

オフィスまるごとサポートデバイスマネジメント クイックスタートマニュアル

最終更新日 2018 年 9 月 14 日


株式会社オプティム

(c)東日本電信電話株式会社

はじめに

本マニュアルの目的

本マニュアルでは、オフィスまるごとサポートデバイスマネジメントの導入の流れについて説明しています。管理サイト側の基本操作や、各設定項目の詳細については、以下を参照してください。







 『管理サイト リファレンス マニュアル』

本マニュアルの見かた

本マニュアルの説明で使用する記号やマークの意味、マニュアルで使用している画面の種類や注意事項は以下のとおりです。


◆記号・マークについて

マニュアルで使用しているマークや記号は以下のとおりです。

記号・マーク	説明
[]	メニュー名、ボタン名、リンク名を表します。
「 」	タブ名や機能名、項目名、マニュアル内の参照先など、強調したい名称を表します。
『 』	参照先のマニュアルを表します。
⇒	操作の結果を表します。
	マニュアルや見出しの参照先を記載します。
	注意すべきことについて説明しています。
	運用や操作のポイントや、知っておくと便利なことについて説明しています。
	画面説明において、該当の画面を表示するためのメニュー操作を記載します。
	 [設定] → [iOS] → [アプリケーション] → [アプリケーション配信] → 

◆画面について

- 本マニュアルで使用している管理サイトの画面は、ユーザー種別が「管理者」用です。ユーザー種別「管理者」以外で管理サイトにログインした場合は、ユーザー種別に応じて編集や閲覧に制限がかかります。

 『管理サイト リファレンス マニュアル』の「ユーザー」－「ユーザーの作成」

- 画面上のバージョン表記は実際のものとは異なる場合があります。
- Windows の OS バージョンや、ご使用になるブラウザによって、一部の画面や操作が異なる場合があります。本マニュアルでは、Google Chrome で表示した画面を使用して説明しています。

Web サイトの URL について

マニュアルの説明で記載している弊社以外の Web サイトの URL は、予告なく変更される場合があります。

商標について

- iPhone、iPad は、Apple Inc.の商標です。
- iPhone 商標は、アイホン株式会社のライセンスに基づき使用されています。
- 記載の会社名および製品名は、各社の登録商標および商標です。

目次

1 オフィスまるごとサポートデバイスマネジメントとは	4
1.1 製品概要	5
1.2 管理サイトの動作環境	5
2 ご利用を開始するまでの流れ	6
2.1 事前準備	7
2.1.1 グループ分けを検討する	7
2.1.2 制限やルールをどのように適用するか検討する	8
2.2 機器管理の基本設定	9
2.2.1 Android 機器用の基本設定	9
2.2.2 iOS 機器用の基本設定	11
2.2.3 Windows 機器用の基本設定	15
2.3 グループ／ユーザー／組織を登録する	18
2.3.1 ユーザーグループを登録する	19
2.3.2 機器グループを登録する	21
2.3.3 組織を登録する	23
2.3.4 ユーザーを登録する	25
2.3.5 複数ユーザーをまとめて登録する	27
2.4 機器にエージェントアプリをインストールする	31
2.4.1 Android 端末の場合	31
2.4.2 iOS 機器の場合	36
2.4.3 Windows 機器の場合	41
2.5 ユーザー／組織／機器グループと各機器を関連付ける	43
2.6 ルールの作成・設定を行う	46
2.6.1 設定セットの作成を行う	47
2.6.2 グループヘルールを適用する	49
2.6.3 組織ヘルールを設定する	52

1 オフィスまるごとサポートデバイスマネジメントとは

オフィスまるごとサポートデバイスマネジメントの製品の概要、動作環境について説明します。

項目	ページ
製品概要	5
管理サイトの動作環境	5

1.1 製品概要

オフィスまるごとサポートデバイスマネジメントは、PC（Windows）・Android・iOS などの一元管理や、セキュリティ対策、アプリケーションの配信をブラウザー上から簡単に実現できる MDM（Mobile Device Management）／EMM（Enterprise Mobility Management）サービスです。

オフィスまるごとサポートデバイスマネジメントの管理下におくための設定ファイルやアプリケーションを管理対象端末にインストール・認証することで、管理サイトから端末の情報を確認したり、セキュリティポリシーを反映させることができます。



1.2 管理サイトの動作環境

オフィスまるごとサポートデバイスマネジメント管理サイトは、以下の環境で利用できます。

項番	項目	動作環境
1	対応ブラウザ	<p>以下のブラウザに対応しています。</p> <ul style="list-style-type: none"> ●Internet Explorer 9、10、11 ●Firefox ●Google Chrome <p>☑Internet Explorer 9 をご利用の場合、ダッシュボードのレイアウトが一部崩れることがございます。機能のご利用に大きな影響はございませんが、Internet Explorer 10 以降のご利用を推奨いたします。</p> <p>☑Firefox、Google Chrome は、最新版にのみ対応しています。</p> <p>☑ディスプレイの解像度は、横 1,250 ピクセル以上の表示を推奨します。</p> <p>☑Apple Push 証明書の登録および更新のとき、Internet Explorer では Apple Push Certificates Portal サイトを表示できないため、Safari、Google Chrome、Firefox などのブラウザで開いてください。</p> <p>☑対応ブラウザのインストール方法や設定など、また OS に依存する設定については対応いたしかねます。</p>
2	ネットワーク接続	<p>インターネットへ接続し、直接またはプロキシを介して管理サイトと HTTPS 通信（443 番ポート）ができる環境が必要です。</p>
3	対応言語	<p>以下の言語に対応しています。</p> <ul style="list-style-type: none"> ●「日本語」、「英語」

☑各エージェント側の動作環境については、以下のマニュアルを参照してください。

- 📖 『Android ユーザーマニュアル』
- 📖 『iOS ユーザーマニュアル』
- 📖 『Windows ユーザーマニュアル』

2 ご利用を開始するまでの流れ

オフィスまるごとサポートデバイスマネジメントを使用して、Android 端末、iPhone／iPad、Windows 機器の管理を開始するまでの初期設定を説明します。


項目	ページ
事前準備	7
機器管理の基本設定	9
グループ／ユーザー／組織を登録する	18
機器にエージェントアプリをインストールする	31
ユーザー／組織／機器グループと各機器を関連付ける	43
ルールを作成・設定を行う	46

2.1 事前準備

オフィスまるごとサポートデバイスマネジメントでは、端末へのセキュリティ設定や、業務端末の不正利用を行うアプリケーション起動禁止の設定を行えますが、これらの機能を使用するためには、各端末ヘルールを設定する必要があります。

ルールとは、端末に行う設定（セキュリティ設定やインストール制限など）を意味します。

ルールは端末ごとでも設定はできますが、ユーザーの部署や役職ごと、または機器の使用用途ごとにグループを作成し、グループごとに設定できます。

 ここでは、事前準備として、グループ分けが必要な場合はどのようなグループを作成するのか、管理対象の端末にどのようなルールを設定するのかなど検討します。


2.1.1 グループ分けを検討する


例として、ユーザーと機器のグループ分けを考えます。

●ユーザーのグループ分け

端末ユーザーの所属部署と役職をリストアップし、検討の結果、以下のようにグループを作成することになります。

- ・「所属（部）」として「営業部」と「企画部」の2グループを作成する。
- ・「役職」として「部長」、「課長」、「役職なし」の3グループを作成する。


 管理サイトでのユーザーのグループ分けは、「ユーザー」の「入力項目のカスタマイズ」メニューから行います。以下を参照してください。


 「ユーザーグループを登録する」19 ページ

社員番号	名前	所属（部）	役職
0001	鈴木〇〇	営業部	部長
0002	田中△△	営業部	課長
0003	山田〇〇	営業部	なし
0004	井上△△	企画部	部長
0005	阿部〇〇	企画部	課長
0006		企画部	なし

●機器のグループ分け

機器の用途を検討し、「機器用途」として「社内使用端末」と「社外持ち出し用端末」の2グループを作成します。

 管理サイトでの機器のグループ分けは、「機器」の「入力項目のカスタマイズ」メニューから行います。以下を参照してください。

 「機器グループを登録する」21 ページ

2.1.2 制限やルールをどのように適用するか検討する

端末に適用したい制限やルールを検討します。

全員に適用する制限は、その機能の「デフォルト」に設定します。

特定のグループのみに適用する制限は、グループを作成し、そのグループにのみルールを適用します。

例では、「グループ分けを検討する」で検討したグループに対して、以下の制限を適用することにします。

制限の種類	ルール	適用する対象
カメラ禁止	カメラ機能を禁止します。	全員
SD カード禁止	SD カードの使用を禁止します。	所属が「営業部」
Web フィルタリング	Web 閲覧に制限をかけます。	全員
アプリケーション禁止	アプリケーションの起動を禁止します。	「役職」が「なし」
発信先制限	発信先に制限をかけます。	所属が「企画部」

2.2 機器管理の基本設定

機器管理の設定を行います。利用する機器の種別ごとに設定を行ってください。

2.2.1 Android 機器用の基本設定

Android 端末と管理サーバー間での通信間隔、端末側でのリモートロックの解除コード、パスワード設定などを、以下の管理サイトの「管理アプリの通信と動作」の画面で設定します。

設定を行わない場合は、デフォルト値が使用されます。基本設定が終わったら、以下の操作に進みます。

🔗「グループ／ユーザー／組織を登録する」18 ページ

📌Android の設定については、以下を参照してください。

🔗『管理サイト リファレンス マニュアル』の「設定－Android」

◆管理アプリの通信と動作の設定

表示操作 [設定] → [Android] → [管理アプリの通信と動作] → [編集]

エージェント共通管理 - 編集

1

管理サーバーとの通信間隔
☒ 分数指定: 30 分
☐ 時間指定: 時間
☐ 日数指定: 日
※機種によって端末のスリープ中は通信が行われないことがあります。
※通信間隔が短い場合、端末のバッテリー消費が早まる可能性があります。

2

管理サーバーと通信できなかった場合
☒ なにもしない
☐ 指定分数後にロック: 分
☐ 指定時間後にロック: 時間
☐ 指定日数後にロック: 日
※通信間隔の設定によってはロックまでに時間がかかることがあります。

3

ロックメッセージ

4

リモートロックの解除コード

5

端末でのエージェント停止・ライセンス解除・アンインストールの制限
☒ 制限なし
☐ パスワードの入力

6

root化状態検知
☐ 検知しない
☒ 検知する

取消

保存

◆ 設定項目

項番	項目	デフォルト値	説明
1	管理サーバーとの通信間隔	30 分	管理サーバーとの通信間隔を設定します。
2	管理サーバーと通信できなかった場合	なにもしない	端末が管理サーバーと一定時間通信できなかった場合に端末をロックできます。
3	ロックメッセージ	なし	端末が管理サーバーと一定時間通信ができずに端末がロックされた場合に、ロック画面に表示されるメッセージの設定を行います。
4	リモートロックの解除コード	解除コードの入力：ランダム値で自動生成されたパスワード	リモートロック解除用コードの設定を行います。
5	端末でのエージェント停止・ライセンス解除・アンインストールの制限	パスワードの入力：ランダム値で自動生成されたパスワード	端末からエージェントを停止したり、ライセンス解除をしたり、アンインストールをする場合のパスワードを設定します。
6	Root 化状態検知	検知する	端末が root 化されている場合、検知するかどうか設定します。

2.2.2 iOS 機器用の基本設定

iPhone/iPad を管理するには、Apple Push 証明書を登録する必要があります。この登録を行わないと、iPhone/iPad を管理できません。機器用の基本設定が終わったら、以下の操作に進みます。

📖 「グループ/ユーザー/組織を登録する」18 ページ

- ❗ Apple Push 証明書登録は導入時に 1 度登録すれば、1 年間有効です。端末ごとに登録する必要はありません。また、Apple Push 証明書の取得には Apple ID が必要です。1 年後の Apple Push 証明書更新時には、最初に Apple Push 証明書を登録したときの Apple ID が必要となります。
- ❗ Apple ID を忘れた場合や失効した場合は、Apple ID および Apple Push 証明書を新規に取得し直す必要があるため、端末の構成プロファイルの継続使用ができなくなり、導入済みのプロファイル、エージェントも再度インストールする必要があります。そのため Apple ID は忘れないよう必ず控えてください。
- ❗ iOS の設定については、以下を参照してください。

📖 『管理サイト リファレンス マニュアル』の「設定-iOS」

◆ Apple Push 証明書の登録

- [1]** [設定] → [サービス環境設定] → [Apple Push 証明書] → [編集] → 「1.署名済みの証明書要求 (CSR) ファイルの生成とダウンロード」の [ダウンロード] をクリックします。

⇒ 証明書登録に必要なとなるファイルのダウンロードが開始されます。

📎 ファイルは任意の場所へ保存します。

- [2]** 「2.証明書ファイルの取得」の URL [<https://identity.apple.com/pushcert/>] をクリックします。

- ❗ Internet Explorer では Apple Push Certificates Portal サイトを表示できないため、Safari、Google Chrome、Firefox などのブラウザで開いてください。
- ❗ 証明書発行のときに使用された Apple ID は、お忘れになりませんようご注意ください。証明書の更新（1 年に 1 回）のときに必要となります。証明書の有効期限が切れた場合、本製品はご利用いただけなくなります。

