

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7月18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	3
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
管理サイト動作環境.....	4
本マニュアルの見かた.....	5
ご利用開始までのステップ	6
STEP0 事前準備.....	7
STEP1 機器管理の基本設定を行う.....	8
・ Android 端末の場合.....	8
・ iOS 端末の場合(※必須).....	9
・ Windows 機器の場合.....	11
STEP2 グループ/ユーザー/組織を登録する.....	12
・ ユーザーグループを登録する.....	12
・ 機器グループを登録する.....	13
・ 組織を登録する.....	14
・ ユーザーを登録する(※必須).....	15
・ 複数人のユーザーをまとめて登録する.....	16
STEP3 機器へアプリをインストールする(※必須).....	18
・ Android 端末の場合.....	18
・ iOS 端末の場合.....	20
・ Windows 機器の場合.....	23
STEP4 STEP2 で登録したユーザー、組織、機器グループと STEP3 で登録した機器を関連付ける.....	25
STEP5 ルールの作成・設定を行う.....	26
・ 設定セットの作成を行う.....	26
・ グループヘルールを設定する.....	26
・ 組織ヘルールを設定する.....	27

はじめに

本製品の概要、特徴、動作環境等について説明します。

オフィスまるごとサポートデバイスマネジメントとは.....	4
管理サイト動作環境.....	4
本マニュアルの見かた.....	5

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とは企業におけるスマートフォン、タブレット端末、パソコンの管理をサポートする IT サポートツールです。Android 端末、iPhone/iPad、Windows 機器にエージェントアプリをインストールし、端末紛失・盗難時のリモートロックや、業務端末の不正利用を行うアプリケーションの起動禁止、資産管理としての端末情報の一括管理をすべてウェブブラウザ上から簡単に行うことができ、面倒なセキュリティ対策や資産管理の対応負荷を解消するソリューションです。



初期設定を行えば、簡単に管理が始められます。本マニュアルでは以下の流れで説明を行います。

「ご利用開始までのステップ」6 ページを参照し初期設定を行った後、機器の管理・運用を始めてください。機能一覧は 7 ページを参照してください。

管理サイト動作環境

対応ブラウザ	Internet Explorer 9、Internet Explorer 10、Internet Explorer 11、Firefox、Google Chrome ※Firefox、Google Chrome は最新版のみ対応。 ※横 960 ピクセル以上の表示を推奨します。 ※Apple Push 証明書の登録および更新の際、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。
ネットワーク接続	インターネットへ接続可能なこと。 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) ができること。

※Android エージェント動作環境については、「Android ユーザーマニュアル」を、iPhone/iPad 動作環境については、「iOS ユーザーマニュアル」を、Windows 動作環境については、「Windows ユーザーマニュアル」を参照してください。

本マニュアルの見かた

- ・ ボタン名、リンク名、タブ名などは[]で表記します。
- ・ 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。
- ・ 本マニュアルはユーザー種別「管理者」用です。ユーザー種別「閲覧者」で管理サイトにログインすると新規作成、編集、削除等設定を変更する操作はできません。また、設定を変更するメニュー、ボタンも表示されません。

ご利用開始までのステップ

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。初期設定を終えたのち、機器の管理・運用を始めてください。

STEP0 事前準備.....	7
STEP1 機器管理の基本設定を行う	8
・ Android 端末の場合.....	8
・ iOS 端末の場合(※必須).....	9
・ Windows 機器の場合	11
STEP2 グループ/ユーザー/組織を登録する	12
・ ユーザーグループを登録する	12
・ 機器グループを登録する	13
・ 組織を登録する.....	14
・ ユーザーを登録する(※必須)	15
・ 複数人のユーザーをまとめて登録する	16
STEP3 機器へアプリをインストールする(※必須).....	18
・ Android 端末の場合.....	18
・ iOS 端末の場合	20
・ Windows 機器の場合	23
STEP4 STEP2 で登録したユーザー、組織、機器グループと STEP3 で登録した機器を関連付ける	25
STEP5 ルールの作成・設定を行う	26
・ 設定セットの作成を行う	26
・ グループヘルールを設定する	26
・ 組織ヘルールを設定する	27

STEP0 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をおこなうことができますが、これらの機能を使用するためには、各端末へルール(※)を設定する必要があります。

