たよれーる デバイスマネジメントサービス

Ver. 8.1.1

サービス仕様書

第 2.3 版

2017 年 5 月 28 日

株式会社 大塚商会

更新履歴

日付	版数	変更内容
2011 年 12 月 26 日	1.0 (4.0)	初版発行
2012 年 02 月 06 日	1.1 (4.5)	管理サイト制約事項に関して追記
2012 年 04 月 24 日	1.2 (5.0.0)	Android 端末対応機能追加、iOS 端末機能追加による追記
2012 年 09 月 07 日	1.3 (5.0.1)	Windows 端末対応機能追加、その他端末機能追加による追記
2013 年 06 月 14 日	1.4 (5.6.0)	管理機能追加による追記
2013 年 10 月 11 日	1.5 (5.8.0)	管理機能追加による追記
2013 年 12 月 16 日	1.6 (5.8.1)	管理機能追加による追記
2014 年 01 月 16 日	1.6.1 (5.8.1)	仕様追記
2014 年 04 月 11 日	1.7 (5.9.0)	管理機能追加による追記
2014 年 07 月 14 日	1.8 (6.1.0)	管理機能追加による追記
2015 年 04 月 07 日	1.9 (7.2.0)	管理機能追加による追記
2015 年 09 月 07 日	1.9.1 (7.2.0)	Windows 端末対応 OS 追記
2015 年 11 月 03 日	2.0 (7.4.0)	管理機能追加による追記
2016 年 05 月 19 日	2.0.1 (7.4.0)	Android 端末対応 OS 追記
2016 年 08 月 20 日	2.1 (7.7.0)	管理機能追加による追記
2017 年 03 月 11 日	2.2 (8.1.0)	管理機能追加による追記
2017 年 05 月 28 日	2.3 (8.1.1)	管理機能追加による追記

目次

1. サービス概要

本仕様書は、たよれーる デバイスマネジメント サービスの仕様を定義するものです。

たよれーる デバイスマネジメント サービス（以下、本サービス）は、Android、iOS、Windows、Mac 端末の管理・運用を行うために環境を提供する株式会社 大塚商会(以下、「当社」という。)が提供するインターネットサービスです。機器情報やインストールされたアプリケーション情報を確認したり、管理サイトよりリモートロック等の操作をすることができます。

お使いのパソコンにインターネット接続環境があれば、ブラウザーにて管理サイトを操作することができます。

※Windows 端末の管理を行う場合は【基本サービス(Windows)】のご契約が必要です。

※Mac OS 機器の管理を行えるのは、【アカデミック版】のみとなります。

※Apple School Manager と連携を行えるのは、【アカデミック版】のみとなります。

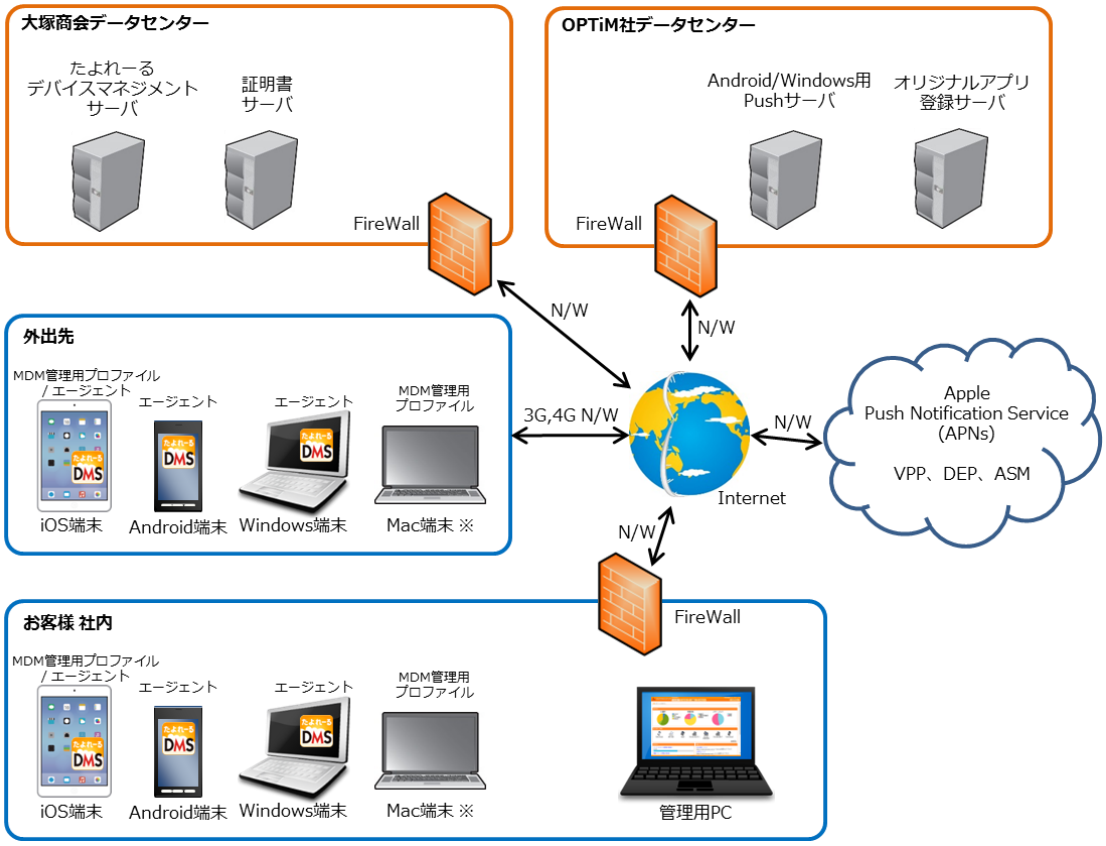
1-1 サービス内容

i. 本サービスは、以下の項目を提供いたします。

お客様に対し、本サービスの管理サイトおよび各エージェントを提供します。

1-2 システム構成

本サービスを提供するためのシステム構成を図 1 に示します。



※Mac 端末/ASM は「アカデミック版」でのみ対応

(図 1)

本サービスのシステム構成要素について以下で説明します。

i. たよれーる デバイスマネジメント エージェント

サポート対象となる Android、iOS、Windows 端末にインストールされるモジュールです。Android 版、Windows 版は管理者が設定した時間単位(初期値は 30 分)で端末情報を定期的に収集し、本製品サーバーへ送信する機能を持ちます。iOS 版は特定契機を元に位置情報を本製品サーバーへ送信する機能を持ちます。

iOS と Mac 端末はエージェントの他、MDM 管理用プロファイルを端末にインストールすることにより、端末情報を定期的(約 8 時間毎)に本製品サーバーへ送信する機能を持ちます。

対応 OS は、4-1「対応端末・OS」を参照してください。

ii. **たよれーる デバイスマネジメント サーバー**

株式会社大塚商会により、管理されるサーバーのひとつです。以下のサイトを提供します。

1) 管理サイト

本製品 エージェントが収集した情報を、お客様管理者向けに提示する機能を持ちます。お客様管理者は、ブラウザーを使用し、管理サイトにアクセスします。詳しい動作環境は、4-2「動作環境（管理サイト）」を参照してください。

iii. **Push サーバー**

Android、Windows 端末への Push 通知を行うためのサーバーです。

iv. **オリジナルアプリ登録サーバー**

iOS のオリジナルアプリ（インハウスアプリ）を登録するためのストレージサーバーです。

v. **証明書サーバー**

iOS および Mac 端末への証明書を発行するためのサーバーです。

vi. **APNs**

Apple 社が保有するサーバーです。iOS および Mac 端末への Push 通知を行うためのサーバーです。

vii. **VPP、DEP、ASM**

Apple 社が保有するサーバー（サービス）です。iOS 端末への各種サービスを提供します。

1-3 使用通信ポート

本サービスで使用する通信ポートを以下に記述します。以下のポートはすべて TCP を用いています。

使用通信ポート	本製品サーバー	Push サーバー	証明書サーバー	APNs	Apple サービスサーバー（DEP・VPP・ASM）	オリジナルアプリ登録サーバー
Android 端末	443(HTTPS)	443(HTTPS)	–	–	–	–
iOS 端末	443(HTTPS)	–	443(HTTPS)	5223	443(HTTPS)	443(HTTPS)
Windows 端末	443(HTTPS)	443(HTTPS)	–	–	–	–
Mac 端末	443(HTTPS)		443(HTTPS)	5223	–	–
管理 PC	443(HTTPS)	–	–	–	443(HTTPS)	443(HTTPS)
本製品サーバー	–	443(HTTPS)	443(HTTPS)	2195	443(HTTPS)	443(HTTPS)

1-4 機能

i. 本製品 エージェント

1) インストール機能

本製品 エージェントをサポート対象の Android、iOS、Windows 端末にインストールします。予め指定されたサイトより、インストーラをダウンロードし、実行することでインストールを行います。インストーラを実行すると、本製品 エージェントがインストールされます。インストール後、ライセンス認証を行います。

※iOS 端末は、予め指定されたサイトより、ライセンス認証（MDM 管理用プロファイルのインストール）します。その後 App Store より以下に記載している本製品 エージェントアプリをダウンロードしインストールを行います。

・たよれーる DMS(デバイスマネージメントサービス)
http://itunes.apple.com/jp/app/tayoreru-dms/id534138396?mt=8

2) ライセンス認証機能

本製品 エージェントを企業コードと紐付け、利用可能な状態にします。ライセンス認証が指示されると、企業コードおよび認証コードを入力するダイアログを表示します。iOS 向けエージェントにおいては、企業コードおよびアクティベーションコードを入力します。アクティベーションコードは、ライセンス認証後に生成される 12 桁の英数字で、管理サイトの機器画面より確認することができます。入力された企業コードおよび認証コードを元に本製品サーバーへ認証を行い、認証に成功した場合、ライセンスを 1 つ消費し Android、iOS、Windows 端末の情報を収集、本製品サーバーへ送信します。残りライセンスがない場合は、ライセンス認証を行うことはできません。他 MDM 製品がインストールされている場合、Apple 社の製品仕様上、iOS 端末の認証を行うことはできません。

3) ライセンス解除機能

本製品 エージェントと企業コードとの紐付けを解除します。エージェントからのライセンス解除のみではライセンスは返却されません。ライセンスを返却するためには、管理サイトから対象機器を削除します。

4)　本製品 エージェント起動機能

本製品エージェントが起動していない場合、本製品 エージェントを起動します。起動後、Android、iOS、Windows 端末の情報を収集し本製品サーバーへ送信します。

5)　本製品 エージェント終了機能

本製品 エージェントが起動済みの場合、本製品 エージェントを終了します。終了することで本製品による Android、iOS、Windows 端末の管理・運用を一時的に終了します。

6)　情報収集機能

Android、iOS、Windows 端末の情報を収集し、本製品サーバーへ通知します。収集した情報は管理サイトより確認することができます。詳細は 4-4「エージェント収集情報」を参照してください。

7)　同期機能

管理サイトで行った設定を手動または自動で Android、iOS、Windows 端末に反映できます。同時に、Android、iOS、Windows 端末の情報を収集し、本製品 サーバーへ通知します。

8)　アンインストール機能

本製品 エージェントをアンインストールします。ライセンス認証されている場合は、ライセンス解除されてからアンインストールを行います。ライセンスを返却するためには、管理サイトから対象機器を削除します。

9)　手動バックアップ機能(Android 端末)

Android 端末の設定を任意のタイミングで管理サイトにバックアップすることができます。バックアップ完了後、復元コードが表示されます。復元コードはバックアップ設定の復元時に使用します。バックアップの最大容量は 1MB となります。目安として連絡先が約 700 件までバックアップできます。

10）復元機能(Android 端末)

復元コードを入力することで管理サイトにバックアップした Android 端末の設定を復元することができます。復元コードはバックアップ時に表示される他、管理サイトにて確認できます。

11）プロキシ設定機能(Android 端末)

