サービス仕様書

第 9 版（Ver3.2）

2015 年 7 月 3 日

ナレッジスイート株式会社

目次

1. 基本サービス

MDM+（以下、本サービス）は、ナレッジスイート株式会社が提供する、貴社の社内で管理されるモバイルデバイス（スマートフォン、タブレット）を遠隔で管理するサービスです。

【機能一覧】

区分	機能	説明	iOS	Android	Windows 8.1
管理	ユーザー管理	ユーザー情報の登録・変更・管理をする機能。 ユーザー別のデバイス管理をすることができる。	○	○	○
	チーム管理	登録されたユーザーからチームを作成して管理する機能。 チーム単位でポリシーの適用、メッセージの送信、ドキュメントやアプリの配布等をすることができる。	○	○	○
	デバイス管理	デバイス情報の登録・変更・管理をする機能。 管理状態のステータスや、インストールされているアプリ一覧を確認できる。 また、デバイス別に各種設定をすることができる。	○	○	△ ※デバイス情報表示画面ロックのみ
設定	ポリシーの設定	ポリシーの設定・管理をする機能。 パスコード、デバイスの機能制限、アプリケーション制限、コンテンツ制限等、セキュリティに関するポリシーを設定することができる。	○	○	－
	プッシュ通知	デバイスにプッシュメッセージを送信する機能。（最大入力　1024 bytes）	○	○	－
	MCM （モバイルコンテンツ マネジメント）	ドキュメントの管理及びモバイル端末への配布をする機能。	○	○	－
	MAM （モバイルアプリケーション マネジメント）	アプリケーションの管理及びモバイル端末への配布をする機能。 インストールされたアプリケーションを管理する他、使用禁止アプリを設定することもできる。	○	○	－
	住所録の配布	取引先の電話番号や住所等の情報を各モバイル端末に一括登録する機能。 配布した住所録のリモート更新及び削除することもできる。	○	○	－
	位置情報の取得	デバイスの位置情報を取得する機能。 現在地のほか、移動経路の履歴確認が可能。 住所録データと GPS 機能を連動させることで、取引先企業を画面に表示、近くにいる社員に業務指示を出すことができる。	○	○	－
	操作ログ	管理者が行った操作ログを確認する機能。	○	○	－
	MDM 無効化防止	MDM のプロファイルを削除した時に、MDM の管理機能が無効になってしまうことを阻止する機能。	○	○	－

1.1.ユーザー管理

ユーザー管理画面では以下の項目を管理することができます。

【機能一覧】

アクション	詳細
ユーザー登録	管理するユーザーを登録する。 csv ファイルで一括登録することも可能。
ユーザー情報管理	登録されたユーザーの情報を管理（編集・削除）する。 【管理する項目】 ・姓/姓の読み ・名/名の読み ・部署 ・社員番号 ・権限（管理者/ユーザー） ・メールアドレス
デバイスの登録	ユーザーの所有するデバイスを登録する。 csv ファイルでユーザーと同時に一括登録することも可能。 （※Android OS のみ対応）
ユーザーごとの所有デバイスの表示	各ユーザーが所有するデバイスが一覧表示される。 デバイスの詳細画面へ遷移することができる。 ※1-3「デバイス管理」参照

1.2.チーム管理

登録されたユーザーからチームを作成して管理します。

チーム管理画面ではチームに所属するユーザーのデバイスに、以下の操作を一括で行うことができます。

【機能一覧】

アクション	詳細
ポリシー設定の適用	※1-4「ポリシーの設定」参照
ドキュメントの配布	※1-5「ドキュメントの配布」参照
アプリの配布	※1-6「アプリの配布」参照
住所録の配布	※1-7「住所録の配布」参照
位置情報の取得	※1-8「位置情報の取得」参照
メッセージ送信（プッシュ通知）	デバイスにプッシュメッセージを送信する。(最大入力　1024 bytes)

1.3.デバイス管理

デバイス管理画面では、登録されたデバイスに以下の操作を行うことができます。

【機能一覧】

アクション	詳細
ポリシー設定の適用	※1-4「ポリシーの設定」参照
ドキュメントの配布	※1-5「ドキュメントの配布」参照
アプリの配布	※1-6「アプリの配布」参照
住所録の配布	※1-7「住所録の配布」参照
位置情報の取得	※1-8「位置情報の取得」参照
メッセージ送信（プッシュ通知）	デバイスにプッシュメッセージを送信する。(最大入力　1024 bytes)
画面ロック	デバイスの画面をロックする。

