特集論文

スマートデバイスによる業務効率向上を実現する“MINDセキュアモバイルマネジメント”

手束裕司*

"MIND Secure Mobile Management" for Achieving Improvement of Work Efficiency with Smart Device

Yuji Tetsuka

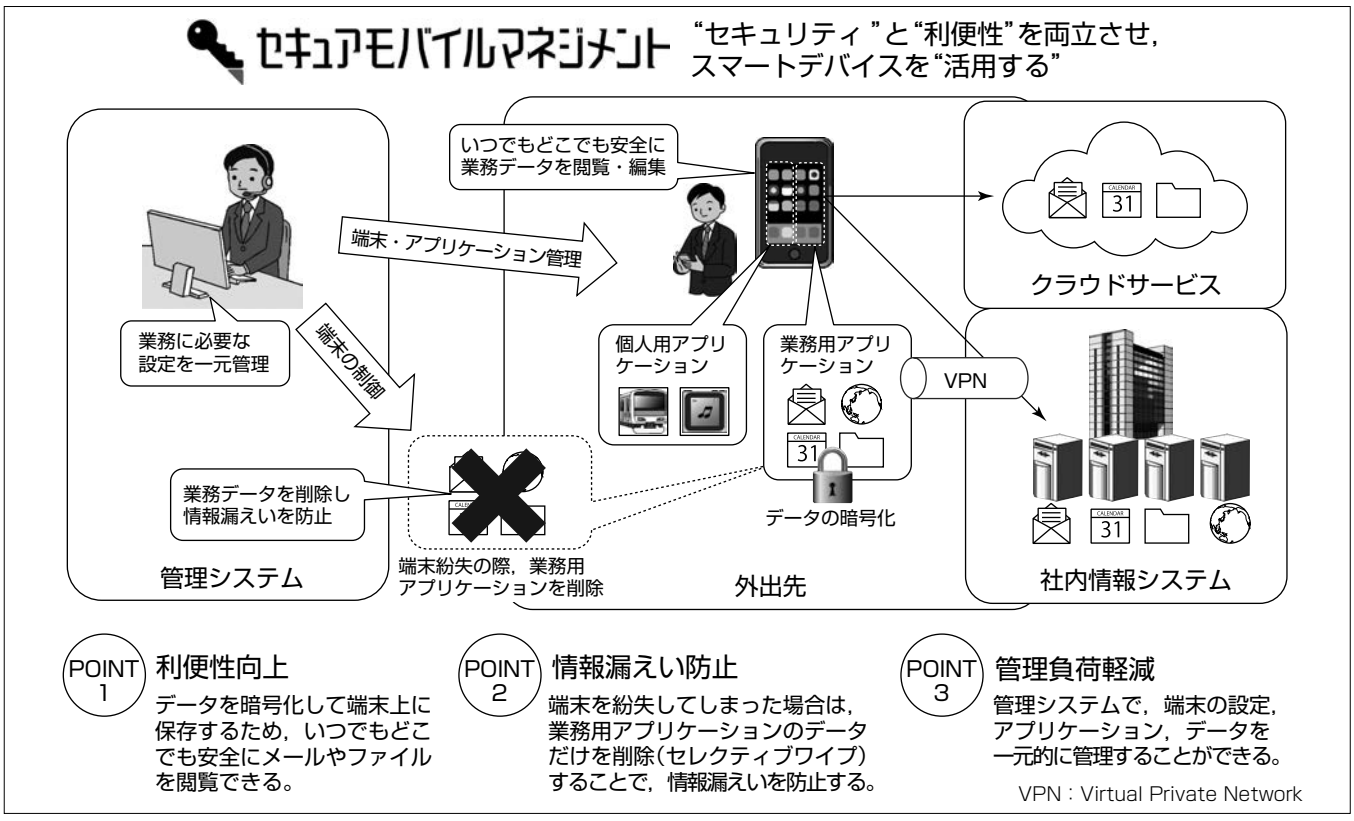
要　旨

スマートフォンやタブレットなどのスマートデバイスの普及が世の中で進む中，それらのスマートデバイスを業務で利用する動きが年々加速している。2013年には企業の半数以上がスマートフォンを業務で利用しており，その数は年々増加している。

