KDDI Smart Mobile Safety Manager

クイックスタートマニュアル

最終更新日　2015 年 9 月 24 日
Document ver.1.13

変更履歴

日付	Document ver.	変更箇所	変更内容
2013/02/08	1.00	-	新規作成
2013/02/27	1.01	STEP5	急ぎの場合は機器ごとの設定を行っていただくよう追記
2013/04/15	1.02	管理サイト動作環境	対応ブラウザに Internet Explorer 10 を追記。
		機能一覧	機能を追加(MDM 専用ブラウザ) iOS エージェントインストールが必要なものについて注釈を追記
		STEP1:iOS の場合	エージェントインストールが必要な機能について、機能をすべて記載。
2013/06/19	1.03	KDDI Smart Mobile Safety Manager とは	Windows について追加
		管理サイト動作環境	注釈に Windows エージェントマニュアルについて追記
		STEP1:Windows の場合	新規追加
		STEP3:Windows の場合	新規追加
		機能一覧	Windows 機能について追加
2013/07/05	1.04	機能一覧	フォーマット差し替え
2013/08/20	1.05	STEP1:Windows の場合	ライセンス認証オプションを追加
		STEP5:ルールの作成・設定を行う	画像差し替え
2013/10/09	1.06	STEP0	組織登録についての参照ページを追加
		STEP2	・画像差し替え ・「組織を登録する」を新規追加 ・タイトルに「組織」を追加 ・「ユーザーグループを登録する」に権限ボタンについての注釈を追加
		STEP3：iOS の場合	エージェント認証のフローを変更
		STEP4	・画像差し替え ・タイトルと説明文に「組織」を追加
		STEP5	「組織へルールを設定する」を新規追加
		こんな時は・・・: ・資産管理を行いたい ・役職ごと、端末の用途ごとで機器のグルーピングを行いたい ・アプリがインストールされたか確認したい	画像差し替え

		こんな時は・・・: ・端末やユーザーに所属する組織を登録したい ・管理サイトの閲覧のみを行えるユーザーを作成したい ・ユーザーが行える操作を追加したい ・組織を登録し、組織ごとに設定を行いたい	新規追加
2014/01/20	1.07	STEP5	「ルールの作成」と「対象機器に設定を反映する」を STEP 分割
		STEP6	「対象機器にルールを反映する」を追加
		こんな時は・・・	管理サイトマニュアルの参照箇所を追加
2014/02/20	1.08	機能一覧	機能を追加
2014/03/17	1.09	全体	リンクを修正
2014/04/07	1.10	機能一覧	Windows XP の記載を削除
2014/07/07	1.11	管理サイト動作環境	対応ブラウザーを追加
2015/2/16	1.12	全体	「STEP2　グループ/ユーザー/組織を登録する」を「こんな時は・・・」のセクションに移動。
		STEP2 機器へアプリをインストールする(※必須)	ポータルに関する文章を削除。
		機能一覧	ポータルに関する文章を削除
		こんな時は・・・	端末の位置情報に関する文章を追加
		STEP1 機器管理の基本設定を行う ・iOS の場合(※必須)	「iOS ID」を「Apple Push 証明書」で置換。備考欄、メール通知の説明を追加。
2015/3/2		STEP2　機器へアプリをインストールする（※必須）	DEP 設定とポータルの挙動に関する記述において追加。
2015/4/16	1.13	機能一覧	表を刷新
2015/5/15		全体	「設定ポリシー」を「設定テンプレート」に更新。
		組織単位にルールを作成する	現在のメニューの仕様に合わせて変更（「機器」ボックス内[組織]⇒「組織」ボックス内[組織]）
2015/6/23		STEP2 機器へアプリをインストールする(※必須)	iOS セクションのレイアウト修正、手順⑭のキャプチャに赤枠と項番追加。
2015/9/24		STEP2 機器へアプリをインストールする(※必須)	「Windows の場合」に同一の MAC アドレス重複時の注意点を追加。
		STEP2 機器へアプリをインストールする(※必須)	「ユーザーID・パスワードによる認証」オプションの表記を追加。
		こんな時は・・・	「ライセンス認証に失敗したら・・・」のセクションを追加。
		STEP1 機器管理の基本設定を行う	「Mac の場合」を追加。

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。

KDDI Smart Mobile Safety Manager とは

KDDI Smart Mobile Safety Manager 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ー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。本マニュアルでは下記の流れで説明を行います。
「ご利用開始までのステップ」9 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。よく利用する機能については、「こんな時は・・・」33 ページを参照してください。機能一覧は 62 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 8、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 エージェント ユーザーマニュアル」を、iPhone/iPad 動作環境については、「iPhone/iPad 向け ユーザーマニュアル」を、Windows 動作環境については、「Windows エージェントユーザーマニュアル」をご参照ください。

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

KDDI Smart Mobile Safety Manager を使用して、Android 端末、iPhone/iPad、Windows 機器等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

KDDI Smart Mobile Safety Manager 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。グループとルールの設定については 49 ページ「こんな時は・・・」の「【グループ/ユーザー/組織を登録する】」を参照してください。

STEP1 機器管理の基本設定を行う

・Android 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方法、パスワード設定、自動バックアップの設定等を行います。詳細は「管理サイトマニュアル」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「機器へアプリをインストールする(※必須)」18 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。
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	リモートロックの解除方法の設定を行います。
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
自動バックアップ	無効	自動バックアップの設定を行います。

・iOS の場合(※必須)

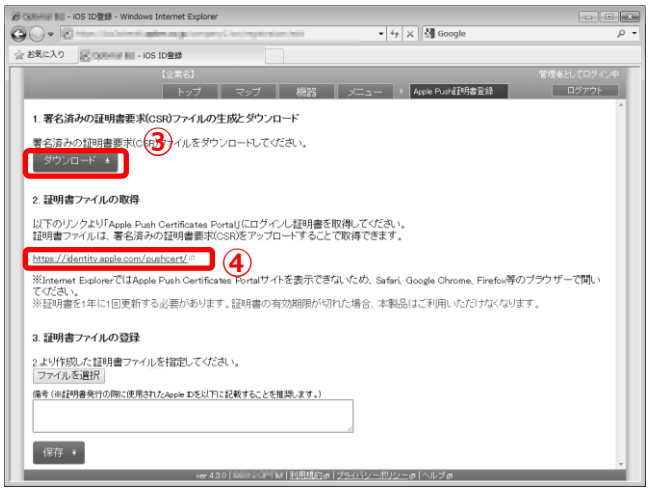
iPhone/iPad を管理するには、Apple Push 証明書を登録する必要があります。この登録を行わないと、iPhone/iPad を管理することはできません。下記手順にしたがって、登録を行ってください。

※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。また管理サイトの「管理」⇒「通知設定」から Apple Push 証明書の有効期限の通知メール設定を行うことができます。「メール送信先」で「管理者」と「機器のユーザー」に通知を送るように設定を行えますが、「管理者」と「機器のユーザー」に該当するユーザーにメールアドレスが登録されていない場合があります。その場合は「メール送信先(カスタム)」から担当者のメールアドレスを登録してください（詳しくは「管理サイトマニュアル」の「通知設定」を参照してください）。

※「ログメール通知」オプションの「Apple Push 証明書有効期限」のチェックボックスはデフォルトで有効です。

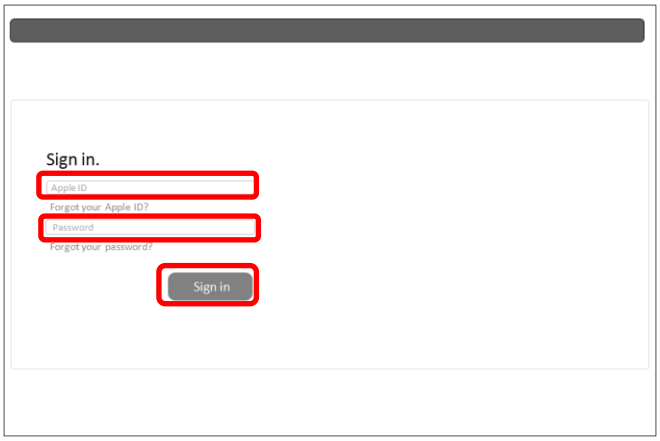
①メニュー画面⇒「iOS/Mac OS」ボックス内[Apple Push 証明書登録]をクリックします。
②[編集]をクリックします。
③[ダウンロード]をクリックし、任意の場所に保存します。
④Apple Push Certificates Portal サイトを開きます。

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

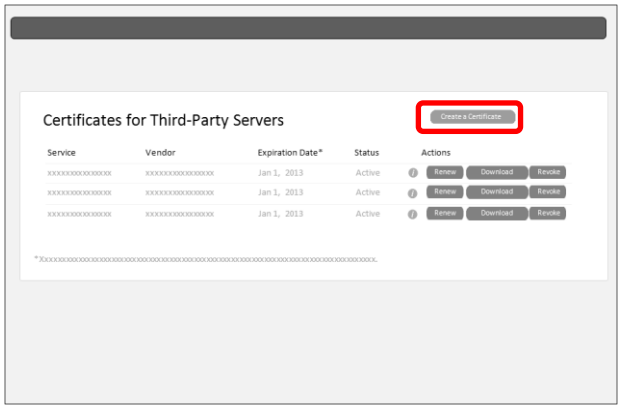


ここから先⑤~⑩は、Apple Push Certificates Portal サイトになります。画像はイメージです。
⑤Apple ID と Apple ID のパスワードを入力し、[Sign in]をクリックします。

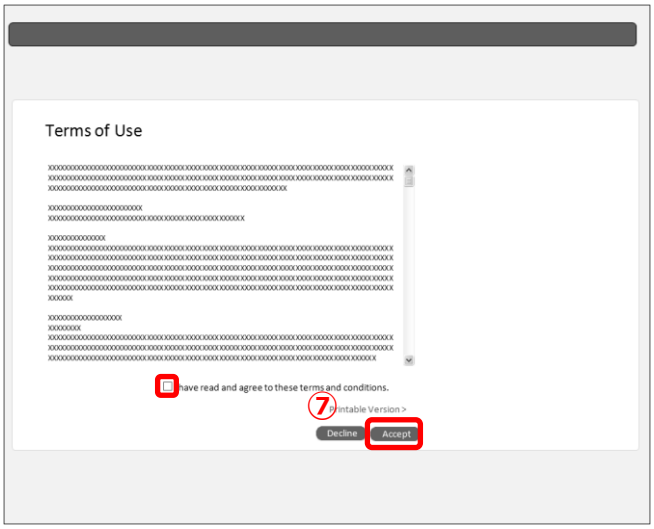
※Apple ID を持っていない場合は、Apple のサイトから取得してください。



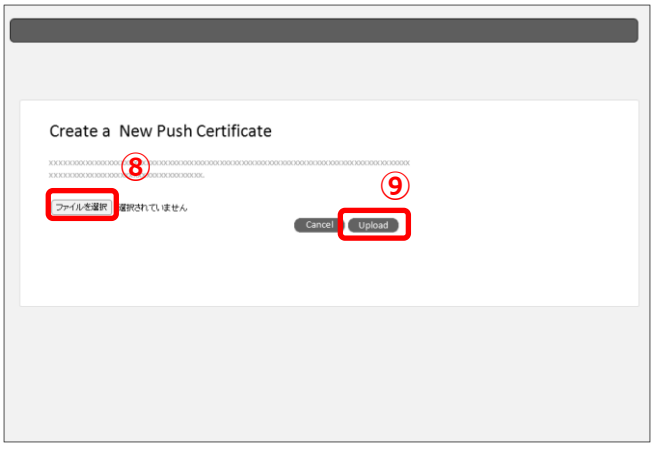
⑥[Create a Certificate]をクリックします。



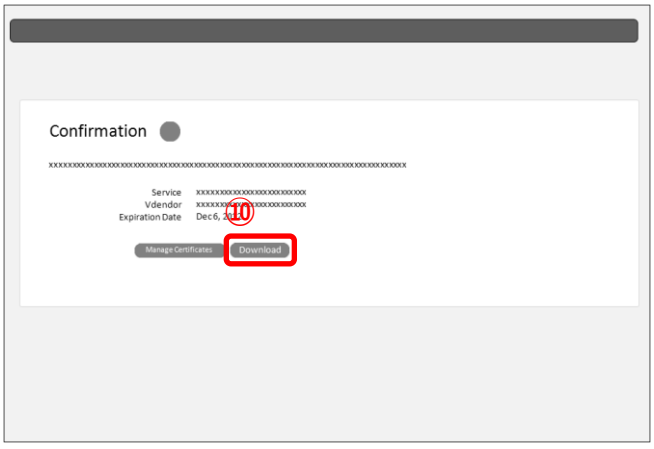
⑦規約を確認し、チェックボックスにチェックを入れ、[Accept]をクリックします。



