スマートデバイスによる社内リソースアクセスとセキュリティー

Intranet Access by Smart Device and its Security

井　上　将　生

要　約　スマートデバイスを社内システムに接続して使用するには，セキュリティー面の様々な脅威（紛失・盗難，悪意のあるユーザーによる情報漏洩，公衆 Wi-Fi，シャドー IT 等）への対策が必須となる．本稿ではこれらの脅威と対策について記述し，企業システムにおいてそれらを統一的に対策管理する製品として MDM/MAM/MCM を紹介する．MDM によるデバイス管理は以前より一般的に適用されてきたが，MDM だけの管理に限界があるケースもあることが認識されつつある．そこでスマートデバイス上にセキュアな業務領域を設定し，その領域内でアプリやコンテンツを管理する MAM/MCM といった概念が登場して，注目されている．

一方ネットワークの種類によって，スマートデバイスの管理上考慮しなくてはならない点もある．特に金融系のようにセキュリティーを重視する案件では，スマートデバイスを閉域網に接続させて使用するケースが増えているが，MDM 等のスマートデバイス管理基盤は閉域網と組み合わせて活用するには課題がある．ここでは問題の詳細と現時点でとりうる回避策について記述する．

Abstract　If you use the smart device by connecting with the Intranet system, security measures against various threats (device loss, theft, information leak by malicious user, public Wi-Fi, shadow IT, etc.) are needed. This paper describes these threats and measures and introduces the MDM/MAM/MCM as a product of unified management solution for these threats.

Previously device management by MDM has been applied in a general way, but there is a limitation in management only by MDM. So the following concepts appeared such as MAM to manage the business application on the smart devices, MCM to manage the content by setting a secure operational area on the smart device.

On the other hand, there are some points that must be taken into account in a smart device management according to the type of network. The cases that smart devices are connected to the closed networks are increasing, especially in the finance computer systems that focus on the security. But Smart device management infrastructure, like MDM has problem when the MDM is used in the closed network. This paper describes the detail of this problem and the workaround plan.

1. は　じ　め　に

社外に持ち出したスマートデバイスから社内リソースへ接続して使用する事例が増えてきている．業務で使用しているメールやスケジューラーをいつでもどこからでも閲覧できることから，利便性の向上と意思決定の迅速化を図ることができる．ただし実際の運用に当たってセキュリティー面の考慮が欠けていると，企業情報の漏洩に直結する危険性があることに留意しなくてはならない．

本稿では2章にて社内リソースへアクセスするスマートデバイスのセキュリティー上の脅威を挙げ，3章でその対応策や対応製品について，企業が保護すべきと判断したアプリやコンテンツを「業務領域」としてセキュアに管理するMAM（Mobile Application Management）を中心に記述する．また閉域網のような特殊なネットワーク環境で実際にシステムを構築した際の留意点も併せて記述する．

なお本稿では対象とするスマートデバイスとして，iOSもしくはAndroidが稼働するスマートフォンおよびタブレットを前提とする．企業で使用するスマートデバイスは，iOSとAndroidがほとんどのシェアを占めていること，企業向けのセキュリティー対策機能が両OSに比べてWindows Mobileは立ち遅れていることが理由である．

2.　スマートデバイスにおけるセキュリティー脅威

スマートデバイスと同様に社外に持ち出して使用するケースが多いノートPCについては，セキュリティー脅威とその対策が長く検討されてきた．ただスマートデバイスにはノートPCとは異なる固有の要素が存在するので，セキュリティー脅威と対策を検討するに当たっては，それらを視野に入れて考える必要がある．主なセキュリティー脅威を本章で説明する．

2.1　紛失・盗難

スマートデバイスはノートPCと比べると，重さ，サイズの面で携帯性が圧倒的に優れている．ただその反面，デバイス本体紛失の可能性が常に付きまとう．仮に社内リソースにアクセス可能なスマートデバイスを紛失し，悪意ある第三者に渡ってしまうと，以下のような脅威にさらされる危険性がある．

- ローカルに保存してあるファイルの漏洩
- 社内リソースアクセス手段の不正利用

2.2　機能の不正利用

一般的なスマートデバイスには，カメラ，Bluetooth，USB等の外部インターフェース，Wi-Fi，音声記録マイク等の機能が装備されている．またインターネット上の各種クラウドサービスへアクセスするためのアプリが標準でインストールされていることも多い．さらに常時インターネットに接続していること，各種アプリを検索・導入可能なアプリストアが用意されていることから，企業が想定しているもの以外のアプリを簡単に導入できる環境となっている．こうした機能が容易に利用できる点から，使用者がある意図をもって（若しくは無意識に）機密情報が含まれるデータを漏洩する可能性が出てくる．例えば

