SMSM v9.18.0 機能一覧表

『〇』…機能有 /『×』…機能なし /『-』…OS非対応・技術的不可
※Ver9.17.0対応版の機能一覧となります。
※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」
※4G LTEケータイ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。
「WEBフィルター」「メッセージ通知」「ステータス管理」「ウイルス対策」

更新日　2024/1/11

【基本機能】端末管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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	-	-	-
Device Owner Mode	QRコード(Android(TM) 7.0以降)、NFC(Android(TM) 6.0以降)、afw識別子(Android(TM) 6.0以降)、G SuiteGoogle Workspaceアカウント(Android(TM) 6.0以降)、ゼロタッチ登録(Android(TM) 6.0以降)、Knox Mobile Enrollment(Samsung端末Knox対応端末)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。	-	〇(注1,6)	-	-	-
エージェント移行	従来版エージェントから、ストア版エージェントへDevice Owner権限を移行することができます。	-	〇(注65)	-	-	-
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(注2)	〇	-	〇
エージェント自動認証機能	エージェントをApp Configuration対応し、認証に必要な情報を管理サイトから配信と同時に送信することによって、手動認証を不必要にすることができます。	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	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	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(注51)	〇(注3)	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	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。	-	-	〇	-	-
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(注4)	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	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(注47)	〇	-	〇
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	-	-
管理外機器の検出	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。	-	-	〇	-	-
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	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	〇	-

注1) QRコードキッティングはWi-Fi接続時のみ行えます。
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)10/11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/5G/Wi-Fi端末を混在して表示します。
注6) Android 12 以降、afw/Google Workspace及びG Suiteキッティングは Wi-Fi接続時のみ行えます。
注47) 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。
注65)2023年2月20日に従来版エージェントの提供が終了いたします。従来版アプリをご利用のお客様は、新エージェント（「ストア版エージェント」）への移行をお願いいたします。

【基本機能】端末管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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。	○（注48）	–	–	–	–
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ことができます。	×	○	○	×	–
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。	○	○	○	–	○
位置情報取得設定検知	端末における、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。	–	○	–	–	○
位置情報取得 許可/不許可表示	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。1端末で5つまでSIM情報を表示することができます。	○	○	○	–	–
管理サイト上機器名の端末反映	管理サイト上に設定されている機器名を、端末に反映させることができます。	○(注23)	–	–	–	–
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できます。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。	○	○	○	○	–
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。	○	–	–	–	–
Apple Business Manager(Apple 提供) 登録サービス by KDDI	「Apple Business Manager(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することができます。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7)	–	–	–	–
Apple Business Manager	Apple Business Managerと連携し、iOS/iPadOS端末の各種設定や、購入したアプリケーション・書籍の配信を行うことができます。	○	–	–	–	–
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。	–	○	–	–	–
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。エージェントアプリケーションを強制的に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。	–	○(注55)	–	–	–
Knox Mobile Enrollment	Samsung社が提供するKnox Mobile Enrollment機能に対応します。Samsung端末においても、エージェントアプリケーションを強制的に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。	–	○(注59)	–	–	–
電話番号取得および表示	端末の電話番号情報を取得し、管理サイトに表示することができます。	–	–	–	–	○

注7) 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。
注23) 監視対象モードの端末の場合ご利用いただけます。
注48) 監視対象モードの端末の場合ご利用いただけます。
注55) ゼロタッチ登録に対応した端末を、専用の手続で購入する必要があります。詳しくはお問い合わせ下さい。
注59) Knox Mobile Enrollmentに対応した端末を、専用の手続きで購入する必要があります。詳しくはお問い合わせください。

【基本機能】セキュリティ管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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8)	×	○
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10)	○	×	○
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/iPadOS】	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11)	–	–	–	–
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。	–	–	○	–	–
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。	○(注11、14)	○	–	–	–
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15)	○(注15)	○(注15)	○(注17)	○(注1)
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(紛失モード)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48)	–	–	–	–
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18、19)	○(注20)	○
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)	iOS/iPadOS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。	○(注21)	–	–	×	–
リモートシャットダウン	管理サイトから端末のシャットダウン操作を行うことができます。複数台の端末の一括シャットダウンも可能です。	○	–	–	–	–
リモート再起動	管理サイトから端末の再起動操作を行うことができます。複数台の端末の一括再起動も可能です。	○	–	–	–	–
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。	○(注23)	–	–	–	–