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。

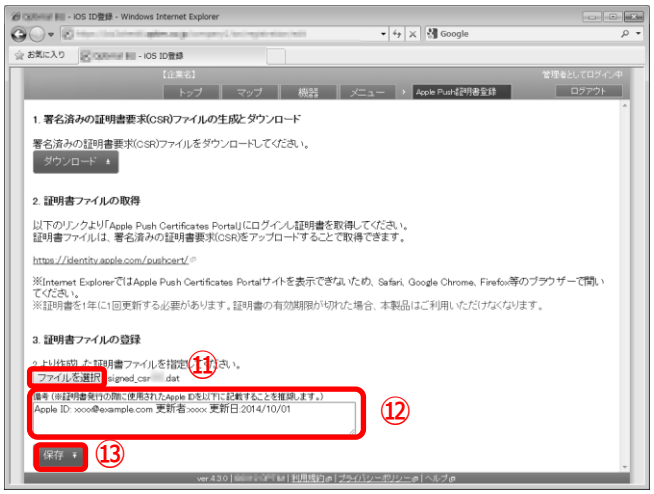


⑪管理サイトの[参照]をクリックし、⑩で取得した証明書ファイルを選択します。

⑫「備考」欄には、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[登録]をクリックします。



⑬Apple Push 証明書の登録が完了しました！

・Windows 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「機器へアプリをインストールする(※必須)」18 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。
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。

・Mac の場合

下記の手順に従ってライセンス認証(プロファイルのインストール)を行ってください。
※管理サイトの認証制御設定で管理者が登録した機器のみ認証する設定になっている場合は、ライセンス認証前に、管理者に端末を事前に登録していただく必要があります。詳細は管理者にお問い合わせください。
※Mac では構成プロファイルで基本設定を行うので、STEP2 のアプリのインストールは必要ありません。

①ブラウザを起動し、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。

②[利用規約]をクリックし、規約を確認します。

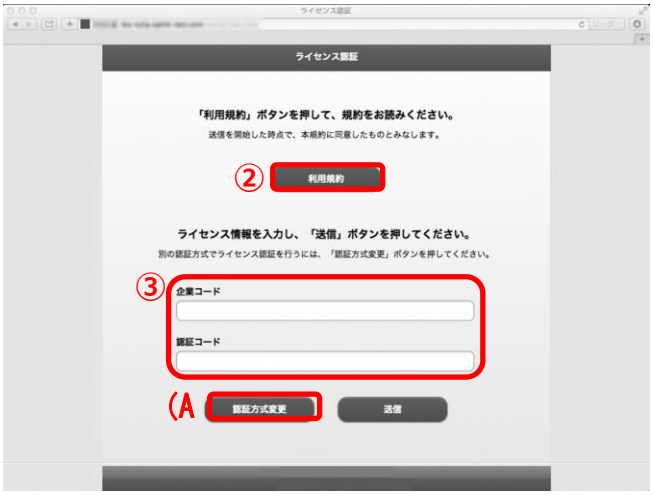
※送信を開始した時点で、本規約に同意したものとみなします。

③企業コード、認証コードを入力し、[送信]をクリックします。

※使用状況によっては「企業コード」は表示されない場合があります。

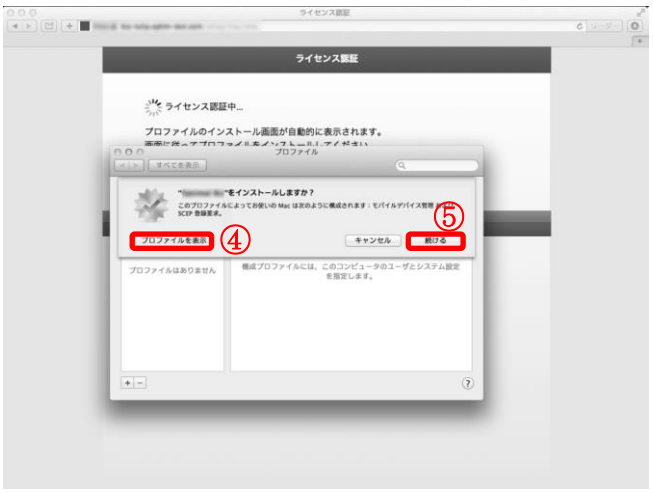
※ユーザーID またはメールアドレス、パスワードが表示されている場合は、[認証方式変更](A)をクリックします。

※ユーザーID とパスワードによる認証の場合は Mac 向けユーザーマニュアルを参照して下さい。



④プロファイルの詳細を表示する場合は[プロファイルを表示](A)をクリックします。

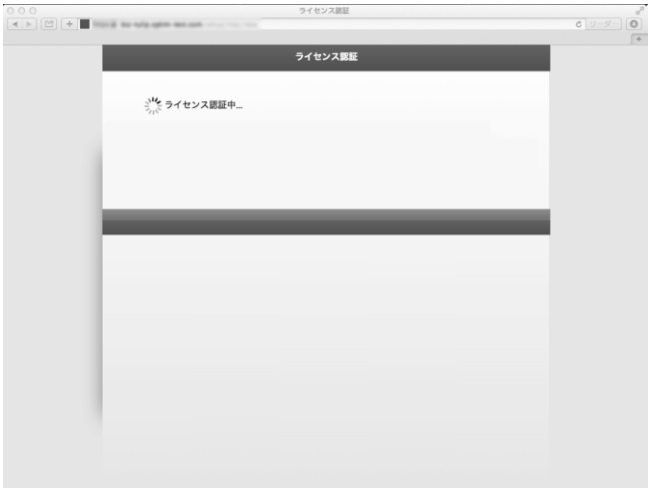
⑤[続ける](B)をクリックします。



⑥作成者を検証できない場合、確認画面が表示されます。[インストール]をクリックします。

⑦システム環境設定によりパスワードの入力を求められます。パスワードを記入して[OK]をクリックします。

⑧インストールをしています。しばらくお待ちください。



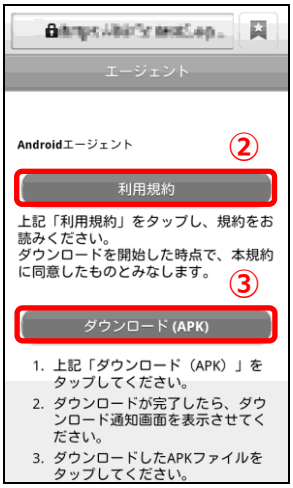
⑨ライセンス認証が完了しました。

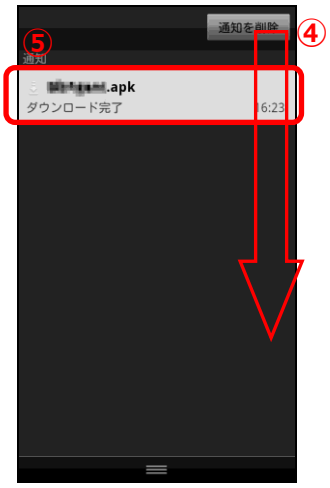
⑩Dock にポータルのアイコンが表示されていることを確認します。

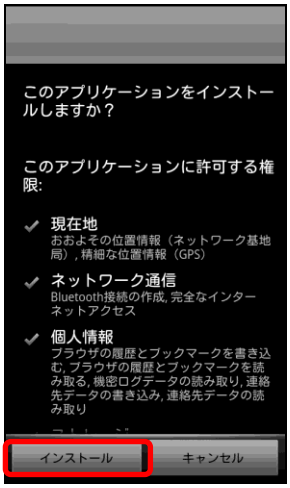
STEP2 機器へアプリをインストールする(※必須)

・Android の場合

Android の場合は、Andorid 端末へエージェントアプリをインストールし、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。



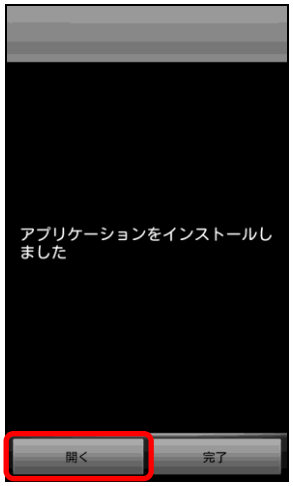




①ブラウザを起動し、エージェントアプリのダウンロードページを表示します。
※エージェントアプリダウンロードのアドレスは管理者またはオペレーターにお問い合わせください。
②[利用規約]をタップし、利用規約を確認します。
③[ダウンロード(APK)]をタップします。

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

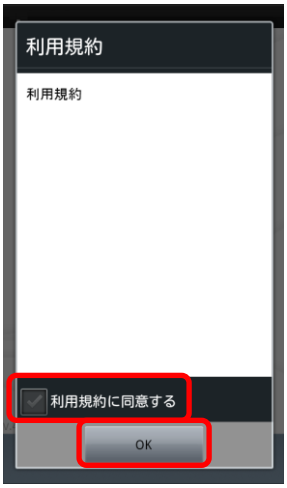
⑥[インストール]をタップします。



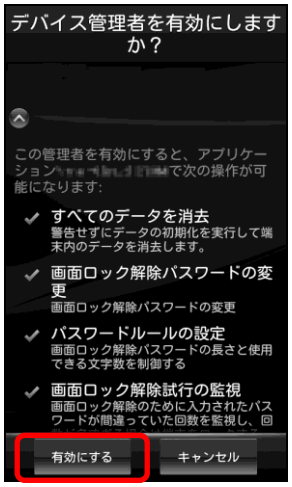
⑦インストールしています。しばらくお待ちください。

⑧インストールが完了しました。[開く]をタップします。

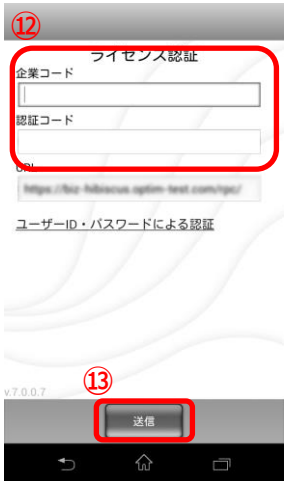
⑨[ライセンス認証]をタップします。



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。



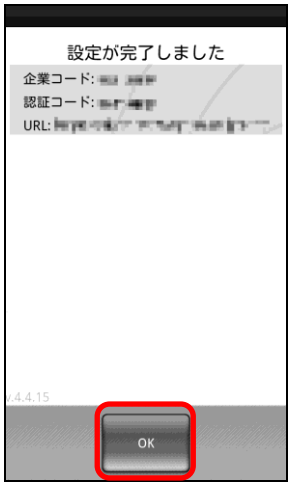
⑫企業コード、認証コードを入力します。

※ユーザーID とパスワードによる認証の場合は Android エージェント ユーザーマニュアルを参照して下さい。

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。



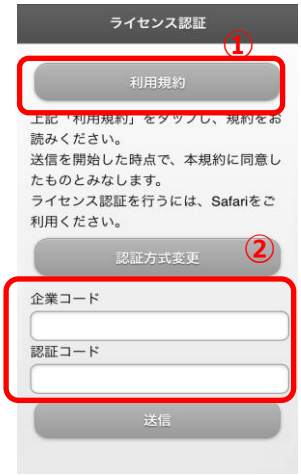
⑮設定が完了しました。[OK]をタップします

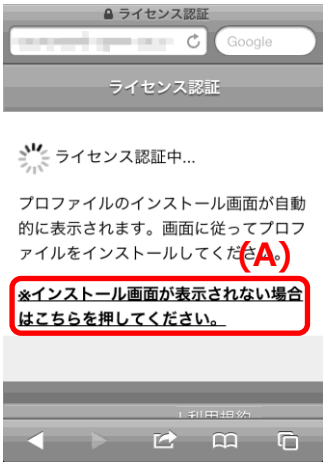
ユーザー登録、機器グループの登録を行うことができます。登録を行わない場合は[閉じる]をタップします。登録は管理サイトからも行えます。管理サイトからの登録方法は「STEP3」26 ページを参照してください。登録を行う場合は、画面に従って登録してください。