パスワード初期化	デバイスに設定されていたパスワードを初期化する。
工場初期化	デバイスを工場出荷時の状態に初期化する。
所有者の変更	デバイスの所有者を変更する。
デバイス削除	デバイスを MDM+のリストから削除する。
端末管理状況	端末ライセンスをはじめ、管理下にある端末の OS 種別/バージョン、情報更新状態など一覧で把握できます。

【ステータスの表示】

デバイス名の右側にあるカラー表示がそれぞれのデバイスの状態を示しています。

表示色	内容
緑	MDM+によって正常に管理されているデバイス
黄	MDM+の管理が出来なくなっています。 iOS の場合：端末上の MDM プロファイルが削除されました。 Android の場合：端末の[デバイス管理機能]設定がオフになっています。 Windows8.1 の場合：端末の「社内ネットワーク/デバイス管理」設定がオフになっています。

【デバイス情報に表示される情報】

項目名	詳細	iOS	Android	Windows 8.1
IMEI	International Mobile Equipment Identity （IMEI） 。GSM/W-CDMA/iDEN など全ての携帯電話や一部の衛星電話に付与される識別番号	○	○	―
モデル	該当機器のモデル名	○	○	○
内部容量(使用可/全体容量)		○	○	○
外部容量(使用可/全体容量)	SD カードなど Android のみ該当	―	○	○
OS	OS のバージョンの表示	○	○	○
製造	製造メーカー	○	○	―
シリアルナンバー	製造メーカーから付与される製品番号	○	○	○
キャリア	通信事業者。ただし、WI-FI のみ利用するモデルの場合には「不明」と表示される	○	○	―
現在のポリシー	現在のポリシー名が表示	○	○	―
MDM+バージョン	現在デバイスにインストールされているバージョンの表示	○	○	―
デバイス名	デバイス名を表示	○	―	○
データ暗号化		―	○	―
Data Roaming 可否		○	○	○
バッテリーレベル		○	○	―
SIM カード番号（ICCID）	SIM カードの固有番号	○	○	―
電話番号		○	○	―
Wifi Mac Address	ネットワーク機器のハードウェアに（原則として）一意に割り当てられるユニークな番号	○	○	○
WifiEnabled		―	―	○
BluetoothEnabled		―	―	○
PC SettingsSyncEnabled		―	―	○
Rooting / Jailbreak	Android 端末において、ルート権限でシステムを操作できるように改造されたか否か、また、iOS 端末において、Apple の認可を受けていないソフトウェアをインストールできるように改造されたか否かを表示	△	△	―

デバイス情報更新日時	デバイス情報が更新された日時	○	○	○

デバイス情報を更新したい場合に「更新する」とクリックします。
クリックすると該当デバイスに情報を更新するための信号が送信されます。
デバイスの状況により反映までに時間が掛かります。数分後にご確認ください。
【アプリ利用状況】
インストール済のアプリ名とバージョン、禁止アプリ名とバージョンを確認することができます。
MDM+エージェントアプリを操作したタイミングで更新されます。
【ログ履歴】
各デバイスのログを確認することができます。(ポリシー/リモートロック/リモートワイプ/パスコードの初期化の成功/失敗のログ)

1.4.ポリシーの設定

パスコード、デバイスの機能制限、アプリケーション制限、コンテンツ制限等、セキュリティに関するポリシーを設定することができます。設定したポリシーはチーム単位、デバイス単位で適用が可能です。
設定できる項目はデバイスの OS によって異なります。(Windows8.1 は非対応)

