スマートデバイスマネジメント（SDM）

提供機能（2018年5月現在）

基本機能

端末管理　セキュリティ管理　設定管理　デバイス管理　アプリケーション管理　メッセージ通知機能　コンテンツ配信機能　インターネット接続管理

端末管理			iOS	Android	Windows
デバイスオーナー	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。	－	○（*22）（*23）（Android 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。	－	○（*23）（Android 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。	○	○	○
	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。	○	○	○（*9）
	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。	○	○	－
	パスワードポリシーの取得	機器のパスワードポリシーに関する項目を確認することが出来ます。	○	○	○
	SIM情報の取得	電話番号や現在のキャリアネットワークなどのSIM情報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	管理されている端末をネットワークマップ上に表示します。	○（*1）	○	○
	IT機器自動検出	スマートデバイスマネジメント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。 ※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。	○	○	○
	更新プログラム適用状況の取得	未適用かつ「重要」とされている更新プログラムを取得し、管理者がその適用状況を管理サイト上より確認することが出来ます。	－	－	○
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。	○（*16）（iOS 9.3～）	－	－
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。	－	○	－

	端末管理		iOS	Android	Windows
	位置情報の取得	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。	○(*3)	○	○ (Windows 8.1 ～)
	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。	–	○	–
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。	○	○	○(*15)
	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。	○	○	○
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	ユーザ管理	管理サイトを利用するユーザ、端末を利用するユーザ等を管理サイトへ登録、管理することが出来ます。	○	○	○
	ユーザ権限制御	ユーザに対して、権限を設定することが出来ます。	○	○	○
	ユーザ情報インポート	CSVを用いて、ユーザを一括登録することが出来ます。	○	○	○
	ユーザ情報のレポート出力	登録済みユーザをCSVとしてレポート出力することが出来ます。	○	○	○
	所属グループ設定	管理下における所属グループを設定することが出来ます。	○	○	○
	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。	○	○	○
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。	–	○(*24)	○
	エージェントアンインストール保護	アプリのアンインストールを禁止することにより、エージェントがアンインストールされることを防ぎます。	○(*16)	–	–
	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(Device Enrollment 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。	○(*21)	–	–
同期機能	自動同期	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出来ます。	○	○	○
	手動同期	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出来ます。	○	○	○

ページの先頭へ

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を設定します。	○	○	○(*19)
	端末パスワード設定の強制設定	端末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。	○	○（Android 3.0～）	○(*19)
	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。	○	○（Android 3.0～）	○(*19)
	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。	○	○（Android 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。	−	○（Android 4.0～）	−
	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。	−	○(*24)	−
	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。	○	−	−
	スクリーンセーバーのポリシー設定	スクリーンセーバーの有効/無効、スクリーンセーバーパスワードの有効/無効、スクリーンセーバーのタイムアウト時間を設定することが出来ます。	−	−	○(*20)
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。	○	○	○
	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。	−	○	−
	構成プロファイル削除検知	インストールされている構成プロファイルが削除されたか否か検知することが出来ます。 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出来ます。	○	−	−
root化/Jailbreak検知	root化、JailBreak検知機能	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。	○(*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。	−	○	○
	メッセージ出力(オリジナルロック画面)	オリジナルロック画面に管理者からのメッセージを表示することが出来ます。	−	○	○
	アラート音(オリジナルロック画面)	リモートロック時にアラート音を鳴らすことが出来ます。	−	○	−
	リモートロック（スクリーンロック） ※スクリーンロックの場合、端末のログイン画面を表示します。	遠隔から端末をスクリーンロック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。	○	○	○
	メッセージ出力(スクリーンロック)	スクリーンロック画面に管理者からのメッセージを表示することが出来ます。	○	−	−
	緊急連絡先発信(スクリーンロック)	スクリーンロック画面に緊急連絡先を表示させ、緊急連絡先へ連絡することが出来ます。	○	−	−

セキュリティ管理			iOS	Android	Windows
紛失モード	紛失モード	遠隔から端末を「紛失モード」に設定することで、端末をロックすることが出来ます。（端末側からロック不可） また「紛失モード」中は、エージェントがインストールされていなくとも、遠隔から位置情報の取得が出来ます。	○（*16）（iOS 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。	○	○	○(*18)
	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（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。	○（*8）	－	－
	リモートワイプ（オフライン）	以下の場合、端末を初期化することが出来ます。 ・管理サイトとの通信が一定時間行われなかった場合 ・ロック解除に指定回数失敗した場合	－	－	○
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。	○（*16）	－	－
	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。	○（*16）（*21）	－	－
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。	○（*16）（iOS 7.0～）	－	－
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出来ます。	○（*16）（iOS 7.0～）	－	－
	Store購入制限	iTunes Store内の購入を制限することが出来ます。	○	－	－
	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。	○（*16）（iOS 6.0～）	－	－
	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。	○	－	－
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	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。	○	○	○
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。	－	－	○（*13）

