KDDI Smart Mobile Safety Manager
基本プラン向け
機能詳細一覧

2017年5月24日現在

KDDI株式会社

And:Android(TM)　Win:Windows(R)　Win10m:Windows(R)10mobile

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【基本機能】端末管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	-	-	-	○(注1)	○	○	○	-	-	-
デバイスオーナー	QRコード(Android (TM) 7.0以降)、NFC(Android (TM) 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。	-	-	-	-	×	○	○	-	-	-
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。	○	○	○	○	○	○(注2)	○(注2)	-	○	-
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。	○	○	○	○	○	○	○	○	○	○
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。	○	○	○	○	○	○	○	○	○	○
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。	○	○	○	○	○	○	-	-	○(注3)	○
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。	○	○	○	○	○	○	○	-	○	○
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。	○(注4)	○	○	○	○	○	○	○	○	○
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。	○	○	○	○	○	○	○	○	○	○
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。	×	○	○	○	○	○	○(注5)	-	○	-
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。	○	○	○	○	○	○	○	-	○	-
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。	○	○	○	○	○	○	○	○	○	○

注1) Android (TM) OS 4.0.3以降に対応しています。
注2) 取得できるMACアドレスがAndroid(TM)の仕様上、すべて特定の固定値になります。
注3) Windows Server(R)では更新プログラムの情報が取得できません。また、Windows(R)10では更新プログラムの情報や自動更新情報が取得できないものがあります。
注4) 3G/4G/Wi-Fi端末を混在して表示します。
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。

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【基本機能】端末管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	○	○	○	○	○	○	○	○	○	○
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。	○	○	○	○	○	○	○	○	○	○
ホーム画面レイアウト	アプリケーションアイコンとフォルダーの位置指定および固定を行うことができます。	○(注6)	-	-	-	-	-	-	-	-	-
Zone Management	端末で検知したSSID、スケジュールおよ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。	×	○	○	○	○	○	○	-	○(注7)	×
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。	○	○	○	○	○	○	○	○	○	○
Web閲覧履歴取得・削除	OS標準ブラウザに対して、Web閲覧履歴の取得・削除を行うことができます。	-	○	○	○(注8)	○(注8)	-	-	-	-	-
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。	○	○	○	○	○	○	○	○	○	-
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。	-	-	-	○	○	○	○	-	-	-
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。	-	-	-	○	○	○	○	-	-	-
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。	○	○	○	○	○	○	○	○	○	-
かんたん初期設定ウィザード	「KDDI Smart Mobile Safety Manager」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できます。	○	○	○	○	○	○	○	○	○	○
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をメモできる備考欄をご利用いただくことも可能です。	○	-	-	-	-	-	-	-	-	-
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。	○(注9)	-	-	-	-	-	-	-	-	-

注6) iOS 9.3以降かつ監視対象モードの端末の場合ご利用いただけます。
注7) Wi-Fiが認識されている状態でのみ有効です。
注8) シークレットモード設定時は利用不可です。
注9) Apple School Managerの利用には、アカウント取得が必要です。詳しくはAppleへお問い合わせください。

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【基本機能】セキュリティ管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	○	○	○	○	○	○	○	×	○(注10)	×
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11)	○(注12)	○(注12)	○(注12)	×	○	×
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。	○(注13)	-	-	-	-	-	-	-	-	-
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。	-	-	-	-	-	-	-	-	○(注14)	-
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。	○(注15)	○	○	○	○	○	○	○	×	×
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。	○(注13、16)	○	○	○	○	○	○	-	-	-

注10) ドメイン参加端末に対するパスワードポリシーの設定には非対応です。
注11) スクリーンロック解除失敗時の「KDDI Smart Mobile Safety Manager」のロック画面表示機能はAndroid(TM) 4系以降の端末が対象です。
注12) 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13) 機能の利用にはエージェントアプリケーションのインストールが必要です。また、iOS 8以降ではエージェントアプリケーションがApp Switcherにあることが前提です。
注14) Windows(R) 8.1 以上の端末に対応した機能です。
注15) iOS 8以上に対応しています。
注16) iOS 9以降の端末で『低電力モード』に設定されている場合、OS仕様上、情報更新のためにはエージェントアプリケーションをフォアグラウンドで起動する必要があります。