- 機密情報エリアでカメラを操作し，撮影する
- 業務アプリで使用したデータを，インターネットストレージクライアント経由でクラウドへ転送する
- 外部記憶装置を使ってデータを不正に保存し持ち出す

等が考えられる．

iOSやAndroid等のスマートデバイス用OSでは，システムの重要な領域にアクセスできないようにセキュリティー的に保護（アクセス制限）されている．ところがある手順を踏むとこ

うしたセキュリティー保護機能を迂回して様々な操作を実行することができるようになる．この手順を iOS では Jailbreak，Android では root 化と称している．企業で使用するスマートデバイスで Jailbreak/root 化が行われると，ベンダーが提供する公式アプリストア（App Store や Google Play）以外からもアプリを入手できたり，ユーザーのアクセスが禁止されているシステム領域をアクセスできるようになるが，それはセキュリティー的に非常に危険な状態である．

2. 3　公衆 Wi-Fi

Wi-Fi 接続機能を持つスマートデバイスは，社外の公衆 Wi-Fi スポットに接続することができる．また一度接続してしまうと，次回からその公衆 Wi-Fi スポットに近づいただけで自動接続することも可能である．公衆 Wi-Fi のなかには，暗号化がされていない，もしくは暗号化強度が弱い状態に設定されているものも多くあり，接続端末への不正アクセスやマルウエア感染を狙った野良 Wi-Fi も存在するため，第三者によって通信内容が盗聴される可能性がある．

2. 4　シャドー IT

企業が管理するシステムの範囲外の機器やサービスを業務に使用することをシャドー IT と呼び，企業システムをセキュリティー脅威にさらす恐れがあるとして問題となっている．スマートデバイスに関しては，私物デバイスを業務に使用する，企業配布デバイスであってもクラウドサービスを私用アカウントで使う，といったケースがあり，管理者の監視の目が届かないため，セキュリティーリスクが高い状態となる．

3.　スマートデバイスに必要なセキュリティー対策

前章で述べたとおり，スマートデバイスに搭載されている機能には，便利なものがある反面，注意深く使用しないとデータ漏洩等のセキュリティー脅威につながるものも存在するため，セキュリティー対策を行う統一的な仕組みが必要である．

3. 1　セキュリティーポリシー

企業でスマートデバイスを使用する場合には，情報資産を守るために，紛失時の対策，利用を許可/禁止する機能やアプリなど，セキュリティー対策のルールを定めることが必要である．また，Jailbreak/root 化されたスマートデバイスはセキュリティー上の非常な脅威となりうるため，このような改造を禁止，もしくは検知できる仕組みがあることも必要である．

3. 1. 1　紛失時対策

紛失時の対策としては，「データ暗号化」「リモートワイプ」がある．iOS や Android では OS レベルで暗号化機能を実装しており，スマートデバイス上に保存されたデータの保護に有効である．OS や機種によってはデフォルトで暗号化機能が有効になっていない場合がある（例：iOS ではパスコードを設定することで暗号化が有効になる）ので，運用に当たっては注意する必要がある．また 3. 3 節で述べる MAM 機能では，業務で使用するデータ領域だけを OS とは別の暗号化機能で保護することができる．

リモートワイプは紛失，盗難デバイスに対して，リモートから工場出荷時の状態へ初期化する機能である．デバイス上の全てのデータが消去される強力な機能であるが，デバイスがネットワークに繋がっていなくてはならないこと，電源が入っていなければならないこと等の前提条件があり，実行確実性は必ずしも高いものではないため，パスコードの適用を強制するなどの基本的な対策が重要となる．

なお紛失時の情報漏洩を防ぐものではないが，紛失，盗難デバイスが初期化されて転売されることを防ぐ「アクティベーションロック」という機能がある（iOS のみ）．デバイスのデータ初期化や再アクティベート時に，AppleID とパスワードの入力が要求されるようになるもので．デバイス盗難時に取得者のアカウントで初期化されて使用されることを防ぐ．