	セキュリティ管理		iOS	Android	Windows
	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。	−	−	○
	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。	−	−	○（Vista〜）
	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。	−	[モバイルウイルス対策]	○

ページの先頭へ

	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。	−	○	−

ページの先頭へ

	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。	−	○(*6)	○
	USB利用禁止・許可設定・ホワイトリスト設定	USBの禁止・書込みのみ禁止・許可を設定することが出来ます。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出来ます。大容量ストレージのみ、または、全てのUSBデバイスを対象に禁止する事が出来ます。	−	−	○
	CD/DVD/ブルーレイ利用禁止設定	CD/DVD/ブルーレイの禁止・書込み禁止・許可を設定することが出来ます。	−	−	○
	IEEE1394デバイス	IEEE1394デバイスを禁止することが出来ます。	−	−	○
	フロッピーディスク	フロッピーディスクを禁止することが出来ます。	−	−	○
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出来ます。	○	○	−
	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出来ます。	−	○	−
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。	○	○（Android 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。	−	−	○(*14)

	デバイス管理		iOS	Android	Windows
	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。	−	−	○(*14)
	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。	−	−	○ (Vista〜)
	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。	−	−	○(*14)
	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 ように設定することができます。	−	−	○

ページの先頭へ

アプリケーション管理			iOS	Android	Windows
App Manager	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	端末へ、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出来ます。	○	○	−
	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出来ます。	○	−	−
	アプリケーション配信(管理対象)	AppStore/in-houseアプリを管理対象として配信することが出来ます。	○	−	−
	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出来ます。	○(*7) (*16)	−	−
	オリジナルアプリ登録・配信	in-houseアプリを50MB(1アプリ当たり)/50アプリまでアップロードし、配信することが出来ます。	○	−	−
	プロビジョニングプロファイル配信	Inhouse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出来ます。	○	−	−
	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出来ます。	○	○	−
アプリケーション配信 (VPP対応)	アプリケーション配信(VPP対応)	Appleが提供するVPP(Volume Purchase Program)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出来ます。 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。	○ (iOS 7.0〜)	−	−
アプリケーションアップデート	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。	○(*17)	○	−
アプリケーション起動禁止	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起動を禁止することが出来ます。 また、ブラックリストに登録されたアプリケーションの起動を禁止することが出来ます。	○(*16)	○	−
	対象アプリケーション一覧のインポート/エクスポート	CSVを用いて、ホワイトリスト・ブラックリストにアプリケーションを一括登録することが出来ます。 また、ホワイトリスト・ブラックリストに登録済みのアプリケーションをCSVで出力することが出来ます。	−	○	−
	アプリケーション起動禁止 (特定アプリ)	Safari、iTunes Store、Youtubeの禁止が可能です。	○(*10)	−	−
アプリケーション制御	アプリ削除防止	アプリの削除を防止することが出来ます。これにより、配布した業務アプリの削除を防ぐことが出来ます。	○ (iOS 7.0〜)	−	−

	アプリケーション管理		iOS	Android	Windows
	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可能です。	○（iOS 7.0～）	–	–
インストール制限機能	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。	○	○（*4）	–
アプリ・ライセンス数集計・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。	○	○	–
	VPPライセンス数検知	VPPライセンスの付与状況を確認することが出来ます。	○（iOS 7.0～）	–	–

ページの先頭へ

	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。	○（*3）	○	–
	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。	○（*3）	○	–
	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出来ます。	○（*3）	○	–
	既読・未読集計	配信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。	○（*3）	○	–

ページの先頭へ

	コンテンツ配信機能		iOS	Android	Windows
コンテンツ配信	各種ファイルの配信	各種ファイル（PDF等のオフィスファイル）を、端末へ配信することが出来ます。複数のファイルをまとめたZIPファイルを指定することにより、まとめてファイルを配信することも可能です。	–	○	–
	アプリケーション配信	APKファイルを配信対象に指定することで、端末に対してアプリケーションインストールを促すことが出来ます。Advance機能を利用している場合、サイレントインストールすることも可能です。	–	○	–
	再配信機能	配信失敗時の再配信機能に対応します。	–	○	–
	レポート出力	コンテンツ配信の配信状況を、CSV形式でダウンロード可能です。	–	○	–
	スケジュール配信	指定した曜日の時刻にのみ、配信設定されたファイルのダウンロードを実施します。	–	○	–
	配信状況確認	配付した各種ファイルの配信状況を確認することが出来ます。	–	○	–

