機能一覧

掲載している情報は、2024年2月19日現在のものです。

（※L：Light版サービス 対応機能）

機能項目名	説明	OS種別		
		Android	iOS	Windows
コマンド	選択した端末に対してコマンドを発行します。コマンドは1度実行されます。 通信環境によりコマンドが届かない場合は、90日間サーバで保持されます。			
リモートロック	端末の画面ロックを行います。 ・Android ランダムなパスワードもしくは端末で設定済みのパスワードでロックが行われます。 管理サーバからロック解除の制御コマンドを出すか、解除用パスワードをロック画面で入力することによりロックを解除します。 ・iOS 端末で設定済みのパスコードでロックが行われます。管理サーバからロック解除の制御コマンドを出すか、解除用パスワードをロック画面で入力することによりロックを解除します。 ・Windows Windows標準機能の「コンピュータのロック」が強制的に行われます。ログオンユーザのパスワードをロック画面で入力することによりロックを解除します。	○ （※L）	○ （※L）	○ （※L）
リモートロック解除	リモートロックの解除を行います。パスコードはクリアされます。 ・Android ロック解除時のパスコードを指定することができます。	○ （※L）	○ （※L）	–
リモートワイプ	端末内の情報を消去します。 ・Android 管理サーバからの制御コマンドによって、端末を初期化します。初期化方法は端末内の初期化機能と同等となります。 端末に挿入されているSDカードに格納されているデータも削除します。 ・iOS 管理サーバからの制御コマンドによって、端末を初期化します。初期化方法は端末内の初期化機能と同等となります。 ・Windows 管理サーバからの制御コマンドによって、ポリシーで定義された消去方法で、HDD内のデータを消去します。	○ （※L）	○ （※L）	○ （※L）
位置情報取得	管理サーバに端末の位置情報を収集し、端末の場所を確認できます。 端末にて位置情報の取得設定が有効である必要があります。	○ （※L）	○ [3]	○ （※L）
端末情報取得	端末情報取得コマンドを実行し、情報の最新化を行います。	○ （※L）	○ （※L）	○ （※L）
端末ログ取得	ViRobot(ウィルス対策ソフト)のログ収集を実行し、情報の最新化を行います。	○ （※L）	–	–
紛失モード設定	iOS端末を紛失モードに設定します。紛失モード解除以外ではロックを解除できない状態となります。 「iPhoneを探す」(Find iPhone)とは別の設定になります。	–	○ [4] （※L）	–
紛失モード解除	紛失モードを解除します。	–	○ [4] （※L）	–
位置情報取得（紛失モード時）	iOS端末が紛失モードに設定されているとき、位置情報の取得を実施できます。	–	○ [4] （※L）	–
アプリケーション配布	アプリケーションの配布を行います。	○	○	○ [20]
アプリケーション削除	アプリケーションの削除を行います。	○	○	○ [21]
プロビジョニングプロファイル配布	iOSのプロビジョニングプロファイルの配布を行います。	–	○	–
プロファイルロック	ビジネス用プロファイルのロックを行います。 プロファイルはランダムなパスワードでロックが行われます。 管理サーバからプロファイルロック解除の制御コマンドを出すか、解除用パスワードをロック画面で入力することによりロックを解除します。 Android 7.0以降で利用できます。	○ [9] （※L）	–	–
プロファイルロック解除	プロファイルロックを解除します。	○ [9] （※L）	–	–
プロファイルワイプ	ビジネス用プロファイル全体を削除します。	○ [1] （※L）	–	–
[iOSクライアントアプリ]起動指示	iOSクライアントアプリを利用している端末に、アプリの起動を促すメッセージ通知を送信します。	–	○ [3]	–
[ViRobot]パターンファイルの更新	ViRobotのパターンファイルの更新指示を行います。	○ （※L）	–	–
[ViRobot]セキュリティスキャン	ViRobotのセキュリティスキャンの実行指示を行います。	○ （※L）	–	–
詳細調査ログ収集	端末から詳細調査ログの取得を行います。 詳細調査ログは、アプリ内部の調査に用いるため、サービス管理者またはシステム管理者に送信されます。	○ （※L）	–	–
ポリシーの再適用	ポリシーの再適用を実施します。	○ （※L）	○ （※L）	–