3. 1. 2　機能制限

情報漏洩につながる機能を制限することも考える必要がある．制限対象の機能としては「カメラによる撮影」「カードスロットから外部記憶への書き込み」「USB 接続した外部記憶への書き込み」等がある．また OS のバージョンアップに伴い新しい機能が日々追加されている現状で，企業で使用される全てのスマートデバイスに対して，機能制限を行う統一的な仕組みが必要である．

3. 1. 3　アプリ制限

業務と関係のないアプリを導入されることを防ぐため，不要なアプリが勝手に導入されない仕組み，もしくは導入されたことを速やかに検知する仕組みが必要である．

3. 2　Mobile Device Management によるデバイス管理

企業においてスマートデバイスを使用するには，各種機能制限，セキュリティーポリシーを適用する必要があるが，これらを統一的に設定・管理するソリューションとして，Mobile Device Management（以降，MDM と表記）製品がある．MDM の主な機能は以下のとおり．

- 管理デバイスのインベントリー情報収集
- デバイスレベルの機能制限を強制設定
- Jailbreak 検知，パスワード強制のセキュリティーポリシー設定
- 紛失時のリモートロック，リモートワイプ
- 位置情報取得
- アプリホワイトリスト，ブラックリスト，商用ストア（App Store や Google Play）利用禁止

企業がユーザーにスマートデバイスを配布して使用する場合，各種機能制限・セキュリティーポリシーを統一的に適用するために MDM は有用である．ただ機能を制限することやセキュリティーを強固にすることで，スマートデバイス本来の有用性，利便性をスポイルしてしまう側面があることも事実である．このため実際の運用の場面では，せっかくスマートデバイスを社員に配布しても電話としてしか使われずうまく活用できないケースや，逆にスマートデバイスに詳しい社員が企業の管理ポリシーをかいくぐって便利な機能を使おうとするケース（シャドー IT）が出てきている．

3.3　MAM と MCM

前節で述べた MDM の限界を踏まえ，スマートデバイスそのものを強固に管理するのではなく，企業が保護すべきと判断したアプリやコンテンツそのものをセキュアに管理し，それ以外の企業システムに関係ない領域はスマートデバイスの利便性を損なわないレベルのセキュリティーポリシーとする，という考え方が出てきた．これらが Mobile Application Management（以降，MAM と表記），Mobile Content Management（以降，MCM と表記）と呼ばれるものである．MAM と MCM は MDM と協調して稼働することで真価を発揮する概念で，MDM が不要になるということではない．例えば MDM で基本的なセキュリティーポリシーを適用し，企業エリアは MAM/MCM で強固に管理するといった階層的なセキュリティー対策ができる等，企業のスマートデバイスの利用形態やセキュリティーの考え方に柔軟な対応が可能となる．この三者の機能を合わせたものを EMM（Enterprise Mobility Management）と称している．本節では MAM と MCM について述べる．

3.3.1　MAM 概要

MAM の基本的な考え方は，スマートデバイス内にセキュアな仮想領域を定義し，そこに業務アプリ（例えば社内システムにアクセスして重要データを取り扱う等）だけを格納できるようにすることである．この仮想領域を「業務領域」と呼ぶ．業務領域に格納されるデータが暗号化されるのはもちろんのこと，データの受け渡しを業務領域内に制限する機能や，業務領域に格納されたアプリだけが使用できる VPN，またセキュリティー違反が発生したときに VPN の接続をブロックする，業務領域のアプリとデータだけをワイプする，といった機能が実装される（図 1）．これにより業務領域をセキュアな環境に保つことができ，またスマートデバイス全体に影響を与えることなく業務領域だけをワイプできるようになる．