【設定できる項目（iOS)】

区分	機能	説明
パスコード	単純なパスコードを許可	簡単なパスコードを許可するか否かを指定。簡単なパスコードとは、同じ文字の繰り返し、あるいは単純上昇/下降形（123、CBA など）の文字列が含まれるもののこと。
	1 文字以上の英数字	英字を入力しなければならないか、数字だけでよいか指定。
	パスコードの最少文字数	パスコードの長さの最小値を指定。
	複合文字の最小文字数	「&%$#」のような英数字以外の複雑な文字の最小数を指定。
	パスコードの有効期限	パスコードを変更せずに利用できる最大日数を指定。
	自動ロックまでの最長時間	指定した上限時間デバイスがアイドル状態になると、デバイスを自動ロックする。
	パスコードの履歴	過去パスコードの重複を確認。最小値は 1 で、最大値は 50。
	デバイスロックの最長猶予期間	パスコードを再入力せずにデハイスのロックを解除できる時間。「すぐ」を選択するとロックされる毎度パスコードを要求されます。
	ロックまでの入力失敗回数	指定した回数を超えて入力に失敗すると、デバイスを工場初期化する。
機能制限	カメラの使用を制御	制御すると、カメラが無効になり、ホーム画面のカメラアイコンが削除され、写真やビデオを撮ることができない。（Face Time も制御される）
	Face Time を制御	制御すると、ユーザーは Face Time ビデオ通話の送受信ができない。
	フォトストリームを制御	iCloud のフォトストリームオプションを制御する。（制御するとデータ損失の可能性あり）
	画面の取り込みを制御	制御すると、ディスプレイのスクリーンショットを保存できない。
	アプリケーションのインストールを制御	制御すると、App Store が無効になり、ホーム画面のアイコンが削除され、Apple Store や iTunes を使用したアプリケーションのインストールやアップデートを行うことができない。
	App 内での購入を制御	制御すると、アプリケーション内課金を利用できない。
	iTunes パスワードを強制	購入したすべての項目の iTunes Store パスワードを要求する。
	マルチプレイヤーゲームを	制御すると、マルチプレイヤーゲームをプレイできない。

	制御	
	Game Center の友人追加を制御	制御すると、Game Center で友人を追加できない。
	iCloud バックアップを制御	iCloud のバックアップオプションを制御する。
	iCloud 書類の同期を制御	iCloud の書類の同期オプションを制御する。
	ローミング中の自動同期を制御	制御すると、ローミング中のデバイスはアカウントにアクセスしたときにのみ同期する。
	音声ダイヤルを制御	制御すると、ユーザーは音声コマンドを使用して電話をダイヤルできない。
	強制的に暗号化バックアップを制御	制御すると、iTunes で作成されたデバイスのバックアップを暗号化された形式でコンピュータに保存するかどうかを選択できる。制御しないと、iTunes によって強制的にバックアップの暗号化が行われる。 ※iPhone 構成ユーティリティによってデバイスにインストールされたプロファイルは常に暗号化されている。
	信頼できない TLS 証明書の受け入れを制御	制御すると、信頼できない TLS 証明書を受け入れることができない。
	Siri を制御	制御すると、Siri が無効になる。
	スクリーンロック中に Siri を制御	制御すると、スクリーンロック中に Siri を利用できない。
	iCloud キーチェーンを許可	このオプションをオフにすると、iCloud キーチェーンは無効になる。 「設定 > Icloutd > キーチェーン」項目が消えます。
	Touch ID によるデバイスのロック解除を許可	このオプションをオフにすると、ユーザーはデバイスのロックを解除するためにパスコードを入力する必要がある 「設定 > Touch ID とパスワード > iPhone ロックを解除」項目の設定ができない。
	ロック中の Passbook 通知を許可	このオプションをオンにすると、デバイスがロックされているときに Passbook 通知が表示される。 「設定 > パスコード > Passbook」項目の設定ができない。
	ロック画面にコントロールセンターを表示	このオプションをオフにすると、ユーザーは上にスワイプしてコントロールセンターを表示できなくなります。 「設定 > コントロールセンター > ロック画面でのアクセス」項目の設定ができない
	ロック画面に通知センターを表示	このオプションをオフにすると、画面がロックされている場合にユーザーは通知を受信できない。 「設定 > 通知センター > 通知の表示」項目の設定ができない。
	ロック画面に今日表示を表示	このオプションをオフにすると、ユーザーは下にスワイプして今日表示を使用する通知センターをロック画面で表示できない。 「設定 > 通知センター > 今日の表示」項目の設定ができない。
	証明書信頼設定の自動アップデートを許可	このオプションをオンにすると、iOS デバイスは既知の信頼できる証明書の信頼設定変更を自動的に受け入れるようになる。
コンテンツ制限	YouTube の使用	制御すると、YouTube アプリケーションが無効になり、ホーム画面のアイコンが削除される。
	iTunes Music Store の使用	制御すると、iTunes Music Store が無効になり、ホーム画面のアイコンが削除され、コンテンツのプレビュー、購入、ダウンロードを行うことができない。
	Safari の使用	制御すると、Safari Web ブラウザアプリケーションが無効になり、ホーム画面のアイコンが削除される。また、Web クリップを開くことができない。
	Safari での自動入力	制御すると、Web フォームに入力した内容を Safari が記憶しない。
	Safari の詐欺サイト警告機能	制御すると、詐欺または不正であると識別された Web サイトにアクセスしても、Safari が警告を発しない。
	Safari の JavaScript 利用	制御すると、Safari は Web サイトの JavaScript をすべて無視する。