ルール(※)は各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する事ができます。

※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等)を意味します。

事前準備として、誰にどのようなルールを設定したいのか、グループ分けはどのようなグループを作成する必要があるのかを考えます。

例として、ユーザーの部署や役職ごとにわかる場合

1. グループ分けを考えます。

- ・端末のユーザー、部署名、役職名をリストアップします。

社員番号	名前	所属(部)	役職
0001	〇〇 〇〇	営業部	部長
0001	営業部	課長
0001	営業部	なし
0001	企画部	部長
		企画部	課長
		企画部	なし
以下略			

- ・この場合、グループは部ごと、役職ごとにわかることにします。

・部で2グループ：[営業部][企画部]、役職で3グループ：[部長][課長][役職なし]の合計5グループに分けます。実際のグループ作成方法は、「STEP2 グループ/ユーザーを登録する」12 ページを参照してください。

2. 使いたいルールをリスト化し、ルールをあてる対象のグループを考えます。

ルール	説明	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。	[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。	[役職なし]
発信先制限	発信先に制限をかけます。	[企画部]

全員にあてるルールは、その機能の「デフォルト」に設定します。

一部のグループのみにあてるルールは、グループを作成し、そのグループにのみルールをあてます。

グループ、ルールのリストアップができれば、STEP1 から実際の設定に入ります。

STEP1 機器管理の基本設定を行う

・Android 端末の場合

この設定は、PC 上の管理サイトから行います。

管理サーバーとの通信間隔や端末でのリモートロックの解除コード、パスワード設定、定期バックアップの設定等を行います。詳細は「管理サイトユーザーマニュアル」を参照してください。設定を行わない場合は、デフォルトのものが使用されます。デフォルト値は以下の通りです。デフォルト値を変更しない場合は、STEP2「グループ/ユーザーを登録する」12 ページへ進みます。

«メニュー画面⇒「Android」ボックス内[エージェント共通管理]をクリックして修正»

項目	デフォルト値	説明
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。
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することができます。
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。
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。
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。
Root 化状態検知	検知する	端末が root 化されている場合、検知するかどうかが設定します。

«メニュー画面⇒「Android」ボックス内[設定バックアップ]をクリックして修正»

項目	デフォルト値	説明
定期バックアップ	無効	定期バックアップの設定を行います。

・iOS 端末の場合(※必須)

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 を管理することはできません。以下の手順にしたがって、登録を行ってください。

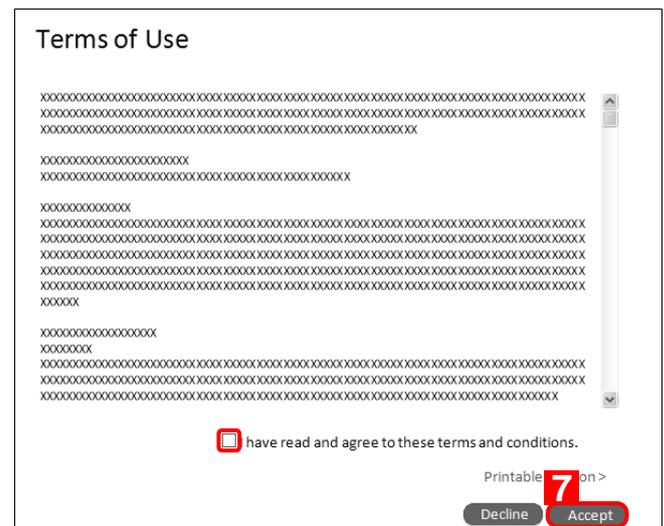
※Apple Push 証明書登録は導入時に1度登録すれば、1年間有効です。端末ごとに登録する必要はありません。また、Apple Push 証明書の取得には Apple ID が必要です。1年後の Apple Push 証明書更新時には、最初に Apple Push 証明書を登録した際の Apple ID が必要となります。Apple ID を忘れた場合や失効した場合は、Apple ID 及び Apple Push 証明書を新規で取得し直す必要があるため、端末の構成プロファイルの継続使用ができなくなり、導入済みのプロファイル、エージェントも再度インストールする必要があります。そのため、Apple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

