IBM Security
Thought Leadership White Paper

モバイル・アプリケーション・ライフサイクル管理のベスト・プラクティス

設計から導入までのセキュリティー

IBM

モバイル・アプリケーション開発におけるセキュリティーの役割

モバイル機器は現在、多くの企業で現実に使われています。生産性、事業提携、顧客満足度、収益の業績を改善するための特定の作業用に、企業が Mobile Device Management (MDM) と Mobile Application Management (MAM) を基に、自社アプリを特定業務用に開発することが増えています。ただし、これらのメリットを達成するには、モバイル・セキュリティーのベスト・プラクティスをアプリケーションのライフサイクル全体に組み込むことが必要不可欠です。

企業は、コンプライアンスとセキュリティーのベスト・プラクティスをノートパソコンや他のモバイル機器に広げるにはどうすればよいのかという、新たな課題に直面しています。

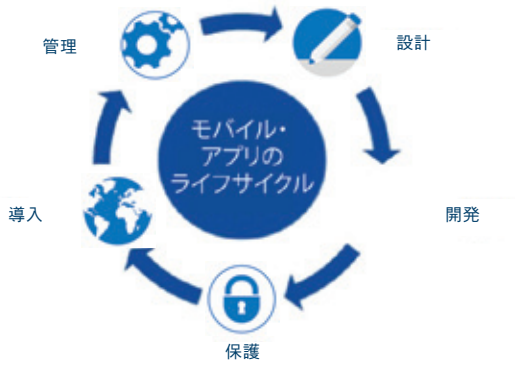

*図 1:*モバイル・アプリ・ライフサイクルには、アプリの開発、保護、管理が含まれる

Mobile Application Lifecycle Management (MALM) は、モバイル時代の当初からあった、セキュリティー、コンプライアンス、プライバシーの問題すべてを継承しています。これには、企業データと個人データのセキュリティー、行政と業界規制とのコンプライアンス、従業員のプライバシーが含まれます。カスタム・モバイル・アプリの開発が厄介な作業に見える一方で、もっと大変な課題はアプリと関連データを導入した後、保護することです。

Enterprise Mobility Management (EMM) の認知されたリーダー、IBM Security は、アプリケーションの開発と導入中に使用するアプリケーションのセキュリティー・ベスト・プラクティスを提供します。自社モバイル・アプリを設計、開発している企業の場合、これらの機能はソフトウェア開発キット (SDK) または自動アプリ・ラッピングを介して提供できます。

先見的なアプリケーションのセキュリティー・ベスト・プラクティス

セキュリティー・ポリシーを設け、アプリの導入準備が整った後でポリシーを適用することは素晴らしいことですが、セキュリティーをアプリの設計と開発に組み込めば、長期間にわたって労力を軽減し、その成果を強化することができます。デバイス OS で使用可能なデータ暗号化に加え、アプリケーション開発中に MaaS360® から追加できる先見的なセキュリティー機能が複数あります。これらの機能は次のとおりです。

認証

基本的なパスコード登録または Active Directory や LDAP と同期する 2 段階認証を使用できる MaaS360 でのデバイス認証のほか、認証をアプリにも埋め込むことができます。誤って不正ユーザーに配布された場合でも、特定のアプリと関連データにアクセスすることになっているユーザーのみがこれらを開くことができます。

シングル・サインオン

認可されたすべてのエンタープライズ・アプリに、ユーザーが 1 つの共有パスコードでアクセスできるようにアプリを設計することができます。この MaaS360 のサポート機能により、

IBM Worklight®. などの開発者プラットフォームでモバイル・アプリを構築する際、ユーザーをより中心に据えたアプローチが実現します。ユーザーの生産性に影響しない、強力な認証を支援できます。IBM® MaaS360® Trusted Workplace は、複数のモバイル・プラットフォームにまたがる認証、シングル・サインオン、データ損失防止 (DLP)、In-App VPN、App Blocking のアプリ設計を簡素化します。

データ損失防止 (DLP)