	Safari のポップアップブロック	制御すると、Safari のポップアップブロック機能が無効になる。
	Cookie の受け入れ	Safari の Cookie ポリシーを設定する。すべての Cookie を受け入れるか、Cookie を受け入れないか、直接アクセスしていないサイトからの Cookie を拒絶するかを選択することができる。
監視対象デバイス	AirDrop を許可	オフにすると、ユーザーはアプリで AirDrop を使用できなくなります。
	iMessage を許可	オフにすると、iMessage を使用したメッセージの送受信ができなくなります。お使いのデバイスがテキストメッセージに対応している場合、テキストメッセージの送受信はできます。お使いのデバイスがテキストメッセージに対応していない場合は、ホーム画面から「メッセージ」アイコンが削除されます。
	iBook を許可	オフにすると、iBook Store が無効になり、ユーザーが「iBook」アプリから iBook Store にアクセスできなくなります。
	App の削除を許可	オフにすると、ユーザーはアプリを削除できるようになります。App Store や「iTunes」など、iOS に付属しているアプリをユーザーは削除することはできません。
	Game Center の使用を許可	オフにすると、「Game Center」が無効になり、ホーム画面からアイコンが削除されます。
	“友達を探す”設定の変更を許可	オフにすると、ユーザーは「友達を探す」アプリの設定を変更できなくなります。
	Apple Configurator 以外のホストとペアリングを許可	オフにすると、デバイスを任意の Mac と同期することができます。
	Web サイト制御 成人コンテンツを制限	Apple がアダルトコンテンツと判定した Web サイトへのアクセスを遮断します。
	Web サイト制御 指定した Web サイトのみ許可	アクセスを許可したい Web サイトは追加します。
カレンダー	カレンダー連携	カレンダーサーバーの接続情報を設定
連絡先	連絡先連携	連絡先サーバーの接続情報を設定
VPN	VPN 設定	VPN をご利用されるお客様向けに設定画面をご提供しています。※当画面で行う設定は、接続タイプは L2TP、PPTP、IPSec のみ対応
Web Clip	Web Clip 設定	デバイスのホーム画面に Web ページのリンクを追加可能
メール	メール連携	POP または IMAP メールを設定。連携されるメールアドレスは MDM＋のユーザー情報にて設定したメールアドレスとパスワードになります。
Excahange	Excahange 連携	Microsoft Exchange サーバーの接続情報を設定
Wi-Fi	Wi-Fi 連携	Wi-Fi の接続情報を設定
Black アプリ	使用禁止アプリのリスト表示及び追加、処理	※2【(iOS のみ) 使用禁止アプリを設定】参照
White アプリ	使用許可アプリのリスト表示及び追加・処理	ユーザーに必須アプリとして使用を強制したいアプリを登録及び配布することができます。White アプリが指定されたポリシーを配布された端末に、他のアプリをインストールした場合、管理者にメール通知、さらに MDM+アプリへの接続禁止に設定できます。
おすすめアプリ	おすすめアプリ設定	おすすめアプリに登録したアプリは MDM アプリのアプリリストに表示されます。

※1【(iOS のみ) 使用禁止アプリを設定】
インストールや起動そのもの自体を止めることはできません。使用禁止アプリがインストールされた場合、管理者は次のように３つのアクションを設定することができます。

アクション	説明
管理者とユーザーにメールで通知	禁止アプリをインストールした場合、メールにて通知します。
MDM+アプリへの接続制限及びメール通知	禁止アプリをインストールした場合、メールにて通知します。また、ユーザーのデバイスの MDM+アプリを利用できなくします。
デバイスの工場初期化	デバイスの工場初期化を選択すると､禁止アプリをインストールした瞬間に該当端末は初期化されてしまいます｡各利用ユーザーに禁止リストを徹底させ､お客様の責任において行ってください。

