SMSM エージェントアプリ 機能差分一覧　『〇』…機能有 /『×』…機能なし /『-』…OS非対応・技術的不可　　更新日　2019年4月12日

※機種やOSによって操作方法や確認できる項目が異なる場合がありますので、詳細はマニュアルをご参照ください。
※基本プランでは次の機能がオプションサービスとなり別途料金が発生します。
「インターネット接続管理」「バックアップ」「ウイルス対策」「メッセージ通知」「WEBフィルター」

従来版はAndroid 8、Store版はAndroid 9（DOM）を想定

【基本機能】端末管理		従来版（非DOM）	従来版（DOM）	Store版
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。	〇	〇	〇
デバイスオーナー	QRコード(Android 7.0以降)、NFC(Android 6.0以降)、afw識別子(Android 6.0以降)、G Suiteアカウント(Android 6.0以降)、ゼロタッチ登録(Android 6.0以降)を使ったGoogle社のデバイスオーナー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。	-	〇	〇
ユーザーによる同期	端末ユーザーにより同期を実施することができます。ユーザーのタイミングで最新の情報を取得・送信することが可能です。	〇	〇	〇
ハードウエア情報の取得	端末のハードウエア状態を確認することができます。	〇	〇	〇
ハードウエ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できます。	〇	〇	〇
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できます。	〇	〇	〇
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できます。	〇	〇	〇
更新プログラムの提供状態表示	各Windows(R)端末において未適用なWindows(R)更新プログラムを取得・表示することができます。	-	-	-
ネットワークマップの取得	アクセスポイントごとに端末一覧を取得することができます。	〇	〇	〇
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。	〇	〇	〇
エージェントアプリケーションのアンインストールパスワード設定	ツールのアンインストール防止用としてパスワードによるアンインストール制限を行うことができます。	〇	〇(注1)	〇(注1)
エージェントアプリケーションログのレポート出力	端末内のエージェントアプリケーションが行った動作ログをCSV形式でレポート出力できます。	〇	〇	〇
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、NASなど)を収集します。	-	-	-
組織管理	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。	〇	〇	〇
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できます。	〇	〇	〇
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。	〇	〇	〇
ホーム画面レイアウト	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。	-	-	-
Zone Management	端末で検知したSSID、スケジュール及び端末の位置情報を用いて、自動的に設定セットを切り替える事ができます。	〇	〇	〇
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できます。	〇	〇	〇
Web閲覧履歴取得・削除	OS標準ブラウザのWeb閲覧履歴の取得・削除を行うことができます。	-	-	-
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。履歴として確認することができます。最大100件まで履歴を表示することが可能です。エクスポート機能により、CSVによるレポート出力を行うことができます。	〇	〇	〇
位置情報取得設定検知	端末上における、GPS機能およびWi-Fiにおける位置取得設定の有効/無効を管理サイト上で検知することができます。	〇	〇	〇
エージェントアプリケーションの位置情報測位ステータス	エージェントアプリケーションの位置情報取得可否を管理サイト上で確認することができます。	〇	〇	〇
SIM情報取得および表示	端末のSIM情報を取得、管理サイトに表示することができます。	〇	〇	〇
かんたん初期設定ウィザード	SMSM導入時の初期設定作業をウィザード形式で進めることが出来ます。認証済み機器が存在しない場合に、トップページに表示されます。	〇	〇	〇

注1) Android7.0以降の場合、デバイスオーナーモードでご利用いただく必要があります。デバイスオーナーモードの場合、エージェントのアンインストールには端末初期化を伴います。

