安全で便利な モバイル・デバイスの社内利用

エンタープライズ・モビリティー・マネジメントを実現する 「IBM MobileFirst Protect」

スマートフォンやタブレットの業務活用の推進により、モバイル・デバイスの管理の重要性は日々増してきています。初期のモバイル・デバイス管理は、デバイス機能の制御を主な目的として、できることを制限することでセキュリティーの確保を行っていました。スマートフォン、タブレットで得られる利便性を削ることで安全性を確保するという考え方でした。この手法では確かに安全性の確保はできますが、利便性は大きく下がってしまいます。そこで単にデバイスの機能制限だけで安全性を確保するのではなく、安全な社内環境への接続やデータ・セキュリティーの確保などをモバイル・デバイス管理に追加する形で、安全性を確保しつつ利便性も追求するソリューションが登場してきました。

「IBM MobileFirst Protect」（旧製品名: MaaS360）は、まさに安全性と利便性を同時に確立することができるソリューションです。ここでは、モバイル・デバイスの社内利用における課題とその解決を行うIBM MobileFirst Protectをご紹介します。

1. モバイルの活用

2011年には世界のスマートフォン出荷台数がPCの出荷台数を超え、2012年には日本の携帯電話出荷台数の半数以上がスマートフォンになっています。2016年には世界の企業において3億5千万人の社員がモバイル・デバイスを使用し、そのうち2億人が個人所有のデバイスを使用するという予測もあります[1]。モバイル・デバイスの企業利用が急速に進んでいる状況において、そのデバイスのセキュリティーを確保することが企業の課題になっています[2]。

欧米では利便性に注目し、セキュリティーにはあまり注目せずにモバイル・デバイスの企業利用を推進した結果、ほとんどの企業でモバイル・デバイスの業務利用を原因とするセキュリティー事故を経験しています。逆に日本ではモバイル・デバイスの業務利用にあたりセキュリティーを強固にし、デバイスの機能制限を重要視した結果、多くの企業でモバイル・デバイスが従来の携帯電話と同様にメールと電話機能のみに制限された運用となってきたという現状があります。セキュリティーと利便性の両立ができないという典型的な事例と考えられます。この日本の事例のように、当初モバイル・デバイス管理は機能制限から始まりました。そして、モバイル・デバイスの機能制限＝利便性の阻害要因と考えられていました。

この一見相反する二つの要因を両立させるために、エンタープライズ向けのモバイル・カタログ、VPNによらない安全な社内接続、コンテナ化、モバイル・デバイス

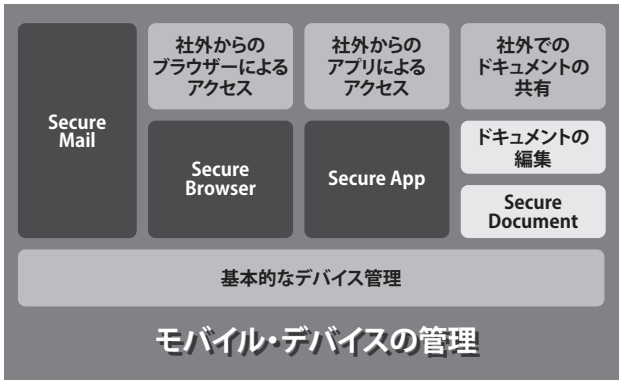

図1. IBM MobileFirst Protectによるエンタープライズ・モビリティー・マネジメント

管理から広がったエンタープライズ・モビリティー・マネジメントが必要とされています（**図1**）。

2. 企業利用におけるアプリ配布の課題

モバイル・アプリはアプリ・ストアでダウンロードしてインストールするのが一般的です。アプリ・ストアは、課金、バージョン管理、評価・コメント付けなどの機能を提供してくれます。しかし、この環境を社内アプリでそのまま使うのは望ましいことではありません。