※2【(iOS のみ) 構成ユーティリティから設定をアップロード】
iOS 構成プロファイル(拡張子:.mobileconfig)を配布して VPN 構成情報､Wi-Fi 設定､APN 設定､Exchange アカウント設定、メール設定、Web クリップなどの設定ができます。
アップル社の iPhone 構成ユーティリティで設定した設定をそのまま MDM+の設定画面に反映できます。

複数の構成プロファイルを使うことができますが､同じ項目に対して両方の構成を機能させることはできません。

【ポリシーで設定できる項目 (Android)】

区分	機能	説明
パスコード	パスコードのタイプ	パスコードのタイプを指定します。 OS のバージョンにより、パスコードの設定が可能な条件に差異あり。
	パスコードの最少文字数	パスコードの長さの最小値を指定します。
	デバイスロックまでの最長時間	指定した上限時間デバイスがアイドル状態になると、デバイスを自動ロックします。
	ロックまでの入力失敗回数	指定した回数を超えて入力に失敗すると、デバイスを工場初期化します。
機能制限	カメラの使用を制御	制御すると、アプリでカメラ機能を使用できません。
	SD カードの使用を制御	制御すると、SD カードが解除され、利用できません。
	Bluetooth の使用を制御	制御すると、Bluetooth をオンにできません。
コンテンツ	デバイス「設定」へのアクセスを許可	「デバイス「設定」へのアクセスを許可」のチェックを外すと、ユーザーはアンドロイド端末の「設定」メニューに入れなくなります。つまりどのような設定も変更できません。 設定には十分気をつけてください。また、「パスコード設定」や「SD カードの使用禁止」などユーザーによる設定変更が必要なときはチェックを外さないでください。
	メール同期の使用を許可	アンドロイド端末は、最初の設定で、Google アカウントとパスワードを入力し、携帯上にある「Gmail」「カレンダー」、「連絡先」がそれぞれ PC 版の「Gmail」や「カレンダー」、「連絡先」と同期すると、常に PC からアクセスした内容と同じになります。 「メール同期の使用を許可」のチェックを外すと「設定」→「アカウントと同期」が off になり、自動的に同期しなくなります。（※アンドロイドのバージョンにより項目が違います。）
	データ暗号化の使用許可	データ暗号化を使用する場合にチェックします。
	YouTube の使用	制御すると、YouTube アプリケーションが無効になり、起動できません。
	ブラウザの使用	制御すると、ブラウザアプリケーションが無効になり、起動できません。
	Google Play の使用	制御すると、Google Play アプリケーションが無効になり、アプリをダウンロードできません。

1.5.ドキュメントの配布

ドキュメントファイルを管理し、各デバイスに配布することができます。ドキュメントはチーム単位、デバイス単位で配布が可能です。(Windows8.1 は非対応)

【配布可能なファイル形式】

「.doc, .docx, .pdf, .xls, .xlsx, .mp3, .mp4, .pages, .ppt, .pptx, .rtf, .txt, .png, .jpg, .gif, .psd, .numbers, .keynote」

※ iOS の場合、OpenIn（「外部アプリ」を選択してファイルを開くことができる iOS の機能）を使ったドキュメント閲覧が可能です。

※ 管理できるファイルは、１ファイル最大１GB、総容量 20GB までとなります。容量を追加することはできません。また一度に配布するファイル数の上限はありません。

1.6.アプリの配布

各デバイスにインストールするアプリを管理することができます。(Windows8.1 は非対応)

【自社アプリの配布】

自社で開発したアプリを App Store や Google Play を介さず、直接配布することができます。アプリを追加するだけで、社内限定で公開しているアプリ配信用ポータルの構築が可能ですので、配信専用のサーバーは不要。
自社アプリの最大容量は、スマートプラン：最大 100MB、エンタープライズプラン：最大 300MB となります。

【iTunes/Google Play のアプリを配布】

推奨するアプリを登録し、共有することができます。

【使用禁止アプリの設定】

デバイスに使用禁止アプリがインストールされた際に以下アクションを設定することができます。

- 管理者とユーザーにメールで通知
  禁止アプリがインストールされたことをメールにて通知
- 接続制限及びメール通知
  禁止アプリがインストールされたことをメールにて通知、ユーザーのデバイスの MDM+アプリの接続を制限する。
- デバイスの工場初期化
  禁止アプリをインストールした瞬間にデバイスを工場初期化する。0