Android端末のWi-Fi環境下におけるプロキシ設定を行うことができます。接続するWi-Fiネットワークを選択し、プロキシホスト名、プロキシポート番号を入力することでプロキシ環境下でのWi-Fi接続ができます。

12）プロキシ認証機能(Windows 端末)

Windows 端末のエージェントの認証で、プロキシ認証が設定された環境でご利用になる場合に、プロキシ認証設定に指定されたユーザー名と、パスワードを入力することでプロキシ認証を行うことができます。

13）メッセージ配信機能

Android、iOS 端末で、管理サイトより作成・配信したメッセージを受信・閲覧することができます。

ii. 本製品 サーバー(管理サイト)

1) ログイン機能

企業コード、ID/パスワードを入力するためのページを表示します。企業コード、ID/パスワードが入力されると、認証を行い、認証に成功した場合、トップページを表示します。

2) トップページ機能

トップページで以下の情報が確認できます。

(a) お知らせエリア

当社より公開されたお知らせ内容が表示されます。お知らせ内容が公開されていない場合、お知らせエリアは非表示となります。

(b) 最近使用した機器

最近使用した機器が表示されます。

(c) 利用状況

ユーザーの利用状況に関する以下の情報が表示されます。

① ユーザーライセンス(使用数/契約数)
② 機器ライセンス(使用数/契約数)
③ 機器数
④ 基本パッケージ
⑤ オプションパッケージ(使用数/契約数)
⑥ Apple Push 証明書 登録
⑦ DEP サーバートークン登録
⑧ 端末状況（OS 種別/管理状態/スクリーンロックの有効無効）

(d) 機器セットアップ

機器にエージェントをセットアップするために、必要な以下の情報が表示されます。

① Android 用エージェント(エージェントセットアップ用 URL)
② iOS 用セットアップ(セットアップ URL)
③ Windows 用エージェント(URL)
④ Mac 用セットアップ(セットアップ URL)
⑤ 企業コード
⑥ 認証コード

3) ネットワークマップ機能

エージェントがインストールされている Android 端末、iOS 端末、Windows 端末をネットワークマップに表示し管理することができます。表示の上限数は、1,000 端末です。

(a) 検索機能

表示するネットワークマップを絞り込んで表示させることが可能です。機器の種類を選択、ネットワーク名を入力して検索することが可能です。

(b) 機器の種類表示機能

ネットワークマップに表示される機器は以下の種類で表示されます。

① ライセンス認証済み機器

② ライセンス認証対象機器

4) 設定セット複製

作成済みの設定セットを複製することができます。

5)　機器管理機能(Android 端末)

エージェントが収集した以下の機器情報を管理サイトから確認することで機器を管理できます。端末の状態によって、取得されない情報があります。機器登録数の上限は、契約ライセンス数です。

(a) 管理情報

以下の情報が確認できます。

① 機器名
② 所属
③ 分類
④ 追加情報
⑤ エージェントバージョン
⑥ 最終通信日時
⑦ 認証日時
⑧ 位置情報取得
⑨ ネットワーク(グローバル IP アドレス)
⑩ 機器ログ

(b) 機器情報

以下の情報が確認できます。

【Android 端末】

① モデル名
② 電話番号
③ ネットワークモード
④ ネットワークオペレータ
⑤ IMEI（International Mobile Equipment Identity）
⑥ ファームウェアバージョン
⑦ ビルド番号
⑧ シリアル番号
⑨ SSID
⑩ MAC アドレス
⑪ IP アドレス
⑫ Bluetooth の状態
⑬ 位置情報(無線ネットワーク)
⑭ 位置情報(GPS 機能)
⑮ バッテリー残量
⑯ バッテリー状態
⑰ パスワードのポリシー
⑱ パスワードの再利用
⑲ パスワードの有効期限
⑳ 自動ロックまでの時間
㉑ ロック解除失敗時の設定
㉒ リモートロック状態
㉓ 暗号化状態
㉔ root 化状態
㉕ root 化検知内容

(c) アプリケーション

インストールされているアプリケーション一覧を表示できます。各アプリケーションの以下の詳細情報も確認できます。端末の状態によって、取得されない情報があります。

【Android 端末】

① メモ
② アプリケーション名
③ パッケージ名
④ メモリサイズ
⑤ バージョン番号
⑥ バージョン名
⑦ インストール日時
⑧ アップデート日時
⑨ アプリケーションサイズ
⑩ データサイズ
⑪ キャッシュサイズ

(d) 位置情報機能

機器の位置情報を地図上で確認できます。また、位置情報は履歴を含めて 100 件分閲覧できます。Google マップを新しいウィンドウで開き、機器の位置情報を確認することもできます。位置情報が取得できないときは、位置情報タブが表示されません。端末にて GPS もしくは、位置情報の無線ネットワーク機能を ON にしている場合のみ取得可能です。

(e) その他機能

機器にその他の設定を設定することができます。

(i)　リモート操作

リモートロック、ロック解除、リモートワイプ、スクリーンロックパスワード再設定を実行することができます。リモートロック時、端末に指定されている警告音を鳴動させることができます。

(ii) 設定機能

機器に各設定セットを設定できます。設定セットについては、33)(e)「設定セット機能」をご覧ください。

(iii) メッセージ配信

配信予定のメッセージを表示します。また、メッセージボックスに配信済みメッセージの履歴を表示します。

(f)　同期機能

Android 端末で弊社提供の Push サーバーを利用して端末の設定をリアルタイムに同期することができます。端末の電源が OFF である状態や、端末が通信できない状態等では、リアルタイムに同期することができません。

(g) 操作機能

対象の機器を管理サイトから削除できます。削除されると、削除された機器のライセンスが返却されます。

6)　機器管理機能(iOS 端末)

エージェント並びに MDM 管理用プロファイル経由で収集した以下の機器情報を管理サイトから確認することで機器を管理できます。端末の状態によって、取得されない情報があります。機器登録数の上限は、契約ライセンス数です。

(a)　管理情報

以下の情報が確認できます。

①　機器名
②　所属
③　分類
④　追加情報
⑤　エージェントバージョン
⑥　アクティベーションコード
⑦　通信日時
⑧　通信日時（エージェント）
⑨　通信日時（ブラウザー）
⑩　認証日時
⑪　ネットワーク(グローバル IP アドレス)
⑫　機器ログ

(b)　機器情報

以下の情報が確認できます。

【iOS 端末】

① デバイス名
② 電話番号
③ 現在のキャリアネットワーク
④ ホームのキャリアネットワーク
⑤ IMEI（International Mobile Equipment Identity）
⑥ MEID（Mobile Equipment Identifier）
⑦ OS バージョン
⑧ ビルドバージョン
⑨ モデル名
⑩ モデル番号
⑪ モデルファームウェアバージョン
⑫ シリアル番号
⑬ Exchange ActiveSync デバイス ID
⑭ MDM プロファイルトピック値
⑮ UDID
⑯ Bluetooth MAC アドレス
⑰ Wi-Fi MAC アドレス
⑱ インターネット共有（テザリング）
⑲ 監視対象
⑳ バッテリー残量
㉑ デバイス容量
㉒ 利用可能なデバイス容量
㉓ iCloud バックアップ
㉔ 前回の iCloud バックアップ日時
㉕ パスコード保護
㉖ パスコード準拠状況（デバイス）
㉗ パスコード準拠状況（プロファイル）
㉘ アップデートの名前
㉙ アップデートのバージョン
㉚ アップデートのビルド番号
㉛ 重要なアップデートかどうか
㉜ アップデートのステータス※常時"(Unknown)"表示
㉝ 音声ローミング設定
㉞ ローミング状態
㉟ ハードウェア暗号化レベル

㊱ Jailbreak 状態(iOS エージェントインストール時)
㊲ iTunes Store アカウント
㊳ iTunes Store アカウントハッシュ
㊴ アクティベーションロック
㊵ BypassCode
㊶ ロケーターサービス
㊷ おやすみモード
㊸ 紛失モード
㊹ Shared iPad 設定
㊺ Shared iPad ユーザー最大数

(c) アプリケーション

プリインストールされているアプリケーション以外にインストールされているアプリケーションの一覧を表示できます。各アプリケーションの以下の詳細情報も確認できます。端末の状態によって、取得されない情報があります。

① アプリケーション名
② バージョン
③ メモリサイズ
④ アプリケーション ID
⑤ アプリケーションサイズ
⑥ データサイズ

(d) プロファイル

機器にインストールされている以下の情報を確認できます。

(1) 構成プロファイル

インストールされている構成プロファイルが確認できます。端末を管理するためにインストールされたプロファイルには管理セルにチェックアイコンが表示されます。本製品デフォルトのプロファイルは、チャックアイコンが表示されません。以下項目が確認できます。

(a) 名前
(b) 認識子
(c) 組織
(d) 説明
(e) 削除を許可
(f) 暗号化状態
(g) 管理対象
(h) UUID
(i) バージョン

(2) プロビジョニングプロファイル

端末で使用されているプロビジョニングプロファイルが確認できます。プロビジョニングプロファイルはアプリケーションをデバイスで使用する際やアプリケーションを App Store に登録する最に必要となるファイルです。本製品からは使用しているプロビジョニングプロファイルを確認ができるだけで、作成することはできません。以下項目が確認できます。

(a) 名前
(b) 有効期限
(c) 詳細

(3) 証明書

インストールされている証明書の情報が確認できます。以下項目が確認できます。

(a) ID
(b) コモンネーム

(e) 位置情報機能

機器の位置情報を地図上で確認できます。また、位置情報は履歴を含めて100 件分閲覧できます。Google マップを新しいウィンドウで開き、機器の位置情報を確認することもできます。位置情報が取得できないときは、位置情報タブが表示されません。端末にて位置情報サービス機能を ON にしている場合のみ取得可能です。iOS 端末では、エージェントを入れた場合のみ本機能をご利用いただけます。また、iOS 7 では OS の仕様上、エージェントアプリが起動している必要があります。「位置情報を更新」ボタンを押下すると、エージェントに対して、位置情報送信を要求します。

(f)　リモート操作

(i)　リモートロック機能

対象端末をロックします。パスコードが設定されていない場合、スワイプのみで解除できます。 パスコードを設定している場合、リモートロック時には、ロック画面に表示させるメッセージ(200 文字以内)および電話番号(20 文字以内)を指定することが可能です。

(ii)　リモートワイプ機能

対象機器のデータを削除します。同意するチェックボックスにチェックし、実行ボタンを押下すると実行され、端末が初期化されます。

(iii)　リモートワイプ機能（管理領域）

MDM 構成プロファイルを含む、管理領域のデータを削除します。同意するチェックボックスにチェックし、実行ボタンを押下すると実行されます。実行後、端末は管理外となります。

(iv)　パスコード削除機能

対象機器のパスコードを削除し、スワイプのみでロックを解除できるようにします。同意するチェックボックスにチェックし、実行ボタンを押下すると実行されます。

(v)　紛失モード

対象機器の紛失モードを有効化します。

(vi)　位置情報取得

紛失モードである場合、端末の位置情報を取得します。

(vii)　紛失モード解除

紛失モードを解除します。

(g)　設定

登録済み構成プロファイルを選択し、構成プロファイルを端末に設定できます。

(h) Exchange 設定

以下の Exchange 設定を機器ごとに設定できます。また、該当端末があるユーザーに所属している場合、「所属ユーザーの情報を利用」にチェックを入れることで、Exchange 設定適用時に自動的に所属ユーザーのユーザーID が「ユーザー」へ、メールアドレスが「メールアドレス」へ入力されて適用されます。（以後、「所属ユーザーの情報を利用」によって入力を省略する機能を、「ユーザー情報引き継ぎ機能」と呼びます）

① Exchange ActiveSync ホスト
② SSL の使用
③ ドメイン
④ 所属ユーザーの情報を利用
⑤ ユーザー
⑥ メールアドレス
⑦ パスワード
⑧ 認証資格情報
⑨ 過去のメールを同期する期間
⑩ 移動を許可
⑪ 最近使ったアドレスの同期を許可
⑫ メールのみで使用