そのアプリは、すべてのユーザーの目に留まる場所に置かれています。たとえ使えないようにしていたとしても、ダウンロードすることは可能だからです。アプリを社内利用する場合に、In-House型配布という方法があります。そのような配布方法では、アプリをダウンロード可能な形式にビルドし、httpサーバーなどに置くことでアプリを配布できます。多くの場合、その配布は単純なhttpサーバーで、バージョン管理やカタログ化などは自作することになります。

●カタログ機能

IBM MobileFirst Protectでは、社内アプリ利用に対応したカタログ機能を提供します。IBM MobileFirst Protectのカタログ機能はアプリ・カタログと呼ばれ、モバイル・デバイスにインストールされます。管理はWebブラウザーにてアクセスするポータルから実施します。管理者は社内利用するアプリをWebブラウザーからアップロードするだけで登録できます。また、このカタログはiOS・Android・Windows Phoneといった各プラットフォームのアプリを統合的に登録・管理できます。そのため、プラットフォームごとの管理などは必要なくなります。

●App Storeアプリも登録・インストール可能

スマートフォンやタブレットを社内利用するにあたり社内開発したアプリだけを使用するのであれば、社内アプリ配布機能だけで十分かもしれません。初期のモバイル・デバイス管理を考えると確かにそれでも事足りていた時期があります。しかし、たとえ社内利用とはいえ、モバイルで活躍する社員は社内利用アプリだけではスマートフォン、タブレットの活用に限界があると感じています。簡単な調べ物や次の約束へ向かうための経路の検索など、公開アプリで提供されているサービスの活用の必要性は日々高まっています。さらに、基幹システムに他社のサービスを利用している場合、そのモバイル・アプリは公開アプリとしてだけ提供されている場合もあります。

そのためIBM MobileFirst Protectのアプリ・カタログは、社内アプリだけでなく、App StoreやGoogle Playのアプリも登録することができます。社内アプリと同列に公開アプリもカタログに登録し、ユーザーに公開します。公開アプリの登録は管理者が選択しますので、カタログには管理者が推奨するアプリのみが表示され、ユーザーは管理者が認めたアプリを安心してインストールすることができます。このようにIBM Mobile First Protectのアプリ・カタログ機能を使うことで、社内専用のカタログを公開し、アプリを安全に配布・管理することが可能になります。

3. 企業イントラネット・アクセスの障壁

モバイル向け社内アプリを作成した場合、イントラネット上にあるコンテンツへのアクセスや、社内システムとの統合はどのように行えばよいのでしょうか。

Webブラウザーで操作するようなWebアプリであれば、VPNを使ってイントラネットにアクセスし通常のブラウザーでアクセスさせることができます。しかし、その方法には通常アクセス元のアプリを限定できない課題があり、デバイスおよびそこにあるすべてのアプリが信頼できるものでない限り、社内アクセスにおけるセキュリティー・ホールとなってしまいます。特に社内アプリだけでなく公開アプリの使用も認めている場合、そのアプリが原因となりイントラネットへ悪意のある第三者の侵入を許してしまうことになりかねません。App Storeは審査が厳しく行われているので安心だと考える方も多いかと思いますが、そのiOS上でもマルウェアが発見され始めています。たとえユーザーに悪意がなくとも、そういった一見無害に見えるアプリと社内接続のためのVPNによって、それまで頑強にセキュリティーを守っていたイントラネットへ、簡単に悪意のある第三者の侵入を許してしまうことになります。

また、Webブラウザーや各アプリ、メールなどを使用して各種データをモバイルで参照・編集などを行うよ

うになると、そのデータの扱いについても課題があります。イントラネットのファイル共有サーバーやメールなどで入手したデータは各プラットフォームに保管されます。これは安全でしょうか？　例えば、悪意のない場合でも簡単に情報漏洩が起こる例として連絡先データがあります。メールや電話をするために登録している社内外の連絡先のデータは、他のアプリから参照されることがあります。アプリ導入時に連絡先へのアクセスを許可するかどうかを聞かれた記憶のある方も多いと思います。ここで許可をすると連絡先のデータはそのアプリから自由にアクセス可能になります。SNSアプリや無料通話アプリでは連絡先のデータを参照できて便利ですが、このデータはアプリ内に留まりません。それぞれのサーバーへアップロードされ、ユーザーが承諾した各アプリの規約の下、使用されてしまいます。このようにイントラネットへのアクセスとそこから各デバイスに保管されるデータの扱いには課題があることが分かります。

