スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「－」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】端末管理							
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。	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。	-	-	-	◎
Device Owner Mode **初期化必須**	afw識別子、G Suiteアカウント、QRコード、NFC、ゼロタッチ登録を使ったGoogle社のDevice Owner Modeキッティングに対応し、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。	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。	-	-	-	◎
		afw識別子によるDevice Owner Modeキッティング	端末初期設定時にafw#から始まる識別子をメールアドレス欄に入力することで、 エージェントアプリを自動プロビジョニングできます。	-	-	-	◎
		G SuiteアカウントによるDevice Owner Modeキッティング	端末初期設定時にG Suiteアカウントをメールアドレス欄に入力しログインすることで、 エージェントアプリを自動プロビジョニングできます。	-	-	-	◎
		QRコードによるDevice Owner Modeキッティング	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を Device Owner Modeにすることができます。	-	-	-	◎
		NFCバンプによるDevice Owner Modeキッティング	NFCバンプを使用し、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。	-	-	-	◎(9.x) -(10.x～)
機器情報管理	機器を登録し、取得した機器のハードウェア情報を管理サイト上で閲覧することができます。CSVによるレポート出力も可能です。	ハードウェア情報の取得	機器のハードウェア状態を確認することができます。	◎#	◎	◎	○※38
		ハードウェア情報のレポート出力	機器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できます。	◎#	◎	◎	◎
		機器のインポート登録	CSVを用いて、機器を一括登録することができます。	◎#※10	◎	◎	◎
		機器分類の作成	機器に分類情報を付与することができます。ライセンス認証時、 機器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	機器のバッテリー残容量を確認することができます。	-	◎	◎	◎
IT機器自動検出	SDMで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。	IT機器自動検出	同一セグメントのIT機器を自動検出、類推判別してネットワーク内に存在する機器 (プリンター、ルーター、NASなど)を収集し、管理画面上で管理します。	○※65	-	-	-
		MFP状態取得・表示	「IT機器自動検出」機能により検出されたネットワーク接続中のMFPについて、 トナーや印刷用紙の状態を取得、表示します。	○※65	-	-	-
		自動検出切り替え機能	自動的に機器を検出するか否か、設定することができます。	○※65	-	-	-
ネットワークマップ	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。	検出通知	機器が検出されたことを契機に、管理者もしくはその他ユーザに対して、 機器を検出した旨の通知が可能です。	◎	-	-	-
		ネットワークマップの取得、表示	アクセスポイントごとに機器一覧を取得、表示することができます。	◎	◎	◎	◎
		ネットワークマップの検索	IPアドレスやネットワーク名で検索できます。 大規模ネットワーク環境でも、目的のネットワークを簡単に確認することができます。	◎	◎	◎	◎
		ネットワークの管理	自動検出したネットワークの管理や機器検出の有効・無効切り替え、 ネットワークに対して名前の変更及び備考登録が可能です。	◎	◎	◎	◎
設定管理	機器へ適用する設定を作成し、管理することができます。機器を登録した時に自動的に適用することや、作成した数種類の設定をまとめることも可能です。	デフォルト設定	機器登録時、自動的に適用する設定を選ぶことができます。	◎	◎	◎	◎
		設定一括適用	登録済み機器全て、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	機器に適用する設定をまとめて管理することができます。	◎	◎	◎	◎
		設定情報のレポート出力	機器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できます。	◎	◎	◎	◎
		かんたん初期設定ウィザード	SDM導入時の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 **初期化必須**	アプリケーションアイコン及びフォルダーの位置を、指定及び固定することができます。	Dock設定	Dockに配置するアプリケーションアイコン及びフォルダーの位置を、指定及び固定することができます。	-	-	◎ (iOS 12.0～) (iPadOS 13.1～)	-
		Page設定	Pageに配置するアプリケーションアイコン及びフォルダーの位置を、指定及び固定することができます。 複数Pageへの設定が可能です。	-	-	◎ (iOS 12.0～) (iPadOS 13.1～)	-

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「ー」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】端末管理							
位置情報取得	機器の位置情報を取得し、管理画面上で確認することができます。 また、過去に取得した位置情報履歴を確認することも可能です。	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できます。	-	-	-	○※68
		位置情報の取得及び表示	位置情報を取得し、管理サイト上で確認することができます。 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できます。	◎ （Windows 8.1～）	○※2、35	○※2、35	◎
		位置情報履歴取得	機器で取得、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できます。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できます。	◎	◎	◎	◎
		位置情報取得 許可/不許可表示	Androidエージェントにおける位置情報取得の許可/不許可状態を、 機器情報として管理サイト上に表示することができます。	-	-	-	◎
アプリケーション情報取得	機器にインストールされているアプリケーション情報を取得、確認することができます。アプリケーション情報は、OSや機器名等の条件を指定してレポートを出力することも可能です。	アプリケーション情報の取得	機器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できます。	◎	◎	◎	◎
		アプリケーション情報のレポート出力	機器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できます。	◎	◎	◎	◎
		アプリケーション情報のレポート出力（高速版）	アプリケーション情報について、限定された項目のみ高速でCSVレポート出力を行うことができます。	◎	◎	◎	◎