スマートデバイスの業務での利用方法は，“店舗や製造現場などで業務システムの一部としての利用”と“情報システムツールとしての利用”との大きく２つに分類される。業務システムとしての利用では，紙マニュアルの電子化や，店舗での受発注など多くの事例が出ている。一方で，情報システムツールとしての利用については，メールの送受信やスケジュールの閲覧が主であり，利用者も経営幹部や一部の営業社員などにとどまっており，企業として，ワークスタイル変革を実現するまでの活用には至っていない。

情報システムツールとしてスマートデバイスを活用するためには，“セキュリティを確保するための技術”と“業務アプリケーションを利用するための技術”が必要となる。その２つの技術を実現するのがEMM(Enterprise Mobility Management)であり，EMMは従来デバイス管理として利用されているMDM(Mobile Device Management)に，アプリケーション管理のMAM(Mobile Application Management)，コンテンツ管理のMCM(Mobile Contents Management)を併せ持つ技術である。

三菱電機インフォメーションネットワーク㈱(MIND)では，情報システムツールとしてのスマートデバイスを“利用する”から“活用する”に変革するためのソリューションとして，EMMをサービス型で利用してもらえるソリューションとして“MINDセキュアモバイルマネジメント”を提供する。これによって，企業におけるスマートデバイスの活用を支援する。



MINDセキュアモバイルマネジメント

MINDセキュアモバイルマネジメントは，スマートデバイスの管理製品であるMDM，MAM，MCMの３つの機能を併せ持つEMM製品をサービス基盤としたスマートデバイスの管理・活用ソリューションである。スマートデバイスの業務利用で重要となる“セキュリティ”と“利便性”を両立させ，企業でスマートデバイスを“利用する”から“活用する”へ変革することを支援する。

*三菱電機インフォメーションネットワーク㈱

1. まえがき

スマートフォンやタブレットなどのスマートデバイスの普及が世の中で進む中，それらのスマートデバイスを業務で利用する動きが年々加速している。2013年には企業の半数以上でスマートフォンを業務で利用しており(1)，その数は年々増加している。

スマートデバイスを業務で利用することは，企業で一般的なことになってきているが，その利用方法は，“店舗や製造現場などで業務システムの一部として組み込んで利用する”と“情報システムツールとして利用する”との２つに大別される。前者の業務システムの一部として利用するケースは，航空会社における紙マニュアルの電子化，店舗での受注端末，倉庫での在庫管理などいろいろな場面での利用が実現されている。一方，情報システムツールとしての利用については，メールの送受信やスケジュールの閲覧が主となっており，営業社員の生産性向上や外出先からの業務利用などまだまだ十分に活用されておらず，ワークスタイルを変革するまでの利用方法には至っていないのが現状である。また，情報システムツールとしてスマートデバイスを導入したが，社内での展開が一向に進まないケースも多く出ている。

本稿では，情報システムツールとしてのスマートデバイスの活用に関し，その課題と解決策を述べる。

2. スマートデバイスの業務利用

2.1 スマートデバイスの業務利用での課題

企業におけるスマートデバイスの業務利用は2010年ごろから本格的に始まり，2011年には約３割の企業で何らかの形でスマートデバイスを業務で利用し，2012年には約４割，2013年には約５割の企業で利用している(1)。スマートデバイスの業務利用が進む一方で，その情報システムツールとしての用途はメールの送受信やスケジュールの閲覧にとどまり，また，利用者も企業の経営幹部など一部の人に限られ，全社的に展開している企業は多くはない。その第１の理由として挙げられるのが，従来の携帯電話に比べスマートデバイスの本体価格と通信料金が高額なことであり，第２の理由は，企業がスマートデバイスを導入する際に最大の懸念事項として挙げるセキュリティ対策である。スマートデバイスは従来の携帯電話に比べ，デバイスの中に多くのデータとアプリケーションを保持している。各種アプリケーションはデバイス内のデータにアクセスし，クラウドサービスなど外部のサービスとのデータ交換を可能とする。また，アプリケーションは個人が自由にダウンロードすることが可能であり，中には情報漏えいにつながるような不正なアプリケーションも存在する。企業の情報システム部門にとっては，セキュリティリスクを回避するため利用者を限定したり，MDMのようなデバイス管理のシステムを導入したり，対策を講じている。