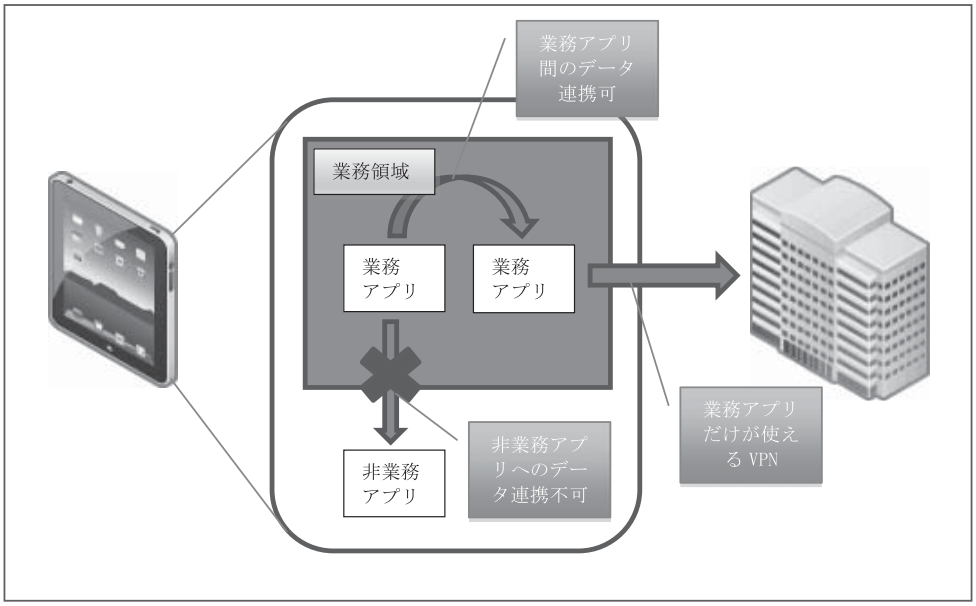

図 1　MAM の概要図

3. 3. 2　MCM 概要

MAM がスマートデバイスのアプリを管理するソリューションであるのに対し，MCM は業務アプリのコンテンツを管理するソリューションである．MAM と同様に「MCM とは何か」という明確な定義は存在せず，また「管理」という言葉で若干誤解を招くところもあるが，各ベンダーから出ている MCM 対応製品の機能からは，「スマートデバイスから社内やクラウドに保存してあるファイル/データをセキュアに閲覧・編集するための仕組み」という定義が実態に近い．管理対象がアプリかコンテンツかの違いであり，個々の技術要素は MAM と共通していることが多い．

3. 3. 3　業務領域の実装機能

本項では MAM の基本的な考え方である業務領域について述べる．

1）　業務データのセキュリティー制御

iOS や Android ではアプリ間でデータを受け渡す仕組みが標準で用意されている（iOS では Open-In，Extensibility（iOS 8 以降），Android では共有，Intent）．このため業務アプリで使用したデータを，クラウドサービスにアクセスするアプリに受け渡す等してインターネット上にアップロードすることが容易にできてしまう．

MAM では業務領域と非業務領域間でアプリのデータ受け渡しを許可/禁止することが可能となる．これにより業務領域で使用したデータファイルを，非業務領域にインストールされたアプリに引き渡すことを禁止することができる．

またスマートデバイスの種類/OS/管理サーバー製品の種類によっては，業務領域にインストールされたアプリ上でのコピー＆ペーストの禁止，印刷の禁止，スクリーンショット取得の禁止等の機能も提供される．

2）　セキュアな通信経路

スマートデバイスから社内システムへアクセスする手段として，一般的に利用されるのは VPN である．しかし VPN はデバイス単位でコネクションを確立するため，アプリ単位の有効/無効を定義できず，スマートデバイスに業務と関係のないアプリが導入されていたとすると，そのアプリも VPN 経由で社内システムへアクセスできてしまう可能性がある．

MAM ではこうした問題を回避するため，業務領域に格納されたアプリ単位で個別に設定可能な VPN が利用できる．これにより業務アプリは VPN で社内システムへアクセス可，そうでないアプリはアクセス不可というような構成が可能となる．

3）　アプリの管理

業務領域には企業で管理されたアプリだけをインストールすることができる．スマートデバイス使用者が App Store や Google Play から勝手に導入するアプリを業務領域に格納することは禁止される．アプリの導入は管理サーバーからの指示によってエンドユーザーが行うのが一般的だが，スマートデバイスの種類/OS/管理サーバー製品の種類によっては，強制インストール/強制アンインストールが可能なケースもある．

4)　アプリの設定配布

管理サーバーから業務領域に格納されたアプリの設定・構成情報を配布することができる．例えばある URL にアクセスするアプリに対して，管理サーバーから全ユーザーのアプリに該当 URL 設定を配信する，といったことが可能である．

5)　認証

業務領域に導入されたアプリに対して，独自の認証を設定することができる．例えばアプリ起動時に OS とは別のパスコードを設定する等である．

6)　セレクティブワイプ

通常 MDM 製品にはリモートワイプ機能が実装されている．これはスマートデバイス紛失等の緊急時にネットワーク経由でリモートからワイプすることができる機能である．ワイプするとスマートデバイスは工場出荷時の状態に初期化され，デバイス上のアプリやデータは全て消去される．ただしスマートデバイス全体が初期化されてしまうので，BYOD のように業務以外のアプリやデータが導入されているスマートデバイスでは不都合がある．