MaaS360 は、モバイル上で企業データを個人データから分離するデュアル・ペルソナ環境をサポートします。開発者と MDM 管理者はこの保護コンテナー、MaaS360 Trusted Workplace を様々な方法で使って、データ漏洩を防止し、企業データと個人データの混在を阻止し、従業員のプライバシー問題に対処できます。

- **MaaS360 Trusted Workplace:** FIPS 140-2 準拠の AES-256 暗号化に対応するこのコンテナーは、パスワードで保護することができ、デバイス所有者の認証がなければアクセスできません。デバイスが紛失または盗難にあった場合は、企業アプリ、ドキュメント、データが保護され続ける一方で、インシデントが報告され、コンテナーがリモートでワイプされます。デバイスをなくして悩んだ従業員が数日してから IT に届け出た場合でも、企業情報は保護されます。
- **選択的ワイプ**: 実質的に、MaaS360 からデバイスにプッシュされた全情報はコンテナーからリモートでワイプでき、ユーザーが私用目的でダウンロードした情報に影響が及ぶことはありません(MaaS360 は、デバイスを工場出荷時の設定にリストアできる完全ワイプ機能も提供します)。
- **コピー・アンド・ペーストを制限**: MaaS360 は、コンテナー外の情報のコピー・アンド・ペーストを無効にする機能を提供します。ノートパッド、ネイティブ・メール・アプリケーション、ファイル共有 Web サイト、またはバックアップ・データ・クラウドなど、個人スペースからアクセスできるリソースにコンテナーから貼り付けようとすると、企業セキュリティー・ポリシーをリマインドするメッセージが代わりに貼り付けられます。試行されたアクティビティに関する自動アラートも MaaS360 管理者に送信できます。
- **オープンイン・コントロール**: MaaS360 では「オープンイン」コントロールも提供しているため、ユーザーは、会社の MaaS360 Trusted Workplace コンテナーに属し、その管理下にあるアプリのみでドキュメントとファイルを開くことができます。企業情報はコンテナーを開いたり、コンテナーから移動したりすることはできません。

モバイル機器は、マネージャーとIT スタッフの直接管理下にないため、従業員のミス、そして従業員による悪用に対して特に無防備です。

In-App VPN

上記のすべてがモバイル機器で休眠中のデータのセキュリティーを固める一方で、エンタープライズ・アプリ開発者は移動中のデータ、つまり、MaaS360 Trusted Workplace コンテナーから企業サーバーに送信されるすべての情報を保護する必要もあります。これらの送信を保護するには、VPN 接続が必要です。アプリレベルのトンネルを使用すると、アプリレベルの VPN 接続のみを経由して安全、確実に送信できます。デバイスレベルの VPN は不要です。IBM® MaaS360® Gateway for Apps を使用すると、どのような VPN インフラストラクチャーを使っていても保護を実現できます。

アプリ・ブロック

アプリ開発チームは、MaaS360 の自動セキュリティー監視機能によって非準拠とされたデバイス上でアプリを開こうとすると、ブロックを実行するポリシーを設定できます。

エンタープライズ・アプリ・ストアのベスト・プラクティス

アプリの開発後、アプリをシンプルかつセキュアに配布、管理するには、エンタープライズ・アプリ・ストアを使うことをお勧めします。実際、多くの MaaS360 のお客様はすでにシステムの App Catalog 機能を使って、iTunes App Store、Google Play、Windows Store、社内エンタープライズ・アプリなどのストアのパブリック・アプリを管理しています。MaaS360 Trusted Workplace コンテナーと MaaS360 App Catalog を併せて使うと、アプリをよりきめ細かく管理できます。このアプローチを利用すると、他社製、自家製を問わず、IT が購入したアプリが完全に個人アプリから分離されます。