スマートデバイスの業務利用に当たっては，ワークスタイル変革に伴う生産性の向上を目的とする企業が多いが，先に述べたとおり価格の面から社内での利用者が限られていること，セキュリティ対策を重視するがあまり利便性が損なわれ，利用したいと思う人が増えないことなど，その本来の目的を達成できない場合がある。特に導入目的を明確に策定せずに導入することで，本来の目的である生産性向上に代わり，“スマートデバイスを導入すること”自体が目的となっているような場合には，スマートデバイスの展開が進まず，生産性の向上が図れない。

2.2 スマートデバイスを業務で活用するための技術と導入ポイント

スマートデバイスを業務で活用するためには，“セキュリティを確保するための技術”と“業務アプリケーションを利用するための技術”の大きく２つの技術が必要となる。

“セキュリティを確保するための技術”としては，データ及び通信の暗号化，個人及びデバイスの認証，マルウェアの検知及び駆除，デバイスにインストールするアプリケーションの制御及び保護，さらにスマートデバイス紛失時の対策としてはGPS(Global Positioning System)によるデバイスの捜索，遠隔からのデバイスのロック及び内部データの削除などが挙げられる。

これらのセキュリティ対策を採用するに当たっては，企業のセキュリティポリシーに基づき，スマートデバイス利用時のリスクを分析し，そのリスクに合わせて適用する技術を採用することが必要である。過度のセキュリティ対策を実施することは，**2. 1節**で述べたとおり利用者の利便性を損ね，本来のスマートデバイスの導入目的である生産性の向上を実現することはできない。

一方の“業務アプリケーションを利用するための技術”であるが，情報システムツールとしての利用と考えた場合には，社内メールの送受信，スケジュールなどのグループウェアの利用，各種システムの利用(閲覧・入力・申請・承認)，ファイルストレージからのファイルの閲覧及び編集が主な用途として挙げられる。また，これらのシステムは，①自社保有のオンプレミス型として社内又はデータセンターに設置している場合，②Microsoft Office365(注1)やGoogle Apps for Works(注2)などのクラウドサービスを利用している場合，③その両方を利用している場合に分けられる。

スマートデバイスの導入では，“セキュリティ”と“利便性”のバランスを取り，それぞれを両立させることのできる仕組みが必要となる。“MINDセキュアモバイルマネジメント”は，スマートデバイスにおけるセキュリティと利便性の両立を実現したソリューションである。

MINDセキュアモバイルマネジメントを実現するため

の技術がEMMであり，EMMの構成要素であるMDM，MAM，MCMについて次に述べる。

（注１） Microsoft Office365は，Microsoft Corp. の登録商標である。
（注２） Google Apps for Workは，Google Inc. の登録商標である。

2.2.1 MDM（モバイルデバイス管理）

MDMは，企業のセキュリティポリシーに合わせてスマートデバイスの設定などを一元的に管理する製品又はサービスであり，パスワードの設定や，利用するアプリケーションの制限などスマートデバイス自体を管理する仕組みを提供する。

この機能によって，企業の情報システム部門では配布したスマートデバイスのハードウェアの一元的な管理，スマートデバイスごとにインストールしたアプリケーションの管理，アプリケーションのバージョン管理など，統合的にスマートデバイス及びスマートデバイス内にインストールされているアプリケーションの管理を行うことができる（**図１**）。さらに，万が一のスマートデバイスの紛失時には，拾得者が操作できないよう遠隔からロックを実施したり，デバイス自体を初期化して一切のデータを削除（ワイプ）したりすることによって情報漏えいを防止することが可能である。拾得されたスマートデバイスの90％は，拾得者がデバイスの中身にアクセスを試みているとの調査結果も出ており，この対策は必要である。

