スマートデバイスマネジメント（SDM）

提供機能（2020年3月現在）

■基本機能

端末管理			iOS	Android	Windows
QRコード認証		QRコードを読み取ることにより、エージェントアプリケーションの認証に必要な企業コード、認証コード、認証URLを自動的に入力することができます。	–	○ (OS 4.0.3~)	–
Device Owner Mode	Device Owner Mode	エージェントアプリケーションをDevice Owner Modeにすることができます。Device Owner Modeのエージェントアプリケーションがインストールされた機器は、組織の管理下に置くために最適な設定を行うことができます。	–	○ (OS 7.0~)	–
	デバイスオーナーキッティング（NFC）	親機となる端末をキッティング対象端末（子機）にかざしていくだけで、子機の初期キッティングを行うことが出来ます。	–	○ (OS 6.0～)	–
	デバイスオーナーキッティング（QRコード）	キッティング対象端末でキッティング用QRコードを読み込ませることで、初期キッティングを行うことが出来ます。	–	○ (OS 7.0~)	–
端末情報管理	ハードウェア情報の取得	端末のハードウェア状態を確認することが出来ます。	○	○(*13)	○
	ハードウェア情報のレポート出力	端末のデバイス情報を一覧化し、CSVによるレポート出力を行うことが出来ます。	○	○	○
	端末のインポート登録	CSVを用いて、端末を一括登録することが出来ます。	○	○	○(*25)
	機器分類の作成	端末に分類情報を付与することが出来ます。ライセンス認証時、端末側から入力させることも可能です。	○	○	○
	自由入力項目の作成	自由入力可能な、機器に付与する分類情報を作成可能です。	○	○	○
	バッテリー残容量の取得	端末のバッテリー残容量を確認することが出来ます。	○	○	–
ネットワークマップ	ネットワークマップの取得、表示、管理	機器をアクセスポイント／ネットワークごとに分類して表示することにより、機器の場所を把握することができます。	○	○	○
IT機器自動検出		管理されている機器と同一のネットワーク内に接続されている機器の情報を自動的に収集し、ネットワークマップへ表示します。 ※注意 エージェント（パソコンやスマートフォンなどにインストールするソフト、アプリ）をインストールする場合には、本サービスを利用する企業内ネットワークでおこなってください。	–	–	○
設定管理	デフォルト設定	端末登録時、自動的に適用する設定を選ぶことが出来ます。	○	○	○
	設定一括適用	登録済み端末全て、もしくは機器分類ごとに一括して設定を適用できます。	○	○	○
	設定のテンプレート設定	端末に適用する設定をまとめて管理することが出来ます。	○	○	○
	設定情報のレポート出力	端末へ設定した設定情報を一覧化し、CSVによるレポート出力を行うことが出来ます。	○	○	○
	かんたん初期設定ウィザード	初期設定をウィザードに沿って進めることで、かんたんに実行することができます。	○	○	○
ホーム画面レイアウト	アプリケーションアイコン・フォルダの位置指定	ホーム画面上のアプリケーションアイコン及びフォルダーの位置を指定することが出来ます。 ただし、位置指定後は、アプリケーションアイコンの移動・削除・フォルダーの作成は一切行うことができません。	○ (*1) (OS 9.3～)	–	–