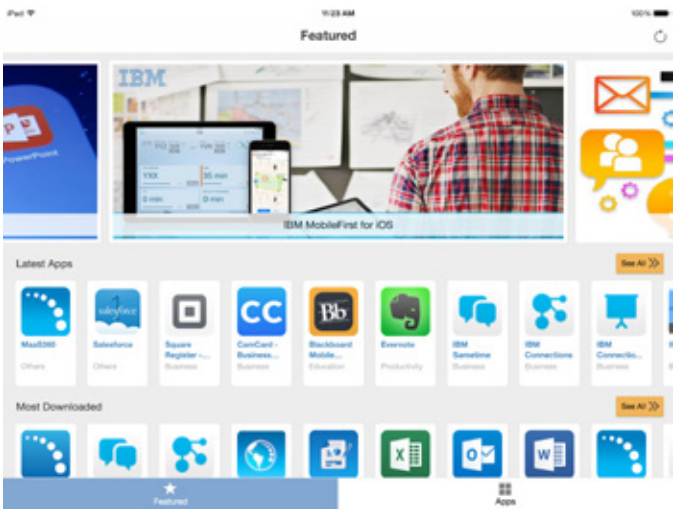

*図 2:*アプリ・カタログにより、ユーザーは認可アプリを簡単に見つけることが可能に

完全統合型アプリ・ストアのメリット

MaaS360 App Catalog では、モバイル OS から独立した統合インターフェースを提供しているため、様々なプラットフォームを 1 つのウィンドウからアプリを管理できます。完全統合型アプリ・ストアのその他のメリットは次のとおりです。

遅延なくアプリを展開、更新

App Catalog はカスタム・エンタープライズ・アプリのほか、パブリック・アプリ・ストアと統合します。アプリを個々のデバイス、ユーザー・グループに無線でプッシュし、そのインストールを追跡できます。また、全ユーザーに一括配信することもできます。たとえば、Apple の Volume Purchase Program (VPP) を使って、購入済み iOS アプリを従業員に送りたい場合は、VPP ファイルを直接アップロードして、これらのライセンスを MaaS360 から管理できます。ユーザーが退職する場合は、そのアプリケーションをユーザーのデバイスから削除し、ライセンスを再配布することができます。ユーザーがアプリを削除して再インストールする必要がある場合でも、IT に依頼して別のライセンスを入手したり、パブリック・アプリ・ストアを調べたりする必要はありません。代わりに、社内の App Catalog にアクセスして、アプリのインストール・ボタンをクリックするだけで済みます。

既存のエンタープライズ・セキュリティーと ID インフラストラクチャーとの統合

多くの企業は特定のユーザー・グループにアプリを展開する必要があります。MaaS360 でユーザー・グループをセットアップできる一方で、Active Directory または LDAP を基に Enterprise Mobility を既存のユーザー ID に合わせて調整すると、適切なアプリが適切なユーザーに配布されていることを確認するための手順を省略できます。これは MaaS360 Cloud Extender で達成可能です。カスタム機能の場合、MaaS360 を様々なタイプの IT インフラストラクチャーと統合させるには、Web サービスを強くお勧めします。Web サービスは堅牢、柔軟、効率的で、簡単にコードを作成でき、インターネットへの公開も容易です。その一方で、アプリ、ドキュメント、データも保護し続けます。

アプリのセキュリティーと管理の強固なコントロール

MaaS360 から管理する場合、他のアプリに提供されているものと同じ保護機能をカスタム・エンタープライズ・アプリに対して実行できます(「パッシブ」アプリケーションのセキュリティー・ベスト・プラクティスに関する次のセクションを参照。)

アプリのバージョン管理

パブリック・アプリの場合、通常、全対象ユーザーに対するアプリのバージョンは 1 つだけです。社内または他社が開発したカスタム・エンタープライズ・アプリの場合、アプリの新しいバージョンを持つことができ、全社的に配布する前に、一握りのユーザーだけにプッシュできます。MaaS360 を使用すれば、同じアプリの様々なバージョンを導入、管理することができます。