セレクティブワイプは業務領域に格納されたアプリとデータだけを初期化できる機能で，ワイプを実行しても業務領域外のアプリやデータに影響を与えることはない．

3. 3. 4　コンテンツビューアー

スマートデバイスから社内やクラウドにあるファイルをセキュアに閲覧・編集する機能である．「セキュアに閲覧・編集」という特徴はベンダーの実装にある程度差異はあるが，概ね以下のような機能が実装されていると考えてよい．

- 認証
  アプリ起動時のパスコード設定
- 暗号化
  OS レベルとは別のアプリ独自暗号化
- ローカルキャッシュ禁止/暗号化
  ファイルデータをローカルに保存することなく閲覧する，もしくは保存したとしても暗号化して保存する機能．これによりスマートデバイス紛失時のデータ漏洩を防ぐ
- Open-In，印刷，コピー＆ペースト禁止
- アプリ単位の VPN
- セキュリティー違反発生時のデータ保護
  MDM と連携して，セキュリティー違反が発生したときに VPN 接続のブロック，保存データの削除等のアクションを実行する

個別要素は MAM と共通する部分が多く，MAM の管理基盤上で MCM のソリューションが稼働する形になっていることがわかる．

3. 3. 5　セキュアブラウザー

コンテンツビューアーの一種であり，Web コンテンツに特化した形でコンテンツをセキュアに閲覧するための仕組みがセキュアブラウザーである．データ暗号化，ローカルキャッシュ禁止，データ連携制御といったセキュリティー要素はコンテンツビューアーと同様である．

多くの場合標準ブラウザーとの細かな仕様の違いがあり，導入時にシステムが問題なく稼働するかどうかの検証が必須である．

3. 3. 6　MAM の動向

MAM は MDM ベンダーが機能を拡張していく形で実装されてきた．2013 年頃から MDM ベンダーがいくつか対応製品を提供しているが，当時は注目度が高かったもののそれほど導入が進んだという結果にはならなかった．これは主に以下の理由があったと考えられる．

- ベンダー提供の API に対応するようソースコードを修正して，対応 SDK でコンパイルしなおさなくてはならない
- 対応アプリは該当 SDK を提供する MDM でしか MAM 機能が動作しない
- 自社開発ではないアプリ（App Store や Google Play から入手できる通常アプリ等）は対応できない，もしくは事実上不可能

しかし 2013 年後半に Apple が Managed Apps を，2015 年前半に Google が Android for Work を発表した．これらは OS ベンダーが提供する MAM 基盤を外部 EMM から制御する構成をとっている．対応アプリはベンダー独自の SDK で再コンパイルする必要はなく，通常のアプリがそのまま使えるため，これまでの製品より敷居が低くなり，企業の導入がしやすくなってきている．

3. 3. 7　製品実装の例

本項では 2015 年 10 月現在で利用可能な MAM の製品実装例を 2 点と MCM の製品実装例を紹介する．最初は EMM ベンダーの実装の代表として MobileIron 社の AppConnect，続いて Apple の Managed Apps である．

1）　AppConnect

EMM ベンダーとして古くから対応製品をリリースしている米国 MobileIron 社の MobileIron は，MAM 対応機能として AppConnect を提供している．AppConnect SDK でコンパイルした対応アプリはセキュアコンテナー化され，スマートデバイスに導入することでスマートデバイス上の業務領域を構成する一要素となる．セキュアコンテナー化された AppConnect アプリは以下の機能を持つ．

- Open-In 許可/禁止，コピー＆ペースト許可/禁止，印刷許可/禁止（iOS のみ）
  Open-In については許可先を「全アプリ」「AppConnect アプリ」「ホワイトリストに定義されたアプリ」から選択可能．
- スクリーンキャプチャー許可/禁止（Android のみ）
- アプリ設定配布
  AppConnect 対応アプリの設定情報を管理コンソールから配布可能．その際固定パラ

メーターだけでなく，MobileIron で提供する変数（ユーザー ID，パスワード，メールアドレス等）も利用可能.

