モバイルデバイス管理（MDM）：入門編

スマートフォン活用を支援

2011年に入り、iOSとAndroid端末を安全に活用するためのモバイルデバイス管理（MDM）システムが充実してきた。その機能や仕組み、選択におけるポイントなどをレポートする。

文◎坪田弘樹（本誌）

iPhone/iPad、Android端末の企業への普及が本格化している。それとともに、これらの新端末を安全に活用し、また効率的に管理するために必須のソリューションとして導入検討が進んでいるのが、モバイルデバイス管理（MDM：Mobile Device Management）だ。

スマートフォン／タブレット端末の業務活用において最大の課題となるのが、端末内のデータの保護と、端末・アプリの管理である。

従来も携帯電話や、Windows Mobile／BlackBerry等のスマートフォンでモバイル環境でのデータ活用を行う企業はあったが、ごく少数に留まっていた。IT／ネットワーク管理者にとって、情報漏えい等のリスク対策とセキュリティポリシーに則った運用を徹底すべきモバイルデバイスといえば、これまではほぼノートPCに限られていた。

その状況が今、急激に変わりつつある。管理すべきモバイル端末は、数もOSの種類も格段に増える。これに対応した体制を整備しつつ管理負荷の増大を押し留めることは、企業にとって急務の課題だ。

こうしたニーズに応じて、2010年後半から国内でも、iOSとAndroid端末に対応したMDMが登場し始めた。2011年になってその数は増加し、「MDM」はあっという間に注目ソリューションの1つとなった。

本稿では、まずMDMの基本的な機能と仕組みから解説しながら、導入・検討のポイントを探っていくことにしょう。

図表1　モバイルデバイス管理（MDM）の主な機能

目的	機能	詳細
紛失・盗難時の情報漏えい対策	リモートロック	管理コンソールから遠隔で端末の起動をロックし、解除指示されるまで使用不可の状態にする
	リモートワイプ	管理コンソールから遠隔で端末を工場出荷状態にする。挿入されているSDカード内のデータを削除する機能なども
	パスワード利用強制（ローカルロック）	パスワードの利用を義務化・強制。文字数や英数字利用の指定、パスワード更新の強制など
	ローカルワイプ	ローカルロック解除失敗（パスワード入力の失敗）時にデバイスを初期化
	位置情報取得	GPSによる端末の位置情報を取得する
不正利用の防止	デバイス制御	カメラ、Bluetooth、無線LAN、SDカード等の機能のうち、業務に不要なものを無効化する
	発信先制限	許可された発信先以外の電話番号への発信を制限する
	発着信番号履歴の取得	発信および着信した電話番号の履歴情報を取得する
	アプリケーション利用制限	許可されたアプリ以外の利用を制限する（ホワイトリスト）、または特定のアプリを利用不可にする
	アプリケーション情報取得／監視	端末にインストールされているアプリの情報を取得、利用状況を監視する。追加や削除があった場合に再取得、管理者に通知する機能など
	アプリケーション強制削除	ポリシーに違反するアプリケーションを強制的に削除する
ポリシー違反対策	異常状態検知、通報	ポリシー違反の可能性のある端末（サーバーとの通信を一定期間行っていない、パスワード連続失敗など）を自動検知し、管理者やユーザー自身にメールで通知
	エージェント管理	MDMのエージェントアプリのアンイストールの防止、リモートバージョンアップの実行など
端末・アプリ管理の効率化	インベントリ管理	OSバージンや起動状況、セキュリティポリシーの適用状況、アプリの導入状況などの情報を遠隔で取得する
	ポリシー設定・配布	セキュリティポリシーをグループや部署に応じて設定・配布する
	アプリケーション配信・インストール	業務アプリや利用推奨アプリを端末に配布しインストールする。または、アプリの更新を通知し、インストールを促す
	ファイル配信	指定したファイルを端末に配信する

MDMで何ができるのか

端末・アプリの利用状況を遠隔から一元管理

MDMで何ができるのか。

簡単にまとめると、統一したポリシーの下に遠隔から複数の端末を一元管理するということになる。

搭載する機能は多岐にわたるが、スマートデバイスの業務活用における課題に照らして整理すると、大きく次の3つに分けることができる。①紛失・盗難時の情報漏えい対策、②不正利用の防止、③端末情報の収集とポリシー一斉適用等による管理の効率化だ。この観点で主要機能をまとめると**図表1**のようになる。

①の情報漏えい対策は、パスワードロックの強制化と、リモートロック／ワイプの機能で、悪意ある第三者による端末操作を防止する。

パスワードロックは端末自体が持つ基本的な機能だが、これをエンドユーザーに徹底させることがまずは肝要だ。口頭などで通知するだけでは難しい。管理者がMDMの管理画面から遠隔指示でロック機能を強制適用できるだけでなく、パスワードの桁数や、英数字が混在した文字列の使用を強制することもできる。

リモートロック／ワイプは、端末の紛失・盗難が判明した後に、操作をロックあるいは工場出荷時の状態に戻す（ワイプ）機能だ。情報漏えい対策は、パスワード強制とリモートロック／ワイプの二重の仕組みを徹底することがポイントになる。最も危険なのは、端末を失くしてからその事実に気がつくまでの時間だ。この間をローカルロックで守り、かつリモートロック／ワイプでより完全な対処が可能になる。

リモートロック機能を実行すると、緊急通報以外の操作は一切行えなくなる。パスワードを入力するほか、管理画面からも解除できる

パスワード強制入力の設定画面（インヴェンティットの「MobiConnect」）。パスワードポリシーを強制化するだけでなく、文字列の種類や長さ、ワイプを行うまでの認証失敗回数などが設定できる

アイキューブドシステムズが提供する「CLOMO MDM」の管理画面。社員が持つiOS端末とAndroid端末を一覧で表示しながら、指定した端末の詳細情報も取得できる

スマホを「業務専用端末」に

スマートデバイスはもともと多機能なうえ、アプリを追加すればさらに使い道を拡張できる。この利点は、管理者にとって非常に厄介なものでもある。エンドユーザーの裁量に任せて野放図に利用させればセキュリティリスクは増大し、また、業務以外に使うことでかえって生産性を損なうことにもなりかねない。

そうした不正利用を防止するための機能（②）が、デバイス制御やアプリ利用制限だ。デバイス制御は、カメラやBluetooth、無線LAN、SDカード等のうち、業務に不要なものを