		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	機器／ユーザーが所属する組織や、その階層構造を作ることができます。これにより、支所／部署単位による機器の管理が可能となります。	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できます。 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できます。	◎	◎	◎	◎
		組織管理	管理サイト内に「組織」を定義、機器やユーザを組織と紐付けて管理することができます。	◎	◎	◎	◎
		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できます。	◎	◎	◎	◎
		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できます。	◎	◎	◎	◎
ユーザー管理	管理サイトの管理者や機器の所有者等のユーザーの情報を作成し、登録することができます。ユーザーの役割に対応した権限付与やユーザー情報の一括登録、アカウントポリシー設定が可能です。また、ユーザー自身がパスワードを管理することも可能です。	ユーザー管理	管理サイトを利用するユーザー、機器を利用するユーザー等を管理サイトへ登録、管理することができます。	◎	◎	◎	◎
		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できます。	◎	◎	◎	◎
		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できます。	◎	◎	◎	◎
		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できます。	◎	◎	◎	◎
		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できます。	◎	◎	◎	◎
		自由入力項目の作成	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。	◎	◎	◎	◎
エージェント管理	エージェント停止・削除に必要なパスワードを設定し、エージェントがユーザーによって管理外にされることを防止します。また、エージェントが管理サイトと定期的に行う通信の間隔を設定可能です。	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策として、パスワードの入力を強制させることができます。	◎	-	-	○※48
		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できます。	◎	-	-	◎
ログ取得・閲覧	管理サイトの操作やエージェントの動作をログで確認することができます。CSVによるレポート出力が可能です。	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できます。	◎	◎	◎	◎
		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できます。	◎	◎	◎	◎
		ログのレポート出力	機器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できます。	◎	◎	◎	◎
Android Enterprise **初期化必須**	Google社のAndroid Enterpriseに対応し、社用端末をより強固なセキュリティで保護しつつ、高度なアプリケーション管理を実現します。	Android Enterprise	Google社のAndroid Enterpriseに対応し、社用端末をより強固なセキュリティで保護しつつ、 高度なアプリケーション管理を実現します。	-	-	-	◎

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「－」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】端末管理							
ADE（Automated Device Enrollment） [旧名称：DEP(Device Enrollment Program)] **初期化必須**	Apple社のADE（旧名称：DEP）に対応し、機器アクティベーションのセットアップ時、すぐにMDMサーバに割り当てることができます。これにより、初期設定時のMDM登録の自動化と、設定プロセスの省略が可能です。また、MDMプロファイルの削除防止もできます。	MDM登録の強制	初回起動時にMDMライセンスの認証を必須とし、スキップを禁止できます。	-	◎※24	◎※24	-
		認証情報入力の省略	認証時に必要な企業コード・認証コードの入力を省略できます。	-	◎※24	◎※24	-
		監視対象モードの設定	機器のアクティベーション時に自動で監視対象モード（Supervised mode）に設定できます。	-	◎※24	◎※24	-
		MDMプロファイル削除防止	MDMプロファイルの削除ボタンを非表示にし、機器からMDMプロファイルの削除を禁止できます。	-	◎※24	◎※24	-
		ペアリングの禁止	機器のアクティベーション完了後、iTunesを介してMac機器・Windows機器と接続することを禁止します。	-	◎※24	◎※24	-
		セットアップアシスタントの省略	初回起動時の設定をあらかじめ管理サイトから設定することで、機器利用者は初回のセットアップを省略できます。	-	◎※24	◎※24	-
同期機能	ユーザー自身の操作、もしくは自動的に同期を実行することができます。	ユーザーによる同期	機器利用者自身により、同期することができます。	◎	◎	◎	◎
		定期同期	管理サイト上で設定された間隔、もしくはSDM標準の間隔に応じて、自動的に同期を実行することができます。	◎	-	-	◎
Apple Business Manager	Apple Business Managerと連携し、iOS/iPadOS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。	Apple Business Manager	Apple Business Managerと連携し、iOS/iPadOS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。	-	◎	◎	-
【基本機能】セキュリティ管理							
Windows 情報保護	Windowsに備わっている「Windows情報保護」機能をSDMから有効化することにより、企業データへ様々な制限をかけることが可能です。	企業データ指定	Microsoft社製、サードパーティ製のアプリを管理サイトで指定することにより、企業データとして保護対象にすることが可能です。	◎※59	-	-	-
		保護レベル指定	企業データへ一定操作を行おうとしたときの挙動を、ログ取得のみ、警告表示、禁止のレベルで指定することが可能です。	◎※59	-	-	-
		個別ログ表示	通常の管理サイトとは別表示のログで、Windows情報保護のログを表示することができます。	◎※59	-	-	-
設定変更の制限	ユーザーによる機器設定の変更を制限することが可能です。提供元不明アプリのインストール、開発者向けオプション、ステータスバー、アプリ確認(Google Playプロテクト)の設定変更制限ができます。	提供元不明アプリのインストール制限	Google Play store以外で提供されているアプリケーションのインストールを制限することができます。	-	-	-	◎※48
		開発者向けオプションの制限	開発者オプションの利用を制限することができます。	-	-	-	◎※48
		ステータスバーの制限	ステータスバーの利用を制限し、ステータスバーで設定可能なWi-FiやBluetooth等の設定変更を防ぎます。	-	-	-	◎※48
		アプリ確認の強制	「アプリの確認(Google Playプロテクト)」機能を強制することができます。	-	-	-	◎※48
