FUJITSU Security Solution FENCE シリーズ

FENCE-Mobile RemoteManager サービス機能概要

働き方改革の推進で、今注目を浴びているのが、テレワークのセキュリティ。
なかでもスマートフォン、タブレット、パソコンなどのモバイルデバイスはテレワークには欠かせない必携アイテムとなります。また、グループウェアを利用する企業も増えており、モバイルデバイスを用いて社外で仕事をする機会も増え、紛失、盗難、あるいは内部不正対策含むセキュリティ対策を行うことが企業の最重要課題となっています。
FENCE-Mobile RemoteManager は、モバイルデバイスの資産管理やセキュリティ対策を実現するエンタープライズモビリティ管理サービス。モバイルデバイスを導入する企業の導入プロセスから運用に至るまでの様々な課題解決を支援します。
本書では、FENCE-Mobile RemoteManager が提供するサービス機能概要を紹介することで、モバイルデバイスの運用管理イメージを掴んでいただくことを目的としています。

コンテンツ

1. FENCE-Mobile RemoteManager サービス概要

1-1. FENCE-Mobile RemoteManager とは

FENCE-Mobile RemoteManager は、モバイルデバイスの資産管理やセキュリティ対策を実現するエンタープライズモビリティ管理サービスです。モバイルデバイスを導入する企業の導入プロセスから運用に至るまでの様々な課題解決を支援します。

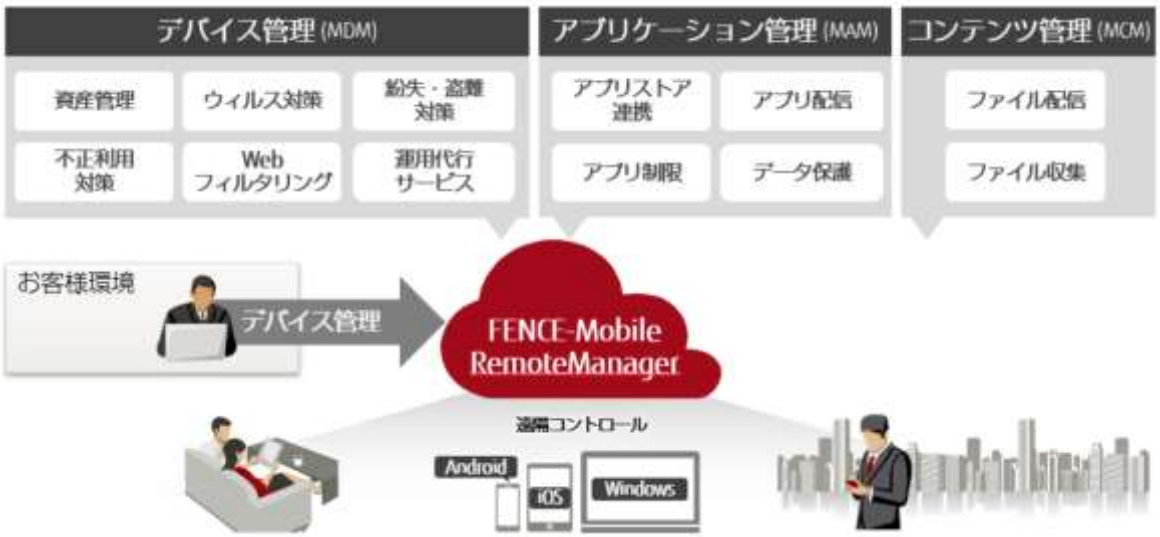

図 1：サービス概要図

1-2. サービス体系

サービス名称	サービス内容
基本利用サービス（必須）	
基本利用サービス	資産管理、アプリケーション管理、デバイス制御、リモートロック・ワイプなど EMM のすべての機能を網羅したサービス。
基本利用サービス（Light）	資産管理、リモートロックやワイプなどの基本機能に限定した安価なサービス。
オプションサービス（任意）	
運用代行	端末の紛失・盗難事故が発生した際に、お客様のシステム管理者に代わって、リモートロック・ワイプを行う 24 時間 365 日対応のサービス。
ウイルス対策	McAfee 社の Android デバイス向けウイルス対策サービス。
i-FILTER ブラウザー	デジタルアーツ社の i-FILTER ブラウザーサービス。

2. FENCE-Mobile RemoteManager 機能一覧

2-1. デバイス導入サポート

デバイス導入時の作業負荷を軽減する Device Enrollment Program や Android Enterprise のゼロタッチ登録(Zero-touch enrollment)に対応しています。