1. 署名済みの証明書要求(CSR)ファイルの生成とダウンロード

- 1** 済みの証明書要求(CSR)ファイルをダウンロードしてください。

ダウンロード

2. 証明書ファイルの取得

以下のリンクより「Apple Push Certificates Portal」にログインし証明書を取得してください。

- 2** 月書ファイルは、署名済みの証明書要求(CSR)をアップロードすることで取得できます。

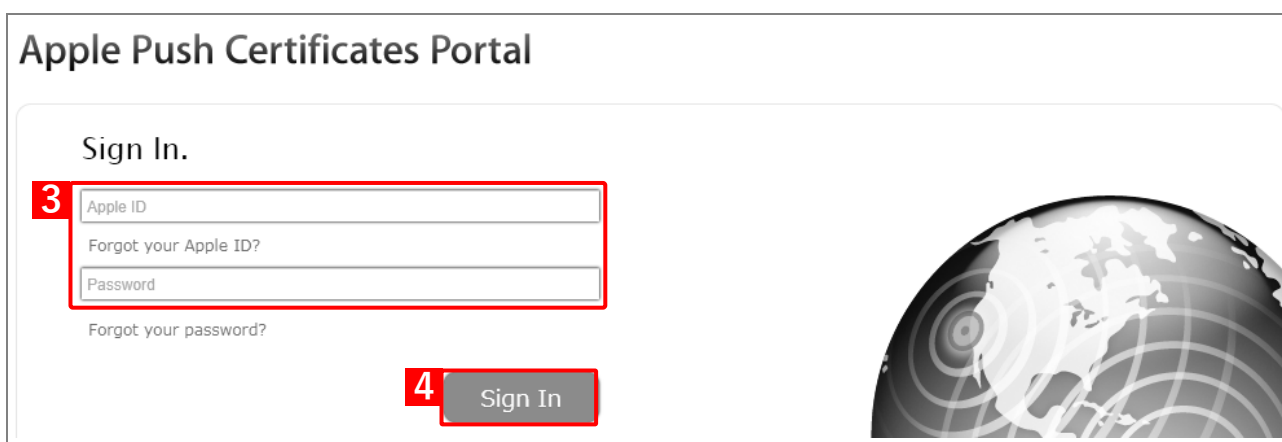
<https://identity.apple.com/pushcert/>

※Internet ExplorerではApple Push Certificates Portalサイトを表示できないため、Safari、Google Chrome、Firefox等のブラウザで開いてください。

※証明書を1年に1回更新する必要があります。証明書の有効期限が切れた場合、本製品はご利用いただけなくなります。

【3】 Apple ID と Apple ID のパスワードを入力します。

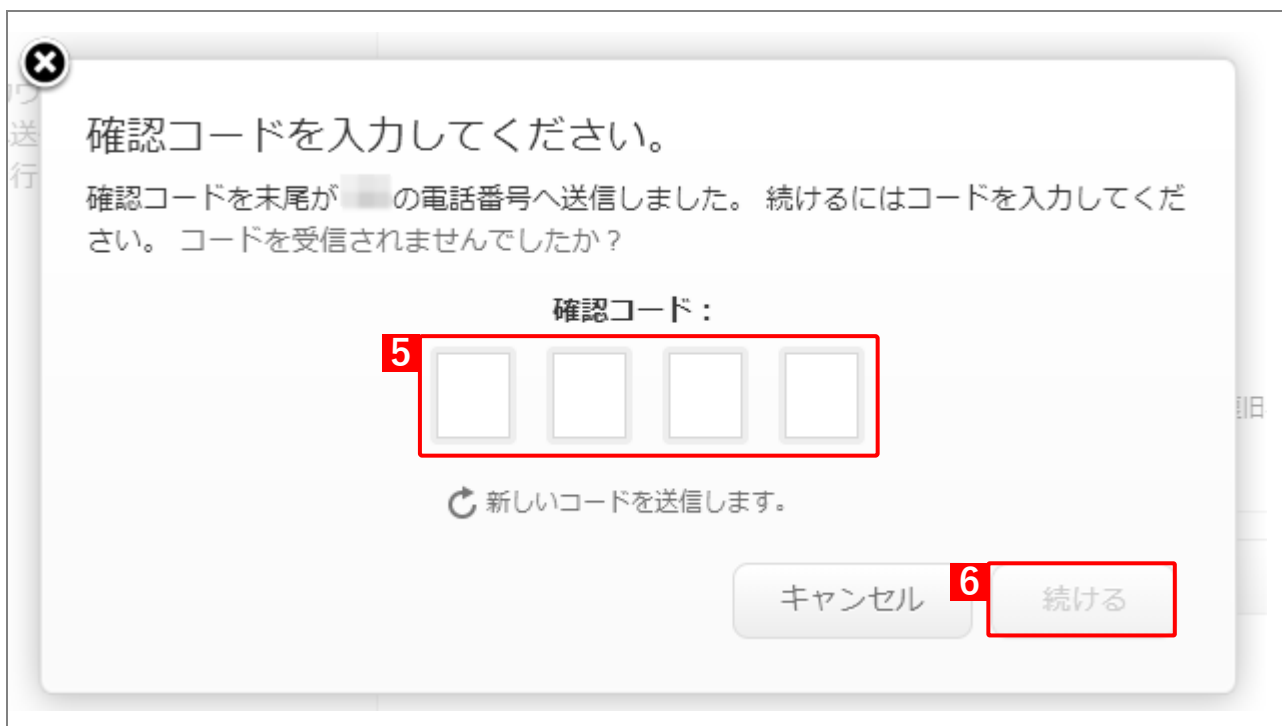
【4】 [Sign In] をクリックします。



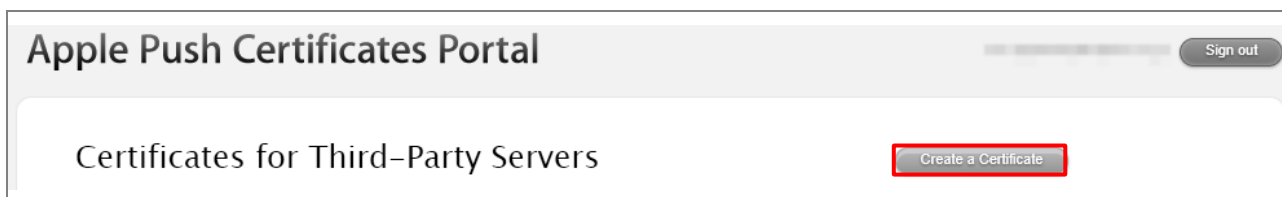
☑手順【3】から【12】は、Apple Push Certificates Portal サイトになります。

【5】 4桁の確認コードを求められるので入力します。

【6】 [続ける] をクリックして先に進めます。



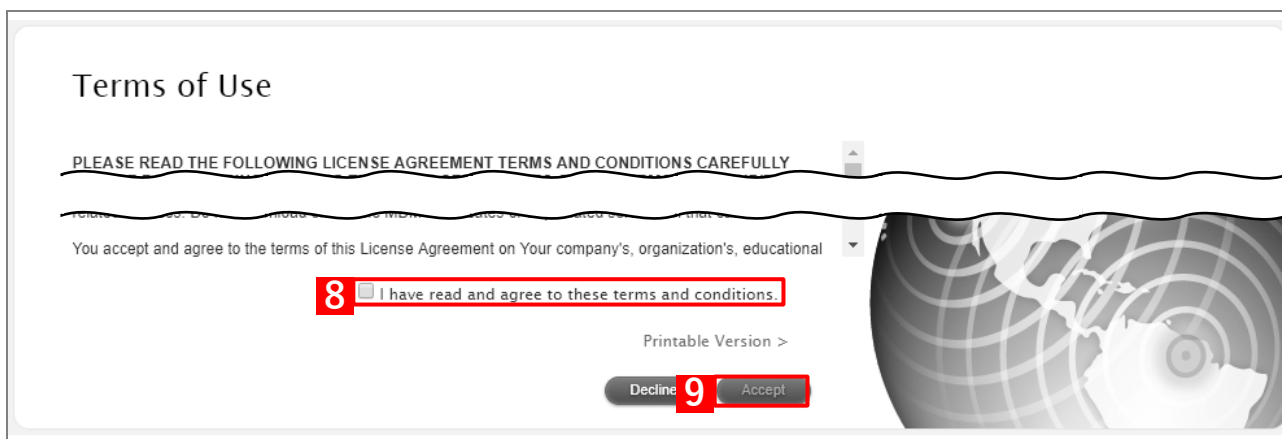
【7】 [Create a Certificate] をクリックします。



☑新規登録とすでに登録されている場合、画面の表示が異なります。

【8】規約を確認し、チェックボックスにチェックを入れます。

【9】 [Accept] をクリックします。

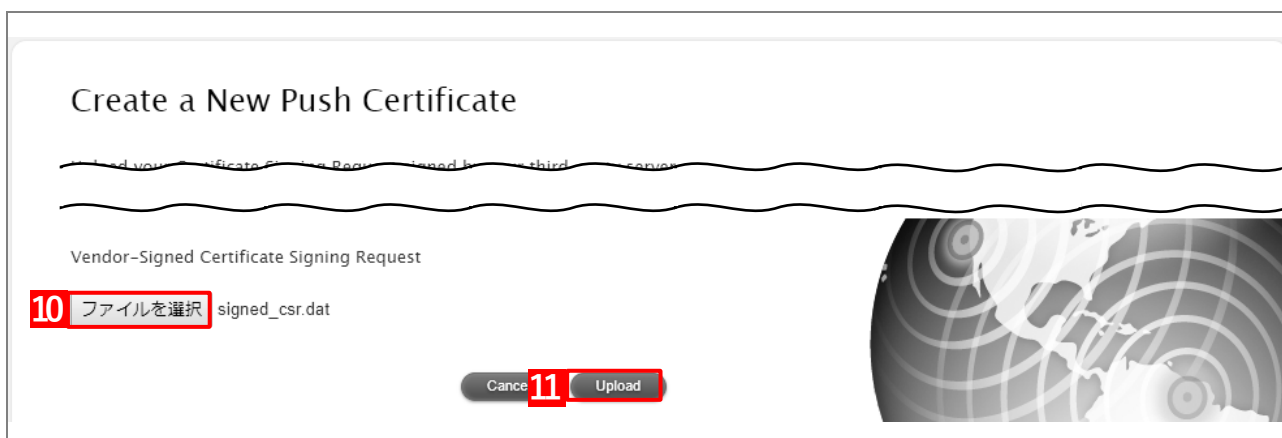


【10】 [ファイルを選択] をクリックします。

⇒手順【1】でダウンロードしたファイルを指定します。

☑選択したファイル名が [ファイルを選択] の右側に表示されます。

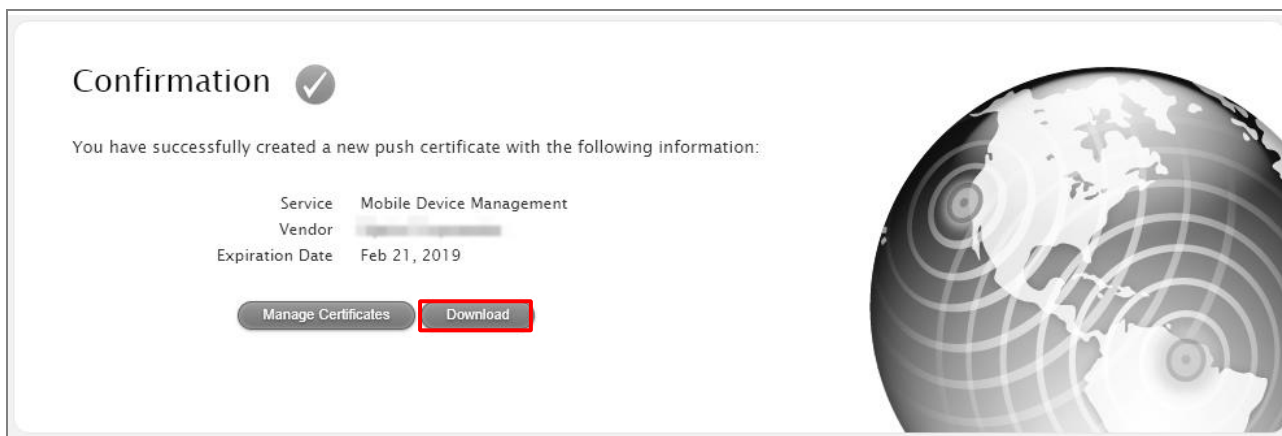
【11】 [Upload] をクリックします。



【12】 証明書が作成されました。[Download] をクリックします。

⇒作成された証明書のダウンロードが開始されます。

☑ファイルは任意の場所に保存します。



【13】 管理サイトに戻り、「3.証明書ファイルの登録」の「ファイルを選択」をクリックします。

⇒ Apple Push Certificates Portal で作成した証明書ファイルを指定します。

☑ 選択したファイル名が「ファイルを選択」の右側に表示されます。

☑ 「Apple ID」には、証明書発行のときに利用した Apple ID を入力してください。

【14】 「保存」をクリックします。

3. 証明書ファイルの登録

13 り作成した証明書ファイルを指定してください。

ファイルを選択 選択されていません

Apple ID (証明書発行の際に使用された Apple ID を以下に記載してください。)

備考

14

保存 **取消**

【15】 Apple Push 証明書の登録が完了しました。

① 証明書を登録しました。

証明書
2019/02/21 17:29:50まで有効
トピック
Apple ID
備考

編集 **証明書を削除**

2.2.3 Windows 機器用の基本設定

Windows 端末と管理サーバー間での通信間隔、端末側でのエージェント停止・ライセンス解除・アンインストール時のパスワードの設定を管理サイトで設定します。設定を行わない場合は、デフォルト値が使用されます。機器用の基本設定が終わったら、以下の操作に進みます。

🔗「グループ/ユーザー/組織を登録する」18 ページ

🔗Windows の設定については、以下を参照してください。

🔗『管理サイト リファレンス マニュアル』の「設定 - Windows」

◆管理アプリの通信と動作の設定画面

表示操作 [設定] → [Windows] → [管理アプリの通信と動作] → [編集]

エージェント共通管理 - 編集

1 管理サーバーとの通信間隔

- ☒ 分数指定: 分
- ☐ 時間指定: 時間
- ☐ 日数指定: 日

※機種によって端末のスリープ・休止中は通信が行われないことがあります。
※通信間隔が短い場合、端末のバッテリー消費が早まる可能性があります。

2 管理サーバーと通信できなかった場合

ロック

- ☒ ロックしない
- ☐ 指定分数後にロック: 分
- ☐ 指定時間後にロック: 時間
- ☐ 指定日数後にロック: 日

※通信間隔の設定によってはロックまでに時間がかかることがあります。

ロックメッセージ

2 ワイプ

- ☒ ワイプしない
- ☐ 指定分数後にワイプ: 分
- ☐ 指定時間後にワイプ: 時間
- ☐ 指定日数後にワイプ: 日

※通信間隔の設定によってはワイプまでに時間がかかることがあります。

▲ 管理サーバーや端末の状況に関わらず、通信できなかった場合にワイプされます。設定保存前に、内容を今一度ご確認ください。

ワイプの方法

- ☐ BitLocker

暗号化済みドライブの暗号化キーを削除することで、リモートワイプに相当する機能を提供します。

▲ 非対応のOSの場合や、BitLockerが有効でない場合はワイプできません。

- ☐ データ削除

ファイルの削除やドライブのフォーマットにより、リモートワイプを実行します。

▲ OSが起動できなくなります。クラウドのオンラインストレージをご利用の場合は、同期されているクラウドサービス内のデータが削除されることがあります。リモートワイプのデータ削除を設定する前に、クラウドストレージサービスのご利用アカウントを停止する処置を必ず行ってください。