- 1.メニュー画面⇒「iOS」ボックス内[Apple Push 証明書登録]をクリックします。
- 2.[編集]をクリックします。
- 3.[ダウンロード]をクリックし、任意の場所に保存します。
- 4.Apple Push Certificates Portal サイトを開きます。

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

ここから先 5.~10.は、Apple Push Certificates Portal サイトになります。画像はイメージです。

- 5.Apple ID と Apple ID のパスワードを入力し、[Sign in]をクリックします。
※Apple ID を持っていない場合は、Apple のサイトから取得してください。
- 6.[Create a Certificate]をクリックします。
- 7.規約を確認し、チェックボックスにチェックを入れ、[Accept]をクリックします。



- 8.[ファイルを選択]をクリックし、3.でダウンロードしたファイルを選択します。
- 9.[Upload]をクリックします。



- 10.証明書が作成されました。[Download]をクリックし、任意の場所に保存します。



- 11.管理サイトの[ファイルを選択]をクリックし、10.で取得した証明書ファイルを選択します。
- 12.「備考」欄には、任意の文字列を登録できます。以下のように証明書発行の際に使用された Apple ID を登録することが推奨されています。

Apple ID: xxxx@example.com 更新者:xxxx 更新日:2014/10/01

- 13.[保存]をクリックします。

- 14.Apple Push 証明書の登録が完了しました！



・Windows 機器の場合

この設定は、PC 上の管理サイトから行います。

管理サーバーとの通信間隔や、端末でのエージェント停止・ライセンス解除・アンインストール時のパスワードの設定を行います。詳細は「管理サイトユーザーマニュアル」を参照してください。設定を行わない場合は、デフォルトのものが使用されます。デフォルト値は以下の通りです。デフォルト値を変更しない場合は、STEP2「グループ/ユーザーを登録する」12 ページへ進みます。

«メニュー画面⇒「Windows」ボックス内[エージェント共通管理]をクリックして修正»

項目	デフォルト値	説明
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。
管理サーバーと通信できなかった場合	ロック	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可能です。
	ワイプ	管理サーバーと通信できなくなった場合に、端末をワイプする(初期化する)ことができます。
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。
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。
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。
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。

STEP2 グループ/ユーザー/組織を登録する

機器を使用するグループ/ユーザーの登録をおこないます。

グループとは、ユーザーや機器を一つにまとめ効率よく管理を行うためのものです。「部署」、「役職」といったように自由にグループを設定することができます。グループを作成し、ユーザーをそのグループに所属させることで、機器の設定等をグループごと一括で設定することが可能です。グループはユーザーグループ(役職、部署で分ける場合等)、機器グループ(機器の用途ごとに分けたい場合等)の2種類作成することが可能です。

- ・ユーザーグループ(役職、部署で分ける場合等)
- ・機器グループ(機器の用途ごとに分けたい場合等)

※グループ分けの考え方については、STEP0 に一例がございますので参照してください。

組織とは、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)を付与することができます。

・ユーザーグループを登録する

- 1.メニュー画面⇒「ユーザー」ボックス内[ユーザーカスタム項目]をクリックします。
- 2.[分類]タブの[+]をクリックし、作成画面を表示します。
- 3.分類名、グループを入力し、[保存]をクリックします。

※グループを増やすためには[+] (A)をクリックします。

※[×](B)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](C)をクリックし、設定します。



入力例) 会社内の部署、役職でわける場合

「所属(部) (営業部、企画部)、役職(部長、課長、なし)」

上記の場合、分類は2つ作ります。

- ・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

・ 機器グループを登録する

- 1.メニュー画面⇒「機器」ボックス内[機器カスタム項目]をクリックします。
- 2.[分類]タブの[+]をクリックし、作成画面を表示します。
- 3.項目名、グループを入力し、[保存]をクリックします。機器からグループの選択をできるようにする場合は、「機器から入力可」にチェックをいれます。

※機器グループを増やすためには[+] (A)をクリックします。

※[×](B)をクリックすると入力欄が削除されます。

分類 自由入力

新規作成

管理

管理情報 - 編集

項目名

グループ

グループ名

(+ボタンで追加: 300件まで)