【基本機能】端末管理		従来版（非DOM）	従来版（DOM）	Store版
Apple Push証明書誤登録防止	トピック値の異なるPush証明書登録時にはエラーを表示します。また、登録時に使用したApple IDを登録することで更新時の誤登録を防ぎます。	－	－	－
Device Enrollment Program（Apple提供）登録サービス by KDDI	「Device Enrollment Program（Apple提供）登録サービス by KDDI」の仕組みに対応した端末設定を実施することができます。事前に設定された内容(監視モード強制、MDM構成プロファイル削除不可など)に基づき、端末を設定することが可能です。	－	－	－
Apple School Manager	Appleが提供するApple School Managerと連携し、Apple School Managerサイトに登録された名簿およびクラス情報を取得ことができます。これにより、Shared iPad・Photo ID(画像)指定、クラスルームアプリケーションも利用できます。	－	－	－
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。	－	－	－
Android Enterprise	Google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。	－	－	○
ゼロタッチ登録	Google社が提供するゼロタッチ登録機能に対応します。SMSMのエージェントアプリを強制的にDevice Owner Modeとしてインストールさせることが可能です。この方法でインストールした場合も、Android Enterpriseは利用可能です。	－	－	○
設定情報バックアップ	端末の設定情報を自動・手動にてバックアップすることができます。	－	－	－
設定情報復元	バックアップされた設定情報を元に、端末の設定情報を復元することができます。	－	－	－
【基本機能】セキュリティ管理		従来版（非DOM）	従来版（DOM）	Store版
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。	○	○	○
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できます。	○	○	○
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。	○	○	○
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端末を初期化やデータ削除およびロックする設定を行うことができます。	○(注2)	○(注2)	○(注2)
スクリーンセーバーの設定	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。	－	－	－
位置情報の取得【Android（TM）】	位置情報の測位タイミングを設定することができます。また、定期的もしくは任意のタイミングで取得した位置情報を確認することができます。	○	○	○
位置情報の取得【iOS】	取得した位置情報を確認することができます。また、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。	－	－	－
位置情報の取得【Windows(R)】	取得した位置情報を確認することができます。また、位置情報取得有無を管理サイトより設定することが可能です。	－	－	－
位置情報の取得【Windows(R) 10 Mobile】	取得した位置情報を確認することができます。	－	－	－
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。	○	○	○
無通信時の設定	無通信状態となった場合、オフラインにおいても端末のロックもしくはワイプを実行することができます。	○	○	○
root化、JailBreak検知機能	端末のroot化、JailBreakの状態を検知することができます。	○	○	○
リモートロック	端末を遠隔操作にてロックをかけることができます。リモートロック時に、端末の画面へ表示するメッセージを指定することも可能です。指定期間通信が行われなかった際にロックすることもできます。 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。Android（TM）は警告音のオプションにチェックを入れていただくことで、ロック時アラート音を鳴らすこともできます。	○(注3)	○(注3)	○(注3)
紛失時強制リモートロック/位置情報取得	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。	－	－	－
リモートワイプ(本体内部)	端末を遠隔にて初期化することができます。 またワイプ実行の際に管理者へメールによる通知を行うことができます。	○	○	○

注2) スクリーンロック解除失敗ロック時、ロックされない端末があります。
注3) Android(TM) およびWindows(R) は「KDDI Smart Mobile Safety Manager」独自のロック、Android(TM)(Android 6系以降)およびiOSはスクリーンロックをかけることができます。

【基本機能】セキュリティ管理		従来版（非DOM）	従来版（DOM）	Store版
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できます。	○	○	○
リモートワイプ(管理領域)	iOS5.1.1以降の端末でMDMの管理領域(MDMプロファイル、管理されたアプリケーション)のリモート削除を実施することができます。	－	－	－
アクティベーションロック有効/無効/解除	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。	－	－	－
スクリーンロックパスワード削除/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削除(iOS,auケータイ(4G LTE))/変更(Android ™,auケータイ(4G LTE)) することができます。	○(注4、5)	○(注4、5)	○(注4、5)
発信先制限	機器の発信先を特定の番号のみに指定したり、特定の番号の発信を禁止するように設定することができます。	○	○	○
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』『グローバルHTTPプロキシ』『Webフィルタリング』『Wi-Fi』『ドメイン』『メール』『VPN』『Webクリップ』の項目を作成、閲覧、編集、削除ができます。iOS 10.3までの制御項目にも対応しています。	－	－	－
監視対象モードによる制御機能	『Siri の不適切な単語フィルタを有効にする/アプリケーションによるモバイルデータ使用方法の変更を許可/アカウント設定の変更を許可/"友達を探す"設定の変更を許可/Game Centerの使用を許可/構成プロファイルのインストールを許可/AirDrop を許可/iBooks Store を許可/iBooks Store を許可/iMessage を許可/App の削除を許可/Configurator 以外のホストとのペアリングを許可/制限の構成を許可/"すべてのコンテンツと設定を消去"を許可/Bluetooth設定の変更を許可(iOS 10以降)/Apple Music を許可(iOS 9.3以降)/Appの使用制限(iOS 9.3以降)』の制限項目が拡張されます。	－	－	－
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。	－	－	－
構成プロファイル削除防止	Apple-MDM構成プロファイル以外の構成プロファイルを、削除禁止もしくはパスワード入力必須とすることができます。	－	－	－
セキュリティ設定の強制適用および診断	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、Officeにおけるマクロ実行制御およびInternet Explorer(R)に対する各種設定などセキュリティに関する設定を強制適用することができます。また、左記に加えてウイルス対策ソフトやスパイウエ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。	－	－	－
認証制御設定	事前に登録された端末のみ「KDDI Smart Mobile Safety Manager」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。	○	○	○
Internet Explorer(R)自動更新設定	最新のInternet Explorer(R)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。	－	－	－
OSアップデート管理	iOSでは新たなOSアップデートが表示される時期を、最長90日遅らせる設定が可能です。Windows(R)では、Windows Updateの延期日数や再起動時刻の設定等が可能です。	－	－	－