3 端末でのリモートロックの解除方法

- ☐ なし
- ☐ 解除コードの入力

4 端末でのエージェント停止・ライセンス解除・アンインストールの制限

- ☐ 制限なし
- ☐ パスワードの入力

5 ライセンス認証オプション

- ☐ 管理外機器の検出を有効にする
- ☐ 管理外機器の検出を有効にする(次回ライセンス認証時のみ)
- ☐ なし

6 管理サイトログイン画面へのリンク

- ☐ 表示
- ☒ 非表示

取消


保存


◆ 設定項目


項番	項目		デフォルト値	説明
1	管理サーバーとの通信間隔		30 分	管理サーバーとの通信間隔を設定します。
2	管理サーバーと通信できなかった場合	ロック	ロックしない	管理サーバーと通信できなくなった場合に、端末にロックをかけることができます。ロック後の端末にメッセージを表示することもできます。
		ワイプ	ワイプしない	管理サーバーと通信できなくなった場合に、端末のワイプ（初期化）を行えます。
3	端末でのリモートロックの解除方法		解除コードの入力：ランダム値で自動生成されたパスワード	端末でのリモートロックの解除方法を設定します。
4	端末でのエージェント停止・ライセンス解除・アンインストールの制限		制限なし	端末からエージェントを停止したり、ライセンス解除をしたり、アンインストールをする場合のパスワードを設定します。
5	ライセンス認証オプション		管理外機器の検出を有効にする（次回ライセンス認証時のみ）	ライセンス認証時に管理外機器の検出を有効にするかどうかを選択します。
6	管理サイトログイン画面へのリンク		非表示	エージェントに管理サイトログイン画面へのリンクを設定するかどうかを設定します。

2.3 グループ／ユーザー／組織を登録する

機器を使用するために、必要に応じて、機器グループやユーザーグループ、ユーザー、組織の登録を行います。登録が完了しましたら、以下の操作に進みます。

 「機器にエージェントアプリをインストールする」 31 ページ

 グループ分けの考え方については、以下を参照してください。

 「グループ分けを検討する」 7 ページ

●ユーザーグループ（所属部署や役職で分ける場合など）

ユーザーを部署や役職なのでまとめて、効率よく管理したい場合に利用します。

例えば、部署や役職でグループを設定し、機器の管理情報でその部署や役職に所属するユーザーを設定することによって、「全機器一括設定」で対象のユーザーグループごとに設定した機能を同じグループに所属するユーザーが紐付いた機器に対して、まとめて適応できます。

●機器グループ（機器の用途ごとに分けたい場合など）

機器を用途ごとのグループにまとめて、効率よく管理したい場合に利用します。

例えば、機器の用途に応じて、「社内使用端末」、「社外持ち出し用端末」のように必要な機器グループを設定し、機器の管理情報でグループを設定にすることによって、「全機器一括設定」で対象の機器グループごとに設定した機能を同じグループの機器に対して、まとめて適応できます。

●ユーザー

ユーザーを作成し、ユーザーグループと併用することで、機器の管理情報でユーザーと紐付いている機器に対して機能を適用できます。

ユーザーは、個別に登録する方法と、CSV ファイルからまとめて追加する方法があります。

●組織

ユーザーや機器を所属させ、組織単位で機器設定を行ったり、ユーザー分類と組織を併用することで組織別のアクセス権限（追加権限）を付与できます。

2.3.1 ユーザーグループを登録する

入力項目のカスタマイズ機能で、以下の手順にしたがってグループを登録します。

【1】 [ユーザー] → [入力項目のカスタマイズ] → 「分類」 タブをクリックします。

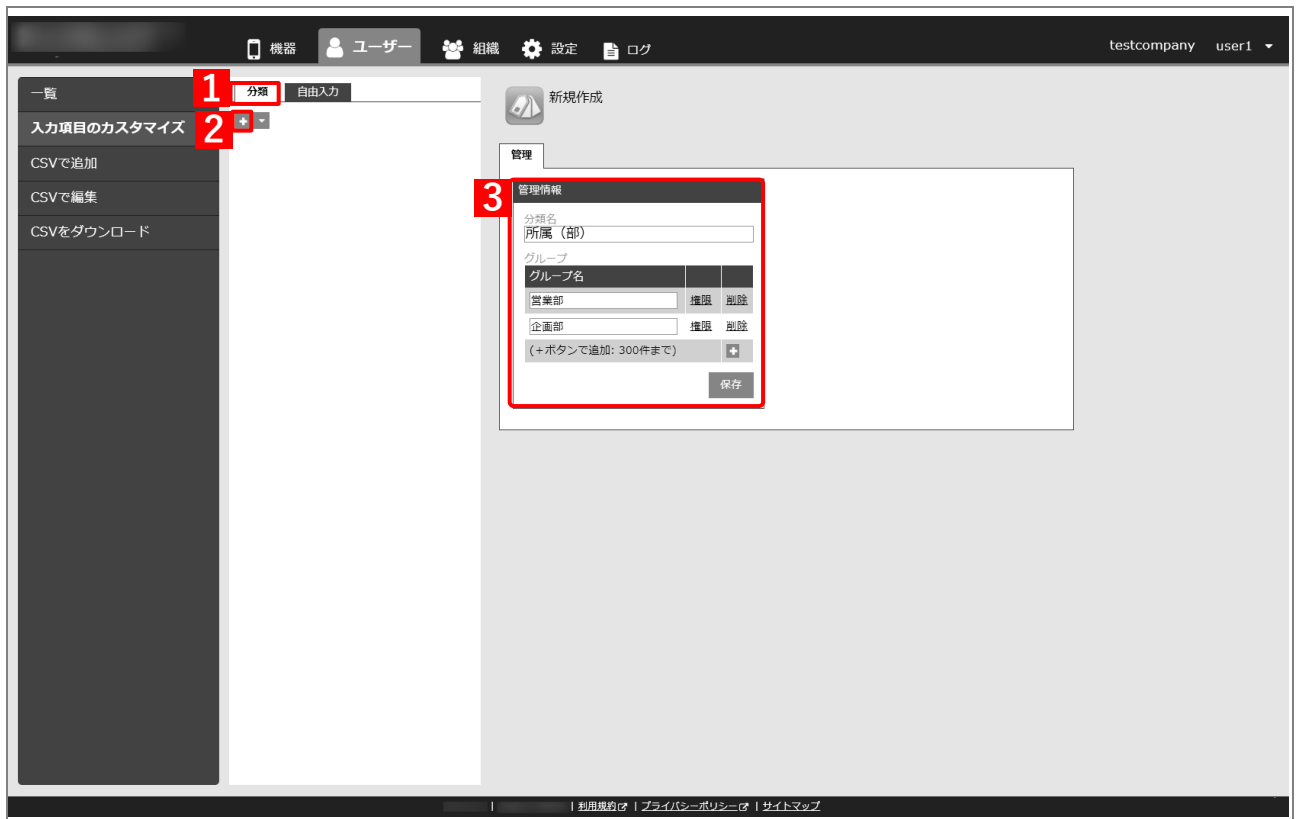
【2】 **+** をクリックします。

⇒新規作成画面が表示されます。

【3】 「分類名」を「グループ」を入力し、[保存] をクリックします。

✎グループの項目を追加するには **+** をクリックします。**×** をクリックすると入力欄が削除されます。

✎グループに権限を与える場合には、「権限」のリンクをクリックし、設定します。



【4】「分類」タブの一覧に分類が登録されたことを確認します。

☑ 例として、以下が登録されています。

分類名：所属（部） グループ名：営業部、企画部

分類名：役職 グループ名：部長、課長、なし

The screenshot shows the 'Classification' tab in the Office Management System. The left sidebar contains a list of items, with '分類' (Classification) selected. The main area displays a list of classifications. A red box highlights the '所属（部）' (Department) and '役職' (Position) entries. The '所属（部）' entry is selected, and its details are shown in a modal window on the right.

分類名: 所属（部）
グループ名: 営業部, 企画部

分類名: 役職
グループ名: 部長, 課長, 役職なし

管理情報

グループ名	権限
部長	権限
課長	権限
役職なし	権限

編集


2.3.2 機器グループを登録する

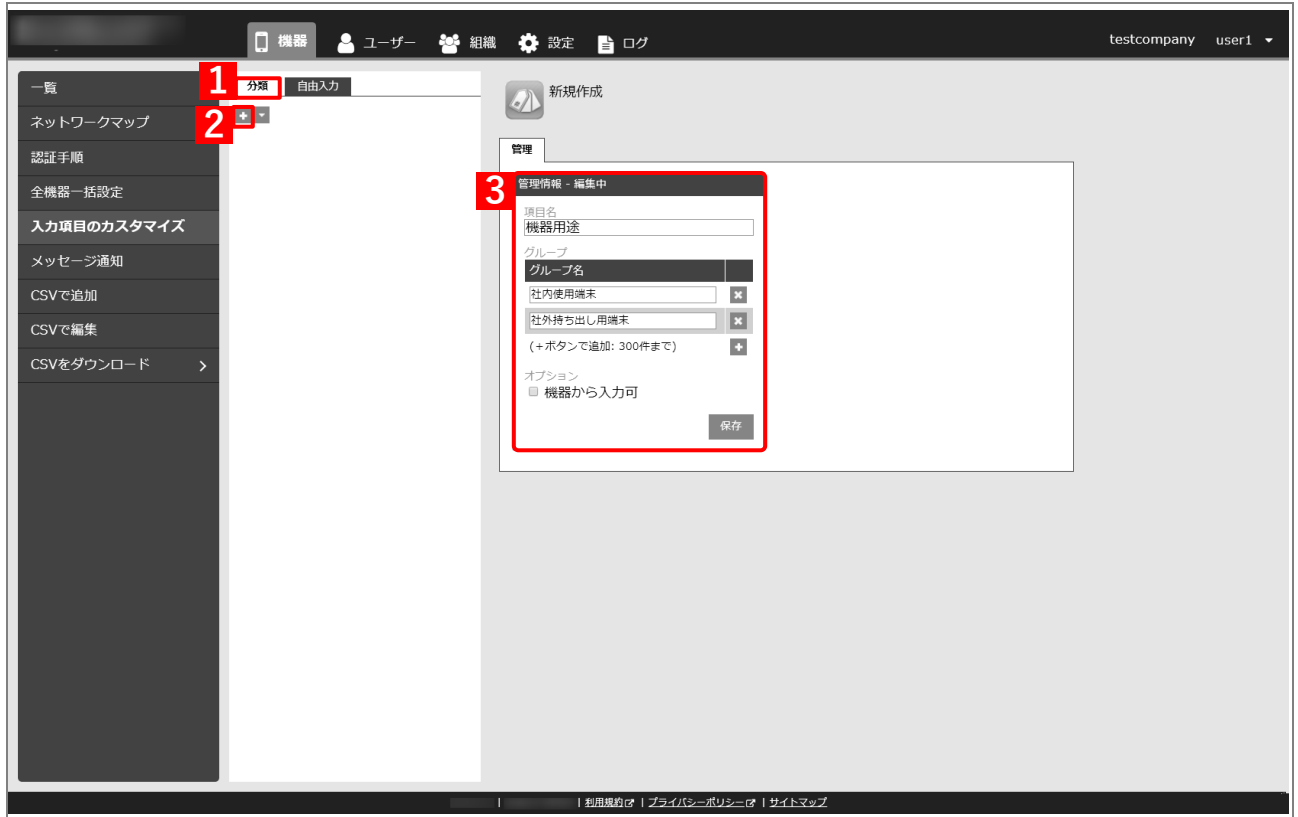
【1】 [機器] → [入力項目のカスタマイズ] → 「分類」 タブをクリックします。

【2】 **+** をクリックします。

⇒ 新規作成画面が表示されます。

【3】 「項目名」と「グループ」を入力し、[保存] をクリックします。

 グループの項目を追加するには **+** をクリックします。**×** をクリックすると入力欄が削除されます。



The screenshot shows the 'New Device Group' (新規作成) screen. The sidebar on the left has a 'Classification' (分類) tab selected, indicated by a red '1'. Below it, a '+' button is highlighted with a red '2'. The main form area is titled 'Management Information - Editing' (管理情報 - 編集) and contains the following fields:

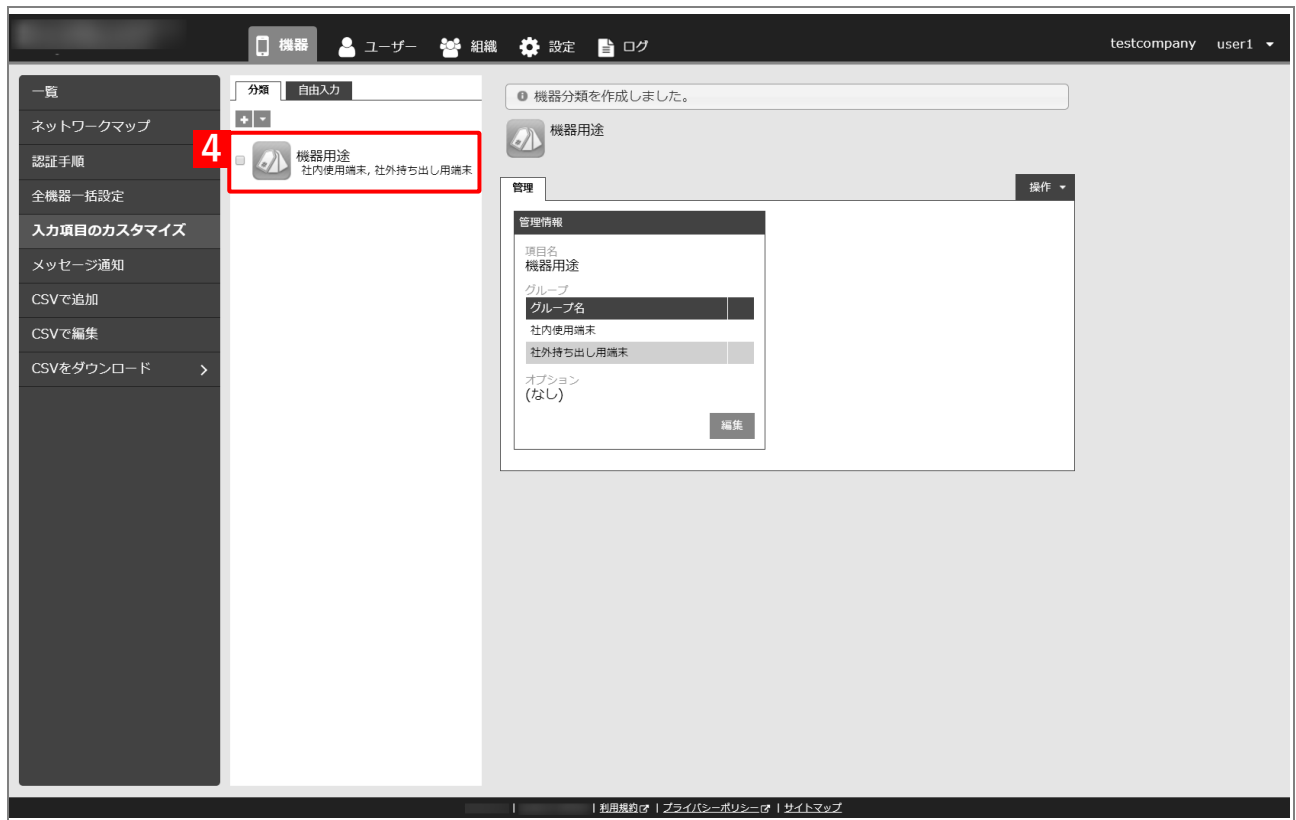
- Item Name (項目名): 機器用途
- Group (グループ): 機器用途
- Group Name (グループ名): [Empty]
- In-house Use End (社内使用端末): [Empty]
- Outside Use End (社外持ち出し用端末): [Empty]
- (+ button to add: 300 items max) (+ボタンで追加: 300件まで)
- Options (オプション): ☒ Device Input (機器から入力可)
- Save (保存) button

A red box highlights the form fields, and a red '3' indicates the step to fill in the form and click 'Save'.