2-1-1. Device Enrollment Program

Device Enrollment Program(以下、DEP)とは、Apple が提供する、iOS デバイスの企業および教育機関向け導入支援サービスです。

DEP を採用することで、以下のような効果が得られます。

- デバイス導入作業（キッティング）の負荷軽減
- EMM への自動登録、および EMM 用構成プロファイルの削除制限
- 監視モードの自動有効化

2-1-1-1. 監視モード

企業の管理者が、デバイスの監視／管理をより強固にできるデバイス設定方式です。監視モードに設定されたデバイスには、従来の管理方式より多くのセキュリティ項目を制御することができます。

2-1-2. Android Enterprise

Android Enterprise は、Google が提供する、企業向け Android デバイス管理プログラムです。
Android Enterprise に対応したデバイスでは、デバイス管理の徹底や高度なセキュリティを実現するための様々な機能や仕組みが実装されています。FENCE-Mobile RemoteManager では Android Enterprise に対応することで、従来の管理方式より強固なセキュリティ対策や柔軟なデバイスの運用管理を実現します。

2-1-2-1. ゼロタッチ登録

ゼロタッチ登録は、効率的に大量のデバイスを導入するための仕組みです。ゼロタッチ登録に対応したデバイスを EMM と事前に紐づけておくことで、デバイスの電源を入れてから簡単な操作で EMM の登録までが完了できます。
Android8.0 以上のデバイスで利用できます。

ゼロタッチ登録を採用することで、以下のような効果が得られます。

- デバイス導入作業（キッティング）の負荷軽減
- EMM への自動登録、および EMM クライアントエージェントのアンインストール制限
- Fully managed device の自動有効化

2-1-2-2. Fully managed device

Fully managed device（以下、FMD）は、企業管理者がデバイスの監視／管理をより強化するデバイス管理方式です。
Android 5.0 以上のデバイスで使用できます。

FMD では、次のセキュリティ項目が制御できます。

- 位置情報設定の強制化
- USB 接続制御
- アカウント設定抑止
- アプリケーションのインストール抑止
- アプリケーションのサイレントインストール
- 利用制限されたアプリケーションの非表示化　など

デバイスの初期設定時（電源入力時）に FMD として設定することで、FENCE-Mobile RemoteManager クライアントエージェントも同時に自動インストールされます。ただし、最初にデバイスの初期化が行われるため注意が必要です。

2-1-2-3. Work Profile

Work Profile（以下、WP）は、デバイス内の領域を「企業」と「個人」に分割し、「企業領域」のみポリシー設定やアプリケーション配布などの管理が行なえるデバイス管理方式です。
Android 5.0 以上のデバイスで使用できます。

WP では、次のデバイス管理、アプリケーション管理が実現できます。

- 企業領域のみセキュリティポリシーを適用
- 企業／個人領域間のデータコピーを禁止
- デバイス紛失時、企業領域のみリモートワイプ適用
- 利用制限された企業領域のアプリケーションの非表示化　など

2-2. デバイス管理(MDM)

2-2-1. 資産管理

OS 種類、モデルなどのハードウェア情報、インストールされたアプリケーション情報などを収集し一元管理します。また、Wi-Fi 設定や証明書、各種デバイス設定などの構成プロファイルをデバイスへ配信し自動設定します。

機能名	機能概要	iOS		Android			Windows
		監視モード		FMD	WP		
デバイス管理	電話番号や機体番号、ユーザー情報などに基づいて認証されたデバイスを登録します。 管理されたデバイスは、企業ポリシーが適用され、事故発生時には即座に制御コマンドを発行できます。また、アラートやログ情報からデバイスの状況を把握することも可能です。 ● CSVファイルの取り込みによるデバイス情報の一括登録が可能。	○*L	○*L	○*L	○*L	○*L	○*L
デバイス情報の取得	OS、モデル、SIMカードなどのデバイス情報を収集し一元管理します。 定期的な情報収集や情報の最新化を即時に行うことも可能です。	○*L	○*L	○*L	○*L	○*L	○*L
構成プロファイルの配布	構成プロファイルを配信することで、VPNやメールアカウント、LDAP、Webクリップなどの構成情報をデバイスへ配信します。	○*L	○*L	–	–	–	–
Wi-Fi設定の配布	デバイスへWi-Fi設定を配信します。 *iOS:「構成プロファイルの配布」として実現。*	○*L	○*L	○	○	○ *2.2以上*	–
証明書の配布	デバイスへVPNおよびアプリケーション用の証明書を配信します。 *iOS:「構成プロファイルの配布」として実現。*	○*L	○*L	○	○	–	–
システムアップデート制御	OSベンダーから提供されるOS・システムアップデートを制御します。 *iOS: アップデートの即時指示、延期(11.3以上)が可能。* *Android: アップデートの自動化、時刻指定、延期などが可能。*	○ *10.3以上*	–	○ *6.0以上*	–	–	–
専用デバイス化	任意のアプリケーションのみ表示し、その他は非表示により操作不能を実現します。業務専用デバイスやキオスクデバイスなど単一業務に最適な利用法です。 *iOS: 専用アプリケーション(シングルAppモード)の指定が可能。* *Android: 専用アプリケーションの指定、設定アプリケーションの表示制御が可能。*	○ *7.0以上*	–	○ *6.0以上*	–	–	–
デバイス再起動	指定時刻にデバイスをリブート(再起動)します。	–	–	○ *7.0以上*	–	–	–