端末管理			iOS	Android	Windows
Zone Management		無線LANの接続先、位置情報、時間帯に応じて、設定や利用可能なアプリケーションを自動的に切り替える事ができます。	–	○ (OS 4.0～) (ｵﾌﾟｼｮﾝ:WiFi ZoneManagement)	–
位置情報取得	位置情報取得契機設定	位置情報の測位タイミングを設定し、定期的に位置情報を取得することが出来ます。	–	○	–
	位置情報の取得及び表示	取得した位置情報を確認することが出来ます。管理サイトより任意のタイミングで位置情報の更新要求を行うことも出来ます。	○ (*2*3)	○	○
	位置情報履歴取得	端末で取得、管理サイトに送信された位置情報を保存することにより、履歴として確認することが出来ます。Data Export（追加機能）により、CSVによるレポート出力を行うことが出来ます。	○	○	○
	位置情報取得許可/不許可表示	エージェント（パソコンやスマートフォンなどにインストールするソフト、アプリ）位置情報取得の許可/不許可状態 を確認することが出来ます。	–	○ (OS 4.0～)	–
アプリケーション情報取得	アプリケーション情報の取得	端末内にインストールされているアプリケーション情報を確認することが出来ます。	○	○ (*14)	○
	アプリケーション情報のレポート出力	端末のアプリケーション情報を一覧化し、CSVによるレポート出力を行うことが出来ます。	○	○	○
	更新プログラム適用状況の取得	機器に適用済もしくは未適用のWindows更新プログラムの一覧を取得、確認することができます。	–	–	○
組織管理	階層化管理	組織構造に合わせて、階層的な端末管理を行うことが出来ます。また、ユーザーに対して組織単位の権限を割り振ることが出来ます。	○	○	○
	組織管理	管理サイト内に「組織」を定義、端末やユーザーを組織と紐付けて管理することが出来ます。	○	○	○
	組織インポート	CSVを用いて、組織を一括インポートすることが出来ます。	○	○	○
	組織情報のレポート出力	登録済みの組織情報をCSVとしてレポート出力することが 出来ます。	○	○	○
ユーザー管理	ユーザー管理	管理サイトを利用するユーザー、端末を利用するユーザー等を管理サイトへ登録、管理することが出来ます。	○	○	○
	ユーザー権限制御	ユーザーに対して、権限を設定することが出来ます。	○	○	○
	ユーザー情報インポート	CSVを用いて、ユーザーを一括登録することが出来ます。	○	○	○
	ユーザー情報のレポート出力	登録済みユーザーをCSVとしてレポート出力することが出来 ます。	○	○	○
	ユーザーの分類設定	ユーザーに分類情報を付与することができます。	○	○	○
	ユーザー別機器数上限指定	上限を超えた認証を行えないようにすることにより、管理者の意図しないライセンスの利用を防ぐことが出来ます。	○	○	○
	自由入力の項目作成	自由入力可能な、ユーザーに付与する分類情報を作成可能です。	○	○	○
	ユーザーによるパスワード管理	管理サイトログイン画面より、パスワード設定用URLを発行することができます。	○	○	○
	アカウントポリシー設定	管理サイトログイン時のパスワードのポリシーを設定することができます。誤入力回数に基づくアカウントロックも可能です。	○	○	○

端末管理			iOS	Android	Windows
エージェント管理	エージェントアンインストール保護（パスワード）	エージェントアンインストール防止のために、パスワードによるアンインストール制限を行うことが出来ます。	–	○ (*15)	○
	定期通信間隔設定	管理サイトとエージェントアプリ間の定期通信間隔を設定することが出来ます。	–	○	○
ログ取得・閲覧	管理サイト操作ログ	管理サイトで操作した内容をログへ出力、管理サイト上で閲覧することが出来ます。	○	○	○
	エージェントログ	エージェントによる動作を、管理サイト上で確認することが出来ます。	○	○	○
	ログのレポート出力	端末内のエージェントが行った動作ログをCSVによるレポ ート出力を行うことが出来ます。	○	○	○
DEP(DeviceEnrollment Program)	DEPサーバ連携	Apple社のDEPサーバと連携し、管理サイト上で作成したDEP定義プロファイルを元に「スマートデバイスマネジメントの端末認証」「監視対象端末化」などの初期設定ができます。また、プロファイルの削除防止もできます。	○ (*4)	–	–
同期機能	ユーザーによる同期	端末側でユーザー自身が操作することで、エージェントアプリと管理サイト間を同期することができます。	○	○	○
	自動同期	管理サイト上で設定された間隔に応じて、自動的にエージェントアプリと管理サイト間を同期することができます。	○	○	○
Apple Business Manager		Apple Business Managerと連携し、iOS端末の各種設定や、購入したアプリ・書籍の配信を行うことができます。	○	–	–

セキュリティ管理			iOS	Android	Windows
パスワードポリシー設定	パスワードポリシーの設定	端末のパスワード解除方法、パスワードの指定文字数入力の強制等、ポリシーを設定します。	○	○	○(*26)
	端末パスワード設定の強制設定	端末のパスワード設定を必ず行うように設定します。	○	○	–
	パスワード再利用禁止設定	パスワード再設定の際に指定回数前までに使用していた パスワードを使用させないように設定することが出来ます。	○	○ (OS 3.0～)	○(*26)
	使用パスワードの有効期限設定	現在使用しているパスワードの有効期限を設定することが出来ます。	○	○ (OS 3.0～)	○(*26)
	パスワード自動ロック時間の設定	無操作状態から端末がパスワード自動ロックされるまでの時間を設定することが出来ます。	○	○	–
	パスワードロック解除時の設定	パスワードロックの入力に指定回数失敗すると自動的に 端末を初期化およびロックすることができる設定を行うことが出来ます。	○	○(*16) (OS 4.0～)	○
	パスワードロック解除時の設定（オリジナルロック画面）	パスワードロック解除に失敗したときのロック画面に、 スマートデバイスマネジメントのロック画面を表示し、データ漏えいを防ぎます。	–	○ （OS 4.0～）	○
	スクリーンセーバー設定	端末のスクリーンセーバー設定について、管理サイトから設定を適用することができます。	–	–	○ (*27)
	スクリーンロックパスワード変更	端末に設定されているスクリーンロックパスワードを変更することが出来ます。	–	○ (*15*17) (OS 4.0～)	–
	スクリーンロックパスワード削除	端末に設定されているスクリーンロックパスワードを削除することが出来ます。	○	–	–