・iOS の場合

iOS の場合は、下記、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。
※本章では認証先の URL を選択し、手動で認証を行います。ポータル機能のエージェント自動認証機能を使用する場合は、「iPhone/iPad 向けユーザーマニュアル」を参照してください。





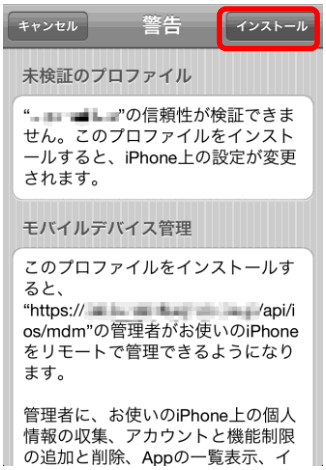
①[利用規約]をタップし、規約を確認します。
※送信を開始した時点で、本規約に同意したものとみなします。
②企業コード、認証コードを入力し、[送信]をタップします。
※企業コード、認証コードは管理者にお問い合わせください。
※ユーザーID とパスワードによる認証の場合は iPhone/iPad 向けユーザーマニュアルを参照して下さい。

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。

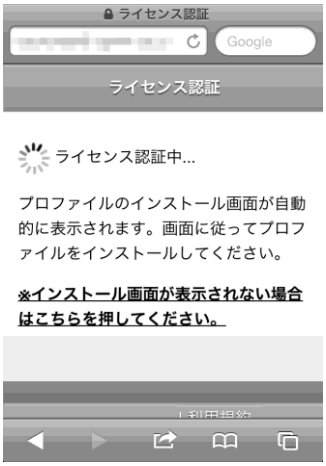
⑥インストールをしています。しばらくお待ちください。



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。

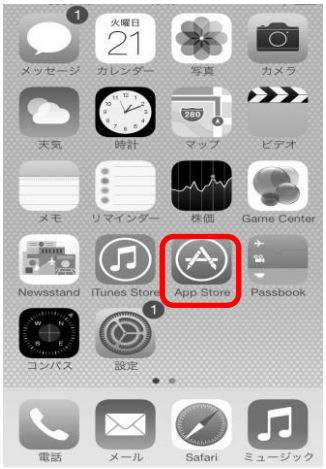
⑨インストールが完了しました。[完了]をタップします。



⑩ライセンス認証を行っています。

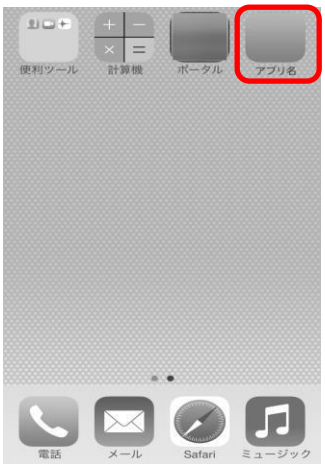
⑪ライセンス認証が完了しました。ホームボタンをタップしてホーム画面に戻ります。

※ポータル機能のエージェント自動認証機能を使用する場合は、「次へ」が表示されます。詳細は「iPhone/iPad向けユーザーマニュアル」を参照してください。



⑫[App Store] から「KDDI Smart Mobile Safety Manager」(エージェント)をインストールします。

※手順は App Store のインストール手順に従ってください。

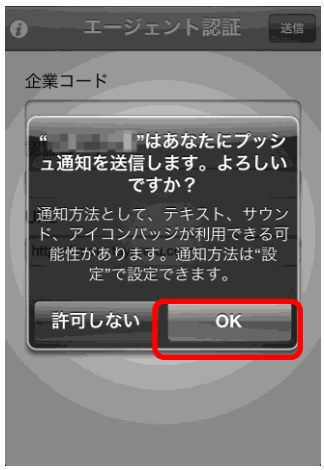


⑬エージェントがインストールされました。
エージェントアイコン(KDDI Safety Manager)をタップし、エージェントを起動します。

⑭企業コード、アクティベーションコードを入力します。
URL 入力欄(A)をタップすると、URL 選択画面(B)が表示されますので、該当のサービスを選択し、[完了](C)をタップします。

⑮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。

⑯[OK]をタップします。



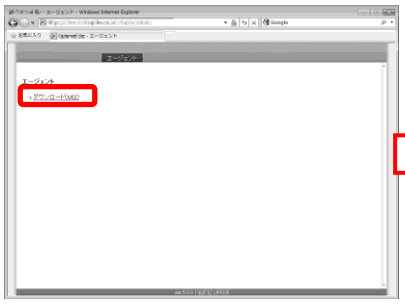
[OK]をタップします。
※一度[OK]をタップすると、再度エージェントを起動する際には、ポップアップ画面は表示されません。

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 の場合

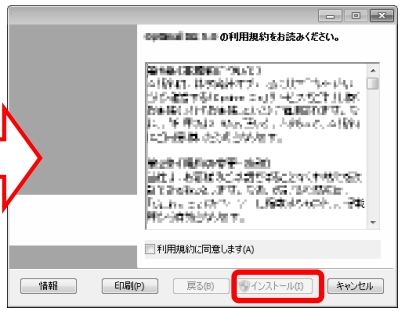
Windows の場合は、Windows 機器へエージェントをインストールし、ライセンス認証を行う必要があります。

※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るため、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。



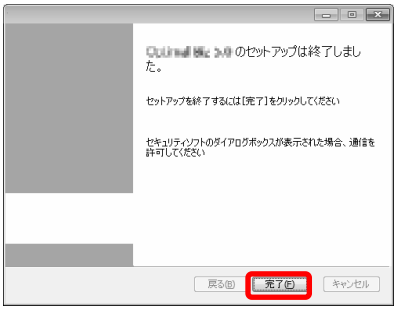
①ブラウザを起動し、エージェントダウンロード画面を表示します。
②[ダウンロード(MSI)]をクリックします。

③[実行]をクリックします。

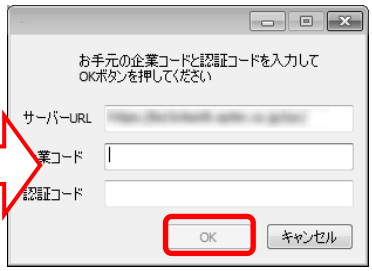


④利用規約を確認後、「利用規約に同意します」にチェックを入れ、[インストール]をクリックします。

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。

ライセンス認証完了後、左記のブラウザが表示されます。ユーザー情報、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。詳細は、「Windows エージェント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「STEP3」26 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。

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

登録したユーザー、組織、機器グループと STEP2 で登録した機器を関連付けます。下記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、「こんな時は・・・」の「ユーザーを登録したい」52 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。

STEP4　設定セット、設定テンプレートの作成、および組織単位にルールを作成する

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」を設定する方法をご紹介します。
他の設定も基本的な設定の流れは同じです。

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。

(1)設定セットの作成を行います。
手順 1.設定セットを作成する

(2)複数の設定セットを 1 つにまとめルールを機器に設定する場合は、下記の流れで作成します。
手順 1.設定セットを作成する⇒手順 2. 設定テンプレートを作成する

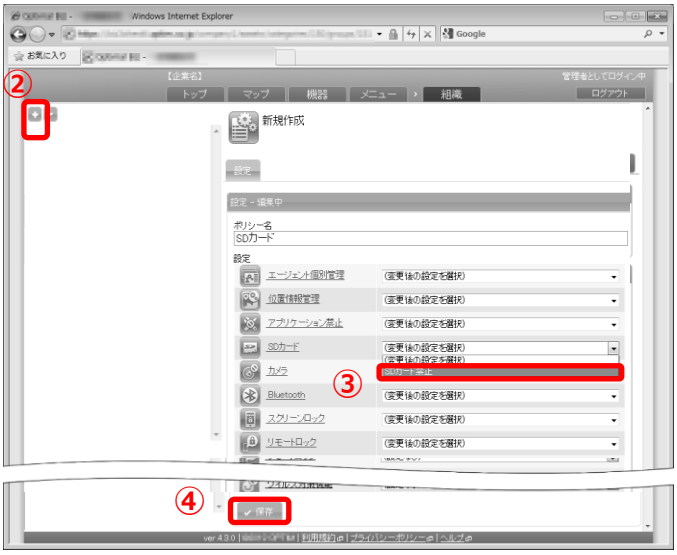
(3)組織単位に機器の設定ルールを作成する場合は、下記の流れで作成します。
・設定セットよりルールを作成する場合
手順 1.設定セットを作成する⇒手順 2.組織単位にルールを作成する
・複数の設定セットを 1 つにまとめた設定テンプレートよりルールを作成する場合
手順 1.設定セットを作成する⇒手順 2. 設定テンプレートを作成する⇒手順 3.組織単位にルールを作成する

・設定セットを作成する

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、「新規作成」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。

・設定テンプレートを作成する

①メニュー画面⇒「Android」ボックス内[設定テンプレート]をクリックします。
②[＋]をクリックし「新規作成」を選択すると[新規作成]画面を表示します。
③テンプレート名を入力し、機能「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。

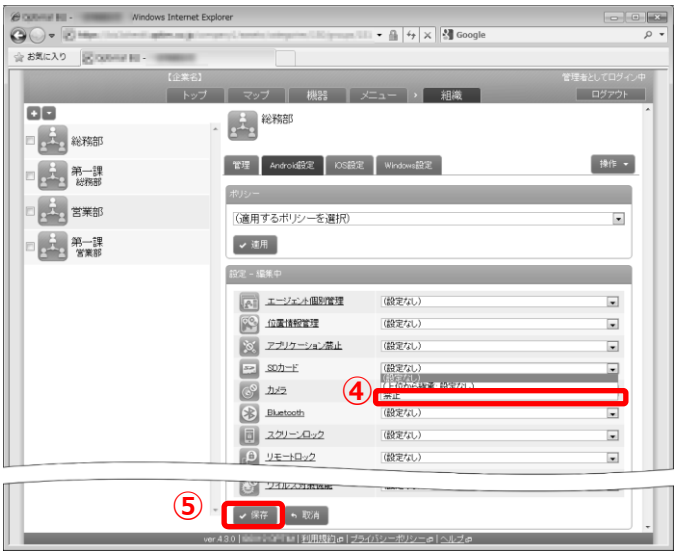


・組織単位にルールを作成する

設定セットでルールを作成する場合

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設定を行う組織を選択します。
③該当 OS[Android 設定]タブをクリックします。
最下段の[編集]をクリックします。

④機能「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。
⑤[保存]をクリックします。



設定テンプレートでルールを作成する場合

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設定を行う組織を選択します。
③該当 OS[Android 設定]タブをクリックします。
「設定テンプレートを作成する」で作成したテンプレート名を選択します。
④[適用]をクリックします。

以上で設定セットの作成、および組織のルールの作成は完了です。
STEP5 では、STEP4 で作成したルールを対象機器に反映する方法をご紹介します。

STEP5　対象機器にルールを反映する

STEP4 で作成したルール(SD カードの利用を禁止する／カメラの利用を禁止する／リモートロックを行う／リモートワイプを行うなど)をもとに、対象機器に反映します。
なお、本手順(STEP5)でリモートワイプの設定セットを選択し実行すると対象機器が初期化されます。ご利用には細心の注意を払って行ってください。

一例として、ルール「SD カード禁止」で反映する方法をご紹介します。
他の設定も基本的な反映方法は同じです。

下記設定は反映されるまでに定期同期等で時間がかかることがございます。
お急ぎの場合は、手動で同期を行ってください。
※一括機器設定の場合は機器ごとに設定を行い、手動で同期を行ってください。