*L: 基本利用サービス（Light）で提供される機能を指します。

表 1：デバイス管理(MDM) - 資産管理

2-2-2. 不正利用対策

カメラや画面キャプチャー、USB 接続、SD カードなどの機能を制御することでデバイスの悪用を未然に防ぎます。また、Jailbreak や root 化されたデバイスの検知が可能です。

機能名	機能概要	iOS		Android			Windows
		監視モード		FMD	WP		
カメラ抑止	カメラ機能の利用を制限します。 *Windows: 『カメラデバイス』などと識別できる機器が制御対象。*	○	○	○	○	○	○
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。	○	○	○	○	○ *2.2以上*	–
無線LAN抑止	無線LANデバイスの利用を制限します。 *iOS: 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。* *Android: WP以外は、任意のアクセスポイントをホワイトリスト方式で許可。* *Windows: 任意のアクセスポイントをホワイトリスト方式で許可。*	○ *10.3以上*	–	○	○	○	○
Bluetooth®抑止	Bluetooth®機能の利用を制限します。 *iOS: Bluetooth® 設定の変更可否を制限。*	○ *10.0以上*	–	○	○	○	○
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。	–	–	–	–	–	○ *10以上*
USB接続制御	USB接続を制限します。 *iOS: 監視モード設定時に用いたApple Configurator以外とのペアリングを制限。* *Android: FMDでは、充電以外のUSB接続を制限可能。それ以外は、一部制限あり。* *Windows: 詳細は「SDカード抑止/外部ストレージ抑止」を参照。*	○ *7.0以上*	–	○	–	○ *4.2未満*	○
構成プロファイルのインストール抑止	構成プロファイルののインストールを制限します。	○ *11.0以上*	–	–	–	–	–
FaceTime抑止	FaceTime機能の利用を制限します。	○	○ *13.0未満*	–	–	–	–
Siri抑止	Siriの利用を制限します。	○	○	–	–	–	–
音声ダイヤル抑止	デバイスロック中の音声ダイヤルの利用を制限します。	○	○	–	–	–	–
App内での購入抑止	App内での購入を制限します。	○	○	–	–	–	–
購入時のiTunes Storeパスワード要求	App 内での購入、および『iTunes』での購入時、アカウントパスワードの入力を強制します。	○ *5.0以上*	○ *5.0以上*	–	–	–	–
Game Center抑止	Game Centerの利用を制限します。	○ *6.0以上*	–	–	–	–	–
Touch ID抑止	ロック解除におけるTouch ID利用を制限します。	○ *7.0以上*	○ *7.0以上*	–	–	–	–
ロック画面での通知センター、コントロールセンター抑止	ロック画面でのコントロールセンター、通知センターの表示を制限します。	○ *7.0以上*	○ *7.0以上*	–	–	–	–
AirDrop抑止	AirDropを制限します。	○ *7.0以上*	–	–	–	–	–
AirPrint抑止	AirPrintを制限します。	○ *11.0以上*	–	–	–	–	–
Apple Music抑止	Apple Musicを制限します。	○ *9.3以上*	–	–	–	–	–
"ファイル"アプリ抑止	"ファイル"Appからネットワークドライブ、USBドライブへのアクセスを制限します。	○ *13.0以上*	–	–	–	–	–
Radio抑止	Apple MusicでのRadioを制限します。	○ *9.3以上*	–	–	–	–	–
デバイスロック中のUSB抑止	デバイスロック中のUSBアクセサリー接続を制限します。	○ *11.4.1以上*	–	–	–	–	–
通知設定の変更抑止	通知設定の構成変更を制限します。	○ *9.3以上*	–	–	–	–	–
eSIM設定の変更抑止	eSIM設定の構成変更を制限します。	○ *12.1以上*	–	–	–	–	–
Wi-Fiの電源を強制的にオン	Wi-Fiを強制的に有効化します。	○ *13.0以上*	–	–	–	–	–
Wi-Fiパスワード共有抑止	Wi-Fiのパスワード共有(公開)を制限します。	○ *12.0以上*	–	–	–	–	–