(i) VPN 設定

端末に対して VPN を設定できます。接続タイプが「IPSec (Cisco)」の時、「クライアント証明書」もしくは「クライアント証明書一括アップロード」でアップロード済みのクライアント証明書を指定できます。また、「ユーザー情報引き継ぎ機能」により、所属ユーザーのユーザーID が「ユーザーアカウント」へ入力されて適用されます。

(j) 個別構成プロファイル

端末個別の構成プロファイルを設定できます。構成プロファイルが削除された場合、管理者へアラートメールを送信することが可能です。

(k) メッセージ配信機能

配信予定のメッセージを表示することができます。また、メッセージボックスに配信済みメッセージの履歴を表示します。iOS 端末は、エージェントを入れた場合のみ本機能をご利用いただけます。

(l) VPP 設定

iOS 端末は、デバイス（シリアル ID）に対する VPP ライセンス付与設定を適用することができます。

(m) 同期機能

iOS 端末は、アップル社提供の APNs を利用して端末と同期を行います。端末の電源が OFF の状態や、端末が通信できない状態等では、リアルタイムに同期することができません。

(n) 操作機能

対象の機器を管理サイトから削除できます。削除されると、削除された機器のライセンスが返却されます。

7)　機器管理機能(Windows 端末)

エージェントが収集した以下の機器情報を管理サイトから確認することで機器を管理できます。端末の状態によって、取得されない情報があります。機器登録数の上限は、契約ライセンス数です。

(a) 管理情報

①　機器名
②　所属
③　分類
④　追加情報
⑤　エージェントバージョン
⑥　通信日時
⑦　認証日時
⑧　グローバル IP アドレス
⑨　機器ログ
⑩　ゾーン
⑪　ポリシー

(b) 機器情報

以下の情報が確認できます。

【Windows 端末】

① コンピューター名
② ワークグループ名
③ Windows バージョン
④ システム製造元
⑤ システムモデル名
⑥ シリアル番号
⑦ NIC 名
⑧ 接続方法
⑨ MAC アドレス
⑩ IP アドレス
⑪ デフォルトゲートウェイ
⑫ DHCP
⑬ DHCP サーバー
⑭ DNS サーバー
⑮ DNS サフィックス
⑯ ネットワーク
⑰ 電話番号
⑱ 現在のキャリアネットワーク
⑲ IMEI/MEID
⑳ ハードウェア種別
㉑ CPU
㉒ メモリ
㉓ マザーボード
㉔ ビデオカード
㉕ TPM

㉖ BIOS メーカー
㉗ バージョン
㉘ 日付
㉙ (ドライブ名)総容量
㉚ (ドライブ名)空き容量
㉛ ログオンユーザー名
㉜ SID
㉝ 既定の Web ブラウザー　名前
㉞ 既定の Web ブラウザー　バージョン
㉟ 既定の電子メールプログラム　名前
㊱ 既定の電子メールプログラム　バージョン
㊲ 通常使うプリンター　名前
㊳ 通常使うプリンター　ポート
㊴ 文字数
㊵ 有効期間
㊶ 履歴記録数
㊷ 変更禁止期間
㊸ 複雑なパスワードを強制する
㊹ リモートロック　状態

(c) **アプリケーション**

インストールされているアプリケーション一覧を表示できます。各アプリケーションの以下の詳細情報も確認できます。端末の状態によって、取得されない情報があります。

【Windows 端末】
① アプリケーション名
② バージョン番号
③ インストール日時
④ アプリケーションサイズ
⑤ 発行日
⑥ インストール先
⑦ プロダクト ID
⑧ パッケージファミリー名

(d) セキュリティ機能

セキュリティ設定情報を確認することができます。

(i)　Windows 自動更新

更新プログラムの自動更新設定日時を確認することができます。

(ii) ファイアウォール

ファイアウォール状態を確認することができます。

(iii) ウイルス対策ソフト

ウイルス対策ソフトの名前、インストール有無、状態、定義ファイルの状態、エンジンバージョン、パターンファイルバージョンを確認することができます。

(iv) スパイウェア対策ソフト

スパイウェア対策ソフトの名前、インストール有無、状態、定義ファイルの状態を確認することができます。

(v)　スクリーンセーバー

ログオンユーザー名、設定、パスワードロック、起動までの時間を確認することができます。

(vi) ドライブ暗号化

ドライブ名、BitLocker 状態、暗号化進捗、回復パスワードを確認することができます。

(e) 位置情報機能

機器の位置情報を地図上で確認できます。また、位置情報は履歴を含めて 100 件分閲覧できます。Google マップを新しいウィンドウで開き、機器の位置情報を確認することもできます。位置情報が取得できないときは、位置情報タブが表示されません。端末にて位置情報取得を ON にしていて、「位置情報管理」設定セットが ON の場合のみ取得可能です。

(f)　リモート操作

(i)　リモートロック

対象機器をロックします。リモートロック時には管理サイトで指定されたメッセージを専用のロック画面に表示可能です。解除時には指定された解除コードを入力します。

(ii)　リモートワイプ

対象機器にワイプ相当する処理を行う BitLocker 方式と、対象機器のデータ削除を行うデータ削除方式の 2 種類から選択します。

BitLocker 方式は、BitLocker を用いた暗号化済みディスクドライブに対し、暗号化キーを削除することにより情報漏洩防止状態にします。データ削除方式は、対象機器にロック画面を表示させた後にデータドライブのクイックフォーマットおよびシステムドライブのデータ削除を行い、自動的に電源をシャットダウンします。その後、OS は起動しなくなります。

※詳細についてはご利用の手引きの「Windows リモートワイプ利用判定条件」を参照してください。

(g)　Microsoft Update 更新プログラム

機器に対して、各 Microsoft Update 更新プログラムが適用済か否かを確認することができます。

(h)　設定

機器に各設定セットを設定できます。設定セットについては、38)Windows 機能をご覧ください。

(i)　同期機能

サーバーと同期を行います。端末の電源が OFF の状態や、端末が通信できない状態等では、リアルタイムに同期することができません。

(j)　操作機能

対象の機器を管理サイトから削除できます。削除されると、削除された機器のライセンスが返却されます。

8)　機器管理機能(Mac 端末)

MDM 管理用プロファイル経由で収集した以下の機器情報を管理サイトから確認することで機器を管理できます。端末の状態によって、取得されない情報があります。機器登録数の上限は、契約ライセンス数です。

(a) 管理情報

以下の情報が確認できます。

① 機器名
② 所属
③ 分類
④ 追加情報
⑤ エージェントバージョン
⑥ アクティベーションコード
⑦ 最終通信日時
⑧ 認証日時
⑨ ネットワーク(グローバル IP アドレス)
⑩ 機器ログ

(b) 機器情報

以下の情報が確認できます。

【Mac 端末】
① デバイス名
② OS バージョン
③ ビルドバージョン
④ モデル名
⑤ モデル番号
⑥ シリアル番号
⑦ MDM プロファイルトピック値
⑧ デバイス容量
⑨ 利用可能なデバイス容量
⑩ 暗号化有無
⑪ パーソナル復旧キー
⑫ 所属団体の復旧キー

(c) アプリケーション

プリインストールされているアプリケーション以外にインストールされているアプリケーションの一覧を表示できます。各アプリケーションの以下の詳細情報も確認できます。端末の状態によって、取得されない情報があります。

① アプリケーション名
② バージョン
③ アプリケーション ID
④ アプリケーションサイズ

(d) プロファイル

機器にインストールされている以下の情報を確認できます。

(1) 構成プロファイル

インストールされている構成プロファイルが確認できます。端末を管理するためにインストールされたプロファイルには管理セルにチェックアイコンが表示されます。本製品デフォルトのプロファイルは、チャックアイコンが表示されません。以下項目が確認できます。

(a) 名前
(b) 認識子
(c) 組織
(d) ユーザー名
(e) 説明
(f) 削除を許可
(g) 暗号化
(h) UUID
(i) バージョン

(2) 証明書

インストールされている証明書の情報が確認できます。以下項目が確認できます。

(a) ID
(b) コモンネーム

(e) リモート操作

(i)　リモートロック機能

対象端末をロックします。端末側でリモートロックを解除する際には、管理サイトで設定されている 6 桁の解除コードを入力します。

(ii) リモートワイプ機能

対象機器のデータを削除します。同意するチェックボックスにチェックし、実行ボタンを押下すると実行され、端末が初期化されます。端末上においては、ワイプ後に「リモートロック機能」と同様のロック画面を表示します。解除コードもリモートロックと同様のものとなります。同期機能

Mac 端末は、アップル社提供の APNs を利用して端末と同期を行います。端末の電源が OFF の状態や、端末が通信できない状態等では、リアルタイムに同期することができません。また、ご利用いただく OS と同一バージョンの復元パーティションから起動が行える必要があります。

(f) 操作機能

対象の機器を管理サイトから削除できます。削除されると、削除された機器のライセンスが返却されます。

9)　ユーザー管理機能

ユーザーの新規追加、削除、ユーザー情報の編集ができます。ユーザーと端末を紐づけることや、ユーザー種別によってユーザーに権限を付与することが可能です。その他、ユーザー毎に機器認証が可能な上限数の指定や、VPP ライセンスの設定をすることが可能です。メールアドレスは、3 以上 256 以下の半角英数字、半角記号かつ@を含む必要があります。パスワードは 4 文字以上 20 文字以下の半角英数字、半角記号である必要があります。ユーザー数の上限は、契約ライセンス数となります。また、ユーザーオプションパッケージが企業に適用されている場合、本画面よりユーザーに対して紐付けをすることができます。その際のユーザーオプションパッケージの上限は、該当企業に付与されている数となります。Apple School Manager の機能が有効の場合、36)(h)DEP サーバートークン登録で取り込まれたユーザーは「Managed Apple Id」、「Unique Identifier」、「ユーザーアイコンの URL」を新たに表示し、専用のアイコンで表示します。

ユーザー種別による権限の種類は次のとおりです。

(a) 管理者

利用企業内の全権限を保有します。

(b) 操作

リモートロックおよびリモートワイプに関わる権限（設定の閲覧や編集）ができないことを除き、管理者と同等の権限を保有します。

(c) 閲覧者

操作に直結する項目（リモート操作、ユーザーインポート、証明書一括アップロード画面）を除き、すべてのページを閲覧することができます。

(d) ロック・ワイプ

リモートロックおよびリモートワイプのみ実行可能な権限を保有します。リモートロックおよびリモートワイプを実行するために必要な情報（機器情報、位置情報等）は閲覧可能です。

(e) ログイン

管理サイトへログインし、自ユーザーの情報のみ閲覧権限を保有し、他の権限は保有していません。この権限は、特定組織内のみに管理者権限を与えたいというケースへ対応する際に、11)ユーザー分類のグループに対して設定する権限と組み合わせて利用することを想定しています。

(f)　一般

管理サイトへログインできず、閲覧および編集が行えない権限です。

10) ユーザーカスタム項目機能

(a) 分類の設定

ユーザー分類を作成し、グループを登録することができます。例えば、ユーザー分類として部署名を作成し、グループとして営業部、開発部等を登録することが可能です。登録したグループとユーザーを紐づけて管理することが可能です。分類は 10 件、1 分類に 30 グループを作成できます。また、登録したグループに対して、組織単位に対する権限を付与することができます。

各グループには、組織と紐付く権限を設定することができます。設定できる権限は管理者、操作者、閲覧者、ロック・ワイプです。この権限を割り振られたグループに紐付けられたユーザーは、設定されている組織およびその配下組織の範囲内で、設定された権限を保有します。この権限は、利用企業全体に影響をおよぼす設定を閲覧および編集することはできません。

(b) 自由入力の設定

ユーザー分類に紐付けることが可能な任意の文字列を入力し、登録することができます。たとえば、ユーザー分類として登録したユーザーの電話番号など、任意の文字列を登録することが可能です。

