QualitySoft

CASE STUDY
ユーザー事例

画像機器製造・サービス
株式会社リコー

ISM CloudOne

スマートデバイスの業務利用に必須 MDM/MAMの機能が備わったISM CloudOne

IT/S本部
ITインフラ統合センター
ワークスタイルイノベーショングループ
シニアスペシャリスト
田崎 淳一 氏

IT/S本部
ITインフラ統合センター
インフラ統轄グループ
シニアスペシャリスト
高崎 和義 氏

社内ワークスタイルの変革を目指すリコーは、スマートデバイスに大きな期待を寄せている。同社はBYODを実施する予定だが、そのためにはまず、セキュリティとプライバシーという相反する課題を解決する必要があった。スマートデバイスを利用する際のガイドラインは策定してあるものの、端末の管理や情報漏えい対策としては、それだけでは不十分。そこでリコーが導入したのが、MDM(Mobile Device Management)／MAM(Mobile Application Management)を同時に運用できる「ISM CloudOne」だ。以前から、ISM CloudOneでMDMを運用してきたが、MAM機能が追加されBYODにも利用できる点がポイントになっているのだという。リコーの担当者にISM CloudOne導入の経緯について話を聞いた。

新たなワークスタイルを創造し、業務の変革を目指す

リコーは、1936年の創業当時からオフィス需要を掘り起こしてきた企業だ。1955年に卓上複写機「リコピー101」で事務機市場に参入してからは、事務用オフセット印刷機や事務用高速ファクシミリなどを次々と開発。1970年代後半には業界で初めて「オフィス・オートメーション(OA)」を提唱し、1980年代にはオフィスコンピューターやワープロ、レーザープリンターといった情報機器を普及させた。2000年代以降は、プリンティングソリューションやドキュメントソリューションなど、ワークフローを効率化する製品・サービスの充実を図り、現在も世界各国の顧客から支持を受けている。

「市場や顧客価値の創造」を目指す一方で、リコーが取り組んできたのが、社内の「業務改革」だ。2012年には、社員の新しいワークスタイルを創造することにより、業務そのものの変革を目指すプロジェクトを立ち上げている。

「プロジェクトでは『いつでも』『どこでも』『どの端末でも』をコンセプトに、組織の階層を超えた情報共有やコミュニケーションを図れるようにしたいと考えています。それには、スマートデバイスが欠かせません」と、IT/S本部・ITインフラ統合センター・ワークスタイルイノベーショングループ・シニアスペシャリストの田崎淳一氏は言う。

スマートデバイスとは、スマートフォンやタブレットなどの総称で、移動中や外出先でも業務を行えるようになるのがメリットだ。

同プロジェクトでは、スマートデバイスを社員に貸与するだけではなく、社員が個人で所有するスマートデバイスを業務にも使うBYOD(Bring Your Own Device)の実施を計画している。とはいえ、BYODに踏み切るためには、セキュリティとプライバシーという2つの課題の解決が必須。そこで白羽の矢が立ったのが、クラウド型のマルチデバイス管理ツール「ISM CloudOne」だった。

MDMで情報漏えい対策を施す

スマートデバイスは、ウイルスに感染するリスクがあり、盗難・紛失による情報漏えいの危険も高い。つまり、業務に利用するためには、何らかのセキュリティ対策が必要だ。

リコーでは、2010年からスマートデバイスのリスク調査を実施して、端末利用のガイドラインを策定した。また、ガイドラインだけでは対応しきれない情報漏えい対策や端末管理のために、MDM(Mobile Device Management)も導入している。

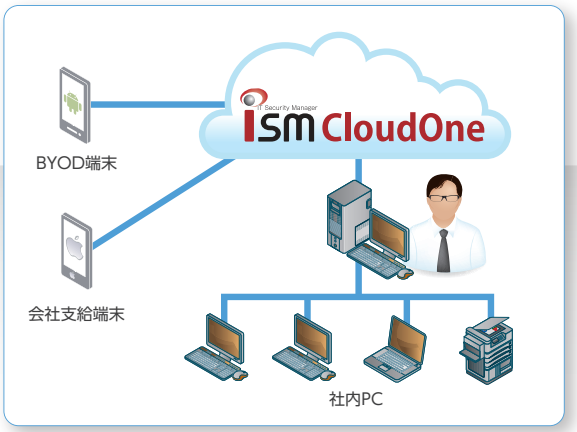
「MDMはいくつか検討しましたが、低コストで導入しやすく、社内の資産管理システムと連携するISM CloudOneを選定しました」と、IT/S本部・ITインフラ統合センター・インフラ統轄グループ・シニアスペシャリストの高崎和義氏。