（※L：Light版サービス 対応機能）

機能項目名	説明	OS種別		
		Android	iOS	Windows
ポリシー	設定内容をあらかじめポリシーとして作成し、端末またはグループに紐付け(リンク)を行います。 端末はポリシーの設定内容に従い制御されます。			
ローカルロック設定(端末用)	強制的に端末の画面ロック設定を行います。	○ [13] (※L)	–	–
ローカルロック設定	・Android 強制的に端末の画面ロック設定を行います。 ビジネス用プロファイルの場合は、強制的にプロファイルのロック設定を行います。 ・iOS 強制的に端末の画面ロック設定を行います。 ・Windows 端末のスクリーンセーバー起動開始時間を設定します。	○ (※L)	○ (※L)	○ (※L)
ポリシー設定遵守	ローカルロック設定違反時に、仕事用アプリを無効化します。	○ [19] (※L)	–	–
ローカルワイプ設定(端末用)	画面ロックを連続で間違えた場合に、ビジネス用プロファイルを初期化します。	○ [13] (※L)	–	–
ローカルワイプ設定	・Android 画面ロックを連続で間違えた場合に、端末を初期化します。 プロファイルのロックを連続で間違えた場合に、ビジネス用プロファイルを初期化します。 ・iOS 画面ロックを連続で間違えた場合に、端末を初期化します。 ・Windows 管理サーバとの通信が一定期間行われない場合に、自動的に端末のデータ消去を行います。	○ (※L)	○ (※L)	○ (※L)
SIM差し替えロック	許可されたSIM以外が挿入されている場合に、画面をロックします。 ビジネス用プロファイルとして登録された端末では利用できません。	○	–	–
カメラ抑止	カメラの利用を制限します。	○	○	○
スクリーンキャプチャー抑止	スクリーンキャプチャーの取得を制限します。	○	○	–
無線LAN制限	無線LANデバイスを無効化、または許可されたアクセスポイント以外への接続を制限します。	○	○ [22]	○
Bluetooth抑止	Bluetoothの利用を制限します。	○	○ [23]	○
Bluetoothデバイス検知抑止	他デバイスからBluetooth®デバイスとして検出されないよう制限します。	–	–	○
テザリング抑止	テザリングの利用を制限します。 ・Android 端末経由でのテザリングを制限します。Android 6.0以上の場合、既に起動済みのテザリングは制限されません。 ・Windows 無線LAN制限、およびUSBネットワークアダプター制限により、テザリング経由での外部通信を制限します。	○	–	○ [6]
USB接続制限	USBの利用を制限します。 ・Android MTPは限定機種での対応となります。 デバイスオーナーでは充電以外を一括で制限します。 ・iOS 端末をキッティングしたApple Configurator以外とのペアリングを禁止します。 ・Windows 外部ストレージ（リムーバブルディスク）の利用を制限します。 任意のストレージ(ベンダーIDやシリアル番号などを指定)をホワイトリスト方式で許可する事も可能です。	○ [2]	○ [4]	○