1.7.住所録の配布

取引先の電話番号や住所等の情報を各モバイル端末に一括登録することができます。
配布した住所録を管理者ページで削除すると、端末内のデータも削除されます。
編集した住所録を再配布すると、端末内のデータに上書きされます。(Windows8.1 は非対応)

【アップロード可能なファイルの形式】

- MS Outlook 2003 CSV
- MS Outlook 2007 CSV
- MS Outlook 2010 CSV
- Google Outlook CSV（Gmail からエクスポートする際、Outlook 形式で書き出し）
- iCloud vcf ： www.icloud.com より連絡先へ移動後、ダウンロードした「vcf」ファイル

【インポート可能なデータ】
- 名前（フリガナ）
- メール（2 アカウントまで）
- 会社名
- 部署
- 役職
- 会社電話／自宅電話／携帯電話
- 会社 FAX／自宅 FAX
- 会社住所／自宅住所
- メモ

住所はフォルダ単位で管理されます。フォルダ内のデータを削除した場合、住所録を配布すると iPhone や Android 上でも削除されるようになります。
配布された住所録のデータが多いときは、追加処理に多少時間がかかる場合があります。追加作業が完了するまで iPhone/iPad のホームボタンを押さずにしばらくお待ちください。
住所録のデータが 500 件を超えるとき、ネットワーク状況によって多少時間がかかる場合があります。
配布された住所録を管理者ページで削除した場合、端末内のデータも削除されます。編集された住所録を再配布すると端末内のデータに上書きされます。

1.8.位置情報の取得

GPS でデバイスの位置情報を取得することができます。位置情報はチーム単位、デバイス単位で取得することが可能です。(Windows8.1 は非対応)

【更新のタイミング】
Android の場合は 15 分単位で更新され、iOS 端末の場合は移動が確認できたタイミンング（3G で基地局が変わったタイミングなど大きく位置を移動した時）で更新されます。

現在地は、最後に更新された位置を表示します。つまり、現在位置を更新するタイミングで室内、または地下鉄など GPS で現在地が取得できない環境におかれた場合は、インターネットに接続されるまでデバイスに保管し送信します。

手動で位置情報を取得する場合は、OS によって取得方法が異なります。

※ iOS
管理者からのリクエストがユーザー端末にメッセージとして送信され、ユーザー側でリクエストを受け付けると現在地情報を取得します。

※ Android
管理者がリクエストすると、ユーザー端末の現在地情報を自動的に取得します。

【トラッキング時間の設定】
業務時間のみ位置情報をトラッキング可能なように時間設定することができます。
位置表示機能を OFF にするとサーバーでは位置情報を保存しません。
位置情報機能が ON の時間帯のみ取得し、情報を保存します。

【住所録との連携】
位置情報表示画面で、配布した住所録にある取引先住所等を表示させることができます。

【GPS 設定】
業務時間のみ位置情報をトラッキング可能なように時間を設定することができます。位置表示機能を OFF にすると、位置情報をサーバーで保存しなくなります。
※　端末の GPS 機能を OFF にする機能ではありません。

(1) 位置情報履歴を保存する/しない
GPS で取得した端末の位置情報履歴をサーバーに保存するか否かを設定します。業務時間のみ位置情報をトラッキング可能なように時間を設定することができます。位置表示機能を OFF にすると、位置情報をサーバーで保存しなくなります。
端末の GPS 機能を OFF にする機能ではありません。

(2) 位置情報取得に関する時間設定
設定時間のみ位置情報を取得し、設定以外の時間には位置情報を取得いたしません。
「(1)位置情報履歴を保存する/しない」で ON にして、時間帯や曜日に絞って現在位置機能の ON/OFF を設定することができます。

1.9.MDM 無効化防止機能

MDM のプロファイルを削除した時に、MDM の管理機能が無効になってしまうことを阻止する機能です。
設定できる内容はデバイスの OS によって異なります。(Windows8.1 は非対応)