MDMとは「端末情報(インベントリ)の収集」や、業務に不要な

CASE STUDY
ユーザー事例

画像機器製造・サービス

株式会社リコー



「アプリケーションや機能の制限」、盗難・紛失時の「遠隔ロック／削除」機能を備えたツールのことだ。ISM CloudOneは、それらの基本機能に加えて、アプリケーションの配布および起動制御、セキュリティ診断などの機能も搭載している。

ISM CloudOneを採用したことで、アンチウイルスソフトが導入されているか監視できるほか、盗難・紛失時には、遠隔ロック／削除することで情報漏えいを防ぐことが可能になった。さらにISM CloudOneの場合、オンプレミス型のIT資産管理ツール「QND」と連携することで、端末情報をQNDにエクスポートできるほか、QND経由でスマートデバイスを遠隔操作することもできる。

リコーは、以前から資産管理システムとしてQND（旧QAW）を導入していたため、既存の資産管理の仕組みで、スマートデバイスの管理と情報漏えい対策を実施できる点も大きなメリットだ。「資産管理システムとMDMをそれぞれ個別に運用する場合と比べて、管理工数を大幅に減らすことができると期待しています」と、高崎氏は運用コストの削減についてもISM CloudOneを高く評価している。

BYODを推進するにはMAMが必須

MDMが端末管理や情報漏えい対策に有効なソリューションであることは間違いないが、それだけでBYODを推進しようとすると、社員からの抵抗に遭う可能性がある。

個人のデバイスは社員の私物であるため、どう使うかは社員の自由だが、MDMの下では端末内の個人情報についても企業側に管理されることになってしまう。そこまでして自分のデバイスを業務に使いたいと考える社員はまずいないと言っていい。BYODを実施するには、社員のプライバシーを考慮した新しい仕組みを導入する必要があるのだ。

その点について、前出の田崎氏は「管理すべきは、端末ではなく『情報資産』そのもの」と指摘した。BYODによる企業のリスクは「情報資産の漏えい」にほかならない。そのリスクを低減するために、MDMで端末を管理してきたわけだが、端末に情報資産を保存しなければ、端末の管理は不要になり、プライバシーの問題も解決できると言うのだ。

そこでリコーでは、業務システムにリモートアクセスするアプリケーションを導入し、端末にデータを残すことなく業務ができるようにした。盗難・紛失の際には、このアプリケーションの利用を停止して業務システムへのアクセスを防ぐ。端末ではなくアプリケーションを制御することで、情報資産を守るというわけだ。

そのために欠かせなかったのが、アプリケーションを制御する「MAM（Mobile Application Management）」機能を搭載するISM CloudOneだった。BYODを推進する企業にとって、MAMは欠かせない機能なのだ。

リコーにおけるMAM機能の検証はほぼ完了し、BYODの導入も秒読み段階となっている。個人のデバイスを業務に活用できるようになれば、社員のワークスタイルも大きく変わっていくだろう。

IT市場では今、スマートデバイスやBYODが旬の話題となっている。リコーの業務改革を支えたISM CloudOneも、さらに多くの企業に注目されることになるだろう。

■ ISM CloudOneに関するお問い合わせは

QualitySoft

クオリティソフト株式会社

URL：http://www.quality.co.jp/　E-Mail：sales@quality.co.jp

本　　社　〒102-0083 東京都千代田区麹町3-3-4 KDX麹町ビル
TEL:03-5275-6123　FAX:03-5275-6130

西日本支店

大阪オフィス　〒541-0053 大阪府大阪市中央区本町2-5-7 大阪丸紅ビル
TEL:06-6125-2161　FAX:06-6125-2170

名古屋オフィス　〒460-0003 愛知県名古屋市中区錦3-22-24 SE第4ビル 6F
TEL:052-955-5866　FAX:052-955-5877