セキュリティ管理			iOS	Android	Windows
無通信検知	無通信検知機能	指定した間隔無通信だった際に、検知する様に設定が出 来ます。また検知した際に管理者へメールによる通知を行うことが出来ます。	○	○	○
	MDM構成プロファイル削除検知	インストールされているMDM構成プロファイルが削除されたことを検知することができます。また削除を検知した際に管理者へメールによる通知を行うことができます。	○	–	–
無通信ロック/ワイプ	無通信時ロック	指定された時間、管理サイトとの通信が行われなかったときに端末をロックすることが出来ます。	–	○	○
	無通信時ワイプ	指定した間隔、管理サイトと無通信だった際に、機器の初期化・データ削除もしくは機器内データの取り出しを困難にすることができます。	–	–	○
root化/Jailbreak検知		端末のroot化、JailBreakの状態を検知することが出来ます。エージェントインストール後、利用可能となります。	○ (*2*3)	○	–
リモートロック	リモートロック（オリジナルロック画面）	遠隔から端末をロック（オリジナルロック画面を表示） することが出来ます。またロックした際に管理者へメールによる通知を行うことが出来ます。	–	○	○
	リモートロック （警告音）	遠隔操作により、端末をロックすることができます。またロックを実行した際に管理者へメールによる通知を行うことができます。 ロック時アラート音を鳴動させることができます。	–	○	–
	リモートロック （スクリーンロック）	端末を遠隔操作にてロックをかけることができます。 またロックを実行した際に管理者へメールによる通知を行うことができます。	○	○ (OS 6.0～)	–
	リモートロック （メッセージ表示）	リモートロック時に、ロック画面に表示させるメッセージを指定することができます。	○	○	○
紛失時強制リモートロック/位置情報強制取得	紛失時強制リモートロック	第三者が解除できない強力なロックをかけることができます。このロック中にはメッセージの表示が可能です。	○（*1) (OS 9.3～)	–	–
	位置情報強制取得	このロック中に強制的な位置情報の取得をエージェントアプリケーションなしに行うことができます。	○（*1) (OS 9.3～)	–	–
リモートワイプ	リモートワイプ	端末を遠隔にて初期化することが出来ます。ワイプ実行前に管理者へメールによる通知を行うことが出来ます。	○	○	–
	リモートワイプ（SDカード）	リモートワイプ時に端末内のSDカードを遠隔にて初期化することが出来ます。	–	○	–
	リモートワイプ （BitLocker）	Bitlockerによる暗号化を実施した端末に対し、暗号キー を削除することによりデータにアクセスできない状態にします。	–	–	○
	リモートワイプ（データ削除）	遠隔で、機器内に保存されているデータを削除することができます。	–	–	○(*28)
	リモートワイプ（管理領域）	MDMの管理領域（MDMプロファイル、管理されたアプリ）のリモート削除を実施することが出来ます。	○(*5)	–	–
	リモートワイプ（PC初期化）	ユーザーがインストールしたアプリやドライバー、個人用ファイルをすべて削除し、実行後にはWindows 10の初期設定画面が表示されます。	–	–	○ (*29)

セキュリティ管理			iOS	Android	Windows
アクティベーションロック	アクティベーションロック	管理サイト上から、アクティベーションロック有効化、無効化を行うことができます。	○（*1）	–	–
	アクティベーションロック解除	管理サイト上から、アクティベーションロック解除を行うことができます。	○（*1）	–	–
構成プロファイル作成	iOS構成プロファイルアップロード	AppleConfiguratorやiPhone構成ユーティリティで作成した構成プロファイルをアップロード出来ます。 お客様環境で作成済みプロファイルを、一括配付することが可能です。	○	–	–
	iOS構成プロファイル画面上設定	管理サイト上で、iOS構成プロファイルの以下の項目を作成、閲覧、編集、削除出来ます。 ・パスコード ・制限 ・Wi-Fi ・メール ・証明書 ・Webフィルタリング ・グローバルHTTPプロキシ ・VPN	○	–	–
	iOS構成プロファイル画面上設定（監視対象限定項目）	監視対象端末限定の設定項目に対応しています。	○（*1）	–	–
構成プロファイル設定	アカウント情報の変更禁止	ユーザーの新規アカウントの作成、ユーザー名やパスワードおよびアカウントに関連付けられたその他の設定の変更を禁止出来ます。	○（*1）	–	–
	Store購入制限	iTunes Store内の購入を制限することが出来ます。	○（*6）	–	–
	コンテンツレーティング	国ごとに定められたレーティングを、ムービー再生やアプリに対して適用することが出来ます。	○（*1）	–	–
	スクリーンショット禁止	iOS端末上におけるスクリーンショット撮影を禁止することが出来ます。	○	–	–
	機能制限の禁止	ユーザー操作による「機能制限」の設定を禁止することができます。	○（*1）	–	–
	初期化禁止	機器上で「すべてのコンテンツと設定を消去」が実行されることを禁止することができます。	○（*1）	–	–
	iCloudへのバックアップ禁止	管理対象アプリに対して、iCloudへのバックアップを禁止することができます。	○	–	–
構成プロファイル削除防止	構成プロファイル削除保護	Apple-MDM構成プロファイル以外の構成プロファイルを、削除時にパスワード入力必須とすることが出来ます。	○	–	–
	構成プロファイル削除禁止	Apple-MDM構成プロファイル以外の構成プロファイルを、削除禁止することが出来ます。	○	–	–
認証制御設定		事前に登録された端末のみスマートデバイスマネジメントのライセンス認証を受けられるようにすることができます。	○	○	○