11) ユーザー情報インポート機能

CSV ファイルをインポートすることで、ユーザーの新規追加、削除、ユーザー情報の編集を一括して行うことができます。一回のインポートで、インポート可能な CSV ファイルのサイズは 10MB 以下です。

12) ユーザー情報エクスポート機能

ユーザー情報を CSV ファイルとしてダウンロードできます。

13) 組織図機能

14)組織で定義されている組織の階層構造をグラフィカルに表示します。各組織を選択すると 14)組織の該当組織画面を表示します。

14）組織機能

組織およびその上位組織を作成することができます。組織に対して、Android、iOS、Windows ごとに設定セットを割り当てることができます。割り当てられた設定セットは、その組織に所属している端末およびその配下の組織に所属している端末に対して一括適用されます。ただし、配下組織が「権限を引き継ぎ」設定をしていない場合は、その上位組織に設定された設定セットは適用されません。

利用状況の中では、その組織に所属している端末の数（「権限を共有する機器」と表示）と、その組織に対して権限を紐付けられているユーザー分類とそのグループ・権限の種類が表示されます。「権限を共有する機器」に表示されている数字を選択すると、その組織に所属している端末一覧が表示されます。

また、VPP 設定タブからは VPP ライセンスの設定をすることが可能です。

組織は最大 10 階層まで管理できます。

15）組織インポート(新規)

ダウンロードした CSV ファイルに組織情報を入力し、インポートすることで、複数の組織情報をまとめて登録することができます。一回のインポートで、インポート可能な CSV ファイルのサイズは 10MB 以下です。

16）組織インポート(変更)

登録済みの組織情報を CSV ファイルに出力し、編集後インポートすることで、組織情報をまとめて変更することができます。一回のインポートで、インポート可能な CSV ファイルのサイズは 10MB 以下です。

17）組織エクスポート

組織情報を CSV ファイルとしてダウンロードできます。

18）機器カスタム項目機能

(a) 分類の設定

機器分類を作成し、グループを登録することができます。例えば、機器分類として使用用途を作成し、グループとして営業用、貸出用等を登録することが可能です。登録したグループと機器を紐づけて管理することが可能です。分類は 50 件、1 分類に 500 グループを作成できます。

(b) 自由入力の設定

機器分類に紐付けることが可能な任意の文字列を入力し、登録することができます。たとえば、機器分類として登録した機器の店舗コードなど、任意の文字列を登録することが可能です。登録したグループと機器を紐づけて管理することが可能です。

19）一括機器設定機能

すべての機器、ユーザーもしくは機器の分類とグループを指定して、一括して機器の設定を行うことができます。対象の機器は、すべての Android 端末、iOS 端末、Windows 端末、Mac 端末のリモート操作を一括して機器の設定が可能です。

20）機器情報インポート機能

CSV ファイルをインポートすることで、機器情報の編集を一括して行うことができます。一回のインポートで、インポート可能な CSV ファイルのサイズは 10MB 以下です。

21）機器情報エクスポート機能

機器情報を CSV ファイルとしてダウンロードできます。

22) アプリケーションレポート機能

Android、iOS、Windows、Mac 端末のアプリケーション情報を CSV ファイルにて出力することが可能です。
レポートに含める項目として、機器の管理情報、機器情報、アプリケーション検知での検知結果を追加することが可能です。また、管理サイト上にて出力内容を確認する際、検知結果(推奨/非推奨)にてフィルタをかけることが可能です。

23) メッセージ通知機能

Android、iOS 端末の配信予定のメッセージを作成・表示します。メッセージは 250 文字まで登録が可能です。また、メッセージボックスに配信済みメッセージの履歴を表示します。iOS 端末は、エージェントを入れた場合のみ本機能をご利用いただけます。メッセージ作成後は、「配信」ボタンを押し、端末と「同期」を行うことで配信が可能です。

(a) メッセージ作成機能

配信するメッセージの、タイトル、内容を作成することができます。オプションとして、「端末での表示時に URL をリンクにするか (リンクの挙動は端末に依存します)」否かを選択することができます。

(b) 配信先設定機能

メッセージの配信先を設定することができます。「一括指定」、「機器のグループを指定」、「機器を指定」から配信先を設定することができます。「機器のグループを指定」、「機器を指定」は、100 件まで登録が可能です。

(c) スケジュール配信機能

スケジュールを指定してメッセージを配信することができます。スケジュール設定は、「なし」、「毎月〇日」、「毎週〇曜日」から設定が可能です。「毎月〇日」は、特定の日にちのみ指定が可能です。29 日以降を設定した場合、その日付が存在しない月の配信は月末に行われます。「毎週〇曜日」は、日、月、火、水、木、金、土、の中からチェックをいれた曜日の指定が可能です。また、配信時刻も指定することができます。配信時刻は、「0～23」時の間で指定が可能です。配信時刻は目安としてご利用ください。

※配信する機器の量、ネットワーク接続状況によっては、配信時間から遅れて受信する場合があります。

(d) 配信履歴閲覧機能

メッセージの配信履歴を閲覧することができます。「配信時間」ごとに「対象機器」グループ内の「未受信」機器数や、「未読」機器数、「既読」機器数をリスト形式で閲覧することができます。また、「未受信」機器数や、「未読」機器数、「既読」機器数のリンクから、それぞれと紐付く機器のみを表示することができます。

(e) メッセージ編集機能

メール通知を行うタイミングを設定することが可能です。随時、1 日 1 回、一時停止のいずれかに設定します。

24) 証明書管理

(a) クライアント証明書アップロード

Exchange 設定や VPN 設定等で利用する PKCS#12 形式のクライアント証明書を登録できます。登録するクライアント証明書がパスワードで保護されている場合、パスワードを入力します。

(b) クライアント証明書一括アップロード

ZIP ファイルに固められたクライアント証明書をアップロードすることで、大量の PKCS#12 形式のクライアント証明書を一括でアップロードできます。ZIP ファイル内に含まれているクライアント証明書がパスワードを含む場合、各証明書のパスワードを記載した CSV ファイルを合わせてアップロードします。一括で登録できる証明書件数は 50,000 件かつ 10MB までです。

(c) CA 証明書管理

Android および Windows 端末にインストールする、PEM または DER 形式の CA 証明書をアップロード、登録することができます。

25) ログ機能

管理サイト操作ログ、エージェントの動作ログ、端末の Web フィルタリングによる閲覧履歴ログ、復元コードが確認できます。期間や文字列でログを検索することも可能です。指定のログを検索し、CSV による出力が可能です。ログは 10,0000 件まで出力可能です。管理サイトでログを保持する期間は 1 年間です。

26) 通知設定

Android、iOS、Windows、Mac 端末のアラートの際にメール通知を行う設定が可能です。以下の設定が可能です。

(a) メール通知タイミング

メール通知を行うタイミングを設定することが可能です。随時、1 日 1 回、一時停止のいずれかに設定します。

(b) メール通知対象ログ

メール通知を行う際の対象ログを設定します。設定したログが発生した際にメール通知を行います。

(c) メール送信先

メールの送信先を設定します。

(d) メール送信先(カスタム)

通知対象のメールアドレスを任意のアドレスを設定することができます。

(e) 言語

送信するメールの言語を設定します。言語設定は、「日本語」、「English」より選択可能です。

(f) 無通信時

指定時間・日数通信がない機器を検知することができます。指定時間・日数を設定します。無通信の端末は、端末の名称が赤く表示されます。

27) ポータル表示設定

Android、iOS、Windows、Mac 毎に、ポータルの「表示」、「非表示」の設定が可能です。

28）認証制御設定

端末からライセンス認証が行われた際の挙動を設定することができます。設定は、「全ての機器を認証する」、「管理者が登録した機器のみを認証する」より選択可能です。「管理者が登録した機器のみを認証する」を選択していた場合、ライセンス認証待ち機器として事前登録した機器のみライセンス認証が可能となります。

事前登録の際に識別子として登録可能な情報は以下のものとなります。

【Android 端末】

① 電話番号
② MAC アドレス
③ IMEI

【iOS 端末】

① 電話番号
② MAC アドレス
③ シリアル番号

【Windows 端末】

① MAC アドレス
② シリアル番号
③ 電話番号
④ IMEI/MEID

【Mac 端末】

① Wi-Fi MAC アドレス
② シリアル番号

29）アカウントポリシー設定

ユーザーに対するパスワードのポリシーを設定することができます。パスワードの長さ、過去のパスワード禁止、複雑なパスワードの要求、パスワードの有効期間、アカウントのロックアウトについて設定可能です。

30）個人設定

(a) 環境

管理サイト表示の際の言語設定が可能です。言語設定は、「ブラウザーの設定を使用する」、「日本語」、「English」より選択可能です。

(b) パスワード

管理サイトへログインしているユーザーのパスワードの変更が可能です。パスワードは 4 文字以上 20 文字以下の半角英数字、半角記号である必要があります。

(c) アプリケーションメモ

アプリケーションメモのクリア設定を行うことが可能です。

31）ブラウザー機能

ブラウザーに対する設定が可能です。iOS は DMS ブラウザ、Android は Optimal Biz Browser に対して設定されます。また、Windows はお気に入り配信のみ設定することができます。

※DMS ブラウザとは iOS 端末の標準ブラウザー(Safari)とは別にインストールする無償ブラウザーです。

※Optimal Biz Browser とは Android 端末の標準ブラウザーとは別にインストールする無償ブラウザーです。

(a) Web フィルタリング

禁止方式(ホワイトリスト/ブラックリスト)と、フィルタリングを行う URL を設定することが可能です。URL は最大 1000 件まで登録することが可能です。

(b) Web 閲覧履歴

Web 閲覧履歴ログを取得するか否かの設定と、定期的に Web 閲覧履歴を削除するか否かの設定をすることが可能です。

(c) お気に入り

お気に入りに登録したい Web ページのタイトルと URL を設定することが可能です。設定可能な Web ページは、最大 300 件まで登録することが可能です。また、Windows に対してはホームページの設定を適用することも可能です。

32）Zone Management

端末側で検知した SSID を元に設定セットを適用することができます。SSID の組み合わせ、設定セットの組み合わせ、およびそれらの組み合わせを設定可能です。以下の設定を作成することができます。

(i)　ゾーン

一つ、もしくは複数の SSID および MAC アドレスや、位置情報(緯度、経度、半径(m))、ゾーン判定に使用するタイムゾーンを設定することが可能です。SSID と MAC アドレスの組み合わせは最大 50 件、位置情報とゾーン判定に使用するタイムゾーンは最大 10 件まで登録することができます。

(ii)　ポリシー

Android と Windows の OS ごとに設定セットの組み合わせを設定し、ポリシーとして作成することができます。

(iii) ゾーンポリシー構成

「ゾーン」および「ポリシー」の組み合わせを、優先度を付与して、設定セットとして作成することができます。この組み合わせは 10 件まで登録することができます。

33）Android 機能

(a)　設定テンプレート機能

作成した設定セットを組み合わせて、設定テンプレートを作成することができます。

(b)　エージェント共通管理機能

以下のエージェントの設定ができます。

(i)　管理サーバーとの通信間隔

エージェントと管理サーバーとの通信間隔が設定できます。分数指定、時間指定、日数指定のいずれかに設定します。デフォルトは、30 分に設定されています。

(ii)　管理サーバーと通信できなかった場合の動作

エージェントが管理サーバーと通信ができなくなった場合の動作を設定できます。通信ができなくなった場合になにもしない設定、分数指定、指定時間後または指定日数後に端末をロックする設定ができます。デフォルトは、「なにもしない」に設定されています。

(iii) ロックメッセージ

管理サーバーと通信できずに端末をロックした時、端末画面に表示するメッセージの設定ができます。メッセージは 200 文字まで登録可能です。デフォルトは、設定されていません。設定セットを用いて端末をリモートロックしたときは、設定セットで登録されているメッセージが表示されます。