●Mobile Enterprise Gatewayによる安全な社内接続

Mobile Enterprise Gatewayはイントラネット内で動作させるサービスです。サービスとして稼働しクラウド上のIBM MobileFirst Protectと連携し、スマートフォン、タブレット上で稼働するアプリのイントラネット・アクセスを中継します（**図2**）。このような動きを見るとVPNと変わらないように見えます。VPNとの違いの一つに外部からのアクセスの処理方法があります。

Mobile Enterprise Gatewayは外部に対してPortをListenして待つことはしません。稼働開始とともにクラウド上のIBM MobileFirst Protectの環境にアクセスしセッションを張り、そのまま待機します。つまり、内側から外側へのアクセスでセッションを確立し、以後外部からの要求はこのセッションを通して処理されます[3]。もちろん、通信は暗号化されます。

VPNとのもう一つの違いは、この経路を使用できるのはIBM MobileFirst ProtectのSDKを使用しているアプリ、ラッピング機能でラップされたアプリで、かつ管理者が許可したアプリに限られるという点です。Mobile Enterprise GatewayはPortをListenせず通信も暗号化されているため外部からの攻撃に強く、たとえSDKを入手して悪意のある攻撃を仕掛けるとしてもIBM MobileFirst Protectがサービスを提供している環境を攻める必要があります。IBM MobileFirst Protectのサービス環境は米国政府機関がそのセキュリティーが問題ないと認めるFISMA認定をSaaS型モバイル管理ソリューションとして唯一受けており、まさにお墨付きと言えます。

つまり、たとえプラットフォーム上にマルウェアやウイルスがいたとしても、イントラネット内への接続の安全は確保できるということです。

●コンテナによる安全なデータ保護

IBM MobileFirst Protectでは、Mobile Enterprise Gatewayによる安全なイントラネット接続に加えて、コンテナ機能を提供することによりデータの保護機能も提供します。

スマートフォン、タブレットでのデータの安全性を

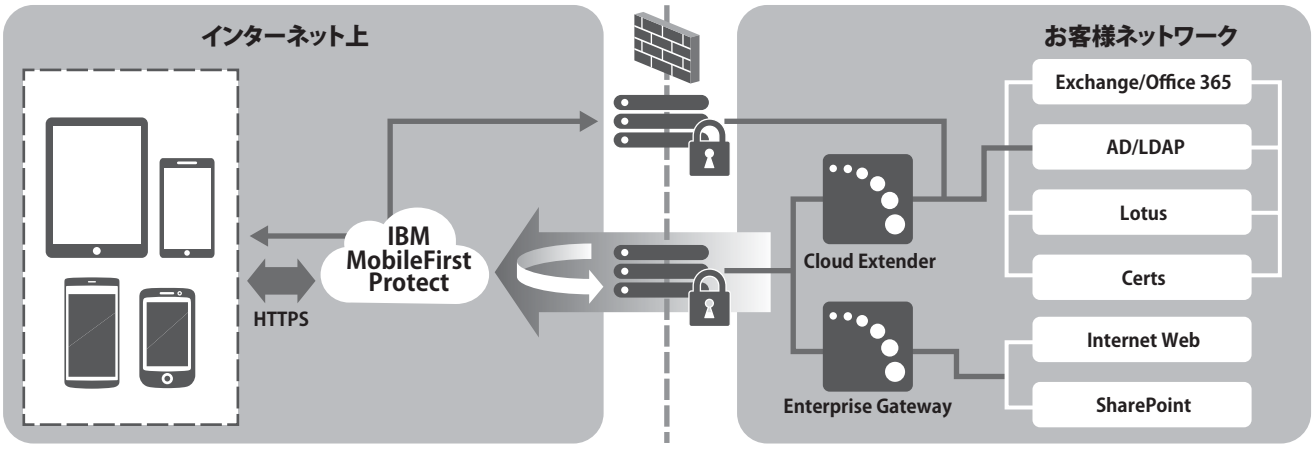

図2. IBM MobileFirst Protectによる社内接続

考える場合、一つの解決方法として「そもそもデータをプラットフォーム上に置かない」という方法があります。プラットフォーム上にデータがなければ、どのようなマルウェアもウイルスもデータの盗みようがないので確かに安全で、完璧に見えます。