セキュリティ管理			iOS	Android	Windows
OSアップデート管理	ソフトウェア・アップデート遅延設定	新しいiOSアップデートが表示される次期を遅らせることが可能です。最長で90日間遅らせることができます。	○ (*1) (OS 11.3～)	–	–
	Windows Update設定	Windows Updateの延期日数や再起動時刻の設定等が可能です。	–	–	○(*30)
	OSアップデート指示・情報取得機能	対象の端末がアップデート可能な最新バージョンへ、アップデートを促すことができます。また、対象の端末がアップデート可能な最新バージョンの情報を取得・表示することも可能です。	○(*1) (OS 12.3～)	–	–
システムセキュリティ	セキュリティ状況取得	端末のセキュリティ対策状況を管理サイト上で確認可能 です。セキュリティを維持するコストを削減出来ます。	–	–	○ (*31*32)
	ファイアウォール有効化設定・診断	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。	–	–	○
	Guestアカウント無効化設定・診断	Guestアカウントが無効化、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。	–	–	○
	自動更新有効化設定・診断	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。	–	–	○ (*33)
	Windows Update設定	Windows Updateの延期日数や再起動時刻の設定等が可能です。	–	–	○(*30)
	スクリーンセーバー解除時画面の設定・診断	スクリーンセーバーを解除した後、パスワード入力を促 すために「ようこそ画面」へ戻す設定を行うか、この設定が有効化否かをログへ出力します。	–	–	○
	スパイウェア対策ソフトの診断	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。	–	–	○
	ウイルス対策ソフトの診断	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。	–	○ (ｵﾌﾟｼｮﾝ:モバイルウイルス対策)	○
	Windows Defender設定・診断	Windows Defenderの「ウイルスと脅威の防止」「ランサムウェアの防止」に関する設定、診断を行い、結果をログへ出力します。	–	–	○ (*29)
	ブラウザーに対するセキュリティ設定	インターネットオプション内に存在するセキュリティ設定項目を強制設定することができます。また、セキュリティーゾーンを既定レベルへの設定、信頼済みサイト・制限付きサイトの登録も可能です。この設定の結果をログへ出力します。	–	–	○ (*35)
SIM抜き差し監視機能		会社から支給された正規のSIM以外の挿入を検知し、端末をロックすることができます。企業所有の端末へ、私物のSIMを挿入し不正な通信を行うことを防ぎ、厳格な端末管理を行うことが可能です。	–	–	○
証明書配布設定	証明書配布設定	クライアント証明書並びにCA証明書を個別・一括アップロード、配布、一括削除することができます。	○	○ (OS 4.0～)	–
	証明書サイレントインストール	クライアント証明書並びにCA証明書を端末利用者の操作なく、サイレントインストールすることができます。	○	○(*15) (OS 6.0～)	–

設定管理			iOS	Android	Windows
連絡先情報設定	連絡先情報の設定	連絡先一覧を作成し、端末へ設定を行うことが出来ます。	–	○	–
	連絡先情報の設定 (CardDAV)	CardDAVによる設定を行います。	○	–	–
	連絡先インポート・エクスポート	予め連絡先を登録しておいたCSVファイルのインポートに より、連絡先を一括登録可能です。また、登録済みの連絡 先をCSVファイルでエクスポート可能です。	–	○	–