(1)グループ単位にルールを反映する場合
・グループでルールを反映する

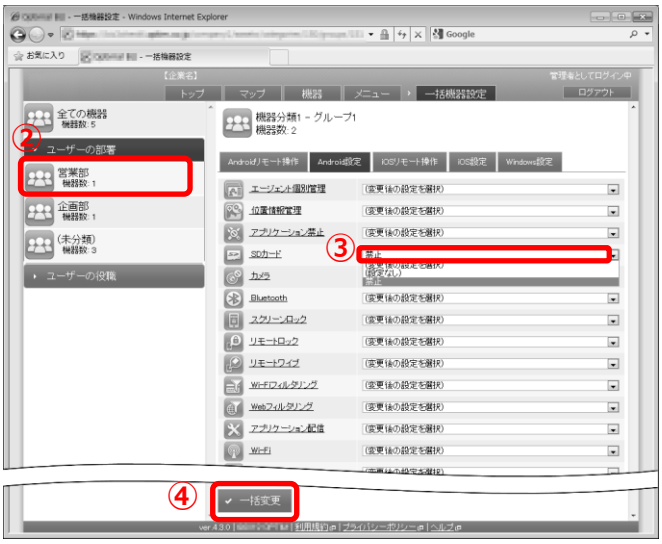
(2)組織単位にルールを反映する場合
・組織でルールを反映する

(3)単一機器ごとに 1 つにまとめた設定テンプレートを反映する場合
・設定テンプレートを単一機器に反映する

(4)単一機器ごとに設定セットで作成したルールを反映する場合
・設定セットを単一機器に反映する

・グループ単位にルールを反映する

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設定を行うグループ[営業部]を選択します。
③該当 OS [Android 設定]の機能「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。

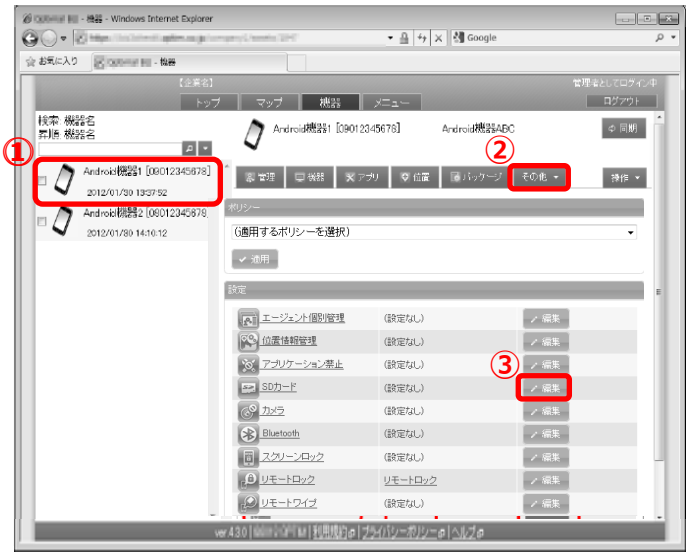


本設定は、次回の同期時に機器に反映されます。

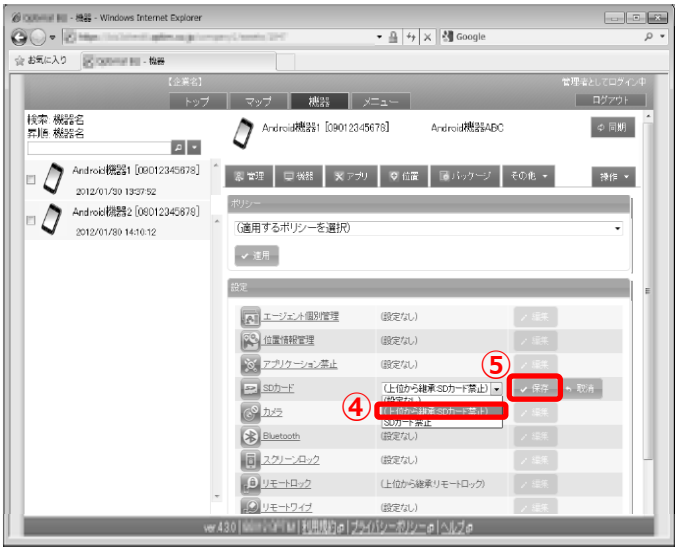
リモートワイプは、「一括変更」をクリック後、確認画面で「OK」をクリックすることで、次回の同期時に対象機器の初期化を行います、
ご利用には細心の注意を払ってください。

・組織単位にルールを反映する

①機器一覧より対象とする機器をクリックします。
②[その他]タブより「設定」をクリックします。
③機能「SD カード」の「編集」をクリックします。



③[上位から継承]を選択します。
④[保存]をクリックします。

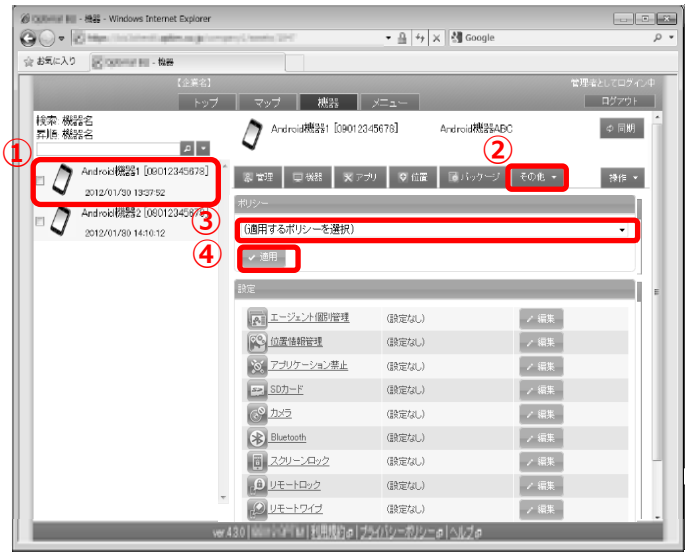


本設定は、次回の同期時に機器に反映されます。

リモートワイプは、「保存」をクリックすることで、次回の同期時(手動同期含む)に機器の初期化を行います。
ご利用には細心の注意を払ってください。

・単一機器ごとに設定テンプレートを反映する

①機器一覧より対象とする機器をクリックします。
②[その他]タブより[設定]をクリックします。
③テンプレート名を選択します。
④[適用]をクリックします。

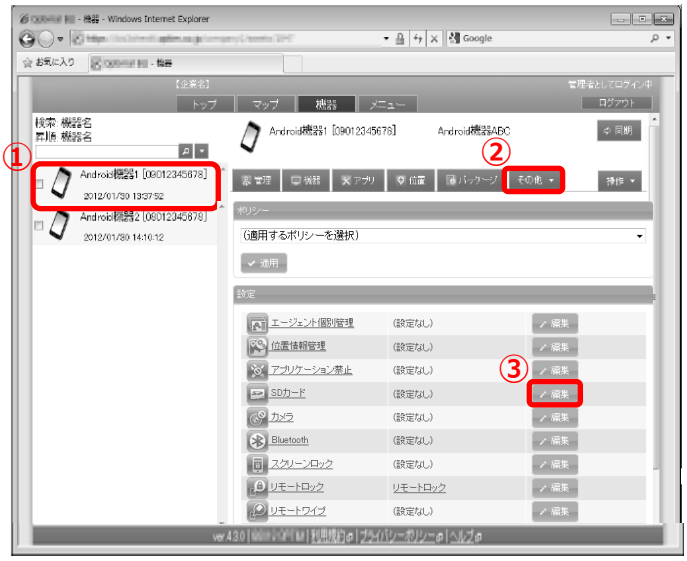


本設定は、次回の同期時に機器に反映されます。

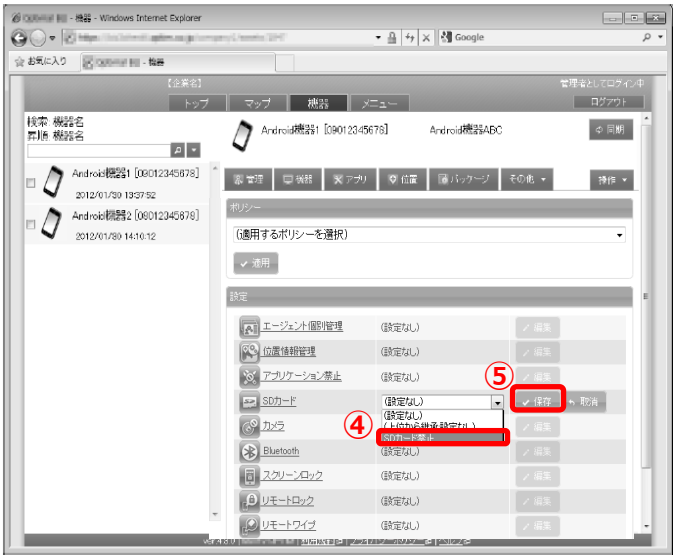
リモートワイプは、「適用」をクリックすることで、次回の同期時(手動同期含む)に機器の初期化を行います。
ご利用には細心の注意を払ってください。

・単一機器ごとに設定セットを反映する

①機器一覧より対象とする機器をクリックします。
②[その他]タブより[設定]をクリックします。
③機能「SD カード」の[編集]をクリックします。



④「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。
⑤[保存]をクリックします。



本設定は、次回の同期時に機器に反映されます。

リモートワイプは、「保存」をクリックすることで、次回の同期時(手動同期含む)に機器の初期化を行います。
ご利用には細心の注意を払ってください。

こんな時は・・・

よく利用する機能を紹介します。全機能の詳細については別紙「管理サイトユーザーマニュアル」を参照してください。

【管理】

・資産管理を行いたい

社内で使用している Android や iOS の端末の管理ができないかしら。どの端末をどの社員が使用しているのか、把握できるといいんだけど。

端末にアプリをインストールするだけで、社内で使用している Android や iOS をブラウザー上で把握することができます。また、機器にユーザー名を登録することで、どの機器をどの社員が使用しているのか確認できます。

･組織を登録し、組織ごとに設定を行いたい

会社の組織構造（支社・部署等）を登録し、組織ごとに権限の設定やルールの設定を行いたい。

①組織上で、誰にどのような権限を与えたいかを考えます。

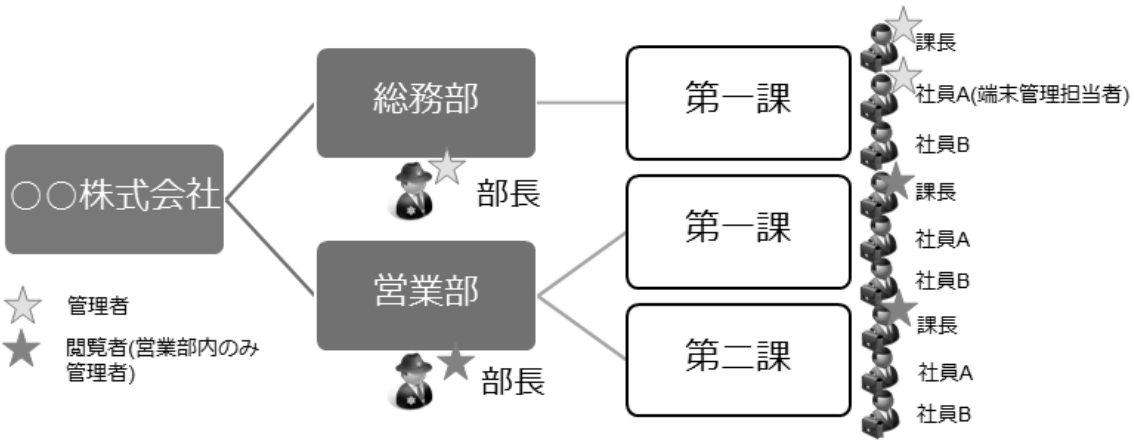
例として、総務部主導で端末管理を始めた会社をあげて考えます。

--総務部の部長、課長と、端末管理担当の社員 A さんには、全社の端末全てに対し全ての操作が行える管理者権限を与えます。

--総務部の社員 B さんは、端末管理担当ではないため、管理者権限ではなく、閲覧権限を与えます。

--営業部の部長と課長は、全体の端末は閲覧のみだが、営業部の端末に対しては、管理者権限を与えます。

--営業部の社員 A さん、B さんは、全体に対しても、営業部の端末に対しても、権限は全く付与しません。



部署	役職	全体の権限	特定の部署に対してのみの権限
総務部	部長	管理者	
総務部第一課	課長	管理者	
総務部第一課	社員 A (端末管理担当)	管理者	
総務部第一課	社員 B	閲覧者	
営業部	部長	閲覧者	営業部の端末に対してのみ管理者権限
営業部第一課	課長	閲覧者	営業部の端末に対してのみ管理者権限
営業部第一課	社員 A	なし	
営業部第一課	社員 B	なし	
・・・			
以下略			