【4】「分類」タブの一覧に分類が登録されたことを確認します。


例として、以下が登録されています。

項目名：機器用途 グループ名：社内使用端末、社外持ち出し用端末




2.3.3 組織を登録する


【1】 [組織] → [一覧] をクリックします。

【2】  をクリックします。

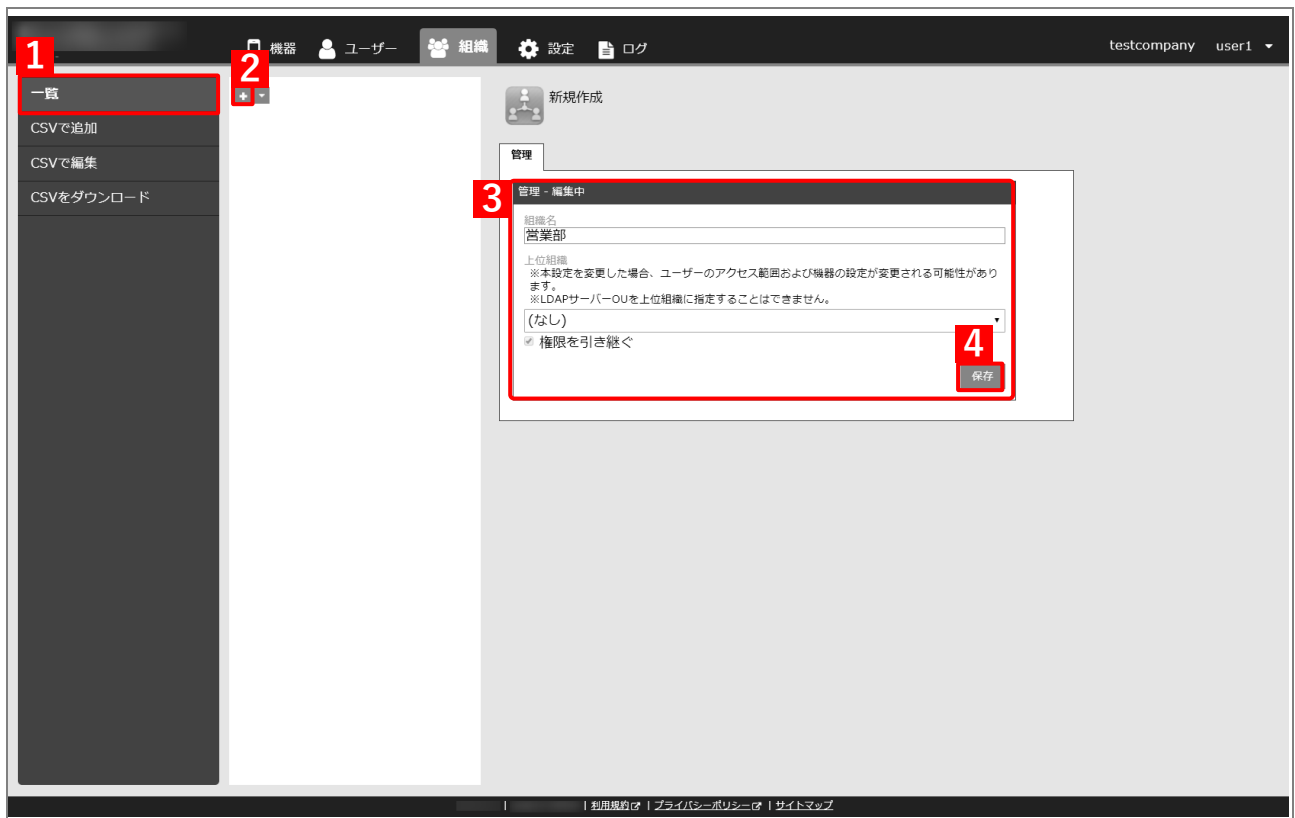
⇒ 新規作成画面が表示されます。

【3】 「組織名」を入力します。

 「上位組織」は、作成中の組織の上位となる組織を設定する場合に選択します。作成中の組織が最上位となる場合、「(なし)」を選択します。

 「権限を引き継ぐ」は、作成中の組織の上位の組織に対し、あるユーザーに追加権限が与えられた場合、そのユーザーが作成中の組織でも同じ追加権限を行使できるかどうかを決めるものです。作成中の組織に対して、追加権限の行使を許可しない場合は、チェックを外してください。

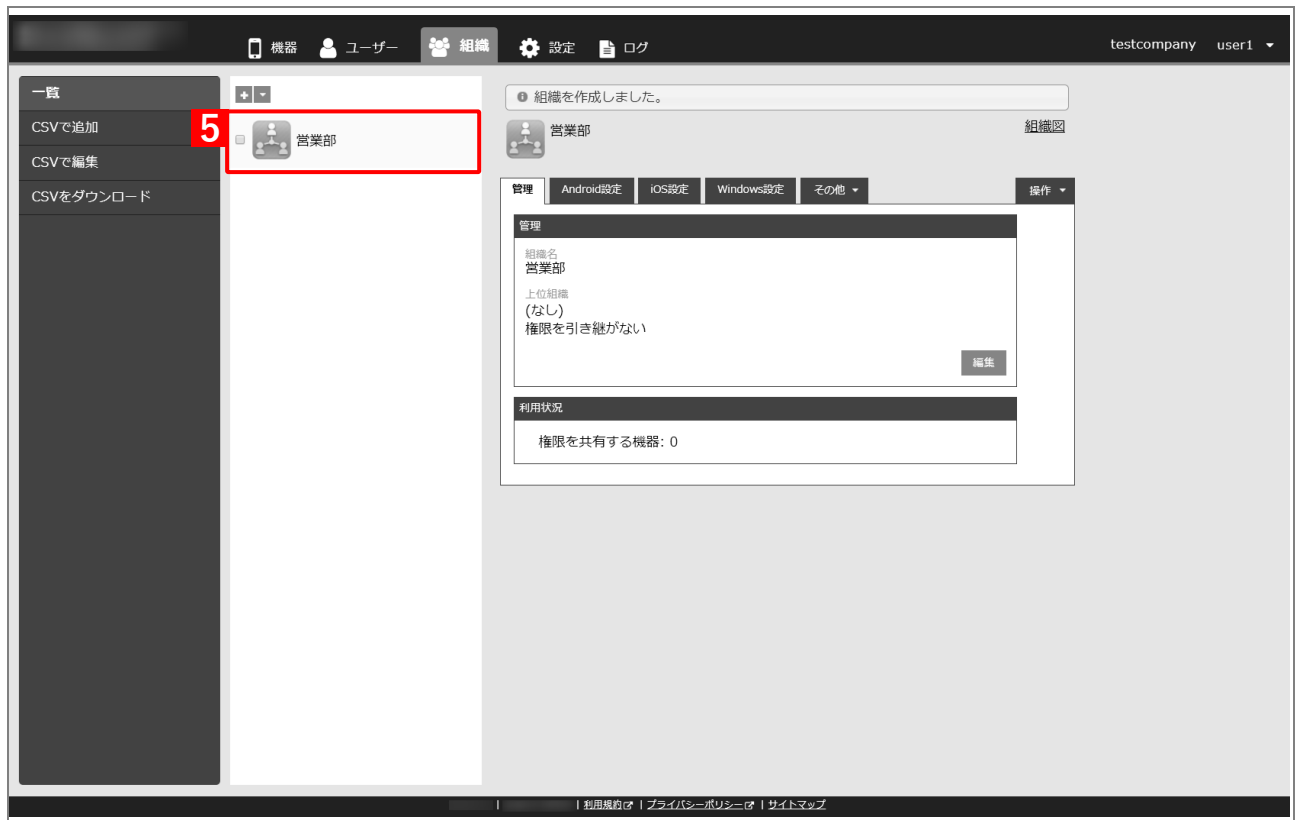
【4】 [保存] をクリックします。



【5】一覧に組織が登録されたことを確認します。

☑ 例として、以下が登録されています。

組織名：営業部



2.3.4 ユーザーを登録する

機器を使用するユーザーの登録を行います。1人ずつ登録する場合は以下の手順で登録を行ってください。
複数まとめてユーザーの登録を行いたい場合は、以下を参照してください。

🔖 「複数ユーザーをまとめて登録する」 27 ページ

管理情報の項目については、以下を参照してください。

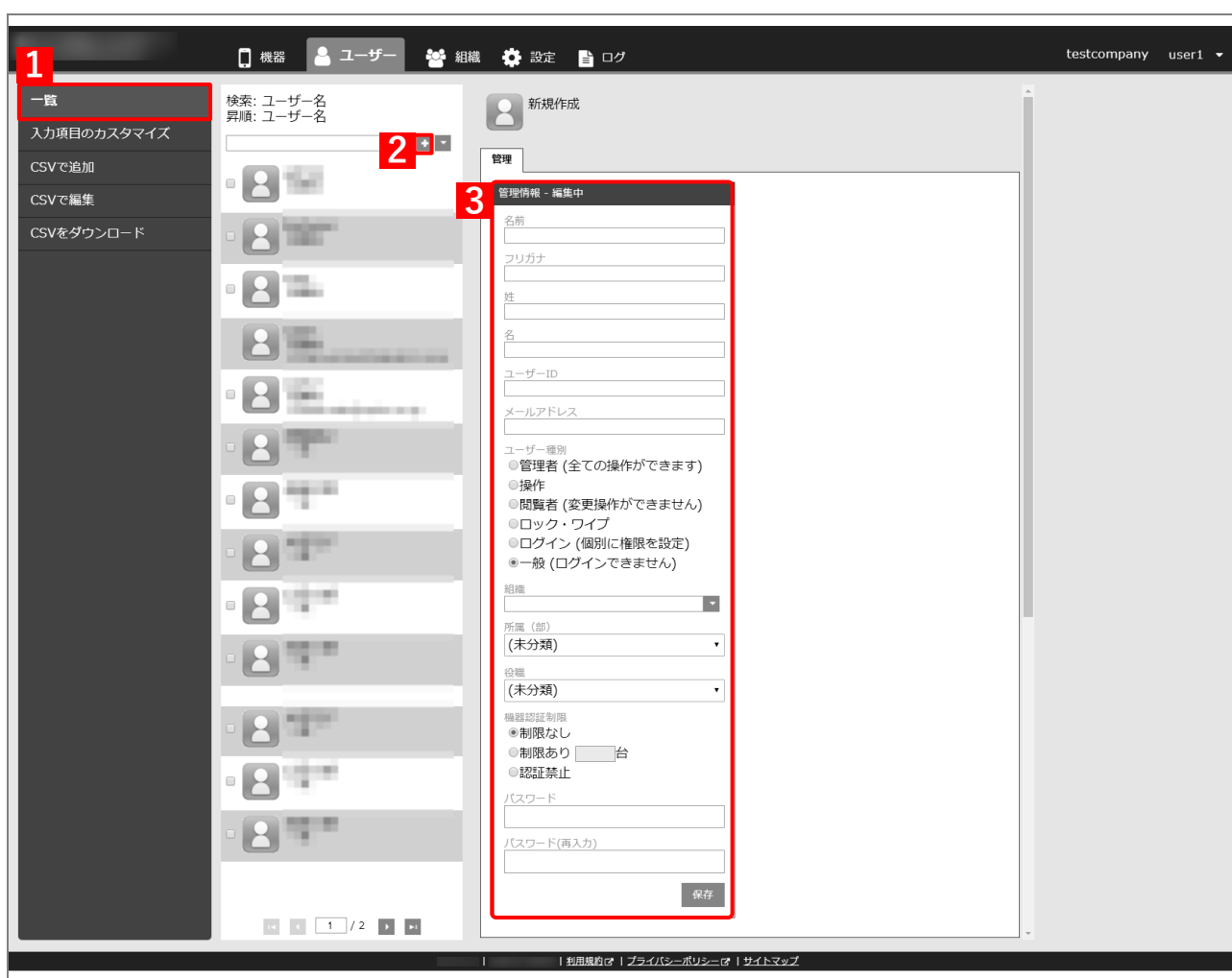
🔖 『管理サイト リファレンス マニュアル』の「ユーザー」 - 「一覧」 - 「ユーザーの作成」

【1】 [ユーザー] → [一覧] をクリックします。

【2】  をクリックします。

⇒ ユーザーの新規作成画面が表示されます。

【3】 管理情報を入力し、[保存] をクリックします。



【4】一覧にユーザーが登録されたことを確認します。

オフィスまるごとサポート
デバイスマネジメント

testcompany 管理者

ユーザー

検索: ユーザー名
昇順: ユーザー名

4 山田 太郎
yamada@example.com

ユーザーを作成しました。

山田 太郎
yamada@example.com

管理 VPP設定 その他 操作

管理情報

名前
山田 太郎
フリガナ
ヤマダ タロウ
姓
山田
名
太郎
ユーザーID
yamada
メールアドレス
yamada@example.com
ユーザー種別
操作
組織
(なし)
機器認証制限
制限なし

