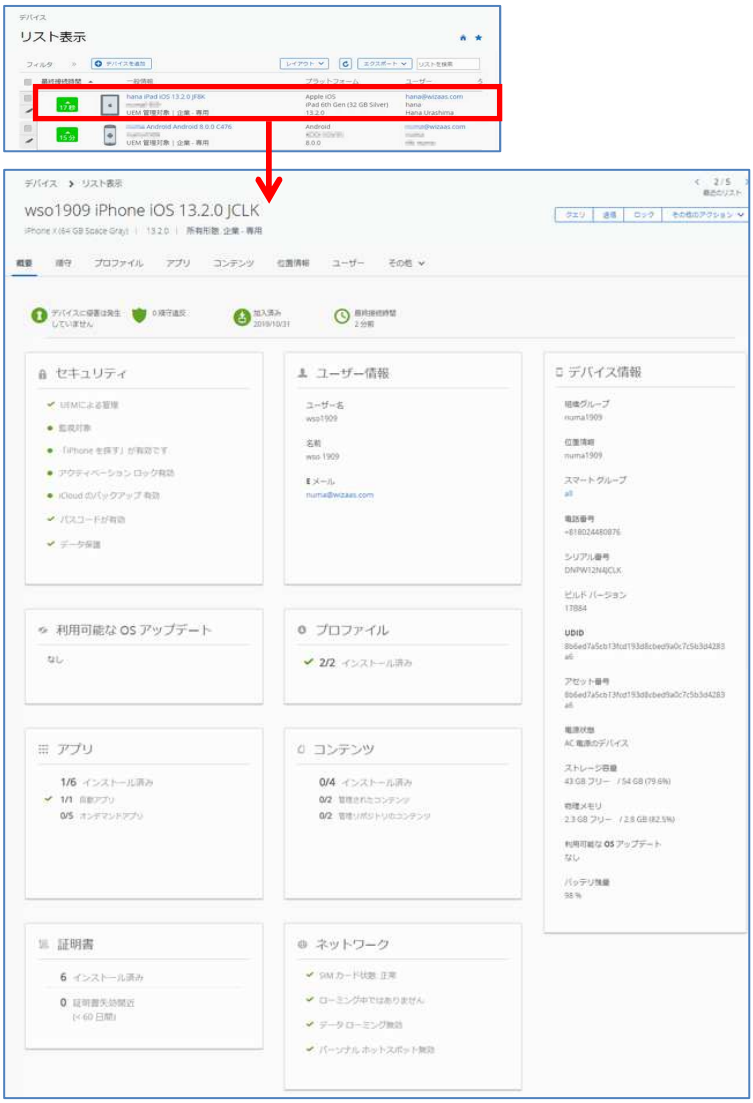
表示対象は、画面で選択されている組織グループ（以下）と配下のサブ組織グループに加入しているデバイスです。

11.2. 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。

2)　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。



11.3. 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「**11.3.1. 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「**11.3.2 企業情報ワイプ**」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「**11.3.3 デバイスワイプ**」をご参照ください。

参考

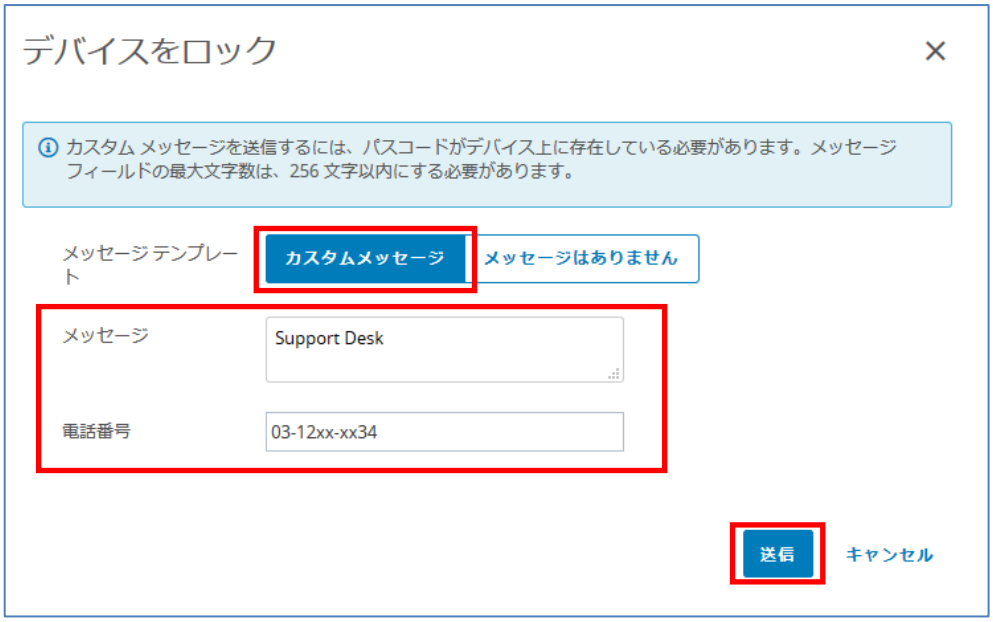
[ロック] [パスワードを消去 – デバイス] [管理 – デバイスワイプ] が表示されない場合は、「**10.1 コマンドの設定**」で記載の設定をご確認ください。