注8) 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10) 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11) 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。
注14) 『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15) 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。
注17) 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18) 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19) 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20) 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21) 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23) 監視対象モードの端末の場合ご利用いただけます。
注48) 監視対象モードの端末の場合ご利用いただけます。

4G LTEケータイプラン
注1) 「KDDI Smart Mobile Safety Manager」独自のロック画面を表示させます。

【基本機能】セキュリティ管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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/iPadOS)・変更(Android (TM))することができます。	○	○(注22、47)	－	－	－
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。	－	×	－	－	－
構成プロファイル画面上設定	管理サイト上で、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』『モバイル通信』の項目を作成、閲覧、編集、削除ができます。	○	－	－	－	－
監視対象モードによる制御機能	『FaceTime を許可・"クラスルーム"にプロンプトなしでの AirPlay と"画面を表示"の実行を許可・AirDrop を許可・iMessage を許可・Apple Music を許可・ラジオを許可・Siri の不適切な単語フィルタを有効にする・Siri でのユーザ生成コンテンツを許可・Apple Books を許可・App のインストールを許可・App Store からの App のインストールを許可・App の自動ダウンロードを許可・App の削除を許可・システム App の削除を許可・App Clip を許可・iCloud 書類とデータを許可・"ファイル" App で USB ドライブへのアクセスを許可・"ファイル" App でネットワークドライブへのアクセスを許可・"すべてのコンテンツと設定を消去"を許可・構成プロファイルのインストールを許可・VPN 構成の追加を許可・日付と時刻を強制的に自動設定・"クラスルーム"にプロンプトなしでの App の制限とデバイスのロックを許可・"クラスルーム"のクラスにプロンプトなしで自動的に参加・"クラスルーム"の管理対象外クラスを退席するときに教師の許可を要求・アカウント設定の変更を許可・Wi-Fi の電源を強制的にオン・Bluetooth 設定の変更を許可・モバイルデータ通信 App 設定の変更を許可・モバイルデータ通信プラン設定の変更を許可・eSIM 設定の変更を許可・デバイス名の変更を許可・通知設定の変更を許可・パスコードの変更を許可・Touch ID の指紋または Face ID の顔の変更を許可・スクリーンタイムを許可・壁紙の変更を許可・インターネット共有設定の変更を許可・"友達を探す"を許可・"探す"の"デバイスを探す"を許可・"友達を探す"設定の変更を許可・デバイスのロック中も USB アクセサリを許可・Configurator 以外のホストとのペアリングを許可・ペアリングが解除されたデバイスのリカバリモードへの移行を許可・診断設定の変更を許可・パスワードの自動入力を許可・自動入力の前にTouch ID/Face ID認証を要求・Apple Watch とのペアリングを許可・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・近くのデバイスの新規設定を許可・近接通信に基づくパスワード共有要求を許可・パスワードの共有を許可・AirPrint を許可・iBeacon を使った AirPrint プリンタの検出を許可・キーチェーンへの AirPrint 資格情報の保存を許可・証明書が信頼されていない出力先への AirPrint を禁止・予測表示キーボードを許可・キーボードショートカットを許可・なぞり入力キーボードを許可・自動修正を許可・スペルチェックを許可・定義を許可・音声入力を許可・ソフトウェア・アップデートの遅延・"ニュース"の使用を許可・Podcast の使用を許可・Game Center を許可・マルチプレイヤーゲームを許可・App の使用を制限』の制限項目が拡張されます。	○(注23)	－	－	－	－
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。	－	－	○(注62)	－	－
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。	－	－	○	－	－
OSアップデート管理	iOS/iPadOS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。Android(TM)では時間による強制アップデート設定や、アップデートを促す通知の送信などが行えます。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56)	○	○(注57)		－

注22) 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23) 監視対象モードの端末の場合ご利用いただけます。

注47) 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56) 監視対象モードの端末の場合ご利用頂けます。

注57) Windows(R) 10 およびWindows 11でのみ動作します。 Windows(R) 10/11 Homeの場合はアクティブ時間のみ設定可能です。