パスワード

現在のパスワード

編集

機器

機器数
1

編集

ver.9.3.0 | ©2017 OPTIM | 利用規約 | プライバシーポリシー | サイトマップ

2.3.5 複数ユーザーをまとめて登録する

複数のユーザーをまとめて登録したい場合は、CSV ファイルをダウンロードし、ユーザー情報を入力しインポートすることで、複数のデータをまとめて登録することができます。

✏️ インポートできるファイルサイズは 10MB までです。

✏️ CSV でユーザーをまとめて追加する方法については、以下を参照してください。

📖 『管理サイト リファレンス マニュアル』の「ユーザー」－「CSV で追加」

【1】 [ユーザー] → [CSV で追加] をクリックします。

【2】 [ダウンロード] をクリックします。

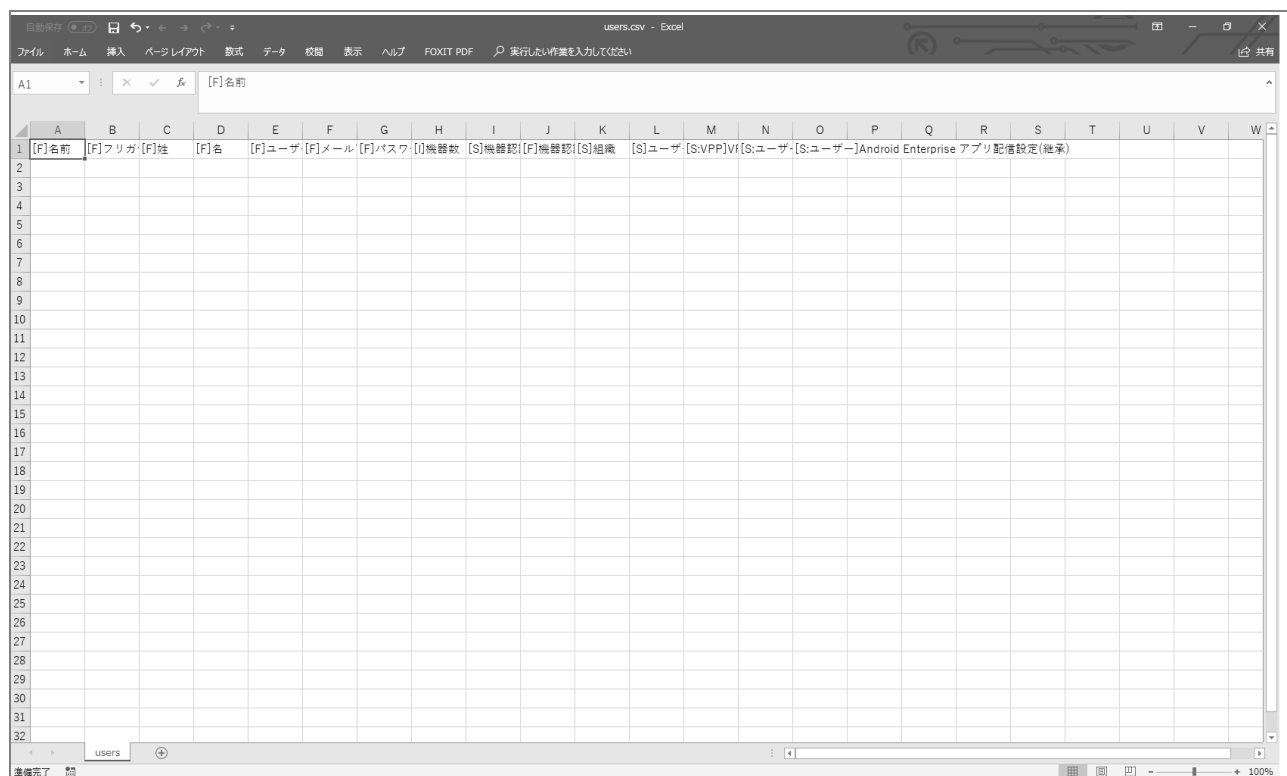
⇒ データ入力用の CSV ファイルがダウンロードされます。

✏️ 任意の場所に保存してください。



【3】ダウンロードした CSV ファイルを開き、2 行目からユーザー情報を入力し、保存します。

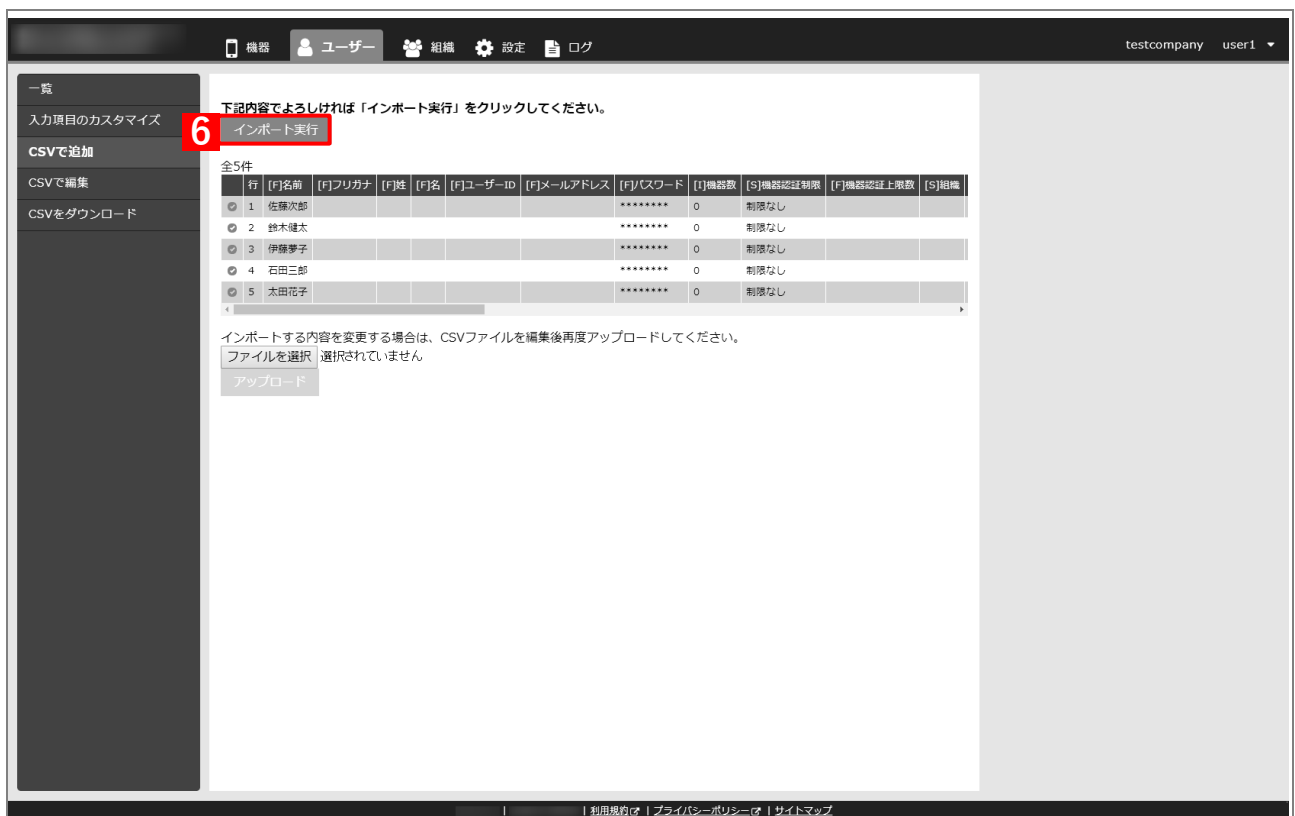
- ☑ CSV ファイルは、メモ帳や EXCEL などで操作してください。
- ☑ 縦列の数やタイトルは、ユーザー項目のカスタマイズにより、分類名やグループが登録されていると追加されます。
- ☑ 「ユーザー種別」には、「管理者」、「閲覧者」、「一般」のいずれかを入力してください。ユーザー分類は、すでに登録されているものを入力してください。
- ☑ ファイルを保存する場合、CSV ファイル名は変更しても問題ありませんが、ファイルの種類は「CSV（コンマ区切り）（*.csv）」を選択してください。



- 【4】 [ファイルを選択] をクリックして、【3】で作成した CSV ファイルを選択します。
⇒ 選択したファイル名が表示されます。
- ☑ ご利用のブラウザによって、[ファイルを選択] ではなく [参照] の場合があります。
- 【5】 [アップロード] をクリックします。
⇒ インポート実行画面が表示されます。



- 【6】 CSV ファイルの内容を確認し、[インポート実行] をクリックします。



【7】インポート結果を確認します。

The screenshot shows the 'ユーザー' (Users) section of the Office 365 User Management interface. A red box highlights a message 'インポートに成功しました。' (Import successful.) and a table of imported users. The table has 11 columns: 行 (Row), [F]名前 (First Name), [F]フリガナ (Furigana), [F]姓 (Last Name), [F]ユーザーID (User ID), [F]メールアドレス (Email Address), [F]パスワード (Password), [I]機器数 (Number of Devices), [S]機器認証制限 (Device Authentication Limit), [F]機器認証上乗数 (Device Authentication Multiplier), and [S]編集 (Edit). The table contains 5 rows of user data.

行	[F]名前	[F]フリガナ	[F]姓	[F]ユーザーID	[F]メールアドレス	[F]パスワード	[I]機器数	[S]機器認証制限	[F]機器認証上乗数	[S]編集
1	佐藤次郎					*****	0	制限なし		
2	鈴木健太					*****	0	制限なし		
3	伊藤夢子					*****	0	制限なし		
4	石田三郎					*****	0	制限なし		
5	太田花子					*****	0	制限なし		

2.4 機器にエージェントアプリをインストールする

機器にエージェントアプリをインストールし、認証を行うことによって、その機器を管理サイトの管理対象にできます。ご利用になる機器ごとに操作してください。

グループ、組織、ユーザーと機器の関連付けを行って機器を管理する場合は、以下の手順に進みます。

🔗 「ユーザー／組織／機器グループと各機器を関連付ける」 43 ページ

2.4.1 Android 端末の場合

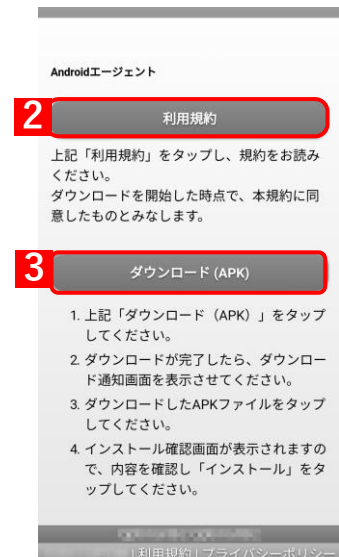
Android 端末の場合は、Android 端末へエージェントをインストールし、ライセンス認証を行う必要があります。

- ❑ インストール時には Android 端末設定画面の「提供元不明のアプリ」にチェックを入れる必要があります。チェックを入れていない場合は、チェックを入れたあとにインストールを行ってください。
- ❑ Android 6.0 以降の場合は、一部操作方法が異なります。詳細は以下を参照してください。
🔗 『Android ユーザーマニュアル』の「エージェントをインストールする」
- ❑ Android 7.0 以降の場合は、Device Owner Mode が利用できます。Device Owner Mode を利用しないと、ご希望の管理ができない場合があります。詳細およびキッティング方法については、以下を参照してください。


🔗 『Device Owner Mode 導入マニュアル』

エージェントのインストールとライセンス認証

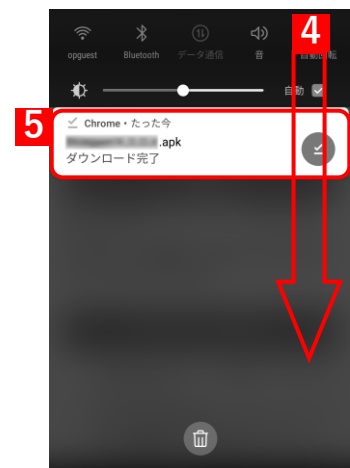
- [1]** ブラウザーを起動し、エージェントダウンロード画面を表示します。
- [2]** 「利用規約」をタップし、利用規約を確認します。
- [3]** 「ダウンロード(APK)」をタップします。



【4】 画面を上から下へスライドし、ダウンロード通知画面を表示させます。

 Android 3.x の Android 端末は、右下の通知をタップしてください。

【5】 ダウンロードしたエージェントをタップします



【6】 [インストール] をタップします。



【7】 インストールしています。しばらくお待ちください。



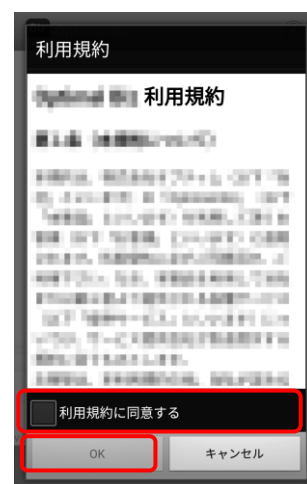
【8】 インストールが完了しました。[開く] をタップします。



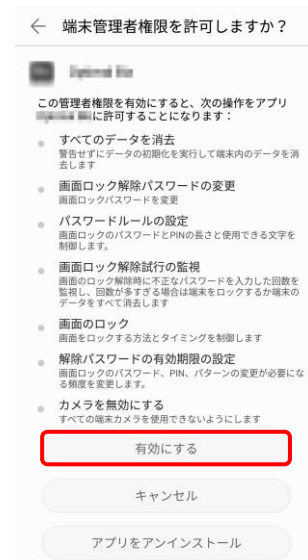
【9】 [ライセンス認証] をタップします。



【10】 利用規約を確認後、「利用規約に同意する」にチェックを入れ、[OK] をタップします。



【11】 エージェントインストール直後にライセンス認証を行った場合は、右の画面が表示されます。[有効にする] をタップします。

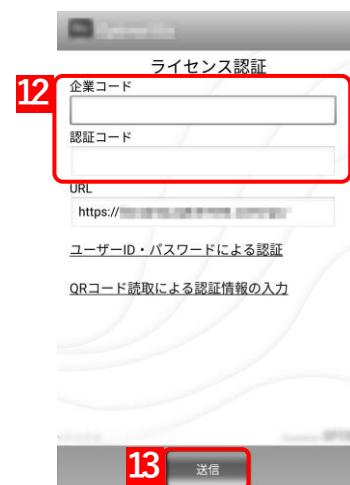


【12】 企業コード、認証コードを入力します。

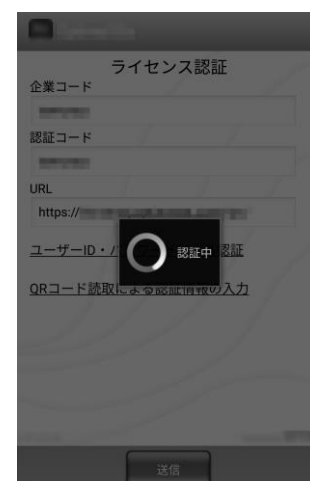
✎ ユーザーID とパスワードによる認証の場合は、[ユーザーID・パスワードによる認証] をタップします。