安全の確保という意味では確かに完璧ですが、モバイル活用という面ではどうでしょうか？　この解決策には一つ重要な前提があります。それは常に何らかネットワークに接続していなければならないという点です。この点も各キャリアの努力により日本国内であればそれほど問題ないと思われるかもしれませんが、実は都心で問題が起こることがあります。高層ビルの上では携帯電話の電波の受信が厳しいことが多々あります。重要なお客様との会議で資料にアクセスできない事態が容易に起こってしまうのです。また、地方を巡るような営業スタイルの場合は、こういったことは顕著です。

IBM MobileFirst Protectではコンテナを安全に守ることにより、データをプラットフォームに保管し利便性と安全性を両立しています[3]。コンテナ内のデータはすべて暗号化されています。そのため、バックアップを含めコンテナのデータを取り出したとしても、その内容を抜き出すことはできません（**図3**）。また、アプリ間のコピー・アンド・ペーストも制御しています。コンテナ上ではメール・アプリやMobile Enterprise Gatewayと連携したSecure Browser、社内ファイルサーバー連携などが動作し、機密性の高いデータがダウンロードされます。例えば、イントラネット上のWebアプリにSecure Browserでアクセスし顧客情報を入手し、お客様へメール・アプリで回答を行うということはよく行われます。Webアプリのデータはメールで使用するためにいったんコピーされており、このコピーされた情報を悪意を持ってプライベートのメール・アカウントで外部に送ることで容易に情報漏洩が発生します。

IBM MobileFirst Protectではこの動作を制御します。コンテナ上のデータやアプリ間であれば通常通り全く問題なくコピー・アンド・ペーストが実行できますが、宛先が外部だとペーストが制御され、コピーされた内容ではなくペーストが禁止されたことを示すメッセージがペーストされます。この制御はコンテナからそれ以外という片方向だけではなく双方向への制御が可能で、コンテナから外部へは禁止するが、コンテナ外からコンテナ内へは許可という制御も可能です。カメラ・アプリで撮影した写真データの取り込みなどが必要な場合は双方向に禁止するのではなく、コンテナへの取り込みを許可することで、写真データをコンテナ内のアプリで使用できるようになります。

●社内アプリ・既存アプリの活用

IBM MobileFirst Protectでは、Mobile Enterprise Gatewayやコンテナで使用するメール、カレンダー、連絡先機能や標準のブラウザーに代わるSecure Browser、社内ファイル共有サーバーと連携する文書参照・編集機能などを提供し、コンテナ内で業務を推進するためのアプリ・機能を提供しています。しかし、イントラネットと接続しモバイルを活用するには、やはり専用アプリを使用した方が格段に効率の良いことが多いようです。そういったアプリに対して、IBM MobileFirst Protectの機能を活用するために二つの方法を提供しています。一つがSDKであり、もう一つがラッピング機能です。

アプリを新規に開発する場合や既存のアプリを改修することができる場合は、SDKを組み込むことでIBM MobileFirst Protectの機能を取り込み細かく制御することが可能になります。