オプション

機器から入力可

保存

入力例) 機器の用途ごとにわかる場合

「社内使用端末、社外持ち出し用端末」

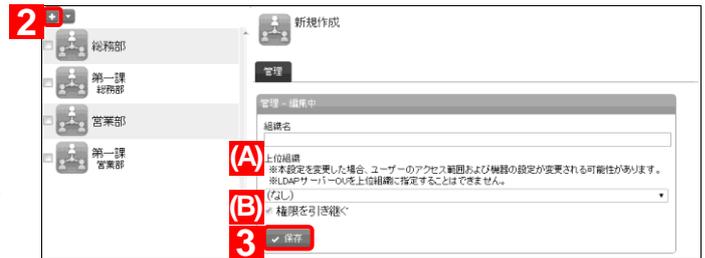
- ・ 項目名：機器用途
- ・ グループ名：社内使用、社外持ち出し用

・組織を登録する

- 1.メニュー画面⇒「組織」ボックス内[組織]をクリックします。
- 2.[+]をクリックし、作成画面を表示します。
- 3.必要事項を入力し、[保存]をクリックします。

※上位組織(A)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](B)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。追加権限についての詳細は、「管理サイトユーザーマニュアル」を参照してください。



・ユーザーを登録する(※必須)

機器を使用するユーザーの登録を行います。一人ずつ登録する場合は以下の手順に従って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、「複数人のユーザーをまとめて登録する」16 ページを参照してください。

- 1.メニュー画面⇒「ユーザー」ボックス内[ユーザー]をクリックします。
- 2.[+]をクリックし、作成画面を表示します。
- 3.必要事項を入力し[保存]をクリックします。

※入力項目の詳細は、「管理サイトユーザーマニュアル」を参照してください。

検索: ユーザー名
昇順: ユーザー名

admin
管理者
admin@example.com

新規作成

管理

管理情報 - 編集

名前

フリガナ

ユーザーID

メールアドレス

ユーザー種別

- 管理者 (全ての操作ができます)
- 操作
- 閲覧者 (変更操作ができません)
- ロック・ワイプ
- ログイン (個別に権限を設定)
- 一般 (ログインできません)

組織

機器認証制限

- 制限なし
- 制限あり 台
- 認証禁止

パスワード

パスワード(再入力)

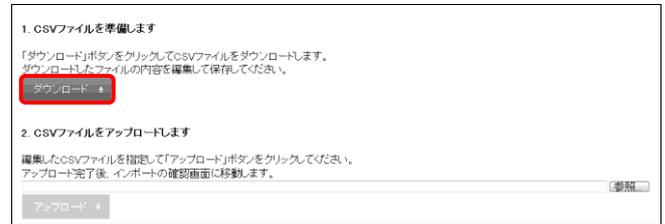
3 保存

・複数人のユーザーをまとめて登録する

複数人のユーザーをまとめて登録したい場合は、以下の手順にしたがってください。

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。

- 1.メニュー画面⇒「ユーザー」ボックス内[ユーザーインポート(新規)]をクリックします。
- 2.[ダウンロード]をクリックし、CSV ファイルをダウンロードします。



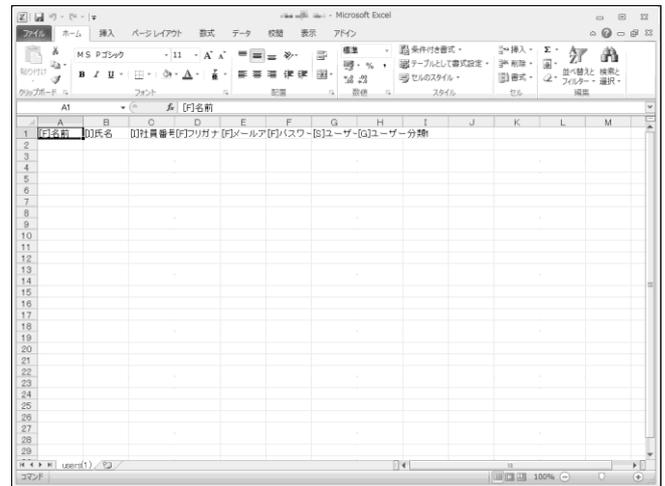
- 3.ファイルを開き、2 行目よりユーザー情報を入力してください。(ファイルは、メモ帳や EXCEL 等で表示してください。)