端末初期化の制限 **初期化必須**	ユーザーによる端末の初期化を制限することができます。ユーザー操作によりMDMの管理下から外れることを防ぎます。	端末初期化の制限	ユーザーによる端末の初期化を制限することができます。ユーザー操作によりMDMの管理下から外れることを防ぎます。	-	-	◎※60	◎※48
セーフブートの制限	セーフモードによる起動を禁止できます。	セーフブートの制限	セーフモードによる起動を禁止できます。	-	-	-	◎※48
アカウントの制限 **初期化必須**	Apple IDやGoogleアカウント、Exchangeアカウント等の追加・削除を制限します。	アカウントの制限	Apple IDやGoogleアカウント、Exchangeアカウント等の追加・削除を制限します。	-	-	◎※61	◎※48
マルチユーザーの制限	ユーザーの追加や削除を制限します。マルチユーザーを制限することで、MDMの管理下から外れることを防ぎます。	ユーザーの制限	ユーザーの追加や削除を制限します。マルチユーザーを制限することで、MDMの管理下から外れることを防ぎます。	-	-	-	◎※48
スクリーンショットの制限	スクリーンショットの取得を制限することができます。業務データの漏えいを防ぎます。	スクリーンショットの制限	スクリーンショットの取得を制限することができます。業務データの漏えいを防ぎます。	-	◎	◎	◎※48
テザリング設定の制限	テザリング設定の変更制限、もしくはテザリング機能を禁止することができます。	テザリング設定の制限	テザリング設定の変更制限、もしくはテザリング機能を禁止することができます。	-	-	-	◎※48

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「ー」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】セキュリティ管理							
パスワードポリシー設定	パスワードの長さや複雑さ、解除失敗時の動作等、パスワードに関する設定が可能です。	パスワードポリシーの設定	機器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。	○※36	◎	◎	◎
		機器パスワード設定の強制設定	機器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できます。	○※36	◎	◎	◎
		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できます。	○※36	◎	◎	◎
		パスワード自動ロック時間の設定	無操作状態から機器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できます。	-	◎	◎	◎
		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機器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できます。	◎	◎	◎	○※20
		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時のロック画面に、SDMのロック画面を表示し、データ漏えいを防ぎます。	◎	-	-	◎
		スクリーンセーバー設定	機器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。	○※47	-	-	-
		スクリーンロックパスワード変更	機器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できます。	-	-	-	○※21,48
		スクリーンロックパスワード削除	機器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できます。	-	◎	◎	-
スクリーンロック画面の制限	スクリーンロック中に利用できる機能(アプリからの通知や、指紋によるロック画面の解除等)を制限することができます。	すべての通知	アプリ等からの通知を制限します。	-	-	-	◎※48
		業務領域内アプリの通知	端末に初期インストールされているアプリ以外の通知を制限します。	-	-	-	◎※48
		信頼できるエージェント	スマートロック機能によるスクリーンロックの解除を制限します。	-	-	-	◎※48
		指紋によるロック解除	指紋によるロック画面解除を制限します。	-	-	-	◎※48
root化/Jailbreak検知	管理している機器がroot化/Jailbreakされたことを検知することができます。検知した場合、メールにて通知することも可能です。	root化、JailBreak検知機能	機器のroot化、JailBreakの状態を検知することができます。エージェントインストール後、利用可能となります。	-	◎※2, 35	◎※2, 35	◎
無通信検知	一定期間通信が行われなかった機器や、ユーザーによるMDM構成プロファイル削除を検知することができます。	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できます。 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できます。	◎	◎	◎	◎
		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	指定した間隔、管理サイトとの通信が行われなかった機器に対して、ロックもしくは機器の初期化・データ削除また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。	無通信時ロック	指定した間隔、管理サイトと無通信だった際に、機器をロックすることができます。	◎	-	-	◎
		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。	◎	-	-	-
リモートロック	管理サイト上から、機器をロックすることができます。	リモートロック　（オリジナルロック画面）	遠隔操作により、機器をロックを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。	◎	-	-	◎
		リモートロック　（警告音）	遠隔操作により、機器をロックを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）	機器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。	-	◎	◎	◎
		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 **初期化必須**	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、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可能です。	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。	-	-	◎ (iOS 12.0～) (iPadOS 13.1～)	-
		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。	-	-	◎ (iOS 12.0～) (iPadOS 13.1～)	-

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「－」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】セキュリティ管理							
リモートワイプ	管理サイト上から、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。	リモートワイプ	機器を遠隔にて初期化することができます。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できます。	-	◎	◎	◎
		リモートワイプ（SDカード）	リモートワイプ時に機器内のSDカードを遠隔にて初期化することができます。	-	-	-	◎