【13】 [送信] をタップします。

✎ URL は変更不要です。



【14】 ライセンス認証を行っています。しばらくお待ちください。



【15】 設定が完了しました。[OK] をタップします。



【16】 機器やユーザーのカスタマイズ項目で、グループや入力項目などが登録されている場合は、初期登録画面で設定できます。設定する場合は画面に従って操作してください。設定を行わない場合は「閉じる」をタップします。

✎ 設定は管理サイトからも行えます。管理サイトからの設定については以下を参照してください。

📖 「ユーザー／組織／機器グループと各機器を関連付ける」43 ページ



2.4.2 iOS 機器の場合

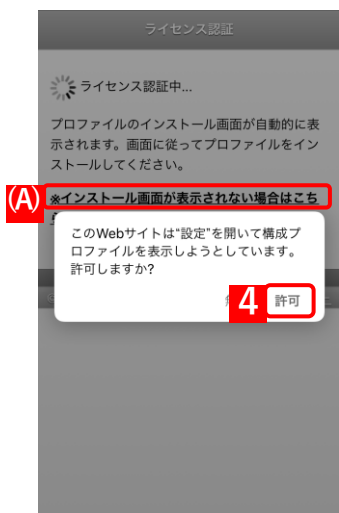
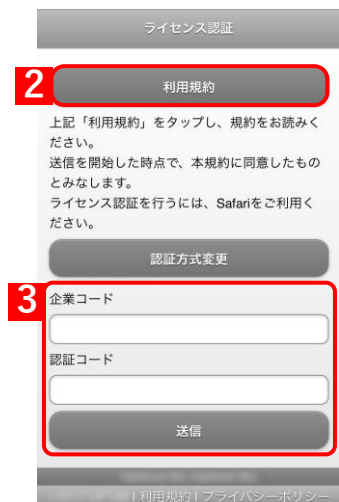
iOS 機器の場合は、以下のインストールと認証を行います。

- プロファイルのインストール、ライセンス認証
iOS 機器を管理サイトで管理するために、必ず行います。
 - エージェントのインストール、エージェント認証
位置情報取得、メッセージ配信、Jailbreak 検知機能を使用する場合に行ってください。
- ✍️ ライセンス認証ページのアドレスは管理者またはオペレーターにお問い合わせください。
- ✍️ 本章ではエージェント自動認証機能を使用する方法を紹介します。認証先の URL を選択し、認証を行う場合は、以下を参照してください。

📖 『iOS ユーザーマニュアル』の「エージェント認証を行う」

◆ エージェント自動認証機能を使ったインストール手順

- 【1】 ブラウザー（Safari）を起動し、ライセンス認証ページを表示します。
- 【2】 「利用規約」をタップし、利用規約を確認します。
✍️ 送信を開始した時点で、本規約に同意したものとみなします。
- 【3】 企業コード、認証コードを入力し、「送信」をタップします。
✍️ 企業コード、認証コードは管理者にお問い合わせください。
✍️ ユーザーID とパスワードによる認証の場合は「認証方式変更」をタップします。
- 【4】 自動的にインストール画面が表示されます。しばらくお待ちください。
✍️ 許可を求められる画面が表示された場合は、「許可」をタップしてください。
✍️ インストール画面が表示されない場合は、(A) をタップします。ダウンロードしたエージェントをタップします



【5】 [インストール] をタップします。

✎ [インストール] の左に「未検証」または「検証済み」と表示されていても問題ございません。そのまま操作を続けてください。

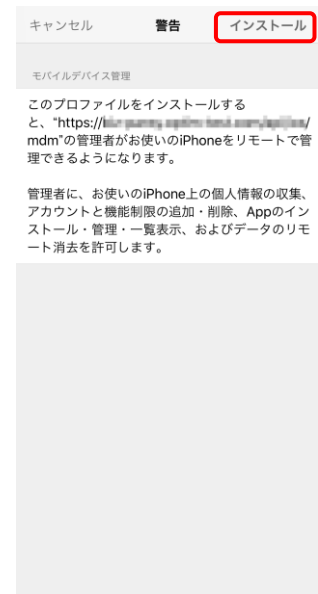


【6】 [インストール] をタップします。

✎ パスコードが設定されている場合は、パスコード入力画面が表示されますので入力してください。



【7】 内容を確認し、[インストール] をタップします。



【8】 内容を確認し、[信頼] をタップします。



【9】 インストールが完了しました。[完了] をタップします。



【10】 ライセンス認証が完了しました。[次へ] をタップします。



- 【11】** 「App Store からインストール」 をタップします。
AppStore 画面へ移ります。AppStore のインストール手順に従い、インストールを行ってください。



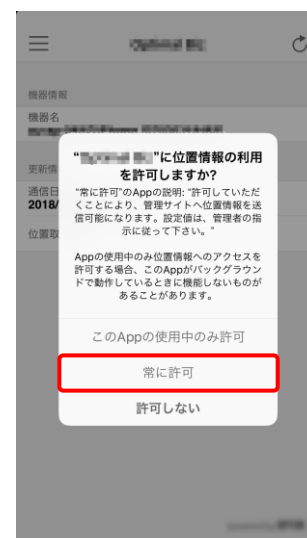
- 【12】** App Store からエージェントのインストールが完了しましたら
ブラウザを開き、手順【11】で開いていた画面を再度開きます。
「起動して認証」 をタップします。



- 【13】** エージェント認証を行っています。しばらくお待ちください。

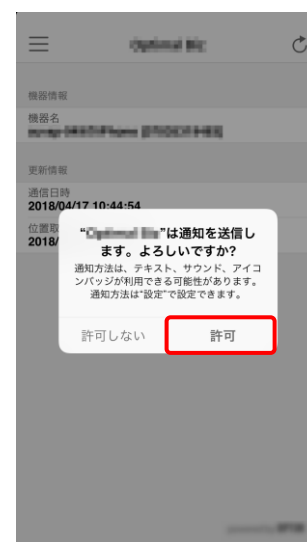


- 【14】 位置情報の利用について許可を求められますので、[常に許可] をタップします。



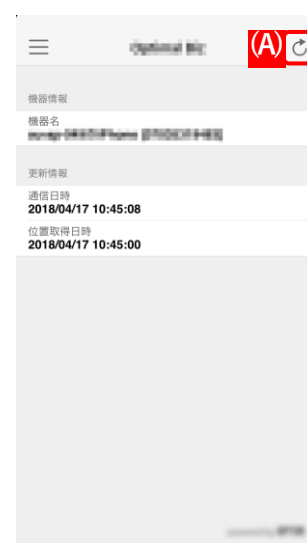
- 【15】 通知の送信について許可を求められますので、[許可] をタップします。

- 一度 [許可] をタップすると、再度エージェントを起動するときには、ポップアップ画面は表示されません。
- メッセージ機能を使用する場合は、必ず [許可] をタップしてください。[許可] をタップしない場合、メッセージ受信時、端末側に通知が表示されません。



- 【16】 エージェント認証が完了しました。
エージェント認証完了後は、自動的に位置情報を取得し、機器情報、ユーザー情報、メッセージの更新が行われます。
以降は、定期的に更新が行われます。(A) をタップすると、手動で更新を行います。

- ユーザー情報は、管理サイト側で登録されていない場合は表示されません。



2.4.3 Windows 機器の場合

Windows 機器の場合は、Windows 機器へエージェントをインストールし、ライセンス認証を行う必要があります。以下の手順に従って操作してください。

- ☑ 認証時に同一の USB LAN アダプターや、仮想ネットワークアダプターを使用した場合、各機器に同一の MAC アドレスが割り当てられます。また、コンピューターSID により機器を判定します。この両方が同一のものを認証した場合、管理サイトでは、各機器を同一機器として判定し、機器情報を上書きします。ご注意ください。上書きされた場合は、機器を削除したあとに、各機器ごとに Windows エージェントのライセンス解除／再認証を行ってください。

◆ Windows 機器へのエージェントインストール手順

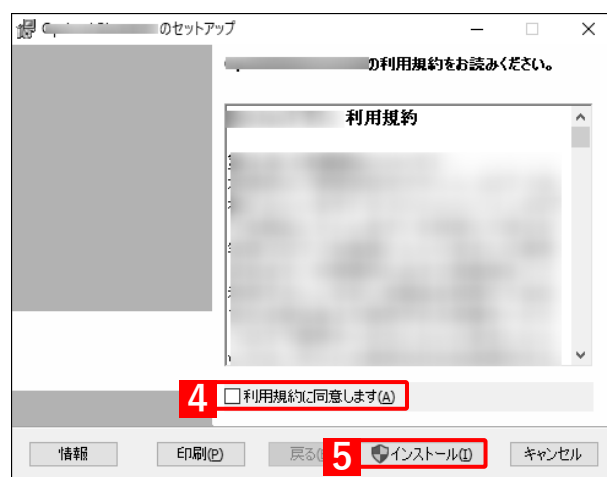
- 【1】 ブラウザーを起動し、エージェントダウンロード画面を表示します。
- 【2】 [ダウンロード (MSI)] をクリックします。



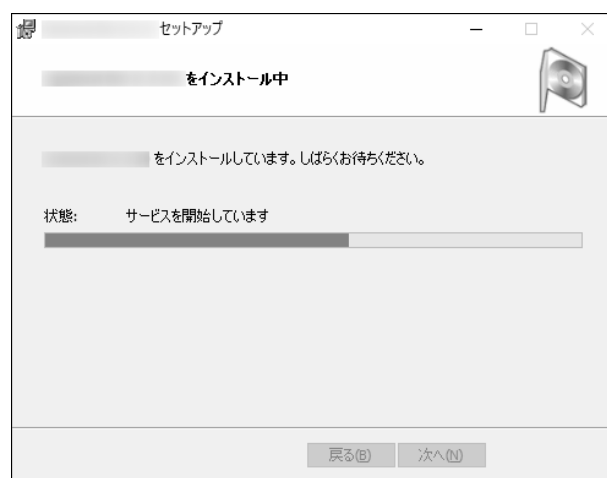
- 【3】 [実行] をクリックします。



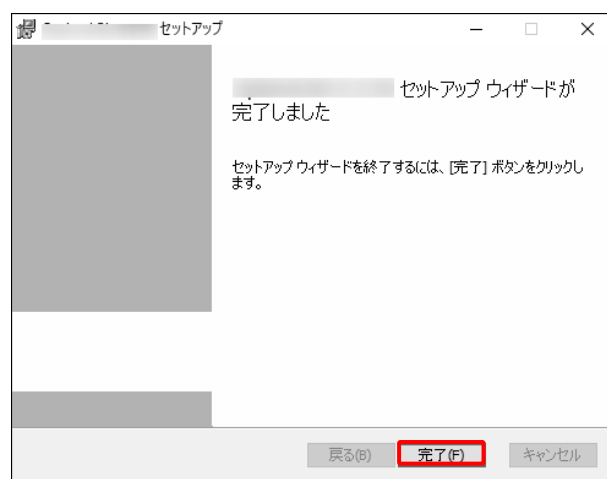
- 【4】 利用規約を確認後、「利用規約に同意します」にチェックを入れます。
- 【5】 「インストール」をクリックします。



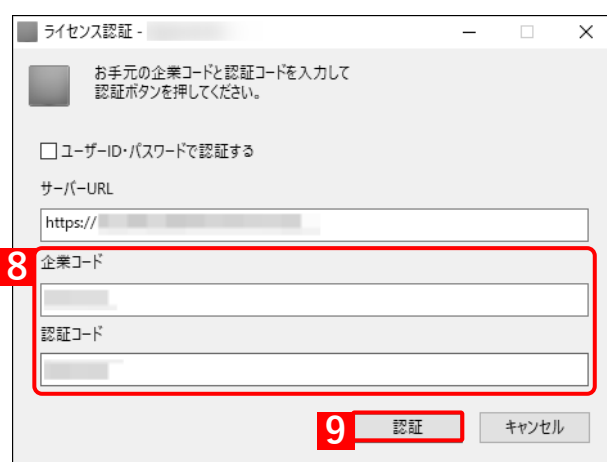
- 【6】 インストールをしています。しばらくお待ちください。



- 【7】 インストールが完了しました。「完了」をクリックします。



- 【8】 企業コード、認証コードを入力します。
 - ✎ 企業コード、認証コードは管理者にお問い合わせください。
 - ✎ ユーザーID とパスワードによる認証の場合は「ユーザー情報で認証する。」にチェックを入れてから、「企業コード」、「ユーザーIDもしくはメールアドレス」、「パスワード」を入力します。
- 【9】 「認証」をクリックします。
⇒ 初期登録画面が表示されます。



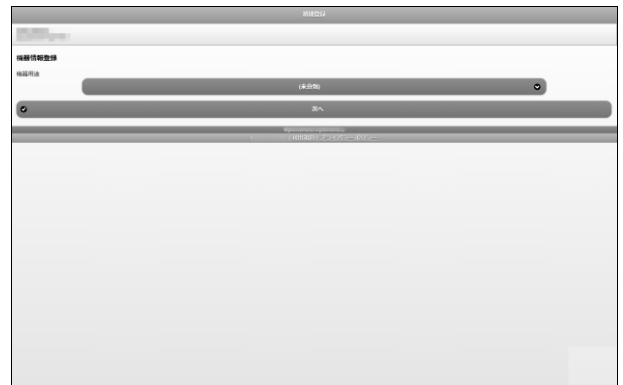
【10】 機器情報の登録ができます。登録を行わない場合はブラウザを閉じてください。