※縦列の数やタイトルは、分類機能により変わります。

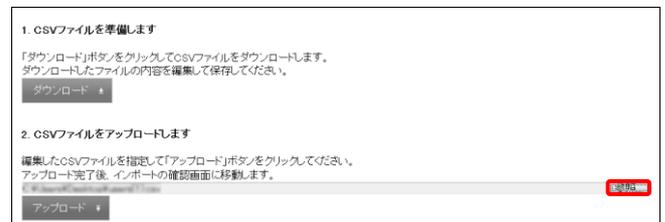
※「ユーザー種別」は「管理者」または「閲覧者」または「一般」を入力してください。ユーザー分類は、既に登録されているものを入力してください。

入力が終わったら、任意の場所に保存します。

※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(カンマ区切り)(* .csv)」を選択し、保存してください。

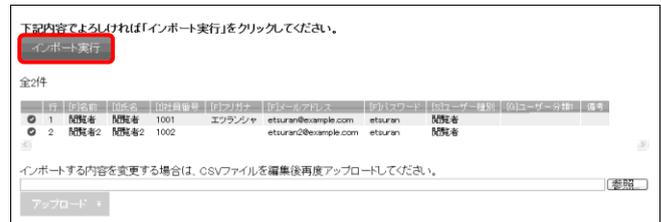


- 4.参照をクリックし、3.で保存したファイルを選択します。
- 5.[アップロード]をクリックします。



6.内容確認画面が表示されます。よろしければ[インポート実行]をクリックします。

※インポート内容に誤りがある場合は、備考欄にエラー内容が表示されます。 CSV ファイルを修正し、再度アップロードしてください。



情報が登録されました。



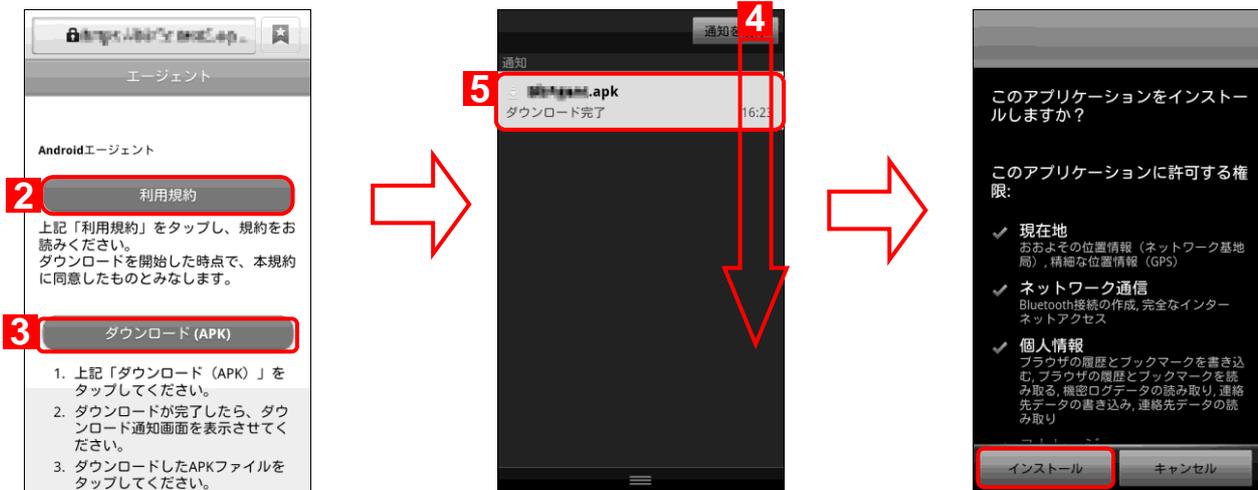
STEP3 機器へアプリをインストールする(※必須)

・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、チェックを入れた後インストールを行ってください。

※Android6.0 以降の場合は、一部操作方法が異なります。詳細は「Android ユーザーマニュアル」を参照してください。

※Android7.0 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、「Device Owner Mode 導入マニュアル」を参照してください。



- 1.ブラウザを起動し、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。
※AndroidOS バージョン 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