インストール抑止	インストールをすべて制限します。 Android6.0以上のデバイスオーナー端末へのアプリケーション配布機能で、Google Playを使用せずapkファイルで配布する場合のみインストール可能です。	○ [2][10]	○	–
時刻設定抑止	端末の時刻の変更を制限します。設定は自動設定となります。	○ [2]	–	○
サウンド抑止	端末のサウンドが無効になります。通話のみ可能です。	○ [2]	–	–
アカウント設定抑止	端末のアカウント設定を制限します。既に登録済みの情報は削除されません。	○ [1][2]	–	–
ユーザー追加抑止	端末のユーザー追加を制限します。既に登録済みのユーザーは削除されません。	○ [2][11]	–	–
開発者向けオプション抑止	端末の「開発者向けオプション」全体の制限、または「USBデバッグ」のみを制限します。	○ [1][2] [11] (※L)	–	○
セルラーデータローミング利用抑止	携帯電話回線を利用したデータローミングを制限します。	–	–	○
セルラー上でVPN利用抑止	携帯電話回線を利用したVPN接続を制限します。	–	–	○
セルラー上でVPNローミング利用抑止	携帯電話回線を利用したデータローミング中にVPN接続を使用できないよう制限します。	–	–	○
言語設定変更抑止	言語設定の構成変更を制限します。	–	–	○
電源とスリープ設定変更抑止	電源とスリープ設定の構成変更を制限します。	–	–	○
サインインオプション変更抑止	サインインオプションの構成変更を制限します。	–	–	○
自動再生設定変更抑止	自動再生設定の構成変更を制限します。	–	–	○
ネットワーク共有フォルダ抑止	ネットワーク共有フォルダへのアクセスを禁止します。	–	–	○
ファイル持ち出し設定	アクセス権を設定した外部ストレージ／ネットワーク共有フォルダへのファイルの持ち出しを制限します。許可した利用者にのみ外部へのファイル持ち出しを許可し、持ち出しの証跡を記録します。 [FENCE-Pro]、[FENCE-Works]と連携することで、暗号化したファイルのみ持ち出しを許可、管理者が承認したファイルのみ持ち出しを許可する設定も可能です。	–	–	○
モバイルネットワーク設定の変更抑止	端末のモバイルネットワーク設定の変更を制限します。	○ [2]	–	–
ネットワーク設定のリセット抑止	端末のネットワーク設定のリセットを制限します。	○ [14]	–	–
データの初期化抑止	端末のデータの初期化を制限します。 ポリシーで、「データの初期化抑止」がONの場合に抑止が可能です。	○ [2]	–	–
セーフモード抑止	端末をセーフモードで起動することを制限します。	○ [2]	–	–