（次ページへ続く）

機能名	機能概要	iOS		Android			Windows
		監視モード		FMD	WP		
AirDropパスワード共有抑止	AirDropを使ってWebサイトやAppのパスワードを共有することを制限します。	○ *12.0以上*	–	–	–	–	–
パスワードの自動入力抑止	WebサイトやAppのパスワード自動入力を制限します。	○ *12.0以上*	–	–	–	–	–
iCloud制御	バックアップや書類の同期などiCloud機能の使用を制御します。	○	○	–	–	–	–
セキュリティとプライバシー制御	Appleへの診断データの送信や暗号化バックアップの強制化、追跡型広告などを制御します。	○	○	–	–	–	–
コンテンツレーティング制御	不適切な内容の音楽/Apple Podcasts/iTunes Uの制御、ムービー/テレビ番組/Appの許可レーティング指定などが可能です。	○	○	–	–	–	–
日付、時刻設定抑止	日付や時刻を自動設定とし、構成変更を制限します。	○ *12.0以上*	–	○	–	–	○ *10以上*
サウンド抑止	サウンドを制限します。制限時でも、通話は可能です。	–	–	○	–	–	–
アカウント設定抑止	アカウント設定を制限します。登録済みのアカウントには影響を与えません。 また、アカウント設定抑止を設定中でも、アプリケーションからのアカウント追加は可能です。	–	–	○	○	–	–
ユーザー追加抑止	ユーザー追加設定を制限します。既に登録済みのユーザーには影響を与えません。	–	–	○	–	–	–
開発者向け機能抑止	開発者向け機能を制限します。 *Android: 開発者向けオプション全体の制限、もしくはUSBデバッグのみを制限。* *Windows: 開発者モードを利用できないよう制限。*	–	–	○*L	○*L	–	○ *10以上*
モバイルネットワーク設定の変更抑止	モバイルネットワーク設定の変更を制限します。	–	–	○	–	–	–
ネットワーク設定のリセット抑止	ネットワーク設定のリセットを制限します。	–	–	○ *6.0以上*	–	–	–
データの初期化抑止	デバイスの初期化を制限します。	–	–	○	–	–	–
セーフモード抑止	デバイスのセーフモード起動を制限します。	–	–	○ *6.0以上*	–	–	–
電話発信先抑止	許可された電話番号以外への発信を制限します。	–	–	○ *9.0以下*	○ *7.0以上* *9.0以下*	○ *9.0以下*	–
URLフィルター	ウェブサイトへのアクセスをURL単位で制限します。 (対象は標準ブラウザー『com.android.browser』)	–	–	○ *6.0未満*	○ *6.0未満*	○ *6.0未満*	–
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。	–	–	–	–	–	○ *10以上*
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。	–	–	–	–	–	○ *10以上*
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。	–	–	–	–	–	○ *10以上*
言語設定変更抑止	言語設定の構成変更を制限します。	–	–	–	–	–	○ *10以上*
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。	–	–	–	–	–	○ *10以上*
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。	–	–	–	–	–	○ *10以上*
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。	–	–	–	–	–	○ *10以上*
テザリング抑止	テザリング機能の利用を制限します。 *Android: デバイス自身のテザリング有効化を制限。* *Windows: デバイス自身のインターネット接続を他デバイスと共有できないよう制限（「モバイル ホットスポット」機能の抑止）(10以上)。また、「無線LAN抑止」、「USBネットワークアダプター抑止」にてテザリングが有効化されたデバイスへの接続を制限可能。*	–	–	○	–	○ *2.2以上* *6.0未満*	○
SDカード抑止/外部ストレージ抑止	SDカード、外部ストレージの利用を制限します。 *Windows: 外部ストレージ(リムーバブルディスク、BD/DVD/CD-ROMなど)の利用を制御。また、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。*	–	–	○	–	○ *6.0未満*	○
USBネットワークアダプター抑止	USB経由で接続されたネットワークアダプターの利用を制限します。また、任意のネットワークアダプター(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できます。	–	–	–	–	–	○