【設定できる内容（iOS)】

端末に「リモートマネージメントプロファイル」と「MDM プロファイル」をインストールすることで、ユーザー側で「リモートマネージメントプロファイル」を削除すると、管理者に警告メールが通知されます。
「MDM」プロファイルは、インストールすると工場初期化以外の方法では削除できません。

【設定できる内容（Android)】

端末にインストールされた「MDM+」の機能をユーザー側で停止した際に端末がどのような動作をするかを以下の２つから管理者側で設定することができます。
①パスコードを自動的に変更して画面ロックがかかる（パスコードは管理者が設定したもの)。
②工場初期化され、データが削除される。

1.10.操作ログ

操作ログを確認することができます。確認できるログには以下のものがあります。(CSV 形式でダウンロードできます。)

【管理者操作ログ 】
管理者のログイン及びログアウト
アプリ配布（チーム、個別デバイス）
ポリシー配布（チーム、個別デバイス）
プッシュメッセージ送信履歴
ドキュメント配布（チーム、個別デバイス）
住所録配布（チーム、個別デバイス）
現在地リクエストの送信履歴
位置情報確認履歴
デバイスロック
パスワード初期化
工場初期化
デバイス削除
ユーザー削除
CSV ダウンロードログ

【ユーザーイベントログ】
デバイスの初期化信号を受信
プロファイル削除（iOS)
MDM 機能が OFF に設定された（Android)
禁止アプリのインストール

ポリシーの適用完了状況

1.11.その他留意事項

1. プッシュ最大入力　1024 bytes
2. ポリシー

デバイスに適用されるまでの時間

Android：2 分（ただし、グーグル本社のサーバー事情によって多少の誤差が発生）

iOS：2 分（ただし、アップル本社のサーバー事情によって多少の誤差が発生）

ポリシー適用の適用までの流れ（iOS）

1. 管理者がデバイスにポリシー配布
2. 配布されたポリシーは、MDM+サーバーを介してアップルサーバに転送
3. アップルサーバがデバイスと通信してポリシー適用

ポリシー適用の適用までの流れ（Android）

1. 管理者がデバイスにポリシー配布
2. ポリシー配布リクエストは、Google サーバーを介してデバイスに転送
3. デバイスのポリシー適用

※iOS の設定ユーティリティの注意点

・モバイルデバイス管理（MDM Profile）プロファイルの使用禁止

・パスコード（Passcode）、制限（Restriction）プロファイルの場合は、MDM+のポリシーにもあるのでなるべく使用しないほうがよい（使用した場合は、各項目ごとに強力な設定が適用される仕様）

3. 禁止アプリ

デバイスに適用されるまでの時間

Android：2 分前後で適用（ネットワークの状況により多少の誤差が発生）

iOS：1 時間（アプリ一覧の更新タイミング）

禁止アプリ適用までの流れ（iOS）

1. 管理者がデバイスにポリシー配布
2. 配布されたポリシーは、MDM+サーバーを介してアプルサーバーに転送
3. アップルサーバがデバイスと通信してポリシー適用
4. デバイスから MDM+サーバーにアプリ一覧を更新
5. MDM+サーバー内で違反が存在するかチェックし、違反するアプリが存在する場合に通知（メール送信）

禁止アプリ適用までの流れ（Android）

1. 管理者がデバイスにポリシー配布
2. ポリシー配布リクエストは、Google サーバーを介してデバイスに転送
3. デバイスのポリシー適用
4. ユーザーが禁止されたアプリをデバイスにインストールした後、該当するアプリの実行時にチェック
5. アプリを終了させ、通知（メール送信）