- アプリ単位の VPN（AppTunnel）
  MobileIron Sentry というゲートウェー製品を経由して社内リソースにアクセスするための VPN．Sentry が VPN のゲートウェーとして動作するため，VPN サーバー機器は不要．MDM 管理コンソールから各 VPN セッションの許可/禁止を設定することが可能．また MDM でセキュリティー違反を検知したときに，該当デバイスからの接続を自動ブロックすることができる.
- パスコード認証

AppConnect アプリは AppConnect SDK でコンパイルする方法に加えて，アプリのバイナリーファイルを MobileIron 社に送付して AppConnect 対応アプリに変換してもらうラッピングサービスを利用することもできる．ただし App Store や Google Play から入手したアプリを変換することはできない.

AppConnect は MAM としては先行して市場に投入されているため，機能面では最も充実している製品の一つである．Open-In 等のデータ連携制御はかなり細かな制限が可能であるが，前項「MAM の動向」で記述したとおり，アプリを MobileIron 社が提供する API に対応するように書き換えてリコンパイルする必要がある．したがって自社開発アプリを自社内で利用するケースが主となる．また SDK は iOS/Android のどちらも提供されているので，マルチデバイス環境への適用で有利である.

2） Managed Apps

Apple 社が提供する Managed Apps は，iOS 5 から iOS の MDM サービスで提供されている機能で，MDM 管理下のスマートデバイスでセキュアなアプリ管理を行うための仕組みである．iOS 7 より MAM に関連する機能が多く追加された.

Managed Apps は MDM 製品と連動する機能で，MDM から Managed Apps としてスマートデバイスに導入したアプリが対象となる．MobileIron も Managed Apps に対応した MDM 製品で，アプリ配布機能からスマートデバイスにアプリを導入すると，当該アプリは Managed Apps となりスマートデバイス上の業務領域を構成する一要素となる．AppConnect と異なり，Managed Apps は対応 SDK で再コンパイルする必要はなく，App Store で配信されている一般アプリも Managed Apps として導入することが可能である.

Managed Apps として導入されたアプリは以下の機能が利用可能となる.

- アプリ間データ連携制御（Managed Open-In）
  業務領域（Managed アプリ）から非業務領域（非 Managed アプリ）へ，またはその逆の Open-In 許可/禁止の制限が可能．現時点で AppConnect のように許可先を細かく定義するようなことはできない.
- 設定配布（Managed App Configuration）
  plist 形式の定義ファイルを MDM 管理サーバーへアップロードすることで，アプリの設定をスマートデバイスに配布することが可能．アプリは NSUserDefaults クラス

で plist からパラメーターを読み取る処理を実装している必要がある．MobileIron から設定を配布する場合は，MobileIron で提供する変数（ユーザーID，パスワード，メールアドレス等）が利用可能．

- アプリ単位の VPN（Per App VPN）
  アプリ毎に VPN の接続を確立できる機能．業務アプリ（Managed アプリ）は VPN 経由で社内リソースにアクセスし，それ以外のアプリ（UnManaged アプリ）は VPN を使用できない，といった制御が可能となる．AppConnect と違うのは，VPN ゲートウェー機器が別途必要な点である．

Managed Apps は Apple が標準で OS に組み込んでいる機能であること，通常の App Store から配信されるアプリでも利用可能であることが特筆すべき点である．この意味でベンダー固有の実装を採用するよりハードルは低いと思われる．ただし AppConnect に比べると制御できる範囲や機能は少ない．また MDM 製品と連動して稼働する機能であるが，現時点で Managed Apps に対応する EMM 製品は，MobileIron や Citrix 等海外製品が主体であり，国内ベンダーの MDM 製品では対応している製品が少ないのが現状である．さらに当然のことながら Android では使えないので，iOS/Android が混在している環境では統一した管理ができない．

3） Docs@Work/Web@Work

MobileIron が提供する MCM 製品は，コンテンツビューアーとして Docs@Work，セキュアブラウザーとして Web@Work がある．Docs@Work はスマートデバイス上から社内リソースの SharePoint サーバー，WebDAV サーバー，CIFS サーバーに格納されたファイルの閲覧・編集が可能な製品である．社内リソースへの接続には MobileIron Sentry というゲートウェーを DMZ に導入することで実現する．ビューアーは専用アプリとしてスマートデバイスに導入して使用する．閲覧可能なファイルは PDF，Word，Excel，PowerPoint 等一般的なフォーマットをサポートする．