アプリの発見とユーザー・コラボレーション

ユーザーは、業務を行う上で会社が推奨または要求する認可アプリを見つけて、アクセスできる必要があります。MaaS360 の App Discovery Portal を使用すると、シンプルで使いやすいインターフェースでアプリを簡単に見つけられます。また、ユーザーは Trusted Workplace コンテナーの承認を受けたアプリを安全に共有、リンクすることもできます。アプリについてコメントを付けたり評価したりして、そのアプリがどのくらい役に立つのかを伝え、業務の価値を向上させる上で更新または強化の必要なアプリを簡単に伝えることができます。

オンデマンドのアプリの在庫管理と報告

MaaS360 管理者は、App Catalog で使用可能なすべてのアプリ、認可ユーザー、および各ユーザーのデバイス上の WorkPlace コンテナー内のアプリをオンデマンドで閲覧、報告することができます。管理者はどのユーザー、グループからでも、または全デバイスから、更新されたアプリの旧バージョンなど、アプリを削除できます。

より高度な製品も登場しており、電子メール、ファイル転送、またはインスタント・メッセージングを使ってストレージ・デバイスと他のコンピューターに転送される機密ファイルを監視、記録したり、そのような転送をすべて完全にブロックしたりすることができます。

1 つのプラットフォームならシンプルで安全

IBM Worklight なら、1 つのウィンドウを使って、複数のモバイル・プラットフォームにまたがるアプリを開発できます。MaaS360 なら、1 つのウィンドウを使って、複数のプラットフォームの MDM、MAM、MALM に対応できます。これらの統合型アプローチは、高いレベルのコントロール、セキュリティー、コンプライアンス、生産性で Enterprise Mobility の長所を高めながら、リソース、時間、予算への要求を下げることができます。

「パッシブ」アプリケーションのセキュリティー・ベスト・プラクティス

MaaS360 から管理する場合、パブリックおよびエンタープライズ・アプリは次のような会社のコントロールと管理機能を等しく利用できます。

- アプリケーションのホワイトリストとブラックリスト
- セキュリティーと制限の構成
- 非準拠への自動的な強制措置 (アラート、デバイスのブロック、デバイスの部分的または完全な削除)
- 脱獄済みデバイス、ルート化端末、非準拠デバイスの自動モニタリング
- デバイスのコンプライアンス・ステータスを常に可視化
- セキュリティーおよびコンプライアンス履歴を報告

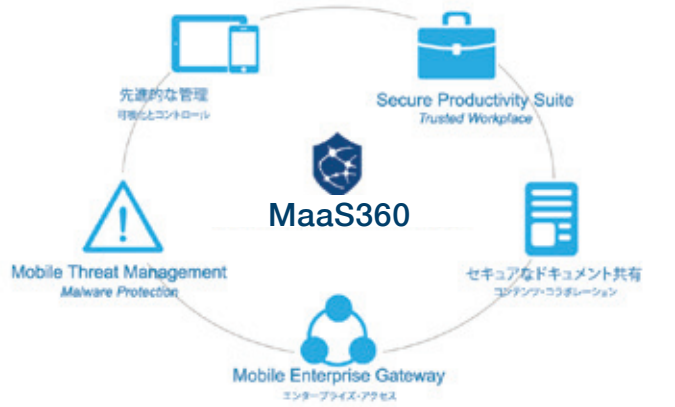

図 3:MaaS360 の 5 つの主要な側面

IBM® MaaS360® Secure Mobile Browser

多くの組織は多大なリソースを投資してきており、既存の Web アプリケーションに依存する安定したビジネス・プロセスを配備しています。MaaS360 Secure Mobile Browser と IBM® MaaS360® Gateway Suite を使用すると、従業員はモバイル機器から、社内イントラネット・サイトおよびアプリケーション (Private SharePoint、Windows File Sharing、社内 Web サイトなど) に安全にアクセスできます。これにより、Web アプリをモバイル・アプリに書き換えたり、完全デバイスレベルの VPN をセットアップしたりしなくても、すべての Web アプリを動員できます。