（※L：Light版サービス 対応機能）

機能項目名	説明	OS種別		
		Android	iOS	Windows
プロファイル間コピー抑止/管理アプリ外コピー抑止	・Android ビジネス用プロファイルのアプリからそれ以外のアプリへのコピー／貼り付けを制限します。 ・iOS 管理アプリ(MDMによりインストールされたアプリ)とそれ以外のアプリの間でコピー／貼り付けを制限します。	○ [1]	○	–
システムアプリ有効化	ビジネス用プロファイルおよびデバイスオーナーとして登録された端末にて、既定で無効化されているシステムアプリを有効化します。 有効化されたシステムアプリを再度無効化することはできません。	○ [1][2] （※L）	–	–
提供元不明のアプリ抑止	端末の「提供元不明のアプリ」設定を制限します。	○ [1][2] [12] （※L）	–	–
MicrosoftStore以外のストアアプリの インストール抑止	Microsoft Store以外から入手したWindowsストアアプリをインストールできないよう制限します。	–	–	○
MicrosoftStoreからアプリ自動更新抑止	Microsoft Storeからインストールしたアプリを自動更新できないよう制限します。	–	–	○
SDカード制限/外部ストレージ制限	・Android 外部SDカードの利用を制限します。 －デバイスオーナーを使用する場合：SDカードがマウントされなくなります。 －デバイスオーナーを使用しない場合： ・Android6.0未満の端末ではSDカードがマウントされている場合に画面ロックを行います。 ・Android6.0以上の端末では本機能は未対応です。 ・Windows 外部ストレージ（リムーバブルディスク）の利用を制限します。	○	–	○
電話発信先制限	許可された電話番号以外への発信を制限します。	○ [15]	–	–
アプリケーション制限	アプリケーションの利用を制限します。 ・Android ビジネス用プロファイルおよびデバイスオーナーとして登録された端末では、アプリケーションが非表示となり利用できません。 それ以外の場合は、アプリケーション起動後に利用が禁止されます。 ・iOS 監視端末の場合のみ任意のアプリを制限できます。 ・Windows 指定された実行プログラムファイルパス、ウィンドウ名、ウィンドウクラス名に合致するアプリが定期的に起動を監視され、 対象のアプリは停止されます。	○	○ [7]	○
URLフィルター	Android標準の「ブラウザ」の利用を制限し、許可されたURL以外へ接続した場合に利用が禁止されます。 対象ブラウザは"com.android.browser"のみとなります。Chrome等その他のブラウザは対象となりません。	○ [8]	–	–
アンインストール制限	アプリケーションのアンインストールを制限します。	○ [1][2]	○ [4]	–
位置情報取得	定期間隔により位置情報の取得を行います。 ・Android / Windows 端末の位置情報設定が無効の場合、有効化を促すメッセージが表示されます。 ・iOS 端末の位置情報設定を有効にする必要があります。（Light版では利用できません）	○ （※L）	○ [3] （※L）	○
iOS制限設定	ポリシーで指定する各種iOS制限設定を行います。 設定項目はポリシーを確認してください。	–	○	–
root化 / JailBreak検知	端末にてroot化(Android)、JailBreak(iOS)が行われているかを検知します。	○ （※L）	○ [3]	–
USBネットワークアダプター制限	USB接続のネットワークアダプターの利用を制限します。	–	–	○
システムアップデート制御	システムアップデートの制御を行います。 ・Android デバイスオーナーモードにて、システムアップデートの抑止（機種限定）や延期を行います。 ・iOS 監視端末にてシステムアップデートの延期を行います。 ・Windows WSUSサーバーの設定、更新の自動化などが可能です。	○	○ [17]	○
再起動設定	指定した時間に再起動を行います。	○	–	–
専用端末化	業務アプリのみ利用可能な専用端末化設定を行います。	○	–	–
アプリケーション管理	アプリケーションの配布または削除を行います。 ・Android インストール時は確認画面が表示されます。 下記の場合は、サイレントインストールが行われます。 －デバイスオーナーとして登録されているAndroid 6.0以上の端末へのインストーラー(apk)配布 －高士通法人向け特定端末へのインストーラー(apk)配布 －managed Google Playによる配布 ・iOS インストール時は確認画面が表示されます。 下記の場合は、サイレントインストールが行われます。 －監視端末として設定されているiOS端末 また、Android端末(デバイスオーナーまたはビジネス用プロファイルのみ)ではパーミッション設定を行います。 －パーミッション許可の既定動作を指定できます。 －アプリ毎に各パーミッションの許可/拒否を指定できます。 ・Windows msi形式のインストーラーの配信が可能です。	○	○	O
アプリ設定情報の配布	Androidはmanaged Google Play、iOSはManaged App Configurationを使用して配布します。	○ [24]	○ [25]	–
アプリ自動バージョンアップ	配布アプリケーションの自動バージョンアップを行います。	○ [24]	○	–
ファイル配布	ファイルを端末に配布します。	○	○ [3]	○
ファイル収集	デバイス上の指定されたディレクトリ直下に格納されたファイルを収集します。	○	–	–
Wi-Fi設定	端末にてWi-Fiの設定を実施します。	○	○ [5] （※L）	–
証明書配布	端末にVPNおよびアプリ用の証明書を配布します。	○ [1][2]	–	–
構成プロファイル配布	端末に構成プロファイルを配布します。	–	○ （※L）	–
Office 365 アプリデータ保護	Office 365 アプリ保護に対応しているアプリケーションに、セキュリティ保護設定を行うことができます。 別途、Intuneライセンスが必要となります。	○	○	–

