ＭＤＭ導入･運用検討ガイド

～　スマートフォンの適切なセキュリティ管理のために　～

【第１版】

平成25年1月24日

一般社団法人日本スマートフォンセキュリティ協会（JSSEC）
技術部会
デバイスワーキンググループ
ＭＤＭタスクフォース

文書管理番号 JSSEC-TECD-MD-GD20130124

■制作■

技術部会デバイスワーキンググループＭＤＭタスクフォース

リーダー	八津川　直伸	（日本ユニシス株式会社）
メンバー	竹森　敬祐	（KDDI株式会社）
	西出　禎	（KDDI株式会社）
	合田　幸司	（サイバートラスト株式会社）
	谷田部　茂	（シスコシステムズ合同会社）
	重田　大助	（シャープ株式会社）
	倉永　英久	（株式会社大和総研ビジネス・イノベーション）
	五代儀　真	（トレンドマイクロ株式会社）
	鈴木　孝彦	（日本電気株式会社）
	関　徳男	（日本電気株式会社）
	磯田　弘司	（日本ベリサイン株式会社）
	松山　啓介	（株式会社富士通ビー・エス・シー）
オブザーバ	佐藤　勝彦	（Androidセキュリティ部）
	飯野　道代	（株式会社NSD）
	竹本　哲也	（株式会社NSD）
	北村　祐司	（サイバートラスト株式会社）
	萩原　栄幸	（社団法人情報セキュリティ相談センター）
	谷本　重和	（情報セキュリティ大学院大学客員研究員）
	和田　貴広	（株式会社大和総研ビジネス・イノベーション）
	倉林　俊介	（トヨタ自動車株式会社）
	栃沢　直樹	（トレンドマイクロ株式会社）
	中川　泰通	（日本システムウエア株式会社）
	片浦　哲平	（日本電気株式会社）
	二村　廉太	（株式会社ネクストジェン）
	相原　弘明	（株式会社ネットマークス）
	岩澤　孝博	（富士ソフト株式会社）
	島津　晴行	（富士ソフト株式会社）
	中野　純一	（富士ソフト株式会社）

（社名五十音順）

文書管理番号 JSSEC-TECD-MD-GD20130124

目次

付録：MDM機能要件チェックリスト

1 はじめに

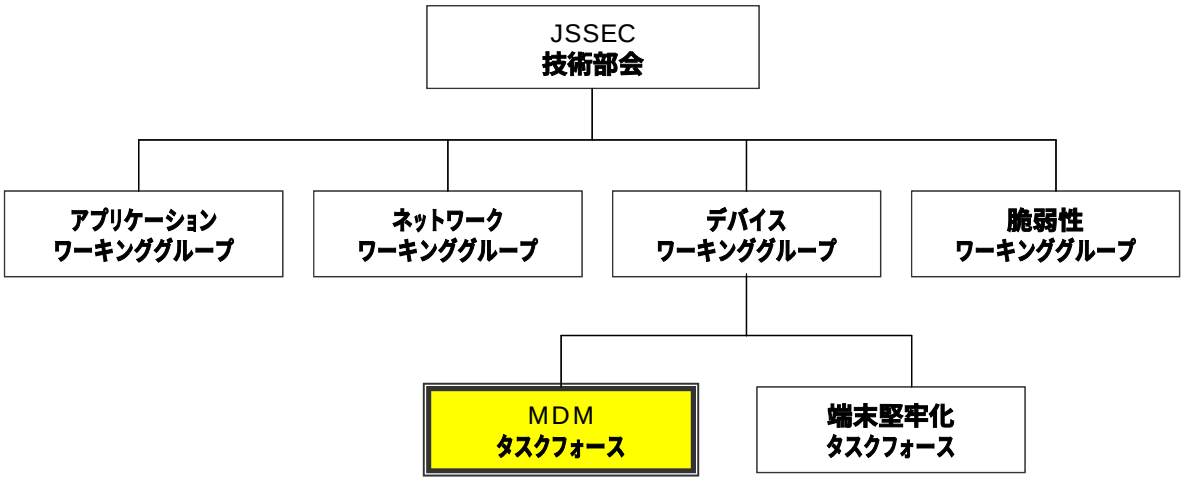
1.1 本ガイドの目的について

スマートフォンやスマートタブレット（以下、スマートフォン）は、電話機能等を持ったPC（パーソナルコンピュータ）であり、従来のモバイルPCよりもモビリティ性能が高く、マルチキャリア、マルチベンダーより多種多様な製品が市場に普及している。これに伴い、セキュリティ管理が煩雑となり、運用や管理コストの上昇が懸念されている。

このような課題を解消する一助として、Mobile Device Management（以下ＭＤＭ）の様々な製品・サービスが、各社から提供されているが、本ガイドでは、スマートフォンの一元的な管理を支援するＭＤＭについて、導入時の検討事項及び運用上の留意点等を解説する。

なお、企業が業務で利用するスマートフォンを対象としているが、スマートフォンの普及は個人利用が先行しているため、これら私物スマートフォンの業務利用上の注意点にも触れている。

本ガイドは、JSSEC技術部会ＭＤＭタスクフォースで作成している。JSSEC技術部会におけるＭＤＭタスクフォースの位置づけは、以下の通りである。



1.2 本ガイドの対象読者について

本ガイドは、以下の方を対象読者として想定している。

対象組織：業務目的で、スマートフォンを利用する法人（企業・団体・組織）

対象読者：(1)企業や組織においてスマートフォンを導入・運用する責任者・担当者

(2)企業や組織においてスマートフォンを導入する際にセキュリティポリシーを策定する責任者・担当者

1.3 本ガイドの構成について

本ガイドでは、スマートフォンの効果的な管理とセキュリティ管理に資するＭＤＭについて、その導入時の検討事項および運用上の留意点等を以下の構成で記述しています。

2章では、スマートフォンの特徴やＭＤＭの導入目的、期待する効果について述べます。

3章では、ＭＤＭの概要ならびにＭＤＭに望まれる機能要件を整理しています。

4章では、MDMの導入・運用にあたり考慮すべきポイントについて説明します。

最後の5章では、導入目的から機能を選択する際のチェックリストとして、MDM機能要件一覧表を付しています。

1.4 用語集

本ガイドで使用される用語の意味は以下のとおりである。

表1-1 用語集

用語	解説
MDM	移動する端末をリモートから一元管理するシステムの総称。
クラウド型	企業や組織の社外で提供されるインターネットを介したシステム形態。
オンプレミス型	企業や組織の社内にネットワーク機器やサーバ等を構築して提供されるシステム形態。
セキュリティポリシー	企業や組織全体の情報セキュリティに関する基本方針。広義では、セキュリティ対策基準や個別の具体的な実施手順なども含む。
BYOD	「Bring Your Own Device」の略称で、私物の端末を企業や組織内に持ち込み、業務利用する行為のこと。
SMS	「Short Message Service」の略称で、携帯電話会社によって提供される短いメッセージを送受信するサービスであり、これによりシステム制御も可能である。
リモートロック	リモートから端末の操作を制限する仕組み。
リモートワイプ	リモートから端末上のデータを消去する仕組み。
Bluetooth	携帯機器などで数m程度の機器間接続に使われる短距離無線の通信技術。
スクリーンショット	表示画面の画像を取得して取り込む機能。
Wi-Fi	Wireless Fidelityの略で、Wi-Fi Alliance によって無線LAN機器間の相互接続性を認証されたことを示す名称。
NFC	Near Field Communicationの略で、十数センチの近距離無線通信技術の国際規格。
FeliCa	ソニー株式会社が開発した非接触型ICカードの技術方式。
ワンセグ	携帯電話・移動端末向けの1セグメントによるTV受信サービス。
UIMカード	携帯電話会社が発行する、契約者情報を記録したICカード。

2 スマートフォンとＭＤＭ

ＭＤＭの導入に際し、自社に適した製品･サービスの選定を行うためには、まずスマートフォンの特徴を知る必要がある。

この章では、従来の携帯電話と比較したスマートフォンの特徴と、一般的なＭＤＭの導入目的について解説する。

2.1 スマートフォンの特徴について

2011年末時点で、企業契約の携帯電話は1,000万回線をこえていると言われ、企業における業務利用目的での携帯電話の配布が進んでいる。

企業において、業務用携帯電話の資産管理は主に総務部等で行われてきたが、PCと同様の機能を持つスマートフォンの場合、セキュリティリスクを緩和するため、情報システム部門で管理されるケースが増えている。

以下は、携帯電話とは異なるスマートフォンの特徴である。

① 従来の携帯電話会社の通信網に加え、公衆Wi-Fiスポット等を経由したインターネット接続が可能でありインターネットへの接続手段が多彩である。

② 日本国内に特有なＯＳを搭載した端末から、世界共通ＯＳを搭載した端末へと変化している。

③ 世界共通ＯＳであることから、アプリケーション開発者がグローバル規模で拡大。開発されたアプリケーションはマーケットと呼ばれる掲載サイトに集積され、ユーザはここにアクセスしてアプリケーションをダウンロードすることで、容易に端末のカスタマイズが可能。

スマートフォンはインターネットへの接続や、インターネット上でのサービス利用をユーザにとってより使いやすいものにする一方で、企業のIT管理者からみれば、考慮すべき管理ポイントを増加させるため、スマートフォンを業務利用するにあたっては、その特徴を加味したセキュリティ管理･資産管理を行わなくてはならない。