(iv) 端末でのリモートロックの解除方法

リモートロックの端末での解除方法を設定できます。なしに設定した場合は管理サイトからのみロックを解除でき、解除コードを設定した場合は端末からもロックを解除できるようになります。解除コードは、4 文字以上 20 文字以下の半角英数字が設定可能です。デフォルトは、なしに設定されています。

(v) 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の設定

ライセンスの解除やエージェントのアンインストールする際のパスワードの設定ができます。パスワードを設定しない場合は、制限なしに設定します。パスワードは、4 文字以上 20 文字以下の半角英数字が設定可能です。デフォルトでは、制限なしに設定されています。

(vi) root 化状態検知

端末の root 化検知の状態を設定ができます。検知しない場合「検知しない」、検知する場合「検知する」を設定します。

(c) エージェント個別管理

エージェント個別の設定ができます。以下の設定が可能です。

(i) Push 通知

「利用する」、「端末が Wi-Fi 接続時は利用しない」、「利用しない」を選択し、設定できます。

(d) 設定バックアップ

設定内容の自動バックアップタイミングを設定できます。毎月の決まった日付や毎週の決まった曜日に自動バックアップするように設定できます。バックアップ項目一覧は、4-5「バックアップ・復元項目一覧」をご覧ください。バックアップの最大容量は 1MB となります。目安として連絡先が約 700 件までバックアップできます。管理サイトでバックアップを保持する期間は 1 年間です。

(e) 位置情報管理機能

Android 端末にインストールされているエージェントに対して機器毎に位置情報管理ポリシーを設定することができます。

(i) エージェントによる測定

エージェントによる位置情報の測位タイミングを設定することができます。「測位しない」に設定すると位置情報の測位を行いません。「エージェント起動時のみ測位する」を設定するとエージェント起動時のみ測位します。「定期的に測位する」を設定すると測位するタイミングを設定することで設定したタイミングに測位します。設定は「分数指定」「時間指定」「日数指定」から設定が可能です。

※端末の位置情報の無線ネットワークと GPS が無効の場合測位を行いません。

※エージェントの位置情報取得が「許可しない」に設定されている場合、位置情報の取得を行いません。

※上記以外でも、測位機能が有効の場合に端末に対して同期処理を実施したタイミングで位置情報の測位・送信処理が実施されます。

(f) App Manager 機能

App Manager の表示・非表示の設定が可能です。表示の場合、端末にインストール可能な MDM 関連アプリケーションが表示され、端末にインストール通知が行われます。

34）Android 端末使用制限機能

Android 端末を管理する為の以下の設定ができます。

(a) アプリケーション禁止

設定したアプリケーション以外を起動させない、もしくは、設定したアプリケーションを起動させないように設定することができます。1 設定セットで 1000 件までのアプリケーションを設定することが可能です。対象とするアプリケーションは、CSV から一括インポート可能です。

(i) アプリケーション禁止

許可するアプリケーションを指定、又は禁止するアプリケーションを指定することでアプリケーションの起動させないようにすることが可能です。指定するアプリケーションのアプリケーション名、パッケージ名を指定することで設定することが可能です。

(ii) アプリケーションのインストール制限

アプリケーションの新規インストールの許可・禁止設定を行うことができます。すべてのアプリケーションのアップデートも不可能になります。

(iii) 設定画面の禁止

[Wi-Fi 設定][VPN 設定][APN 設定][デバイス管理者機能][開発][アプリケーション管理]画面の使用を禁止設定することができます。

※Android OS 2.2,2.3 のみ対応

(iv) 画面の禁止(カスタム)一覧

指定した画面の使用を禁止設定することができます。

(b) SD カード使用制限

Android 端末の通常利用時、または PC 接続時に SD カードの使用を禁止することができます。Android4.2 の端末においては、データ書き込み／エージェント同期/SD カードのマウントを検知したタイミングで SD カードのワイプを実行します。Android4.3、Android4.4 の端末においては、SD カードの挿入を検知したタイミングで端末ロックを実行します。

(c) カメラ使用制限

カメラ機能を使用できないように設定することができます。

(d) Bluetooth 機能

Bluetooth 機能を「変更しない」、「有効にする」、「無効にする」に設定できます。

(e) スクリーンロック

以下のスクリーンロック設定をすることができます。

① パスワードポリシー

端末のパスワードポリシーを「端末の設定を変更しない」「制限なし」「以下の制限に設定する」に設定できます。

「端末の設定を変更しない」に設定すると、端末のパスワードポリシーを変更しません。例えば、一度本製品から端末の解除方法をパスワードのみに変更した後に、「端末の設定を変更しない」に設定すると、端末の解除方法はパスワードのみ選択可能な状態になります。

「制限なし」に設定すると、端末の解除方法の制限を解除します。例えば、一度本製品から端末の解除方法をパスワードのみに変更した後に、「制限なし」に設定すると、すべての解除方法が選択可能になります。パスワードの初期化はされないため、「制限なし」に設定した直後は、設定前と同じパスワードが設定されています。

「以下の制限に設定する」を選択すると、端末の解除方法を「PIN またはパスワード」「パスワード」「数字を含むパスワード」、解除コードの文字数を設定できます。

② パスワードの再利用

パスワードの有効期限が切れた場合、同じパスワードを再度利用できるか設定できます。OS が Android3.0 以降の場合のみ利用できます。

③ パスワードの有効期限

パスワードの設定期限を設定できます。OS が Android3.0 以降の場合の利用できます。

④ 自動ロックまでの時間

端末の自動ロックまでの時間を設定できます。時間は 30 秒、1 分、2 分、5 分、10 分、30 分、時間指定(1 分から 30 分)から選択できます。

⑤ ロック解除失敗時の設定

連続ロック失敗時の挙動を設定できます。設定は、「端末の設定を変更しない」、「○○回失敗でリモートロック」、「○○回失敗でワイプ」、「リモートロック/ワイプを行わない」から選択可能です。

※○○回の○○には、2 以上 50 以下の値が設定可能です。

(f)　リモートロック

管理サイトから端末をロックすることができます。ロック中、端末画面に表示するメッセージも登録可能です。メッセージは 200 文字まで登録可能です。管理サーバーと通信できずに端末をリモートロックした場合は、30(ⅲ)ロックメッセージで設定したメッセージを表示します。リモートロック時に警告音を鳴動させることができます。

(g)　リモートワイプ

管理サイトから端末を初期化することができます。SD カードも初期化することが可能です。

(h)　スクリーンロックパスワード再設定

管理サイトから端末に設定されているスクリーンロックのパスワードを再設定することが可能です。

(i)　Wi-Fi フィルタリング

登録した SSID のアクセスポイントのみ使用できるように設定できます。1 設定セットに 300 件の SSID が登録可能です。

(j)　発信先制限

Android OS 標準の電話から発信される特定の電話番号に対して、発信制限を行うことができます。

①　発信先制御方式設定

許可する発信先を指定する(以下で指定されていない発信先は禁止)、もしくは、禁止する発信先を指定する(以下で指定されていない発信先は許可)のいずれかから制御方式を選択することができます。いずれの方式でも、緊急通報用電話番号への発信は基本的に端末の仕様により制限することはできません。

②　発信先指定

電話番号を入力して、発信先を指定することができます。

また、CSV ファイルから発信先を一括で登録することもできます。制御可能な電話番号は、300 件までです。入力可能文字数は、20 文字以内で、入力可能文字は、半角数字、「-」、「+」、「*」、「#」、「,」です。電話番号を CSV ファイルからインポートする場合は、一度設定を保存した後に、インポート用ファイルをダウンロードし、発信先を入力後、アップロードしてください。

(k) アプリケーション検知

Android 端末へ推奨アプリケーション、非推奨アプリケーションの有無の検知を行うことができます。アプリケーション名、パッケージ名バージョン条件を[全て、≧、＞、＜、≦、=]より設定することが可能です。検知されたアプリケーションは管理者へアラートとして送信されます。推奨アプリケーション、非推奨アプリケーションはそれぞれ 50 件ずつ登録可能です。通知は情報に変化があった場合のみ行います。Android 端末の日付が変更された最初の通知契機で送信を行います。検知は 1 日 1 回適宜に行われます。

(l) Secure Shield

本サービスが提供する Secure Shield の有効・無効設定、禁止項目の設定を行うことができます。Android のバージョンや機種によっては、利用できない機能があります。禁止項目は以下項目から設定可能です。

① 無線とネットワーク
・「Wi-Fi」、「Bluetooth」、「データ使用」、「その他のネットワーク設定」
② 端末
・「音」、「ディスプレイ」、「ストレージ」、「電池」、「アプリ」
③ ユーザー設定
・「アカウントと同期」、「位置情報サービス」、「セキュリティ」、
「言語と入力」、「バックアップとリセット」
④ システム
・「日付と時刻」、「ユーザー補助」、「開発者向けオプション」、「端末情報」
⑤ 機種(キャリア)固有メニュー
・「ドコモサービス」、「ホーム選択」、「WiMAX」、
「モバイルネットワーク」、「PC に接続」

35) Android 端末セットアップ機能

(a) **アプリケーション配信**

設定したアプリケーションのダウンロード案内を端末に通知することができます。アプリケーション名、ダウンロード先の URL、パッケージ名、バージョン番号を設定します。1 設定セットに 300 件のアプリケーションが登録可能です。また、ポップアップオプション設定を行うことにより、通知時に端末にポップアップ表示を行うことができます。

(b) **Wi-Fi 設定**

以下の Wi-Fi 設定をすることができます。1 設定セットに 5 件のネットワーク設定が登録可能です。Hidden SSID の欄にチェックを入れることで Hidden(非公開) SSID に対応可能です。

① Wi-Fi の有効、無効
② Wi-Fi のスリープ設定
③ ネットワーク設定（SSID、暗号方式、パスワード、Hidden SSID）

(c) **連絡先設定**

連絡先を設定することができます。CSV ファイルをインポートすることで一括して連絡先を登録することが可能です。一回のインポートで、インポート可能な CSV ファイルのサイズは 10MB 以下です。1 設定セットに 1,000 件の連絡先が登録可能です。

(d) **暗号化**

端末の暗号化設定の強制設定を行うことができます。Android 3.0,3.1,3.2, 以降の端末の暗号化設定を強制使用設定にするためにポップアップを表示させます。

(e) **NFC キッティング設定**

NFC を用いたデバイスオーナー化に用いる親機を設定することができます。Android 6.0 以降で対応する機能となります。

36）iOS 機能

iOS 端末を管理する為の以下の設定ができます。

(a) 設定テンプレート機能

作成した設定セットと構成プロファイルを組み合わせて、設定テンプレートを作成することができます。

(b) Apple Push 証明書登録

Apple Push 証明書の登録ができます。証明書要求をダウンロードし、Apple Push Certificates Portal から証明書ファイルを作成します。作成した証明書ファイルを登録できます。異なるトピック値を持つ証明書ファイルを登録しようとした場合は、エラーを表示します。登録時には、備考を入力することができます。

(c) エージェント共通設定

Jailbreak 状態検知の検知可否、(p)アプリカタログのタイトル、VPN カスタムキーを設定することができます。Jailbreak 状態を検知するためには iOS 端末用エージェント、アプリカタログを利用する為には専用アプリ（DMS Apps）が必要です。

(d) 構成プロファイル

36)(e)　構成プロファイルアップロード でアップロードした構成プロファイルを参照し、登録することができます。構成プロファイルは複数登録することができます。登録した構成プロファイルに対して、削除防止機能を設定するか否かを設定することができます。なお、削除防止機能を設定した構成プロファイルは、端末のポータルサイトから手動でインストールします。このプロファイルは、ライセンス認証時にインストールされる MDM 構成プロファイルを削除しても、同時には削除されません。削除防止として設定できる値は以下のとおりです。