		リモートワイプ（BitLocker）	Bitlockerによる暗号化を実施した機器に対し、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。	○※18	-	-	-
		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できます。	-	○※9	○※9	-
		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、 実行後には初期設定画面が表示されます。	○※56	-	-	-
アクティベーションロック **初期化必須**	管理サイト上から、機器のアクティベーションロック有効化、無効化及び解除を行うことができます。有効化することにより、設定時のApple ID及びパスワードを知らない第三者による再利用を防ぎます。	アクティベーションロック設定変更	アクティベーションロックの有効・無効設定を行うことができます。	-	-	◎	-
		アクティベーションロック解除	アクティベーションロックを解除することができます。	-	-	◎	-
構成プロファイル作成 **一部の機能、初期化必須**	構成プロファイルを管理サイト上で直接作成し、保存することができます。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し保存することも可能です。	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できます。 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「パスコード」、「制限」、「証明書」、「Wi-Fi」、「メール」、「ドメイン」、「Webフィルタリング」、「グローバルHTTPプロキシ」、「VPN」の項目を作成、閲覧、編集、削除できます。	-	◎	◎	-
		iOS構成プロファイル画面上設定 （監視対象限定項目）	監視対象機器限定の設定項目にも対応しています。	-	-	◎	-
構成プロファイル設定 **一部の機能、初期化必須**	管理サイト上に保存された構成プロファイルを、機器へ適用することができます。	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できます。	-	-	◎	-
		Store購入制限	iTunes Store内の購入を制限することができます。	-	○※28	○※28	-
		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できます。	-	-	◎	-
		スクリーンショット禁止	iOS/iPadOS機器上におけるスクリーンショット撮影を禁止することができます。	-	◎	◎	-
		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。	-	-	◎	-
		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。	-	-	◎	-
		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	構成プロファイルの削除禁止、もしくは削除時にパスワード入力を必須とすることができます。	構成プロファイル削除保護	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できます。	-	◎	◎	-
		構成プロファイル削除禁止	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できます。	-	◎	◎	-
認証制御設定	事前に管理サイトへ登録された機器のみ、SDMのライセンス認証を許可することができます。	認証制御設定	事前に登録された機器のみSDM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。	◎	◎	◎	◎
OSアップデート管理 **一部の機能、初期化必須**	OSアップデートの延期設定等を行うことが可能です。	ソフトウェア・アップデート遅延設定	新しいiOS/iPad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。	-	-	◎ (iOS 12.0～) (iPadOS 13.1～)	-
		OSアップデート管理設定	機器のOSアップデートに対して強制アップデート、指定時間内のみアップデート、OSアップデート促進などを実施することができます。	-	-	-	◎※48
		OSアップデート指示・情報取得	iOS/iPadOS機器に対してOSアップデート指示を出すことが可能です。 また、当該機器のアップデート可能なOSバージョンを取得することができます。	-	-	◎ (iOS 12.3～) (iPadOS 13.1～)	-
		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。	○※55	-	-	-

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「ー」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】セキュリティ管理							
システムセキュリティ	ファイアウォール、スクリーンセーバー、インターネットオプションのセキュリティ設定等の状態を自動診断・設定し、ログを出力することができます。また、ウイルス対策ソフトやWindows Defender、スパイウェア対策ソフトの状態を診断をすることも可能です。	セキュリティ状況取得	機器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できます。	○※14, 30	-	-	-
		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	○※31	-	-	-
		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。	○※55	-	-	-
		スクリーンセーバ解除時画面の設定・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	◎	-	-	-
		Windows Defender設定・診断	Windows Defenderの「ウィルスと脅威の防止」「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。	◎※56	-	-	-
		Officeに対するマクロ実行制限	Microsoft Office Word、Excel、PowerPoint、Outlookに対して、マクロ実行を制限する設定を適用することができます。	◎	-	-	-
		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。	○※33,70	-	-	-
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。	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	機器認証に必要なクライアント証明書、およびCA証明書を管理サイトへアップロードし、配布することが可能です。	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。	◎	◎	◎	◎
		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。	◎	◎	◎	◎※48
		証明書利用アプリの設定	クライアント証明書配信する際、クライアント証明書を利用するアプリケーションを管理者が選択できます。	-	-	-	◎※48
【基本機能】設定管理							
連絡先情報設定	連絡先情報を登録し、機器へ配信することができます。CSVによるインポート、エクスポートやCardDAVによる設定も可能です。	連絡先情報の設定	連絡先一覧を作成し、機器へ設定を行うことができます。	-	-	-	◎