2.2 ＭＤＭの導入目的について

企業が業務用にIT機器を配布する場合、IT管理者にはそれを適切に管理･運用することが求められる。配布時はもとより、配布後も企業が定めた運用ポリシーが守られているかを監視し、運用ポリシーに変更を生じた際には速やかにその内容を機器に反映しなくてはならない。

特に使用場所が固定されないモバイル機器においては、こうした管理を効率的に行うことが難しくなるため、IT管理者が遠隔モバイル機器を管理する仕組み、つまりＭＤＭが必要となる。

スマートフォン利用時にＭＤＭで実現したい目的とその期待する効果をまとめると表2-1のようになる。

なお、この導入の目的および期待する効果についてはあくまで一般論であり、すべての導入企業において当てはまるものではない。

表2-1 一般的なＭＤＭの導入目的と期待する効果

項番	導入目的と期待する効果
1	端末新規配布時に必要な各種設定や、配布後の設定変更を、簡便かつ迅速に行い、大量の端末を一元管理したい。
2	企業の情報資産の漏えい・持ち出しを防ぐため、端末に機能制限を施したい。
3	資産管理の側面から、端末種類、OS種別、利用アプリケーション種別等を管理したい。
4	企業のセキュリティポリシーに基づいた端末設定を徹底したい。また、端末を企業のポリシーに沿って適切に使用させ、またその確認のため、デバイスの状態・使用状況・使用者を把握したい。
5	端末の紛失・盗難時、企業として保護すべき情報が端末から漏えいすることを防ぎたい。
6	マルウェアへの感染によって、企業として保護すべき情報が端末から漏えいすることを防ぎたい。
7	端末のデータ資産を適切に保護・保全したい。
8	端末の法人契約（企業資産）、個人契約（BYOD）を明確にし、端末の利用者を正確に把握したい。

3 MDMの概要

本章では、MDM製品・サービスの導入検討にあたり、企業の導入目的に応じた機能要件を概説する。

3.1節でMDMサービスの提供形態、3.2節でMDMサーバと端末間の通信方式、3.3節ではMDMの機能内容を機能分類別に解説する。

また、3.4節では、その他MDMの特徴として留意すべき項目について言及し、最後に3.5節でMDMサービス・製品の傾向を述べる。

3.1 MDMの提供形態

MDMは基本的に、「管理主体となるMDMサーバ」と「管理対象となる端末」から成る。MDMサービスの提供形態は、次の2パターンに大別される。

表3-1 MDMの提供形態

提供形態		特長
クラウド型	MDMサーバがクラウド側に構築され、これをサービスとして提供されるパターン	複数企業への共用サービスとなるので個別要求に応えにくく、画一的なサービスメニューの範囲での利用に限定される。また、運用管理やセキュリティポリシーコントロールの自由度にやや課題が残る。 ただし、初期費用を安く抑えられることで導入へのハードルが低く、管理上の運用負荷が小さいなどのメリットが考えられる。
オンプレミス型	MDMサーバが製品として提供され、自営で構築・運用するパターン	画一的なメニューでなく、ユーザ企業の独自なセキュリティポリシーに応じた運用管理を行うことができる。 また、基幹システムやユーザディレクトリとの連携性を確保しやすい。 スマートフォン接続環境を閉域網ネットワークで構築する場合にはオンプレミス型による提供形態が適している。

MDMベンダーによって、両方の提供形態をサポートしている場合、何れかの提供形態のみをサポートしている場合に分かれる。

3.2 ＭＤＭの通信方式

通常は、運用管理者がＭＤＭサーバから制御コマンドを送り、該当の端末がＭＤＭサーバと通信することで制御コマンドが反映される。

運用管理者が送る制御コマンドは、次の通信方式で端末へ伝達される。

表3-2 ＭＤＭの通信方式

通信方式		特長
SMS方式	プッシュ方式	携帯電話事業者が提供するSMSを利用して、該当の端末にＭＤＭサーバへ接続するようメッセージ送信を行う方式。 この方法は必要に応じて端末を呼び出すことができ、かつ定期的な同期を必要としないため、即時性やバッテリー消費面からもより効率的と言える。
電話着信方式	プッシュ方式	事前登録された特定の電話番号から、管理対象端末が一定時間内に一定回数の着信を受けた場合にその端末を制御する仕組み。
OSベンダー提供方式	プッシュ方式	OSベンダーが提供するメッセージプッシュシステムを介して、該当の端末にＭＤＭサーバへ接続するようメッセージの送信を行う方式。 代表的な方式として、Apple社がiOS向けに提供するAPNs (Apple Push Notification Server) 、ならびにGoogle社がAndroid向けに提供するC2DM (Cloud to Device Messaging) やGCM (Google Cloud Messaging for Android) がある。 この方法は必要に応じて端末を呼び出すことができ、かつ定期的な同期を必要としないため、即時性やバッテリー消費面からもより効率的と言える。
ポーリング方式	プル方式	端末側のエージェントが一定間隔でＭＤＭサーバへ問い合わせすることで制御コマンドを発行する方式。 同期間隔を短くすると通信料が増えるためバッテリー消費が多くなり、間隔を長くするとコマンド反映 (処置適用) に時間がかかるため、同期間隔のチューニングには端末スペックにより個体差を配慮することが望ましい。 SIMを搭載しないWi-Fi接続端末でも有効な方式であり、スマートフォン、タブレットを問わず一元的な管理が可能な方式。 閉域網ネットワークでも有効な手段で、クライアントから定期的にサーバに情報を上げることも一種のポーリング方式といえ、SMS方式やOSベンダー提供方式とも共存できる手法。

運用管理者が制御コマンドを送った時点ですぐに端末へ反映されるプッシュ方式に対して、プル方式は保険的な役割を担う。

スマートフォンは様々なネットワーク状況下で利用されることが想定されるため、複数の通信方式を組み合わせることで制御コマンド送信の成功率を向上しているＭＤＭもある。

3.3 ＭＤＭの機能

3.3.1 ＭＤＭの導入目的と機能要件

ＭＤＭ製品の導入にあたり最も重要な事は目的、すなわちＭＤＭの導入によりどのような事を達成したいのかを明確にすることである。これによって、必要機能の見極めが可能となる。

既に2.2節で一般的なＭＤＭの導入目的と期待する効果を述べたが、本項では、その導入目的を達成するために必要となる機能要件を表3-3にまとめた。なお、この一覧はあくまで現時点での一般的な分類であり、導入企業の個別事情に応じてそれぞれ異なる優先度を持った複数の導入目的や機能要件が存在し、また一覧に記載されていない項目があることも想定している。

表3-3 ＭＤＭの導入目的と機能要件

項番	導入目的	機能要件
1	端末新規配布時に必要な各種設定や、配布後の設定変更を、簡便かつ迅速に行い、大量の端末を一元管理したい。	資産管理 遠隔ポリシー設定・実行 アプリケーション配信・削除
2	企業の情報資産の漏えい・持ち出しを防ぐため、端末に機能制限を施したい。	デバイス制御 遠隔ポリシー設定・実行 フィルタリング機能の管理
3	資産管理の側面から、端末種類、OS種別、利用アプリケーション種別等を管理したい。	資産管理
4	企業のセキュリティポリシーに基づいた端末設定を徹底したい。また、端末を企業のポリシーに沿って適切に使用させ、またその確認のため、デバイスの状態・使用状況・使用者を把握したい。	遠隔ポリシー設定・実行 アプリケーション利用制限 業務アプリケーション保護 悪性Webサイトへのアクセス制御 遠隔監視
5	端末の紛失・盗難時、企業として保護すべき情報が端末から漏えいすることを防ぎたい。	リモートロック リモートワイプ 暗号化
6	マルウェアへの感染によって、企業として保護すべき情報が端末から漏えいすることを防ぎたい。	マルウェア対策ソフトウェア管理 暗号化
7	端末のデータ資産を適切に保護・保全したい。	バックアップ リストア
8	端末の法人契約（企業資産）、個人契約（BYOD）を明確にし、端末の利用者を正確に把握したい。	資産管理 遠隔監視

次節以降ではＭＤＭ選定にあたり、上記機能要件を実現するために必要となるＭＤＭの諸機能について述べる。

3.3.2 端末管理

スマートフォン等の端末は圧倒的なモビリティを有するため、端末の盗難・紛失時の対策としてのリモートロック／リモートワイプ機能、その他以下に示すようなデータ保護のための暗号化機能、不正利用対策としてのデバイス利用制限機能、遠隔監視、遠隔ポリシー設定・実行機能、および資産管理機能などの端末管理機能が要求される。