3. 4　ネットワークの種類に応じた管理

本節では，スマートデバイスを用いるネットワーク環境に応じた管理の考慮点を述べる．

3. 4. 1　VPN

社外にあるスマートデバイスから社内リソースにアクセスする手段として一般的なのは VPN である．ただし 3. 3. 3 項の 2）で記述したとおり，スマートデバイスから VPN でトンネルを確立すると，スマートデバイス内の全てのアプリが社内リソースにアクセス可能となってしまい，業務に関係のないアプリが導入されているとそこから情報漏洩の恐れがある．それを防ぐために Per App VPN（iOS 7 以降）や AppTunnel（MobileIron）といったアプリ単位の VPN が提供される．

3. 4. 2　Wi-Fi

スマートデバイスを業務に利用する場合，社外ではキャリアー回線（＋VPN），社内では

Wi-Fi 接続という形態が想定される．現状の iOS では，社内の Wi-Fi に接続するためのプロファイルや証明書は MDM で配布することができるが，それ以外の Wi-Fi 接続を禁止することはできない．これはエンドユーザーがスマートデバイス側で Wi-Fi 接続設定を自由に追加できるためで，公衆 Wi-Fi などセキュリティー的に脆弱な出所不明の基地局への接続を制限できないことになる．このことからも，デバイスレベルの機能制限だけでは十分ではなく，アプリやコンテンツレベルのデータ保護という視点が重要となる．

なお一部の Android では，所定の SSID のアクセスポイントにしか接続できないように制限することは可能である．

3. 4. 3　閉域網

スマートデバイスはインターネットに接続できるようになっていることが原則であるが，特にセキュリティーを重視する顧客のために，閉域網に接続するネットワーク構成をとることも可能である．通信事業者の閉域網サービスにモバイル向けオプションが用意されていて，例えば自社の閉域網に接続するための特殊な SIM を提供しているようなケースがある．この SIM を挿入したスマートデバイスは閉域網に参加することができる．

閉域網に接続したスマートデバイスは，インターネット接続を前提とした App Store/Google Play やマップ等のサービスを利用できないが，インターネットからの不特定多数の脅威にさらされないので，セキュリティー的には強固である．特に金融系の顧客では閉域網が要件に含まれることも多い．

ただし閉域網と MDM を組み合わせるには解決しなくてはならない課題が存在する．MDM は管理下のスマートデバイスと MDM 管理サーバー間の通信に，各 OS ベンダーのプッシュサービスを使用している．例えば MDM 管理サーバーからポリシーを各スマートデバイスに配布する場合，MDM 管理サーバーはプッシュサービスに構成が変わったことを示すイベントを送信し，スマートデバイス側はプッシュサービス経由で MDM 管理サーバーが何か通信しようとしていることを検知して，そこで初めて MDM 管理サーバーへのコネクションを確立してポリシーをダウンロードする（図 2）．このプッシュサービスは iOS では Apple Push Notification Service（以降 APNs と略記），Android では Google Cloud Messaging（GCM）という名称で，インターネット上で提供されているサービスである．必然的にプッシュサービスを使用している MDM（ほぼ全ての MDM 製品が該当）はインターネットに接続できることが前提となり，閉域網内では使用できない．

この問題の回避策は今のところ以下が考えられる．

1. 閉域網内からプッシュサービスへ接続するためのポートを開ける
2. MobileIron に実装されている常時接続オプションを使用する
3. 閉域網対応 MDM 製品を使用する

1. は閉域網サービスを提供する通信事業者に依頼し，APNs であれば TCP ポート番号「5223」「2195」「2196」，GCM であれば「5228」を各プッシュサービスの FQDN 向けに疎通できるようにする対応である．ただ TCP ポートを開ければプッシュサービスが使用できるようになるとは限らないことに注意が必要である．プッシュサービスの接続要件には以下のようなものが存在する．

