KDDI Smart Mobile Safety Manager
はじめてお使いになる方へ

最終更新日　2024 年 1 月 14 日
Document ver.1.9
（Web サイト ver.9.18.0）

変更履歴

日付	ver	変更箇所	変更内容
2019/4/25	1.0		新規作成
2019/12/5	1.1	5.2 iOS 端末の導入	記載内容の修正
2020/6/18	1.2	全体	機器を端末に変更
		全体	Android 設定全画面のメニューに「ゼロタッチ登録」と「Samsung knox」を追加
		6.1.3.1 テンプレート CSV ファイルの入手・編集	参考に記載の Android の MAC アドレス削除
		本マニュアルの見かた	注記追加
2021/2/21	1.3	全体	DEP を ADE、VPP を「App とブック」に修正
		1.1 KDDI Smart Mobile Safety Manager とは	注記追加
		3.4.1 設定セットを作成する	上限値件数を追加
2021/7/25	1.4	6.1.3.1 テンプレート CSV ファイルの入手・編集	参考の iOS から MAC アドレスを削除
2022/2/20	1.5	2.6.1 同期の仕組み	Android／Windows の説明文を修正 注記を追加
2022/6/12	1.6	4.4 セキュリティポリシー／設定内容を検討する	OS に関連する以降を以上に修正
		4.6.3 パターン C	
2022/11/20	1.7	はじめに	全改修
2023/8/6	1.8	全体	構成変更に伴う参照先の修正
		はじめに	名称・呼称、用語集を追加 商標登録修正
		2.6 同期とは	Mac OS クライアントマニュアルの参照を削除 注記修正
2024/1/14	1.9	全体	規約に従い、表記揺れなど統一

はじめに

本マニュアルでは、KDDI Smart Mobile Safety Manager（以下、本製品と呼ぶ）の操作ほか、各機能の概要、画面の説明、設定操作について説明しています。

また、要点となる各種の内容を以下に記載しています。これらの内容をご理解のうえ、マニュアルをお読みください。

名称・呼称

本マニュアルに登場する特定の企業、人について、以下の定義で記載しています。

名称	説明
サービス企業	本製品を提供する企業。
管理者	本製品の管理サイト（機器の管理・運用を行う Web サイト）を運用する者。
端末使用者	本製品で管理している端末を使用する者。
システム管理者	企業の社内システム（サーバー・インフラなど）を管理する者。

注意・ポイントマーク

操作を行う場合に注意する点や、操作のポイントとなる点を示す場合は、以下のマークで記載しています。

マーク	説明
	データの破損や消失など、特に注意していただきたい内容を記載しています。
	操作のポイントや知っておくと便利な内容を記載しています。

記号

画面に表示されるボタンやメニュー、キーボードのキーなどを示す場合は、以下の記号で記載しています。

マーク	説明
［ ］	ボタン、メニュー、タブ、リンク、チェックボックス、ラジオボタンなどの名称を示しています。
「 」	画面名、機能名、項目名、マニュアル内の参照先などを示しています。
『 』	マニュアルや資料などの名称を示しています。
〈 〉	キーボードなどのハードキー名称（スペースキーは〈スペース〉と表記）を示しています。

参照マーク

他のマニュアルや他のページへなどの参照を示す場合は、以下のマークで記載しています。

マーク	説明
	他のページや Web サイトへの参照を示しています。クリックすると該当箇所にジャンプします。
	セクション内の画面への参照を示しています。クリックすると該当の画面にジャンプします。
	他のマニュアルや資料への参照を示しています。

用語集

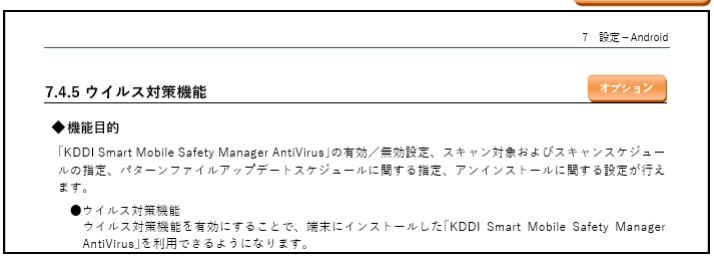
不明な用語については、『よくあるご質問（FAQ）』を参照してください。

☞ https://smsmfaq.smartmanager.jp/kddiproduct/ausl/web/knowledgeList.html?keyword=%E7%94%A8%E8%AA%9E%E9%9B%86%E4%B8%80%E8%A6%A7&searchMethod=0&searchCondition=0&searchCategory=1&searchItem=1&searchTag=1

オプション機能

オプション機能は、オプション契約をした場合に使用できる機能です。

本マニュアルでは、オプション機能の説明の見出しに オプション（オプションマーク）を表示しています。



免責事項

●本マニュアルは、ユーザー種別が［管理者］のユーザーを対象としています。［管理者］以外のユーザー種別でログインした場合は、操作が制限されます。

●iPad OS の操作は iOS と同様です。差異がある場合は iPad OS 用の記載をしています。

●画面上のバージョン表記は、実際の表示と異なる場合があります。

●本マニュアルに記載されている Web サイトの URL は、予告なく変更される場合があります。

●OS のバージョンやブラウザーにより、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 を例に説明しています。

商標登録

●Apple、iPad、iPadOS、iPhone、Mac、macOS は、米国およびその他の国で登録された Apple Inc.の商標です。

●iOS は、Apple Inc.の OS 名称です。
IOS は、Cisco Systems,Inc.またはその関連会社の米国およびその他の国における登録商標または商標であり、ライセンスに基づき使用されています。

●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。

●App Store は、Apple Inc.のサービスマークです。

●Android、Google Chrome、Google Cloud、Google マップ、Google Play、Google Workspace は、Google LLC の商標です。

●Microsoft、Microsoft Edge は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

●Windows の正式名称は、Microsoft Windows Operating System です。Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

●その他記載の会社名、製品名は、各社の登録商標および商標です。

目次

1 KDDI Smart Mobile Safety Manager とは

1.1 概要

本製品とは、PC（Windows や Mac OS を搭載するパソコン）、Android 端末、iOS 端末などの一元管理やセキュリティ対策、アプリの配信をブラウザー（本製品の管理サイト）から簡単に実現できる Mobile Device Management（以降、「MDM」と記載）／Enterprise Mobility Management（以降、「EMM」と記載）サービスです。

本製品の管理下に置くための設定ファイルやアプリを管理対象機器にインストール、認証することで、管理サイトから機器の情報を確認したり、セキュリティポリシーを反映できます。

本製品を利用するには、管理対象の機器へ管理アプリ（エージェントアプリ）や構成プロファイルと呼ばれる設定ファイルのインストールが必要です。

本製品と他社の MDM は、共存できません。

参考

◆Mobile Device Management -モバイルデバイス管理-（MDM）

MDM とは、「Mobile Device Management -モバイルデバイス管理-」の略称です。

PC（Windows や Mac OS を搭載するパソコン）や Android、iOS（iPhone／iPad）などの端末について、情報セキュリティ設定の適用や機器仕様およびインストールされているアプリ一覧などの機器情報の収集、機器紛失や盗難時に情報漏えいを防ぐリモートロックなどを管理できるソフトウェア製品のことを指します。

◆Enterprise Mobility Management -エンタープライズモビリティ管理-（EMM）

EMM とは、「Enterprise Mobility Management -エンタープライズモビリティ管理-」の略称です。

MDM や Mobile Application Management、Mobile Contents Management の包括的なセキュリティ管理機能を提供するプラットフォームを EMM と呼びます。

Mobile Application Management

業務に関わるアプリとデータを適切に管理することを目的とした「モバイルアプリケーション管理」機能を提供するプラットフォームを Mobile Application Management（以降、「MAM」と記載）と呼びます。

Mobile Contents Management

機器全体を管理するのではなく、業務に必要なコンテンツだけを管理することを目的とした「モバイルコンテンツ管理」機能を提供するプラットフォームを Mobile Contents Management（以降、「MCM」と記載）と呼びます。

1.2 優位性

KDDI Smart Mobile Safety Manager

1. **必要な機能をまとめて基本機能で提供**
   他社では有償オプションが必要な MAM 機能も、本製品では基本機能で使えます。

2. **“迷わず使える”を目指した管理サイト**
   機能のアクセス数解析、ユーザーテストやインタビューを重ね、“迷わず使える”管理サイトを提供しています。

3. **迅速な新 OS 対応、マルチデバイス対応**
   新 OS バージョンの利用の妨げにならないよう、迅速な新 OS 対応に注力しています。また、マルチ OS 対応のため、Android 端末、iOS 端末、Mac OS 端末、Windows 端末の管理を統合して行えます。

4. **国内最多、豊富な対応機器**
   機種差分の多い Android 端末も実機で検証しており、安心して機器を導入できます。

   ☞ 最新デバイス一覧：
   https://www.kddi.com/business/security-managed/security/kddi-smsm/device/

1.3 主な機能

本製品は、スマートフォンやタブレットのビジネス活用における幅広い課題を解決します。

ご契約内容により利用できる機能は異なります。

紛失・盗難、情報漏えい対策	セキュリティ設定
●リモートロック ●リモートワイプ ●位置情報取得 ●ローカルロック ●ローカルワイプ	●ウイルス対策設定 ●Wi-Fi フィルタリング ●スクリーンロックポリシー強制 ●ゾーンに応じたアプリの禁止

機器設定の効率化	資産管理・機器監視
●アプリの配信 ●ドキュメントの配信 ●クライアント証明書の配信 ●Wi-Fi 設定 ●機器の暗号化設定	●ハードウェア情報の取得 ●アプリ情報の取得 ●プリンター、ルーターなどの IT 機器情報の管理 ●Microsoft Office 製品のライセンス管理

1.4 利用方法

管理する機器や解決したい課題によって異なりますが、以下の流れで本製品を使用します。詳細については、以下を参照してください。

☞「本製品を導入する」32 ページ

	項目
導入／運用検討	導入目的を決定する
	導入機器／OS を決定する
	導入範囲／スケジュールを決定する
	セキュリティポリシー／設定内容を検討する
	契約プランを検討する
	組織／ユーザー／機器構成を検討する
設定事前準備	事前準備をする
管理サイト設定	ユーザー／組織情報を登録する
	機器情報を事前登録する
	設定セットを作成・適用する
機器設定	機器のキッティングを行う
管理サイト確認	認証状態を確認する

2 本製品の基本知識

2.1 管理サイトとは

管理サイトとは、管理者が管理下におかれている機器の情報を確認したり、その機器に対しなんらかの設定や制御を行うためにアクセスするサイトです。

運用の方法によっては、機器に紐づくユーザーや組織の情報も管理サイト内で管理します。

2.2 管理サイトの構成

2.2.1 ダッシュボード

管理サイトにログインすると、表示される画面を「ダッシュボード」といい、本画面では「お知らせ」や「利用状況」などを確認できます。また、ヘッダーメニューからさまざまな機能に切り替えて操作できます。

ご契約により表示される内容は異なります。

項番	項目	説明
1	ヘッダーメニュー	［機器］、［ユーザー］、［組織］、［設定］、［ログ］、［関連サービス］をクリックすると、各カテゴリの画面に切り替わります。
2	ログイン情報	ログイン中の企業コードとユーザー名が表示されます。ユーザー名をクリックすると、「個人設定」と「ログアウト」のメニューが表示されます。
3	お知らせ	サービス企業からの連絡内容が表示されます。詳細は、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「ダッシュボード」－「お知らせ」
4	利用状況	以下の状況が表示されます。詳細は、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「ダッシュボード」－「ダッシュボードの画面構成」
5	その他	以下の内容が表示されます。詳細は、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「ダッシュボード」－「ダッシュボードの画面構成」
6	サイトマップ	ヘッダーメニューやサイドメニューにない項目は、こちらをご確認ください。
7	マニュアル	クリックすると、各種マニュアルや FAQ へのリンク画面が表示されます。