(i)　削除禁止

端末側の操作では構成プロファイルを削除できないようにします。このプロファイルを消すためには Apple Configurator が必要です。

(ii)　パスワード

端末側の操作で構成プロファイルを削除する際に、パスワードを要求することができます。

(e) 構成プロファイルアップロード

PC 等で作成した構成プロファイルを管理サイトへアップロードし登録を行うことができます。また、空の構成プロファイルを新規で作成し、Apple Configurator 上の「一般」、「パスコード」、「制限」、「Wi-Fi」、「メール」、「証明書」、「グローバル HTTP プロキシ」、「Web フィルタリング」、「ドメイン」、「VPN」、「Web クリップ」に該当する項目の設定を行うことができます。アップロードした構成プロファイルは 36)(d)構成プロファイル にて設定を行うことができます。また登録した構成プロファイルの編集・ダウンロードを行うことができます。登録可能上限数は 300 件です。また、「メール」および「VPN」については、「ユーザー情報引き継ぎ機能」に対応しています。この機能有効時には、構成プロファイル適用時に、「ユーザー表示名」、「メールアドレス」、「ユーザー名」、「パスワード」の項目について自動入力されて適用されます(ユーザー表示名はユーザー情報の「ユーザー名」、ユーザー名は同じく「ユーザーID」からそれぞれ取得します)。

(f)　ローミング設定

音声ローミング、データローミングの有効化・無効化設定を行うことができます。本設定は、iOS5.0 以降のみ対応となる機能です。

(g) ホーム画面レイアウト

iOS 端末のホーム画面レイアウトを管理者から指定し、固定することができます。本設定は、iOS 9.3 以降及び監視対象モードの端末のみ対応となる機能です。

(h) DEP サーバートークン登録

DEP サーバーと通信するために必要な、DEP サーバーから取得できるトークンを登録します。Apple School Manager の機能が有効の場合、同画面でトークンを登録します。

(i) DEP 定義プロファイル

端末がアクティベーションされた際に、端末に適用される DEP の定義プロファイルを作成することができます。Apple School Manager の機能が有効の場合、”Shared iPad”の関連設定を追加表示します。

(j) DEP 機器管理

(h)DEP サーバートークン登録で登録された DEP サーバーに登録されている機器の一覧を表示することができます。

(k) VPP ライセンス

Apple 社の提供する Volume Purchase Program (VPP)を利用する為の、VPP トークンをアップロードすることが可能です。また、アプリケーションタブより、トークンに含まれるライセンスの詳細が確認できます。次の情報が確認可能です。

① Store ID
② アプリケーション名
③ 所持数
④ 使用数
⑤ 残数
⑥ 身割り当て数
⑦ 割り当て
⑧ 回収

※VPP で購入したアプリのみをサービス対象とし、書籍等についてはサービス対象外となります。

(l)　VPP 設定テンプレート

アップロードした VPP ライセンス(トークン)の中から、VPP 設定テンプレートに含める VPP ライセンスを指定することが可能です。また、VPP アプリライセンスを付与するアプリケーション名を選択することが可能です。

(m) 管理対象アプリポリシー

アプリケーションを配信する際に、VPP ライセンスを自動的に付与するか否か、Per app VPN の設定を適用するか否か、AppStore アプリの自動バージョンアップ機能を有効化するか否かの設定が可能です。Per app VPN の設定を適用する場合は、同画面で詳細に設定することができます。なお、Per app VPN の設定は、オリジナルアプリの配信時に管理対象ポリシーとして適用することが可能です。

※Per app VPN とは、iOS のアプリ単位で VPN 接続が可能になる機能です。iOS 7 以上で対応しています。

(n) オリジナルアプリ登録

iOS 端末へ配信するオリジナルアプリおよびプロビジョニングプロファイルを登録することができます。オリジナルアプリの登録上限は 50 件です。

※iOS オリジナルアプリ作成は、Apple の Apple Developer Enterprise Program の契約が必要です。

(o) アプリケーション配信

iOS 端末へ App Store もしくはカスタム B2B アプリで配信されている指定のアプリ情報を送信することができます。また、オリジナルアプリ登録で登録したアプリを指定の iOS 端末へ配信することができます。登録できるアプリは、オリジナルアプリは 50 件、AppStore もしくはカスタム B2B アプリは 300 件です。指定されるアプリは、管理対象に設定すること、およびバックアップ対象とするか否かを設定することができます。管理対象としたアプリを監視対象となっている iOS 端末へ配信すると、サイレントインストールすることが可能です。

また、管理対象アプリとして配布したアプリが端末上に既に存在している場合は、既存の非管理対象アプリを管理対象アプリへと変更します。

※iOS オリジナルアプリ作成は、Apple の Apple Developer Enterprise Program の契約が必要です。

※サイレントインストールは、端末内に iTunes Store / Apple ID のパスワードが保存されている場合に可能です。

(p) アプリカタログ

配布範囲として組織やユーザー分類を指定し、インストール推奨アプリを設定・配信することができます。本設定は通常のアプリケーション配信と異なり、1 端末辺り複数の設定を適用することが可能です。

※本設定を利用する場合は、iOS 端末に対して別途専用アプリの DMS Apps を App Store よりインストールいただく必要があります。

(q) アプリケーション検知

iOS 端末へ推奨アプリケーション、非推奨アプリケーションの有無の検知を行うことができます。アプリケーション名、パッケージ名バージョン条件を[全て、≧、＞、＜、≦、=]より設定することが可能です。検知されたアプリケーションは管理者へアラートとして送信されます。推奨アプリケーション、非推奨アプリケーションはそれぞれ 50 件ずつ登録可能です。通知は情報に変化があった場合のみ行います。iOS 端末の日付が変更された最初の通知契機で送信を行います。検知は 1 日 1 回適宜に行われます。

37）Mac 機能

Mac 端末を管理する為の以下の設定ができます。

(a) エージェント共通管理

以下の項目について設定することができます。

(i)　端末でのリモートロック・リモートワイプ後のロック解除コード

Mac 端末に対してリモートロックおよびリモートワイプを実施した後のロック画面を解除する為の解除コード(6 桁の数字)を指定することができます。

38) Windows 機能

(a) **設定テンプレート機能**

作成した設定セットを組み合わせて、設定テンプレートを作成することができます。

(b) **エージェント共通管理機能**

以下のエージェントの設定ができます。

(i) 管理サーバーとの通信間隔

エージェントと管理サーバーとの通信間隔が設定できます。分数指定、時間指定、日数指定のいずれかに設定します。デフォルトは、30 分に設定されています。

(ii) 管理サーバと通信できなかった場合の動作

エージェントが管理サーバと通信ができなくなった場合の動作を設定できます。通信ができなくなった場合になにもしない設定、分数指定、指定時間後または指定日数後に端末をロックもしくはワイプする設定ができます。ワイプを選択した場合、データ削除方式と BitLocker 方式から選択することができます。デフォルトは、「なにもしない」に設定されています。

(iii) ロックメッセージ

管理サーバと通信できずに端末をロックした時、端末画面に表示するメッセージの設定ができます。メッセージは 200 文字まで登録可能です。デフォルトは、設定されていません。設定セットを用いて端末をリモートロックしたときは、設定セットで登録されているメッセージが表示されます。

(iv) 端末でのリモートロックの解除方法

リモートロックの端末での解除方法を設定できます。なしに設定した場合は管理サイトからのみロックを解除でき、解除コードを設定した場合は端末からもロックを解除できるようになります。解除コードは、4 文字以上 20 文字以下の半角英数字が設定可能です。デフォルトでは、ランダムな解除コードが設定されています。

(v) 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

ライセンスの解除やエージェントのアンインストールする際のパスワードの設定ができます。パスワードを設定しない場合は、制限なしに設定します。パスワードは、4 文字以上 20 文字以下の半角英数字が設定可能です。デフォルトでは、制限なしに設定されています。

(vi) 管理サイトログイン画面へのリンク

Windows エージェントのタスクトレイメニューに、管理サイトへのログインリンクを載せるか否か、設定することができます。

(c) システム診断

CPU 温度やシステムドライブ状態の異常およびドライブ空き容量の診断、デフラグや復元機能を有効化することができます。

(i) ドライブ空き容量診断

システムドライブの空き容量が小さくなってきた時に、MDM のログにアラートを出力します。空き容量のしきい値は Windows XP では 200MB 以下、Windows Vista 以降では 950MB 以下です。

(ii) デフラグを自動実行する

Windows 端末においてデフラグを自動実行させる設定を行います。機能に対応しているのは Windows Vista 以上の Windows 端末です。

(iii) システムドライブの復元を有効化する

システムドライブの復元機能が有効化されていなかった時、それを有効化します。

(iv) CPU 温度診断

CPU 温度が一定値以上になったとき、MDM のログにその旨を出力します。温度のしきい値、摂氏 70 度です。

(v) ハードディスク温度診断

S.M.A.R.T 対応ハードディスクの異常を診断し、MDM のログへその旨を出力します。SSD も対応します。しきい値は、S.M.A.R.T 検査項目に「現在の値またはワースト値が閾値以下である」ものが存在していることです。

(vi) Internet Explorer の新しいバージョンを自動的にインストールしない

最新の Internet Explorer が公開された場合でも、新しいバージョンを自動的にインストールさせないよう設定することができます。

(d) **システムセキュリティ**

ファイアウォールや自動更新の有効化、Guest アカウント無効化等セキュリティに関する設定を強制適用、ウイルス対策ソフトやスパイウェア対策ソフトのインストール状況を診断することができます。また、その他各 Office アプリ（★対象とする Office アプリを明記）やインターネットオプション項目について設定を適用することができます。

(i) ファイアウォール有効化

Windows のファイアウォールを有効化、もしくはファイアウォールが有効か否かをログへ出力します。

(ii) Windows の Guest アカウント無効化

Guest アカウントを無効化、もしくは Guest アカウントが無効化されているか否かをログへ出力します。

(iii) Windows 自動更新設定

Windows の自動更新を実施する設定へ変更、もしくは自動更新が有効になっているか否かをログへ出力します。

(iv) スクリーンセーバー解除時に「ようこそ」画面へ

スクリーンセーバーを加除した後に、パスワード入力を促すために「ようこそ画面」を表示する設定を行うか、この設定が有効か否かをログへ出力します。

(v) ウイルス対策ソフト

ウイルス対策ソフトがインストールされているか、機能が有効になっているか、パターンファイルが最新になっているかをログへ出力します。

(vi) スパイウェア対策ソフト

スパイウェア対策ソフトがインストールされているか、機能が有効になっているか、パターンファイルが最新になっているかをログへ出力します。本機能は Windows XP には非対応です。

(e) MS Office ライセンス管理

MS Office ライセンス数の確認をすることができます。保有数、使用数、残数、未認証数の集計、アップグレード/ダウングレードに伴うライセンス数の調整および確認ができ、CSV にてダウンロードすることも可能です。
※Office 365 には対応していません。

(f) 位置情報管理

Windows 機器の位置情報を取得するか否か、設定することができます。
Windows 8.1 以上の端末が対象となります。

39) Windows 端末使用制限機能

Windows 端末を管理する為の以下の設定ができます。

(a) アプリケーション禁止機能

Windows でのアプリケーション機能を禁止する機能です。実行ファイル名、もしくはウィンドウ名でアプリケーションの起動を禁止設定することができます。

(i) 実行ファイル名でアプリケーション禁止設定

禁止するアプリケーション名と実行ファイル名(exe)もしくはパッケージファミリー名を設定することでアプリケーションの起動を禁止設定することができます。

※実行ファイル名に(.exe)は含みません。

(ii) ウィンドウ名でアプリケーションを禁止設定

禁止するアプリケーション名とウィンドウ名設定することでアプリケーションの起動を禁止設定することができます。条件は「と一致する」「を含む」を含むことが可能です。

(b) 外部デバイス禁止機能

USB メモリ等の USB 大容量記憶装置の使用可否設定をすることができます。USB ストレージの一括での許可と禁止、USB ストレージの製品・個体ごとの許可・禁止(ホワイトリスト)を設定できます。SD デバイスおよび IEEE1394 も制限可能です。