ただし，MDMによる遠隔からのロックや初期化はオンラインの状況で実施する必要があることや，スマートデバイス自体を管理する仕組みであるため，スマートデバイス内に保管している業務データだけを削除するようなことはできない。

現在，個人所有のスマートデバイスを業務用として利用するBYOD（Bring Your Own Device）を実施する企業が増加しているが，MDMの機能だけでは会社による個人データの管理や，紛失時の個人データを含めた全データの削除など，プライバシーや運用面での課題が存在する。

2.2.2 MAM（モバイルアプリケーション管理）

MAMは，スマートデバイスにインストールする業務用のアプリケーションを管理する機能であり，ソフトウェア製品として提供されるのが一般的である。利用する機能はコンテナ機能とラッピング機能の２つが代表的であり，アプリケーションに対して他のアプリケーションからのアクセス制限やデータ保護の設定を行うことによって，業務用のアプリケーションやスマートデバイス内に保管しているデータを安全に利用できるようにする。コンテナ機能は，スマートデバイスの内部をコンテナと言われる単位で特定の領域に分離し，同じコンテナ内部のアプリケーションであれば相互にデータの交換を可能にするが，コンテナ外部のアプリケーションとのデータの交換は制限するというものである。なお，コンテナ内部は暗号化をすることで，万が一スマートデバイスを紛失した際にも情報の漏えいを防ぐことができる。一方，ラッピング機能は，アプリケーション単位にセキュリティの機能を付加するものであり，この機能によって，個人アプリケーションから業務アプリケーションへのアクセスを制限し，個人アプリケーションが業務データを取り込むことを禁止したり，業務アプリケーションが社内のサーバなどへ接続する際には，自動的にVPNを設定して暗号化通信を行うなど，業務データの保護を可能にしている（**図２**）。

2.2.3 MCM（モバイルコンテンツ管理）

MCMは，先に述べたMDMやMAMとは異なり，スマートデバイスを業務でセキュアに活用するための機能であり，ソフトウェア製品として提供される。MCMによって，スマートデバイスから，社内のメールサーバやクラウド型メールシステム，クラウドストレージや専用のファイル共有型システムなどへ安全にアクセスできる環境を提供する。セキュリティ対策は，スマートデバイスの中にデータを保管する際にはファイルごとに暗号化を行ったり，コピーや印刷の禁止などのアクセス制限をかけたり，コンテンツの秘匿レベルに合わせてセキュリティの強度を管理することで実現する。さらに，専用のファイルストレージで管理する場合には，誰が，いつ，どのドキュメントを閲覧・編集したかのログを管理することが可能であり，不正

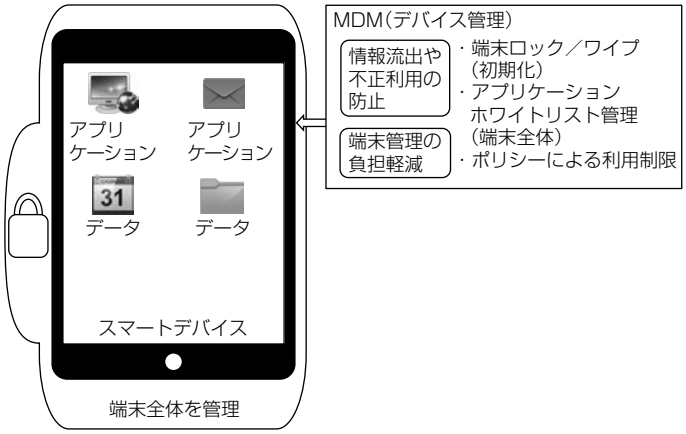
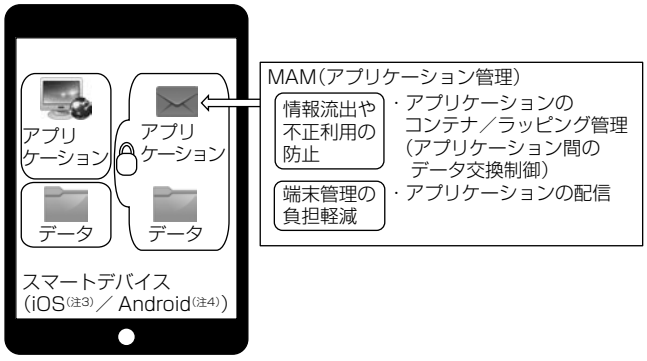