デバイス管理			iOS	Android	Windows
外部記憶制御	SDカード利用禁止・許可設定	SDカードへのアクセス、利用禁止・許可を設定することが出来ます。	–	○ (OS 2.0～5.x *18) (OS 6.0～*15)	○
	USB利用禁止・許可設定 （ブラックリスト方式・ホワイトリスト方式）	USBの利用禁止・許可を設定することができます。また、利用禁止設定適用中に利用を許可したいUSBデバイスのハードウェアＩＤ、インスタンスパスまたは、シリアルＩＤを指定することで、禁止設定から除外する事ができます。大容量ストレージのみ、ストレージへの書き込み禁止のみ、または、全てのUSBデバイスを対象に禁止する事ができます。	–	–	○
	USB利用禁止（WPD）	Windows Portable Devicesを禁止対象とすることが可能です。これにより、スマートフォンやカメラデバイス等の接続時にもデータを抑制することが可能です。	–	–	○
	USBファイル転送	USB経由でのデータ転送を禁止します。MTPやPTPといった種類のファイル転送を制限可能です。	–	○(*15) (OS 6.0～)	–
	USB接続ストレージ利用禁止	PCなどにUSB経由で接続しても、大容量ストレージとしての利用を禁止することができます。Android端末を外部ストレージとして使うこと、Android端末内データを画像以外も含めて取り出すことを防ぎます。	–	○(*15) (OS 6.0～)	–
	IEEE1394デバイス	IEEE1394デバイスを禁止することが出来ます。	–	–	○
	CD/DVD/ブルーレイ/フロッピーディスク利用禁止	CD/DVD/ブルーレイ/フロッピーディスクドライブを禁止することができます。また、CD/DVD/ブルーレイは書き込み禁止を設定することが可能です。	–	–	○
	ログ出力・ログメール通知	外部記憶制御の設定結果をログに出力し、管理者へ通知することができます。	–	–	○
デバイス制御	カメラの利用禁止・許可設定	カメラ機能の使用禁止・許可を設定することができます。	○	○	–
	Bluetooth利用禁止・許可設定	Bluetoothの利用禁止・許可を設定することができます。	–	○(*19)	–
	データ出力NFC利用禁止	NFC経由でのデータ転送を禁止することができます。	–	○(*15) (OS 6.0～)	–
暗号化設定	端末暗号化の設定	端末の暗号化画面を呼び出し、暗号化を促すことが出来ます。	○	○ (OS 3.0～)	○
	端末暗号化の設定（データ保護）	パスコードを設定することで自動的にデータを保護しま す。	○	–	–
システム設定・診断	ドライブ空き容量診断	ドライブの空き容量を診断し、一定値より少なくなったらMDMのログへ出力します。	–	–	○
	CPU温度診断	CPUの温度を取得し、一定値以上になったらMDMのログへ出力します。	–	–	○(*34)
	ハードディスク異常診断	S.M.A.R.T対応ハードディスクの以上を診断し、MDMのログへ出力します。	–	–	○(*34)
	デフラグ自動実行	デフラグを自動実行するよう設定することができます。	–	–	○
	システムドライブの復元有効化	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とき、それを有効化します。	–	–	○(*34)
	IE自動更新設定	最新のIE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。	–	–	○

アプリケーション管理			iOS	Android	Windows
App Manager		エージェントに組み込まれたアプリ配信基盤 App Manager により、エージェント経由で、各種MDM関連アプリをダウ ンロードすることが出来ます。	–	○	–
アプリケーション配信	アプリケーション配信	インストールさせたいアプリケーション情報を配信し、ダウンロード・インストール作業の簡略化ができます。	○(*7)	○	–
	アプリケーション配信 (AppStore/in-house)	ポータルサイト経由、もしくはポップアップ通知により、AppStore、in-houseアプリを配信することができます。	○	–	–
	アプリケーション配信(管理対象)	AppStore/in-houseアプリをスマートデバイスマネジメントの管理対象として配信することができます。	○	–	–
	管理対象アプリ化	スマートデバイスマネジメントの管理下にないインストール済のアプリを、アプリ内データを保持したまま管理対象アプリへと変更することができます。	○ (OS 9.0～)	–	–
	アプリケーション配信(サイレント)	アプリを、サイレントにインストールすることができます。	○ (*1*7*8*9)	○(*20) (OS 6.0～)	–
	オリジナルアプリ登録・配信	アプリをアップロードし、端末へ配信することができます。	○	○(*20)	–
	プロビジョニングプロファイル配信	in-houseアプリケーションに対してプロビジョニングプロファイルを配信することができます。	○	–	–
	アプリケーションインストール催促	配信したアプリケーションが未インストールの場合、定期通信等の同期タイミングでポップアップを表示し、インストールを催促することができます。	○	○	–
アプリケーション配信 （VPP対応）		Apple社が提供するVolume Purchase Programの仕組みに対応したアプリケーション配信が可能です。AppStore上のアプリを一括購入した後に、ユーザーに対するアプリケーションのライセンスの付与・回収などの管理を行うことができます。	○ (*10)	–	–
ブック配信(VPP対応)		Apple社が提供するVPP(Volume Purchase Program)の仕組みに対応したブック配信を実施することができます。iBooks Store上で購入したライセンスの一括付与及び一括配信が可能です。	○	–	–
App Configuration		App Configurationに対応したアプリケーションへOptimal Bizから設定値を配布することができます。	○	–	–