②例に挙げた組織を作成、適用する場合、必要な作業は下記のとおりです。

1)機器管理の基本設定を行います。・・・STEP1　10 ページ参照

2)組織、グループ、ユーザーの登録を行います。・・・「こんな時は・・・」の【登録】　49 ページ参照

2-1：以下のように組織を 4 つ登録します。

組織名	上位組織	権限を引き継ぐ
総務部	(なし)	-
第一課	総務部	チェックあり
営業部	(なし)	-
第一課	営業部	チェックあり

2-2：以下のようにグループ(ユーザー分類)を登録します。

ここでは、営業部の部長、課長に与える追加権限用(営業部のみ管理者権限を与える)のグループを作成します。

分類名	グループ名	権限
特定部署管理者	営業部	組織：営業部、管理者、ユーザー所有の機器：なし、 アプリ：なし

2-3：ユーザーを登録します。

名前、フリガナ、ユーザーID、メールアドレスは任意のものを入力し、
ユーザー種別、組織、ユーザー分類については、下記の通り設定します。

部署	役職	ユーザー種別	組織	ユーザー分類 (特定部署管理者)
総務部	部長	管理者	総務部	なし
総務部第一課	課長	管理者	総務部＞第一課	なし
総務部第一課	社員 A (端末管理担当)	管理者	総務部＞第一課	なし
総務部第一課	社員 B	閲覧者	総務部＞第一課	なし
営業部	部長	閲覧者	営業部	営業部
営業部第一課	課長	閲覧者	営業部＞第一課	営業部
営業部第一課	社員 A	一般	営業部＞第一課	なし
営業部第一課	社員 B	一般	営業部＞第一課	なし
・・・				
以下略				

3)　機器へアプリをインストールする・・STEP2　18 ページ参照

4）2)で登録した組織と機器を紐づける・・STEP3　26 ページ参照

5）ルールの作成及び、組織へのルールの設定を行う・・STEP4　27 ページ参照

・端末やユーザーに所属する組織を登録したい

会社の組織構造（支社・部署等）に沿って端末やユーザーを管理したい。

端末やユーザーの作成時に、所属する組織を登録することができます。登録した組織は管理サイトの各種画面や機器レポートなどで確認できます。

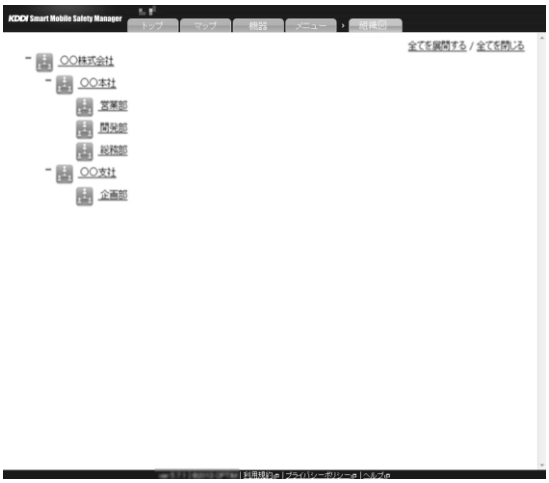
※端末の場合は「ユーザー」と「組織」のどちらか一方を登録することができます。

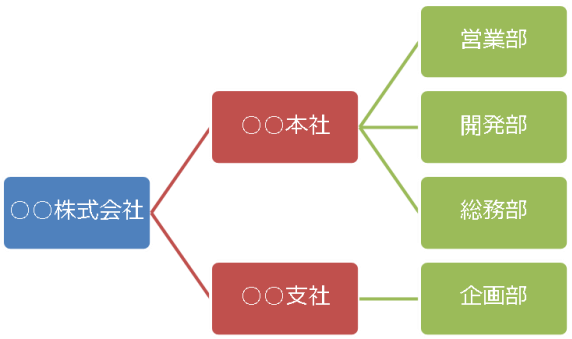
※組織は事前に作成しておく必要があります。詳細は管理サイトユーザーマニュアルを参照してください。

組織には階層構造を持たせることができます。
組織図を利用することで階層構造を視覚的に確認できます。

※組織図にはユーザーや端末は表示されません。

※階層構造は 10 階層まで持たせることができます。





・組織単位で端末の各種設定変更を行いたい

営業部の端末全てに、SD カードの利用禁止設定と、カメラの利用禁止設定を行いたいけど数が多いし大変だな・・。

複数の設定セットをまとめた「設定テンプレート」という機能を利用することで、複数の設定を 1 ステップで端末に行うことができます。また、端末に組織を登録しておくことで（前ページ参照）、設定対象を組織にすることが可能です。

今回の例では、組織「営業部」に、設定テンプレート「SD カード＆カメラ禁止」を適用することで、目的を果たすことが可能となります。

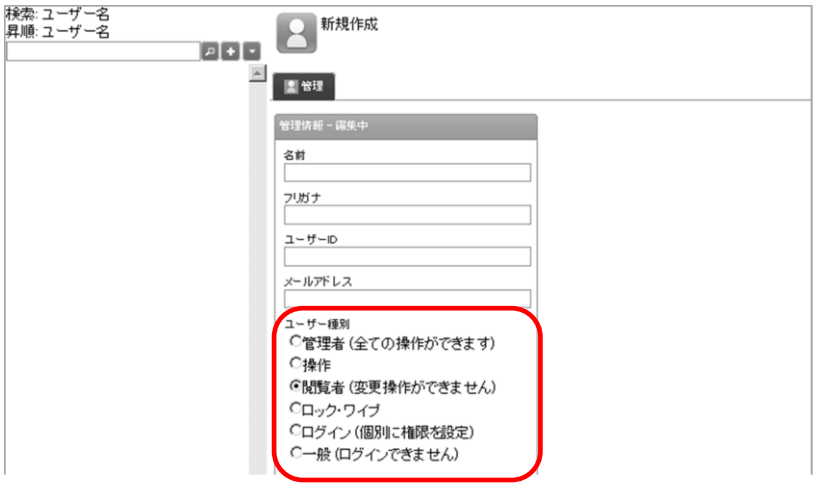
※設定テンプレートおよび組織は事前に作成しておく必要があります。詳細は管理サイトユーザーマニュアルを参照してください。

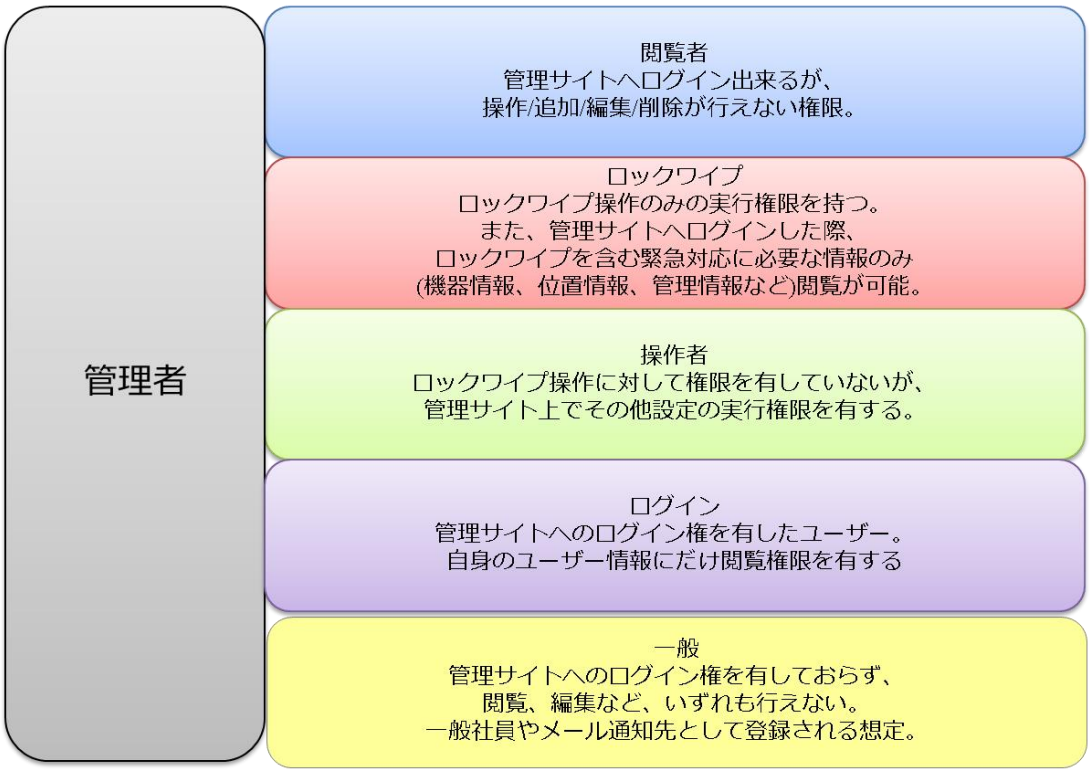
・管理サイトの閲覧のみ行えるユーザーを作成したい

総務部のＡさんには管理サイトの閲覧は行って欲しいけど、
他のことは行わせたくない・・。

ユーザー作成時に「ユーザー種別」を指定しますが、この際に指定したユーザー種別により、可能な操作が異なります。今回の例では「閲覧者」を指定することで、管理サイトの閲覧のみが行えるユーザーを作成できます。用途に応じて適切なユーザー種別を指定してください。

※ユーザー作成方法については、49 ページを参照してください。



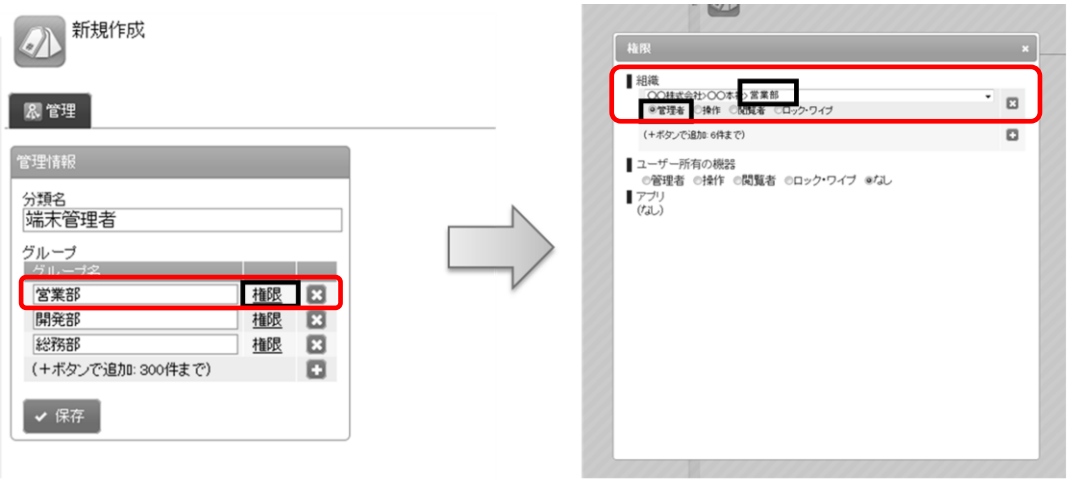


・ユーザーが行える操作を追加したい

総務部のＡさんには管理サイトの閲覧は行って欲しいけど、
他のことは行わせたくない・・。
でも、そろそろ業務にも慣れてきたし、営業部に所属する端末やユーザーだけは管理を任せてみよう。

「A さんには基本的に変更や削除はさせたくない」といった基本権限に、「営業部に対してのみ、変更や削除も許可しよう」といった追加権限を与えることが可能です。
基本権限はユーザー作成時にユーザー種別により付与します。（前ページを参照）
追加権限はユーザー分類を用いて付与します。

① 営業部に対して「管理者」権限を持つユーザー分類を作成します。



② A さんを上記で作成したユーザー分類に含めます。

こちらで、作成は完了です。

※ユーザー種別が「管理者」の場合は最初から全ての権限を持っています。追加権限を付与する必要はありません。

※組織「総務部」は事前に作成しておく必要があります。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

･役職ごと、端末の用途ごとで機器のグルーピングを行いたい

役職ごとに、使える機能を分けて設定できると便利なんだけど。
一般社員には、アプリ禁止等の規制を厳しくして、役職がついている社員には自己判断に任せてある程度規制を緩めたりできたら・・

先に、部署・役職ごとにグループを作成し、ユーザーにそのグループを登録しておくことで、1人ずつルールを設定せずとも､ユーザーのグループごとに一括でルールの設定を行うことができます。