（次ページへ続く）

機能名	機能概要	iOS		Android			Windows
		監視モード		FMD	WP		
Jailbreak/root化検知	デバイスのroot化(Android)、Jailbreak状態(iOS)を検知します。	○*1	○*1	○*L	○*L	○*L	–
エージェント制限	本サービスのクライアントエージェントに対するアンインストール操作を制限します。 *iOS: DEPデバイスでは、EMM構成プロファイルの削除を制限。その他は、EMM構成プロファイルが削除されたことを検知。*	○*L	○*L	○*L	–	–	○*L

*L: 基本利用サービス（Light）で提供される機能を指します。

*1: iOS 向け FENCE-Mobile RemoteManager クライアントエージェントの導入が必要です。

表 2：デバイス管理(MDM) - 不正利用対策

2-2-3. 紛失・盗難対策

紛失・盗難事故に備えてのローカルロック・ワイプの強制適用、事故発生時にデバイスの位置を把握したり、リモートロック・ワイプを即時に発行することで被害を最小限にとどめることができます。

機能名	機能概要	iOS		Android			Windows
		監視モード		FMD	WP		
ローカルロック設定	デバイスのローカルロックを設定します。 パスワードポリシー(文字種類、最小文字数など)の設定、画面ロック設定の強制化が可能です。	○*L	○*L	○*L	○*L *7.0以上*	○*L *2.2以上*	○*L *10以上*
ローカルワイプ設定	デバイスのローカルワイプを設定します。 *iOS: 画面ロック解除を連続で間違えた場合、デバイス初期化。* *Android: 画面ロック解除を連続で間違えた場合、デバイス初期化。SDカードも対象。* *Windows: 一定期間、管理サーバーとの通信が行われない場合、ポリシーで定義された消去方法(消去範囲、方式など)で、デバイス初期化。*	○*L	○*L	○*L	○*L *7.0以上*	○*L *2.2以上*	○*L
ローカルロック設定（デバイス向け）	デバイスの画面ロックを強制的に設定します。	–	–	–	○*L *8.0以上*	–	–
ローカルワイプ設定（デバイス向け）	デバイスの画面ロック解除を連続で間違えた場合、企業領域内を初期化します。	–	–	–	○*L *8.0以上*	–	–
ポリシー設定遵守	ローカルロック設定に違反している場合、アプリケーション(設定やシステムアプリケーションなどは対象外)を無効化します。 また、WPでは、企業領域のアプリケーションのみが無効化対象です。	–	–	○ *7.0以上*	○ *7.0以上*	–	–
SIM差し替えロック	アクティベート時に認識された電話番号と異なる電話番号のSIMが挿入された場合に画面をロックします。	–	–	○	–	○ *2.2以上* *7.0未満*	–
リモートロック	デバイスを画面ロックします。 *iOS: 設定済みのパスコードで画面ロック。「リモートロック解除」で解除可能。7.0以上では、ロック中にメッセージと連絡先の電話番号を表示することが可能。* *Android: ランダムなパスワードで画面ロック。「リモートロック解除」か、解除用パスワードを入力することで解除可能。また、通常モード(7.0以上)では、設定済みのパスワードでの画面ロックが可能。* *Windows: 設定済みのパスコードで画面ロック。*	○*L	○*L	○*L	–	○*L *2.2以上* *7.0未満*	○*L
リモートロック解除	デバイスの画面ロックを解除します。パスコードはクリアされます。 *Android: ロック解除時にパスワードの指定が可能。*	○*L	○*L	○*L	–	○*L *7.0未満*	–
リモートワイプ	遠隔からデバイスを初期化します。 *iOS: OS初期化機能と同等の方式で即座に初期化。* *Android: OS初期化機能と同等の方式で即座に初期化。SDカードも対象。* *Windows: OS標準の『このPCを初期状態に戻す』を適用(10以上)。また、ポリシーで定義された消去方法(消去範囲、方式など)で、即座に初期化も可能。*	○*L	○*L	○*L		○*L *2.2以上*	○*L
紛失モード設定	「紛失モード解除」以外では解除できない画面ロックを設定することで、デバイス紛失・盗難時のセキュリティを強化できます。	○*L	–	–	–	–	–
紛失モード解除	紛失モードを解除します。	○*L	–	–	–	–	–
位置情報取得（紛失モード）	紛失モードに設定されたデバイスの位置情報を収集し、管理コンソールでデバイスの場所を確認できます。位置情報設定に関わらず位置情報の取得が可能です。	○*L	–	–	–	–	–
プロファイルロック	企業領域をランダムなパスワード、もしくは設定済みのパスワードでロックします。「プロファイルロック解除」か、解除用パスワードを入力することで解除できます。	–	–	–	○*L *7.0以上*	–	–
プロファイルロック解除	企業領域の画面ロックを解除し、指定された(新しい)パスワードを設定します。	–	–	–	○*L *7.0以上*	–	–
プロファイルワイプ	企業領域全体を削除します。	–	–	–	○*L	–	–
位置情報取得	位置情報を収集し、管理コンソールでデバイスの場所を確認できます。タイムリーな位置情報の把握、および定期間隔での位置情報の取得が可能です。 *iOS: 位置情報設定が無効の場合、有効化を促すメッセージを表示。* *Android: FMDでは、位置情報設定の強制有効化。それ以外は、位置情報設定が無効の場合、有効化を促すメッセージを継続表示。* *Windows: 位置情報設定が無効の場合、有効化を促すメッセージを継続表示。*	○*1	○*1	○*L	○*L	○*L *2.2以上*	○*L *8.1以上*