2.2.2 ヘッダーメニュー「機器」

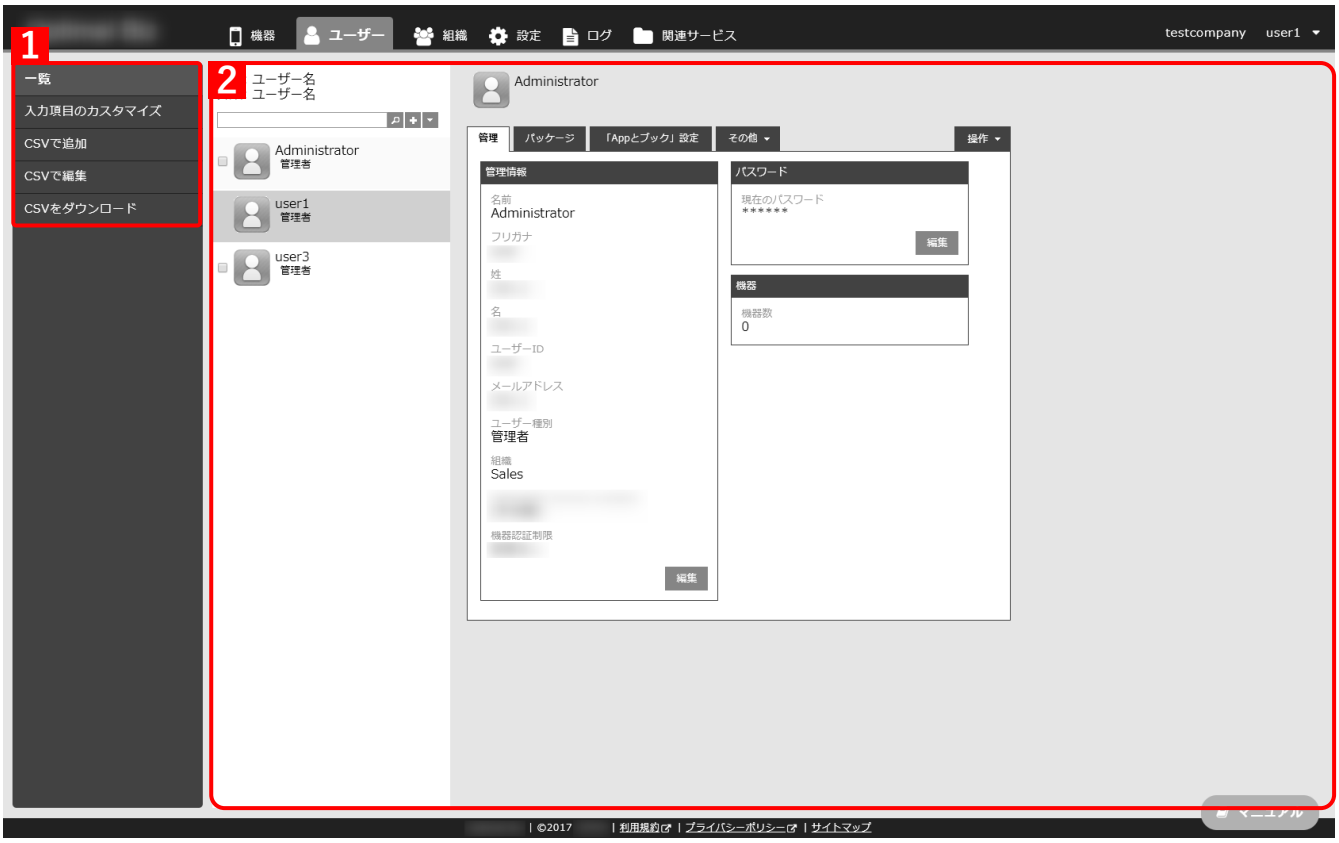
機器の登録、各機能の設定セットの適用など、登録機器に対する各種操作ができます。

項番	項目	説明
1	サイドメニュー	設定できるメニューが表示されます。詳細は、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「機器」 ●一覧 登録機器の情報を表示します。対象の機器に対して各種設定、操作、情報などの確認や機器の検索、絞り込み、並べ替え、機器の一括削除、機器の新規登録もできます。また各機器をクリックすると、(A) 画面右側に「詳細情報」が表示されます。 ●ネットワークマップ 機器のネットワーク接続状況をネットワークマップで確認できます。 ●認証手順 エージェントアプリのダウンロード先や企業コード、認証コードを確認できます。 ●全機器一括設定 すべての機器に対して、各機能の設定セットを一括で適用、変更できます。OS ごとにタブに切り替えて操作します。 ●入力項目のカスタマイズ 部署名や役職名などのような所属を区別する「分類」と、資産番号など必要な情報の入力欄を作成する「自由入力」で、必要な項目を作成できます。 ●メッセージ通知 任意のメッセージを作成して Android 機器や iOS 機器に配信できます。グループ単位、機器単位に配信したり、定期的にスケジュールを指定して配信したり、配信履歴を確認もできます。機器の一覧の詳細情報では、機器ごとに配信予定および配信済みのメッセージを確認できます。 ●CSV で追加 ●CSV で編集 ●CSV をダウンロード 複数の機器情報をまとめて登録したいときや編集したいとき、機器情報のレポートや機器にインストールされているアプリのレポートを作成したいときに CSV ファイルを使用して作業できます。
2	詳細	項番 1 で選択したメニューの詳細が表示されます。詳しくは、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「機器」

2.2.3 ヘッダーメニュー「ユーザー」

ユーザーについて情報の確認、追加、削除、編集ができます。

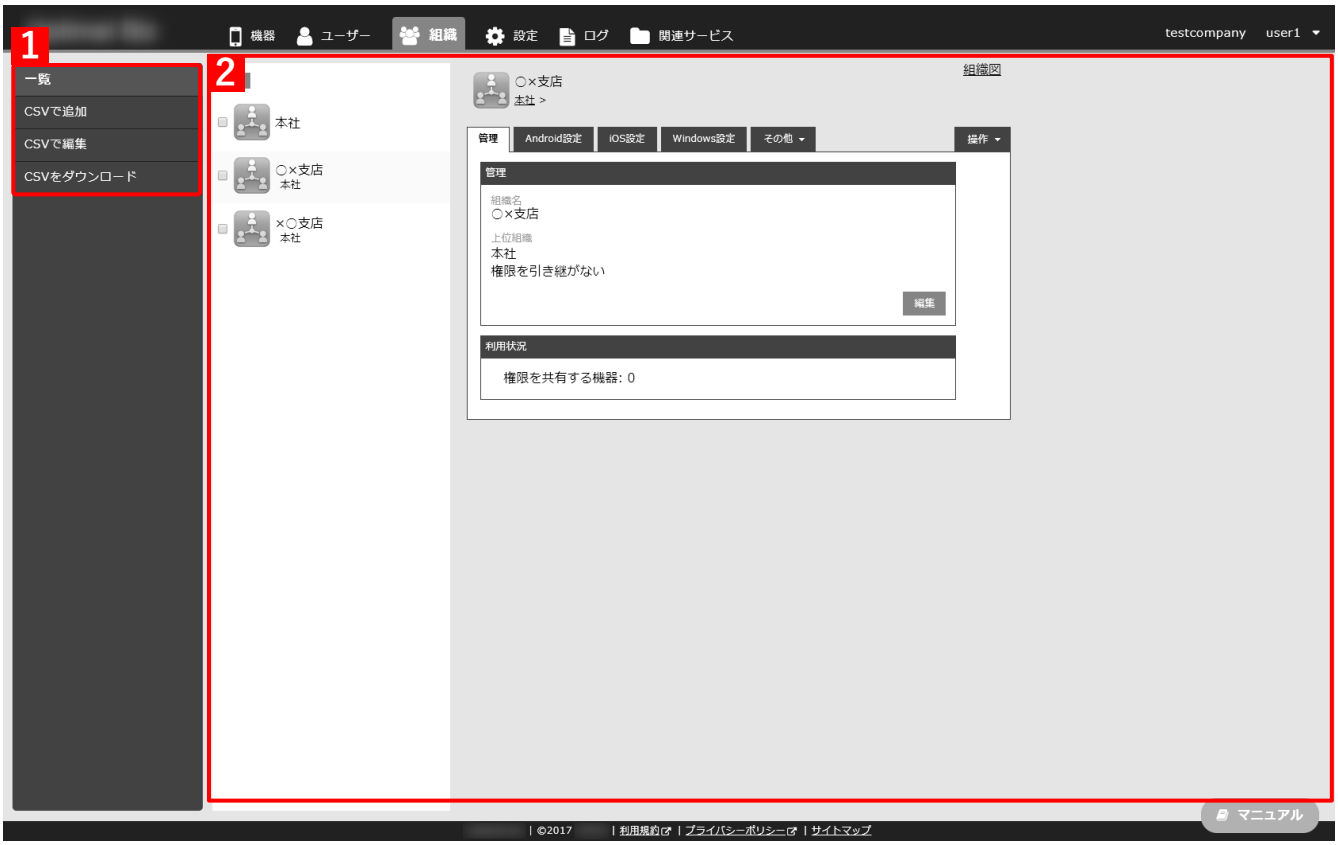
ご契約により表示される内容は異なります。



項番	項目	説明
1	サイドメニュー	設定できるメニューが表示されます。詳細は、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 ユーザーの一覧では、ユーザーの新規作成、情報確認、削除、編集を行います。 ●入力項目のカスタマイズ ユーザーの入力項目のカスタマイズでは、ユーザーをグループ分けするなどのような所属を区別する「分類」と、社員番号や、生年月日などユーザーごとに必要な情報の入力欄を作成する「自由入力」で、必要な項目を作成できます。作成したグループから選択する「分類」と、自由に項目を作成できる「自由入力」の 2 つがあります。 ●CSV で追加 ●CSV で編集 ●CSV をダウンロード 複数のユーザー情報をまとめて登録したいときや編集したいとき、すべてのユーザー情報が記載されたレポートを作成したいときに CSV ファイルを使用して作業できます。
2	詳細	項番 1 で選択したメニューについての詳細が表示されます。詳しくは、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』「ユーザー」

2.2.4 ヘッダーメニュー「組織」

組織についての情報の確認、追加、削除、編集ができます。

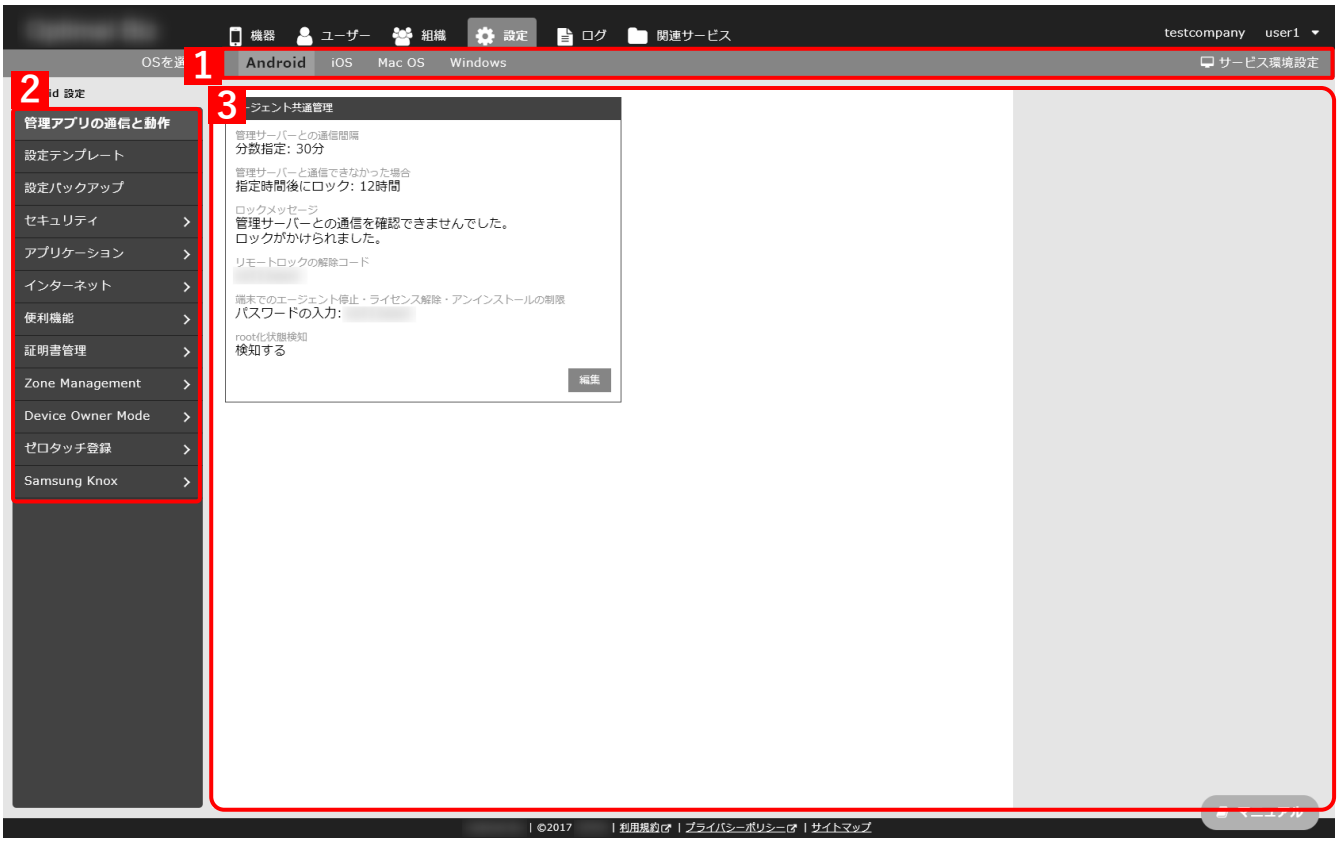


項番	項目	説明
1	サイドメニュー	設定できるメニューが表示されます。詳細は、以下を参照してください。 『管理サイト リファレンスマニュアル』の「組織」 ●一覧 「機器」や「ユーザー」を所属組織の新規追加や削除ができます。 ●CSV で追加 ●CSV で編集 ●CSV をダウンロード 複数の組織情報をまとめて登録したいときや編集したいとき、すべての組織情報が記載されたレポートを作成したいときに CSV ファイルを使用して作業できます。
2	詳細	項番 1 で選択したメニューについて詳細が表示されます。 『管理サイト リファレンスマニュアル』の「組織」