注4) 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いただくことで解除可能です。
注5) Android 7.0以降の場合、デバイスオーナーモードでご利用いただく必要があります。

【基本機能】セキュリティ管理		従来版（非DOM）	従来版（DOM）	Store版
パスワードリマインダー	「KDDI Smart Mobile Safety Manager」に登録されているユーザー自身によって、パスワードを設定することができます。パスワード紛失時に再設定することも可能です。	○	○	○
アカウントパスワードポリシー	「KDDI Smart Mobile Safety Manager」に登録されているユーザー自身に対して、パスワードポリシー、アカウント凍結条件の設定および解除をすることができます。	○	○	○
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。	－	○(注6)	○
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。	－	○(注6)	○
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。	－	○(注6)	○
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。	－	○(注6)	○
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。	－	○(注6)	○
アカウントの制限	GoogleアカウントやExchangeアカウント等の追加・削除を制限します。	－	○(注6)	○
ユーザーの制限	ユーザーの追加や削除を制限することができます。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。	－	○(注6)	○
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。	－	－	○
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出来ます。	－	－	○
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。	－	－	○
【基本機能】デバイス管理		従来版（非DOM）	従来版（DOM）	Store版
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。	○(注7)	○(注7)	○
パソコン接続時のSDカード利用禁止・許可	パソコンへの接続時、SDカードへの参照の禁止・許可を設定することができます。	－	－	○
USB利用禁止・許可設定・ホワイトリスト設定	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エア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ことができます。Windows Portable Devices (WPD)も禁止可能です。	×	×	×
USB接続禁止設定	USB接続機能の利用の禁止・許可を設定することができます。	○(注8)	○(注8)	○
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。	－	○	○
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(TM)端末を外部ストレージとして使うこと、Android(TM)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。	－	○	○
CD/DVD/ブルーレイ	CD/DVD/ブルーレイのドライブを禁止、もしくは書き込みのみ禁止することができます。また、FDの禁止も可能です。	－	－	－
IEEE1394の利用禁止	IEEE1394の利用の禁止・許可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 (R)利用禁止・許可設定	Bluetooth (R)の利用禁止・許可を設定することができます。	○(注9)	○(注9)	○
NFC利用禁止・許可設定	NFCの利用禁止・許可を設定することができます。	－	－	○
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。	－	○	○
端末暗号化の設定	Android (TM) の場合、端末の暗号化画面を呼び出し、暗号化を促すことができます。 iOSの場合、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。	－	－	－

注6) デバイスオーナーモードでご利用いただく必要があります。
注7) Android(TM) 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(TM) 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(TM) 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。
注8) 対応機種については制限がありますので、対応機種一覧をご確認ください。
注9) 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。