- 一度ブラウザを閉じて、Windows エージェントタスクトレイアイコンメニューの「ポータル」から、再度、登録を行えます。詳細は、以下を参照してください。

『Windows ユーザーマニュアル』

- 機器情報の登録は管理サイトからも行えます。管理サイトからの登録方法は、以下を参照してください。

「ユーザー／組織／機器グループと各機器を関連付ける」43 ページ



2.5 ユーザー／組織／機器グループと各機器を関連付ける

「グループ／ユーザー／組織を登録する」で登録したユーザー、組織、グループと「機器にエージェントアプリをインストールする」で管理サイトに登録した機器を以下の手順に従って関連付けます。

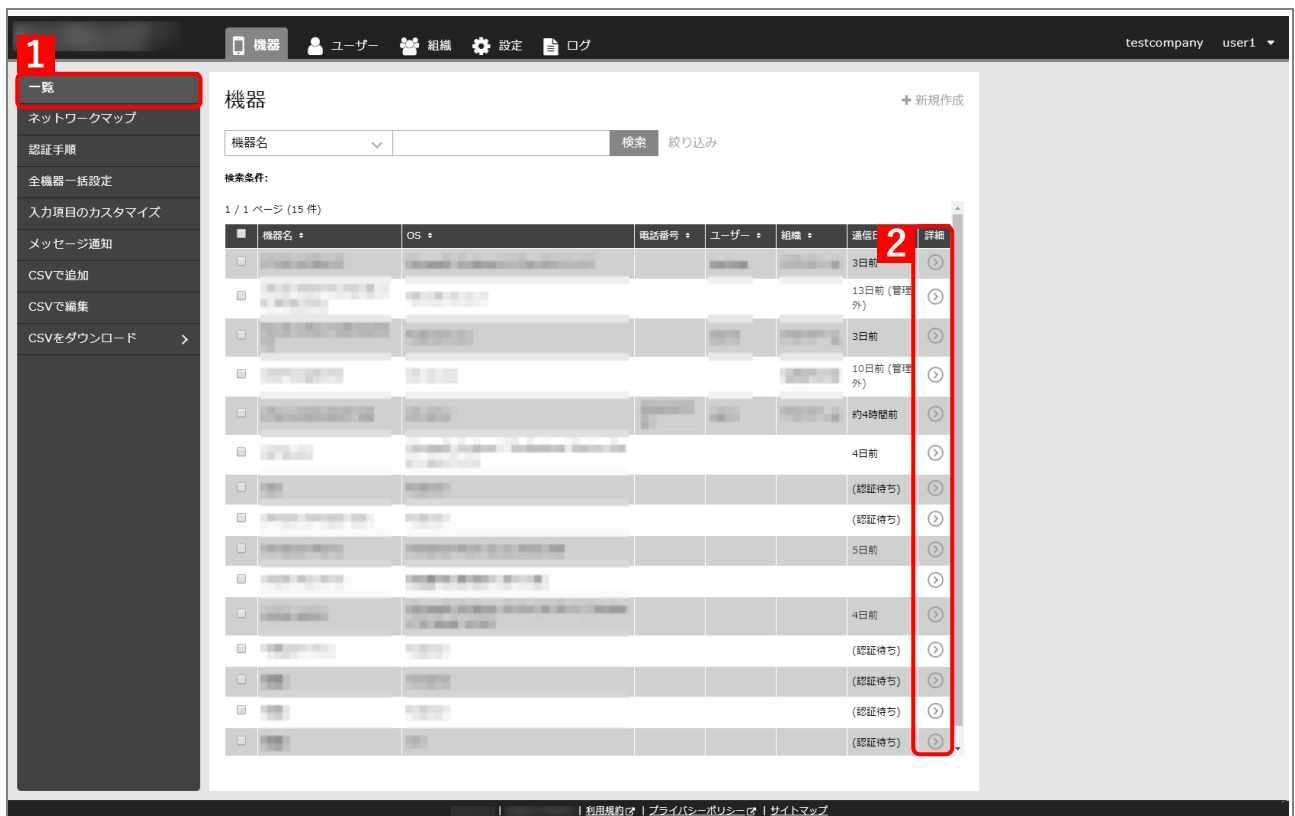
関連付けが終わったら、必要に応じて、以下の操作に進みます。

「ルール作成・設定を行う」46 ページ

◆ 機器に関連付ける手順

- 管理サイトで「機器」→「一覧」をクリックします。
- 対象の機器の「詳細」の をクリックします。

⇒ 機器の管理情報画面が表示されます。



【3】 「管理情報の編集」 をクリックします。

The screenshot displays the '機器' (Device) management page. The left sidebar contains navigation links: 一覧, ネットワークマップ, 認証手順, 全機器一括設定, 入力項目のカスタマイズ, メッセージ通知, CSVで追加, CSVで編集, and CSVをダウンロード. The main area shows a table of devices with columns for device name, OS, phone number, user, organization, last communication time, and details. The right sidebar contains user information and management actions. The '管理情報の編集' (Edit Management Information) button is highlighted with a red rectangle.

機器

検索条件: 機器名 OS 電話番号 ユーザー 組織 通信日時 詳細

1 / 1 ページ (15 件)

機器名	OS	電話番号	ユーザー	組織	通信日時	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	3日前	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	13日前 (管理外)	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	3日前	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	10日前 (管理外)	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	約4時間前	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	4日前	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	(認証待ち)	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	(認証待ち)	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	5日前	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	4日前	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	(認証待ち)	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	(認証待ち)	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	(認証待ち)	詳細
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	(認証待ち)	詳細

OS: Android 7.0

電話番号: (なし)

ユーザー: (なし)

組織: (なし)

管理情報の編集

設定

設定の割り当て

設定テンプレートの割り当て

他の設定を見る

操作

スクリーンロックパスワード変更

リモートロック

他の操作を見る

情報

ログ

エージェント

- 【4】 所属の「ユーザー」または「組織」のいずれかを選択し、リストボックスから紐付けるユーザーまたは組織を選択します。

✎ ユーザーおよび組織の登録方法は、以下を参照してください。

🔗 「ユーザーを登録する」25 ページ / 「組織を登録する」23 ページ

✎ (A) には機器グループの項目名が表示されます。機器グループを登録していない場合は表示されません。

- 【5】 「保存」をクリックします。

⇒ 設定が作成されます。

The screenshot shows the '機器' (Device) management page. The main area displays a table of devices with columns for device name, OS, phone number, user, organization, and last update time. The sidebar on the right, titled '管理情報' (Management Information), contains fields for device name, location (所属), and device group (機器カスタム項目A). Red boxes and numbers indicate the steps: 4 points to the location dropdown menu where 'ユーザー' (User) or '組織' (Organization) is selected; (A) points to the device group dropdown menu; 5 points to the '保存' (Save) button at the bottom of the sidebar.

機器名	OS	電話番号	ユーザー	組織	通信日時	詳細
...	3日前	...
...	13日前 (管理外)	...
...	3日前	...
...	10日前 (管理外)	...
...	約4時間前	...
...	4日前	...
...	(認証待ち)	...
...	(認証待ち)	...
...	5日前	...
...	4日前	...
...	(認証待ち)	...
...	(認証待ち)	...
...	(認証待ち)	...
...	(認証待ち)	...


2.6 ルールの作成・設定を行う

「事前準備」でリストアップしたルールをもとに、機器へ適用するルール（設定セット）を作成します。
作成した設定セットは、全機器一括設定で機器用のグループに適用したり、組織に適用できます。

例として、Android 端末で SD カードの使用を禁止するルールを機器のグループ「営業部」の「営業 1 課」に設定する方法をご紹介します。以下の流れで作成します。ほかの設定も基本的な設定の流れは同じです。