社内使用の端末と社外持ち出しの営業用端末で、セキュリティレベルに差をつけたい。社外持ち出し用の営業用端末は、情報漏えいを防ぐため、SD カードの使用を禁止したり、端末の暗号化を必須にしたい。

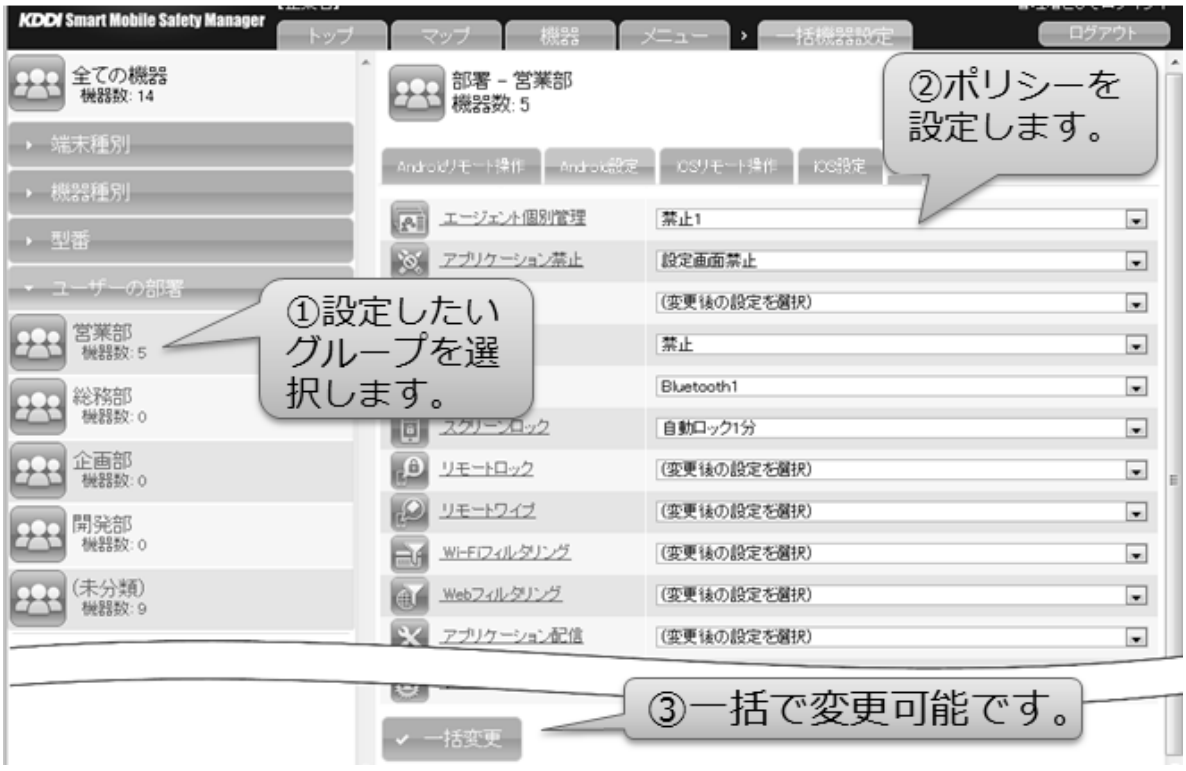
先に、端末の用途ごとにグループを作成し、機器をそのグループに所属させることで、1 機器ずつルールを設定せずとも、機器のグループごとに一括でルールの設定を行うことができます。

･グループごとにルールの設定を行いたい

役職ごと、端末の用途ごとに作成したグループを使って、
一括でルールの設定を行うことはできるの？

※グループ作成方法については、49 ページを参照してください。

一括機器設定機能を使用して、グループごとに一括でルールの設定を行うことができます。
(機器ごとにルール設定を行うこともできます。)



･端末の最新状況を知りたい

端末の位置情報とか、端末のアプリ情報とか最新のデータを確認できないかしら。

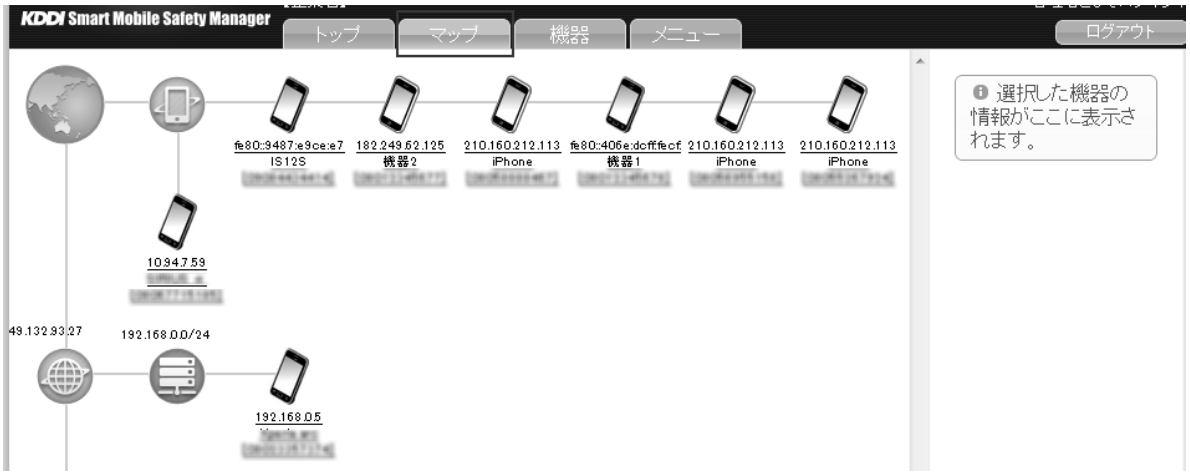
⇒『管理サイトユーザーマニュアル』の管理サイトの操作> 機器
をご参照ください。

・機器情報、アプリケーション情報、位置情報の取得･表示をすることができます。各種情報は、CSV 形式にてエクスポートが可能です。

登録されている機器を一目で確認できないかな。

⇒『管理サイトユーザーマニュアル』のメニュー設定項目> 機器> マップ
をご参照ください。

・ネットワークマップで、登録されている機器を一目で確認することができます。

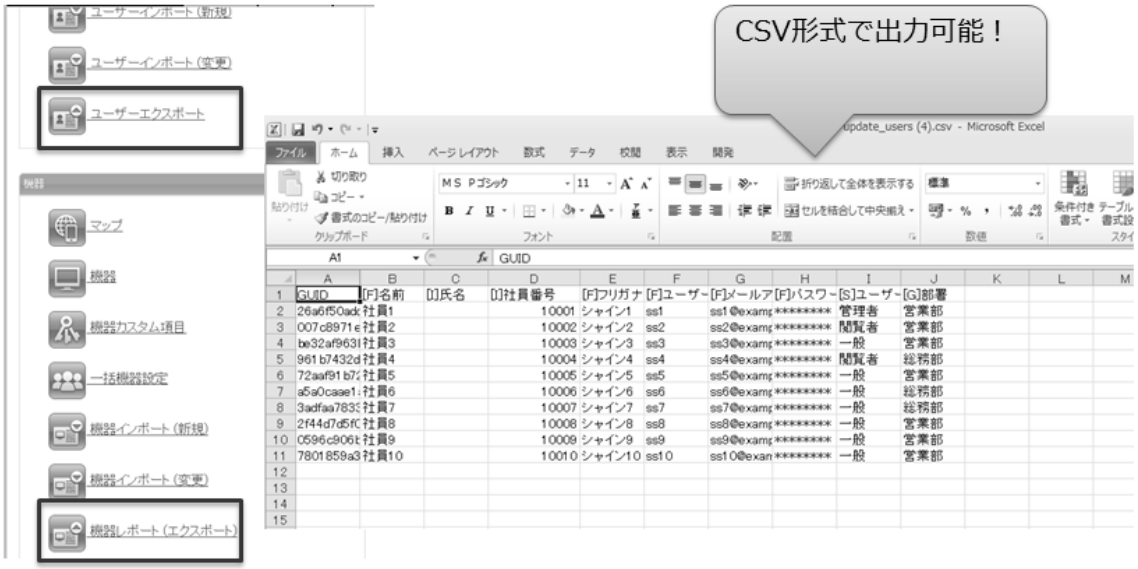


･端末一覧、ユーザー一覧をエクセルで表示したい

資産管理用に総務部に端末一覧を提出しなくてはいけないんだけど、エクセルで端末一覧をみられないだろうか。

⇒『管理サイトユーザーマニュアル』のメニュー設定項目>ユーザー>ユーザーエクスポートをご参照ください。

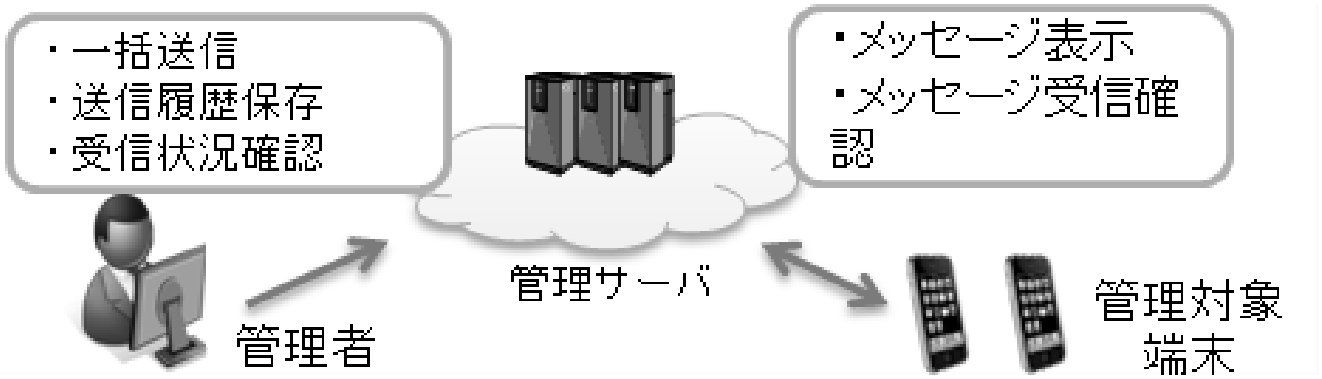
端末情報、ユーザー情報は CSV 形式でダウンロードし、エクセルとして保存することができます。



・業務連絡、緊急時の連絡を一斉配信したい

社員に一斉に連絡をするいい方法はないかな。
定期的なメッセージは、自動で送ってくれたりするといいんだけど。
⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞機器＞メッセージ通知
をご参照ください。

・日々の業務連絡や、緊急時の連絡等を、管理サイトから管理している端末に一斉送信することができます。開封確認機能で、社員がメッセージを確認したかも把握でき、スケジュール配信機能を設定することで、定期的なメッセージは自動で送信することができます。



・業務上必要なアプリを一斉配信したい

新しいアプリを導入したから、社員全員にインストールしてもらいたいんだけど・・

⇒『管理サイトユーザーマニュアル』のメニュー設定項目
(Android の場合) ＞Android-セットアップ＞アプリケーション配信
(iOS の場合)＞iOS＞アプリケーション配信をご参照ください。

・業務上必要なアプリを社員にインストールしてもらいたい場合、管理サイトから設定を行うだけで、インストールするように通知を出すことができます。

・アプリがインストールされたか確認したい

この前配信したアプリは、きちんとみんなインストールしただろうか・・

⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞機器
＞アプリケーションレポートをご参照ください。

・社員にインストールを促したアプリが、実際インストールされたかどうか、アプリケーション一覧で確認することができます。

[1]アプリケーション名	[1]パッケージ名/アプリケーションID	[1]バージョン番号	[1]バージョン名	[1]インストール日時	[1]アップデ
Androidシステム	android	10	2.3.7	2012-02-22 23:16:38 +0900	2012-02-2
TTS Service	android.tts	10	2.3.7	2012-02-22 23:32:30 +0900	2012-02-2
Adobe Flash Player 11.1	com.adobe.flashplayer	111102059	11.1.102.59	2011-11-15 20:34:30 +0900	2011-11-15
Bluetooth共有	com.android.bluetooth	10	2.3.7	2012-02-22 23:33:44 +0900	2012-02-2
ブラウザ	com.android.browser	10	2.3.7	2012-02-22 23:33:44 +0900	2012-02-2
電卓	com.android.calculator2	0	sonyericsson 7.0.0	2012-02-22 23:19:18 +0900	2012-02-2
カレンダー	com.android.calendar	12582923	6.0.A.0.11	2012-01-13 17:06:06 +0900	2012-01-13
証明書インストーラ	com.android.certinstaller	10	2.3.7	2012-02-22 23:33:46 +0900	2012-02-2
電話帳	com.android.contacts	5	01.023.0040	2012-02-22 23:33:46 +0900	2012-02-2