アプリケーション管理			iOS	Android	Windows
アプリケーションアップデート		スマートデバイスマネジメントから配信したアプリケーシ ョンの新バージョンが公開された際に、アプリケーションのアップデート指示を出すことができます。	○ (*11)	○	○
	アプリケーション起動禁止 (ホワイトリスト/ブラックリスト)	ホワイトリストに登録されたアプリケーション以外の利用を禁止することができます。また、ブラックリストに登録されたアプリケーションの利用を禁止することができます。	○(*1) (OS 9.3～)	○	–
	アプリケーション起動禁止 (特定アプリ)	Safari, iTunes Store, Podcastの禁止が可能です。	○(*12)	–	–
Open-In制御	アプリのOpen-In制御	管理対象アプリと非管理対象アプリ間におけるデータの受け渡しを制御することができます。	○	–	–
	アカウントのOpen-In制御	Bizから配信された管理対象アカウント（Exchange ActiveSync、メールアカウント）に対してファイルのデータ受け渡しを制御することができます。	○	–	–
	SafariのOpen-In制御	Safariに対して管理対象URLを追加することができます。これにより、管理対象URLへアクセスした場合に、ダウンロードしたファイルのデータ受け渡し制御が可能です。	○	–	–
インストール制限機能		アプリケーションのインストールを禁止することが出来ます。	○	○ (*21*22)	–
アンインストール制限機能		アプリケーションのアンインストールを禁止することができます。	○(*1)	–	–
アプリケーション検知	指定アプリ検知機能	アプリケーション名やバージョン条件等を指定することで、インストール推奨/非推奨アプリケーションのインストール状況を検知し、管理者に知らせる機能です。	○	○	–
ライセンス管理	VPPライセンス数管理	VPPライセンスの付与状況を確認することができます。	○	–	–

メッセージ通知機能			iOS	Android	Windows
メッセージ通知機能	メッセージ配信設定	管理者より、端末へ指定のメッセージを送信することが出来ます。	○(*2)	○	–
	通知結果の集計	端末より、通知済みのメッセージ閲覧状況を集計することが出来ます。	○(*2)	○	–
	スケジュール配信	予め指定した日時にメッセージを配信することができます。	○(*2)	○	–
	既読・未読集計	通知済みメッセージの未読/既読を集計、閲覧状況を確認することが可能です。	○(*2)	○	–

インターネット接続管理			iOS	Android	Windows
Wi-Fiフィルタリング		指定されたSSIDおよびMACアドレスへのみ、Wi-Fi接続が許可できるよう設定できます。	–	○ (ｵﾌﾟｼｮﾝ:インターネット接続管理)	–
Webフィルタリング	Webフィルタリング設定 (標準ブラウザー) (ホワイトリスト／ブラックリスト)	OS標準ブラウザーに対して、ホワイトリストに登録されたURL以外へのアクセスを禁止することができます。 ブラックリストに登録されたURLへのアクセスを禁止することができます。	○ (OS 8.0～)	○ (OS~5.x) (ｵﾌﾟｼｮﾝ:インターネット接続管理)	–
	Webフィルタリング設定 (DM Browser) (ホワイトリスト／ブラックリスト)	DM Browser に対して、ホワイトリストに登録されたURL以外へのアクセスを禁止することができます。 ブラックリストに登録されたURLへのアクセスを禁止することができます。	○ (OS 8.0～) 構成プロファイル設定にて可能 &ｵﾌﾟｼｮﾝ インターネット接続管理でも可能	○ (ｵﾌﾟｼｮﾝ:インターネット接続管理)	–
Webクリップ配信	Webクリップアイコン指定	配信するWebクリップのアイコンを、自社ブランドロゴや内容に合わせた適切な画像に変更することができます。	○	–	–
	Webクリップ配信	スマートデバイスマネジメントからホーム画面へ、Webクリップを配信することができます。自社サイトのショートカットやヘルプデスクの連絡先などを配信することが可能です。	○	–	–
プロキシ	プロキシ（手動構成）	手動によるプロキシ設定が行えます。	○	○(*23)	○
	プロキシ（自動構成）	自動構成によるプロキシ設定が行えます。	○	–	○
	GlobalHTTPプロキシ設定	管理サイト上で、GlobalHTTPプロキシ設定を作成、閲覧、編集、削除できます。	○(*1)	–	–
接続設定	ローミング設定	「音声」「データ」のローミング設定の有効・無効設定を行うことができます。	○	–	–
デバイスVPN設定		機器ごとにVPN接続を設定することができます。	○	–	–
Exchange ActiveSync設定		機器にExchange ActiveSync設定をすることができます。	○	–	–
メール設定	POP/IMAP設定	機器に対して、POP/IMAPアカウント設定をすることができます。	○	–	–
	誤送信防止設定	指定されたアドレス以外のメールアドレスを強調表示することができます。	○	–	–