表3-4 端末管理機能（1／2）

機能要件	項番	機能内容
リモートロック	1	端末個体ごとのロック・アンロック
リモートワイプ	2	全データ削除
	3	個別データ／特定フォルダ削除※ （電話番号、メールアドレス等のアプリケーション毎のデータ、ブラウザ等のキャッシュ、各種ログ等）
暗号化	4	保存領域の暗号化／復号
	5	外部メモリ（SDカード等）の暗号化／復号
	6	個別データの暗号化／復号※（但し、SDカードはシステム権限不要）
デバイス制御	7	カメラ
	8	スクリーンショット※
	9	Bluetooth
	10	外部メモリ（SDカードなど）※
	11	無線LAN（WiFi）
	12	USB※
	13	赤外線通信※
	14	NFC(Near Field Communication) ISO/IEC 21481
	15	FeliCa、ISO/IEC 14443（MIFARE）※
	16	ワンセグ※
	17	UIMカードメモリ※
	18	発信先制限
遠隔監視	19	端末状態の情報取得 起動確認、起動中アプリ、コンプライアンス違反状態等の端末側情報の取得とアップロード OS、インストール済みアプリケーションのバージョン管理
	20	死活監視 活性化状態（主にネットワーク接続状態）の取得とアップロード
	21	ログ収集 システムログ、操作ログ、アプリ起動ログ等の取得とアップロード
	22	位置情報取得 GPS追跡機能など
	23	アラートメール送信 管理者への通知機能、利用者への警告機能
	24	レポート出力 監視、制御、運用状況のレポート
遠隔ポリシ設定・実行	25	パスワードのポリシー設定 文字複雑性維持、初期パスワード強制変更、有効期限設定、最低利用日数設定、パスワード履歴管理（直近パスワード使用禁止：通常3サイクル） （プラットフォームによって、実装可能な機能は異なる）
	26	MDMのポリシー設定 リモートロックやワイプ、デバイス制御などのMDM動作を規定する設定情報の適用とポリシー外設定の強制復帰
	27	端末の構成設定※ メールサーバーやVPN/WiFiなどの設定情報や証明書ファイルの適用

※印は実現にあたり、端末への組み込みによる制御（システム領域でのシステム権限付与による制御）を要すると考えられるもの。

表3-4 端末管理機能（2／2）

機能要件	項番	機能内容
資産管理	28	端末の数量管理 個体情報（機種、電話番号等）管理
	29	ソフトウェアの数量管理 ソフトウェアの種類（OSの名称、アプリケーションの名称、それらのバージョン等）の管理
	30	所有者属性の管理（部門名、社員番号、指名等）

3.3.3 アプリケーション管理

マーケットから簡単にアプリをダウンロード／インストールできるスマートフォンでは、適正なアプリの確実な配信管理や業務外アプリのインストール／利用制限機能が要求される。

便利なアプリが豊富にある反面、不正なアプリ、正規のアプリを偽装した不正アプリ、情報漏えいの可能性があるセキュリティ設計考慮漏れのアプリなど、セキュリティリスクのあるアプリを排除する必要がある。

これら機能による処理内容に関するログは適切に記録されることが望ましい。特に不正アプリ等が検知された場合、ログを記録するとともに、利用者や管理者に通知され、適切な処理がなされることが必要である。

表3-5 アプリケーションの管理

機能要件	項番	機能内容
配信・削除	1	自社アプリケーションの配信とインストール※
	2	推奨アプリケーションリスト（ホワイトリスト）の配信
	3	アプリケーションの遠隔削除※
業務アプリケーションの保護	4	会社公認アプリケーションの保護※ アンインストールならびに不正終了防止
アプリケーションの利用制限	5	会社非公認アプリケーションのインストール制限もしくは強制終了（ホワイトリスト方式）
	6	会社非公認アプリケーションのインストール制限もしくは強制終了（ブラックリスト方式）
	7	ＵＳＢ／ＳＤカード経由のアプリケーションのインストール抑止※
	8	アプリケーションのパーミッション制御※

※印は実現にあたり、端末への組み込みによる制御（システム領域でのシステム権限付与による制御）を要すると考えられるもの。

3.3.4 ＭＤＭサーバ～端末間の認証および信頼経路の確立

端末をＭＤＭサーバの管理下におくため、各端末側では「アクティベーション」という作業を実施する。運用管理者は、アクティベーションに必要なソフトウェア（ＭＤＭエージェント）や証明書の取得方法を通知し、端末へＭＤＭエージェントのインストールを促す。所定のソフトウェアや証明書をインストールすることで端末のアクティベーションが完了し、以降のＭＤＭサーバ～端末間の通信は、安全な経路が確立された状態で行われる。

表3-6 ＭＤＭサーバ～端末間の認証および信頼経路の確立

機能要件	項番	機能内容
MDMエージェントの正しいインストール	1	エージェントインストール時の認証 （端末証明書またはID／パスワードによる端末認証、利用者認証）
高信頼経路による接続	2	VPN、SSLなど
MDMエージェントの保護	3	MDMエージェントのアンインストール抑止※

※印は実現にあたり、端末への組み込みによる制御（システム領域でのシステム権限付与による制御）を要すると考えられるもの。

3.3.5 フィルタリング機能の管理

スマートフォンからインターネット接続する際には、不正サイトへのアクセス誘導を防止するためにWebフィルタリング機能が要求される。Webフィルタリング機能には、接続先Webサイトの安全性を判定し、安全でない場合には通知、遮断したり、接続先Webサイトが特定のカテゴリに属する場合には通知、遮断したりするような機能が含まれる。

また、業務を阻害するスパムメール、着信スパムやSMSスパム等を判定・除去するフィルタリング機能が必要である。

これらフィルタリング機能を状況に応じて設定・変更・解除する機能が必要である。

表3-7 フィルタリング機能の管理

機能要件	項番	機能内容
悪性Webサイトへのアクセス制御	1	Webフィルタリング（ホワイトリスト方式、ブラックリスト方式）
スパムメール除去	2	メールフィルタリング
着信スパム、SMSスパム除去	3	着信拒否／SMS着信拒否※

※印は実現にあたり、端末への組み込みによる制御（システム領域でのシステム権限付与による制御）を要すると考えられるもの。

3.3.6 マルウェア対策ソフトウェアの管理

インターネットに接続し、マーケットからアプリをダウンロードする端末は、常に不正ウィルスやマルウェア、および不正アプリに汚染されるリスクを有するため、これらを防止するマルウェア対策ソフトウェア機能を端末ごとに導入する傾向にある。ＭＤＭでは、それらマルウェア対策ソフトウェアのポリシーや動作結果の監視などの管理機能が要求される。

表3-8 マルウェア対策ソフトウェアの管理

機能要件	項番	機能内容
遠隔監視	1	ソフトウェア状態およびログの収集 ソフトウェア／エンジン／パターンファイルのバージョン、最後のスキャン時間、最後に駆除したウィルス数等の情報の取得とアップロード
バージョン管理・更新	2	パターンファイル更新の要求
	3	スキャン実行の要求
遠隔ポリシ設定・実行およびスキャン実行	4	ポリシー設定 パターンファイルの自動更新スケジュール、スキャンの自動実行スケジュールなどの一括適用

3.3.7 バックアップ機能

スマートフォンの機種変更、盗難・紛失や故障、または災害の際、全ての重要な情報およびアプリケーションの回復を迅速・確実にするために、適切なバックアップ機能が要求される。

計画した時間に復旧に必要なデータを保存期間と保存条件を定義してバックアップでき、かつ必ずリストアできることが肝要である。

表3-9 バックアップ機能

機能要件	項番	機能内容
端末データのバックアップ	1	端末復旧に必要なデータの定期的、個別的バックアップ※
端末データのリストア	2	各種データの復旧※

※印は実現にあたり、端末への組み込みによる制御（システム領域でのシステム権限付与による制御）を要すると考えられるもの。

3.4 その他

3.4.1 OSの相違によるＭＤＭエージェントの挙動

OSの違いによる、ＭＤＭの特徴を表3-10にまとめた。

表3-10 OSの相違によるＭＤＭエージェントの挙動

	iOS	Android
MDM API	OS標準でMDM向けAPIを提供しており、MDMサーバが発行した制御コマンドを当該APIを通じて構成プロファイルに反映することで、MDMを成立。	OS標準で提供されるMDM向けAPIは少ない。 ただし、アプリケーションからは（ユーザ承認に基づき）広範な端末機能を利用することができる
管理方法	MDM用構成プロファイルを当該端末へインストールすることで実現。 MDM用構成プロファイルは、端末側で削除可能なため、容易にＭＤＭの管理下から抜け出ることが出来る。このため端末がＭＤＭ管理外となった場合に検知できる仕組みを備えることが重要になる。	MDMエージェントアプリケーションを活用することが一般的。 MDMエージェントアプリケーションは、端末側で削除可能なため、削除できない仕組みを備えたり、削除を検知できる仕組みを備えていることが重要になる。
MDMの特色	ＭＤＭ向けAPIは固定的であり、各ベンダーから提供されるＭＤＭは本質的には共通のものとなる。	利用する端末機能によって、さまざまなＭＤＭ機能が提供できるため、ベンダーの工夫次第で独自性のあるＭＤＭ製品・サービスを提供することが可能となる。

3.5 ＭＤＭサービス・製品の傾向

ＭＤＭには多数の提供形態がある。主にはキャリア通信会社とセキュリティベンダー、その他のMDMソリューションベンダーに大別できる。

以下に、これらの特徴と導入時の留意点を示す。

3.5.1 キャリア通信会社

キャリア通信各社が提供する携帯電話、スマートフォン向けの管理サービスで、死活監視、紛失・盗難対策やサービス利用制限などを主としたものを法人契約単位で提供する。

自社が販売する端末のコントロールのみをサポートしているのが特長。企業内で管理する端末が複数存在する場合、セキュリティポリシーの統一が困難な場合もあり、マルチキャリアでの運用管理を必要とする複雑な組織の場合は、利用できるサービス内容に制約されることが課題といえる。