2.2.5 ヘッダーメニュー「設定」

PC（Windows や Mac OS を搭載するパソコン）、Android 端末や iOS 端末に対するセキュリティ設定などを行う、設定セットを作成できます。

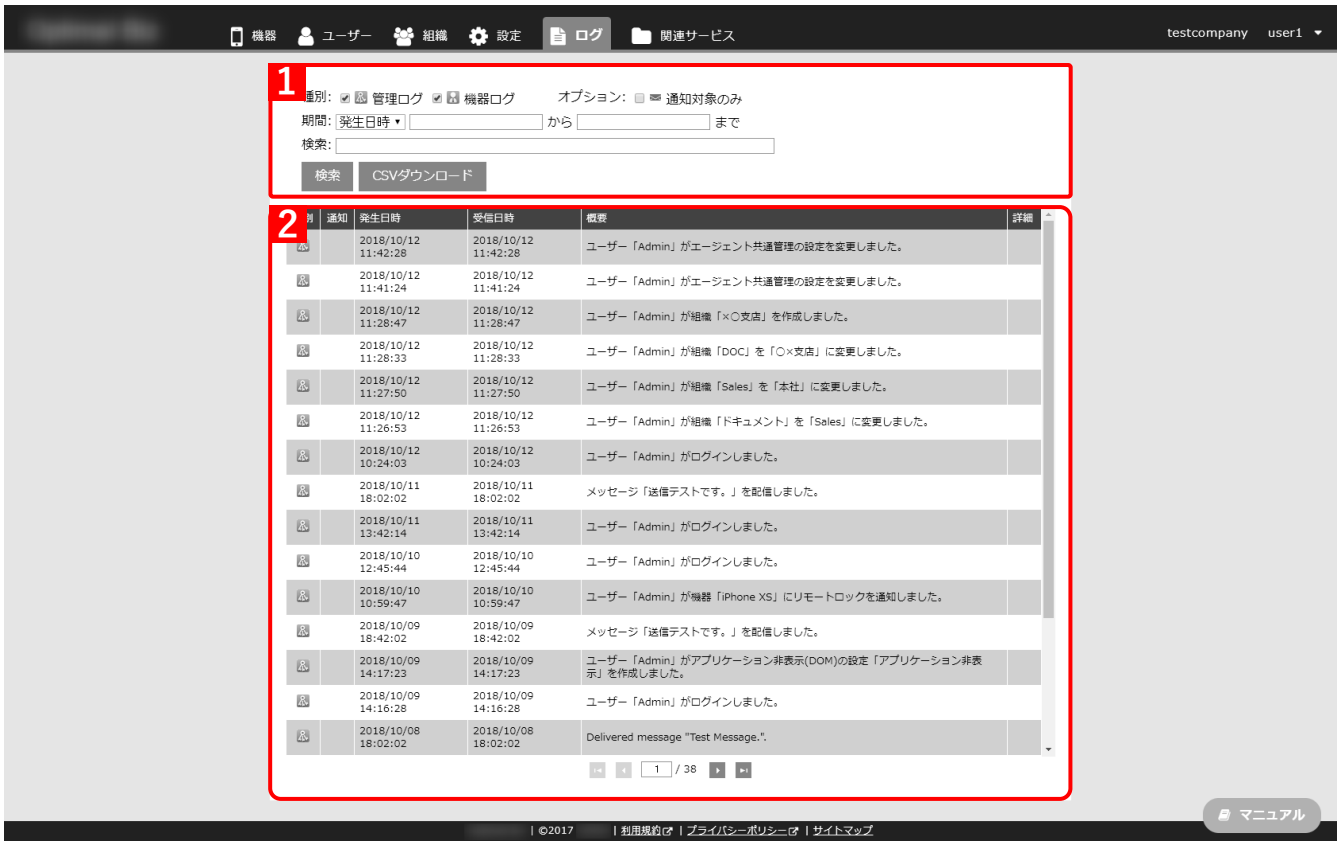
ご契約により表示される内容は異なります。



項番	項目	説明
1	サブヘッダーメニュー	設定を行う OS を以下より選択します。 ●Android ●iOS ●Mac OS ●Windows ●サービス環境設定
2	サイドメニュー	項番 1 の「サブヘッダーメニュー」で選択した項目に対するメニューが表示されます。
3	詳細	項番 2 で選択したメニューについての詳細や選択項目が表示されます。詳細は、項番 2 の各項目でご案内している参照先をご覧ください。

2.2.6 ヘッダーメニュー「ログ」

ログでは管理サイトの操作状況や、機器に対する設定・操作の発生時間、操作概要を確認できます。



項番	項目	説明
1	検索条件	表示するログを絞り込むための条件を設定できます。詳細は、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「ログ」－「ログ画面の見かた」－「画面（ログの絞り込み）」
2	詳細	項番 1 で設定した検索条件の結果が表示されます。詳細は、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「ログ」－「ログ画面の見かた」、「ログ一覧」

2.3 OS ごとの管理手法の違いについて

OS により管理方式が異なります。

管理方式の違いにより、各機器への制御内容や取得できる情報も異なります。

◆管理方式

項目	説明
Android	●エージェント
iOS	●MDM 構成プロファイル ●エージェント（任意）
Mac OS	●MDM 構成プロファイル
Windows	●エージェント

◆Push サーバー

項目	説明
Android	●独自 Push 方式
iOS	●Apple Push Notification Service
Mac OS	●Apple Push Notification Service（以降、「APNs」と記載）
Windows	●独自 Push 方式

◆自動同期のタイミング

項目	説明
Android	●10 分から月 1 まで選択可能（デフォルト 30 分）
iOS	●8 時間毎（処理状況に左右される）
Mac OS	●8 時間毎（処理状況に左右される）
Windows	●10 分から月 1 まで選択可能（デフォルト 30 分）

2.4 エージェントとは

Android 端末、iOS 端末および Windows 端末を本製品で管理するために、管理対象の機器へインストールする本製品のアプリです。このアプリが本製品の管理サーバーと通信することで、管理サイト上で確認できる情報が更新されたり、機器の制御や設定を行えます。

エージェントは、どの企業／組織に紐づく機器なのかを識別するため、インストール後の初回起動時に認証を行う必要があります。

認証が解除されたり、エージェントがアンインストールされた場合、管理サイトから機器の情報を確認したり、制御を行えなくなります。

Android 端末や Windows 端末では、認証解除やアンインストールをできないよう制御もできます。

2.5 MDM 構成プロファイル

MDM 構成プロファイルとは、iOS 端末と Mac OS 端末を本製品で管理するために、本製品から配布される設定ファイルです。MDM 構成プロファイルが端末利用者によって削除された場合、管理サイトから機器の情報を確認したり、制御を行えなくなります。

2.6 同期とは

管理サイトで行った各種設定を機器に反映させたり、各機器の Web 閲覧履歴や位置情報など、管理サイトで保持している機器情報の更新を行うときに「同期」を行います。

通常、同期は定期的に行われますが、管理サイトで行った各種設定をすぐに反映させたい場合は「手動同期」を行います。手動同期を行うには、管理サイトの機器画面内に表示されている 同期 をクリックします。お急ぎの場合は、各端末側のエージェントもしくはポータル画面内からも、同期を行ってください。

定期的な同期のタイミングは、以下を参照してください。

「自動同期のタイミング」19 ページ

各端末側からの同期方法の詳細は、以下のマニュアルを参照してください。

- 『Android クライアント リファレンスマニュアル』の「エージェントの基本操作」－「Android 端末から管理サイトと同期する」
- 『iOS クライアント リファレンスマニュアル』の「ポータルの使用方法」－「iOS 端末から管理サイトに同期する」
- 『Windows クライアント リファレンスマニュアル』の「エージェントの基本操作」－「Windows 端末から管理サイトに同期する」

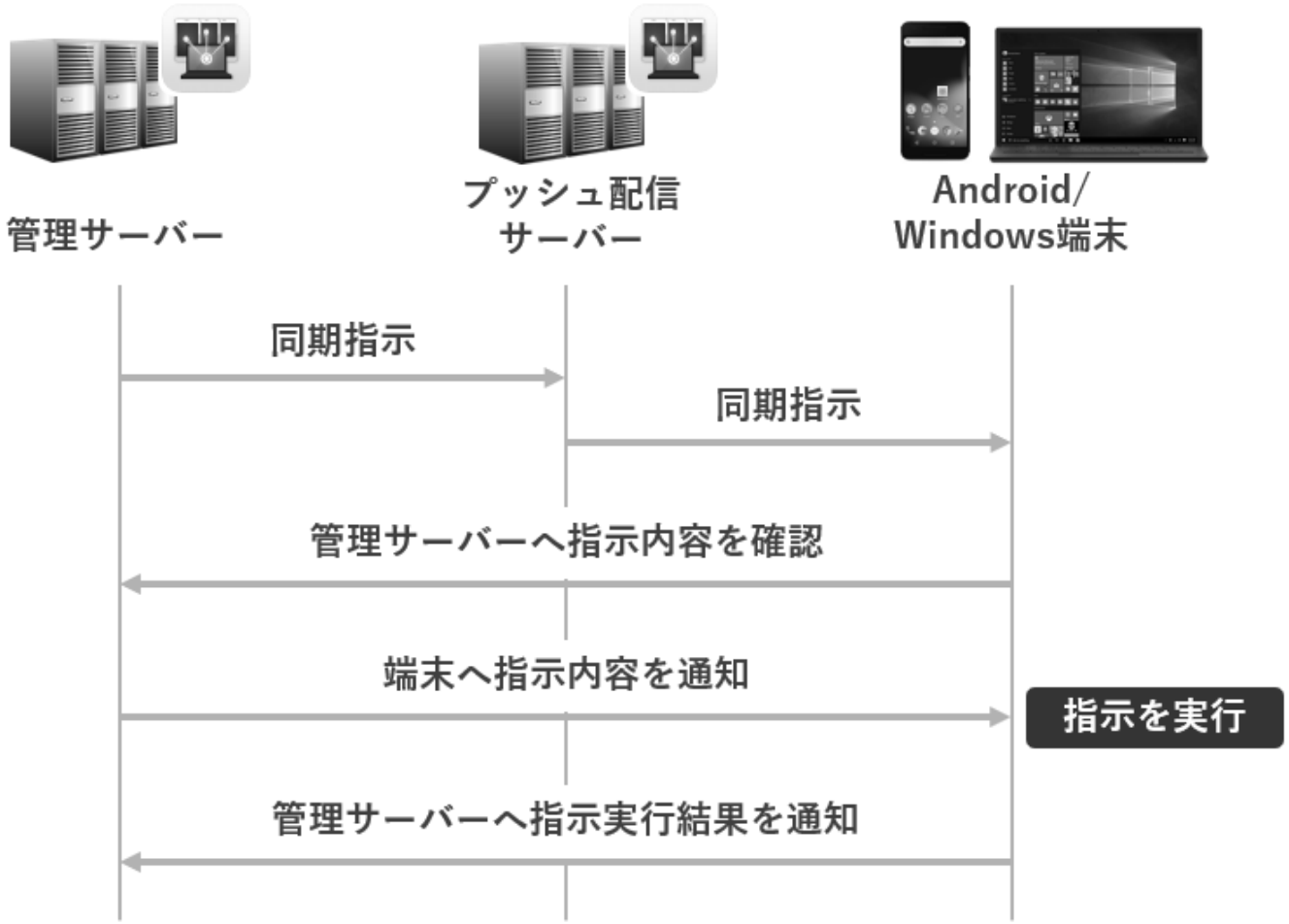
Windows 端末では、スリープ、ハイバネーション、休止状態から起動した場合は、同期がされない場合があります。