- 全機器一括設定で機器用のグループに適用する流れ

1. 設定セットの作成を行う
2. グループヘルールを設定する

 一括機器設定は定期同期のときに機器への設定が行われます。お急ぎの場合は、機器ごとに設定をし、同期を行ってください。

- 組織に適用する流れ

1. 設定セットの作成を行う
2. 組織ヘルールを設定する

 グループと組織へのルールの適用は、定期的な同期で設定が反映されます。

2.6.1 設定セットの作成を行う

ここでは、Android 端末で SD カードの使用を禁止する設定セットを作成します。

✂️ Android 機器の設定セットの作成については、以下を参照してください。

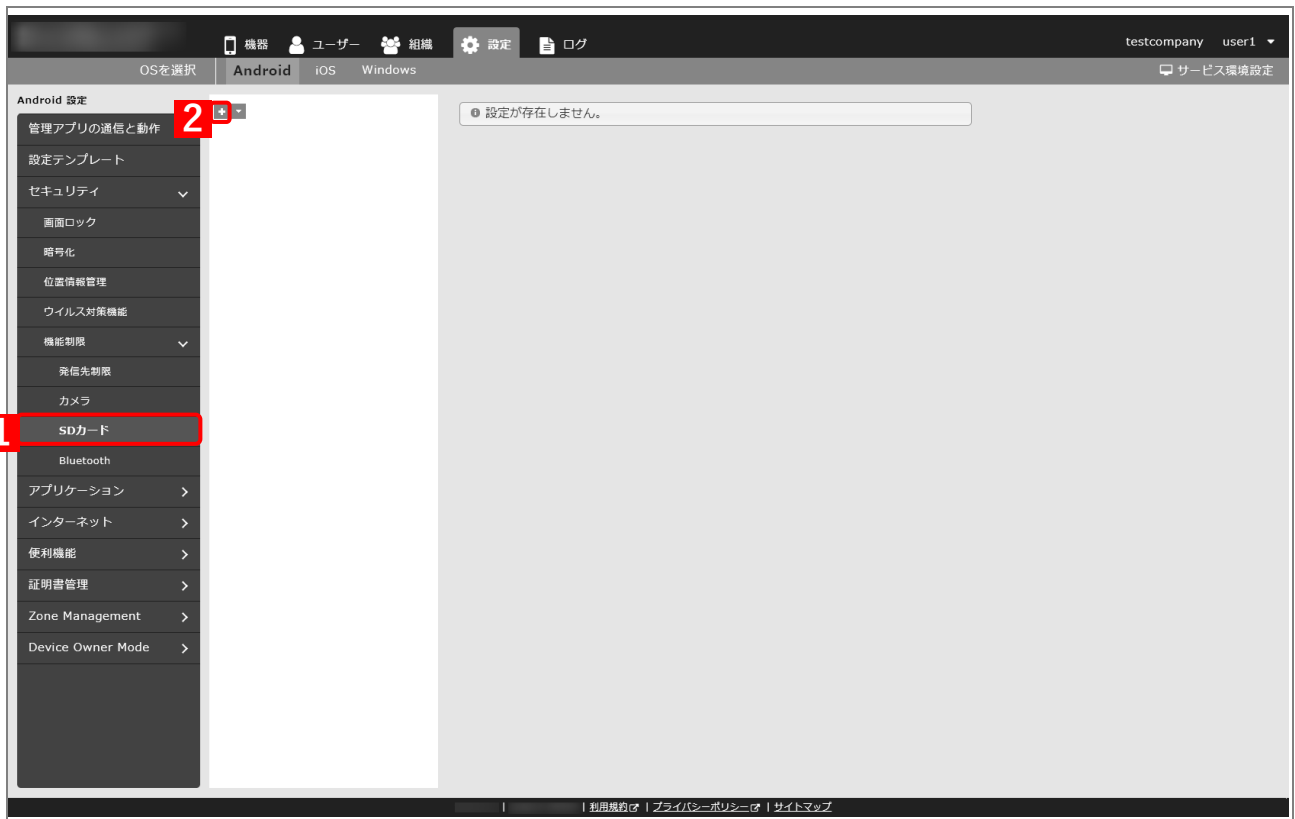
📖 『管理サイト リファレンス マニュアル』の「設定 - Android」

◆例) Android 端末の SD カードの使用禁止の設定セットの作成

【1】 管理サイトで [設定] → [Android] → [セキュリティ] → [機能制限] → [SD カード] をクリックします。

【2】 **+** をクリックします。

⇒ 新規作成画面が表示されます。

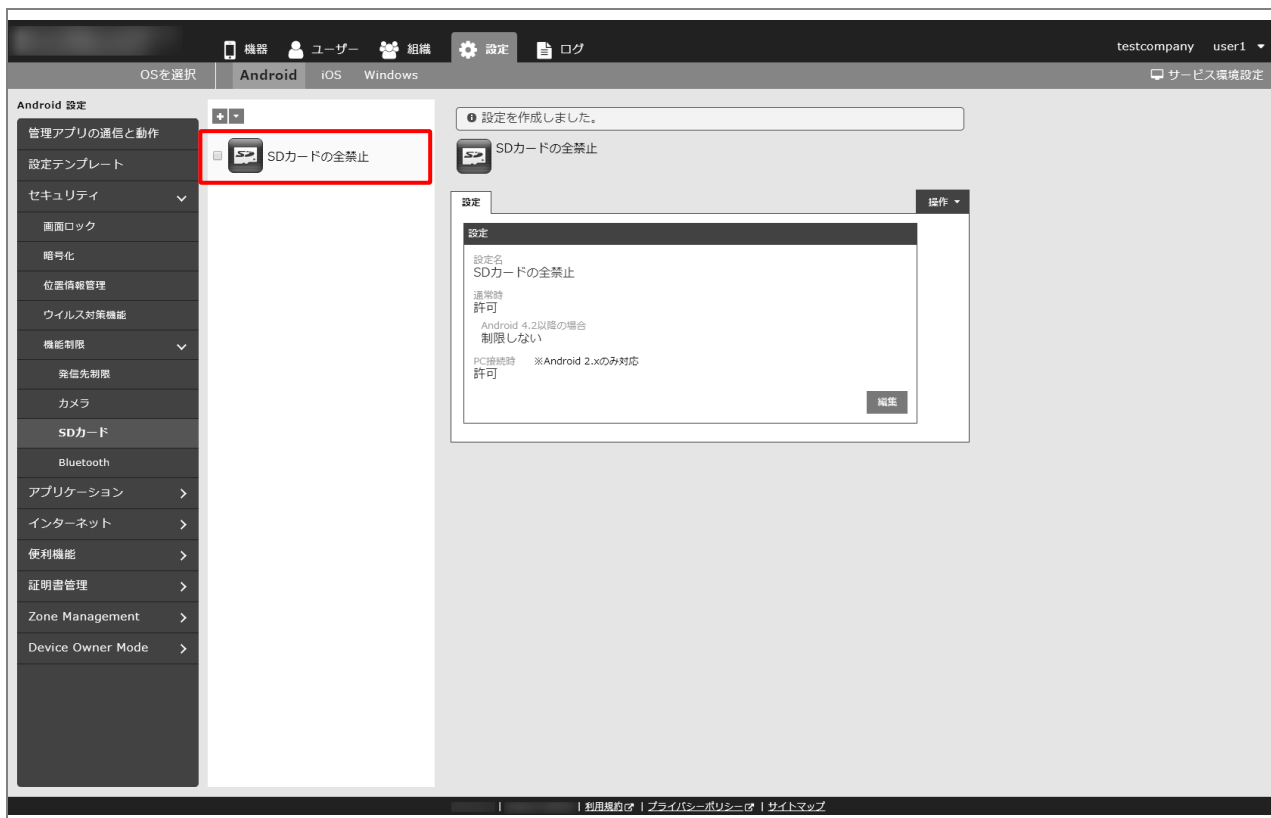


- 【3】「設定名」を入力します。
- 【4】「通常時」と「PC 接続時」で「禁止」を選択します。
- 【5】「保存」をクリックします。

⇒ 入力した設定名で、SD カードの設定セットが作成されます。




- 【6】 設定セットが作成されてることを確認します。



2.6.2 グループヘルールを適用する

「設定セットの作成を行う」で作成した設定セットをグループに適用する場合は、以下の手順に従い操作します。

 ここでは、SD カードの使用禁止の設定セットを、グループに適用する例を説明しますが、ほかの設定セットも同様の操作で適用できます。

◆例) SD カードの使用禁止の設定セットをグループに適用

[1] 管理サイトで「機器」→「全機器一括設定」をクリックします。

[2] ルールを適用するグループを一覧から選択します。

✎ここでは、「ユーザーの所属（部）」の「営業部」を対象にします。

✎「ユーザーの所属（部）」は、以下で登録した「所属（部）」の分類名に「ユーザーの」が付与された名前で表示されています。

📖「ユーザーグループを登録する」19 ページ

✎機器グループに適用する場合は、以下で登録した「機器用途」から対象のグループを選択してください。

📖「機器グループを登録する」21 ページ

[3] 「Android 設定」タブをクリックします。

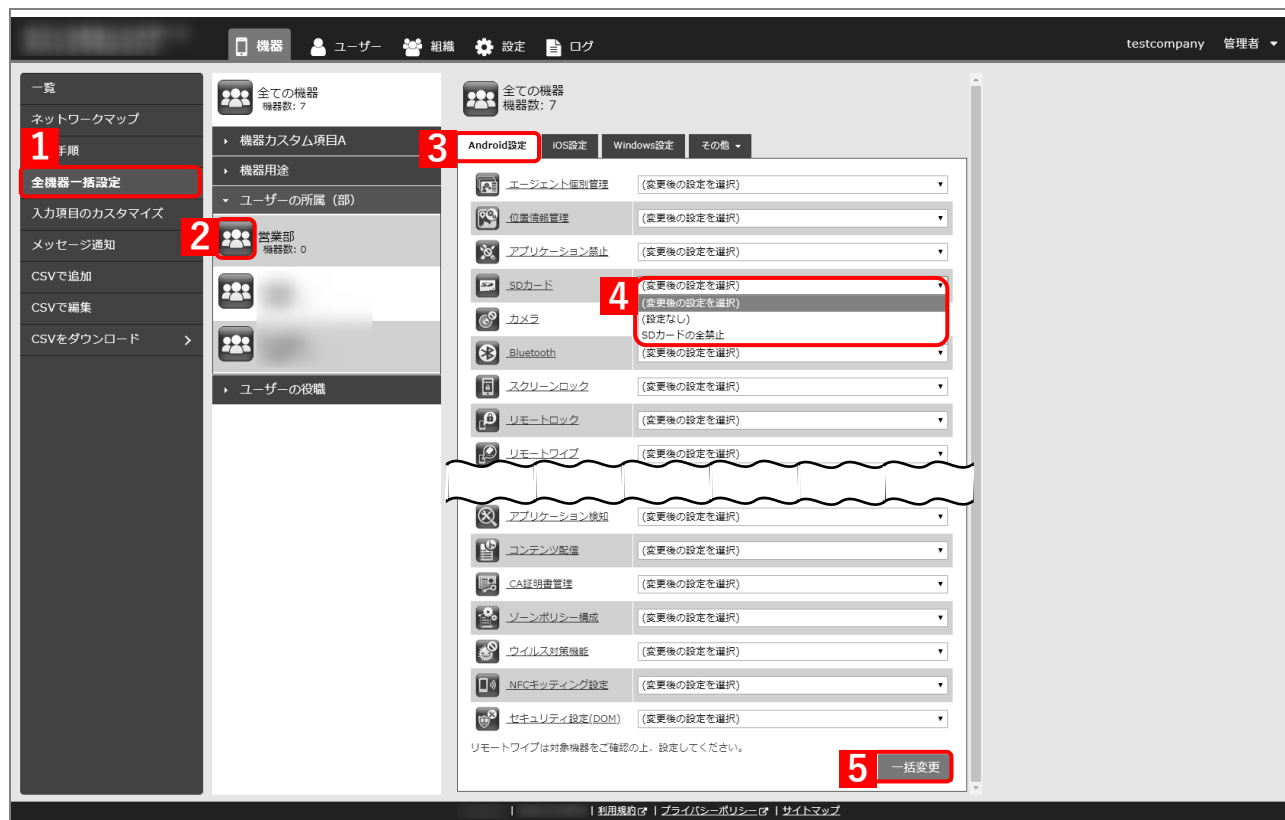
[4] 「SD カード」で適用する設定セットを選択します。

✎ここでは、以下で作成した「SD カードの全禁止」を選択します。

📖「設定セットの作成を行う」47 ページ

[5] 「一括変更」をクリックします。

⇒確認画面が表示されます。

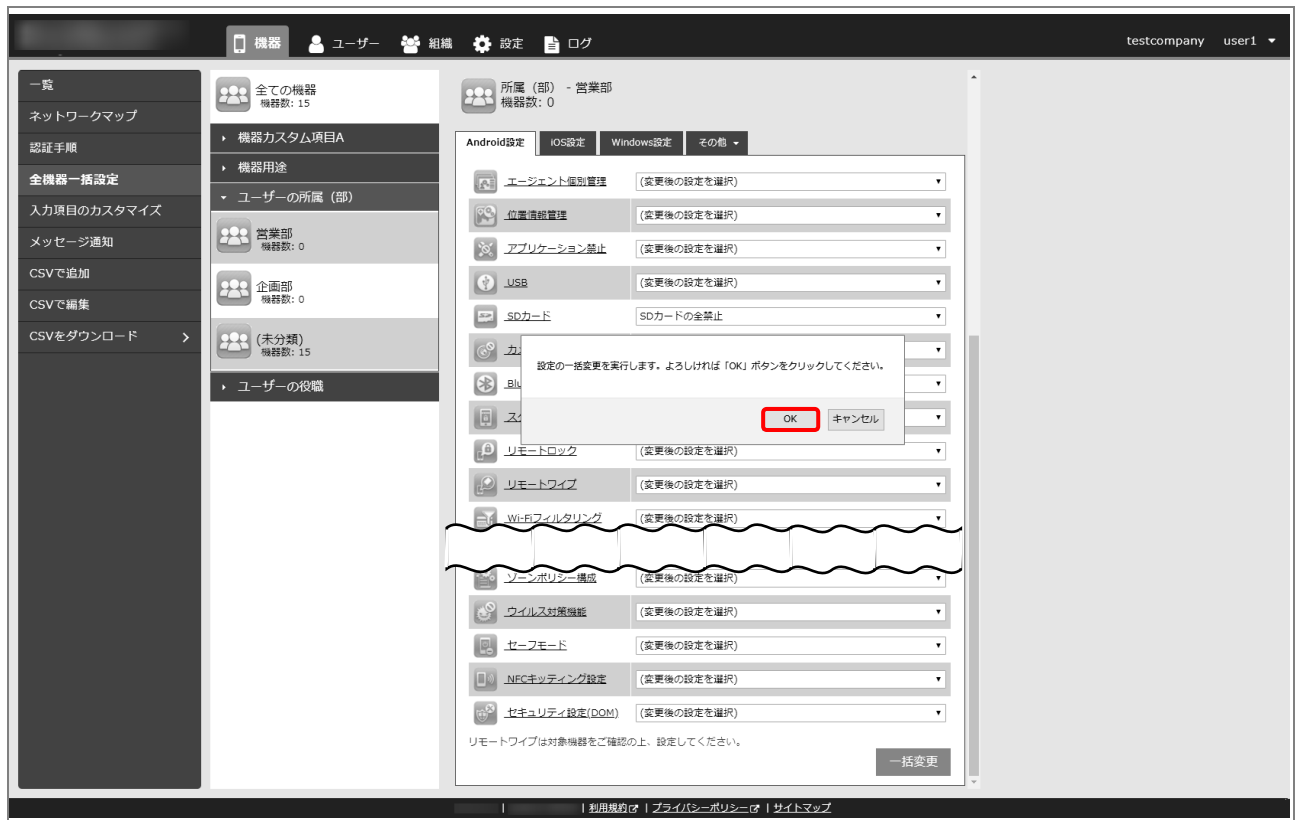


[6] [OK] をクリックします。

⇒「SD カードの全禁止」がユーザーグループの「営業部」に適用されます。

- ✎ この設定は、機器の一覧から、Android 機器の管理情報で所属をユーザーにして、選択したユーザーが「営業部」に所属している場合、その機器に対して適用されます。
適応対象が機器グループの場合は、Android 機器の管理情報で「機器用途」でグループを選択した場合、その機器に対して適用されます。

🔗 「ユーザー／組織／機器グループと各機器を関連付ける」43 ページ



2.6.3 組織ヘルールを設定する

「設定セットの作成を行う」で作成した設定セットを組織に適用する場合は、以下の手順に従って操作します。

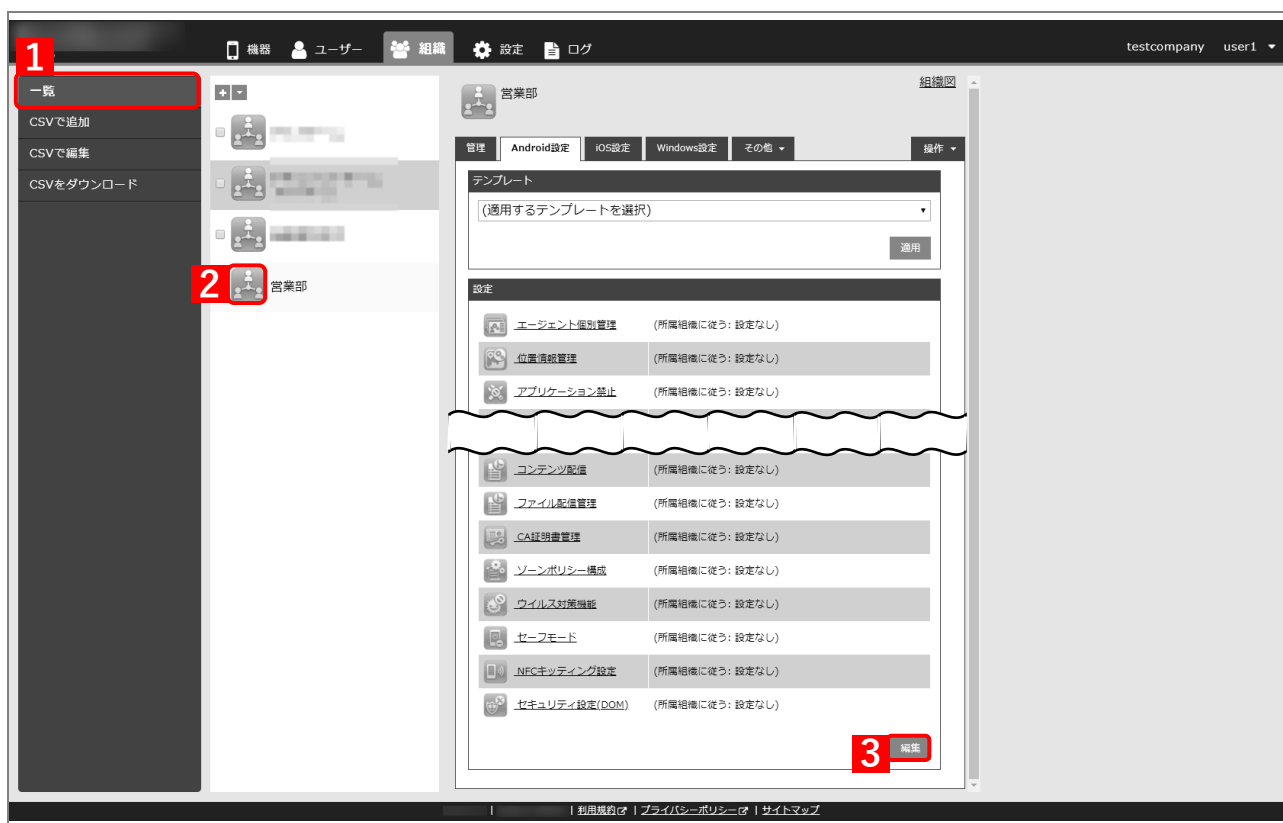
☑ここでは、SD カードの使用禁止の設定セットを組織に適用する例で説明しますが、ほかの設定セットも同様の操作で適用できます。

【1】 管理サイトで [組織] → [一覧] をクリックします。

【2】 ルールを適用する組織を一覧から選択します。

☑ここでは、「営業部」を対象にします。

【3】 「Android 設定」タブ → [編集] をクリックします。



【4】「SD カード」で適用する設定セットを選択します。

✎ ここでは、以下で作成した「SD カードの全禁止」を選択します。

📄 「設定セットの作成を行う」47 ページ

【5】「保存」をクリックします。

⇒ 「SD カードの全禁止」が「営業部」に適用されます。

✎ この設定は、機器の一覧から、Android 機器の管理情報で所属を組織にして「営業部」を選択した場合、その機器に対して適用されます。

📄 「ユーザー／組織／機器グループと各機器を関連付ける」43 ページ

