MobileIron

WHITE PAPER

モバイルセキュリティ:
脅威と対策

はじめに

モバイルデバイスは、企業内のエンドユーザーにとって主要なコンピューティングプラットフォームへと急速に成長しつつあります。優れた操作性、安定した処理性能、充実したアプリの数々、常時接続機能を持ち、持ち運びの容易なモバイルデバイスは、PC の代用として非常に魅力的です。しかし、PC 時代からモバイル時代への移行は管理者にとっては大きな変化であり、企業の IT 部門は企業データを保護し、リスクを最小化する新しい方法を検討しなければなりません。モバイル上の企業コンテンツを保護するには、IT 部門がモバイルと PC の運用上の違いを踏まえ、新しい管理ツールとセキュリティ戦略を導入する必要があります。しかし、モバイルファースト(モバイルデバイスが主役となること)の方針を取り、新しいニーズに対応できた組織は、競争上の利点や高い革新性などのメリットを享受できます。

本書では、企業や個人のモバイルデバイス上の情報漏洩リスクを緩和するため、MobileIron で導入可能な基本的、補足的、代替的なコントロール機能について概説します。

モバイルファースト化における重要事項

ユーザーの生産性向上を追求する際、IT 部門が PC ではなくモバイル上の企業データを保護する新しい戦略を導入すべき理由は主に 2 つあります。

- **モバイルデバイスに対する IT コントロールの弱さ**:モバイルファースト時代の主役はエンドユーザーです。ユーザーは、個人的な好みに合ったモバイルプラットフォームを選び、生産性を維持する多彩なアプリやコンテンツを駆使してビジネスの場面でも活用できることを期待します。PC 時代には、IT 部門が承認済みの PC と選択済みのアプリケーションをユーザーに貸与していました。PC でアクセスできるものについて、エンドユーザーの意見は反映されませんでした。IT 部門は、物理ポートからソフトウェアやアプリケーションのバージョンまで、企業が所有するデバイスのあらゆる面をコントロールしていました。モバイルの場合、エンドユーザーが多くの決定権を持ち、IT 部門はデバイスとアプリケーションを推奨するにすぎません。IT 部門が、全社的に同じ OS、デバイス、アプリの使用を強制する方法はないのです。実は、IT 部門がデバイスに制限をかけようとすればするほど、エンドユーザーはそれをすり抜けようとし、組織のリスクが増大します。

- **旧いセキュリティモデルは通用しません**:PC のオペレーティングシステムでは、エージェントベースのセキュリティが有効でした。これは、PC にソフトウェアを常駐させ、他のアプリケーションに属するプロセスやデータを管理する方法です。しかし、モバイルのオペレーティングシステムは PC と異なるため、エージェントベースのセキュリティモデルでモバイルは保護できません。モバイルオペレーティングシステムは、アプリと関連データを隔離し、明確に定義されたメカニズムを通じてのみ相互作用とデータ共有を行うサンドボックス型アーキテクチャを採用しています。このため、PC 用 OS のオープンファイルシステムより高いセキュリティの導入が可能ですが、デバイスベンダーが提供する具体的なセキュリティ機能を利用するには新しいツールが必要です。

企業におけるモバイルの急速な普及により、成長と革新の可能性は広がりますが、リスクも増大します。本書では、モバイルデバイスがもたらす主な脅威、および IT 部門がエンタ

MAKING ENTERPRISE MOBILE FIRST

MobileIron

415 East Middlefield Road
Mountain View, CA 94043 USA
TEL: +1.650.919.8100
FAX: +1.650.919.8006
info@mobileiron.com

ープライズモビリティ管理（EMM）ツールを利用してリスクを緩和し、エンドユーザーの生産性を低下させることなくビジネスデータを保護する方法について概説します。

モバイル導入によって生じる脅威

BYOD のようなトレンドがモバイルデバイスの利用を促進し、企業の生産性を高めるにつれ、組織はさまざまな情報セキュリティリスクや脅威にさらされます。モバイルがもたらす脅威は、3 つのカテゴリーに分類されます。