注62) Windows(R) 11では以下の機能が非対応です。

- 「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」

Windows(R) 10では以下の機能が非対応です。

- 「ブラウザー(Internet Explorer)」
- 「信頼済みサイト一覧」

【基本機能】セキュリティ管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
OSアップデート指示・情報取得	iOS/iPadOSにおいて、OSアップデート指示を出すことができます。端末ごとに、取得可能なアップデートを機器情報として確認することも可能です。	○(注60)	–	–	–	–
SIMカード変更検出機能	認証に用いたSIMカードが抜かれたり別のSIMカードへ切り替わったことを検出することができます。不正にSIMカードを入れ替えて情報漏洩されることを防いだり事象を検知して早急に対応を進めることが可能です。	○	○	–	–	–
SIM抜き差し監視機能	企業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。私物のSIM挿入による不正な通信が行われることを防ぎ、厳格な端末管理を行うことが可能です。	–	–	○	–	–
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。	○	○	○	○	–
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。	–	○	–	–	–
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。	–	○	–	–	–
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。	–	○	–	–	–
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23)	○	–	–	–
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。	–	○	–	–	–
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23)	○	–	–	–
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。	–	○	–	–	–
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。	○	○	–	–	–
スクリーンロック画面時の機能制限	スクリーンロック画面時における、すべての通知、カメラ機能、業務領域内アプリの通知、信頼できるエージェント、指紋によるロック解除を一部もしくは全て制限することが出来ます。	–	○	–	–	–
ファクトリーリセット保護設定	指定したデバイスのファクトリーリセット保護を有効または無効に設定できます。	–	○	–	–	–
Windows 情報保護	Windowsに備わっている「Windows 情報保護」機能をSMSM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できます。	–	–	○(注61)	–	–
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できます。	–	–	–	–	○
ユーザーポータル	端末所持者が自分で端末のロック / ワイプ(初期化) や位置情報確認を行うことができます。	–	–	–	–	○
発信先制限	共有アドレス帳に登録されている電話番号のみ、発信する制限を実施することができます。	–	–	–	–	○
【基本機能】設定管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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26)	○	×	–	○
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。	○	○	○	–	–
ビジネス便利パックからのアドレス帳取り込み	専用ツールもしくは管理サイトへビジネス便利パックのアドレス帳をアップロードすることにより、ビジネス便利パックのアドレス帳取り込みを簡易化します。	–	–	–	–	○
共有アドレス帳管理・配信	業務用の連絡先を管理サイト上で管理し、端末に配信することができます。	–	–	–	–	○

注23) 監視対象モードの端末の場合ご利用いただけます。

注26) 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。

注60) 監視対象モードの端末の場合ご利用頂けます。

注61) Windows(R) 10 Pro/Enterprise/ EducationおよびWindows(R) 11 Pro/Enterprise/Educationの 32 ビット版と 64 ビット版に対応しています。

【基本機能】デバイス管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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27)	×	×	○(注2)
USB利用禁止・許可設定・セーフリスト設定	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28)	×	−
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29)	−	−	○
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54)	×	×	−
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/iPadOS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31、32)	−	−
Direct Boot モード中の機能制限一部解除	Direct Boot モード中であっても、リモートワイプを実行することができます。	−	○	−	−	−
【基本機能】アプリケーション管理・コンテンツ管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
アプリケーション起動禁止 (セーフリスト)	セーフ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48)	○	×	×	−
アプリケーション起動禁止 (ブロックリスト)	ブロ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。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33、49)	○	○	×	○
アプリケーション起動禁止(セーフリスト)	Windows(R)はセーフ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 (ブロックリスト)	ブロ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。	−	○	−	−	−
アプリケーション起動禁止 (セーフリスト)	Windows(R)はセーフ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58)	−	−
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/iPadOS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(Appとブック対応のみ) に対応しており、iOS/iPadOS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、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。 iOS/iPadOS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150MB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、iOS/iPadOS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。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。	○	○(注36)	×	×	−

注27) Android(TM) OSの仕様上、SDカード禁止に非対応のため SDカード挿入検知時、専用のロック画面を表示します。
注28) 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29) 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31) デフラグ自動実行設定はWindows Vista(R) 以上が対象です。
注32) 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
注33) Safari,iTunes Store, Podcastの禁止が可能です。Podcastは監視対象モードの端末で有効です。
注36) Android Enterprise利用可能な端末である必要があります。
注48) 監視対象モードの端末の場合ご利用いただけます。
注49) 『設定』及び『電話』は仕様上禁止することが出来ません。
注54) 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。
注58) Windows(R) 10/11 Enterprise及びEducationでのみ動作します。