※禁止設定は、禁止(ストレージへの書き込み)、禁止(ストレージのみ)、禁止(ストレージおよびポータブルデバイス)、禁止(USB 受電以外すべて)から選択可能です。

※本機能は Windows 端末を再起動することで有効となります。

(c) CD/DVD/ブルーレイ禁止機能

Windows 端末の CD/DVD/ブルーレイドライブの使用を禁止設定することができます。

※本機能は Windows 端末を再起動することで有効となります。

(d) Wi-Fi フィルタリング

Wi-Fi 接続時に、接続を許可する SSID および MAC アドレスを指定することができます。SSID および MAC アドレスの組み合わせは、300 件まで登録することができます。MAC アドレスは入力を省略することができます。入力を省略した場合は SSID のみで判断、入力されている場合は SSID および MAC アドレスでフィルタリング対象か否かを判断します。

(e) スクリーンロック

ロック解除失敗時の動作として、ロックもしくはワイプのどちらかが動作する解除失敗回数および動作を設定することができます。また、スクリーンセーバーや端末のパスワードポリシーを設定可能です。

(i) スクリーンセーバー

有効/無効、パスワードを保護する機能を有効/無効にする、およびタイムアウトの時間を設定することができます。

(ii) パスワードポリシー

端末のパスワードポリシーとして、最小文字数や有効期間、履歴記録数、変更禁止期間、複雑なパスワードを強制させるか否かを設定することができます。

40）Windows 端末セットアップ機能

(a) **暗号化機能**

BitLocker を用いた暗号化設定の有効化・無効化の設定をすることができます。

※リムーバルディスク等は対象外とします。

※暗号化の有効化および無効化の動作に関して、すべての Windows 端末で正しく動作することを保障いたしかねます。事前にデータが入っていない Windows 端末にて、動作検証をいただくことを推奨いたします。

(b) **プロキシ**

プロキシの設定値を適用すること、および無効化することができます。対応するプロトコルは HTTP、Secure、FTP、Socks となります。また、例外設定を適用できます。ユーザーが手動で設定値を変更した場合、自動的に本設定セットの値が適用されます。本設定は、インターネットオプションの[LAN 設定タブ]配下のプロキシ設定値を変更します。

1-5 サーバー制約事項

i. 管理サイトの仕様の制限

iOS 端末登録時 100 回に 1 回程度、管理サイトから構成プロファイルのインストール時に失敗することがあります。再度ライセンス認証で回避できます。

ii. 構成プロファイルの適応タイミングに関する制限

本サービスから配信された構成プロファイルが iOS デバイスに適応されるタイミングは以下のとおりです。

構成プロファイルが適応されるタイミング

	ロック状態	アンロック状態
インストール	×	○
削除	○	○
更新(上書き)	×	○

デバイスの状態によっては、構成プロファイルが適応されない場合もありますので、ご注意ください。

iii. プロファイル削除時の管理外通知に関する制限

iOS 端末にて本サービスにライセンス認証する際に入るプロファイルは、手動による削除をすることにより本サービスの管理外となります。管理外に関しては通知設定内のログメール通知にある「管理外検知」を選択することで管理者にメールを送ることができます。ただし、iOS 端末が以下の場合は管理外検知が行えません。

① 機内モード。

② 3G/4G LTE や Wi-Fi 等の通信が行えない環境。

iv. インストールできるプロファイルの条件に関して

iPhone 構成ユーティリティにて、作成したプロファイルを登録し iOS 端末に適応させるためには以下の条件が必要です。

① [必須](赤矢印表示) 項目に値が入っていること。

② 個別項目(ユーザ名やパスワード等)に空欄がないこと。

※Apple による iPhone 構成ユーティリティの配布は終了しております。

構成プロファイルの作成には、Apple Configurator をご利用ください。

2. 稼働維持のための指標

2-1 本サービスにおける稼働維持のための指標

本サービスは以下指標を目標としております。

1) サービス時間 ２４時間３６５日（保守等やバージョンアップによる計画停止やAPNs 停止を除く）
2) サービス稼働率（年間） ９９．６％（保守等やバージョンアップによる計画停止やAPNs 停止を除く）
3) サポート時間 受付時間：（電話）９：００～１８：００ 土日祝日および当社指定の休業日を除く（メール）２４時間３６５日受付
4) 最大停止時間 24 時間
5) システム監視基準 １時間毎の稼働確認（H／W、ネットワーク）
6) サービス停止を伴う障害の通知時間 5 時間以内
7) オンライン応答時間 平均応答時間３秒以内（データセンタ内）
8) バックアップの方法 日次でフルバックアップ。日次内で一定時間ごとに差分バックアップ。
9) 業務データのバックアップ保存期間 原則１年
10) セキュリティ要件（公的認証取得の要件） ＩＳＭＳ認証およびプライバシーマークを取得。

3. その他

3-1 本仕様書の改定

本仕様書に記載された内容は、サービスの仕様変更等の理由により予告なく改定する場合がありますので、あらかじめご了承ください。

4. Appendix

4-1 対応端末・OS

各種OSや機器に関するアップデートは発売から2ケ月以内に対応の可否を判断する予定です。また、すべてのOSやすべての端末への対応を保障いたしかねます。

プラットフォーム	OS	補足
Android 端末	2.3	-
	3.0	-
	3.1	-
	3.2	-
	4.0	-
	4.1	-
	4.2	-
	4.3	-
	4.4	-
	5.0	-
	5.1	-
	6.0	-
	7.0	-
iOS 端末	4.3 以上	エージェントアプリは非対応
	5.0 以上	5.1.1 未満においては、 エージェントアプリは非対応
	6.0 以上	-
	7.0 以上	-
	8.0 以上	-
	9.0 以上	-
	10.0 以上	-
Windows 端末	Windows 7 Starter	-
	Windows 7 Home Premium	-
	Windows 7 Professional	-
	Windows 7 Ultimate	-
	Windows 8 Pro	-
	Windows 8 Enterprise	-
	Windows 8.1	-

	Windows 8.1 Pro	-
	Windows 8.1 Enterprise	-
	Windows 10 Home	
	Windows 10 Pro	
	Windows 10 Enterprise	
	Windows Server 2008	
	Windows Server 2008 R2	
	Windows Server 2012	
	Windows Server 2012 R2	
Mac 端末	Mac OS X 10.7 以上	-
	OS X 10.8 以上	-
	OS X 10.9 以上	-
	OS X 10.10 以上	-
	OS X 10.11 以上	-
	macOS 10.12 以上	-

・iOS の対応バージョン記載は MDM 構成プロファイルの対応 OS となります。
エージェントアプリに関して、iOS 5.1.1 未満においては非対応となります。

・Windows7 、Windows8、Windows8.1、Windows10 は 32 ビット版と 64 ビット版に対応。
Windows8、Windows8.1、Windows10 の Modern UI は非対応。いずれの OS も日本語版のみ対応。

・Windows Server は 32 ビット版と 64 ビット版に対応。Windows Small Business Server 2011 にも対応。また、x86 アーキテクチャ版のみ対応し、Itanium-based Systems 版は非対応。

※Microsoft 社による Windows Vista のサポートは、2017 年 4 月 11 日(日本時間)に終了しました。
たよれーる デバイスマネジメントサービスにて直ちに動作しなくなる事はありませんが、後継の OS に移行されることを推奨いたします。Windows Vista に起因するトラブルに関して、弊社では解決できない場合がありますのでご了承ください。

・Android 端末の機器別対応端末は、ヘルプ内の[Home] - [デバイスマネジメント機能ついて] - [Android 検証端末]参照、もしくは下記 URL を直接入力ください。
（http://campaign.otsuka-shokai.co.jp/mmm/management/android.html）

・Mac OS X Server は非対応。

4-2 動作環境（管理サイト）

対応ブラウザー	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。
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。

i. **対応ブラウザーのインストール方法や設定等、また OS に依存する設定に関しては対応いたしかねますので、ご了承ください。万が一動作に不備等で運用が困難な場合がございましたら、異なる対応ブラウザーや OS にてご利用ください。**

4-3 端末側制約事項

i. Android OS 仕様の制限

・Android 6.0 以降の端末では、MAC アドレスの取得が行えない場合があります。

・Android 7.0 以降の端末では、デバイスオーナーモード化していない場合、エージェントのアンインストールの抑止、および管理サイトからのスクリーンロックパスワードの変更が行えません。

・Android のマルチユーザーアカウントを使用した環境には対応しておりません。

ii. iOS 仕様の制限

・ロックしていない状態の端末を iTunes で同期しているとき、リモートロックを行うと、ロックされず、管理サイトの操作ログにロック済みの旨のログが残ります。同期完了後もロック状態ではなくホーム画面が表示されます。

・ライセンス認証完了後にインストールされる MDM 用の構成プロファイルを利用ユーザーが削除可能です。（DEP を利用し、必要な設定を行っている場合を除く）

・位置情報を取得するためには、エージェントアプリケーションがバックグラウンドで動作している必要があります。

・Apple サービスサーバーの稼働状態により、アプリケーション配信等の一部機能の動作に影響がおよぶ場合があります。

iii. Mac OS 仕様の制限

・Mac 端末でリモートロック、リモートワイプを行うには、ご利用いただく OS と同一バージョンの復元パーティションから起動が行える必要があります。

4-4 エージェント収集情報

カテゴリ	項目	補足
Android 端末情報	機器名	-
	モデル名	-
	電話番号	SIM あり端末のみ
	ネットワークモード	3G または Wi-Fi
	ネットワークオペレータ	SIM あり端末のみ
	端末の識別番号(IMEI)	-
	ファームウェアバージョン	-
	ビルド番号	-
	シリアル番号	V-T500-J のみ以下の表記： （独自製造番号）/（シリアル番号）
	SIM の識別番号(IMSI)	SIM あり端末のみ
ネットワーク情報	MAC アドレス	-
	IP アドレス	-
Bluetooth 情報	Bluetooth 状態	-
位置情報	無線ネットワーク	-
	GPS 機能	-
位置情報取得	位置情報取得可否	有効/無効。
バッテリー情報	バッテリー残量	-
	バッテリー状態	-
スクリーンロック	パスワードのポリシー	-
	パスワードの再利用	-
	パスワードの有効期限	-
	自動ロックまでの時間	-
	ロック解除失敗時の設定	ロックをかける、ワイプを行う等
端末ロック	端末ロック状態	端末がロックされているかどうか
暗号化	暗号化状態	Android 3.0 以降のみ
Root 化	Root 化状態	-
	検知内容	-

位置情報	緯度	-
	経度	-
インストール済み **アプリケーション情報**	アプリケーション名	-
	バージョン名	-
	メモリサイズ	アプリケーションサイズ、データサイズ、キャッシュサイズの合計値
	パッケージ名	-
	バージョン番号	-
	アプリケーションサイズ	-
	データサイズ	-
	キャッシュサイズ	-

※ 端末の状態や OS の仕様変更によって取得されない情報があります。

カテゴリ	項目	補足
iOS 端末情報	機器名	-
	デバイス名	-
	電話番号	-
	現在のキャリアネットワーク	3G
	ホームのキャリアネットワーク	3G
	IMEI	SIM あり端末のみ
	MEID	-
	OS バージョン	-
	ビルドバージョン	-
	モデル名	-
	モデル番号	-
	モデルファームウェア バージョン	-
	シリアル番号	-
	Exchange ActiveSync デバイス ID	-
	MDM プロファイルトピック	-
	UDID	
	iCloud	
	前回の iCloud バックアップ日時	
ネットワーク	SSID	-
	Bluetooth MAC アドレス	-
	Wi-Fi MAC アドレス	-
	インターネット共有 （テザリング）	-
監視対象	監視対象	-
バッテリー情報	バッテリー残量	-
ストレージ	デバイス容量	-
	利用可能なデバイス容量	-
スクリーンロック	パスコード保護	-
	パスコード準拠状況 （デバイス）	-
	パスコード準拠状況 （プロファイル）	-