2.6.1 同期の仕組み

端末と管理サイト間での同期は、OS ごとに仕組みが異なります。

◆Android／Windows

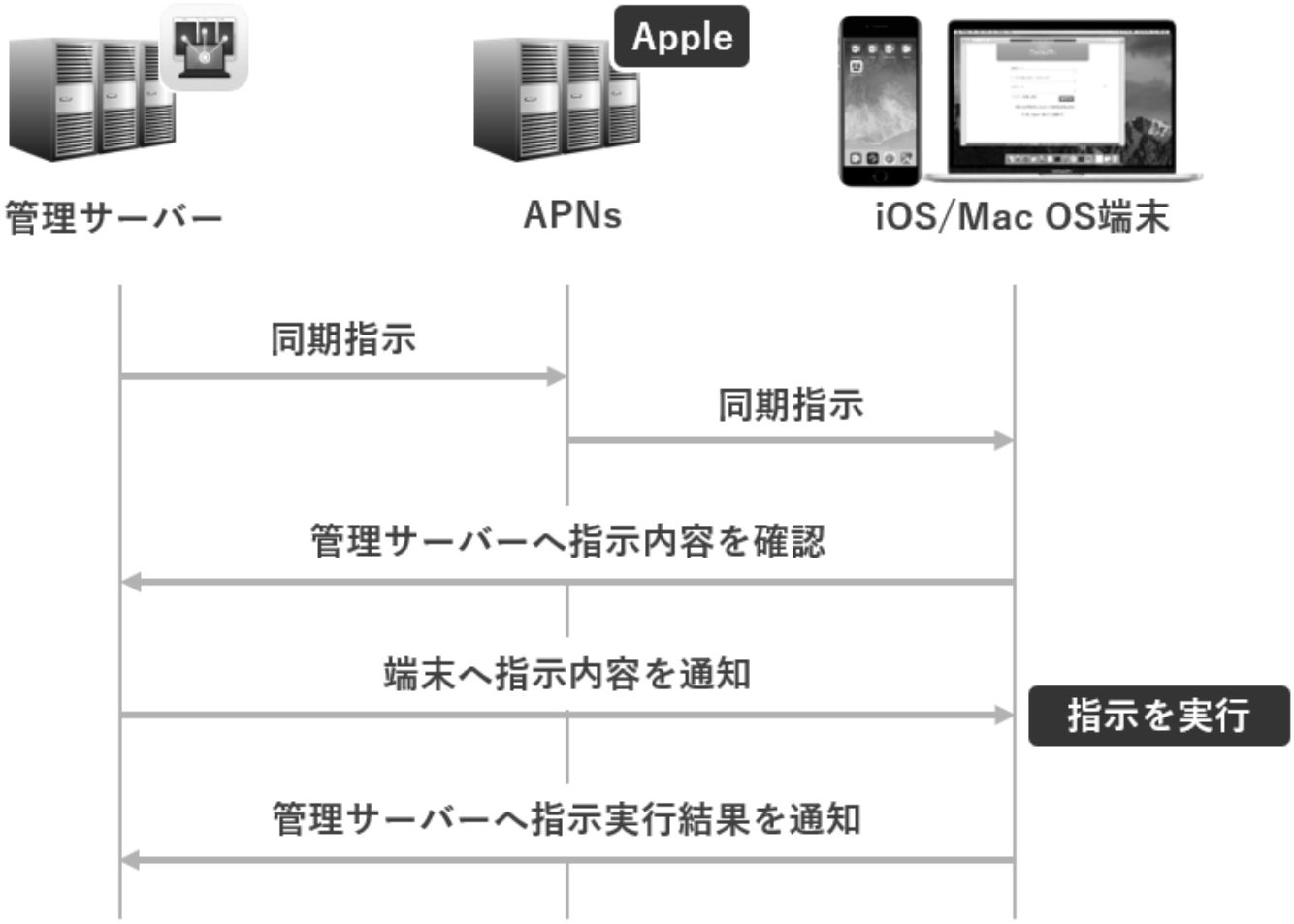
Android 端末または Windows 端末が本製品の管理サーバーと同期するには、プッシュ配信サーバーを経由しますが、本製品では独自のプッシュ配信サーバーを経由します。



◆iOS／Mac OS

iOS 端末または Mac OS 端末が本製品の管理サーバーと同期するには、必ず APNs と呼ばれるプッシュ配信サーバーを経由します。APNs は Apple が提供しているサーバーであり、本製品利用時には APNs と通信できる状態で端末を運用する必要があります。

APNs は管理サーバーおよび端末側から同期の指示があったことを知らせる役割を担います。そのため、同期指示があることを相手に知らせたあとは管理サーバーと端末間で直接通信を行います。

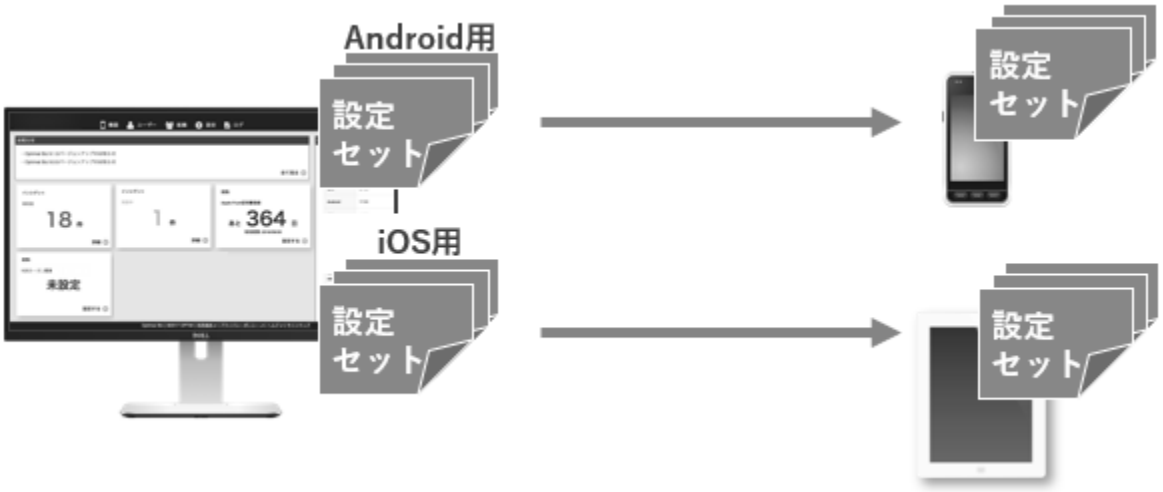


2.7 機器への設定方法

2.7.1 設定セットとは

機器に対して設定を配信するには、「設定セット」と呼ばれる、機器に対する設定を管理サイト上で定義したものを作成し、機器へ適用する必要があります。

設定セットの配信対象は、「機器」または「ユーザー」、もしくは「組織」から選択できます。



3 本製品の基本操作

3.1 管理サイトにログインする

管理サイトのログイン画面を表示して、管理サイトにログインします。

管理サイトの URL、企業コード、ユーザーID またはメールアドレス、パスワードについては、本製品購入時にメールなどで送付されています。あらかじめご用意ください。

【1】ログイン画面を表示します。
【2】「企業コード」、「ユーザーID またはメールアドレス」、「パスワード」を入力します。
【3】［ログイン］をクリックします。

詳細は、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「基本操作」－「ログイン／ログアウト」－「ログイン」

3.2 管理サイトからログアウトする

管理サイトからログアウトしたり、別のユーザーでログインしたい場合は、以下の操作でログアウトします。

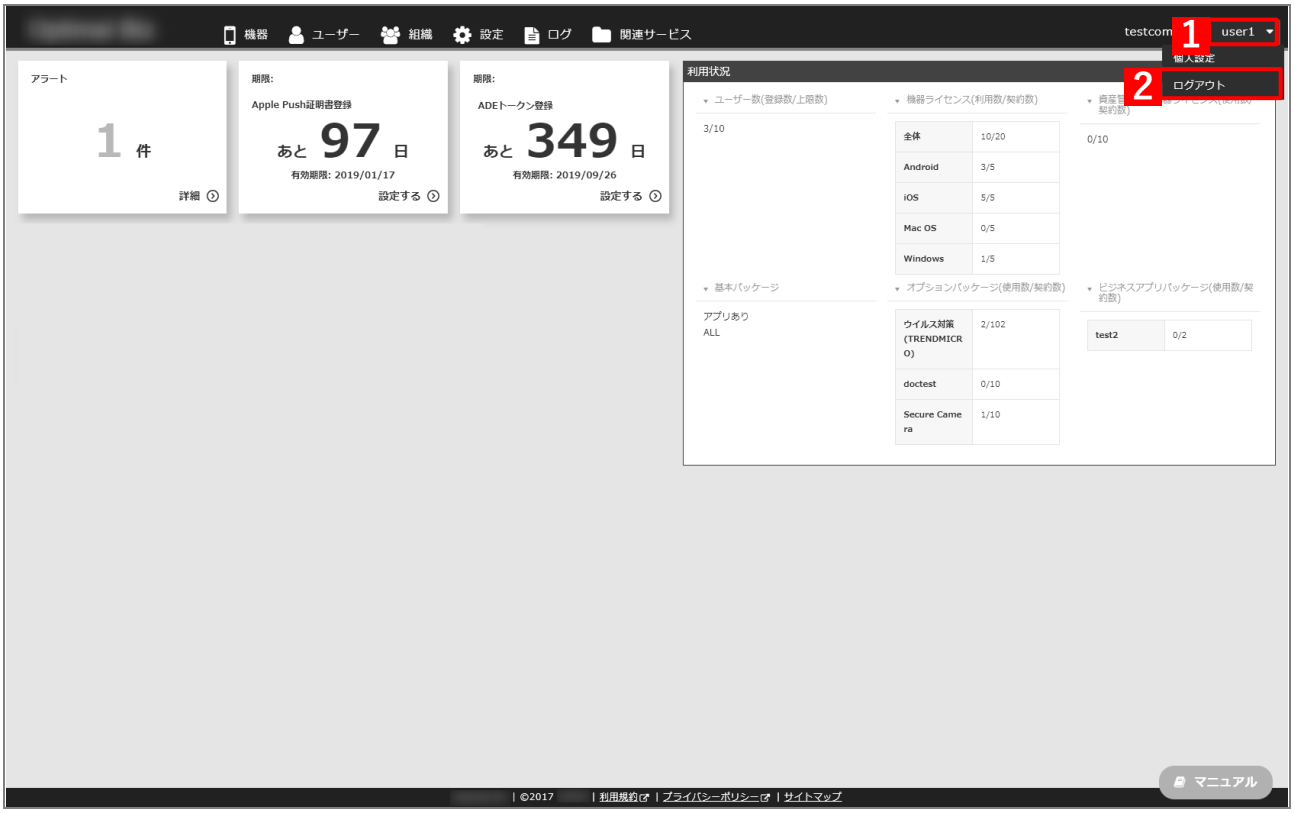
【1】ログイン情報の［ユーザー名］をクリックします。

【2】［ログアウト］をクリックします。

⇒「ログアウトしました。」とメッセージが表示されます。

別のユーザーでログインする場合は、以下を参照してください。

「管理サイトにログインする」26 ページ



詳細は、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「基本操作」－「ログイン／ログアウト」－「ログアウト」

3.3 機器を検索する

機器の情報を確認するときや、機器に対しリモートロックやリモートワイプなどを行うときに対象の機器を管理サイト上で特定する必要があります。

ここでは、機器に紐づく情報（「モデル名」が「iPhone」）から機器を検索するときの操作手順をご紹介します。

【1】［機器］をクリックします。

⇒［一覧］が表示されます。

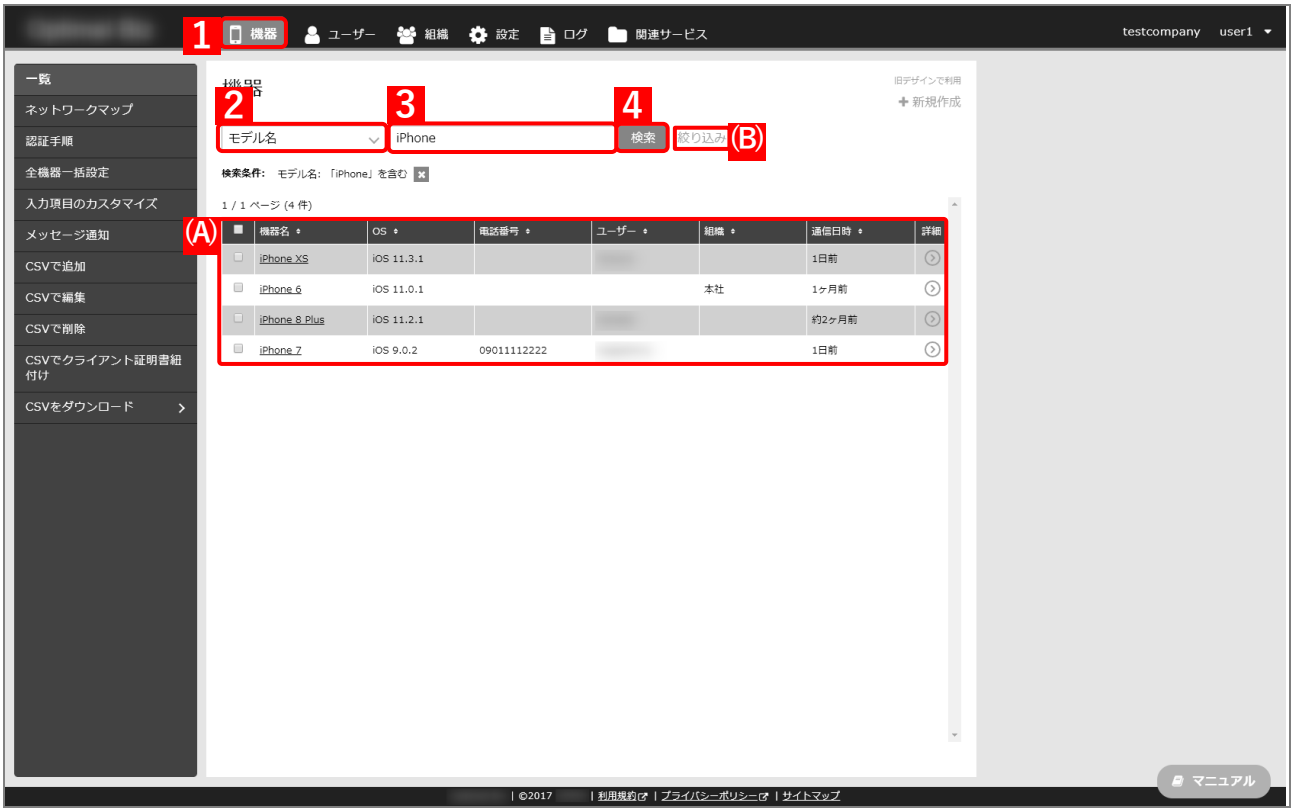
【2】「機器検索」のリストボックスからカテゴリを選択します。

【3】テキストボックスに検索するキーワードを入力します。

（B）「絞り込み」をクリックすると、「OS」や「OS バージョン」などの詳細で検索を絞り込めます。

【4】［検索］をクリックします。

⇒（A）検索結果が表示されます。



詳細は、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「機器」－「一覧」

3.4 設定セットを作成、複製する

機器に対して設定を配信または制御を行うには、管理サイト上で「設定セット」を作成し、機器へ適用する必要があります。作成した設定セットは、「機器」または「ユーザー」、もしくは「組織」に対して割り当てられます。