		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。	-	-	-	◎

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「－」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】デバイス管理							
外部記憶制御	SDカード、USBデバイス、IEEE1394およびCD/DVD/ブルーレイの利用を禁止することができます。	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できます。	◎	-	-	○※5、48
		USB利用禁止・許可設定(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。	◎※66	-	-	-
		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。	-	-	-	◎※48
		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。	-	-	-	◎※48
		IEEE1394利用禁止・許可設定	IEEE1394の利用禁止・許可を設定することができます。	◎	-	-	-
		CD/DVD/ブルーレイ	CD/DVD/ブルーレイの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	カメラやBluetoothの有効／無効を設定することができます。	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。	-	-	-	○※52
		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。	-	-	-	◎(9.x)※48 -(10.x～11.x)
暗号化設定	機器の暗号化を促したり、実際に機器を暗号化することができます。	機器暗号化の設定	機器の暗号化画面を呼び出し、暗号化を促すことができます。	○※69	◎	◎	◎
		機器暗号化の設定（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	ドライブの空き容量やCPUの温度、ハードディスクの異常等のシステムに関する項目を監視し、異常を検知した場合はその旨をログへ出力することができます。	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。	◎※15	-	-	-
		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。	◎※15	-	-	-
		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時、それを有効化します。	◎※15	-	-	-
		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。	◎	-	-	-

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「ー」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】アプリケーション/コンテンツ管理							
アプリケーション配信 **一部の機能、初期化必須**	機器に対してアプリケーションを配信することができます。業務アプリの一括配信や、機器上の操作を必要としないサイレントインストールも可能です。	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	◎※25	◎※25	◎
		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SDM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	SDM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。	-	◎	◎	-
		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。	○※7	-	○※6,25,27	◎※50
		アプリケーション配信（msi,exe,com, bat,cmd)	管理者が指定したアプリケーション（msi, exe, com, bat, cmd形式）を自動的に機器へ配信、インストールを自動実行できます。	○※7	-	-	-
		オリジナルアプリ登録・配信	アプリをアップロードし、機器へ配信することができます。	-	◎	◎	◎
		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。	-	◎	◎	-
アプリケーション配信 （Appとブック=旧名称：VPP）	Apple社が提供するAppとブック(旧名称：VPP)の仕組みに対応したアプリケーション配信を実施することができます。 AppStore上の有償アプリケーションまたはカスタムB2Bアプリケーションを一括購入した後に、指定したデバイスもしくは指定したユーザーに対して、アプリケーションのライセンスの付与・回収が可能です。	アプリケーション配信 （Appとブック=旧名称：VPP）	Apple社が提供する、Appとブック(旧名称：VPP)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。	-	◎※40	◎※40	-
ブック配信 （Appとブック=旧名称：VPP）	Apple社が提供する、Appとブック(旧名称：VPP)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。	ブック配信 （Appとブック=旧名称：VPP）	Apple社が提供する、Appとブック(旧名称：VPP)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。	-	◎※40	◎※40	-
アプリケーション配信 (Android Enterprise対応) **初期化必須**	Android Enterpriseに対応したアプリケーション配信を実施することができます。自社専用のアプリストアの作成、アプリケーションのサイレントインストール/サイレントアンインストールが可能です。	自社専用Google Play storeの作成	自社用のアプリストアを作成できます。管理者は配信したいアプリを指定し、配信対象を設定することが可能です。	-	-	-	◎※48,50
		アプリケーション配信(オンデマンド/サイレント)	インストールさせたいGoogle Play storeのアプリケーションを配信することができます。アプリケーションによってユーザーが任意のタイミングでインストールするオンデマンド形式、ユーザー操作なくインストールを実施するサイレントインストール形式を選ぶことが可能です。	-	-	-	◎※48,50
アプリケーション個別設定	アプリケーションごとに、アプリケーションが使用する権限、アプリケーションが独自に持つ設定値の設定を行うことができます。	アプリケーションの権限制御	アプリケーションが使用する権限の設定ができます。デフォルト値の指定や、使用する権限の許可/不許可を強制することが可能です。	-	-	-	◎※48,50
		アプリが独自に持つ設定値の設定	MDMから設定を行うことを想定された設定値の設定をアプリケーション個別に行うことができます。	-	-	-	◎※48,50
		権限移譲アプリの設定	特定のアプリを「権限移譲アプリ」に設定し、業務用アプリからマルウェアアプリの一時停止を行うなど端末にインストールされている他のアプリを制御する強い権限を与えることが可能です。	-	-	-	◎
App Configuration	App Configurationに対応したアプリケーションへSDMから設定値を配布することができます。	App Configuration	App Configurationに対応したアプリケーションへSDMから設定値を配布することができます。	-	◎	◎	-