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【基本機能】セキュリティ管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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、ロック時にアラート音を鳴らすこともできます。	○(注17)	○(注17)	○(注17)	○(注17)	○(注17)	○(注17)	○(注17)	○(注18)	○(注17)	○(注19)
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。	○(注6)	-	-	-	-	-	-	-	-	-
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。 またワイプ実行前に管理者へメールによる通知を行うことができます。	○	○	○	○	○	○	○	○	○(注20、21)	○(注22)
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)	リモートで端末から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)の削除を実施することができます。	○(注23)	-	-	-	-	-	-	×	-	×
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・無効化およ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 ・パスワードを知らない第三者による再利用を防ぎます。	○(注24)	-	-	-	-	-	-	-	-	-
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)/変更(Android (TM))することができます。	○	×	×	○	○(注25)	○(注25)	○(注5、25)	-	-	-
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 8～10の制御項目にも対応しています。	○	-	-	-	-	-	-	-	-	-

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。
注6) iOS 9.3以降かつ監視対象モードの端末の場合ご利用いただけます。
注17) Android(TM) およびWindows(R) は「KDDI Smart Mobile Safety Manager」独自のロック、iOSはスクリーンロックをかけることができます。
注18) ロック時、設定済のPINが解除され、ランダム生成されたPINが新たに設定されます。生成されたPINは管理サイト上のログから確認可能です。
注19) ロックメッセージ指定に対応していません。ロック解除時には、管理サイトで指定された6けたの数字を入力します。
注20) 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。
TPM搭載のスレート型パソコンにおいては、 Windows(R)の仕様によりBitLocker方式によるリモートワイプ実施後初期化を行っていただく必要があります。
また、データ削除方式にも対応します。データ削除方式は実行後、OSを起動することはできません。また、スリープ状態の場合、ワイプできない場合があります。
注21) TPM搭載のスレート型パソコンにおいては、BitLocker方式によるリモートワイプ実施後の回復パスワード入力後に『システムの復元』画面が表示されます。
復元後も同様のフローが実行されます。
注22) 端末を初期化します。ワイプ中、ワイプ完了後には、ロック画面が表示されます。リモートロックのロック画面と同じ画面となります。
注23) 削除防止設定がされている構成プロファイルは削除されません。
注24) iOS 8以上かつ監視対象モードの端末の場合ご利用いただけます。
注25) 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。

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【基本機能】セキュリティ管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	○(注24)	-	-	-	-	-	-	-	-	-
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。	○(注15)	-	-	-	-	-	-	-	-	○
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。	○(注15)	-	-	-	-	-	-	-	-	×
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。	-	-	-	-	-	-	-	-	○(注26、27)	-
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 よう設定することができます。	-	-	-	-	-	-	-	-	○	-
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。	○	○	○	○	○	○	○	○	○	○
【基本機能】設定管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	○(注28)	○	○	○	○	○	○	-	×	-
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。	○	○	○	○	○	○	○	○	○	-

注15) iOS 8以上に対応しています。
注24) iOS 8以上かつ監視対象モードの端末の場合ご利用いただけます。
注26) Windows Server(R)では、ウイルス対策ソフト・スパイウエア対策ソフト・ファイアウォールの状況は取得できません。
注27) Windows Server(R)では、以下の診断項目について設定をした場合、非対応というログおよびアラートが発生する場合があります：
　　ファイアウォールが無効な場合、Windows(R)ファイアウォールを有効化する
　　ウイルス対策ソフト
　　スパイウエア対策ソフト
注28) 構成プロファイルにCardDAVを設定して配信することが可能です。CardDAVに関しては別途ご用意いただく必要があります。