■オプション機能（有料）

Wi-Fi ZoneManagement		iOS	Android	Windows
ゾーン作成	SSID、位置情報、スケジュールを用いて利用シーンに応じた「ゾーン」を作成することが出来ます。	–	○ (OS 4.0～)	○
ポリシー作成	ゾーン毎に使用する「ポリシー」を作成することが出来ます。 ■ポリシーの設定項目（Android） ・位置情報測位 ・アプリケーション起動禁止 ・SDカード利用禁止・許可 ・カメラ利用禁止・許可 ・Bluetooth利用禁止・許可 ・リモートロック ・Wi-Fiフィルタリング ・Webフィルタリング ・Web閲覧履歴 ■ポリシーの設定項目（Windows） ・プロキシ	–	○ (OS 4.0～)	○ ※ﾌﾟﾛｷｼのみ
SSIDによる「ゾーン」検知	機器で検知したSSIDを用いて、自動的に設定セットを切り替えることができます。	–	○ (OS 4.0～)	○
位置情報による「ゾーン」検知	機器で検知した位置情報用いて、自動的に設定セットを切り替えることができます。	–	○ (OS 4.0～)	○
スケジュールによる「ゾーン」検知	予め登録されたスケジュールを用いて、自動的に設定セットを切り替えることができます。	–	○ (OS 4.0～)	○
ゾーン検知による設定セット切り替え	検知したゾーンによって、機器へ適用する設定を自動的に切り替えることができます。	–	○ (OS 4.0～)	○
所属ゾーン表示	予め定義されたゾーンの範囲内にいることを機器および管理サイト上で確認できます。	–	○ (OS 4.0～)	○

モバイルウイルス対策		iOS	Android	Windows
保護状況確認	ウイルス対策ソフトによる保護状況（有効/無効、パターンファイル更新日等）を確認することができます。	–	○	–
リアムタイムスキャン	不正なアプリがインストールされた場合に検知して削除を促します。	–	○	–
スケジュールスキャン	定期的に機器内をスキャンする日時を設定することができます。	–	○	–
パターンファイル自動更新	パターンファイルの更新日を設定することができます。	–	○	–
アンインストール保護	アンチウイルスソフトのアンインストールに、パスワードを入力させることができます。	–	○	–
ライセンス付与	管理者により、ライセンスの割当を制御することができます。	–	○	–

インターネット接続管理			iOS	Android	Windows
お気に入り設定	お気に入り設定（標準ブラウザー）	お気に入り設定をOS標準ブラウザーに設定することができます。	–	○(*36) (OS～5.x)	–
	お気に入り設定（DM Browser）	お気に入り設定をDM Browserに設定することができます。	○	○	–
Webフィルタリング	Webフィルタリング設定 (標準ブラウザー) (ホワイトリスト／ブラックリスト)	OS標準ブラウザーに対して、ホワイトリストに登録されたURL以外へのアクセスを禁止することができます。 ブラックリストに登録されたURLへのアクセスを禁止することができます。	–	○ (OS 2.x～3.x) (OS 4.x~5.x *37)	–
	Webフィルタリング設定 (DM Browser) (ホワイトリスト／ブラックリスト)	DM Browser に対して、ホワイトリストに登録されたURL以外へのアクセスを禁止することができます。 ブラックリストに登録されたURLへのアクセスを禁止することができます。	○	○	–
Web閲覧履歴取得	Web閲覧履歴取得、削除	DM BrowserのWeb閲覧履歴の取得、削除を行うことができます。	○	○	–
Wi-Fi設定	Wi-Fi設定	Wi-Fiの有効・無効や、Wi-Fiネットワークの追加等を行うことができます。 Wi-Fiネットワークの追加はHidden SSIDにも対応しています。	–	○	–
	Wi-Fiエンタープライズ認証設定	IEEE 802.1xの各EAP方式によるWi-Fi設定を行うことができます。	–	○(*24)	–
DM Browser	連携機能	管理サイトで設定された、Webフィルタリング/お気に入り設定/Web閲覧履歴取得の機能を適用することができます。	○	○	–
	タブブラウザ	Webページをタブで切り替えて表示することができます。	○	○	–
	ブラウジング	戻る/進む/ページ再読み込み/全画面表示/お気に入り登録といった、基本的なブラウジング機能を有しています。	○	○	–