ここでは、Android 端末の画面ロック設定の設定セットを作成する手順および複製する手順をご紹介します。

「画面ロック」の詳細は、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」－「セキュリティ」－「画面ロック」

「複製」の詳細は、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「基本操作」－「設定画面の共通操作」－「複製」

3.4.1 設定セットを作成する

【1】［設定］→［Android］→［セキュリティ］→［画面ロック］→ ＋ をクリックします。

画面ロックの設定セットは、最大 50 件まで作成できます。作成する設定セットによって、作成できる最大数は異なります。

【2】「設定名」や「パスワードポリシー」などの項目について設定を行います。

【3】［保存］をクリックします。

【4】作成した設定セットを「機器」または「ユーザー」、もしくは「組織」に対して割り当てます。

詳細は、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「機器」－「一覧」－「機器の設定」

『管理サイト リファレンスマニュアル』の「ユーザー」－「一覧」

『管理サイト リファレンスマニュアル』の「組織」－「組織」－「一覧」－「［Android 設定］タブ／［iOS 設定］タブ／［Windows 設定］タブ」

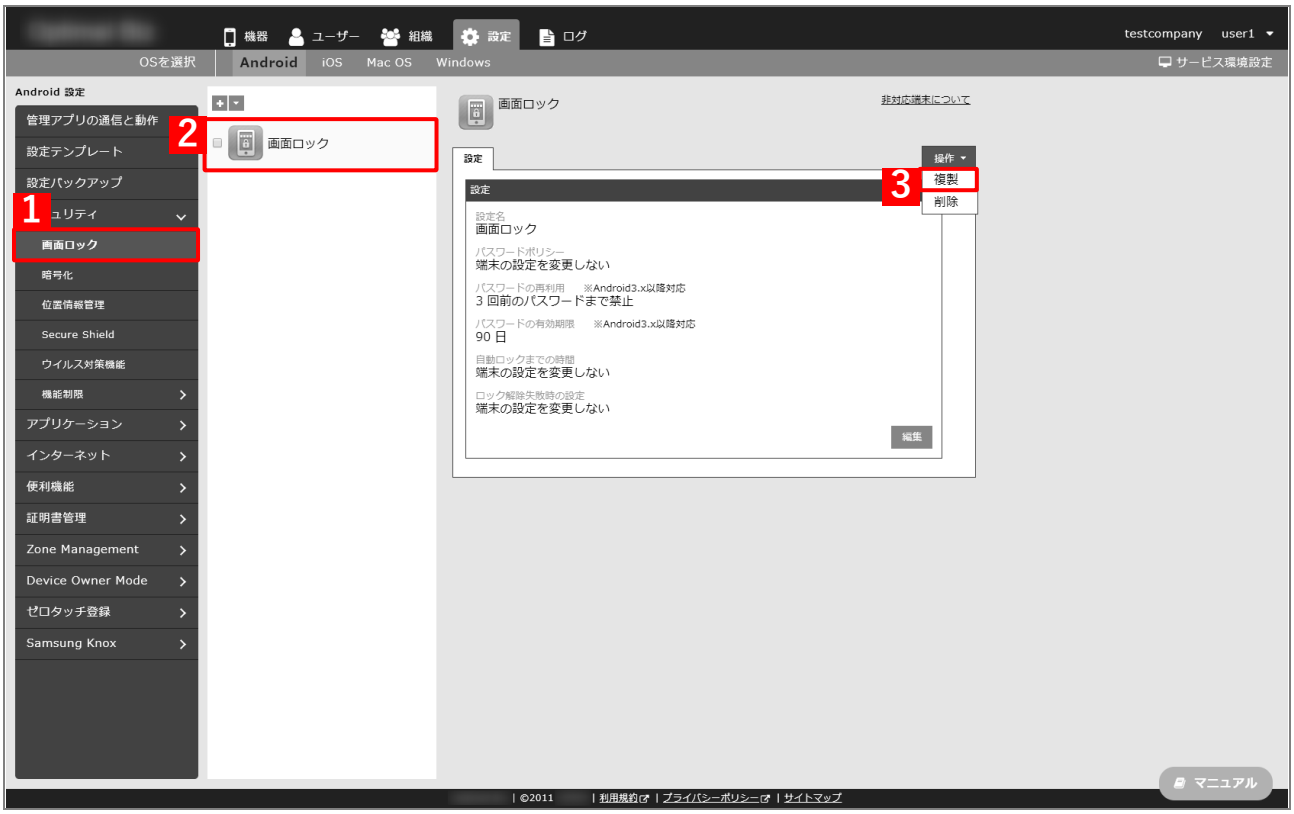
3.4.2 設定セットを複製する

【1】［設定］→［Android］→［セキュリティ］→［画面ロック］をクリックします。

【2】一覧から複製元にする設定セットを選択します。

【3】［操作］→［複製］をクリックします。

⇒設定を複製し、新規作成画面に切り替わります。「設定名」を含め、設定を変更してください。



【4】［保存］をクリックします。

3.5 ログを確認する

管理サイト上から、管理者が行った操作や機器への設定、アプリ配信状況などをログ画面から確認できます。

ここでは、Android 端末へ行ったリモートロックの反映状況を確認する手順をご紹介します。

【1】［ログ］をクリックします。

【2】「検索」欄にキーワードの「リモートロック」を入力します。

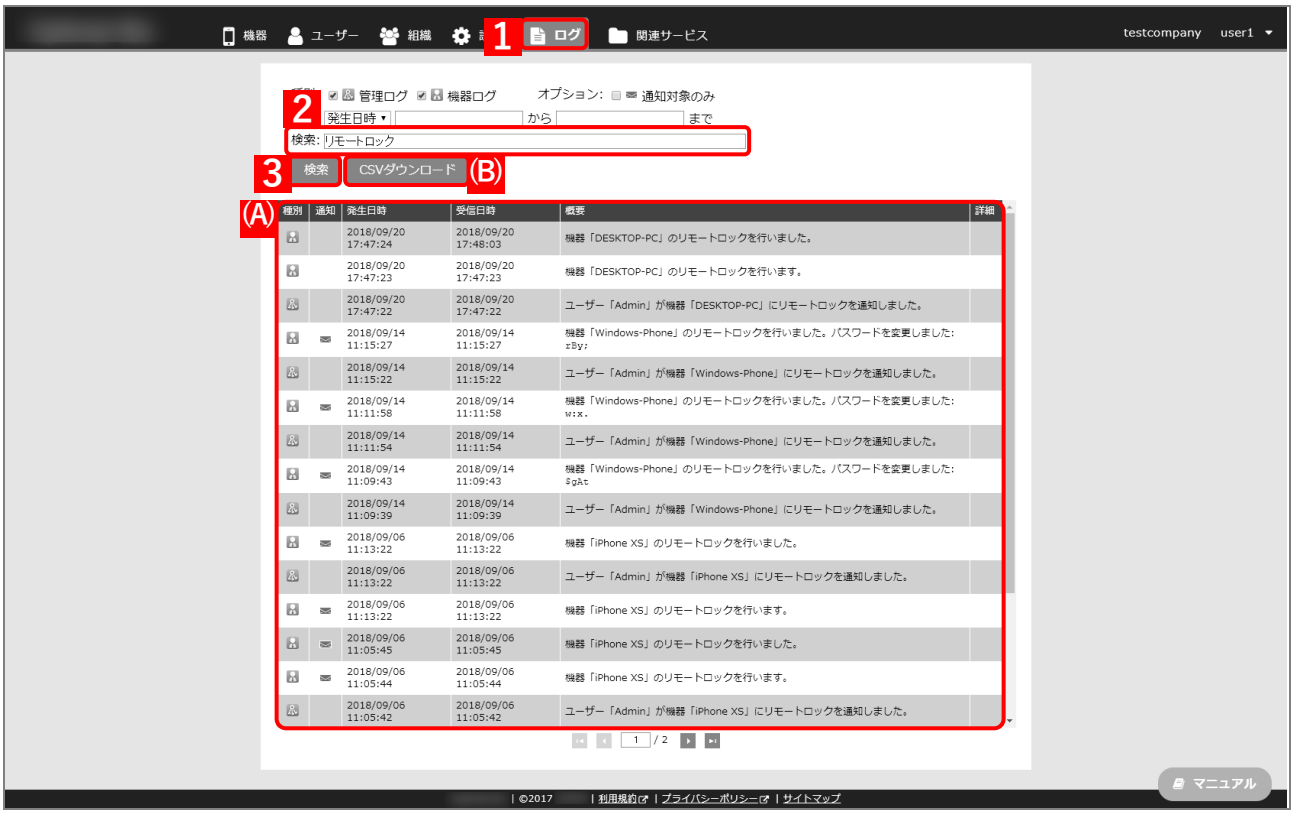
【3】［検索］をクリックします。

⇒検索条件である「リモートロック」に一致したログが（A）「検索結果」に表示されます。

機器「○○」のリモートロックを行います。　：　リモートロックが設定された記録です。
機器「○○」のリモートロックを行いました。：　リモートロックが行われた記録です。

空欄で［検索］をクリックすると、記録されているログの一覧が表示されます。

（B）［CSV ダウンロード］をクリックすると、絞り込んだ結果を CSV ファイルとしてダウンロードできます。



詳細は、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「ログ」

4 本製品を導入する

本製品を導入するときの流れは以下のとおりです。

各項目の具体的な操作手順については、以下の各マニュアル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』
- 『Android キッティングマニュアル』
- 『iOS キッティングマニュアル』
- 『Mac OS キッティングマニュアル』
- 『Windows キッティングマニュアル』

4.1 導入目的を決定する

機器の導入目的および本製品の導入目的を決定します。

機器および本製品の導入によってどのようなメリットを得たいのか整理し、導入目的を決定します。すでに機器を導入しており、あとから本製品を導入する場合は、機器運用上発生している課題を並べ、どう解決したいのかを整理します。

なお、導入後も管理対象機器の OS を変更する、機器を追加する場合は、随時導入目的の見直しを行ってください。

例：営業スタッフへのスマートフォン新規導入の場合

◆機器の導入目的

●営業スタッフの業務効率化および労働環境の改善。

・外出先からもスムーズにメールやスケジュールなどを利用できるようにする。

・顧客に関する情報収集を移動中にも行えるようにする。

◆本製品の導入目的

●メールや電話帳などの利用により、端末内に機密情報が含まれるため、最低限のセキュリティポリシーの適用を行い、機器紛失時の情報漏えいリスクを低減する。

・スクリーンロック設定などを適用する。

●不正な利用を抑止することで、業務に集中できる環境を提供する。

・業務で利用しないアプリや、サイトへのアクセスを禁止する。

●業務で利用するアプリの展開コストを削減する。

・業務で利用するアプリを利用者の手間なくインストールする。

4.2 導入機器／OS を決定する

導入機器および OS 種別を決定します。

「導入目的を決定する」で定めた目的に合う機器および OS 種別を選択してください。

なお、Android 端末および iOS 端末では機種ごとに本製品の動作状況を確認しており、対応機種一覧をご用意しております。必ず導入前に対応機種であることをご確認ください。

☞デバイス一覧：https://www.kddi.com/business/security-managed/security/kddi-smsm/device/

本製品は Android 端末、iOS 端末、Mac OS 端末、Windows 端末の管理ができ、OS ごとにサポートするバージョンを取り決めた OS サポートポリシーがあります。導入機器や OS 種別の決定までに必ずご確認ください。

『Android クライアント リファレンスマニュアル』

『iOS クライアント リファレンスマニュアル』

『Windows クライアント リファレンスマニュアル』

『Mac OS クライアント リファレンスマニュアル』

4.3 導入範囲／スケジュールを決定する

どの組織にいつから導入するのか計画を立て、導入範囲や導入スケジュールを決定します。

スマートデバイスを初めて導入する場合は、数台から百台程度の最小構成で運用を開始し、徐々に台数を増やしていくことを推奨します。

4.4 セキュリティポリシー／設定内容を検討する

スマートデバイスに適用すべきセキュリティポリシーを検討します。

「導入目的を決定する」で定めた目的、組織内の情報セキュリティガイドライン、端末で扱う情報に応じたポリシーとなるようご検討ください。

なお、以下のポリシーについては最低限適用することを推奨しています。

●暗号化設定

●スクリーンロックポリシー設定

端末で顧客情報など機密情報を取り扱う場合は、外部デバイスの接続制御もあわせて行うことを推奨します。

●Android端末： USB ファイル転送制御、SD デバイスなどの物理外部メディアへのマウント制御など

●Windows 端末： USB デバイス、SD デバイスなどの制御など

その他、必要な設定内容を検討します。

端末利用者に活用してもらいたい業務アプリの洗い出しも行います。

注意

Android 端末や iOS 端末では、工場出荷初期状態でないと設定および利用ができない、特殊なモードおよび導入プログラムが存在します。必ず、機器導入前に設定要否を検討してください。