図１．MDM



（注３） iOSは，Cisco Systems，Inc. の登録商標である。
（注４） Androidは，Google Inc. の登録商標である。

図２．MAM

にダウンロードしているファイルを遠隔から削除することもできる。MCMによって，電子メールの送受信やグループウェアの利用，ファイルサーバやクラウドストレージと連携して業務データや文書ファイルの閲覧・編集などを簡易にかつ安全に行うことが可能となる(**図3**)。

MCMの活用としては，商品カタログや価格表など常に情報を最新に保つ必要のある情報を共有のファイルストレージに保管しておき，営業社員がスマートデバイスでこれらの情報にアクセスして活用する場面などが想定される。また，プレゼンテーション資料を共有のファイルストレージに保管し，営業社員が顧客への提案の際に事前にダウンロードして提案活動を行うことにも利用できる。MCMはスマートデバイスの中にデータを保管することができるため，通信の電波が届かない室内でのプレゼンテーションもあらかじめデータをダウンロードしておくことによって可能になる。

3. MINDセキュアモバイルマネジメント

スマートデバイスの管理は，MDMによるデバイスの管理から始まり，その後，アプリケーションの管理であるMAM，そしてスマートデバイスを活用するためのソリューションであるMCMがソフトウェア製品又はサービスとして市場に登場した。EMMはこれら3つの機能を併せ持ち，デバイスの管理からアプリケーションの管理，そして業務で活用するためのメールやグループウェアなどのアプリケーション連携を包括的に提供するものであり，企業でセキュリティを確保しながらスマートデバイスを活用するためのソリューションとして近年注目を集めている。

MINDは“スマートフォンマネージ”という名称でMDMサービスを提供しているが，これに加え，EMMの機能を“MINDセキュアモバイルマネジメント”という名称でサービスとして提供する(**図4**)。なお，EMMは市場ではソフトウェア製品として提供されており，サービスとしての提供は例が少ない。MINDは，各企業のスマートデバイスの利用環境に合わせて，最適なEMMの機能を導入しやすい“サービス”として提供することによって，企業の情報システムツールとしてのスマートデバイスの活用を支援する。