アプリケーションアップデート	SDMから配布済みのアプリにアップデート指示を出すことができます。	アプリケーションをアップデート	SDMから配布済みのアプリに対して、アップデート指示を出すことができます。	◎	◎※43	◎※43	◎
		アップデートするタイミングの指定	Android Enterprise アプリケーション配信を行う際に、配信するアプリのアップデートするタイミングを指定できるようになります。	-	-	-	◎

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「ー」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】アプリケーション/コンテンツ管理							
アプリケーション禁止 **一部の機能、初期化必須**	特定のアプリケーションの利用を禁止できます。	アプリケーション非表示 (ブラックリスト)	ブラックリストに登録されたアプリケーションを端末上で非表示にすることができます。プリインストールアプリケーションもブラックリストに指定することが可能です。	-	-	-	◎※48
		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。	○※67	-	◎	◎
		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。	-	-	○※19	-
		アプリケーション起動禁止 (ブラックリスト)	ブラックリスト形式によるアプリケーション及びUWPアプリ起動禁止が設定できます。	○※67	-	-	-
		アプリケーション起動禁止 (ホワイトリスト)	ホワイトリスト形式によるアプリケーション起動禁止が設定できます。	○※57, 67	-	-	-
		ゲーム及びUWPアプリの制限	ゲーム及びUWPアプリに対して、レーティングレベル、アプリ毎の許可/禁止設定が可能です。	○#※16, 29	-	-	-
Open-In 制御	SDMから配信された管理対象アプリやアカウント・Safariで閲覧したWebサイト間のデータ受け渡しを制御することが可能です。	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	SDM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できます。	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できます。	-	◎	◎	○※49
アンインストール制限機能 **初期化必須**	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。	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。	-	-	◎	-
個別設定画面の使用禁止	ユーザーによって、機器の設定が変更されることを防ぎます。	個別設定画面の使用禁止	OS標準設定アプリ内の「Wi-Fi設定」「VPN設定」「APN設定」「デバイス管理者機能」「デバックモード」「アプリケーション設定」画面の利用を禁止設定することができます。	-	-	-	-
アプリケーション検知	業務上必要なアプリケーションがインストール済みか否かを検知することができます。	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	MS OfficeやAppとブック(旧名称：VPP)のライセンス数を集計、管理することができます。	ソフトウェアライセンス過不足検知	Microsoft Office製品のライセンス情報を管理サイトで管理し、 管理者がライセンス数の過不足を認識できるようレポートを表示できます。	◎	-	-	-
		ソフトウェアライセンス調整	Microsoft Office製品のアップグレード/ダウングレードに伴うライセンス数の移動を管理することができます。	◎	-	-	-
		Appとブック(旧名称：VPP)ライセンス数管理	Appとブック(旧名称：VPP)ライセンスの付与状況を確認することができます。	-	◎	◎	-
業務専用端末化	管理サイト上の操作で特定のアプリケーションのみが起動する設定を配布することができます。	業務専用端末化設定	管理サイト上の操作で特定のアプリケーションのみが起動する設定を配布することができます。	-	◎	◎	-

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「ー」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】インターネット接続管理							
Wi-Fiフィルタリング **iOSのみ初期化必須**	ホワイトリストによるWi-Fiフィルタリングを設定することができます。	Wi-Fiフィルタリング	指定されたSSIDのみ、Wi-Fi接続が許可できるよう設定できます。	◎	-	◎※62	[要：オプション:インターネット接続管理](8.x～)※48
Webフィルタリング	ホワイトリスト、ブラックリストもしくは制限の強さに基づくWebフィルタリングを設定することができます。	Webフィルタリング（ホワイトリスト/ブラックリスト）	ホワイトリスト、ブラックリストに基づくウェブフィルタリングを設定することができます。	-	-	◎	[要：オプション:インターネット接続管理]※63
		Webフィルタリング（制限レベル）	予め用意されている制限レベルに基づいたWebフィルタリングを設定することができます。	-	-	◎	-
お気に入り/ホーム	お気に入りへ追加するWebページを配信、及びホームページを設定することができます。	お気に入り配信	お気に入りを配信することができます。	○※33	[要：オプション:インターネット接続管理]※33	[要：オプション:インターネット接続管理]※33	[要：オプション:インターネット接続管理]※33
		ホームページ設定	機器のホームページを設定することができます。	○※33	-	-	-
Webクリップ配信	SDM 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も可能です。	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	SDM 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 **一部の機能、初期化必須**	プロキシ設定を適用することができます。	プロキシ（手動構成）	手動によるプロキシ設定が行えます。	◎	◎	◎	◎
		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。	-	-	◎	-
接続設定	Wi-Fi接続先の設定を適用することができます。 またローミング設定など接続に関する設定も可能です。	Wi-Fi設定	機器の無線LAN環境設定を行うことができます。Wi-Fi設定のHidden SSIDにも対応しています。	○※64	◎	◎	[要：オプション:インターネット接続管理]
		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。	-	◎	◎	-
		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。	○※64	-	-	[要：オプション:インターネット接続管理]
デバイスVPN設定	VPN接続の設定を適用することができます。	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	Exchange ActiveSyncの設定を適用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アカウント等、メールの送受信に関して設定をすることができます。	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。	-	◎	◎	-

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「－」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【基本機能】メッセージ配信機能							