*L: 基本利用サービス（Light）で提供される機能を指します。

*1: iOS 向け FENCE-Mobile RemoteManager クライアントエージェントの導入が必要です。

表 3：デバイス管理(MDM) - 紛失・盗難対策

2-2-4. ウイルス対策

Android デバイスにおけるウイルス・マルウェア対策の実現、セキュリティポリシーやウイルススキャン結果の一元管理、ウイルススキャンの即時実行などが可能です。

機能名	機能概要	iOS		Android			Windows
		監視モード		FMD	WP		
情報の取得	エージェントやパターンファイルの情報を収集し一元管理します。 ● エージェント情報は、インストール状況やバージョンなど ● パターンファイル情報は、版数や最終更新日時など	–	–	○	○	○ *2.2以上*	–
企業ポリシーの適用とコマンド実行	エージェントの導入方式やリアルタイムスキャンの有効化、パターンファイルの更新スケジュール、ウイルススキャンスケジュールなどの企業ポリシーをデバイスへ適用します。また、緊急時は、パターンファイルの更新、ウイルススキャンを即座に実施できます。						
ログ管理	ウイルススキャン実行状態や最終実行日時などのウイルススキャン結果を収集し一元管理します。						

表 4：デバイス管理(MDM) -ウイルス対策

2-2-5. i-FILTER ブラウザー

ウェブブラウザー経由でアクセス可能なサイトを制限します。カテゴリ指定によるホワイトリスト化で効率的に企業ポリシーを適用することが可能です。

機能名	機能概要	iOS		Android			Windows
		監視モード		FMD	WP		
URLフィルタリング	ウェブサイトへのアクセスを制限します。 ● カテゴリを指定することで制御可能 ● URLを指定することで、ブロック対象/除外対象が指定可能	○	○	○	○	○	○
セキュアブラウザー	ウェブアクセス時に発生する認証情報やキャッシュ・ダウンロードコンテンツの保存操作に対して『禁止/特定のタイミングで削除』などが制御できます。	○	○	○	○	○	–
MultiAgent	バックアップサービスとして実行することで、利用しているアプリケーションを問わずウェブアクセスを制御します。	–	–	–	–	–	○
レポーティング	ウェブサイトへのアクセス状況を可視化することで、潜在する情報漏えいリスクを把握できます。	○	○	○	○	○	○

表 5：デバイス管理(MDM) -i-FILTER ブラウザー

2-2-6. 運用代行サービス

管理者が対応できない夜間や休日に発生した紛失・盗難事故に対して、お客様のセキュリティ対策運用（リモートロック・ワイプ）を当社が代行します。

2-3. アプリケーション管理(MAM)

Volume Purchase Program(以下、VPP)や managed Google Play など OS が提供するフレームワークをサポートし、アプリケーションの配信、利用制限、VPN 設定、データ保護などを実現します。