11.3.1. 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。

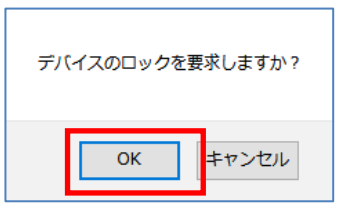
1) [ロック] をクリックします。

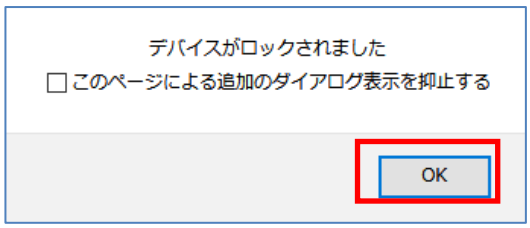
2) iOS の場合は以下の画面が表示され、ロック画面にメッセージと電話番号（拾得時の連絡先）を表示させる事ができます。（[メッセージテンプレート] を[カスタムメッセージ]にした場合）



[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。





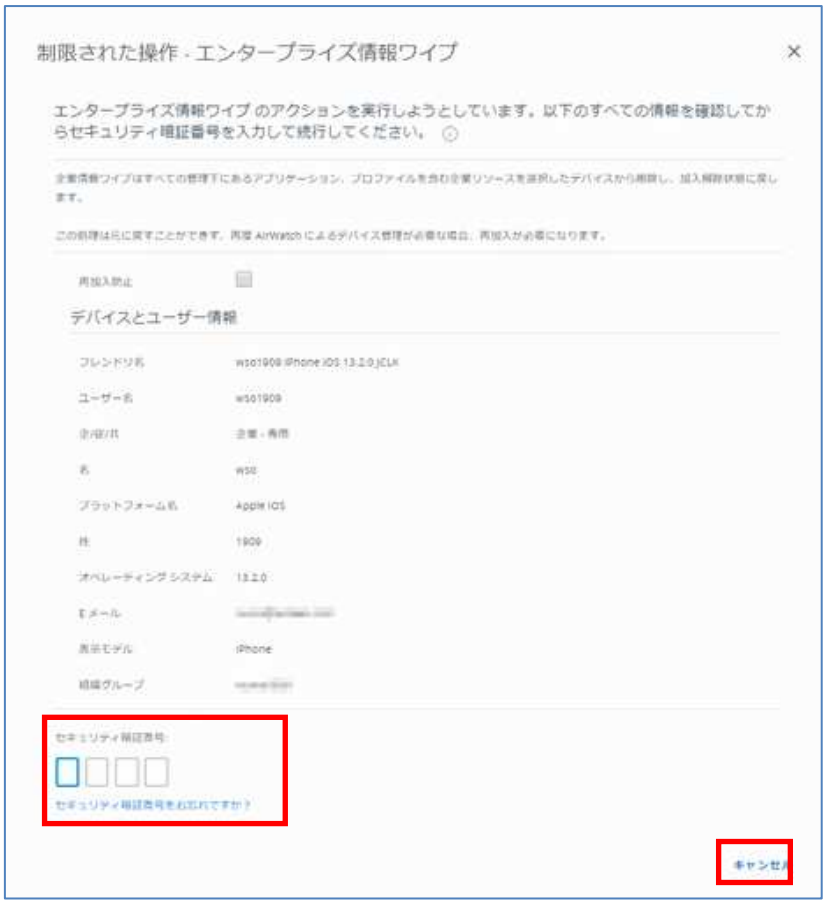
11.3.2. 企業情報ワイプ

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) 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。

11.3.3.　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。

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

平日　　9:00～12:00 13:00～17:00

E-Mail　wso-support@wizaas.co.jp

TEL　　03-3633-4833

Workspace ONE UEM管理コンソールガイド

(Windows 10 初級編)

Workspace ONE UEM 2011 WebUIベース

ver.2.00　2021年1月4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。