社内で専用に使用しているアプリがあるが、開発・改修を外部に委託しておりすぐにはSDKによる対応が厳しい場合には、ラッピング機能が使用できます。この場

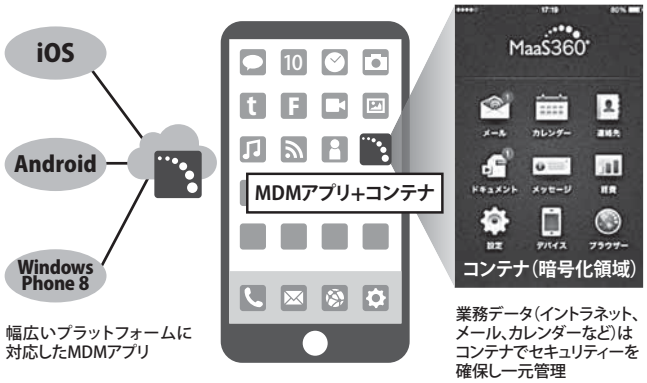

図3. コンテナによりデータ保護

合、アプリ自体に手を入れる必要はありません。ラップを行うだけで、Mobile Enterprise Gatewayによるイントラネット接続機能などが提供できるようになります。

このようにIBM MobileFirst Protectではさまざまな手段でモバイル活用における課題を解決することで安全にイントラネットへのアクセス提供し、モバイルの活用を推進します。

4. インベントリー管理やデバイス紛失・盗難への対応の必要性

モバイル端末を企業利用する際に、もう一つ気になるのが、ユーザー、すなわち社員が、正しいバージョンのソフトウェアを使っているか管理することと、デバイスを紛失したときの情報漏洩の防止などです。このような課題はスマートフォン、タブレット以前の、パソコンをモバイル化した時代からあり、端末管理の必要性を物語っています。そのようなニーズに応える機能を提供するシステムをモバイル端末管理（Mobile Device Management : MDM）と言います。

IBM MobileFirst Protectでは、スマートフォン、タブレットに特化したMDM機能を提供しています。MDM機能として各プラットフォームのAPIに準拠し、各デバイスの機能の制御やそのインベントリー情報の取得を基本機能として備えており、企業配布でもBYODでも同様に管理できます。デバイスはすべてユーザーと関連付けて管理されてるため、その制御はユーザーごと、グループごとに分けて設定することが可能です。

●IBM MobileFirst Protectのデータ消去機能

基本的なMDM機能の網羅だけなでなく、そのデバイス上のデータの消去など簡単な管理を管理者側から行うことができます。一般的なMDM機能で実現されているワイプ機能としてデバイス全体を初期化することも可能ですが、コンテナ機能の活用による企業データのみセレクティブ・ワイプ機能やアプリ・カタログと連携して特定のアプリのデータのみをアプリと一緒に削除することも可能にしています。

また、盗難時対策として時限爆弾機能も備えており、一定期間IBM MobileFirst Protectとデバイスが通信を行わなかった場合、デバイスは自動的にワイプする設定も可能です。このように管理者側からさまざまなレベルでのデータの管理を実現しています。

さらに、ユーザーに対してはセルフ・サービス・ポータル機能を提供し、ワイプ、セレクティブ・ワイプ、ロック、パスコード変更、位置確認機能を提供しています。非常事態にユーザー自身の即時対応も可能にしています。

5. まとめ

本稿では、IBM MobileFirst Protectによってスマートフォン、タブレットの社内活用における課題とその解決方法をお伝えしました。IBM社内でも営業系社員へのiPadの配布や一部管理職へのiPhoneの配布が始まり、BYODから始まった社内モバイル活用が一段と進みつつあります。社内のセキュリティーを守りつつ利便性を得るためには何らかの仕組みが必要であり、IBM社内においてもその解決にIBM MobileFirst Protectを使用しています。このようなツールの適切な活用により、安全にモバイルの推進を進めていただきたいと思います。

[参考文献]
[1] IBM, モバイル市場の動向と課題の解決（2013）
[2] IBM, Securing end-user mobile devices in the enterprise（2012）
[3] Fiberlink Communications, Mobilize Your Corporate Content and Apps（2014）

日本アイ・ビー・エム株式会社
セキュリティー事業部
アプリケーション＆モバイル・セキュリティー　部長

赤松 猛
Takeshi Akamatsu

2003年日本IBM入社。ソフトウェア開発研究所にて運用管理製品の開発を担当。主に各製品の国際化開発に従事、その後WW SWAT Teamの一員として資産管理製品の技術支援を行う。2013年よりエンドポイント・モビリティーの製品担当として活動。