機能名	機能概要	iOS		Android			Windows
		監視モード		FMD	WP		
アプリケーション情報の収集	パッケージ名、バージョン、ファイルサイズなどのアプリケーション情報を収集し一元管理します。	○	○	○	○	○	○
VPP	VPPに対応したアプリケーション配布が可能です。	○	○	–	–	–	–
managed Google Play	managed Google Playに対応したアプリケーション配布が可能です。	–	–	○	○	○ *4.2以上 5.0未満*	–
システムアプリ有効化	既定で無効化されているシステムアプリケーションを有効化します。 有効化されたシステムアプリケーションを再度無効化することはできません。	–	–	○*L	○*L	–	–
システムアプリ削除制御	システムアプリケーションの削除を制限します。	○ *11.0以上*	–	–	–	–	–
アプリのインストール抑止	アプリケーションのインストールを制限します。 *Android: 抑止設定に関わらず、「アプリ配布」でapkファイルを配布する場合はインストール可能。*	○	○	○	–	–	–
アプリのアンインストール抑止	アプリケーションのアンインストールを制限します。	○	–	○	○	–	–
提供元不明アプリのインストール抑止	提供元が不明なアプリケーションのインストールを制限します。	–	–	○*L	○*L	–	–
Microsoft Store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。	–	–	–	–	–	○ *10以上*
Microsoft Store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。	–	–	–	–	–	○ *10以上*
アプリ配布	即時もしくは指定日時でアプリケーションを配布または削除します。 また、インストール開始時には確認画面(インストール通知)を表示します。 *iOS: 監視モードの場合、確認画面は省略。* *Android: managed Google Play での配布、またはFMD(6.0以上)へのapkファイル配布時は、確認画面は省略。* *Windows: msi形式のインストーラーの配信が可能。*	○	○	○	○	○	○ *10以上*
アプリカタログ	デバイス上で、企業が許可したアプリケーション一覧(アプリケーションカタログ)から任意のアプリケーションを選択/インストールすることができます。	○*1	○*1	○	○	○	–
アプリ権限の配布	アプリケーションのパーミッション情報を配布します。	–	–	○	○	–	–
アプリ設定情報の配布	アプリケーションのセットアップ情報を配布します。 *iOS: Managed Configrationを使用して配布。* *Android: managed Google Playを使用して配布。*	○	○	○	○	○ *4.2以上 5.0未満*	–
アプリ単位VPN	アプリケーション単位でVPN接続するための設定情報を配布します。	○	○	–	–	–	–
アプリ管理化	デバイス所有者にてインストールしたアプリケーションを管理対象アプリケーションへ変換します。	○ *9.0以上*	○ *9.0以上*	–	–	–	–
アプリ利用制限	アプリケーションの利用を制限します。 *iOS: 非監視モードおよび監視モード(9.3未満)の場合、『iTunes Store』、『Safari』のみ制限可能。監視モード(9.3以上)では、ホワイトリスト/ブラックリスト方式で利用制限。* *Android: ホワイトリスト/ブラックリスト方式で利用制限(FMD/WPは非表示化)。* *Windows: ブラックリスト方式で利用制限。*	○	○ *13.0未満*	○	○	○ *10.0未満*	○
データ保護	企業が管理するアプリケーションからのデータ持ち出し操作を制限します。 *iOS: 本サービスから配布した『管理アプリケーション』、『管理対象連絡先データ(12.0以上)』からのコピー&貼り付けを制限。* *Android: 企業領域からのコピー&貼り付けを制限。*	○ *7.0以上*	○ *7.0以上*	–	○	–	–
データ保護 （アプリ単位）	Microsoft 365関連、および一部のサードパーティー製アプリケーションにおいて、アプリケーション単位でデータ保護強化(起動時のPIN入力要求、コピー&貼り付けの制限など)を実現します。	○ *11.0以上*	○ *11.0以上*	○	○	○ *4.4以上*	–

*L: 基本利用サービス（Light）で提供される機能を指します。

*1: iOS 向け FENCE-Mobile RemoteManager クライアントエージェントの導入が必要です。

表 6：アプリケーション管理(MAM)

2-3-1. Microsoft 365 連携

Microsoft 365（旧 Office 365）関連のアプリケーションを安心安全に利用するための機能を提供します。

- アプリケーションのセキュア配信
- データ持ち出しを制御するデータ保護
- 紛失・盗難時には Microsoft 365 関連のアプリケーションのみを消去　など

2-3-2. 業務アプリケーション連携

Android デバイス自社開発などの業務アプリケーションを本格運用するための様々な支援機能を提供します。

- 業務アプリケーションのみ操作可能とする専用デバイス化
- アプリケーションのサイレントインストール
- 定時でのデバイス再起動
- 業務データの収集
- OS・システムアップデート制御　など

2-4. コンテンツ管理(MCM)

PDF や業務データなどのコンテンツを各デバイスへ配信し、デバイス上に格納されたコンテンツを収集します。

機能名	機能概要	iOS		Android			Windows
		監視モード		FMD	WP		
ファイル配布	PDFファイル、業務データなどのファイルをデバイスへ配信します。 即時または指定日時での実行が可能です。 *Android: ファイルの配布先は『/mnt/sdcard配下』が対象。*	○*1	○*1	○	○	○	–
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。 収集されたファイルは管理コンソールから参照できます。	–	–	○	○	○ *4.0以上*	–

*1: iOS 向け FENCE-Mobile RemoteManager クライアントエージェントの導入が必要です。

表 7：コンテンツ管理(MCM)