*1： 監視対象端末限定の機能となります。（iOS端末を監視対象端末にする際にはiOS端末の初期化が必要です。）
*2： iOSのエージェントアプリが必要となります。また、iOS7以降においては、エージェントアプリが「最近使用したアプリ一覧」に表示されていない場合、本機能が動作しない場合があります。
*3： iOS9以降機器で「低電力モード」に設定されている場合、OS仕様上、情報更新の為にはエージェントアプリをフォアグラウンドで起動する必要があります。
*4： ご利用の際は、DEPアカウントの登録と、AppleもしくはDEPプログラムに参加する取扱店・通信業者から直接購入した機器が必要となります。DEPアカウント登録及び購入先についての詳細は、Appleへお問い合わせください。
*5： 削除防止設定がされている構成プロファイルおよびプロビジョニングプロファイルは削除されません。
*6：制限項目「購入時に常に iTunes Store パスワードを要求」はiOS8.3以降でご利用できません。
*7：iOS8.3以降機器の、機能制限「パスワードの設定(設定アプリ -> 一般 -> 機能制限)」において、パスワード設定が行われていない場合、アプリケーション配信時に"パスワードの入力を要求するダイアログ"が表示されます。
*8： AppStoreアプリの場合、管理対象アプリに設定されていて、配信先機器が監視対象機器、「iTunesStoreアカウントが登録済み」および「購入済みアプリの配信」の場合、サイレントインストール可能です。In-Houseアプリ配信の場合は「iTunesStoreアカウント未登録」でもサイレントインストール可能です。
*9: iOS8.3以降機器のAppleIDの設定を行っていない機器において、AppStoreアプリを配信した場合にAppleIDと複数回のパスワード入力を求められます。サイレントインストールする場合は、アクティベーション時またはアプリ配信前にAppleIDの登録を行ってください。
*10: 指定したデバイスに対して配信する方式は、対応OSはiOS 9以降となります。なお、この方式においては、従来のユーザーに対する配信方式と違い、Apple IDの入力は不要です。
*11: iOSに対して、管理対象アプリとして配布したアプリのみに対応します。
*12: Podcastを禁止するためには、機器を監視対象とする必要があります。また、対応OSはiOS 8以降となります。
*13: Android 6.x以降の場合、MACアドレスが全て特定の固定値になります。
*14: Android 8.x以降の場合、Bluetoothを「無効にする」設定セットを端末に割り当てた状態で、端末側でBluetoothを有効にすると、通知領域の簡易設定画面のスイッチがON(有効)になります。ただし、通知領域の簡易設定画面上ではONとなっていても、実際には「無効にする」設定は動作しており、BluetoothはOFFになっています。
*15: エージェントアプリケーションをDevice Owner Modeにする必要があります。
*16: Android 5.x以降の場合スクリーンロック解除失敗ロック時、ロックされない機器があります。
*17: Android 5.x以降の場合空のスクリーンロックパスワード指定時、ロック画面でパスワードが要求されます。空のパスワードを入力頂くことで解除可能です。
*18: Android 4.2以降ではOSの仕様上、SDカード禁止に非対応です。データが書き込まれたことを検知、データを削除します。
Android 4.3以降：SDカード挿入検知時、専用のロック画面を表示します。
*19: Bluetoothを「無効にする」設定セットを端末に割り当てた状態で端末側のBluetoothを有効にすると、通知領域の簡易設定画面のスイッチがON(有効)になります。
ただし、通知領域の簡易設定画面上ではONとなっていても、実際には「無効にする」設定は動作しており、BluetoothはOFFになっています。
*20: Fully managed Device(Android Enterprise)機能を利用いただく必要があります。
*21: Android OS 2.xの場合、設定画面の「開発」も開けなくなります。
Android OS 3.x以降の場合、設定画面も開けなくなります。インストールが制限され、アプリのアップデートも制限されます。
*22: エージェントアプリケーションをDevice Owner Modeにすることで設定画面の禁止なくインストール制限を行うことができます。
*23: Android OS 2.x～3.xの場合、エージェントアプリに対してのみプロキシ設定を適用可能です。
*24: CA証明書を複数設定したWi-Fi設定は、Android 7.x以上の端末でしか使用できません。
*25: Windows RT機器を機器インポートするためには、MACアドレスおよびシリアル番号の両方を入力する必要があります。
*26: ドメイン参加機器に対するパスワードポリシーの設定には非対応です。
*27: 以下のWindowsエディションではスクリーンセーバーの設定を行うことはできません。
Win 8.1: 無印
Win 10: Home
*28: Windowsのリモートワイプ（データ削除）は、BitLockerと異なり、実行後にOSを起動することができません。
*29: Windows 10 ver.1709以降でのみ動作します。
*30: Windows 10 ver.1709以降でのみ動作します。Windows 10 Homeの場合はアクティブ時間のみ設定可能です。
*31: Windows Serverでは、ウイルス対策ソフト、スパイウェア対策ソフト、ファイアウォールの状況は取得できません。
*32: Windows 10においては、セキュリティタブの「Windows自動更新」情報が正常に表示できません。

*33: Windows 10においては、システムセキュリティの「Windowsの更新を自動インストールする」が正常に動作しません。
*34: Windows Serverでは提供対象外の機能となります。
*35: Internet Explorerが対象となります。Microsoft Edgeには非対応です。
*36: Chromeが標準ブラウザとなっている場合、お気に入りを追加することができません。
*37: シークレットモードでの利用は非対応です。