通信方式は、SMSプッシュ方式を採用しており、3G回線のSIM搭載端末が前提となるケースが多い。そのため、Wi-Fi接続専用端末の場合、利用が困難なサービスもある。

3.5.2 セキュリティベンダー

ウィルス対策ソリューションなどのセキュリティベンダーが提供するサービスで、スマートフォン（主にiOS、Android端末）の遠隔制御・管理を実現する。

ウィルス感染した端末のロックやウィルス対策エンジンのアップデート機能を発展させ、紛失・盗難対策のためのロック、ワイプ機能が拡張された形が一般的である。

ターゲットが個人ユーザ向け（コンシューマサービス）なため、法人利用視点の管理機能よりも、端末単体で利用する機能が充実している。

通信方式は、主にSMSプッシュ方式、または独自のクライアントエージェント方式による認証検疫のローカルアプリケーションで実現するサービスである。

3.5.3 その他のMDMソリューションベンダー

スマートフォンからタブレットまでキャリア・プラットフォームに依存しないマルチ端末対応を掲げた様々なサービスが展開されている。

端末ベンダーが提供するサービスは、端末やサービスの販売をグループ企業内で完結する利点を生かして、端末機能との独自連携や付加価値機能が備わったサービスが特長。MDMエージェントをプリインストールした機種やモデルも登場し、端末導入時のキッティング負荷を軽減するメリットもある。

資産管理セキュリティ製品から発展したサービスは、パソコンの端末管理機能同様に、スマートフォンへも機能拡張されたもの。セキュリティポリシー管理は、既存パソコンの管理と一元的に行え、組織階層化したポリシーコントロールが適用可能なソリューションもある。

また、前述の様々なMDMサービス・製品のOEM提供を受け独自のサービスに仕立て上げているクラウド型や、端末のキッティングからMDMサービスのオンプレミス型構築、MDM運用支援までをトータルにサポートするシステムインテグレータなどが存在する。

通信方式は、いずれも独自のアプリケーションを実装したエージェント型の通信方式が多く見受けられる。SIMが搭載されていないタブレットや構内無線ＬＡＮへのWi-Fi接続端末にもMDM側からのコントロールが可能となるため、対象となる端末の適用範囲を広範に設定できる。

4 ＭＤＭ導入･運用ガイド

本章では、ＭＤＭ製品を導入･運用するにあたり、配慮すべき事項を提言する。

4.1節で導入にあたり必要な検討事項、4.2節で導入準備、4.3節でＭＤＭからのアクティベーション、4.4節で端末運用管理、4.5節で紛失盗難対策や緊急時対策、4.6節で端末の廃棄など、ライサイクルの各フェーズにおけるＭＤＭ側運用管理面での配慮すべき事項を解説する。

ただし、ＭＤＭのサービスプロバイダーやソリューションベンダーのサービスや製品固有の機能により全てを期待するものではなく、また、導入するスマートフォンの機種特性やネットワーク接続環境により、利用できるセキュリティコントロールの機能が異なるものと想定されるので、ここではあくまで、各運用フェーズでのセキュリティレベル向上のために必要な重要事項を述べ、導入要件の検討に配慮すべき企業のセキュリティポリシーとＭＤＭ運用管理の要件を結びつける参考とされたい。

4.1 導入にあたり検討が必要な事項について

ビジネスユーザにとって、業務利用の効率性や利便性の向上を目的に組織的に利用するシステムへの接続利用の要求が高まるが、企業内ネットワークへの接続には、既存システムにおける従来のＰＣを対象としたセキュリティポリシーや権限認証によるシステム利用の制限を設けているため簡単に接続できない場合が多い。

特に外部接続にはハッキングやマルウェア対策、サイバー攻撃などの対策を講じたシステムがあり、モバイル端末からの接続性に制限をかけるケースが殆どである。このため、従来のＰＣからのモバイル接続のネットワーク環境の既存設備のままでは、スマートフォンからの接続が困難なケースが多い。対策として、4.1.1項で述べるライフサイクル全般に亘って4.2節以降の考察と検討を行い、ＭＤＭによって制御されたセキュリティポリシーを確保できる端末環境での接続を認める仕組みを準備する必要性がある。

4.1.1 MDMライフサイクル

スマートフォンに対するMDM利用においても、要求に応じてシステムを企画し、導入、運営･保守を経て最終的に破棄される情報システムとしての各フェーズがあり、企業のポリシーにマッチした適切な管理コントロールを、適切な時期に、適切なコストで提供する事は、技術的･環境的変化の激しいスマートフォンであっても従来の情報システム構築と同様である。従って、この一連の流れをライフサイクルとして捉え運用して行く事は、企業によるスマートフォンの利用に際して有効に作用するものと期待できる。

4.1.1.1. MDMライフサイクルの各フェーズ

スマートフォンにおけるMDMライフサイクルの基本的なフェーズは、企画、調達、導入、運用、終了の5つである。これに加え、小型デバイスであるが故に、紛失し易いという特性を加味し特殊フェーズとしての「インシデント発生」を加え、6つのフェーズで構成している。

- 企画

  MDM導入の目的、目標を達成するために必要とされるシステムへの要求事項をまとめ、実施計画を策定する。

- 調達

  新しく構築するシステムの仕様を明確化し、ネットワーク回線・機器・ソフトウェア等の選定を経て実際のシステムを調達する。

- 導入

  MDMを実際の情報システムに導入する。このフェーズでは導入する端末をシステムに登録し、ユーザに引き渡すまでを考慮する。

- 運用

  当初の目的の環境で、MDMシステムを運用する。

- インシデント発生

  ここで想定されるインシデントの発生は紛失・盗難である。MDMを適切に運用している場合、インシデントが発生したデバイスに対してリモートでロックやワイプ等が可能であり、また現在のおおよその位置を把握する事が可能であるなど、発見・回収できる確立が高くなると考えられる。回収できたデバイスについては運用フェーズへ、また回収できなかったデバイスについてはデバイス自体の終了のプロセスへ移る事となる。

- 終了

  デバイスに対してデータの消去指示を行い、完了後、デバイスの管理登録を抹消する。

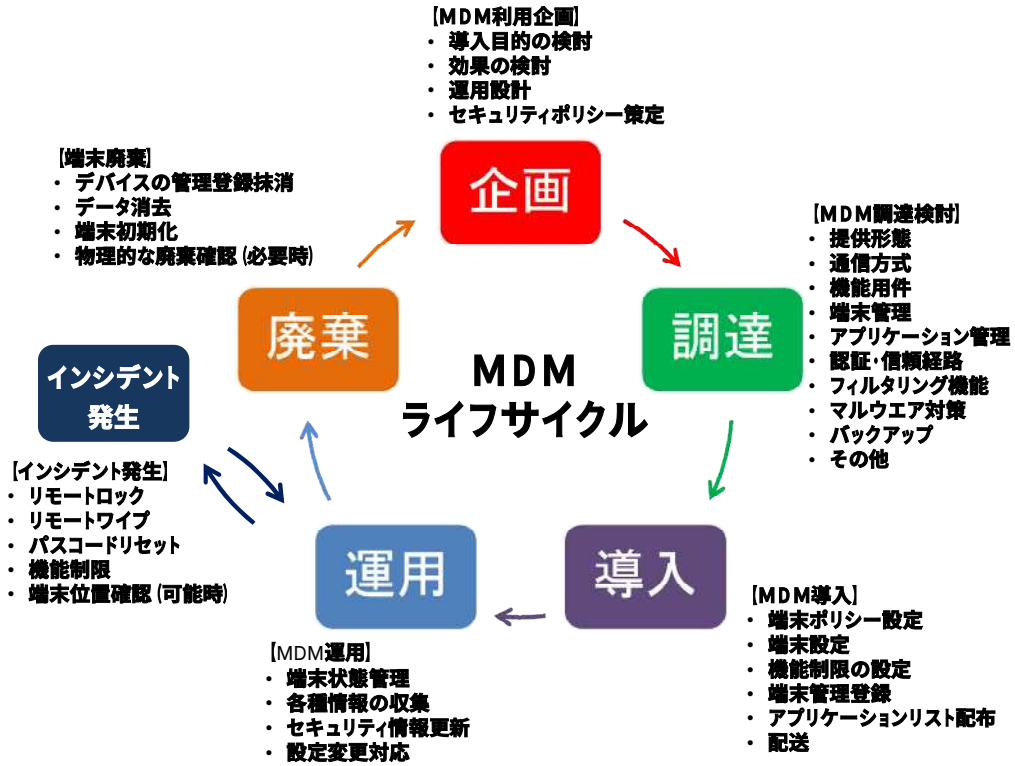


図4-1 MDMライフサイクル

4.1.2 適用条件の検討

導入検討のための条件として、主には以下の条件を検討する必要がある。

表4-1 導入検討のための条件

項番	導入検討のための条件
1	管理端末の範囲（携帯電話、スマートフォン、タブレット）
2	接続条件の範囲（キャリア通信、Wi-Fi通信、構内無線LAN）
3	接続エリアの範囲（社内、国内地域、海外）
4	端末台数規模（初期段階と端末増加見通しを段階的スケール）
5	適用端末機種種別（導入済み、新規取得を含め管理すべき端末種別の把握）
6	監視対象端末搭載のOS（管理対象端末のOS種別と単一か混在か等）
7	組織契約端末（契約主体による条件）、個人契約端末（BYOD）の範囲
8	管理対象の端末のセキュリティポリシールールのパターン化
9	セキュリティポリシーパターンの組織階層化（企業内グループ管理の必要性）