ページの先頭へ

	インターネット接続管理		iOS	Android	Windows
Webフィルタリング	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出来ます。	○（*16）（iOS 7.0～）	–	–
Webクリップ配信	Webクリップ配信	ホーム画面へ、Webクリップを配信することが出来ます。	○	–	–
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。	○	○（*12）	○
	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、削除出来ます。	○（*16）（iOS 7.0～）	–	–
接続設定	Wi-Fi設定	端末の無線LAN環境設定を行うことが出来ます。Wi-Fi設定のHidden SSIDにも対応しています。	○	○	–

	インターネット接続管理		iOS	Android	Windows
	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出来ます。	○	–	–
証明書配付設定	Webクリップ設定	Webクリップの設定を行うことが出来ます。	○	–	–
	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、配布することが出来ます。	○（iOS 7.0～）	○（*5）（Android 4.0～）	○
VPN設定	VPN設定	VPN接続を設定することが出来ます。	○	○（*11）	–
Exchange ActiveSync設定	Exchange ActiveSync設定	端末とのExchange ActiveSync設定をすることが出来ます。	○	–	–

ページの先頭へ

オプション機能（有料）

インターネット接続管理　Wi-Fi ZoneManagement　モバイルウイルス対策

インターネット接続管理			iOS	Android	Windows
Wi-Fiフィルタリング設定	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出来ます。	–	○	–
DM Browser	お気に入り設定	管理サイトからお気に入りを追加することができます。	○	○	–
	Webフィルタリング設定（ホワイトリスト／ブラックリスト）	管理サイトから以下の設定ができます。 • 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 • ブラックリストに登録されたURLへのアクセスを禁止	○	○（*2）	
	Web閲覧履歴取得、削除	管理サイトからWeb閲覧履歴の取得、削除を行うことが出来ます。	○	○（*2）	
	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出来ます。	○	○	–
	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。	○	○	–

ページの先頭へ

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。	–	○（*5）（Android 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	–	○（*5）（Android 4.0～）	○ ※プロキシ設定のみ利用可能
ゾーン検知によるポリシー切り替え	検知したゾーンによって、端末へ設定するポリシーを自動的に切り替えることが出来ます。	–	○（*5）（Android 4.0～）	○

Wi-Fi ZoneManagement		iOS	Android	Windows
所属ゾーン表示	予めSSIDによって定義されたゾーンの範囲内にいることを端末および管理サイト上で確認出来ます。	–	○(*5) (Android 4.0～)	○

ページの先頭へ

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)を確認することが出来ます。	–	○ (～ Android 5.x)	–
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。	–	○ (～ Android 5.x)	–
スケジュールスキャン	定期的に端末内をスキャンする日時を設定することが出来ます。	–	○ (～ Android 5.x)	–
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出来ます。	–	○ (～ Android 5.x)	–
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出来ます。	–	○ (～ Android 5.x)	–
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出来ます。	–	○ (～ Android 5.x)	–

*1: iOS端末の場合、Cellular/Wi-Fiモデルを混在して表示となります。
*2: シークレットモードでの利用時は不可です。
*3: iOSのエージェントアプリが必要となります。また、iOS7においては、エージェントアプリが「最近使用したアプリー覧」に表示されていることが前提となります。
*4: 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。
*5: Android OS 4.3/4.4は証明書パスワードのクリップボードコピーには非対応です。
*6: 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, 4.4:SDカード挿入検知時、専用のロック画面を表示します。
*7: AppStoreアプリの場合、管理対象アプリに設定されていて、配信先端末が監視対象端末、「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。
*8: 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。
*9: 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。
*10: Youtubeアプリ禁止は iOS 6未満のみ対応です。
*11: 端末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。
*12: 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。
*13: 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。
*14: Windows Serverでは提供対象外の機能となります。
*15: Windows Serverでは更新プログラムの情報が取得出来ません。
*16: 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。)
*17: アプリケーション配信で「管理対象」としたアプリが対象になります。
*18: リモートワイプ(BitLocker)と異なり、実行後にOSを起動することが出来ません。
*19: ドメイン参加時には適用されません。
*20: 以下のエディションでは適用されません。
・Windows Vista Home Basic / Home Premium
・Windows 7 Starter / Home Premium
・Windows 8、8.1(無印)
・Windows 10 Home
*21: お客様自身でDEP対応端末の準備、およびDEPへの登録が必要になります。
*22: 端末がNFCに対応している必要があります。
*23: 事前にキッティング対象の端末を工場出荷状態にする必要があります。
*24: Andrpid7.0以降の場合、デバイスオーナーモード限定の機能となります。(Android端末をデバイスオーナーモードにする際にはAndroid端末の初期化が伴います)