1) **デバイスに起因する脅威**
エンドユーザーは、モバイルデバイスにより、メールの受信、各種アプリを通じた企業コンテンツへのアクセス、編集、共有など、さまざまなビジネスタスクを実行します。この結果、モバイルデバイスには大量の機密データが保存されます。このデータは、以下の原因で漏えいまたは損傷する場合があります。
   - 常時接続を通じた不正な人物によるビジネスデータへのアクセス。
   - ソフトウェアの脆弱性を狙った「脱獄（ジェイルブレイク）」や「ルーティング」によるデータセキュリティの低下。
   - ポータブルデバイスの盗難や置き忘れ。

2) **ネットワークに起因する脅威**
常時接続モデルでは、モバイルデバイスが常にインターネットに接続している必要があります。このためエンドユーザーは、信用のおけないパブリックネットワークに依存し、以下を通じて悪意のある第三者に送信データを傍受される可能性があります。
   - 不正アクセスポイント
   - Wi-Fi スニッフィングツール
   - 高度な中間者（マン・イン・ザ・ミドル）攻撃

3) **ユーザーに起因する脅威**
モバイルは、エンドユーザーに権限を与えます。ユーザーの選択肢が増えるのは良いことですが、ユーザーが悪意なしにリスクの高い行動を取り、ビジネスデータを危険にさらす場合もあります。リスクの高い行動には、以下のような例があります。
   - 未承認のクラウド型アプリを使用したデータの共有と同期
   - 未承認のアプリを使用した企業データのコピーの保存
   - セキュリティコントロールをすり抜ける脱獄（ジェイルブレイク）/ルーティングデバイス
   - 未承認のアプリストアから入手した悪意のあるアプリの使用
   - ビジネスデータの悪意的な露出

モバイルデバイスに起因する脅威は、ノートパソコンやポータブル PC と同じだと思われがちですが、モバイルと PC のオペレーティングシステムは根本的に異なるため、IT 部門は、専用のエンタープライズモビリティプラットフォームを使ってモバイルのリスクに対応する必要があります。

モバイル上での情報漏洩防止

モバイルデバイス上で情報漏洩を防止するには、階層型のセキュリティ対策が必要です。階層型のセキュリティ対策は、以下の機能を利用して実施されます。

1) セキュアなオペレーティングシステムアーキテクチャ
2) 認証
3) リモートワイプ
4) 暗号化
5) データ共有
6) ネットワークセキュリティ
7) アプリケーションのライフサイクル管理
8) セキュアブラウジング

以下に、情報漏洩防止に必要な要素と MobileIron がサポートする具体的なコントロール機能を紹介します。各コントロールクラスには、ニーズに直接対応する基本的コントロール、基本的コントロールを強化する補足的コントロール、基本的コントロールが使えない場合に適用する代替的コントロールが含まれます。このような階層型セキュリティコントロールすべてが、モバイル向けの情報漏洩防止モデルを確立します。

1. セキュアなオペレーティングシステムアーキテクチャ

要件:

- マルウェアによるアプリケーションデータへのアクセスを防止するサンドボックスアプリケーション
- 安全なアプリケーションエコシステムの提供
- オペレーティングシステムの完全性保護
- OS 脆弱性に対する迅速なパッチ

サンドボックス型のオペレーティングシステムアーキテクチャは、アプリケーションデータを個々のコンテナに隔離し、マルウェアによるデータの損傷や盗難を防ぎます。

基本的コントロール:

- *サンドボックス*:「サンドボックス」とは、モバイル上のアプリケーション(アプリ)に関連する隔離されたデータセットです。PC のオペレーティングシステムと異なり、モバイルのオペレーティングシステムでは、綿密に定義された共有コントロールを介する以外は、所定のサンドボックス外にあるデータにアプリがアクセスすることはできません。このためマルウェアは、たとえデバイスにダウンロードされても、ファイルシステムにアクセスしてデータを損傷あるいは不正取得することはできず、リスクが緩和されます。
- *アプリのエコシステム*:Google Play、Apple App Store などのモバイルアプリストアは、公開するアプリにマルウェアが可能な限り存在しないよう厳しく監督しています。Apple は、承認済みアプリに新しい実行可能コードをダウンロードするなどのバックドアを禁じています。また、後で方針に反することがわかったアプリは、即座にアプリストアから削除されます。
- *OS の完全性*:「脱獄(ジェイルブレイク)」や「ルーティング」は、モバイル業界では、オペレーティングシステムに内蔵のセキュリティメカニズムを不正に取り除く行為を意味します。MobileIron は、登録された各モバイルデバイスについて継続的に脱獄/ルーティング検出を行い、オペレーティングシステムが改造されていないことを確認します。改造があった場合は、組織が定めた方針に基づき、適切なセキュリティ対策を実行します。デバイスの紛失、盗難、ネットワーク接続喪失の場合に備え、これはオンラインでもオフラインでも実行できます。
- *OS パッチ*:Apple は、iOS オペレーティングシステムのグローバルでの配信を管理しているため、Apple が重大と考える脆弱性があれば、昔からすぐにパッチを発行し、新しいバージョンの iOS を世界のユーザーがダウンロードできるよう提供しています。Android デバイス対応の OS パッチの提供は、デバイスメーカーと通信事業者に依存します。

MobileIron は、オペレーティングシステムの完全性とバージョンを監視し、全社的なコンプライアンスと一貫性を確認します。

補足的コントロール:

- *OS 更新の強制*:MobileIron は、管理下のすべてのデバイスの OS バージョンを監視しています。したがって、パッチが公開された後にユーザーがデバイスの更新を怠っていると、検疫にかかり、問題が改善されるまで企業データが削除される場合があります。

代替的コントロール:

- *OS バージョンの監視*:従来の Windows と異なり、IT 部門は iOS や Android 対応の OS パッチ配布を管理しません。すなわち、新しいパッチは、IT 部門が配布を承認するかどうかに関係なく、デバイスメーカーからユーザーに提供されます。これによって IT 部門のコントロールは弱まりますが、それでも MobileIron を通じて OS バージョンを監視すれば、ユーザーが長期間またはまったく更新していない場合に対策を取ることが可能です。

2. 認証

要件:

- パスワードポリシーのリモート設定
- 認証に所定回数だけ失敗するとデバイスを自動ワイプ
- 企業サービスには ID が必要

基本的コントロール:

- *デバイスパスワード*:MobileIron では、リモート設定とデバイスパスワードポリシーのローカル実行が可能です。IT 部門は、MobileIron を通じて以下のパスワードポリシー変数を設定できます。
  - 種類(数字、英数字)
  - 最小文字数
  - タイムアウトまでの最大無入力時間
  - 複雑な文字の最小文字数
  - パスワードの最大有効期間
  - 入力失敗の最大回数
  - パスワード履歴
  - デバイスロックの時間設定
- *アプリパスワード*:MobileIron AppConnect は、社内アプリと個人用アプリをセキュアに保護するコンテナ化ソリューションです。デバイス上の保護されたアプリにアクセスするための認証機能も備えています。
- *自動ワイプ*:過度の認証失敗は盗難の指標として、デバイスの自動ワイプにつながります。
- *証明書に基づく認証*:MobileIron はデジタル証明書を利用し、メール、Wi-Fi、VPN など、デバイス上の企業サービスへのアクセスをセキュアに保護します。ユーザーにとっては、毎回パスワードを入力する必要がないため、利用が容易になります。デバイスまたはユーザーがコンプライアンスの条件を満たしていない場合、ID 証明書を削除すれば対応サービスへのアクセスも遮断されます。

iOS がサポートする新しいバイオメトリック方式は、認証と暗号化の両方によるコントロールを強化します。

MobileIron は、デバイスレベルとアプリレベルの認証に対応するポリシーエンジンを提供し、企業データへの不正アクセスを防止します。

補足的コントロール:

- *バイオメトリクス認証*:Apple 社は、2013 年後半、iPhone 5S で初のバイオメトリクス認証方式「Touch ID」をリリースしました。Touch ID では、ユーザーがデバイスレベルの認証に指紋を使用できるため、肩越しにパスワードを盗まれるリスクが緩和されます:
  - 親指での認証に所定回数だけ失敗すると、ユーザーに MobileIron パスワードポリシーが設定したパスワード画面が表示されます。
  - Touch ID が提供される前、認証の大きな問題は、パスワードが強力であるほど覚えたり入力したりすることが難しくなり、ユーザーの不満につながる点でした。このため、ほとんどの金融サービス会社は、ユーザーに好まれ、普及するような弱いパスワードを許容していました。弱いパスワードは暗号化の強度も低く、デバイスに対するブルートフォースアタック(総当たり攻撃)を容易にします。
  - しかし、Touch ID を主要な認証手段にすれば、IT 部門は必要に応じて強力なパスワードに戻ることができます。ユーザーがパスワードを入力しなければならないのは、指紋認証が複数回にわたって失敗したとき、つまりデバイスの盗難の可能性が非常に高いときだけだからです。

3. リモートワイプ

要件:

- 企業が所有するデバイスについては、デバイス上の全データをリモートワイプ可能
- 従業員が所有するデバイスについては、デバイス上の企業データのみリモートワイプ可能

基本的コントロール:

- *フルワイプ*: *MobileIron では、管理者またはユーザーが、デバイス上の全データを消去し、工場出荷時のデフォルト設定にリセットするリモートワイプコマンドをデバイスに送信できます。*
- *セレクティブワイプ*: MobileIron では、以下のように管理者がデバイス上の企業データだけを削除することも可能です。
    - デバイス上の個人メールアカウントに影響を与えることなく、企業メールアカウントを削除。
    - デバイス上の個人アプリに影響を与えることなく、MobileIron 企業アプリストアを通じてインストールしたアプリを削除。
    - メール、Wi-Fi、VPN など、企業サービスの認証に使用するデバイス上のデジタル証明書を削除。
    - 文書、プレゼンテーション、スプレッドシートなどの企業コンテンツを削除。
    - 企業ポリシーの実行停止。

デバイス上の個人データとビジネスデータの論理的な分離により、IT 部門は、個人のプライバシーを侵害することなく、企業セキュリティ保護対策を実行することができます。

補足的コントロール:

- *プライバシー*: 企業は、IT 部門の人的ミス、紛失したデバイスのワイプ、訴訟などの事情で、やむなく BYOD デバイス上の個人データを削除してしまうことを恐れています。そのような場合、ユーザーは家族の写真やテキストメッセージなど、重要な個人データを失う可能性があります。
    - MobileIron では、IT 部門がデバイスごと、グループごとにプライバシーポリシーを設定し、セキュリティに影響を与える情報だけにアクセスすることが可能です。
    - すべての BYOD プログラムは、日常業務で実行が想定されるデータアクセスとデータ削除について、明確でわかりやすいポリシーを持つ必要があります。さもなければ、ユーザーがプライバシーに関して誤解し、BYOD の導入に弊害が生じます。
    - また、すべての BYOD プログラムは、たとえ通常業務で生じるとは予想されなくても、万が一、個人データが削除された場合に、企業に法的保護を与えるエンドユーザー契約を持つ必要があります。
    - きわどいケースは常にあるため、すべての BYOD プログラムは、Apple の iCloud サービスなどの個人データのバックアップ方法についてユーザーに教育する必要があります。そうすれば、デバイスがワイプされた場合でも個人データは失われません。これは、IT 部門が企業データのバックアップを取るのと同様、エンドユーザーにとって有用なことです。

MobileIron は、配信、設定、データ保護、削除など、デバイス上の企業サービスのライフサイクルを管理し、企業デバイスと個人デバイスに別々のポリシーを適用します。

4. 暗号化

要件:

- デバイスに保存されている企業データすべての暗号化
- デバイスから/デバイスへ移動する企業データすべての暗号化
- セキュアなアプリ内の企業データすべての暗号化

基本的コントロール:

- *保存中データの暗号化 - 組み込み:*MobileIron は、強力なデバイスパスワードの存在を要求し、デバイスレベルの暗号化を可能にするとともに、それをすべてのアプリに提供します。デバイスパスワードが強力なほど、暗号化の第 2 層が強力になります。Apple のバイオメトリクス認証方式「Touch ID」では、ユーザーのサインインを面倒にすることなく、IT 部門が MobileIron を通じて強力なパスワードを導入することができます。
- *保存中データの暗号化 - 追加*: MobileIron のアプリ向け AppConnect コンテナ化ソリューションは、暗号化を含む複数のセキュリティコントロールを提供します。iOS と Android は暗号化機能を組み込んでいますが、多くの組織は、ロックしていないデバイスについてこのような暗号化レベルの追加を望んでいます。
- *移動中データ*: メール、アプリ、文書、Web ページなどの企業モバイルデータは、MobileIron Sentry と呼ばれる MobileIron のインテリジェントなゲートウェイを通じて通信されます。このデータは、デジタル証明書やトランスポートレイヤの暗号化により、中間者(マン・イン・ザ・ミドル)攻撃や傍受から保護されています。
- *FIPS 140-2 検証*: MobileIron による FIPS 140-2 暗号化ライブラリの使用は、暗号化モジュール検証プログラム(CMVP)にのっとり、認定を受けた暗号およびセキュリティ試験(CST)ラボによって検証されています。バリデーションレターはこちらです。

保存中および移動中のデータを対象とする MobileIron の暗号化は、FIPS 140-2 への適合を検証され、組み込みオペレーティングシステムの暗号化機能を補足しています。

5. データ共有

要件:

- ネイティブメールアプリを使用した会社用の社用メール:
  - 不正なアプリで添付ファイルを開くことを許可しない
  - 個人メールアカウントを通じた転送を許可しない
  - メールテキストのコピー/貼り付け、スクリーンショットを許可しない
  - IT 部門のコントロール外でメールのバックアップを許可しない
- 社用アプリ:
  - 不正アプリによるアプリデータへのアクセスを許可しない
  - アプリデータのコピー/貼り付け、スクリーンショットを許可しない
  - IT 部門のコントロール外でアプリデータのバックアップを許可しない

基本的コントロール:

- ネイティブメールアプリを使用した会社用のメール:
  - *添付ファイル*: MobileIron のインテリジェントゲートウェイである MobileIron Sentry は、すべてのメール添付ファイルを暗号化します。添付ファイルの暗号を解読できるのは、MobileIron Docs@Work だけです。添付ファイルは、デバイス上の Docs@Work セキュアコンテナに保存されます。不正アプリは、添付ファイルへのアクセスや暗号の解読ができません。Android では、すべての会社用のメールがセキュアなワークスペースに保存され、添付ファイルは承認済みアプリでしかアクセスできません。
  - *転送*: MobileIron は、IT 部門がデバイス上の 1 つのアカウントから別のアカウントへのメール転送を無効にすることができます。
  - *コピー*: MobileIron は、デバイスのスクリーンショット機能を無効にすることができます。しかし、iOS のネイティブメールクライアントは、テキストのコピー/貼り付けや印刷機能の無効化をサポートしません。以下の「*代替的なコントロール*」セクションでは、これに対処する方法を説明します。
  - *バックアップ*: MobileIron がデバイス上で管理する会社用メールアカウントは、iCloud のようなサービスではバックアップできません。
- 社用アプリ:
  - *共有*: モバイルオペレーティングシステムは、「Open In」機能を通じてアプリによるデータ共有を許可します。MobileIron では、IT 部門がこの機能を使用してアプリデータにアクセスできるアプリを管理できます。
  - *バックアップ*: MobileIron は、すべてのアプリについて iCloud でのバックアップを無効にできますが、ユーザーが自分の個人データについて iCloud を使用したい場合があります。MobileIron では、管理するアプリごとに iCloud バックアップを無効にすることも可能ですが、IT 部門はそれらのアプリが文書やキー/バリューペアを保持するのに iCloud を使用するよう設定されていないことも確認する必要があります。

モバイル上の情報漏洩の主な要因は、善意のユーザーがセキュアでないアプリで企業データを開くことです。

MobileIron AppConnect は、データ共有に複数のコントロールをかけることで、承認済みのアプリでしか企業データにアクセスできないようにします。

6. ネットワークセキュリティ

要件:

- 企業データのトラフィックが IT 部門のコントロール外で公共の携帯電話事業者/Wi-Fi ネットワークを通じて伝送されることによる情報漏洩を防止します。

基本的コントロール:

- *アプリのトンネリング*: MobileIron Sentry は、メール、アプリ、文書、Web トラフィックなど、すべての企業データをアプリレベルでセキュアにトンネリングします。これにより IT 部門は、企業データのフロー(Sentry のセキュアチャネルを通じた通信)と個人データのフロー(Sentry 外のセキュアでないネットワークを通じた通信)を分離できます。
- *VPN*: Cisco や Juniper などのベンダーの VPN 技術をすべてのデバイスに導入している企業については、MobileIron が VPN の設定によってデータのセキュアチャネルを提供します。
- *NOC なしのアーキテクチャ*: ネットワークオペレーションセンター(NOC)は、ネットワークを集中的に監視/管理する施設です。従来の BlackBerry アーキテクチャにおける NOC は、企業からデバイスへメールトラフィックを伝送するセキュアネットワークの外部管理ポイントであり、BlackBerry 社によって管理されていました。NOC を利用したアーキテクチャの問題は、IT 部門のコントロール外で障害や情報漏洩が生じる可能性があることです。上記で説明したアプリトンネリングや VPN のモデルは、外部 NOC を必要としない点が有利です。BlackBerry が NOC を必要としたのは、旧来のプッシュ型メールのモデルが、企業メールサーバーからメールを収集し、外部(NOC)に保存した後でデバイスに転送するソリューションを必要とするためです。しかし、ActiveSync プロトコルを使用したプッシュ型メールでは、このモデルは不要です。現在、ActiveSync が、ほとんどの組み込み/サードパーティメールクライアントのプッシュ型メールに標準プロトコルとして採用されているのは、保存/転送や NOC ベースのアーキテクチャを必要としないことが主な理由です。

モバイルセキュリティモデルは、すべての企業データが公共ネットワークを通じて送受信されると仮定しています。

MobileIron Sentry は、どんなネットワークでも、アプリレベルで企業データのセキュアなトンネリング機能を提供するインテリジェントなゲートウェイです。

7. アプリケーションのライフサイクル管理

要件:

- 悪意的なアプリがデバイスにダウンロードされるのを防止
- 承認しないアプリのブラックリストを作成
- 承認済みアプリのホワイトリストを作成
- 企業アプリを公開/配信
- 企業アプリを更新

基本的コントロール:

- *悪意的なアプリ*: 以下の理由により、モバイルにおける悪意的なアプリのリスクが大きく緩和されます。
    - モバイルアーキテクチャが独立したサンドボックスに各アプリを隔離するため、MobileIron が管理するデータ共有方式以外では、悪意的なアプリが企業アプリからのデータにアクセスできません。
    - 公共のアプリストアは管理されているため、マルウェアはまれです。
    - Apple 社は、アプリによる実行可能コードのダウンロードを許可しません。これにより、既存アプリに悪意的コードが導入されることを防止しています。
    - Android は、ユーザーによるサイドロード、つまり未承認のアプリストアからのアプリのインストールを許容していますが、IT 管理者はサイドロードされたアプリを無効化するポリシーを適用可能です。
- *ブラックリスト/ホワイトリスト*: MobileIron では、デバイスが不適合の場合に通知したり、アクセスを制限したりするポリシーを通じて、アプリのブラックリスト/ホワイトリストを作成できます。App Store を完全に無効化することも可能ですが、アプリはモバイル機能にとって非常に重要なため、それは推奨されません。MobileIron は、高リスクのアプリの存在を特定するためにサードパーティのアプリ評価サービスも統合しています。
- *企業向けアプリストア*: MobileIron は、企業向けアプリストアを発明し、特許を取得しています。IT 部門は、このストアを通じて社内開発のアプリや公共のアプリを公開したり、ユーザーコミュニティに安全に配信したりできます。
- *アプリ更新*: MobileIron はデバイスにインストールされている企業アプリのバージョンを監視しているため、IT 部門は最新バージョンの公開をユーザーに通知できます。これにより、企業全体でコンプライアンスを確実にし、アプリにセキュリティ上の脆弱性が発見されれば速やかにパッチを適用できます。

補足的コントロール:

- *フィルターをかけたアプリインベントリ*: BYOD を導入する際には、プライバシーが極めて重要です。ユーザーは IT 部門に自分のデバイスにあるアプリケーションすべてを見せたいとは思いません。それらが健康や宗教など、個人的な生活を示す場合があるからです。MobileIron では、IT 部門が、個人アプリのインベントリを見ることなく、企業アプリやブラックリストアプリを監視することができます。

アプリは、モバイル機能の中心であり、ビジネスの生産性に極めて大きく貢献します。

MobileIron は、企業アプリをセキュアに配信し、管理する企業アプリストアを開発しました。

代替的コントロール:

- *悪意的アプリのブロック*: 標準的な導入では、IT 部門がユーザーによるアプリのダウンロードを実際に阻止することはできません。デバイス上にインストールするソフトウェアは、ユーザーが管理するからです。ほとんどのユーザー、特に BYOD のユーザーは、個人用アプリをデバイスにダウンロードすることを希望し、それに制限をかければモバイルの導入は進みません。しかし、モバイルデバイスのセキュリティアーキテクチャと MobileIron のブラックリスト/ホワイトリストポリシーを組み合わせれば、デバイスに悪意的アプリがインストールされるリスクは緩和されます。

8. セキュアブラウジング)

要件:

- ファイアウォールの背後にある企業 Web アプリへのセキュアなアクセス
- ダウンロードした文書やキャッシュ内 Web コンテンツの情報漏洩防止
- マルウェアによる「ドライブバイ」ブラウザ攻撃の防止

基本的コントロール:

- *アクセス*:MobileIron Web@Work は、ユーザーが企業の Web リソースにアクセスするためのセキュアなブラウザです。Web@Work は、ネイティブの Web ビューを利用するため、表示機能は Safari などのネイティブブラウザと同じです。ユーザーはブラウズインターフェースを 2 種類覚えるのを好まないため、ユーザー体験を維持することが普及を促進します。
- *文書と Web キャッシュ*:MobileIron では、IT 部門が、ダウンロードしたコンテンツに関する適切なデータ共有規則を設定し、ポリシーのトリガーに基づいてキャッシュ内データの保護と削除を行います。例えば、キャッシュからデータを取り出すことはできません。脱獄(ジェイルブレイク)などのトリガーでもキャッシュがパージ(消去)されます。
- *「ドライブバイ」攻撃(ユーザーに気づかれないようにソフトウェアをダウンロードさせる行為のこと)をブロックするホワイトリスト*:MobileIron Web@Work は、特定の社内サイトをホワイトリストに指定できます。すなわち、ユーザーが隠れたフレーム(別のサイトなど)を開こうとしても、新しいサイトがホワイトリストに指定されていない限りブロックされます。このコントロールにより、セキュアなブラウザアクセスが承認済みの Web サイトに限定され、ドライブバイ攻撃のリスクが緩和されます。

多くの企業リソースは、ファイアウォールに守られた Web アプリとして存在しますが、ネイティブアプリと同様に保存中データと移動中データのセキュリティコントロールを必要とします。

MobileIron Web@Work は、ネイティブなレンダリングを可能にするセキュアブラウジング機能と、ポリシーベースのコンテナ化を利用したローカルデータ保護機能を提供します。

最後に

新しいモバイルオペレーティングシステムのサポートは、IT 部門にとって常に難しい問題です。オペレーティングシステムやデバイスの選択が今や企業ではなく消費者に任され、頻繁に変更される場合があるためです。モバイルは、IT コンシューマライゼーションの純粋な例であり、どの技術がビジネス用途に普及するかは消費者の行動で決まります。

エンタープライズモビリティ管理（EMM）プラットフォームとしての Android や iOS などのモバイルオペレーティングシステムは、階層型セキュリティコントロールを提供するほどに成熟し、企業が企業所有あるいは個人所有のデバイス上の情報漏洩リスクを緩和する手段となっています。

企業は、今ではこのようなコントロールにより、自社ユーザーが希望する新世代のモバイルオペレーティングシステムやデバイスをサポートしています。

MobileIron の詳細は、www.mobileiron.com/ja をご覧ください。