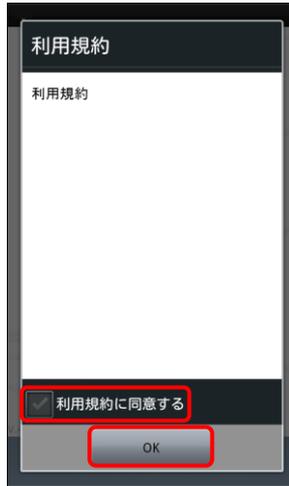
- 6.[インストール]をタップします。



- 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。

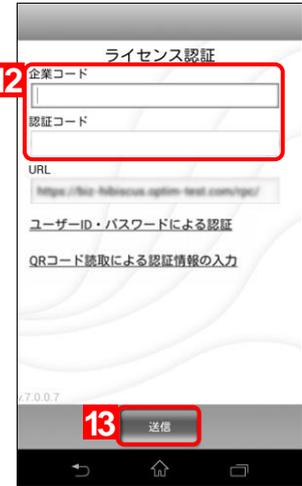
- 9.[ライセンス認証]をタップします。



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、上記のような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。

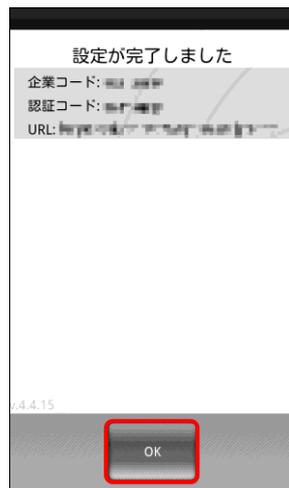
※ユーザーIDとパスワードによる認証の場合は[ユーザーID・パスワードによる認証]をタップします。

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



機器グループの登録を行うことができます。登録を行わない場合は[閉じる]をタップします。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「STEP4」25ページを参照してください。登録を行う場合は、画面に従って登録してください。

・ iOS 端末の場合

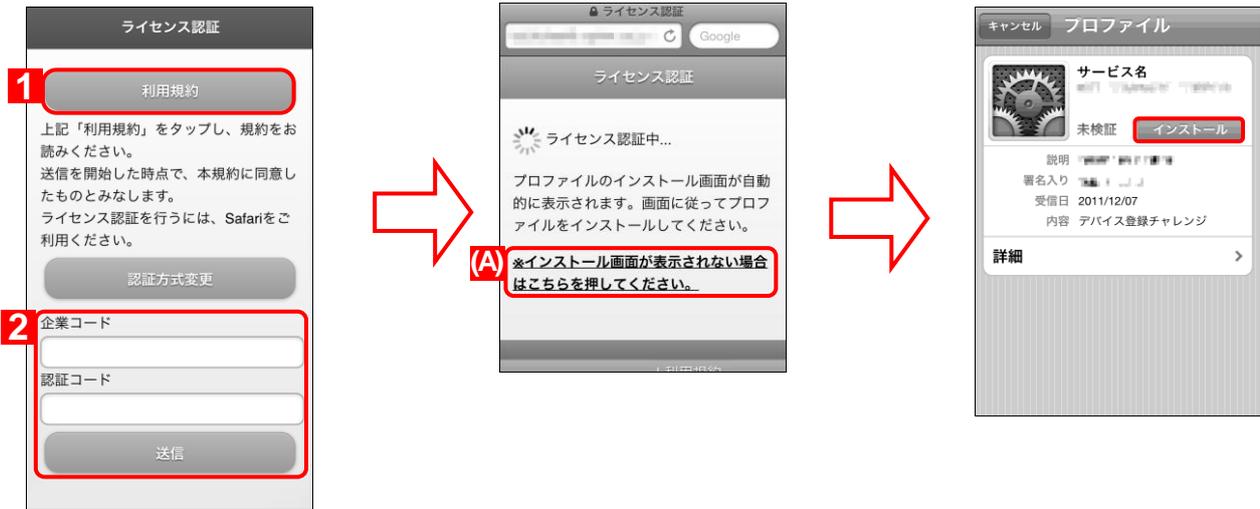
iOS 端末の場合は、以下、2点を行います。

1. プロファイルのインストール、ライセンス認証(※必須)
2. 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のみ)