メッセージ通知	独自Push通信によるメッセージ通知ができます。スケジュールを指定しての自動配信や、通知状況(未受信・既読・未読)の確認も可能です。	メッセージ通知設定	管理者より、機器へ指定のメッセージを送信することができます。	-	○※2	○※2	◎
		通知結果の集計	機器より、通知済みのメッセージ閲覧状況を集計することができます。	-	○※2	○※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	○※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	○※2	◎
【オプション契約】モバイルウイルス対策							
モバイルウイルス対策	ウイルススキャンに関する設定を機器へ適用することで、不正なアプリのインストールを自動検知し、削除を促すことができます。また、対策状況を監視することも可能です。	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。	-	-	-	◎
		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。	-	-	-	◎
【オプション契約】インターネット接続管理							
お気に入り設定	お気に入りのWebサイトを配信することができます。	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(URL)	ホワイトリスト、ブラックリストによるWebフィルタリングを設定することができます。	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	DM BrowserのWebサイト閲覧履歴を取得し、ログに出力することができます。	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接続先設定を配信することができます。	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。	○※64	-	-	◎
		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。	○※64	-	-	◎
Wi-Fiフィルタリング	ホワイトリストによるWi-Fiフィルタリングを設定することができます。	Wi-Fiフィルタリング設定	指定の無線LANアクセスポイントのみ接続を許可する設定を行うことができます。	◎	-	-	◎ ※48
DM Browser	SDMと連携する独自ブラウザーを提供します。ブラウジング機能を有する他、お気に入り設定やWebフィルタリング設定、Web閲覧履歴設定を適用することができます。	SDM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。	-	◎	◎	◎
		タブブラウザー	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。	-	◎	◎	◎

スマートデバイスマネジメント（SDM）提供機能一覧　　更新日　2023/3/24

凡例	
「◎」…提供中	「ー」…OS非対応
「○」…提供中（一部制約有り）	凡例横に「＃」…Windows RTに対応した項目

大項目	中項目	小項目	機能説明	Windows	iOS/iPadOS		Android
					監視対象　未適用時	監視対象　適用時（初期化必須）	ストア版エージェント（初期化必須）
【オプション契約】WiFi Zone Management							
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ことができます。	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。	◎	-	-	◎
		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。	◎	-	-	◎
		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。	◎	-	-	◎
		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。	◎	-	-	◎
		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。	◎	-	-	◎

※1 シークレットモードでの利用時は不可です。
※2 iOSのエージェントアプリが必要。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」に非表示の場合、本機能が動作しない場合があります。
※3 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。
※4 対応機器は限定されています。詳細は、機器対応表を御覧ください。
※5 Android 4.2以降ではOSの仕様上、SDカード禁止に非対応です。以下のように対応します。
Android 4.2：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。
※6 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。
※7 本機能をご利用の際は、お客様環境にてWindowsエージェントと通信可能なファイルサーバが必要となります。
※8 対応OS、対応機種はデジタルアーツ株式会社のWebサイトより確認できます：http://www.daj.jp/bs/ifb/requirements/
※9 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。
※10 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。
※12 機器メーカより署名をいただくことにより対応可能となります。ご希望のお客様はご相談下さい。
※13 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。
※14 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。
※15 Windows Serverでは提供対象外の機能となります。
※16 MS-MDMによりライセンス認証した機器に対して提供可能です。
※17 Mac OSXのリモートワイプでは、リモートワイプ実行後のロック解除の為に、PINコード入力を求めます。
※18 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。
※19 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。
※20 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。
※21 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。
※22 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。
※23 対応するVPNはCisco AnyConnect、Juniper SSL および カスタムSSLです。
※24 ご利用の際は、ADE（旧名称：DEP）アカウントの登録と、AppleもしくはADE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。
ADE（旧名称：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
※25 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
※26　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、