これらの条件項目は、MDMのサービス形態によって端末監視対象の制約となることも想定されるため、導入方針を検討するうえでは重要な要素である。

4.2 MDMによるスマートフォンの導入準備

4.2.1 ユーザ企業のサービス加入と認証登録

MDMサービスへの端末の認証登録が必要になるので、管理対象となる端末と使用者を特定し、認証登録を行う。

導入企業側では、利用シーンに応じたセキュリティポリシーを組織階層ごとに設定する必要があり、端末側での操作者のセキュリティポリシー設定の変更を許可するか否かも含めた以下のポリシー検討が必要である。

表4-2 ポリシー検討事項

項番	検討事項
1	組織階層別のセキュリティポリシーのテンプレート化
2	端末管理者と使用者の設定変更権限の範囲
3	デジタル証明書認証または、クライアントアプリケーションによる認証などMDM認証手順の明確化とルート証明の端末への配備を計画化（MDMクライアントアプリケーションのインストール手順による）
4	利用シーンごとの通信手段（社外：3GまたはWi-Fi、社内：社内無線LAN）の明確化し、MDM認証時のアクティベーションを円滑化

4.2.2 初期設定時のセキュリティ

ＭＤＭ利用のセキュリティ機能実装が端末依存している場合もあり、機種ごとのセキュリティポリシーのコントロール可能な範囲を特定し、サンプルとなる機種でのセキュリティポリシーパラメータを予め検討しておく必要がある。

ほとんどのＭＤＭソリューションがセキュリティポリシーパラメータの一括設定の機能を有している。多数の機種で大量のＭＤＭコントロールを行う必要があるため、セキュリティポリシーパラメータのテンプレート登録機能を利用して一括設定を行う。

ポリシーパラメータのテンプレートは組織階層化およびグループ化できるので、管理効率向上のため利用シーンごとに組織グループ別のパラメータテンプレートを準備することが望ましい。

表4-3 パラメータテンプレートの検討（例）

項番	検討事項
1	営業職向け外部接続専用端末向けテンプレート
2	社内スタッフ（構内作業員）向けテンプレート
3	個人所有端末（ＢＹＯＤ）テンプレート
4	サービス専用端末（セルフオーダリング専用端末、ＧＯＴ発注端末等）

端末ごとの権限による例外設定を許可する場合は、テンプレートによる標準設定と固体ごとの例外設定のパラメータを整理しておく必要がある。これらは、企業利用の場合、使用者の使い廻しによる不正利用の防止と混乱を防ぐため重要である。

設定変更のログを追跡することで、不正利用者の端末を特定する場合もあり、初期値と操作者変更の履歴を管理し、不測の事態（紛失盗難、不正利用発覚）に追跡調査が可能なように設定変更ログを適切に管理する。

4.2.3 アクティベーションとポリシーパラメータ配信による一括設定

ＭＤＭ管理対象となる端末の基礎情報をＭＤＭサービス側へ事前登録し、端末側のアクティベーションを行うが、サービス形態により手順が異なる。

4.2.3.1. キャリア通信サービス

キャリア通信サービス事業者が予めルート証明書をインポートした端末でプリインストール済のアプリケーションのアクティベーションを、ＭＤＭ側からのコントロールで行うサービスが多い。

4.2.3.2. セキュリティベンダーサービスまたはオンプレミス型サービス

端末側でＭＤＭエージェントをインストール後、ＭＤＭサービスへのアクティベーションの認証を行い、ＭＤＭ管理対象の端末として登録される。

アクティベーションが完了した端末には、ＭＤＭサーバ側から端末の基礎情報取得後にセキュリティパラメータの一括配信により、設定変更を行う。

利用端末ごとに、使用者が企業内への接続ポリシーを個人で初期設定する場合、セキュリティポリシーパラメータの徹底が困難なため、企業側で準備したセキュリティポリシーパラメータテンプレートの一括配信と設定を誘導させる必要がある。

この場合、セキュリティ管理者権限で強制的に変更する場合と基本的な初期設定のみの制御で操作者が独自にマニュアル（手順書）で初期設定する場合とを企業側が明快に周知する必要があるので留意する。例えば、ＭＤＭエージェントのアンインストールやポーリング条件等、例外的な利用を必要とするような組織内のセキュリティテンプレートと異なる設定で運用したい場合、ポリシー条件を独自に変更し

ても、次回の更新タイミングで強制的に戻されてしまう。、そのため、MDM管理者側で個別のパラメータ設定を行なうなど、設定条件のMDMサーバ側と個人操作の設定の重複を避けるための整合を図ることが肝要である。

また、端末の機種特性によりMDMサーバ側からのセキュリティパラメータの強制的な変更ができる項目が異なる場合があるため、事前に評価機での検証を行い、テンプレート配信や強制的なパラメータ変更、ロックやワイプの挙動などMDMサーバ側からの制御を機種別に検証しておくことが望ましい。

4.3 MDMサーバからの端末アクティベーション

MDMサーバから制御できる端末にするためには、導入形態により以下の方法があり、導入企業の選択するソリューションの導入手順によって、それぞれ準備の進め方が異なる。

4.3.1 キャリアサービスを利用する場合

法人契約の端末を特定し、回線契約単位ごとにサービス加入を行う。この場合、MDMサーバの制御配下となるようにアクティベーションを行うのはキャリア通信会社である。

SIM搭載の端末で加入契約後にキャリア通信会社側からのSMSによるサービス加入の同意とアクティベーションを行う。端末（スマートフォンやタブレット）側の認証登録を行うサイト誘導によるアクティベーションやMDMエージェントのインストールはキャリア通信会社のサービス内容によって異なるため、企業情報システム部門から端末使用者への事前の周知が必要となる。

4.3.2 クラウドサービスを利用する場合

利用企業側から、クラウドサービスでMDM制御する端末のプロファイル情報をクラウドサービス企業へ提供しアクティベーションを行う。

端末側へは、アクティベーションに必要なソフトウェア（MDMエージェントを含む）の配布方法を明確にし、使用者へ通知して社内ダウンロードサイトまたはクラウドサービス加入ダウンロードへ誘導し、MDMエージェントのインストールを強制する。

インストール時のアクティベーションチェックでクラウドサービス会社への初期セットアップとセキュリティポリシーパラメータの更新がMDMエージェントによって実施されることになる。

4.3.3 オンプレミス型の独自導入を利用する場合

社員向けのサイトサービスとして、自社内サーバ環境、または、ホスティングサービス環境にMDMソリューションを独自に導入し、業務利用する端末（スマートフォンやタブレット）の初期登録を行う。

端末側へは、アクティベーションに必要なソフトウェア（MDMエージェントを含む）の配布方法を明確にし、使用者へ通知して社内ダウンロードサイトまたはクラウドサービス加入ダウンロードへ誘導し、MDMエージェントのインストールを強制する。

インストール時のアクティベーションチェックでは、独自構築したソリューションに登録したセキュリティパラメータのテンプレートを利用して初期セットアップとセキュリティポリシーパラメータの更新がMDMエージェントによって実施されることになる。

大規模組織での利用には、組織階層や部門によって、ネットワーク接続先やセキュリティポリシー、端末利用制限を異なるパターンで利用制限を施す必要がある。組織階層ごとにセキュリティポリシー変更権限を各組織別に準備する必要があり、これらの権限管理やパラメータパターンテンプレート管理できるには、MDMサーバ上で使用者プロファイルのグループ階層管理の機能を実装し、権限ロールを利用できるMDM製品が望ましいことになる。

この点、独自構築のＭＤＭの場合、システムのバックボーンの発展に合わせて、セキュリティポリシーを拡大し、適用パターンや適用対象を拡大できる計画化ができることになるので、ＭＤＭ側のフレキシビリティや標準化にはオンプレミス型独自構築は、有効といえる。

大規模組織で利用シーンや使用者の組織ごとにセキュリティポリシーが異なる管理を行う必要がある場合は、重要な要素といえる。

4.3.4 ＢＹＯＤ (Bring In Your Device) ポリシーと検疫

個人契約の端末を会社利用に使う (BYOD) 場合、セキュリティポリシーの設定状況や個人情報や企業機密情報の漏洩対策のための対処がなされているかをチェックし認証時に検疫するＢＹＯＤの仕組みを導入することが望ましい。

ＭＤＭによる制御は、個人所有の端末を利用する場合のセキュリティポリシーのルール化と所有者本人の同意を前提としたセキュリティ対策がとられているか否かを監視する仕組みを設け、必要時監視される端末となることを所有者が容認することが前提となる、

表4-4 BYODでの検疫チェックの主な要素

項番	BYODでの検疫チェック要素
1	ソフト (特にウィルス･マルウェア対策) のバージョンチェック
2	企業接続のための端末側ソフト (VPN関連ツール) と接続方式の指定
3	VPN接続用の電子証明書の要否
4	端末の保有するソフトウェアのブラックリスト、ホワイトリスト
5	データの保管状況
6	暗号化対策状況

通常の業務利用PCのセキュリティポリシーにおけるネットワーク利用上の運用ポリシーに合わせ、ＭＤＭによる管理を義務化するためのルールと周知策を上述の検疫チェックの条件と合わせて検討することが望ましい。