Safari を起動し、ライセンス認証ページを開きます。

※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、「iOS ユーザーマニュアル」を参照してください。



- 1.[利用規約]をタップし、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。

- 2.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。

- 3.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。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。

- 4.[インストール]をタップします。

※表記上「未検証」とでていても「検証済み」とでていても、問題ございません。そのまま操作を続けてください。

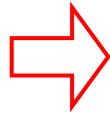


- 5.[インストール]をタップします。

※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。

- 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.内容を確認し、[インストール]をタップします。



8.しばらくお待ちください。

9.インストールが完了しました。**[完了]**をタップします。

10.ライセンス認証を行っています。



11.ライセンス認証が完了しました。**[次へ]**をタップします。

12.**[App Store からインストール]**をタップします。AppStore 画面へ移りません。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。

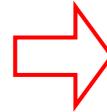
13.App Store からエージェントインストール完了後、ブラウザを開き、12.で開いていた画面を再度開きます。**[起動して認証]**をタップします。



14. 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。



15. [OK]をタップします。



16. [OK]をタップします。

※一度[OK]をタップすると、再度エージェントを起動する際には、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[OK]をタップしてください。[OK]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。



17. 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。

・ 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。

※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、機器を削除した後に、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。



1. ブラウザを起動し、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、[インストール] をクリックします。



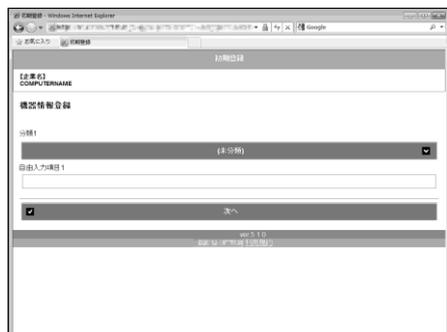
5. インストールしています。しばらくお待ちください。

6. インストールが完了しました。[完了] をクリックします。

7. 企業コード、認証コードを入力し、[OK] をクリックします。これでライセンス認証は完了です。

※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。]を選択します。



ライセンス認証完了後、左記のブラウザが表示されます。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]より、再度、登録を行うことができます。詳細は、「Windows ユーザーマニュアル」を参照してください。また、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「STEP4」25 ページを参照してください。登録を行う場合は、画面に従って登録してください。

STEP4 STEP2 で登録したユーザー、組織、機器グループと STEP3 で登録した機器を関連付ける

STEP2 で登録したユーザー、組織、機器グループと STEP3 で登録した機器を関連付けます。以下の手順に従ってください。

- 1.メニュー画面⇒「機器」ボックス内[機器]をクリックし、機器画面を表示します。
- 2.関連付けをする機器を選択します。
- 3.[編集]をクリックし、編集画面を表示します。



- 4.プルダウンよりユーザーまたは組織と、機器グループを選択します。

※ユーザーの登録方法は、STEP2の「ユーザーを登録する」15ページを参照してください。

※(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。



STEP5 ルールの作成・設定を行う

STEP0 でリストアップしたルールをもとに、ルールの作成を行います。

一例として、ルール「SD カード禁止」をグループ「営業部」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。他の設定も基本的な設定の流れは同じです。

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にて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。

ルール「SD カード禁止」を組織へ設定する場合は、以下の流れで作成します。

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。

・設定セットの作成を行う

- 1.メニュー画面⇒「Android-使用制限」ボックス内 [SD カード]をクリックします。
- 2.[+]をクリックし、作成画面を表示します。
- 3.設定名を入力し、通常時も PC 接続時も[禁止]を選択し、[保存]をクリックします。



・グループヘルールを設定する

- 1.メニュー画面⇒「機器」ボックス内[一括機器設定]をクリックします。
- 2.[営業部]を選択します。
- 3.[Android 設定]の「SD カード」より、「設定セットの作成を行う」で作成した設定名を選択します。
- 4.[一括変更]をクリックします。



・組織ヘルールを設定する

- 1.メニュー画面⇒「機器」ボックス内[組織]をクリックします。
- 2.設定を行う組織を選択します。
- 3.該当の OS の[設定]タブの「SD カード」より、「設定セットの作成を行う」で作成した設定名を選択します。
- 4.[保存]をクリックします。