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【基本機能】デバイス管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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29)	○(注29)	○(注29)	○(注29)	×	×	×
パソコン接続時のSDカード利用禁止・許可設定	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。	-	×	×	×	×	×	×	-	○(注30)	×
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31)	○(注31)	○(注31)	○	-	-
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。	-	○	○	○	○	○	○	○	×	×
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。	-	-	-	-	-	-	-	○	-	-
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。	○	-	○(注32)	○	○	○	○	×	×	×
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33、34)	-

注29) 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30) 大容量ストレージのみ、または、すべてのUSBデバイスを対象に禁止することができます。
注31) 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32) Android(TM) 3.1以降に対応しています。
注33) デフラグ自動実行設定はWindows Vista(R) 以上が対象です。
注34) Windows Server(R) では以下の機能は対象外となります：
CPU温度診断
ハードディスク異常診断
システムドライブの復元有効化

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【基本機能】アプリケーション管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	○(注6)	○	○	○	○	○	○	×	×	×
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。	○(注35、36)	○	○	○	○	○	○	×	○	×
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。	-	-	-	-	-	-	-	×	○(注37)	-
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。	-	-	-	-	-	-	-	×	○(注37)	-
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。	-	○(注38)	-	-	-	-	-	-	-	-
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アプリケーション最大50件、カスタムB2Bアプリケーションおよび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まで配信が可能です。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。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、iOS 8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。iOS 8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39)	○(注39)	○(注39)	×	×	×
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。	○(注40)	-	-	-	-	-	-	-	-	×

注6) iOS 9.3以降かつ監視対象モードの端末の場合ご利用いただけます。
注35) Safari,iTunes Store, Podcastの禁止が可能です。PodcastはiOS 8以上かつ監視対象モードの端末で有効です。
注36) 『設定』および『電話』はiOSの仕様上、禁止することができません。
注37) MS-MDM認証された機種にのみ対応します。Windows(R) 10ではMS-MDMに未対応です。
注38) Android(TM) 2.2,2.3に対応しています。Android(TM) 4.0以上は独自の設定アプリケーション(Secure Shield)を利用して禁止が可能です。
注39) 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40) 機器に対するVPPライセンス付与は iOS 9以降に対応した機能です。

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【基本機能】アプリケーション管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
アプリケーションアップデート指示	管理サイトより、アプリケーションに対してバージョンアップ指示を出すことができます。	○(注41)	○	○	○	○	○	○	×	-	×
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。	○(注42)	○	○	○	○	○	○	-	×	×
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。	○	○(注43)	○(注43)	○(注43)	○(注43)	○(注43)	○(注43)	×	×	-
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。	-	×	○(注44)	○(注44)	○(注44)	○(注44)	○(注44)	-	-	-
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41) iOSにおいては、管理対象として配布されたアプリケーションにのみアップデート指示が可能です。
注42) 監視対象モードの端末かつVPPアプリケーションではサイレントでインストールされるため、ポップアップは表示されません。
注43) Android(TM) 2.xの場合、設定画面の『開発』も開けなくなります。
　　Android(TM) 3.x以降の場合、設定画面も開けなくなります。
注44) 対応端末は限定されています。また、端末により設定可能な項目が異なります。

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【基本機能】インターネット接続管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	○	-	-	-	-	-	-	×	-	×
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。	○(注15)	-	-	-	-	-	-	×	-	-
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。	○(注45)	-	-	-	-	-	-	-	-	-
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。	○(注24)	-	-	-	-	-	-	×	-	×
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。	○(注24)	-	-	-	-	-	-	-	-	×
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。	-	-	-	-	-	-	-	×	○	-

注15) iOS 8以上に対応しています。
注24) iOS 8以上かつ監視対象モードの端末の場合ご利用いただけます。
注45) iOS 8以降に対応した機能となります。

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【基本機能】インターネット接続管理		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	○(注24)	-	-	-	-	-	-	-	-	×
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。	○(注24)	-	-	-	-	-	-	×	○(注46)	×
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)		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	-	○	○	○	○(注47)	○(注48)	○(注48)	-	-	-
Webフィルタリング設定(ホワイトリスト)	OS標準ブラウザや独自ブラウザ(+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。	-	○	○	○(注8)	○(注8)	○(注48)	○(注48)	-	-	-
Webフィルタリング設定(ブラックリスト)	OS標準ブラウザや独自ブラウザ(+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。	-	○	○	○(注8)	○(注8)	○(注48)	○(注48)	-	-	-