また、上述の一部の状況把握はＭＤＭサーバからの端末アクティベーション時に端末状態の取得を行うことで認証チェックできるＭＤＭソリューションもある。

また、これらの機能を利用してＭＤＭサーバ側からチェックしてセキュリティパラメータを強制変更することができるものもある。これらのポリシーを企業単独で指定できるよう、各導入企業のポリシーに合わせたり、組織ごとや個人ごとに可変性が担保できることも重要である。

4.4 ＭＤＭによる端末運用管理 (平常時の通常運用)

通常運用時の端末のセキュリティ状況監視について、機能要素ごとにＭＤＭのシステム運用上の留意点を以下に解説する。

4.4.1 利用状況監視

端末のセキュリティポリシーに関連するパラメータや利用状況をＭＤＭ側から定期的に監視できる。ＳＭＳ送信方式による状態取得やクライアントエージェントの状態監視データアップロード方式など、いずれの方法でもタイマー監視が可能なので一定の定期監視を行うことが望ましい。

一般的には、エージェント方式の場合、数十分単位にログ取得する設定が望ましい。GPSログ取得等、紛失盗難時のロケーション情報による移動経路の追跡調査に役立てることができる。

アクティベーション時にセキュリティポリシーパラメータが正当な状態であることをチェックしていても、操作者の独自な操作により変更ができてしまうので、一定間隔での状態監視と不当な状態の端末にはセキュリティポリシーパラメータの強制更新による制御が有効となる。

端末のMDMエージェントを使用者が強制的にプロセス削除したり、アンインストールするケースもあるので、アプリケーションを指定してアンインストール制限できる端末を選択することも有益と考えられるが、端末ベンダーによるキッティング時にプレインストールすることも一考の価値がある。

Wi-Fi接続端末でのエージェントスキャンの間隔を短く頻発させるとアンテナ受信状態を継続させバッテリーの消耗を早めることになるので、端末機種ごとにバッテリー性能の低い端末には利用状況取得間隔を長めに設定するなどの配慮も肝要である。

4.4.2 利用アプリケーションの利用制限とバージョン管理

4.4.2.1. アプリケーションの利用制限

アプリケーションの管理において、ブラックリスト方式よりも、ホワイトリスト方式の方が実用的である。アプリケーションのログについては、インシデント発生時の検証目的で残す方法と、ログ情報から更なるセキュリティリスクを回避するために敢えて残さない方法があり、意見が二分される。

企業利用端末の場合、利用目的が明確であれば、不正利用を防止するため、ホワイトリスト方式で利用できるアプリケーションを制限する要求がある。

例えば、ツイッターやフリーの掲示板サイトへのアップロードを禁止したいが、オープンなコンシューマ用途のアプリケーションは日常的に発展、急増しているためブラックリスト方式での利用制限が困難となる。このため、一般的には、ホワイトリスト方式でのアプリケーション制限を行なえることが望ましい。端末固有機能でアプリケーション利用制限が可能な端末に対して、MDMクライアントエージェントが利用可能なアプリケーションを指定することになる。この方法が困難な機種の場合は、利用制限をかけたアプリケーション以外を起動した場合、ログアップロードのタイミングで、不正利用の検知を行い追跡が可能な監視状態を行えるようにすることが望ましい。

企業利用の場合、一般的には、著作権、使用権の問題から、ソフトウェア開発元不明のアプリケーションに利用制限を行う場合が多いため、アプリケーションのインストール制限を行うことが望ましい。

なお昨今話題の標的型攻撃を考慮した場合、メールとWebアクセスの出口対策が重要になる。これらは、PCの利用で企業が既に導入している製品(メールサーバのアーカイブログ管理と、ネットワーク境界のウィルス対策製品等を含むWeb Proxyサーバなど)を活用すると、管理工数の増加を抑制できる。

4.4.2.2. アプリケーションのバージョン管理

アプリケーションのバージョン管理は、PCよりも重大である。なぜならば、一度インストールされたアプリケーションは、ユーザへの明示的許諾なしでアップデート出来るため、初版は無害な便利ツールでも、アップデート版に不正アプリケーションが混入していた場合、ユーザが気付かずにインストールしてしまう可能性がある。

MDMの端末側アプリケーション管理機能は、インストールされたアプリケーション名とバージョン情報を取得することができる。これは主には、MDMエージェントのスキャンにより端末側の保有アプリケーションのバージョン情報をMDMサーバへアップロードする仕組みによって成り立っている。

MDM側から管理端末全ての保有アプリケーションを監視し、バージョンが古い場合やウィルススキャンのエンジンのバージョンが古い場合、更新や最新アプリケーションへのアップグレードを促すためのプッシュ配信と併用することで、管理端末のアプリケーションの最新化や機能拡張、パッチ適用を促すことができる。

また、特定の業務アプリケーションの配信やコンテンツデータの更新にはＭＤＭ経由で一括配信と端末側でのインストールを促すことが業務用途の端末管理には効果的である。(例えば、営業マンのカタログ配信やオーダエントリ業務アプリケーションの保有するマスタファイルの強制配信に利用できる)

特に、アプリケーションのセキュリティパッチの適用やウィルスエンジンのバージョンチェックにはＭＤＭサーバ側からのバージョンチェックと強制配信は、有益な手段と考えられる。

また、近年では、これらの機能を応用して企業側のネットワークへの認証時の検疫システムと併用し、インストールされたアプリケーションの種類やバージョンによって、イントラネット接続利用の不正接続を防止する効果も期待されている。(4.3.4参照)

4.4.2.3. アプリケーション配信とユーザ認証

企業側が社内利用を目的に独自にアプリケーションを配信した場合、社内システムに接続して業務使用するアプリケーションの利用を限定させることが要求される。しかし、端末の使い廻しにより権限範囲以外の使用者に機密データを閲覧ダウンロードできてしまうリスクを伴うため、端末認証のほか、操作者のユーザ認証で利用制限を設けることが望ましい。

この対策(ユーザ認証)は、社内システムのユーザプロファイルとの連携を想定したID権限チェックの仕組みが必要になるので、全てのＭＤＭで実現できるものではない。オンプレミス型の独自導入の場合、シングルサインオンのIDポリシーに合わせ自動的にポリシー変更も可能となる。また、クラウド型の場合、操作者認証時にセキュリティポリシーパラメータのテンプレートで自動的に切り替えることができることが望ましい。

端末購入コストを削減するため企業購入端末を使い廻し(端末を貸し借りして利用する)シーンがある場合は、本対策が必要である。利用者に業務専用アプリケーションを配布する企業には、むしろ基幹システム側でコンテンツデータの閲覧･ダウンロード制限、専用アプリケーション上でのログオフ時の自動削除機能を有したアプリケーションの配備も検討すべきである。

4.4.3 不正利用防止

4.4.3.1. 状態監視とセキュリティパラメータの正常化

操作者が、端末のセキュリティポリシーを独自に変更したり、ロック解除パスワードを変更した場合、ＭＤＭ側からの状態監視により、不正利用端末を特定し、強制的にセキュリティポリシーを変更させることもできる。

例えば、企業側のホワイトリストで指定したウィルス対策ソフトをアンインストールした端末やロック解除パスワード設定を解除した端末に対しては、エージェントスキャン後のステータスアップロードの情報によりＭＤＭ側で端末の特定･検知が可能になるので、強制配信しインストールを促したり、セキュリティポリシーパラメータの強制更新を行なえる。

このように端末の監視と強制更新の併用によって、利用企業の組織内統制とセキュリティポリシーの統一化を図ることが重要である。

＜セキュリティパラメータ強制設定の例＞

精密機器製造会社の工場内勤務者には、機密情報漏えい対策としてカメラ撮影禁止にしている場合、デバイス利用制限で端末のカメラ利用禁止(デバイス-カメラ:ＯＦＦ)とするが、顧客設置機器検査担当には検査訪問先での撮影画像データのアップロード用アプリケーションの利用を許可している場合、端末カメラ利用許可(デバイス-カメラＯＮ)とする場合がある。

このような場合、ＭＤＭ制御としては、工場内勤務者には、デバイス設定のカメラＯＦＦとし、外出時の検査担当にはカメラＯＮとなるよう、強制設定変更を行うことが必要となる。

工場内勤務者は、端末のカメラ機能は利用できないが、操作者本人が設定パラメータを変更してカメラを利用することもできる。そのためＭＤＭは定期的に状態を監視し、設定変更がないことを確認し、不正にカメラＯＮにした場合、次回のエージェントスキャンで変更を検知し、自動的にカメラＯＦＦに強制変更させる。

ＭＤＭにより不正状態のパラメータを強制修正した場合でも、操作者の独自な操作により再度変更ができてしまうので、一定間隔での状態監視と不適切な状態の端末には強制更新による制御が有効である。

スマートフォンやタブレット等の端末は、携帯電話同様に個人利用を目的としたＯＳを搭載している。これらは、ネットワーク利用やセキュリティポリシーパラメータを操作者が自己責任で変更することを前提として開発されたものである。そのため、業務使用端末の運用ルールで制限をかけたとしても、システムで不正利用を制限する仕組みを設けることが困難である。そこで、ＭＤＭの機能で強制的に必要時、適切な状態に変更できることが重要である。