2-5. 管理者サポート

デバイス管理者の負荷軽減、運用支援を実現するため、管理者分掌機能やログ機能、ダッシュボード含めたアラート機能、メッセージ通知機能、CSV ダウンロード機能などを提供します。

機能名	機能概要	iOS		Android			Windows
		監視モード		FMD	WP		
アラート	『一定期間アクセスなし』や『制御エラー発生』、『マルウェア対策不備』などのデバイス動作状況をダッシュボード画面で簡単に把握できます。 ● アラートルールの閾値(ルール評価期間)指定が可能。 ● アラート情報を定期的にメール通知。	○*L	○*L	○*L	○*L	○*L	○*L
グループ管理	デバイスやユーザーを管理するグループ情報を登録します。 グループは、管理者ユーザーの権限範囲やポリシーの適用範囲に使用します。 ● 組織グループは、組織構造(階層化)に基づいて部門やユーザー、デバイスを管理。 ● 端末グループは、職種やプロジェクト単位など任意の役割に応じてデバイスを管理。 ● CSVファイルの取り込み、Azure Active Directory連携でグループ情報の一括登録が可能。	○*L	○*L	○*L	○*L	○*L	○*L
ユーザー管理	組織に属するユーザーやデバイス所有者、デバイス管理者などのユーザー情報を登録します。 ● 管理者ユーザーは、テナント全体や特定グループなど権限範囲の定義、および『リモートロック/ワイプ』や『端末登録のみ』など役割に応じた操作権限を付与。 ● CSVファイルの取り込み、Azure Active Directory連携でユーザー情報の一括登録が可能。	○*L	○*L	○*L	○*L	○*L	○*L
ポリシー管理	任意のデバイスやグループに対して、企業ポリシーを適用します。 企業ポリシーでは、「紛失・盗難対策」や「不正利用対策」、「ウイルス対策」、「アプリケーション管理(MAM)」、「コンテンツ管理(MCM)」のセキュリティ対策項目、配布指示を定義します。	○*L	○*L	○*L	○*L	○*L	○*L
コマンド実行	任意のデバイスに対して即座に実行する制御指示を発行します。 コマンド実行には、「紛失・盗難対策」や「ウイルス対策」、「アプリケーション管理(MAM)」の各制御項目が含まれます。	○*L	○*L	○*L	○*L	○*L	○*L
メッセージ通知	任意のデバイスやグループに対して、メッセージを即時配信します。 ● 件名、メッセージ本文、通知時の効果音有無などを指定可能 ● 各デバイスのメッセージ未既読状態が管理可能	○*1	○*1	○	○	○	○
ログ管理	ポリシーの適用状況やコマンド実行履歴、デバイス上で発生したイベントなどデバイス管理状況を収集し一元管理します。	○*L	○*L	○*L	○*L	○*L	○*L
CSVダウンロード	『デバイス情報』や『アプリケーション情報』、『ポリシー情報』などをCSVファイルでダウンロードできます。	○*L	○*L	○*L	○*L	○*L	○*L

*L: 基本利用サービス（Light）で提供される機能を指します。

*1: iOS 向け FENCE-Mobile RemoteManager クライアントエージェントの導入が必要です。

表 8：管理者サポート

3. 最後に

3-1. 最新情報

その他、より詳細な機能説明（OS および機種ごとの制限事項など）や最新の機能概要は、以下サイトを併せてご覧ください。

管理者マニュアル: https://www.fence-mobile.bsc.fujitsu.com/manual/index.html

注意事項: https://www.fujitsu.com/jp/group/bsc/services/fence/fencemobilerm/function/notes.html

3-2. 無償トライアルサービス

無償トライアルサービスでは、本書で紹介した FENCE-Mobile RemoteManager のサービス機能や使用感を試すことができます。また、ご契約時は、トライアル環境をそのまま引き継ぐことも可能ですので、ぜひご活用ください。

- 提供機能は、全サービス機能（ただし、運用代行サービスは対象外）
- 登録可能なデバイス数は、10 台まで（デバイスは、お客様にてご準備願います）
- 利用期間は、30 日まで

無償トライアルサービスのお申し込みは、こちら！

https://www.fujitsu.com/jp/group/bsc/services/fence/fencemobilerm/trial.html

お問い合わせ先

富士通株式会社

〒212-0014 神奈川県川崎市幸区大宮町１番地５ JR 川崎タワー
E-Mail: bsc-spinfo@cs.jp.fujitsu.com
当社 ホームページ https ://www.fujitsu.com/

FMRM-BSC-W-v0210（2021 年 7 月製作）