MINDセキュアモバイルマネジメントはセキュリティと利便性の両方を兼ね備えたサービスであり，次にその特長を整理して列挙する(**図5**)。

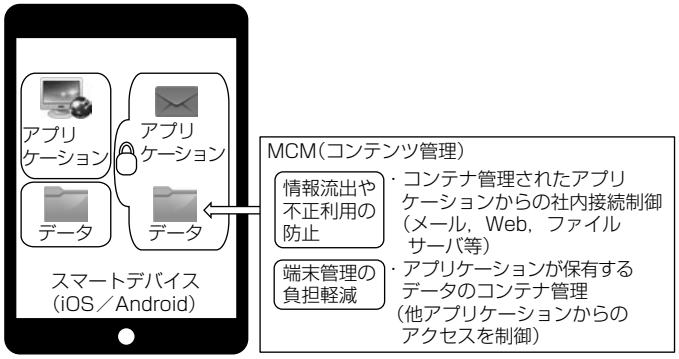


図3．MCM

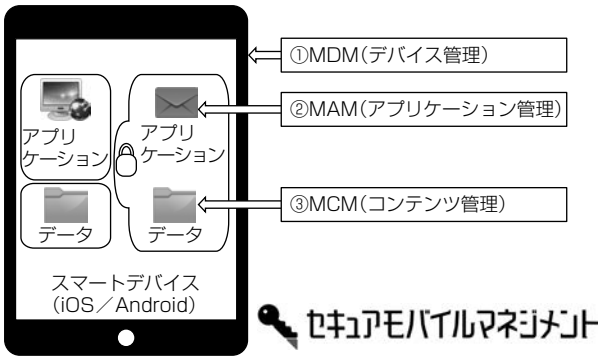
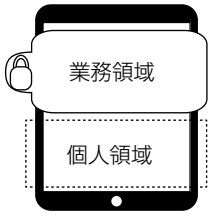
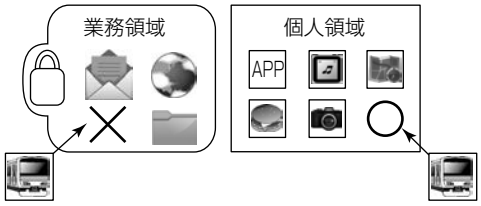


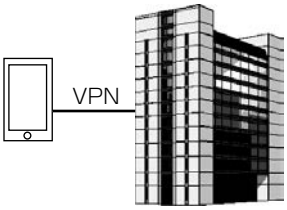
図4．MINDセキュアモバイルマネジメント



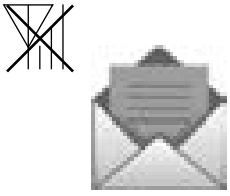
業務領域と個人領域との分離



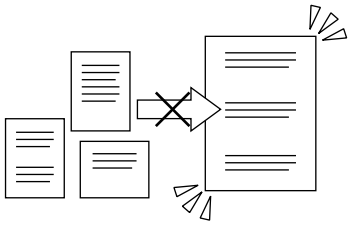
業務領域には業務アプリケーションだけを，個人領域は自由に利用



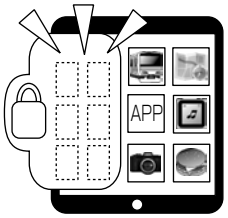
業務アプリケーションはVPNによる社内接続



オフラインでの閲覧・編集が可能



コピー &ペースト機能の制限



業務領域だけ初期化(ワイプ)

図5．MINDセキュアモバイルマネジメントの特長

(1) セキュリティの特長

①スマートデバイス内部を業務領域と個人領域にコンテナ機能で分離し，業務領域は暗号化によって保護する。

②業務領域は暗号化によって保護され，さらに遠隔から業務領域だけを削除することによって，デバイスの紛失時にも個人領域には影響を与えずに企業の情報漏えいを防ぐ。

③業務領域と個人領域の間でのデータの交換，文書のコピー／貼付けなどを一切禁止し，個人領域からの情報の漏えいを防ぐ。

(2) 利便性の特長

①アプリケーションごとに自動的にVPNを設定して暗号化通信を行うことで，セキュリティを確保しながら，VPN設定の手間を省き，迅速なアプリケーションの利用を可能にする。

②業務領域の暗号化によって，デバイス内にデータを保持し，オフラインで利用することができる。これによって，電波の届かない環境でのスマートデバイスを利用したプレゼンテーションや，メールやファイルの編集などが可能となり，生産性の向上につながる。

4. むすび

MINDセキュアモバイルマネジメントは，2016年度中のサービス提供開始を予定している。このサービスの提供によって，企業がスマートデバイスを“利用する”から“活用する”へと進化を遂げ，ワークスタイル変革そして生産性の向上を達成することを支援する。

また，スマートデバイスの業務利用とともに企業で急速に広まっているのがOffice365などのSaaS(Software as a Service)の利用である。ワークスタイルの変革に伴いスマートデバイスから，直接SaaSを利用する業務形態が今後増加していくものと思われる。これに対して，MINDではスマートデバイスの業務利用を含め，クラウドサービスをセキュアに活用するためのソリューションとして“MINDセキュアクラウドアクセス”を提供することも検討中である。今後，MINDセキュアモバイルマネジメントとMINDセキュアクラウドアクセスを組み合わせ，企業が安全にかつ利便性を損なわずに，スマートデバイスからクラウドサービスを活用する仕組みを提供していく。

参考文献

(1) (独)情報処理推進機構： 2014年度 情報セキュリティ事象被害状況調査 報告書 (2015)
http://www.ipa.go.jp/files/000043418.pdf