4.4.3.2. フィルタリング機能の管理

フィルタリング機能を実装しているＭＤＭ製品･サービスは非常に少ないと思われるが、不正サイトへのアクセス誘導を防止するために、Webフィルタリング機能は重要である。Webフィルタリング機能は、ユーザのWebアクセスで接続先サイトの安全性を判定し、アクセスコントロールを行う。ほとんどの企業で、ファイヤーウォールやIPS、Web Proxyサーバが実装されているので、スマートフォンもこれを利用するとセキュリティリスクの低減が図れる。

また、業務を阻害する着信スパムやSMSスパム等を判定･除去するフィルタリング機能があるとユーザの利便性とセキュリティ向上が図れる。

さらにスパムメール対策を実装したメールサーバを利用することにより、情報漏えいなどのセキュリティリスクの低減と、運用コストの増加を抑制できる。

4.4.4 操作ログ監視

操作者の端末利用ログを保存できる端末の場合、ＭＤＭサーバからの指令によってログ取得とアップロードを行える機能を利用することも有益である。

不正利用監視でセキュリティポリシーが不適切な端末には、操作ログの解析により本人の意図で不適切に設定変更されたものかどうかを推定できる場合がある。

ただし、アップロードされたログデータの解析手段は、ＭＤＭのソリューションで実装されているものではなく、操作ログ解析には別途のシステム準備が必要となる。

端末の利用ログから設定変更された時点を解析できるログ管理体制が望ましい。

4.4.5 アプリケーション、コンテンツデータの一括配信、更新

業務利用端末専用の端末アプリケーションを使用する場合、端末のアプリケーションや保有データのバージョン管理とアップデートの仕組みを配慮すべきである。

4.4.2項で述べた、ホワイトリスト化したアプリケーションに限定したバージョン管理と配布方法をサービスに実装し、企業利用時のアプリケーションの持続的な脆弱性対策や保有データの秘匿性を維持するためコンテンツデータの最新化は有益な手段といえる。

4.4.6 ウィルス･マルウェア検知エンジン配信

特にインストールを避けるべきアプリケーションは、ウィルス･マルウェア対策ソフトで検知できるので、これらの利用は有効である。この場合、業務利用ＰＣのセキュリティポリシーに準じたウィルス･マルウェア対策ソフトに限定し、バージョン管理によってエンジンファイルが最新バージョンであるかをチェックし、最新でない場合に更新を促すためのプッシュ情報を配信できることが望ましい。

セキュリティベンダーが提供するサービスでは、これらの一連の動作を自動的に行える機能を有していることが一般的である。しかし、法人契約の場合、独自にファイル更新の仕組みを取り入れる必要がある場合もある。

ＭＤＭソリューション製品では、ウィルス対策ソフトの配信と自動更新をサービス化している場合が多く、特に企業側で指定のウィルス対策ソフトの選択に制限がない場合は、ＭＤＭ側の機能で実現することも可能となる。ＭＤＭサービスはウィルス対策ソフトを限定的に採用していることが多く、多数のウィルス対策ソフトから自由に選択できるものではないため、導入検討段階で既存ＰＣのウィルス対策ソフトの利用状況と合わせた検討が必要である。

4.4.7 端末資産管理

ＭＤＭ側で端末管理情報と使用者情報（プロファイル）の一元管理を行なうため、誰がどの端末を所有し、使用者が誰なのかを管理することができる。これは、使用者のヘルプデスク業務や紛失盗難時の処置を行ううえでは、重要な情報となる。特に、社内での持ち回り使用を容認する場合、貸出管理等の配慮も必要となる。

個人利用のＭＤＭクラウドサービスの場合、個人管理のため使用者情報のみの管理となり、契約者情報と使用者情報で社内で別途の台帳管理を行なうこと重要と考えられる。

オンプレミス型ＭＤＭの場合は、独自に構築したプロファイル管理や組織階層化したポリシー管理への応用性が高く、組織情報やポリシーグループ情報などの付帯情報の管理が可能で設備資産管理と使用者情報やポリシーグループ管理と紐付けた資産管理運用が望ましい。

ＭＤＭエージェントのアクティベーション時の端末認証データ（IMEI、MAC、電話番号、SIMID等）の固体識別データとは別に使用者ログインIDで認証する仕組みのＭＤＭもある。この場合は、端末認証とは別に使用者ユーザ認証をアプリケーションレベルで行なってポリシーコントロールするで、使い廻しを許容した場合の貸出管理に近い資産管理ができる。

4.5 ＭＤＭによる紛失･盗難対策、故障対策（異常時の運用）

4.5.1 紛失、盗難時の運用

紛失･盗難時には、まず端末使用者の捜索経過のなかで、紛失･盗難の情報を基にシステム管理者が処置を行なう場合と、使用者がなんらかの手段を通して、ロックワイプの指示を行なう場合がある。

表4-5 紛失･盗難時の運用

処置者	内容
システム管理者が処置を行なう場合	端末使用者本人のみでもＭＤＭサービスへログインして端末操作をＭＤＭ側から行えるものが望ましいが、セキュリティポリシー変更までもできてしまうのは好ましくないため、ＭＤＭログインIDにより処置可能な権限範囲を制限できる仕組みが望ましい。
端末使用者が処置を行なう場合	キャリア通信会社やセキュリティベンダーのクラウド型ＭＤＭの場合、使用者本人が紛失盗難時の処置を行なうサービスが提供されている。Webサービスにログインしロック操作、サービス提供者への電話連絡、特定ダイアルサービスでのロックワイプ操作等、端末使用者個人が直接に行なうことができる。

いずれの場合でも、セキュリティポリシーの周知とあわせ、紛失･盗難時の運用ルールを明確化し使用者に周知徹底することが重要となる。

4.5.2 リモートロック

ＭＤＭサーバから、端末のロック指示を行う機能を利用して、紛失･盗難対策の処置を行う。

ロック解除パスワードを設定済みの端末にはロック指示のみでも問題ないが、ロック解除パスワードが判るメモと一緒に扮した場合等は、拾得者や窃盗者がロック解除できてしまうケースも想定されるため、ＭＤＭ側から強制的にロック解除パスワードの変更を行なうことが望ましい。

盗難されたものか、紛失したものか、特定されていない段階では、リモートロックのみを行い、盗難または捜索困難と判断できる場合、リモートワイプの処置を行なう。

紛失の発覚、捜索、盗難、発見、ロック解除の各段階で、ＭＤＭの運用処置をルール化しておくことが望ましい。

4.5.3 リモートワイプ

一般的なリモートワイプでは、ＳＤ内格納データ消去や個人情報（プロファイルやメールアカウント）の削除のみを行なうＭＤＭもあるが、工場出荷時に戻すこともできる端末の場合、工場出荷時に戻す処置のほうが、情報漏えい対策としては安全といえる。

ローカルワイプの機能を利用して、拾得者や窃盗者がロック解除を試みた場合でもロック解除の失敗回数に応じて、自動的にローカルワイプし工場出荷時に戻せる設定も効果的である。

ＭＤＭクライアントエージェントに、ロック解除失敗許容回数を指定し、許容回数を超えた場合のワイプ起動の挙動を初期設定できるものもある。

なお、リモートワイプまたはローカルワイプによるデータ消去の程度は、デバイスのOSや端末機種によって異なる点に留意する必要がある。

端末特性とＭＤＭの機能を十分に検証したうえで、運用ルールを検討する必要がある。

4.5.4 位置情報取得

紛失・盗難時にリモートワイプを起動させる前に位置情報を取得することで、紛失場所の特定や移動追跡を行える。これにより、紛失・盗難時の捜索回収に役立てることができる。

ただし、ＧＰＳデータの取得は、端末特性や通信環境により常時ＧＰＳデータログを取得できているとは限らないし、紛失・盗難後にネットワークアクセスをさせていない場合は位置情報を取得しても、使用者の最終操作時点のＧＰＳデータであり、必ずしも固体の現在時点の所在として認識できない場合がある。そのため、位置情報取得による追跡は、使用者の紛失・盗難時の時間やロケーションを特定する最終情報とＧＰＳ取得時間との差異により所在精度を推定する参考と考えるべきである。

ＭＤＭで取得したＧＰＳ位置情報は、３Ｇ搭載機種の場合はある程度精度が高いが、Wi-Fi端末の場合、アウトドアにありネットワーク接続した時点のログ情報と解釈できるので、端末固体の現在位置情報の正確性に欠ける場合もあることに留意する。

4.5.5 ワイプ後に発見した場合や故障時の復旧策（バックアップリストアの対応）

ＭＤＭ側から強制ワイプを実施したり、不慮の故障による機種交換を行う場合、それまで利用してきた端末の設定情報やローカル保存したデータの復旧が必要である。

復旧対策のためのバックアップとリストアをサポートするため、ＭＤＭサーバでバックアップアーカイブを利用できるサービスもある。

クラウドサービスの場合、Ｐａａｓ型のホスティングサービスとの併用や、オンプレミス型の場合、バックアップサーバへのアーカイブとリストアの仕組みを準備することが望ましい。

これらは、ＭＤＭエージェントのプロファイルバックアップやログアップロードにも応用できるため有益なサービスとなる。

4.5.6 遠隔監視サポート

ＭＤＭソリューションのなかには、リモートコントロールによりOne to Oneサービスの機能を実現することもできる。

主には、PCのヘルプデスクによる端末管理から発展したもので、MDMエージェントの機能でインシデントIDを発行して、MDMサービスのヘルプデスク側からネットワークを経由して、端末操作を行なうサービスが可能となる。