Android 端末

●Device Owner Mode

Device Owner とは機器を管理するためのアプリ（エージェントアプリ）に持たせられる特別な権限のことです。その権限を持っている状態のことを Device Owner Mode(以降、「DOM」と記載)と呼びます。

- Android 6.0 以上の端末では、必ずエージェントアプリを DOM 化する必要があります。
- エージェントアプリを DOM 化すると、Google が提供する Android 端末の管理プログラム「Android Enterprise」の「Full Device Management」を利用できます。
- DOM 化するには、端末が工場出荷初期状態である必要があります。

●Tips

・Android Enterprise とは、端末やアプリを従業員に配備し、企業データを安全に保つために Google が提供している法人向けプログラムです。Android Enterprise ではいくつかの機能がありますが、本製品ではこのうち Full Device Management に対応しています。Full Device Management への対応により、本製品では企業所有の端末に適した端末管理を行えます。マルチユーザーの利用制限、スクリーンショットの利用制限など堅牢なセキュリティ対策を実現します。

iOS 端末

●Automated Device Enrollment（以降、「ADE」と記載）
Apple が提供する Apple Business Manage で、iOS 端末の導入を支援する機能です。詳細については、以下を参照してください。

☞『iOS 端末の導入』41 ページ

ADE の利用は必須ではありませんが、端末利用者が本製品の管理下から抜けることを防げるため、Bring Your Own Device（自分のデバイスを持ち込む／以降、「BYOD」と記載）ではなく会社からの支給端末へ本製品を導入する場合は、ADE の利用を推奨します。

端末を新規導入するときは、ADE 端末を購入することで、管理者自身で ADE 端末へと設定変更する必要がありません。詳しくは、ADE 端末の販売元へお問い合わせください。

●監視対象モード（Supervised mode）
組織が端末をより強固に管理するためのモードのことです。

監視対象モードの利用は必須ではありませんが、多くのメリットがあるため、BYOD ではなく会社からの支給端末へ本製品を導入する場合は、本モードに切り替えることを強く推奨します。

監視対象モードにするには、端末が工場出荷初期状態である必要があります。

監視対象モードの利用には大きく 3 つのメリットがあります。

- 本製品から制御できる設定項目が増えます。
  アプリケーション禁止設定や、ソフトウェアアップデートの遅延設定など、監視対象モードでしかできない設定があり、これらの設定項目を利用できるようになります。
- アプリのサイレントインストールができます。

  利用規約への同意や、Apple ID のパスワード入力を求められることがあります。
- 紛失モードによるリモートロック、位置情報取得
  監視対象モードでない場合、端末紛失時にリモートロックを指示しても、第三者の不正操作により端末側のスクリーンロックを解除される可能性が残ります。
  一方、監視対象モードの場合は紛失モード（ロストモード）と呼ばれる特殊な状態でロックがかかるため、管理者からロック解除指示を出さない限り、解除できません。

  紛失モードでは端末側の位置情報取得設定状態によらず、位置情報を取得し管理サイトに表示できます。

4.5 契約プランを検討する

検討したセキュリティポリシーおよび設定内容に合う本製品の契約プランを選択します。

満たすべきポリシーと予算を踏まえ、適切な機能を選択し、必要に応じて追加オプションもご検討ください。

各オプションで利用できる機能は、以下の機能一覧をご覧ください。

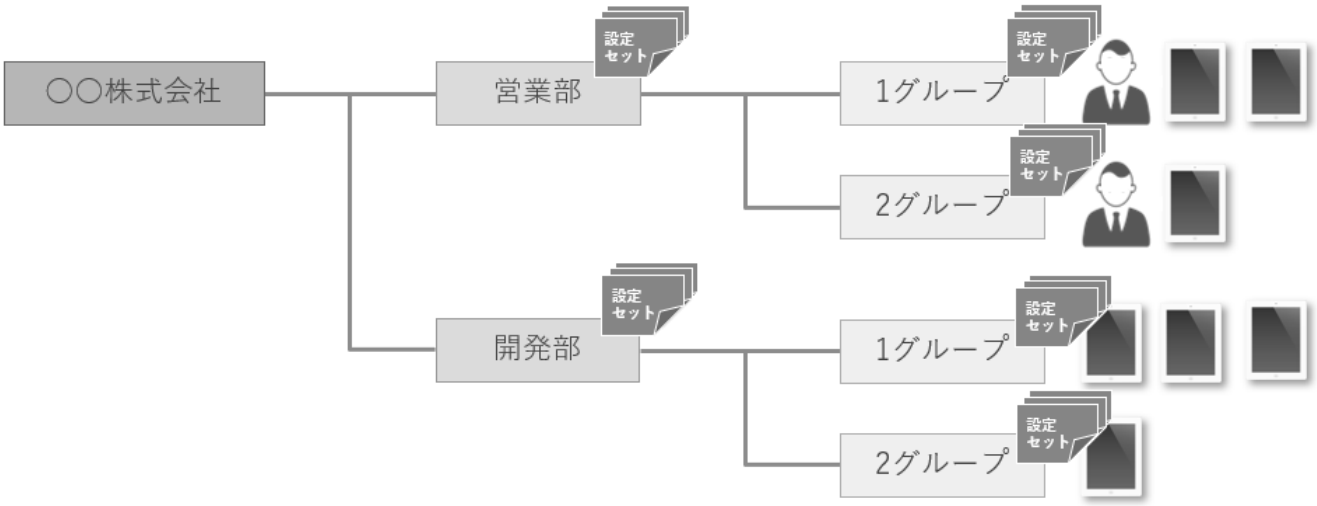
☞本製品機能一覧：https://www.kddi.com/business/security-managed/security/kddi-smsm/function/

4.6 組織／ユーザー／機器構成を検討する

組織／ユーザー／機器をそれぞれどう紐づけるかを検討します。

本製品では、ユーザーや機器を組織構成で管理し、階層構造を構築できます。1 台ごとに設定もできますが、組織を活用することで大量の機器に対し、一括で設定の変更ができ、管理者の作業負担を軽減できます。

次から、本製品で設定できる運用パターン例をご紹介します。



4.6.1 パターン A

●組織と機器を紐づける。

●ユーザーは登録しない。

◆想定ユースケース

●特に端末へユーザー情報が紐づかず、組織ごとに一括で設定ができれば良い場合。

◆メリット

●階層数にもよりますが、シンプルな構成のため管理者の運用負荷が少なくなります。

◆注意

Android Enterprise のご利用には機器とユーザーとの紐づけが必須のため、本パターンはご利用いただけません。パターン B もしくはパターン C をご選択ください。

4.6.2 パターン B

●ユーザーは登録しない。

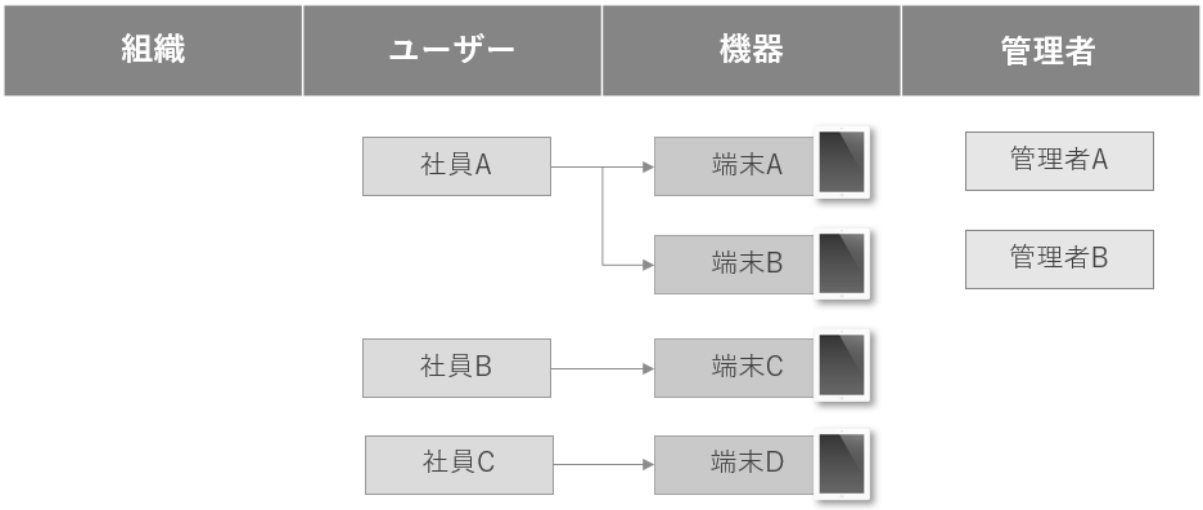
●組織は登録しない。

◆想定ユースケース

●組織ごとに設定を変える必要のない、小規模な運用の場合。

◆メリット

●シンプルな構成のため管理者の運用負荷が少なくなります。



4.6.3 パターン C

●組織とユーザーを紐づける。

●機器使用者をすべてユーザーとして登録し、ユーザーと機器を紐づける。

◆想定ユースケース

●社員が異動したときに端末もあわせて移動し、自動的に異動先の設定セットへ切り替えたい場合。

●Android 端末の機器管理を行う場合。

●Apple School Manager を利用し、教員や生徒に特定の端末を紐づける場合。

◆メリット

●ユーザーが部署を移動したときに、ユーザー変更だけで機器も一緒に移動し、移動先のポリシーを円滑に適用できます。

●Apple School Manager 利用時に Apple が提供するクラスルームアプリ用の設定を端末へ適用できます。

◆Tips

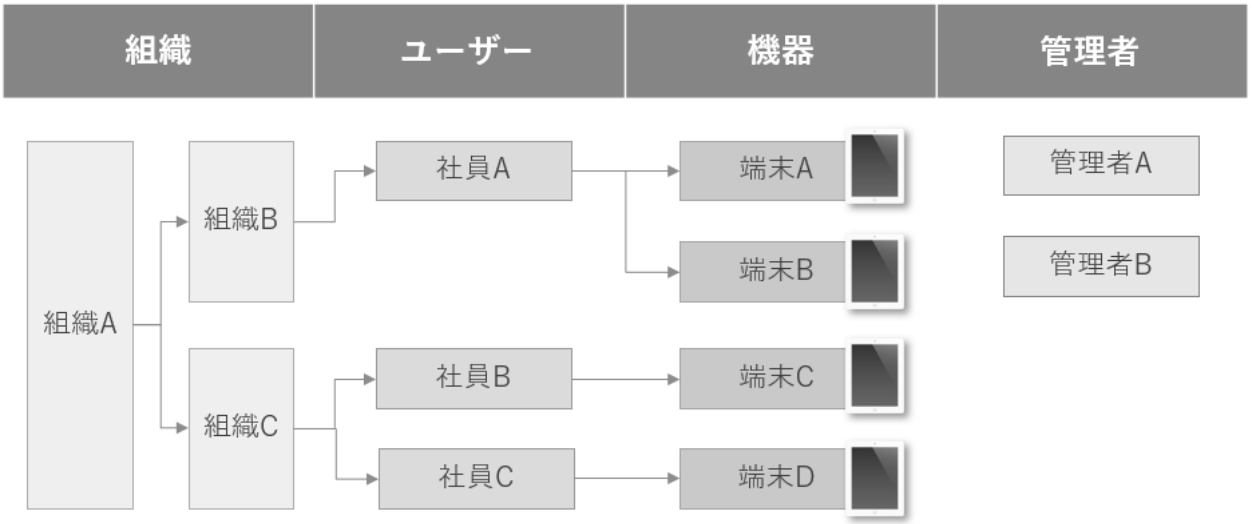
●Android 6.0 以上の Android 端末の管理には、Android Enterprise の利用が必須です。

●Android Enterprise 利用時には、機器とユーザーの紐づけは必須となります。ただし、必ずしもユーザー名などを実在するユーザーとする必要はないので、任意のユーザー名（機器名をそのままユーザー名にするなど）を入力し紐づけを行ってください。

●Apple School Manager 利用時、Apple School Manager のユーザー情報を本製品に反映できます。

◆注意

Android Enterprise の仕組み上、1 ユーザーに対し 11 台以上の機器を紐づけると、機能が正常に動作しないことがあります。1 人が大量の機器を所持する場合は、複数ユーザーを作成し紐づけを行ってください。



5 事前準備をする

5.1 Android 端末の導入

◆Android Enterprise 企業登録

Android Enterprise の機能を利用するためには、Google のサーバーとの連携設定が必要です。詳細については、以下の各マニュアルを参照してください。

『Android キッティングマニュアル』

キッティング方法によっては、最初に選択した方法から別の方法に変更できません。『Android キッティングマニュアル』の「キッティング方法を選択する」をご確認いただき、慎重にご検討のうえ、ご選択ください。