OS アップデート情報	アップデートの名前	-
	アップデートのバージョン	-
	アップデートのビルド番号	-
	重要なアップデートかどうか	-
	アップデートのステータス	常時"(Unknown)"表示
ローミング	音声ローミング設定	-
	データローミング設定	-
	ローミング状態	-
暗号化	ハードウェア暗号化レベル	-
JailBreak	JailBreak 状態	-
その他の情報	iTunes Store アカウント	-
	iTunes Store アカウントハッシュ	-
	アクティベーションロック	-
	ロケーターサービス	-
	BypassCode	-
	紛失モード	-
	Shared iPad 設定	-
	Shared iPad ユーザー最大数	-
	おやすみモード	-
インストール済み アプリケーション情報	アプリケーション名	※プリインストールアプリは 表示されません。
	バージョン名	-
	メモリサイズ	-
	アプリケーション ID	-
	アプリケーションサイズ	-
	データサイズ	-
プロファイル	構成プロファイル	-
	プロビジョニングプロファイル	-
	証明書	-
位置情報	緯度	-
	経度	-

Apple School Manager	名前	-
	Managed Apple ID	-
	Unique Identifier	-
	Source	UI 上表示無し
	Grade	同上
	User ID	同上
	Class Name	同上
	Class Unique Identifier	同上
	Class Source	同上
	Class Source Identifier	同上
	Class room	同上
	Location Name	同上
	Location Unique Identifier	同上
	Location Source System Identifier	同上
	Location Source	同上

カテゴリ	項目	補足
Windows 端末情報	機器名	
	コンピューター名	-
	ワークグループ名	-
	Windows バージョン	-
	Windows プロダクト ID	-
	システム製造元	-
	システムモデル名	-
	シリアル番号	-
	コンピューターSID	-
ネットワーク	NIC 名	-
	接続方法	-
	MAC アドレス	-
	IP アドレス	-
	デフォルトゲートウェイ	-
	DHCP	-
	DHCP サーバー	-
	DNS サーバー	-

	DNS サフィックス	-
	ネットワーク	-
	電話番号	-
	IMEI/MEID	-
	現在のキャリアネットワーク	-
	SSID	取得のみ実施
	接続中 SSID の MAC アドレス	取得のみ。
ハードウェア	種別	-
	CPU	-
	メモリ	-
	マザーボード	-
	ビデオカード	-
	TPM	-
BIOS	メーカー	-
	Version	-
	日付	-
ドライブ	総容量	-
	空き容量	-
ログオンユーザー	ユーザー名	-
	SID	-
	既定の Web ブラウザー　名前	-
	既定の Web ブラウザー バージョン	-
	既定の電子メールプログラム 名前	-
	既定の電子メールプログラム バージョン	-
	通常使うプリンター　名前	-
	通常使うプリンター　ポート	-
リモートロック	リモートロック　状態	-
パスワードポリシー	文字数	-
	有効期間	-
	履歴記録数	-
	変更禁止期間	-
	複雑なパスワードを強制する	-

インストール済み アプリケーション情報	アプリケーション名	-
	バージョン名	-
	インストール日	-
	アプリケーションサイズ	-
	発行元	-
	インストール先	-
	パッケージファミリー名	-
	プロダクト ID	-
セキュリティ	Windows 自動更新	-
	ファイアウォール	-
	ウイルス対策ソフト	-
	スパイウェア対策ソフト	-
	スクリーンセーバー	-
	ドライブ暗号化	-

位置情報	緯度	-
	経度	-
	精度	-
	取得時刻	-

カテゴリ	項目	補足
Mac OS 端末情報	デバイス名	-
	OS バージョン	-
	ビルドバージョン	-
	モデル名	-
	モデル番号	-
	シリアル番号	-
	MDM プロファイルトピック	-
ネットワーク	Bluetooth MAC アドレス	-
	Wi-Fi MAC アドレス	-
	Ethernet MAC アドレス	-
	グローバル IP アドレス	-
ストレージ	デバイス容量	-
	利用可能なデバイス容量	-
暗号化	暗号化有無	-

	パーソナル復旧キー	-
	所属団体の復旧キー	-
プロファイル	構成プロファイル	-
	証明書	-
インストール済み **アプリケーション情報**	アプリケーション名	-
	アプリケーション ID	-
	バージョン	-
	アプリケーションサイズ	-

4-5 バックアップ･復元項目一覧

大項目	小項目	バックアップ	復元
システム設定	機内モード	○	○
	タッチ操作音	○	○
	選択時の操作音	○	○
	入力時バイブレーション	○	○
	画面の明るさ	○	○
	アニメーションの表示	○	○
	バックライト消灯	○	○
	パスワードを表示	○	×
	スリープモードにしない	○	×
	日付と時刻の自動	○	○
	24 時間表示	○	○
	日付形式	○	○
セキュリティ設定	Bluetooth	○	×
	データローミング	○	×
	GPS 機能を使用	○	×
	提供元不明のアプリ	○	×
	USB デバッグ	○	×
	疑似ロケーションを許可	○	×
	読み上げ設定を使用	○	×
	音声の速度	○	×
Wi-Fi 設定	Wi-Fi 有効	○	○
	Wi-Fi スリープ設定	○	○
	DHCP 有効	○	○
	IP アドレス	○	○
	ゲートウェイ	○	○
	ネットマスク	○	○
	DNS1	○	○
	DNS2	○	○
	Wi-Fi ネットワーク(SSID)	○	○
	SSID 非表示	○	○

	Wi-Fi ネットワーク(Key)	○	○
	Wi-Fi ネットワーク(パスワード) ※管理画面からの設定した場合のみ。	○	○
お気に入り設定	タイトル	○	○
	アドレス	○	○
	作成日	○	○
	アクセス回数	○	○
	最終アクセス日	○	○
電話帳情報	名前	○	○
	名字	○	○
	敬称	○	○
	名前のカタカナ	○	○
	名字のカタカナ	○	○
	電話番号	○	○
	電話番号タイプ	○	○
	電話番号ラベル	○	○
	Email アドレス	○	○
	Email タイプ	○	○
	Email ラベル	○	○
	住所タイプ	○	○
	住所ラベル	○	○
	住所(番地)	○	○
	住所(町名)	○	○
	住所(市区町村)	○	○
	住所(都道府県)	○	○
	住所(国)	○	○
	近地情報	○	○
	住所の郵便番号	○	○
	IM アドレス	○	○
	IM タイプ	○	○
	IM ラベル	○	○
	IM プロトコル	○	○
	プロトコルラベル	○	○
	組織名	○	○

	組織タイプ	○	○
	組織ラベル	○	○
	役職	○	○
	所属	○	○
	仕事内容	○	○
	組織読み仮名	○	○
	組織所在地	○	○
	イベント日付	○	○
	イベントタイプ	○	○
	イベントラベル	○	○
	Web アドレス	○	○
	Web アドレスタイプ	○	○
	Web アドレスラベル	○	○
	ニックネーム	○	○
	ニックネームタイプ	○	○
	ニックネームラベル	○	○
	関係者	○	○
	関係タイプ	○	○
	関係ラベル	○	○
	備考	○	○

i. **バックアップ・復元項目に関する注意事項**

1) 本一覧はすべての端末にて確認したものではございません。システムとして取得できる値です。
2) 当社ではすべての端末において各項目のバックアップと復元に関して調査は行っておりません。
3) 各端末による動作はお客様にてご確認いただき、ご理解いただいた上でご利用ください。
4) 端末により設定項目にてバックアップ・復元できないことがあります。
5) 端末により取得した情報を別の形で書き出し、閲覧、再利用する方法はありません。
6) 端末により取得した情報のすべてを確認する方法は提供しておりません。
7) 端末に存在しない設定項目に関しては、バックアップ・復元できません。
8) 異なる機種間でのバックアップ・復元では、バックアップ・復元できない項目があります。
9) セキュリティ設定は将来のバージョンのための予約で、現状は復元できません。
10) たよれーる デバイスマネジメントサービスでバックアップを保持する期間は、バックアップ正常取得後 1 年間です。

4-6 用語集

用語	説明
お客様	本サービスをご利用いただく管理者様
オペレータ	本サービスを用いてお客様の対応を行うもの
Android 端末	本サービスを用いたサポートの対象となるお客様の Android 端末
iOS 端末	本サービスを用いたサポートの対象となるお客様の iOS 端末
Windows 端末	本サービスを用いたサポートの対象となるお客様の Windows 端末
Mac 端末	本サービスを用いたサポートの対象となるお客様の Mac 端末

4-7 個人情報保護方針その他

本保護方針は当社が保有する個人情報を適切に管理運用するために、遵守するべき基本的事項を定めたものです。

1.法令・規範の遵守
当社は個人情報の取り扱いに関する法令、国が定める指針その他の規範を、常に最新状態に維持するとともにこれを遵守いたします。

2.適切な情報管理の徹底
当社は個人情報の管理者を任命し、個人情報の不正利用・紛失・破壊・改ざん、および漏えいに対し適切な予防ならびに是正に関する措置を講じます。また、すべての就労者に対し「個人情報の取り扱い」についての教育訓練を行い、適切な管理に取り組みます。尚、企業情報についても個人情報と同様に適切な管理をいたします。

3.取得目的と範囲
当社は個人情報をお預かりする際には、その利用目的を明らかにして、必要な範囲で取得いたします。また、同意を得た利用目的の範囲あるいは法令・規範に基づく要請の範囲（以下、「利用目的等の範囲」）を越えた利用、提供、取り扱いの委託は行いません。

4. 利用等の制限と管理
当社は個人情報を守秘し、利用目的等の範囲あるいは法令・規範に基づく要請の範囲を越える取り扱いを行わないよう、適切に管理します。
また、利用目的等の範囲に基づき、社外と個人情報の授受を行う場合には、厳格な管理の下で取り扱うよう、当社が監理いたします。

5. 個人情報保護マネジメントシステムの確立と継続的改善
当社は取り扱う個人情報を適切に行うよう規程類および体制を整備して、個人情報保護マネジメントシステムを構築・実施し、これらを継続的に改善してまいります。

6. 個人情報の相談および苦情窓口
当社は「個人情報相談窓口」を設置し、ご本人からの個人情報に関するお問い合わせや苦情に対して、適切かつ誠実、迅速に対応いたします。
開示対象個人情報について、ご本人からの利用目的の通知、開示、内容の訂正、追加、削除、利用の停止、および第三者への提供の停止要請を受け付け、合理的に対処いたします。

制定：平成 16 年 9 月 24 日
改訂：平成 25 年 5 月 15 日

個人情報の取り扱いに関しては詳細下記 URL もご確認ください。
http://www.otsuka-shokai.co.jp/privacy/

4-8 免責事項

・故意や正常な操作に関わらず、管理サイトをご利用いただいたことにより生じる直接的また間接的な損失に対して当社および関連会社には一切責任を負うものはありません。
・故意や正常な操作に関わらず、各デバイスに対するワイプを実行した結果、端末内のデータが消えても当社および関連会社にはデータ復旧や再設定のための作業等一切責任を負うものはありません。
・Android 端末のバックアップ機能に関して記載されている、すべてのデータが過不足なく取得し、復元できることの保障はいたしかねます。重要なデータ等は必ず別途バックアップを取得ください。
・本サービスの設定により、各端末との通信が増えることが想定されます。キャリアモデルの場合はパケット定額プランを推奨します。また設定により、定額プランの上限値を超えないか等の確認はお客様にて行ってください。
・本サービス仕様は予告なしに変更を行う可能性があります。なお、当社は理由の如何に関わらず、情報の内容および変更により生じるお客様の直接的または関節的な損失に関しても、一切責任を負うものではありません。
・本仕様書情報の正確性を保障するものではありません。