「AppStoreから無料アプリダウンロードの際にパスワードを求められない」設定にした場合、長時間経過後に無料アプリの配信でAppleIDのパスワード入力を求められます
※27 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。
※28 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
※29 Windows 10、11においてはMS-MDMに未対応となります。
※30 Windows 10、11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。
※31 Windows 10、11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。
※32 Windows 10、11においては、「厳密なP3P検証を有効にする」、『プライバシーが「中」未満の場合に「中」に設定する』に非対応です
※33 Windowsの場合、Internet Explorerのみ対象となります。Microsoft Edgeには非対応です。Windows 11以降、インターネットの「お気に入り」設定は非対応になり
iOSの場合、DM Browser のみで有効です。
Android 5.x 以下の場合、標準ブラウザーおよびDM Browser のみ有効です。Android 6.x 以降の場合、DM Browser のみで有効です。
※34 Exchange、Cybozu等接続先サービスについてはお客様にて予め別途ご契約いただく必要がございます。
※35 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（アプリを最前面の状態）で起動する必要があります。
※36　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。
※37 プロキシ通信を使用中の環境では、Webフィルタリング（MS-MDM）が機能しません。
※38 Android 9.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。Android 10以降はWi-FiのMACアドレスがランダム値になります。
※39 Android 2.2以下はSHA-2に非対応の為、モバイルウイルス対策はAndroid 2.2以下で非対応です。
※40 指定したデバイスに対して配信する方式は、対応OSはiOS 12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。
※41 Shared iPadをご利用の際は、機器の容量は32GB以上である必要があります。
※42 クラスルームアプリケーションをご利用の際は、生徒の機器を監視対象とする必要があります。また，機器間に通信可能なWi-Fi設定、Bluetoothをオンにする設定が必要です。
※43 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。
※44 リモートロックした後、PINコードがランダムに再設定されます。PINコードは機器のログから確認できます。
※45 機器からの機器分類入力に対応していません。
※46 GoogleChromeによる動作を確認。
※47 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、Win 11: Home
※48 エージェントアプリケーションをDevice Owner Modeにてキッティングいただく必要があります。
※49 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する事なくインストール制限を行うことができます。
※50 Fully managed Device(Android Enterprise)機能を利用いただく必要があります。
※51 アプリケーションのメモリサイズがすべて0byteと表示されます。
※52 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。
※53 ご利用の際は、ゼロタッチ登録に対応しているキャリアから、ゼロタッチ登録に対応した端末を購入する必要があります。
※54 CA証明書を複数設定したWi-Fi設定は、Android 9.x以上の端末でしか使用できません。
※55 Windows 10、11 以降でのみ動作します。Windows 10、11 Homeの場合はアクティブ時間のみ設定可能です。
※56 Windows 10、11 以降でのみ動作します。
※57 Windows 10、11　Enterprise及びEducationでのみ動作します。
※58 端末がAndroid 9にアップデート可能、かつ従来版エージェントがDevice Owner Mode化されている必要があります。
※59 Windows10 Pro（20H2以降）、Windows10 Ent（1909 以降、但し2004は除く）および Windows10 Edu（1909 以降、但し2004は除く）、Windows 11 Pro/Ent/Eduの 32 ビット版と 64 ビット版に対応しています。
※60 構成プロファイル内、[すべてのコンテンツと設定を消去"を許可(監視対象のみ)]のチェックを外す事で制限いただけます。
※61 構成プロファイル内、[アカウント設定の変更を許可(監視対象のみ)]のチェックを外す事で制限いただけます。
※62 構成プロファイル内、[Wi-Fi ペイロードによってインストールされたWi-Fi ネットワークのみに接続(監視対象のみ)]にチェックボックスにチェックを入れると、構成プロファイルで登録済みのWi-Fi のみにアクセスできるようになります.
※63 本機能は、Android 5.x以下の端末の場合、標準ブラウザーおよびDM Browserに対応しています。Android 6.x以降の端末の場合、DM Browserにのみ対応しています。
Android 4．0 ～5.xの端末の場合は、本機能で禁止しているウェブサイトであっても標準ブラウザーのシークレットモードからは閲覧が可能になります、
これを回避するには、アプリケーション禁止機能を利用して標準ブラウザーの使用を禁止し、DM Browserのみ使用できるよう制限してください。
Android 6．0 ～の端末の場合は、オプション:インターネット接続管理にて提供しております、DM Browserのみ制限可能となります為、本機能で禁止しているウェブサイトであっても、他のブラウザーアプリからは閲覧が可能になります。
これを回避するには、アプリケーション禁止機能を利用して他のブラウザーアプリの使用を禁止し、DM Browserのみ使用できるよう制限してください。
※64　Windowsは、EAP方式はTLSのみ対応となります。
※65 契約後、Windows PCを初めて認証された最初の1回のみ、同一ネットワークセグメント内にて機器検出を行います。以後は検出無最初に登録された検出有効なネットワークを削除されましても、リセットされません。
※66 禁止できる外部デバイスには条件があります。詳細は、弊社担当窓口またはお問合せフォームよりお問合せ下さい。
※67 本設定で外部デバイスCD、DVD、ブルーレイ機能を含むアプリケーションを禁止にしなくても、機能制限で、外部デバイス、CD、DVD、ブルーレイの使用が禁止されている場合は、CD、DVD、ブルーレイ機能を含むアプリケーションの機能が制限
※68 Android 9 以降、位置情報の取得は 1 時間に 1 回程度へ制限されます。
※69 BitLocker機能を備える以下のOS以外は本設定を行うことはできません。
Win 8.1: Pro、Enterprise
Win 10: Pro、Education、Enterprise
Win 11: Pro、Education、Enterprise
WindowsServer 2012: 無印
※70 Windows 11以降、ブラウザ関連設定における「拡張保護モードを有効にする」「拡張保護モードで64ビットプロセッサを有効にする」は非対応になります。