5.2 iOS 端末の導入

◆Apple Push 証明書の登録

Apple Push 証明書とは、APNs の利用に必要な証明書のことです。Apple Push Cretificate Potal より Apple Push 証明書のファイルをダウンロードし、本製品の管理サイトにアップロードする必要があります。

『Apple Push 証明書登録・更新手順 管理者マニュアル』の「Apple Push 証明書登録・削除」－「Apple Push 証明書の登録」

◆Apple Business Manager の事前登録

Apple Business Manager（以降、「ABM」と記載）とは、機器管理者が iOS 端末の導入、コンテンツの購入と配布を円滑に行うための機能を備えた、Apple が提供する Web ベースのポータルサイトです。利用には、Apple との契約および管理サイト上での設定が必要です。Apple との契約には数週間程度かかることがあるため、早めに準備を進めてください。

『Apple Business Manager（ABM）マニュアル（利用方法・年次更新手順)』

◆Automated Device Enrollment（ADE）の事前登録

ADE とは、ABM または ASM で iOS 端末の導入を支援する機能です。利用には、Apple との契約および管理サイトで設定が必要です。

『Apple Business Manager（ABM）マニュアル（利用方法・年次更新手順)』の「Automated Device Enrollment（ADE)」

『Apple School Manager（ASM）マニュアル（利用方法・年次更新手順)』の「Automated Device Enrollment（ADE)」

『iOS キッティングマニュアル』の「ADE を利用してライセンス認証を行う」

◆「App とブック」の事前登録

「App とブック」とは、ABM または ASM で機器管理者がアプリや書籍の購入、配布および管理をするための機能です。利用には、Apple との契約および管理サイトで設定が必要です。

『Apple Business Manager（ABM）マニュアル（利用方法・年次更新手順)』の「App とブック」

『Apple School Manager（ASM）マニュアル（利用方法・年次更新手順)』の「App とブック」

『iOS アプリケーション配信 手順書』

◆監視対象モードへの設定変更

ADE を利用しない場合は、iOS 端末を監視対象モードへ変更する必要があります。変更するには Mac にインストールした Apple Configurator 2 を利用してください。工場出荷初期状態の機器でのみ設定変更ができますので、本製品導入前に準備を行ってください。

5.3 Mac OS 端末の導入

◆Apple Push 証明書の登録

Apple Push 証明書とは、APNs の利用に必要な証明書のことです。

Apple Push Certificate Portal より Apple Push 証明書のファイルをダウンロードし、本製品の管理サイトにアップロードする必要があります。詳細は以下を参照してください。

『Apple Push 証明書登録・更新手順 管理者マニュアル』の「Apple Push 証明書登録・削除」－「Apple Push 証明書の登録」

5.4 Windows 端末の導入

特に必要な準備はありません。

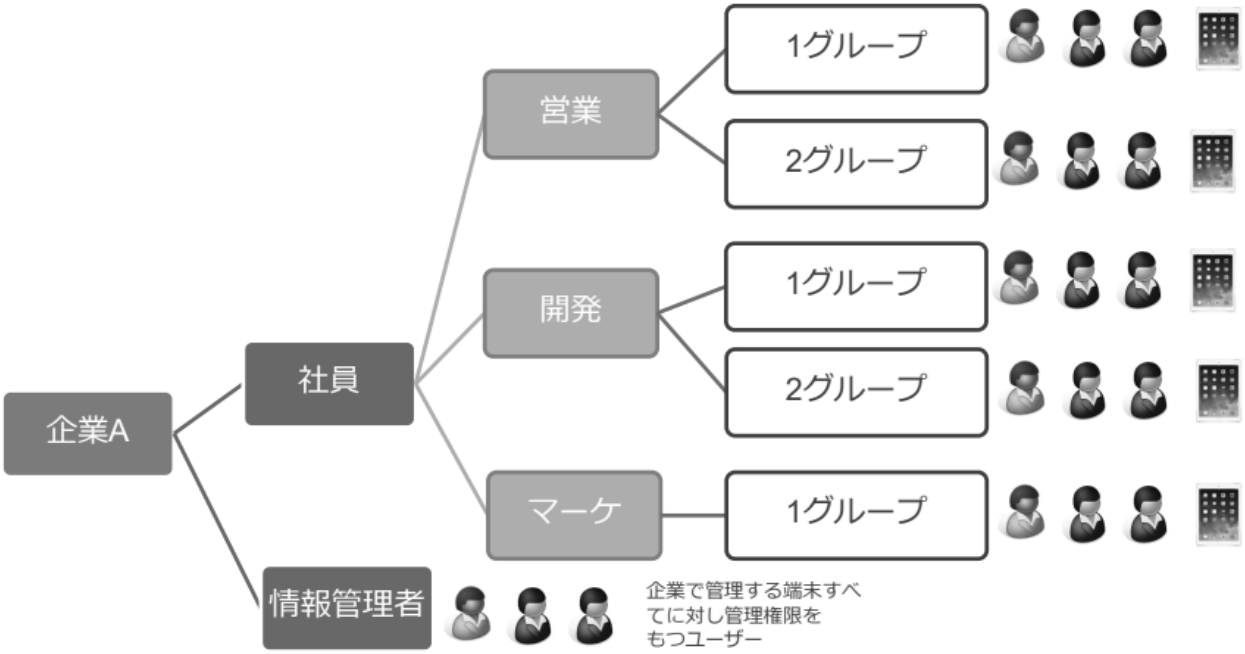
6 ユーザー／組織情報／機器を登録する

「組織／ユーザー／機器構成を検討する」で検討した構成を管理サイトに設定します。

6.1 ユーザー／組織情報／機器を登録する

本製品ではユーザーを組織構成で管理し、階層構造で「組織」や「ユーザー」、「機器」を管理できます。

1台1台の機器に個別設定もできますが、組織ごとに管理すると属性に応じた一括の設定ができるメリットがあり、便利にご利用いただけます。



登録項目	登録	登録のメリット	紐づけ先
機器	●必須	●管理サイトから機器の遠隔操作などができる ●機器の利用制限、アプリ配布ができる ●資産管理に活用できる	●ユーザー ●組織
ユーザー	●一部必須 管理サイトの利用者は登録必須だが、一般ユーザーは登録必須ではない	●管理サイトの利用者の権限管理ができる ●機器とユーザーが紐づく場合、ユーザーの所属する組織に応じた設定ができる	●組織
組織	●必須ではない 10階層まで作成できる	●組織を階層構造にて管理し、一括での設定ができる 「機器⇔ユーザー⇔組織」の紐づけ、もしくは「機器⇔組織」も紐づけができる	●上位組織
ユーザー分類	●必須ではない	●自由入力もしくは分類での登録ができる ●組織以外の分類（役職など）で権限設定を変えたい場合に活用できる	●なし
機器分類	●必須ではない	●自由入力もしくは分類での登録ができる ●ユーザー分類と同じく組織以外での機器分類を設定したい場合に活用できる	●なし

6.1.1 ユーザー／組織とは

ユーザー

ユーザー権限には、種類があります。

それぞれのユーザーにどの権限を付与するかを考え、設定します。

項番	権限	権限内容
1	管理者	すべての操作（項番 2 と 4）が行えます。
2	操作	ロック・ワイプ操作に対して権限を有していないが、管理サイト上でその他の設定の実行権限を有します。
3	閲覧者	管理サイトへログインできるが操作／追加／編集／削除が行えない権限です。
4	ロック・ワイプ	ロック・ワイプ操作のみの実行権限を持ちます。また、管理サイトへログインしたとき、ロック・ワイプを含む緊急対応に必要な情報のみ（機器情報、位置情報、管理情報など）閲覧ができます。
5	ログイン	管理サイトへのログイン権を有したユーザーです。自身のユーザー情報にだけ閲覧権限を有します。
6	一般	管理サイトのログイン権を有しておらず、閲覧、編集など、いずれも行えません。一般社員やメール通知先として登録されることを想定しています。

6.1.2 ユーザー／組織情報を登録する

複数のユーザーおよび組織の情報は CSV ファイルを使用し、まとめて登録できます。

管理サイトで 1 名または 1 組織ずつ登録する手順の詳細は、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」
- 『管理サイト リファレンスマニュアル』の「組織」

事前に管理サイトでユーザーや組織の登録を一度行い、［CSV で編集］または［CSV をダウンロード］からダウンロードできる CSV ファイルを参照することで、どのように登録すればいいのか確認できます。

テンプレート CSV ファイルを入手・編集する

【1】管理サイトにアクセスし、［ユーザー］または［組織］→［CSV で追加］をクリックします。

【2】「CSV ファイルを準備します」の［ダウンロード］をクリックします。

⇒ユーザー情報を登録するテンプレート CSV ファイルのダウンロードが始まります。

【3】ダウンロードした CSV ファイルを開き、ユーザー／組織の登録作業を行います。

1 行目は項目名が登録されています。削除しないようご注意ください。

CSV ファイルを編集するソフトウェア（メモ帳、CSV エディタ、表計算ソフトなど）の操作手順は、開発元へお問い合わせください。

ユーザーに組織を紐づけることをおすすめします。

CSV ファイルの詳細は、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「基本操作」－「CSV ファイルの共通操作」－「インポート用の CSV ファイルの構造」
- 『管理サイト リファレンスマニュアル』の「機器」－「CSV で追加」－「インポート用の CSV ファイルの項目」

【4】作成したファイルを保存します。

次のページで組織およびユーザーを登録するための CSV ファイルの必須項目について説明しています。

上記の『管理サイト リファレンスマニュアル』とあわせてご確認ください。

参考

組織を登録するための CSV ファイル必須項目は以下のとおりです。

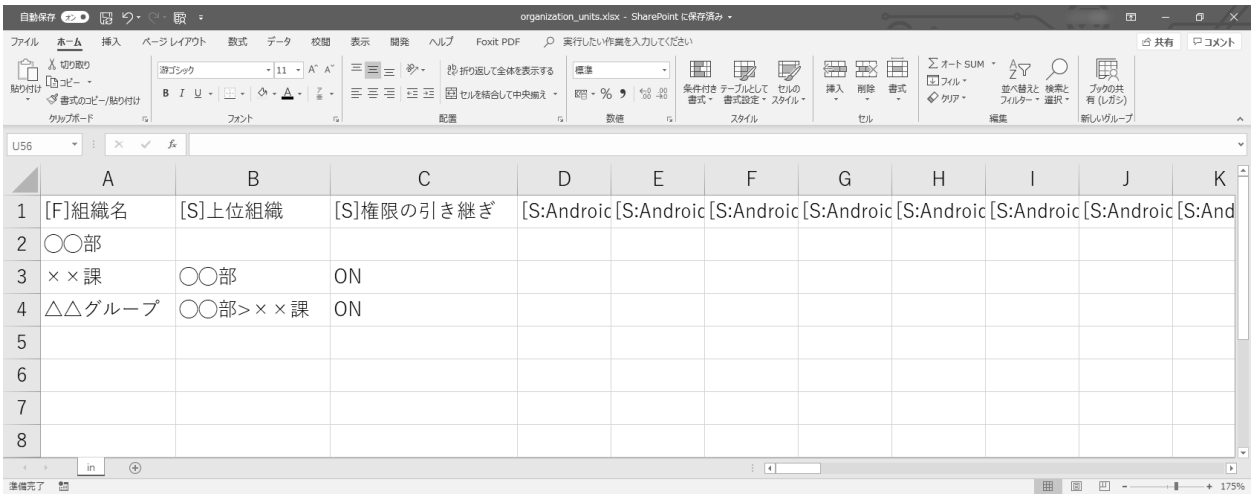
●[F]組織名

階層構造を作るには、上記の他に以下を記載する必要があります。

[S]上位組織：上位になる組織名

上位組織を登録するときは、最上位組織以外は、最上位組織から登録したい組織までを「>」でつなぎ、入力する必要があります。

例）「○○部」-「××課」-「△△グループ」を登録したい場合



	A	B	C	D	E	F	G	H	I	J	K
1	[F]組織名	[S]上位組織	[S]権限の引き継ぎ	[S:Androic	[S:Androic	[S:Androic	[S:Androic	[S:Androic	[S:Androic	[S:Androic	[S:And
2	○○部										
3	××課	○○部	ON								
4	△△グループ	○○部>××課	ON								
5											
6											
7											
8											

●[S]権限の引き継ぎ：ON もしくは空欄で指定してください。ON を選択すると、上位組織に対して何らか権限を持つユーザーの権限を、下位組織へ引き継ぐことができます。

ユーザーを登録するための CSV ファイル必須項目は以下のとおりです。

●[F]名前

●[F]ユーザーID

●[S]ユーザー種別

名前の代わりに、[F]姓・[F]名を入力することも可能です。

ユーザー種別は、「管理者」、「閲覧者」、「ロック・ワイプ」、「操作」、「ログイン」、「一般」からお選びください。「

ユーザー／組織とは」45 ページ

作成した CSV ファイルをアップロードする

【1】管理サイトにアクセスし、［ユーザー］または［組織］→［CSV で追加］をクリックします。

【2】「CSV ファイルをアップロードします」の［ファイルを選択］をクリックします。

⇒「テンプレート CSV ファイルを入手・編集する」で編集した、ユーザーまたは組織の情報が登録されている CSV ファイルを選択します。

【3】［アップロード］をクリックします。

⇒データの確認中画面が表示されます。しばらくお待ちください。

内容に誤りがある場合は、一覧の最後の「備考」欄にエラー内容が表示されます。エラー内容を参考に CSV ファイルを修正し、あらためて修正した CSV ファイルのアップロードを行ってください。