注8) シークレットモード設定時は利用不可です。
注24) iOS 8以上かつ監視対象モードの端末の場合ご利用いただけます。
注46) Windows Server(R)ではマルチログインの環境下において以下の制限があります。
　　同期状態の確認がない場合があります。
　　プロキシ設定下における同期では、ログオンしているユーザーに設定が反映されない場合があります。
　　プロキシ設定下の同期後の認証リクエストが表示されない場合があります。
注47) 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。
注48) +browser Safety Managerにのみ適用されます。標準ブラウザには対応していません。

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【追加機能】インターネット接続管理　Android (TM)		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
Web閲覧履歴取得、削除	OS標準ブラウザや独自ブラウザ(+browser Safety Manager)のWeb閲覧履歴の取得、削除を行うことができます。	-	○	○	○(注8)	○(注8)	○(注48)	○(注48)	-	-	-
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		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	○	-	-	-	-	-	-	-	-	-

注8) シークレットモード設定時は利用不可です。
注48) +browser Safety Managerにのみ適用されます。標準ブラウザには対応していません。

『○』…機能有 / 『×』…機能なし / 『-』…非対応

【追加機能】インターネット接続管理　Windows(R)		iOS	And 2系	And 3系	And 4系	And 5系	And 6系	And 7系	Win 10m	Win	Mac
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。	-	-	-	-	-	-	-	-	○(注37、49)	×
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。	-	-	-	-	-	-	-	-	○	-
【追加機能】Webフィルター　Android (TM) 、iOS		**iOS**	**And 2系**	**And 3系**	**And 4系**	**And 5系**	**And 6系**	**And 7系**	**Win 10m**	**Win**	**Mac**
Webフィルタリング設定(ホワイトリスト)	OS標準ブラウザや独自ブラウザ(+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。	○(注48)	○	○	○(注8)	○(注8)	○(注48)	○(注48)	-	-	-
Webフィルタリング設定(ブラックリスト)	OS標準ブラウザや独自ブラウザ(+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。	○(注48)	○	○	○(注8)	○(注8)	○(注48)	○(注48)	-	-	-
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。	○(注48)	○(注48)	○(注48)	○(注48)	○(注48)	○(注48)	○(注48)	-	-	-
【追加機能】バックアップ　Android (TM)		**iOS**	**And 2系**	**And 3系**	**And 4系**	**And 5系**	**And 6系**	**And 7系**	**Win 10m**	**Win**	**Mac**
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】メッセージ通知　Android (TM) 、iOS		**iOS**	**And 2系**	**And 3系**	**And 4系**	**And 5系**	**And 6系**	**And 7系**	**Win 10m**	**Win**	**Mac**
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。	○(注13、16)	○	○	○	○	○	○	-	-	-
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。	○(注13、16)	○	○	○	○	○	○	-	-	-
【追加機能】ウイルス対策　Android (TM)		**iOS**	**And 2系**	**And 3系**	**And 4系**	**And 5系**	**And 6系**	**And 7系**	**Win 10m**	**Win**	**Mac**
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。	-	○	○	○	○	○	○	-	-	-

注8) シークレットモード設定時は利用不可です。
注13) 機能の利用にはエージェントアプリケーションのインストールが必要です。また、iOS 8以降ではエージェントアプリケーションがApp Switcherにあることが前提です。
注16) iOS 9以降の端末で『低電力モード』に設定されている場合、OS仕様上、情報更新のためにはエージェントアプリケーションをフォアグラウンドで起動する必要があります。
注37) MS-MDM認証された機種にのみ対応します。Windows(R) 10ではMS-MDMに未対応です。
注48) +browser Safety Managerにのみ適用されます。標準ブラウザには対応していません。
注49) 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。