複雑なセキュリティポリシーにより操作を混乱した操作者への解説やポリシー設定の誘導を行なうために、遠隔監視したり、遠隔操作で設定変更までできるため、使用者から端末を回収して保守支援することなく、遠隔操作によるセキュリティコントロールを行なうことが可能である。

MDMの一部のオプション機能として実装しヘルプデスクサポートサービスを行うことで、業務利用の端末管理を効率化できる。

ただし、多数の端末使用者にサービスを行なうため、サービス提供側には一定のマンパワーを要する。また、サービスプロセスや窓口となるスタッフのノウハウに依存することになるので企業独自のサービスを行なうには定常的な負担が要求される。このため、要員体制やサービス内容の制約等を考慮する必要がある。

4.6 MDMによる廃棄準備

4.6.1 端末廃棄に伴うMDM側の処置

機種変更や端末使用終了時には、それら端末に格納された取扱いに慎重を要するデータを回復不能とすることが望ましい。

これは、廃棄に伴い端末内に残る個人情報や機密情報を含むコンテンツデータ、VPNやアクセスポイント、プロファイルデータ等の情報漏洩を防止するための重要な処置である。

また、取り外し可能媒体（SDカード等）がある場合は、それらについても同様の処置が望ましい。

4.6.2 更新機種の適用（アクティベーション）

機種変更に伴い、MDMの管理端末情報の新規追加を行なう。

キャリア通信会社が提供するMDMサービスの場合、契約変更時にサービスのアクティベーションを継続的に行なえるよう処置をしてもらえる。

オンプレミス型の独自導入やクラウドサービスの場合、機種変更に伴い端末管理プロファイルの新規登録とセキュリティポリシーの継承のためのアクティベーションを行なう必要がある。

後者の場合、通信キャリアとMDMサービスが切り離されているため、固体認証やプロファイル変更など使用者の都合で連絡がない場合、廃棄された従来機種を固体認証するためのプロファイルが残り、管理精度が低下することになる。（使っていない端末プロファイルが残されていくことになり、資産管理上、問題となりえる）

5 MDM機能要件チェックリスト

最後に、MDMの導入目的から機能を選定するための要件一覧を付録「MDM機能要件チェックリスト」としてまとめた。なお、要件項目を満たすとどのような効果が得られるかをリストの右欄に付記した。

世の中に存在する様々なスマートフォンに対し、統一したセキュリティポリシーのもと企業情報システムのリスク分析を経て、端末の特性や用途に応じて必要なセキュリティ要件を洗い出し、それら要件を満たし、かつ管理コストを低減する施策として、本チェックリストの中から必要機能を選択し、4章で述べた運用用件を考慮しながらそれら機能を実装するMDM製品やサービスを選択することが望ましい。

付録「MDM機能要件チェックリスト」参照。

6 おわりに

スマートフォンはコミュニケーションツールとして優れた特性を持つ反面、普及が先行したためセキュリティ機能は総じて発展段階にある。そのため試行錯誤的に多数のMDM製品が出現し、その機能や方式も千差万別である。世の中に統一したMDMの定義すら存在しないのが現状である。

このような状況下、MDMタスクフォースは、企業の管理者がMDMの導入検討に何をどのように考えたらよいのかについての助言を提供することを目指した。

導入検討にあたっては本来のセキュリティ対策ステップを踏まえ、利用する企業システムの構成と守るべき情報資産、それらのセキュリティリスクを分析した上で、MDM導入の目的、用途を明確化し、セキュリティ対策、コストおよび利便性のバランスを考慮することが肝要である。

本書は、このMDM導入目的を達成するために必要な機能要件とその導入･運用時の注意点や留意点をまとめたので、MDM製品の選定ならびに導入･運用する際の参考としていただけたら幸いである。

付録：MDM機能要件チェックリスト

※印は実現にあたり、端末への組み込みによる制御（システム領域でのシステム権限付与による制御）を要すると考えられるもの。

MDM機能					効果
項番	機能分類	機能要件	項番	機能内容	
1	端末管理	リモートロック	1	端末個体ごとのロック・アンロック	・盗難／紛失対策
		リモートワイプ	2	全データ削除	
			3	個別データ／特定フォルダ削除※ （電話番号、メールアドレス等のアプリケーション毎のデータ、ブラウザ等のキャッシュ、各種ログ等）	
		暗号化	4	保存領域の暗号化／復号	・内蔵メモリの抜取対策 ・外部記憶のデータ抜取対策 ・アプリデータの漏洩・改ざん対策
			5	外部メモリ（SDカード等）の暗号化／復号	
			6	個別データの暗号化／復号※（但し、SDカードはシステム権限不要）	
		デバイス制御	7	カメラ	・デバイス不正利用対策 ・業務外利用対策
			8	スクリーンショット※	
			9	Bluetooth	
			10	外部メモリ（SDカードなど）※	
			11	無線LAN（WiFi）	
			12	USB※	
			13	赤外線通信※	
			14	NFC(Near Field Communication) ISO/IEC 21481	
			15	FeliCa、ISO/IEC 14443（MIFARE）※	
			16	ワンセグ※	
			17	UIMカードメモリ※	
			18	発信先制限	
		遠隔監視	19	端末状態の情報取得 起動確認、起動中アプリ、コンプライアンス違反状態等の端末側情報の取得とアップロード OS、インストール済みアプリケーションのバージョン管理	・盗難・紛失対策 ・不正利用対策 ・業務外利用対策 ・管理コスト削減
			20	死活監視 活性化状態（主にネットワーク接続状態）の取得とアップロード	
			21	ログ収集 システムログ、操作ログ、アプリ起動ログ等の取得とアップロード	
			22	位置情報取得 GPS追跡機能など	
			23	アラートメール送信 管理者への通知機能、利用者への警告機能	
			24	レポート出力 監視、制御、運用状況のレポート	
		遠隔ポリシ設定・実行	25	パスワードのポリシー設定 文字複雑性維持、初期パスワード強制変更、有効期限設定、最低利用日数設定、パスワード履歴管理（直近パスワード使用禁止：通常3サイクル） （プラットフォームによって、実装可能な機能は異なる）	・不正利用対策 ・管理コスト削減
			26	MDMのポリシー設定 リモートロックやワイプ、デバイス制御などのMDM動作を規定する設定情報の適用とポリシー外設定の強制復帰	
			27	端末の構成設定※ メールサーバーやVPN/WiFiなどの設定情報や証明書ファイルの適用	
		資産管理	28	端末の数量管理 個体情報（機種、電話番号等）管理	・管理コスト削減 ・不正利用対策
			29	ソフトウェアの数量管理 ソフトウェアの種類（OSの名称、アプリケーションの名称、それらのバージョン等）の管理	
			30	所有者属性の管理（部門名、社員番号、指名等）	
2	アプリケーション管理	配信・削除	31	自社アプリケーションの配信とインストール※	・管理コスト削減 ・不正利用対策
			32	推奨アプリケーションリスト（ホワイトリスト）の配信	
			33	アプリケーションの遠隔削除※	
		業務アプリケーションの保護	34	会社公認アプリケーションの保護※ アンインストールならびに不正終了防止	・不正利用対策 ・不正アプリインストール制限 ・不正アプリ強制削除 ・不正アプリ起動制限 ・管理コスト削減
		アプリケーションの利用制限	35	会社非公認アプリケーションのインストール制限もしくは強制終了（ホワイトリスト方式）	
			36	会社非公認アプリケーションのインストール制限もしくは強制終了（ブラックリスト方式）	
			37	USB／SDカード経由のアプリケーションのインストール抑止※	
			38	アプリケーションのパーミッション制御※	
3	MDMエージェントの認証および保護	MDMエージェントの正しいインストール	39	エージェントインストール時の認証 （端末証明書またはID／パスワードによる端末認証、利用者認証）	・盗聴対策 ・不正アクセス対策 ・社内システム保護
		高信頼経路による接続	40	VPN、SSLなど	
		MDMエージェントの保護	41	MDMエージェントのアンインストール抑止※	
4	フィルタリング機能の管理	悪性Webサイトへのアクセス制御	42	Webフィルタリング（ホワイトリスト方式、ブラックリスト方式）	・不正利用対策 ・フィッシング詐欺対策 ・スパム対策
		スパムメール除去	43	メールフィルタリング	
		着信スパム、SMSスパム除去	44	着信拒否／SMS着信拒否※	
5	マルウェア対策ソフトウェアの管理	遠隔監視	45	ソフトウェア状態およびログの収集 ソフトウェア／エンジン／パターンファイルのバージョン、最後のスキャン時間、最後に駆除したウィルス数等の情報の取得とアップロード	・端末の汚染対策
		バージョン管理・更新	46	パターンファイル更新の要求	
			47	スキャン実行の要求	
		遠隔ポリシ設定・実行およびスキャン実行	48	ポリシー設定 パターンファイルの自動更新スケジュール、スキャンの自動実行スケジュールなどの一括適用	
6	バックアップ管理	端末データのバックアップ	49	端末復旧に必要なデータの定期的、個別的バックアップ※	・故障／滅失対策
		端末データのリストア	50	各種データの復旧※	