【4】［インポート実行］をクリックします。

⇒データがインポートされるのをお待ちください。

6.1.3 機器情報を事前登録する

本製品では、エージェントを認証する前に管理サイト上へ事前に機器情報を登録できます。

事前登録をしておくと、以下のようなメリットがあります。

機器台数が少ない場合などは、事前に機器登録を実施せず、直接、機器にエージェントアプリをインストールし、機器認証を行う方法もご選択いただけます。

◆事前登録のメリット

●組織、ユーザーに機器を紐づける場合、事前登録することで、効率的な紐づけができます。

●機器を事前登録することで、キッティング開始後、直ちに設定を適用できます。

特に、機器利用者がエージェントアプリをインストールする場合、事前登録がおすすめです。

●事前機器登録を実施した機器以外からの認証を拒否する設定ができます。

◆Tips

iOS 端末の ADE、Android 端末のゼロタッチ登録を利用すると、連携設定を行うことで自動的に機器が登録されます。詳しくは以下のマニュアルを参照してください。

『Apple Business Manager（ABM）マニュアル（利用方法・年次更新手順)』の「Automated Device Enrollment（ADE)」

『Apple School Manager（ASM）マニュアル（利用方法・年次更新手順)』の「Automated Device Enrollment（ADE)」

『iOS キッティングマニュアル』の「ADE を利用してライセンス認証を行う」

『Android キッティングマニュアル』

◆事前機器登録方法

事前機器登録には、CSV ファイルを使った一括インポートがおすすめです。

次のページまたは以下のマニュアルで詳細を確認してください。

『管理サイト リファレンスマニュアル』の「機器」－「CSV で追加」

◆注意

●Android Enterprise やユーザーベースの「App とブック」配信を使用するのであれば、ユーザーと機器の紐づけは必須です。

●Android Enterprise の場合、一度紐づけた機器とユーザーは紐づけの解除はできません。紐づけ解除を行うには、機器の初期化が必要となります。

6.1.3.1 テンプレート CSV ファイルの入手・編集

【1】管理サイトにアクセスし、［機器］→［CSV で追加］をクリックします。

【2】「CSV ファイルを準備します」の［ダウンロード］をクリックします。

⇒機器情報を登録するテンプレート CSV ファイルのダウンロードが始まります。

【3】ダウンロードした CSV ファイルを開き、機器の登録作業を行います。

1 行目は項目名が登録されています。削除しないようご注意ください。

CSV ファイルを編集するソフトウェア（メモ帳、CSV エディタ、表計算ソフトなど）の操作手順は、開発元へお問い合わせください。

事前に管理サイトで機器の登録を 1 台行い、［CSV で編集］または［CSV をダウンロード］からダウンロードできる CSV ファイルを参照することで、どのように登録すればいいのか確認できます。

CSV ファイルの詳細は、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「基本操作」－「CSV ファイルの共通操作」－「インポート用の CSV ファイルの構造」

『管理サイト リファレンスマニュアル』の「機器」－「CSV で追加」－「インポート用の CSV ファイルの項目」

【4】作成したファイルを保存します。

参考

CSV ファイルの必須項目は以下のとおりです。

●機器名

●OS 種別

「Android 機器」、「iOS 機器」、「Mac OS 機器」、「Windows 機器」、「資産管理対象機器」のいずれかに「ON」と入力します。

●ライセンス認証時の紐づけ項目のうち、いずれか 1 つ

事前機器登録には、認証する機器と管理サイト上の情報を紐づけるための機器ごとに一意なキーが必要です。キーは OS ごとに指定できるものが異なります。

- Android：電話番号、IMEI/MEID
- iOS：電話番号、シリアル番号
- Mac OS：シリアル番号、MAC アドレス
- Windows：シリアル番号、MAC アドレス

Windows 機器の新規作成のときに SIM に割り当てられている MAC アドレスは端末識別用として使用できません。

6.1.3.2 作成した CSV ファイルのアップロード

【1】管理サイトにアクセスし、［機器］→［CSV で追加］をクリックします。

【2】「CSV ファイルをアップロードします」の［ファイルを選択］をクリックします。

⇒「テンプレート CSV ファイルの入手・編集」で編集した、機器情報が登録されている CSV ファイルを選択します。

【3】［アップロード］をクリックします。

⇒データの確認中画面が表示されます。しばらくお待ちください。

内容に誤りがある場合は、一覧の最後の「備考」欄にエラー内容が表示されます。エラー内容を参考に CSV ファイルを修正し、あらためて修正した CSV ファイルのアップロードを行ってください。

【4】［インポート実行］をクリックします。

⇒データがインポートされるのをお待ちください。

インポート用 CSV ファイルの詳細については、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』の「基本操作」－「CSV ファイルの共通操作」－「インポート用の CSV ファイルの構造」

『管理サイト リファレンスマニュアル』の「機器」－「CSV で追加」－「インポート用の CSV ファイルの項目

6.2 機器とユーザー／組織情報の紐づけを行う

登録した機器とユーザー／組織情報を紐づけます。

管理サイトで 1 台ずつ紐づけする手順の詳細は、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「機器」－「一覧」－「機器の管理情報」

Android Enterprise を利用する場合、機器とユーザーの紐づけは必須となります。

Android Enterprise の場合、一度紐づけた機器とユーザーは紐づけの解除はできません。紐づけ解除を行うには、機器の初期化が必要となります。

iOS 機器においてユーザーベースとなる「App とブック」配信を使う場合、機器とユーザーの紐づけは必須となります。

事前に管理サイトで機器とユーザー／組織の紐づけを一度行い、［CSV で編集］または［CSV をダウンロード］からダウンロードできる CSV ファイルを参照することで、どのように登録すればいいのか確認できます。

6.2.1 CSV ファイルを入手・編集する

【1】管理サイトにアクセスし、［CSV で編集］をクリックします。

【2】「CSV ファイルを準備します」の［ダウンロード］をクリックします。

⇒管理サイトに登録されている情報が記載された CSV ファイルのダウンロードが始まります。

【3】ダウンロードした CSV ファイルを開き、機器とユーザーまたは組織情報の紐づけ作業を行います。

1 行目は項目名が登録されています。削除しないようご注意ください。

CSV ファイルを編集するソフトウェア（メモ帳、CSV エディタ、表計算ソフトなど）の操作手順は、開発元へお問い合わせください。

[S]ユーザー：機器に紐づけしたい「ユーザー」を入力します。
[S]組織：機器に紐づけしたい「組織」を入力します。

CSV ファイルの詳細は、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「基本操作」－「CSV ファイルの共通操作」－「インポート用の CSV ファイルの構造」

『管理サイト リファレンスマニュアル』の「機器」－「CSV で追加」－「インポート用の CSV ファイルの項目」

【4】作成したファイルを保存します。

6.2.2 編集した CSV ファイルをアップロードする

【1】管理サイトにアクセスし、［機器］→［CSV で編集］をクリックします。

【2】「CSV ファイルをアップロードします」の［ファイルを選択］をクリックします。

⇒「CSV ファイルを入手・編集する」で編集した、ユーザーまたは組織の情報が登録されている CSV ファイルを選択します。

【3】［アップロード］をクリックします。

⇒データの確認中画面が表示されます。しばらくお待ちください。

内容に誤りがある場合は、一覧の最後の「備考」欄にエラー内容が表示されます。エラー内容を参考に CSV ファイルを修正し、あらためて修正した CSV ファイルのアップロードを行ってください。

【4】［インポート実行］をクリックします。

⇒データがインポートされるのをお待ちください。

6.3 設定セットを作成・適用する

管理サイト上でセキュリティポリシーに応じた設定セットを作成し、各機器に適用します。設定セットの作成方法については、以下を参照してください。

「設定セットを作成、複製する」29 ページ

組織を利用している場合は、組織に設定を適用することで大量の機器に対し一括で適用できます。

『管理サイト リファレンスマニュアル』の「組織」－「一覧」－「［Android 設定］タブ／［iOS 設定］タブ／［Windows 設定］タブ」

6.3.1 CSV ファイルを入手・編集する

【1】管理サイトにアクセスし、［機器］→［CSV をダウンロード］→［機器レポート］をクリックします。

【2】必要な項目にチェックを入れます。

「機器インポートで使用可能な形式にする」には必ずチェックを入れてください。

【3】［レポート作成］をクリックします。

【4】［CSV ダウンロード］をクリックします。

⇒管理サイトに登録されている情報が記載された CSV ファイルのダウンロードが始まります。

【5】ダウンロードした CSV ファイルを開き、設定セットの登録作業を行います。

1 行目は項目名が登録されています。削除しないようご注意ください。

CSV ファイルを編集するソフトウェア（メモ帳、CSV エディタ、表計算ソフトなど）の操作手順は、開発元へお問い合わせください。

[S:Android]スクリーンロック：設定セット名
該当機種の同項目へ「設定セットを作成する」で作成した設定名を入力します。

CSV ファイルの詳細は、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「基本操作」－「CSV ファイルの共通操作」－「インポート用の CSV ファイルの構造」

『管理サイト リファレンスマニュアル』の「機器」－「CSV で追加」－「インポート用の CSV ファイルの項目」

【6】作成したファイルを保存します。

6.3.2 編集した CSV ファイルをアップロードする

【1】管理サイトにアクセスし、［機器］→［CSV で編集］をクリックします。

【2】「CSV ファイルをアップロードします」の［ファイルを選択］をクリックします。

⇒「CSV ファイルを入手・編集する」で編集した、設定セットの情報が登録されている CSV ファイルを選択します。

【3】［アップロード］をクリックします。

⇒データの確認中画面が表示されます。しばらくお待ちください。

内容に誤りがある場合は、一覧の最後の「備考」欄にエラー内容が表示されます。エラー内容を参考に CSV ファイルを修正し、あらためて修正した CSV ファイルのアップロードを行ってください。

【4】［インポート実行］をクリックします。

⇒データがインポートされるのをお待ちください。

6.4 機器のキッティングを行う

PC（Windows や Mac OS を搭載するパソコン）、Android 端末、iOS 端末のキッティングの詳細については、以下を参照してください。

- 『Android キッティングマニュアル』
- 『iOS キッティングマニュアル』
- 『Mac OS キッティングマニュアル』
- 『Windows キッティングマニュアル』

6.5 認証状態を確認する

登録を行った機器について、管理サイトから認証状態を確認できます。

6.5.1 CSV ファイルを入手・確認する

【1】管理サイトにアクセスし、［機器］→［CSV をダウンロード］→［機器レポート］をクリックします。

【2】必要な項目にチェックを入れます。

【3】［レポート作成］をクリックします。

【4】［CSV ダウンロード］をクリックします。

⇒管理サイトに登録されている情報が記載された CSV ファイルのダウンロードが始まります。

【5】ダウンロードした CSV ファイルを開き、確認します。

1 行目は項目名が登録されています。削除しないようご注意ください。

CSV ファイルを編集するソフトウェア（メモ帳、CSV エディタ、表計算ソフトなど）の操作手順は、開発元へお問い合わせください。

[I]認証日時：機器が認証された日時が記載されています。

CSV ファイルの詳細は、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「基本操作」－「CSV ファイルの共通操作」－「インポート用の CSV ファイルの構造」

『管理サイト リファレンスマニュアル』の「機器」－「CSV で追加」－「インポート用の CSV ファイルの項目」

AA	AB	AC	AD	AE	
[I]通信日時	[I]通信日時(エージェント)	[I]通信日時(ブラウザー)	[I]認証日時	[I]位置情報取得	[I]
2015-05-20 18:53:40 +0900			2015-05-20 16:09:34 +0900		
2015-12-15 13:54:54 +0900			2015-12-15 13:51:02 +0900		
2015-12-25 15:53:09 +0900			2015-12-25 15:52:45 +0900	許可	
2016-02-25 14:50:17 +0900			2016-02-25 14:07:08 +0900	許可	
2016-04-04 18:23:12 +0900			2016-04-04 18:19:23 +0900	許可	
2016-07-07 16:55:26 +0900			2016-07-07 10:33:54 +0900	許可	
2016-08-17 16:22:10 +0900			2016-08-17 15:53:30 +0900		

7 その他

7.1 その他、導入時の推奨設定について

ここまでの作業で、本製品の導入は完了となります。

本項では、本製品を運用する上で設定しておくと便利な機能についてご紹介いたします。

◆通知設定

- 本製品は管理サイト側の操作や、エージェント側の実行状況などをログとして管理サイトに表示する機能があります。
- 表示されているログのうち、一部は指定したメールアドレスに通知できますが、ご利用にはメールアドレスの登録が必要です。運用開始前の登録をおすすめします。

  ⇒登録すると、リモートロックやリモートワイプを実行したとき、Apple Push 証明書有効期限が近付いたときにメールに通知が届き、検知できます。

   『管理サイト リファレンスマニュアル』の「サービス環境設定」－「通知設定」