【グループ/ユーザー/組織を登録する】

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ける場合を考えます。
（組織単位で管理を行いたい場合は、「組織を登録し、組織ごとに設定を行いたい」36 ページを参照してください。）

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	○○　○○	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、役職ごとにわけることにします。
・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、「こんな時は・・・」の「ユーザーグループを登録したい」49 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。
どの場合に、どのルールを使えばいいのかの詳細は、「こんな時は･･･」33 ページを参照してください。

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たら、STEP1 から実際の設定に入ります。

・ユーザーグループを登録したい

ユーザーをグループにまとめて管理したい！

⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞ユーザー＞ユーザー分類をご参照ください。

機器を使用するグループ/ユーザー/組織の登録を行います。

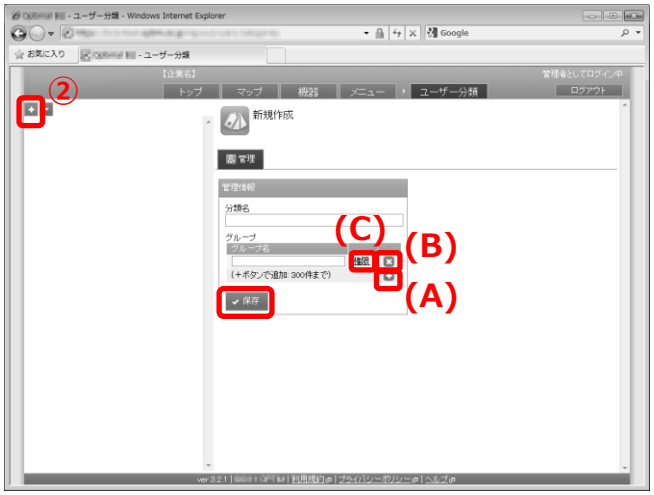
グループとは、ユーザーや機器を一つにまとめ効率よく管理を行うためのものです。「部署」、「役職」といったように自由にグループを設定することができます。グループを作成し、ユーザーをそのグループに所属させることで、機器の設定等をグループごとに一括で設定することが可能です。グループはユーザーグループ(役職、部署で分ける場合等)、機器グループ(機器の用途ごとに分けたい場合等) の 2 種類作成することが可能です。

・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ご参照ください。

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。
※組織分けの考え方やアクセス権限の付与方法については、「組織を登録し、組織ごとに設定を行いたい」36 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[ユーザー分類]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分類名、グループを入力し、[保存]をクリックします。

※ユーザー分類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したい

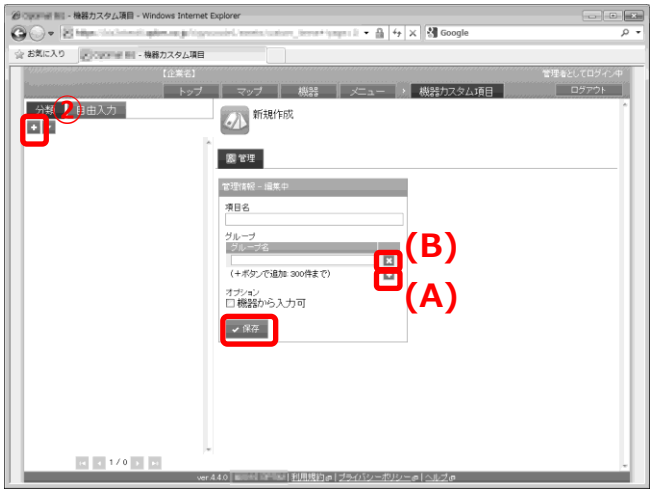
機器をグループにまとめて管理できたら便利だな

⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞機器＞機器カスタム項目をご参照ください。

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。



入力例）機器の用途ごとにわける場合

「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

・組織を登録したい

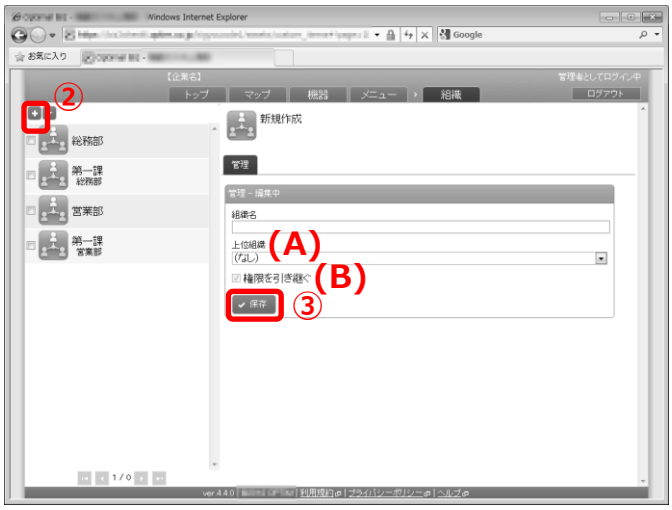
組織を登録して管理したい。

⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞組織＞組織をご参照ください。

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[＋]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、管理サイトマニュアルを参照してください。



・ユーザーを登録したい(※必須)

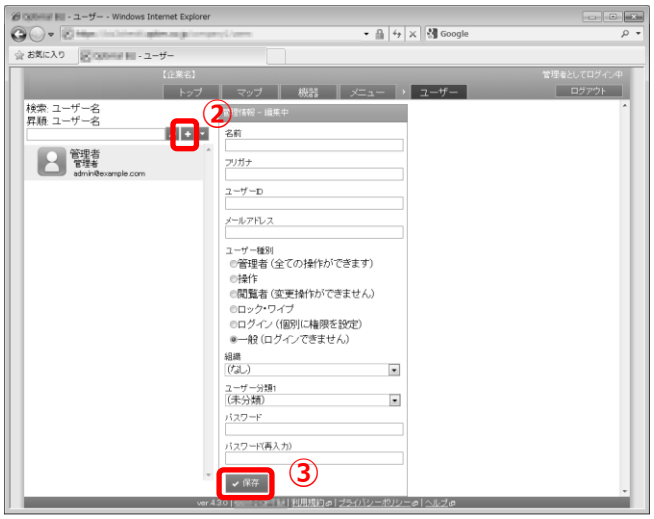
ユーザーを登録して管理したい。

⇒『管理サイトユーザーマニュアル』のメニュー設定項目>ユーザー>ユーザー をご参照ください。

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下記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」53 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。



・複数人のユーザーをまとめて登録したい

ユーザーをまとめて登録できれば便利なのに。
⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞ユーザー＞ユーザーインポート(新規)をご参照ください。

複数人のユーザーをまとめて登録したい場合は、下記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。

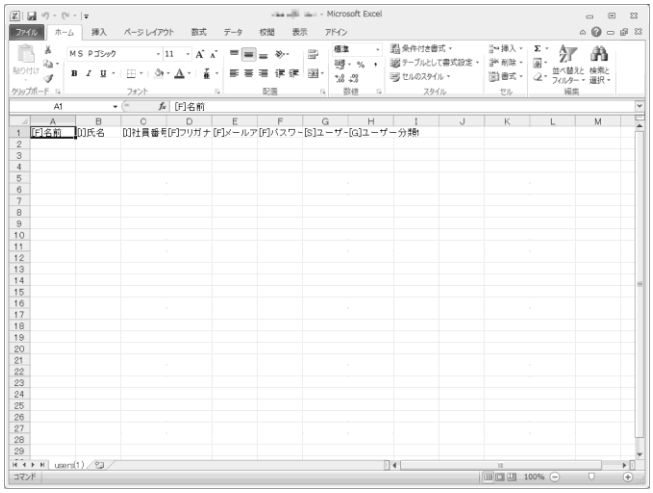
③ファイルを開き、2 行目よりユーザー情報を入力してください。(ファイルは、メモ帳や EXCEL 等で表示してください。)

※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。

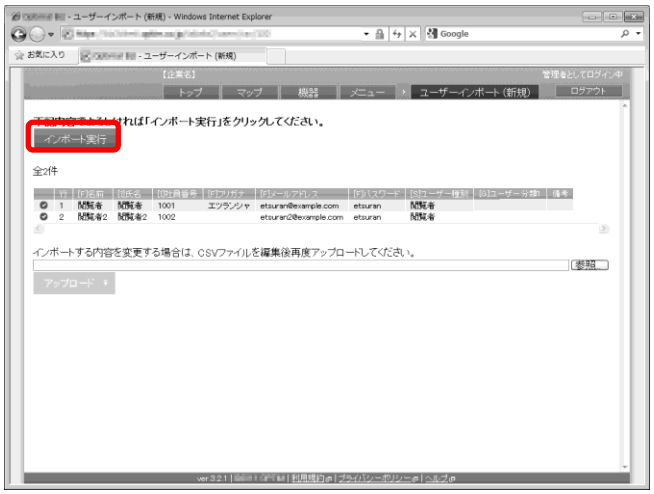
※ファイル名は変更しても問題ありませんが、ファイルの種類は「CSV(カンマ区切り)(*.csv)」を選択し、保存してください。



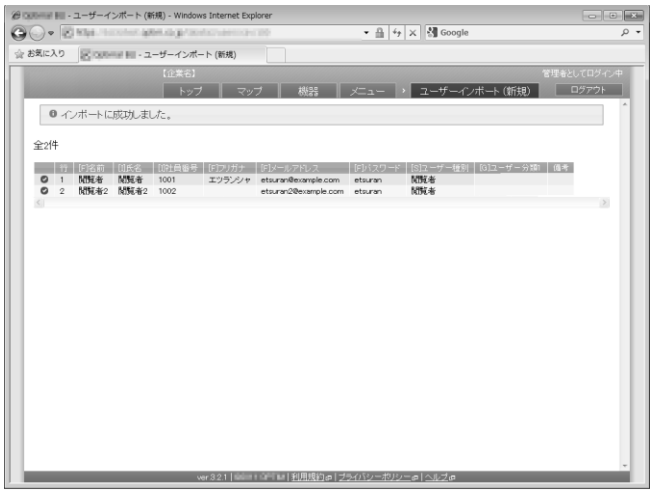
④参照をクリックし、③で保存したファイルを選択します。
⑤[アップロード]をクリックします。

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。



【セキュリティ】

･社員が端末を私的に使用するのを防ぎたい

ゲームアプリや業務外アプリを入れていないかしら。
⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞Android-使用制限
＞アプリケーション禁止をご参照ください。

・社員が業務用の端末を私的に使用するのを防ぐために、業務外のアプリを禁止したり、アプリのインストールを制限することができます。

業務用の端末で私用電話するのを防ぎたい！
⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞Android-使用制限＞発信先制限
をご参照ください。

・社員が業務用の端末で私用電話をするのを防ぐために、業務用電話番号以外への発信を禁止することができます。※緊急通報用電話番号(110,119 等)への発信制限は端末の仕様により制限できません。

カメラや Bluetooth の使用を防げないかしら。
⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞Android-使用制限
＞カメラ orBluetooth をご参照ください。