【基本機能】設定管理		従来版（非DOM）	従来版（DOM）	Store版
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できます。	○	○	○
機器カスタム項目の入力・送信	機器カスタム項目を入力・送信できます。	○	○	○
【基本機能】アプリケーション管理/コンテンツ管理		従来版（非DOM）	従来版（DOM）	Store版
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できます。	○	○	○
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できます。 Windows(R) は、デスクトップアプリケーションおよびユニバーサルWindows(R) プラットフォームアプリケーションの、両方に対応するアプリケーション起動禁止が設定できます。iOS 9.3 以上かつ監視対象モードの端末は『制限』プロファイルの『Appの使用制限』で設定することも可能です。	○	○	○
アプリケーション起動禁止(ホワイトリスト)	Windows(R)は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。	－	－	－
ゲームおよびWindows(R) ストアアプリケーションの制限	ゲームおよびWindows(R) ストアのアプリケーションに対して、レーティングレベル、アプリケーションごとの許可/禁止設定が可能です。	－	－	－
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。	－	－	○(注11)
アプリケーション起動禁止（ホワイトリスト）	Windows(R)は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。	－	－	－
個別設定画面の使用禁止	OS標準設定アプリケーション内の『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できます。iOSの場合、App Store、in-houseアプリケーション、カスタムB2Bアプリケーション(Volume Purchase Program対応のみ) に対応しており、iOSに対しては、1つの設定セットの中にin-houseアプリケーション、カスタムB2Bアプリケーション及びAppStoreアプリケーション最大300件、計350件の登録が可能です。Androidに対しては、1つの設定セットの中にオリジナルアプリケーションとPlayストアアプリケーションの合計300件まで登録が可能です。 iOSの場合、in-houseアプリケーションのアプリケーション配信は1アプリケーション当たり50MBまで、1アプリケーション最大3バージョンまで登録が可能で、最大600件まで登録が可能です。また、ポータルサイト経由でのアプリケーション情報配信、iOS5以降の端末で管理されたアプリケーション情報はポップアップ通知が可能です。Android (TM) の場合は、1アプリケーション当たり150MBまで配信することが可能です。iOS7以上かつ監視対象モードの端末で利用している場合、サイレントでアプリケーションのインストールを実施することができます。Android (TM) 端末の場合、5系以降8以下の一部機種において、サイレントインストールすることが可能です。	○(注10)	○(注10)	－
アプリケーション配信 (Volume Purchase Program対応)	Apple社が提供するVolume Purchase Programの仕組みに対応しました。AppStore上のアプリケーション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。組織に対して一括適用することも可能です。	－	－	－
ブック配信 (Volume Purchase Program対応)	Apple社が提供する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。	－	－	－
アプリケーション配信(Android Enterprise対応)	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。	－	－	○
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。	－	－	○
App Configuration	App Configurationに対応したアプリケーションへSMSMから設定値の設定を行うことができます。	－	－	－
アプリケーションアップデート指示	管理サイトより、アプリに対してバージョンアップ指示を出すことができます。			
非管理対象アプリケーションを管理対象アプリケーション化	端末にインストール済の『非管理対象アプリケーション』を管理サイトから『管理対象アプリケーション』として配信すると、管理対象アプリケーション化することが可能です。iOS 9以降対応の機能になります。	－	－	－
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、定期通信など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。			
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。	－	－	－
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。			
指定アプリケーション検知機能	アプリケーション名やバージョン条件などを指定することで、インストール推奨アプリケーション・インストール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。	○	○	○
ソフトウエ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。	－	－	－
ソフトウエアライセンス調整	Microsoft Office製品のライセンス情報のうち、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ができます。	－	－	－
Secure Shield	「KDDI Smart Mobile Safety Manager」が提供する端末設定アプリケーションを利用いただくことで、管理者がユーザーの端末設定可能範囲を制限することができます。	×	×	×
App Manager	エージェントアプリケーションに組み込まれたアプリケーション配信基盤 App Managerにより、エージェントアプリケーション経由で、各種MDM関連アプリケーションをダウンロードすることができます。	○	○	－

注10) サイレントインストール可能端末については、制限がありますので対応機種一覧をご確認ください。また、Google Playストア掲載アプリケーションについては非対応です。
注11) デバイスオーナーモードでご利用いただく必要があります。