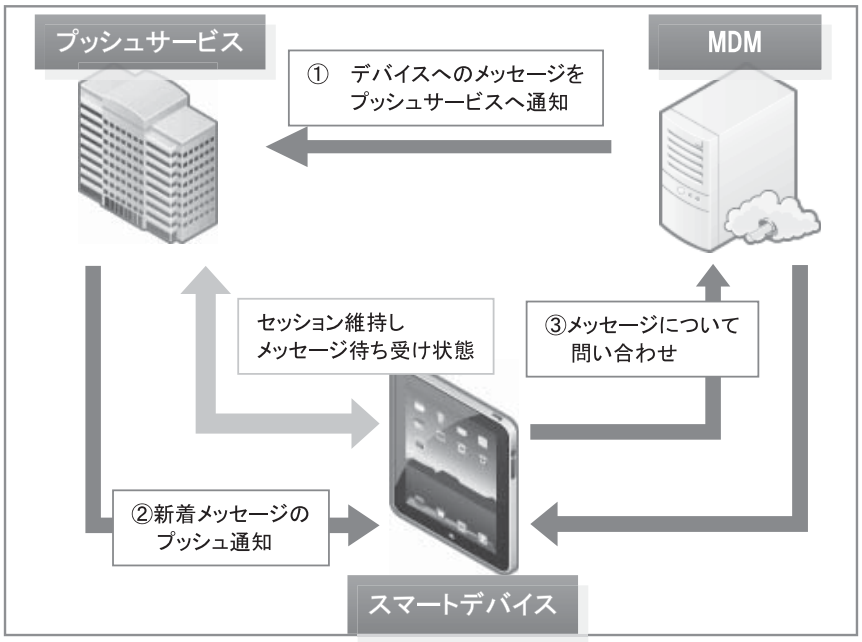

図 2　MDM とプッシュサービスの仕組み

- スマートデバイスとプッシュサービス間のコネクションは常に確立している必要がある．中間に無通信タイムアウトを監視するようなモジュールがあってはならない
- プッシュサービスへの通信は HTTP(S)ではないので，プロキシーが介在してはならない

閉域網からインターネットへの接続オプションは，提供する通信事業者により仕様が様々なので，結局のところ実際の通信環境で検証してみないとわからない，というのが実情である．またせっかく閉域網を採用してセキュリティーが強固な状態なのに，わざわざインターネットへのポートを開ける，ということに難色を示す顧客もある．

2. は MobileIron に実装されている機能で，MDM 管理サーバーとスマートデバイスが，プッシュサービスを使わず直接接続することで管理を行うものである．この機能はプッシュサービスそのものを使用しないため，インターネットへの接続ポートを開ける必要はない．閉域網のネットワーク構成に大きな変更を加える必要がなく，セキュリティー強度が変わらないことが利点であるが，対応機種が Android のみに限定されていることが欠点といえる．

3. は 2014 年以降，国産 MDM で閉域網に対応する製品がいくつか発表されている状況である．現時点では実績面で不透明なところがあるが，需要は大きいため今後は順次環境が整備されてくるものと思われる．

上記の通り，閉域網でのスマートデバイス運用はニーズがあるものの，閉域網内で MDM を使用する場合に問題があり，今の時点では 2. の対応を行うのがベストであると考えられる．ただしあくまで現時点の最適解であり，日々新製品/新機能が追加されている分野であることから，今後よりよい対応策が出現することを期待したい．

4. お わ り に

「スマートデバイスで社内システムにセキュアにアクセスしたい」というユーザーの要望は増えているが，それが具体化したときに管理をどうするか，セキュリティーをどう考えるか，といった点は，まだ決定的な方法論があるわけではなく，試行錯誤を続けていかなくてはならない部分がある．MAM という概念も，従来から注目されてはいたものの，様々な MDM ベンダーが固有な実装を提供していた経緯もあり，拡張性や将来性に疑問を持たれる場合があった．しかし Apple や Google といった OS ベンダーが MAM 機能を標準提供するようになったことから，そうした懸念が払拭され，今後はスマートデバイスにおける主流のセキュリティー技術として認知されていくと思われる．方向性としては，デバイスとアプリ，コンテンツがバラバラなソリューションで管理されるのではなく，EMM で統一的に管理する将来像が予想されるが，本稿で記述した MAM 機能はその基礎となるインフラ技術となるであろう．

参考文献　［1］ MobileIron, “AppConnect”,
https://www.mobileiron.com/ja/products/product-overview/appconnect
［2］ Google, “Android for Work 概要”,
https://support.google.com/work/android/answer/6095397?hl=ja

※上記参考文献の URL は，2015 年 10 月 16 日現在の存在を確認．

執筆者紹介　井　上　将　生（Masao Inoue）
1991 年日本ユニシス(株)入社．主に Unix，Windows 等で稼働するソフトウエアプロダクトの保守業務に従事．2006 年ユニアデックス(株)転籍．LDAP/認証系プロダクトの製品主管を経て，現在はモバイルデバイス管理製品の主管を担当．