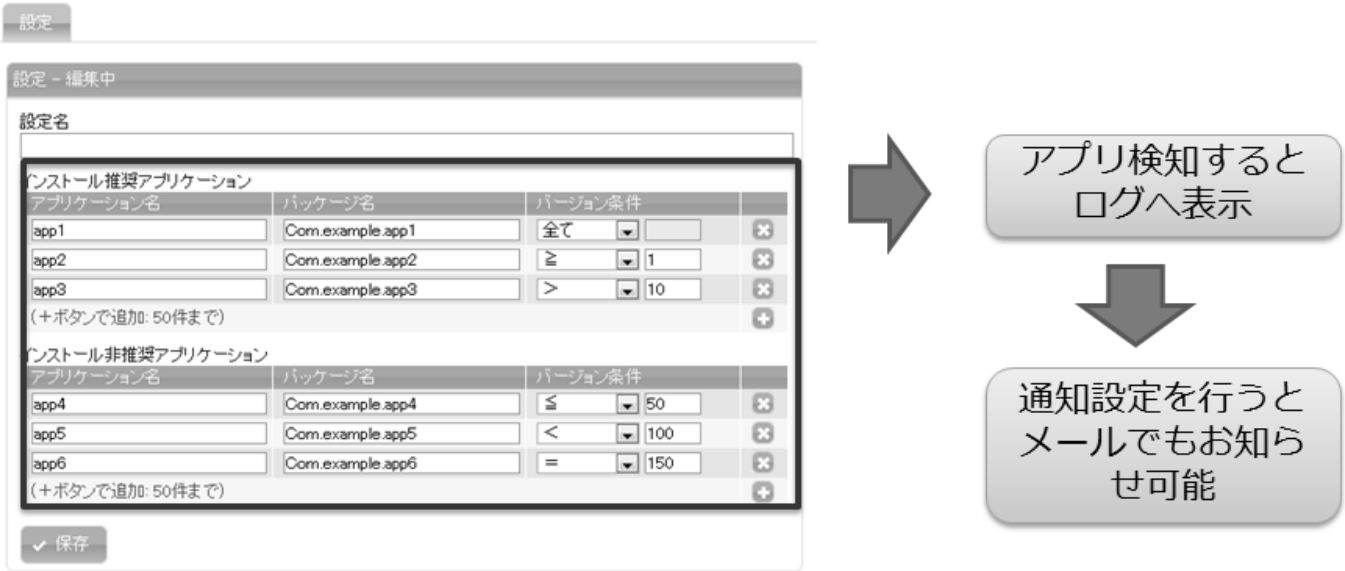
・業務上必要のない、カメラ、Bluetooth 等の使用できないように設定できます。

・端末に不審なアプリが入っていないか監視したい

端末の情報を勝手に吸い上げてしまうような不審なアプリは入れていないかしら。

⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞Android-使用制限＞アプリケーション検知をご参照ください。

・管理者が指定した不要なアプリがインストールされた場合に、ログへ表示します。管理者にメール通知を行うこともでき、利用状況を把握することができます。
※メール通知を行うためには、アプリケーション検知機能設定後、通知設定機能でアプリケーション検知時にメールを配信するように設定をする必要があります。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。



･端末の情報漏洩を防ぎたい

端末からの情報漏えいを防ぐにはどうしたらいいんだろう・・？
⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞Android-セットアップ＞暗号化をご参照ください。

・紛失･盗難等により、たとえ情報が流出したとしても、端末に残された情報そのものが読めないようにするため、端末に標準搭載されている暗号化設定をするように促すことができます。端末に暗号化設定がされるまで、暗号化設定を促すポップアップメッセージを表示します。

SD カードから情報を持ち出されたりしてしまわないかしら。
⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞Android-使用制限＞SD カードをご参照ください。

・SD カードでお客様の顧客情報や、業務上の機密情報を抜き取られないように、SD カードの使用を禁止することができます。

社外のフリーのホットスポットで Wi-Fi 接続をすると、情報の盗聴をされると聞いたことがあるけど・・
⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞Android-使用制限＞Wi-Fi フィルタリングをご参照ください。

・端末を社外に持ち出した際、フリーのホットスポット等への接続を禁止し、情報の改ざんや盗聴を防ぐために、許可していない SSID への Wi-Fi 接続を禁止することができます。

【問題発生時】

･もし端末が管理下から外れたら・・？

もし、ライセンス解除を勝手にされて、管理下から外れてしまったら大変！

⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞管理＞通知設定をご参照ください。

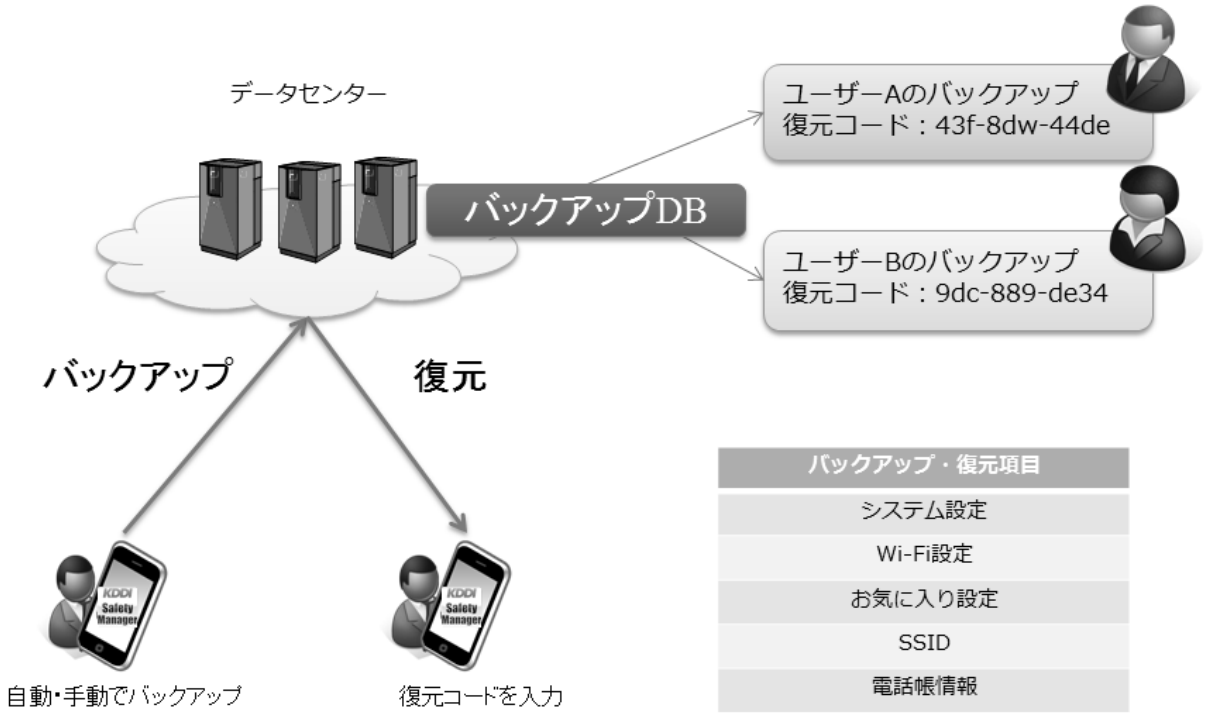
・ライセンス解除等により端末が管理下から外れた可能性をお知らせします。指定期間内に通信がない機器の通信日時を赤字で表示し、管理者にアラートメールを送信します。

･故障・紛失時に備え、情報をバックアップしておきたい

端末が壊れてしまった。電話帳のデータも全部入っていたのに、どうしよう。

⇒『管理サイトユーザーマニュアル』のメニュー設定項目＞Android＞設定バックアップをご参照ください。

・端末の故障･紛失時に備え、データをバックアップし、万が一故障･紛失した場合にも、すぐに最新の状態に復元することができます。お客様情報が入った大切な電話帳や、Wi-Fi 設定、お気に入り設定を定期的に自動バックアップすることができます。



バックアップ・復元項目
システム設定
Wi-Fi設定
お気に入り設定
SSID
電話帳情報

･紛失したり盗まれたりしたら・・・

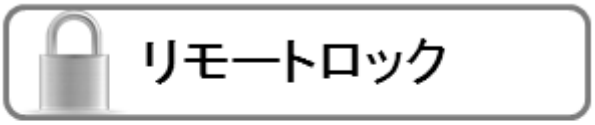
端末をなくしてしまったんだけどどうしよう。
今すぐ探したい・・どこにあるんだろう。
⇒『管理サイトユーザーマニュアル』の管理サイトの操作> 機器> 位置
をご参照ください。

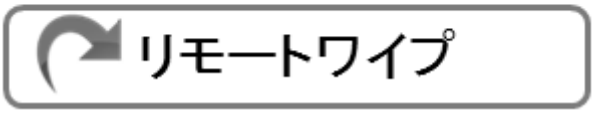
・位置情報を確認することで、紛失場所の手がかりになります。
※端末の位置情報を正確に取得するには､エージェントが端末上で位置情報の取得を許可されていること、そしてエージェントが認証されていることが必要条件となります。

他人に使用されて、情報漏洩するのを防がなきゃ。
⇒『管理サイトユーザーマニュアル』の管理サイトの操作> 機器> リモート操作
をご参照ください。

・遠隔(管理サイト)から端末にロックをかけ、端末が使用できないようにすることができます。

・端末の情報漏えいを防ぐために、遠隔(管理サイト)からデータを初期化することができます。
※一度データを削除すると元に戻すことはできませんのでご注意ください。





･ライセンス認証に失敗したら・・・

機器の利用開始時に、ライセンス認証に失敗してしまう…

■端末が、インターネットに接続可能であるか確認してください。ブラウザで、他のウェブサイトに接続できるか確認してください(端末内に保存されたキャッシュを閲覧している可能性もあるので、ニュースサイトなどで現在の日付のニュースが閲覧できるか確認します)。

■ライセンス認証に失敗するときは､まず企業コードと認証コードが正しいか確認してください。企業コードと認証コードの後に不要なスペースなどが混在していないことを確認してください。

■ユーザーライセンスが利用可能かどうか、管理者にお問い合わせください。

■iOS をご利用の場合は、Safari 以外のブラウザではライセンス認証は行えません。

■端末のインターネット設定をご確認ください。ポート番号「80」「5223」「443」が遮断されておらず、使用可能であることを確認してください。

■以上の確認事項をすべて確認してもライセンス認証が失敗する場合は、ブラウザを終了し、以下の手順に従ってブラウザのキャッシュを消去してください。キャッシュ消去後に、ブラウザを起動して再度ライセンス認証を行ってください。キャッシュ消去後も認証に失敗する場合は、再度管理者にご連絡ください。

・Android の場合：ホーム画面→「アプリ」→「設定」→ブラウザの設定から
・iOS の場合：ホーム画面→「設定」→「Safari」の設定画面で「Cookie とデータを消去」を選択
・Windows の場合：Internet Explorer をご利用の場合は「設定」→「インターネットオプション」から「全般」タブの「履歴の削除」から「削除」を選択

機能一覧

KDDI Smart Mobile Safety Manager を使用して、管理できる機能について説明します。詳細の設定方法については、管理サイトユーザーマニュアルを参照してください。

KDDI Smart Mobile Safety Manager では、下記の端末管理、アプリケーション管理、セキュリティ管理等が行えます。下記の機能一覧より機器へ設定したい項目を選択し、機器への設定を行ってください。詳細な設定方法については、管理サイトユーザーマニュアルを参照してください。

基本機能	
端末管理	ハードウエア情報の取得
	アプリケーション情報の取得
	各種レポート出力
	IT 機器自動検出
	組織管理
	Zone Management
	位置情報履歴取得
	Apple Push 証明書誤登録防止
セキュリティ管理	パスワードポリシーの設定
	位置情報の取得
	無通信検知機能
	root 化、JailBreak 検知機能
	リモートロック
	リモートワイプ
	発信先制限
	iOS 構成プロファイル画面上設定
	構成プロファイル削除防止・検知機能
設定管理	連絡先情報の設定
デバイス管理	SD カード利用禁止・許可設定
	USB 利用禁止・許可設定・ホワイトリスト設定
	カメラの利用禁止・許可設定
アプリケーション管理	アプリケーション利用設定
	アプリケーション配信
	プロビジョニングプロファイル配信
	Windows ソフトウエアライセンス設定
	SecureShield
	App Manager
インターネット接続管理	Web クリップ設定
	Exchange Active Sync 設定
	メール設定
	Web フィルタリング設定
	HTTP プロキシ設定
オプション機能	
インターネット接続管理	お気に入り設定
	Web フィルタリング設定
	+browser Safety Manager (独自ブラウザ)

	ファイルダウンロード制限
バックアップ機能	設定情報バックアップ
	設定情報復元
メッセージ配信	メッセージ配信設定
	通知結果の集計
ウィルス対策機能	Safety Manager AntiVirus

※こちらに掲載している機能は一部となります。

※詳細については下記をご確認ください。

http://media3.kddi.com/extlib/business/security-managed/security/kddi-smsm/function/pdf/functionlist.pdf