4G LTEケータイプラン
注2)SDカード挿入検知時、専用のロック画面を表示します。

【基本機能】アプリケーション管理・コンテンツ管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
アプリケーション配信（Appとブック対応）	Apple社が提供するAppとブック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（Appとブック対応）	Apple社が提供するAppとブック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。	○	－	－	－	－
アプリカタログ	自社用のアプリストアを作成できます。管理者はアプリケーションをまとめた『カタログ』を作成して、配信対象を設定します。利用者はオンデマンド形式でアプリをインストールすることが可能です。アプリカタログからインストールしたアプリを自動アップデートすることもできます。	○	－	－	－	－
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。	－	○(注53)	－	－	－
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。	－	○(注53)	－	－	－
App Configuration	App Configurationに対応したアプリケーションへ「KDDI Smart Mobile Safety Manager」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38)	○(注36)	－	×	－
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。	○	－	－	－	－
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39)	－	×	×	－
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40)	×	－	－
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41)	－	－	－
業務専用端末化設定	Optimal Bizの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。	◎	－	－	－	－
【基本機能】インターネット接続管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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や802.1X認証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。	○(注50)	－	－	－	－
Wi-Fi無効・有効設定	Wi-Fiの無効・有効を設定することができます。	－	－	－	－	○（注3）
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（マーク）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（セーフリスト）	Appleが提供している機能で、セーフ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23)	－	－	×	－
Webフィルタリング設定（ブロックリスト）	Appleが提供している機能で、アダルトコンテンツおよびブロ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23)	－	－	×	－
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63、64)	－	－

注36) Android Enterprise利用可能な端末である必要があります。
注38) iOSにおいては、管理対象として配布されたアプリにのみアップデート指示が可能です。
注39) 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40) Android(TM) OS標準の設定画面も開けなくなります。
注41) 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。
注43) 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50) 監視対象モードの端末の場合ご利用頂けます。
注53) Android Enterpriseでご利用いただく必要があります。
注63) Windows(R) 11では非対応です。
注64) Microsoft Edgeには非対応です。Windows(R) 10では、Internet Explorer(R)のサポート終了に伴い本機能はサポート範囲外となります。

4 GTEケータイプラン
注3)端末側から設定を変更できます。

【追加機能】インターネット接続管理　Android (TM)		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
グローバルHTTPプロキシ設定	管理サイト上で、グローバルHTTPプロキシ設定を作成、閲覧、編集、削除できます。	○(注23)	－	－	×	－
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23)	－	○	×	－
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。	－	－	○	－	－
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 (セーフリスト)	独自ブラウザ(+browser Safety Manager)に対して、管理サイトにてセーフ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 (ブロックリスト)	独自ブラウザ(+browser Safety Manager)に対して、管理サイトでブロ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や802.1X認証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。	－	○	－	－	－
Webフィルター	URLフィルターとカテゴリフィルターをセットで利用できます。 URLフィルターはホワイトセーフリスト、ブラックブロックリスト方式で指定したサイトへのアクセスを許可、もしくは禁止することができます。 また、CSVファイル読み込みによる一括URLインポートも可能です。 カテゴリフィルターはアルプス システム インテグレーション株式会社が提供するURLデータベースのうち、特定のカテゴリに属するサイトへのアクセスを制限します。	－	－	－	－	○
【追加機能】インターネット接続管理　iOS/iPadOS		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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 (セーフリスト)	セーフ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 (ブロックリスト)	ブロ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)		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
Webフィルタリング(セーフリスト・ブロックリスト)	セーフリスト、ブロ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/iPadOS		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
Webフィルタリング設定 (セーフリスト)	独自ブラウザ(+browser Safety Manager)に対して、管理サイトにてセーフ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 (ブロックリスト)	独自ブラウザ(+browser Safety Manager)に対して、管理サイトでブロ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。	○	○	－	－	－

注23) 監視対象モードの端末の場合ご利用いただけます。

【追加機能】バックアップ機能　Android（TM）		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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。	－	○	－	－	－
アドレス帳バックアップ	アドレス帳のバックアップを行います。	－	－	－	－	○
アドレス帳復元	バックアップされたアドレス情報を復元します。	－	－	－	－	○
【追加機能】ステータス管理		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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】メッセージ配信機能　Android（TM）、iOS/iPadOS		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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11、14)	○	－	－	○
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11、14)	○	－	－	－
【追加機能】ウイルス対策機能　Android（TM）		iOS/iPadOS	Android	Win	Mac	4G LTE ケータイ
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4)

注11) 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。

注14) 『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。

4G LTEケータイ

注4)TMMSの「サブメニュー」→「バージョン情報」をタップしたときに表示される、バージョン情報のダイアログは画面スクロールができないため、低解像度のFP端末（KYF37、KYF39）ではダイアログ下部の情報(サードパーティのライセンス情報)を選択し表示することができません。