（※L：Light版サービス 対応機能）

機能項目名		説明	OS種別		
			Android	iOS	Windows
その他					
	DEP管理	DEP端末の登録に対応しています。	–	○ （※L）	–
	メッセージ通知	端末に管理サーバで登録したメッセージを通知することができます。	○	○ [3]	○
	エージェント削除制限	FENCE-Mobile RemoteManagerの登録を端末で削除されることを禁止します。 ・Android デバイスオーナーとしてキッティングしている場合は、クライアントエージェントをアンインストールすることはできません。 ・iOS DEP端末では、MDM構成プロファイルの削除を禁止できます。 ・Windows 許可されない場合、クライアントを削除できません。	○ （※L）	○ （※L）	○ （※L）
	CSP管理の利用解除抑止	利用者端末からCSP管理の切断を無効化します。	–	–	○ （※L）
	ビジネス用プロファイルの作成	ビジネス用プロファイル領域を作成できます。	○ [1] （※L）	–	–
	デバイスオーナーとして登録	デバイスオーナーとして登録できます。	○ [2] （※L）	–	–
	アプリ単位VPN	アプリ単位VPNを配布できます。	–	○	–
	VPP管理	VPP(Volume Purchase Program)によるライセンス配布に対応しています。	–	○	–
	managed Google Play	managed Google PlayによるGoogleアカウントの設定、アプリケーションの配布、管理対象設定を行います。	○ [18]	–	–
	アプリケーション情報収集	アプリケーション情報の収集を行います。	○ （※L）	○ （※L）	○ （※L）
	ゼロタッチ登録	ゼロタッチ登録に対応しています。	○ [16]	–	–
	管理対象設定	アプリケーションに設定値を配信します。 ・Android managed Google Playを使用して行います。 ・iOS Managed App Configurationを使用して行います。	○	○	–
	Azure AD連携	Azure AD連携からユーザーグループを同期することができます。	○ （※L）	○ （※L）	○ （※L）
	二要素認証	FENCE-Mobile RemoteManagerの管理コンソールのログイン認証に、ユーザーID/パスワードに加えて、ワンタイム パスワードコードを使用することができます。 認証アプリ(Microsoft AuthenticatorまたはGoogle Authenticator)を使用します。	–	–	–
	Azure AD Join連携	Azure ADのテナントに端末を参加させることで、本サービスのインストールやアクティベート作業を自動化できます。	–	–	○
	Windows Autopilot対応	端末のキッティング時に、Windows Autopilotを利用して端末初回起動後の設定作業を自動化できます。	–	–	○

オプションサービス

■ウィルス対策サービス（オプション）をご利用いただくには、別途『FENCE-Mobile RemoteManager ウィルス対策サービス』のご契約が必要となります。

機能名	機能概要	And	iOS	Win
ウィルス対策サービス				
エージェント情報の取得	インストール状況、バージョンなどのエージェント情報を収集し一元管理。	○※L	–	–
パターンファイル情報の取得	バージョン、最終更新日時などのパターンファイル情報を収集し一元管理。	○※L	–	–
スキャン情報の取得	スキャン実行モード、最終実行日時などのスキャン結果を収集し一元管理。	○※L	–	–
パターンファイル更新	遠隔からパターンファイルを即時に最新化。スケジュール実行も可能。	○※L	–	–
ウィルススキャン	遠隔から端末内に進入したウィルスを即時に検知。スケジュール実行も可能。	○※L	–	–

■i-FILTERブラウザーサービス（オプション）をご利用いただくには、別途『FENCE-Mobile RemoteManager i-FILTERブラウザーサービス』の ご契約が必要となります。
本資料では、i-FILTERブラウザーサービス（オプション）の機能は主な機能のみを掲載しております。