【基本機能】インターネット接続管理		従来版（非DOM）	従来版（DOM）	Store版
Webクリップ設定	Webクリップの設定を行うことができます。	–	–	–
Wi-Fi設定	端末の無線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。	–	–	–
Wi-Fi接続制限	構成プロファイルによって設定されたWi-Fiにのみ接続することができます。	–	–	–
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。	–	–	–
Exchange ActiveSync設定	端末とのExchange ActiveSync設定をすることができます。	–	–	–
メール設定	POP/IMAPの設定をすることができます。	–	–	–
メール誤送信防止	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。	–	–	–
Webフィルタリング設定（ホワイトリスト）	Appleが提供している機能で、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。	–	–	–
Webフィルタリング設定（ブラックリスト）	Appleが提供している機能で、アダルトコンテンツおよび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。	–	–	–
お気に入り/ホーム	Internet Explorer(R)に対し、お気に入りへ追加するウェブサイトを配信、およびホームページを設定することができます。	–	–	–
HTTPプロキシ設定	管理サイト上で、HTTPプロキシ設定を作成、閲覧、編集、削除できます。	–	–	–
証明書配布設定	クライアント証明書並びにCA証明書をアップロード、配布することができます。	○	○	○
VPN設定	VPN接続を設定することができます。	–	–	–
アプリケーションVPN設定	アプリケーションごとにVPN接続を確立できます。本設定が適用されたアプリケーションのみ、VPN接続可能です。	–	–	–
プロキシ	手動および自動設定によるプロキシ設定が行えます。	–	–	–
管理サイトログインボタン	Windows(R)エージェントアプリケーションに対して、管理サイトを表示するボタンをツールバー上に表示します。	–	–	–
【追加機能】インターネット接続管理　Android（TM）		従来版（非DOM）	従来版（DOM）	Store版
お気に入り設定	お気に入り設定をOS標準ブラウザや独自ブラウザ(+browser Safety Manager)に設定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）	独自ブラウザ(+browser Safety Manager)に対して、管理サイトに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。	○	○	○
Webフィルタリング設定（ブラックリスト）	独自ブラウザ(+browser Safety Manager)に対して、管理サイトでブラックリストに登録した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、削除	独自ブラウザ(+browser Safety Manager)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の有効・無効や、Wi-Fiネットワークの追加など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。	○	○	○
+browser Safety Manager	「KDDI Smart Mobile Safety Manager」が提供するブラウザを利用いただくことで、標準ブラウザのシークレットモードによる制限を解消します。	○	○	○
【追加機能】インターネット接続管理　iOS		従来版（非DOM）	従来版（DOM）	Store版
お気に入り設定	お気に入り設定を独自ブラウザ(+browser Safety Manager)に設定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）	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。	–	–	–
Webフィルタリング設定（ブラックリスト）	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、削除	独自ブラウザ(+browser Safety Manager)のWeb閲覧履歴の取得、削除を行うことができます。	–	–	–
+browser Safety Manager	「KDDI Smart Mobile Safety Manager」が提供するブラウザを利用いただくことで、標準ブラウザ(Safari)を禁止すると同時に、Webフィルタリング/お気に入り設定を適用することができます。	–	–	–
【追加機能】インターネット接続管理　Windows(R)		従来版（非DOM）	従来版（DOM）	Store版
Webフィルタリング(ホワイトリスト/ブラックリ	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。	–	–	–
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。	–	–	–
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。	–	–	–
【追加機能】Webフィルター　Android（TM）、iOS、auケータイ（4G LTE）		従来版（非DOM）	従来版（DOM）	Store版
Webフィルタリング設定（ホワイトリスト）	独自ブラウザ(+browser Safety Manager)に対して、管理サイトに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。	○	○	○
Webフィルタリング設定（ブラックリスト）	独自ブラウザ(+browser Safety Manager)に対して、管理サイトでブラックリストに登録したURLへのアクセスを禁止することができます。	○	○	○
Webフィルタリング設定（カテゴリ）	独自ブラウザ(+browser Safety Manager)に対して、管理サイトにてフィルタリング対象に登録したカテゴリに含まれるURLへのアクセスを禁止することができます。	○	○	○
【追加機能】バックアップ機能　Android（TM）		従来版（非DOM）	従来版（DOM）	Store版
設定情報バックアップ	端末の設定情報を自動・手動にてバックアップすることができます。	○	○	○
設定情報復元	バックアップされた設定情報を元に、端末の設定情報を復元することができます。	○	○	○
【追加機能】メッセージ配信機能　Android（TM）、iOS、auケータイ（4G LTE）		従来版（非DOM）	従来版（DOM）	Store版
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できます。	○	○	○
通知結果の集計	端末より、通知済のメッセージ閲覧状況を集計することができます。	○	○	○

【追加機能】ステータス管理　auケータイ（4G LTE）		従来版（非DOM）	従来版（DOM）	Store版
ステータス管理	端末利用者のステータス（作業中/訪問中/帰社中等）を、管理サイトで閲覧・管理することができます。初期状態では、作業中/移動中/訪問中/休憩中/帰社中の5種類が設定されており、最大10個まで登録することが可能です。端末上から、他ユーザーのステータスを閲覧することも可能です。	－	－	－
【追加機能】ウイルス対策機能　Android（TM）、auケータイ（4G LTE）		従来版（非DOM）	従来版（DOM）	Store版
Safety Manager AntiVirus	不正なアプリケーションがインストールされた場合に検知して削除を促すエージェントアプリケーションを提供します。管理サイトから、スキャンポリシーを適用させたり対策状況監視や脅威検知ログを確認できます。	○	○	○