また、MaaS360 管理者は MaaS360 Secure Mobile Browser により、どのようなデバイスから Web サイトにアクセスされても、そのアクセスをカテゴリー別に制限でき、ビジネス目的のために、アクセス制限の例外を設けることができます。たとえば、会社でソーシャル・ネットワークをブラックリストに載せる場合、管理者は、マーケティングや PR 担当者が必要に応じて LinkedIn を使ってビジネス投稿を行えるように、例外を作成できます。他の誰かがソーシャル・ネットワークにアクセスしようとした場合、アクセスは拒否されます(管理者は、制限された Web サイトにユーザーがアクセスしようとするたびに、ユーザーとデバイスを特定する時間と日付のタイムスタンプが付いた監査ログを入手できます。何回も攻撃してくる者に対しては、MaaS360 メッセージング・システムから警告を出すことができます)。

IBM® MaaS360® Mobile Application Security SDK

MaaS360 Mobile Application Security SDK により、開発者はわずか 2、3 時間で、MaaS360 の強固なセキュリティー機能を構成可能なセキュリティー・レイヤーとしてアプリに埋め込むことができます。SDK により、開発者はわずか 2、3 時間で、強固なセキュリティー機能を構成可能なセキュリティー・レイヤーとしてアプリに埋め込むことができます。あるいは、これらのセキュリティー機能をアプリ・ラッピングで即座に埋め込むことも可能です。開発中にSDK を組み込むことで、エンタープライズ・アプリは、すべての MaaS360 保護機能をその正確なニーズに合わせることができます。また、開発者は SDK により、iOS、Android、Windows Phone デバイスに組み込まれた多くの機能と MaaS360 を統合できます。

MaaS360 インスタント・アプリ・ラッピング

開発済みのアプリの場合は、MaaS360 アプリ・ラッピングによって必要なコードがアプリに自動的に注入されます。ボタンをクリックするだけで、MaaS360 の強固なアプリ・セキュリティおよび管理機能を数秒で追加できます。

エンタープライズ・モビリティに至る道のりへのもう 1 つの重要なステップ

BYOD が企業に受け入れられるまで 2、3 年かかりましたが、MALM ははるかに速いペースで起こるでしょう。組織のミッションと運用に合わせて調整した Enterprise Mobility の価値は、生産性、顧客/パートナー関係、従業員の満足度、収益の業績の面で否定できないほど大きなものです。雇用から退職者面談の段階まで、従業員のモバイル・デバイスは最終的には、社内で認可されたデジタル資産と物理資産への主要アクセス・ポイントになります。モバイル・セキュリティーが固定 IT インフラストラクチャーと同じレベルで情報を保護できる場合、カスタム・エンタープライズ・モバイル・アプリケーションは、多くの企業が熱望している次の重要なステップになります。MaaS360 はすでに、世界中の多くの企業を支援しています。企業は MaaS360 により、IT が素早く実装、管理することができ、ユーザーにスムーズに受け入れられ、進化するモバイルの世界に敏捷に適応できるソリューション、およびモバイル・イニシアチブを使って、MDM、MAN、MALM に対処しています。

IBM MaaS360 について

IBM MaaS360 は、業務のあり方に合わせて生産性とデータ保護を実現するエンタープライズ・モビリティ管理プラットフォームです。モバイル・イニシアチブの基盤として多数の組織から信頼されています。MaaS360 は包括的な管理機能を提供し、ユーザー、デバイス、アプリ、コンテンツへのセキュリティーを強力に制御することで、どのようなモバイル導入もサポートします。IBM MaaS360 の詳細と 30 日間の無料トライアルのご利用については、次の Web サイトをご覧ください。www.ibm.com/maas360

IBM Security について

IBM のセキュリティー・プラットフォームはセキュリティー・インテリジェンスを提供して、組織が人々、データ、アプリケーション、インフラストラクチャーを包括的に保護できるように支援します。IBM は、ID およびアクセス管理、セキュリティー情報およびイベントの管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、次世代侵入保護などのためのソリューションを提供しています。IBM は、世界で最も幅広くセキュリティー研究開発を行い、セキュリティーを提供している組織の一つです。詳細は、以下をご覧ください。
www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in Japan
March 2016

WGW03110-JPJA-01