機能名	機能概要	And	iOS	Win
i-FILTERブラウザーサービス				
URLフィルタ （カテゴリ別）	予め準備されたカテゴリにより簡単にＵＲＬフィルタを設定可能	○※L	○※L	○※L
ブロック対象URL登録	URLを登録することで、閲覧可能なWebイトをブロック対象にする。 URLの一致条件は「部分一致」（2,000まで／グループ）。	○※L	○※L	○※L
ブロック除外URL登録	URLを登録することで、ブロック対象のWebサイトを閲覧可能にする。 URLの一致条件は「部分一致」（2,000まで／グループ）。	○※L	○※L	○※L
ホワイトリスト機能	URLを登録することで、登録したサイトだけを閲覧可能にする。 URLの一致条件は「部分一致」（2,000まで／グループ）。	○※L	○※L	○※L
ブロック解除機能	ブロック画面でパスワード入力することで、フィルタリングを一時的に解除可能。 パスワードはグループ毎に設定可能。	○※L	○※L	○※L

■リモートヘルプサービス（オプション）をご利用いただくには、別途『FENCE-Mobile RemoteManager リモートヘルプサービス』の ご契約が必要となります。
本資料では、リモートヘルプサービス（オプション）の機能は主な機能のみを掲載しております。

機能名	機能概要	And	iOS	Win
リモートヘルプサービス				
画面の転送機能	Androidデバイスの画面をWindowsデバイス上のFENCEリモートヘルプアプリへ転送して参照可能にする。	○ [26] ※L	−	−
ホワイトペン機能	Androidデバイスの画面上にWindowsデバイス上のFENCEリモートヘルプアプリから線を描画する。	○ [26] ※L	−	−
端末の遠隔操作（対応機種：BZ02、BZ03のみ）	AndroidデバイスのタッチパネルおよびハードウェアボタンをWindowsデバイス上のFENCEリモートヘルプアプリから遠隔で操作する。	○ [26] ※L	−	−

[1]ビジネス用プロファイル内で利用できます
[2]デバイスオーナーとして登録した場合に利用できます。
[3]iOSクライアントアプリのインストールが必要です。
[4]監視端末として設定されている必要があります。
[5]構成プロファイル配布として実施します。
[6]Windowsでは、テザリングへの接続制限となります。
[7]iOS端末が監視端末の場合のみ任意のアプリを制限できます。
[8]Android 6以降では利用できません。
[9]Android 7以降のビジネス用プロファイル内で利用できます。
[10]システムアプリ有効化の処理中、機能の競合を避けるため、インストール抑止は一時的にOFFとなります。処理後は自動で元の状態に戻ります。
[11]Android 7以降のデバイスオーナーでは、端末をセットアップした時点でユーザー追加操作ができなくなります。
[12]ポリシー作成直後およびシステムデフォルトポリシーの初期状態はONとなります。
[13]Android 8以降のビジネス用プロファイル内で利用できます。
[14]Android 6以降でデバイスオーナーとして登録した場合に利用できます。
[15]クライアントアプリのバージョンが1.20以下の場合に利用できます。
[16]Android 8以降のゼロタッチ対応端末の場合に利用できます。
[17]iOS10.3以上の監視端末でのみ利用できます。
[18]デバイスオーナーおよびビジネス用プロファイルにて利用可能です。
[19]Android 7.0以上かつ「デバイスオーナーまたはビジネス用プロファイル」の場合のみ適用されます。
[20]Windows10以上で、msi形式のインストーラー配信により可能です。
[21]Windows10以上で、msiがパラメータなしで、サイレントアンインストールに対応したアプリであれば削除可能です。
[22]iOS10.3以上の監視端末にて、構成プロファイルで設定したWi-Fiネットワークのみに接続を制限する事が可能です。
[23]iOS10.0以上の監視端末にて、Bluetooth設定の変更可否を制限する事が可能です。
[24]managed Google Playを使用します。
[25]Managed App Configurationを使用します。
[26]Androidクライアントエージェントのバージョンが1.24.5以上の場合に利用できます。Windows10以上で利用可能です。ご利用になる際のネットワークには条件があります。

＜注意＞そのほかここに掲載がないOSおよび機種による制限事項がございますので、詳細は以下のURLをご参照ください。
https://www.fujitsu.com/jp/solutions/business-technology/security/secure/fence/fencemobilerm/function/notes.html