4. ドキュメントの配布

デバイスに適用されるまでの時間

・ドキュメント配布の通知プッシュをデバイス上でクリック時に更新

・MDM+アプリの[ドキュメント]タブで更新した場合

・バックグラウンドで MDM+アプリが動いていない状態で MDM+アプリが実行される場合

ドキュメントファイルのサイズ

・エンタープライズ　アップロード最大 1GB　保存総容量 20GB

・スマート　アップロード最大 20MB　保存総容量 2GB

フォルダ名の制限：a-zA-Z0-9¥-_ぁ-ヶ亜-黒０－９　許可された文字セット

ファイル名の制限：UTF-8 の範囲以外の文字（例：髙）

テキストファイルの場合、内容が UTF-8 のみ対応

5. アプリ配布

デバイスに適用されるまでの時間

iOS：・アプリ配布の通知プッシュをデバイス上でクリック時に更新

・MDM+アプリの[アプリ]タブで更新した場合

・バックグラウンドで MDM+アプリが動いていない状態で MDM+アプリが実行される場合

Android：・アプリ配布の通知プッシュをデバイス上でクリック時に更新

・MDM+アプリの[アプリ]タブで更新した場合

・MDM+アプリのアプリのタブに移動する場合

アプリの保存サイズ

・エンタープライズ　300MB

6. GPS

取得タイミング 15 分に一回

※ 取得した時点でインターネットに接続されていない場合は、インターネットに接続されるまでデバイスに保管して送信

7. デバイス情報

更新のタイミング

(1) 定期的（１日２回）にサーバーから更新をデバイスに要請し、デバイスが応答した時

(2) 管理画面のデバイス情報で「更新する」をクリックし、デバイスが応答した時

(3) 端末のポリシーが変更し、デバイスに適用された時

(4) その他、下記のタイミングで更新

・iOS ： 1 時間以上経った時点で、再起動またはバックグラウンドからの復帰時に更新

ポリシーで禁止アプリ違反された場合に更新

・Android ： MDM+アプリの起動時に更新

8. 無通信レベルの設定及びリスト表示

端末の情報更新について、管理者は無通信チェックの日数を「レベル 1」と「レベル 2」に指定し、レベル 2 に当たるデバイスがあるときは管理者にメールで通知します。

2.動作環境

以下に記載する動作環境は、サービス仕様書更新日時点のものです。
追加、変更の場合がありますのでご了承ください。

2.1.動作確認環境 (管理画面)

【動作確認ブラウザ】

ブラウザ	バージョン
Internet Explorer	8 以降
Google Chrome	最新バージョン
Firefox	最新バージョン
Safari	最新バージョン
Opera	最新バージョン

2.2.必要な通信要件

##お客様環境からの Outbound 通信①
#宛先 IP アドレス（MDM＋サーバー）
219.120.12.64/26
#許可ポート
80(tcp), 443(tcp), 1640(tcp)

##お客様環境からの Outbound 通信②
#宛先 IP アドレス（Apple iDC）
17.0.0.0/8
#許可ポート
80(tcp), 443(tcp), 1640(tcp), 2195(tcp), 2196(tcp), 5223(tcp)

##お客様環境からの Outbound 通信③
#宛先 IP アドレス（GCM）
GCM は特定の IP を提供しません。

#許可ポート
5228(tcp), 5229(tcp), 5230 (tcp)

2.3.動作確認端末 (制御デバイス)

動作確認済みの端末一覧を WEB サイト上に記載しておりますので、ご確認ください。
WEB サイト：https://mdmplus.zendesk.com/hc/ja

3.サービス窓口

【サービス概要】

管理者様からのお問い合わせに対して、以下のとおり回答します。

- 操作マニュアルに記載されたとおりに動作しない場合
- 操作マニュアルに記載された操作を行った際にシステムの故障が発生する場合
- その他弊社が回答すべきであると判断する場合

【問い合わせ方法】

連絡方法	連絡先
WEB サイト 専用お問い合わせフォーム	https://mdmplus.zendesk.com/hc/ja/requests/new
電子メール	mdmplus@ksj.co.jp
電話番号	03-5440-2082

【回答時間】

土曜、日曜、祝祭日、年末年始（12 月 29 日～1 月３日）、及び弊社所定の休日を除く平日

9：30～12：00　及び　13：00～18：30　を回答時間とします。

【障害、メンテナンスの連絡】

事務局より以下のいずれかの手段にてお知らせいたします。

- 管理者用ログイン画面「障害・メンテナンス情報」に掲示
- 管理者様の登録メールアドレス宛てにご連絡
- 弊社営業担当、もしくはサポート担当から個別にご連絡

4.禁止事項

※　第三者にウィルスを送信するような行為

※　サーバーへ極端な高負荷を与える恐れのある行為

※　第三者及び弊社の著作権を侵害する行為

※　本サービスの運営を妨げる行為

※　弊社が承認していない営業行為

※　ＩＤ及びパスワードを不正に使用する行為

※　その他 MDM+の利用規約にて定める事項

5.留意事項

各サービスの料金、契約に関する留意事項は、それぞれの利用申込書に記載されている内容に準じます。