モバイル・エンタープライズの保護

目次

エグゼクティブ・サマリー

モビリティーにより、私たちの働き方、コミュニケーションの方法、人との付き合い方が一変しています。消費者を中心とした現象として登場したモビリティーのメリットにより、企業は従業員の生産性と顧客エンゲージメントを押し上げる方法として、迅速にその受け入れを迫られました。

これは決して整然としたプロセスではありませんでした。従業員は、管理されていないデバイスを、まずは経営層レベルから企業ネットワークへと持ち込めるよう IT 部門に迫りました。消費者は、個人・医療・財務情報へとアクセスする好ましい方法として、モバイル・アプリケーションを急速に導入しました。IT 部門のセキュリティー・チームやモビリティー・チームは、その後を追いかけねばなりませんでした。ビジネスが必要とするものを提供しなければならない一方で、新たな脅威を管理する必要もありました。デバイスの紛失/盗難、脆弱なアプリケーションを狙うマルウェア、新たなソーシャル・エンジニアリング戦術により、データ侵害のリスクや、犯罪行為や不正行為を目的としたモバイル・デバイスの使用が増加しました。

従業員が所有するデバイスに企業の管理を適用することは、必要な第一歩でした。次に必要とされたのが、企業のデータを保護することです。データ損失はビジネスに大きなリスクをもたらします。企業では、従業員、パートナー、顧客向けのモバイル・アプリケーション使用を模索するにあたり、新たなプロセスを構築して、このようなアプリケーションの安全を確保する必要がありました。最後に、企業リソースへのモバイル・アクセスを全体的な侵害防御戦略の一環として管理しなければなりませんでした。

ポイント・プロダクトは、特定のモバイル・セキュリティー・ニーズに対応し、企業ではそれらをまとめて一貫性のあるソリューションへと統合する必要があります。多くの IT 部門はこの複雑で多面的な取り組みという課題を抱えており、全体的に統合された、スケーラブルなソリューションを切実に必要としています。

本書では、モバイル・デバイスに関連する固有のリスクと、安全なモバイル・エンタープライズへと至るロードマップの策定にあたり、企業が考慮すべき能力を検討します。また、エンドツーエンドの戦略およびソリューションであり、デバイス、デバイス間で開発・転送されるコンテンツ、モバイル・アプリケーション、モバイル・トランザクション、モバイルの ID およびアクセス管理要件におけるモバイル・セキュリティー要件に対応する、IBM Mobile Security Framework を紹介します。IBM 独自の脅威インテリジェンス・プラットフォーム上に構築された Mobile Security Framework は、自動的にコンテキストとリスク認識をモバイル・セキュリティーの各コンポーネントに組み込み、モビリティー管理とセキュリティーの効果を最大化します。

モバイル・エンタープライズのチャンスと脅威

モビリティーは、消費者のソーシャル・サークルへの関わり方、買い物方法、情報へのアクセス方法を根底から変えています。企業は、従業員が e-メール、カレンダー、連絡先などの業務上のリソースに出張先からアクセスできるようにすることで、ビジネスにモビリティーのメリットを活用しています。モバイルによるアクセスを、企業コンテンツ、アプリケーション、サービスにまで広げることで、従業員の生産性をさらに押し上げ、全体的な競争力の向上と顧客サービスの向上を実現します。顧客は、手軽にものごとを済ませられるため、モバイル・チャネル経由で企業と関わることを期待しています。例えばモバイル・バンキングは、財務データや取り引きへのアクセスを、いつでもどこからでも可能にすることにいち早く成功しています。

従業員、顧客の両者が、卓越したストレスのないユーザー・エクスペリエンスを期待しています。実際、消費者がモバイルを採用したことで、従業員が扱うアプリケーションに対する期待値が高まっています。いわゆる「IT コンシューマライゼーション」が個人所有端末の業務使用 (bring-your-own-device–: 以下 BYOD) プログラムの登場と、より良い企業アプリケーションのユーザー・エクスペリエンスの追求の背後にある原動力となっています[1]。

ビジネスにおけるモビリティーは、単に新しいアクセス装置というだけではなく、新たなパラダイムを提示しており、次のような固有の特徴があります。

- **モバイル・デバイスは簡単に長距離を移動する:** モバイル・デバイスの移動速度は速く、常に手が届く範囲にあります[2]。そのような使用状況が、デスクトップやノート PC でさえ通用した、ロケーションや時間帯に関連する厳格なパターンに従うことは期待できません。
- **モバイル・デバイスには柔軟な使用モデルがある:** 従来型の業務用デバイスと個人デバイスの区別は、急速に消滅しています。ユーザーは、1 日を通してさまざまなアクティビティーに単一のデバイスを使用したいと考えています。例えば、従業員はお気に入りのソーシャル・アプリケーションと仕事関連のビジネス・コンテンツへのアクセスを混在させたいと思っています。顧客は、スマートフォンやタブレットを使用してオンライン・ゲームやコンテンツ消費だけではなく、モバイル・バンキング、株式取引、診療予約を行いたいと思っています。
- **モバイル・デバイスの安全確保は困難:** 企業によるモバイル・エンドポイントの制御はますます困難になっています。悪意あるアプリケーションをインストールすることでデバイスの安全性を危うくする恐れがありながらも、ユーザーはそのデバイスを使用して慎重な扱いが求められる商取引の実行を期待します。事態はさらに複雑です - Android および iOS モバイル・オペレーティング・システムは、デバイスの状態やセキュリティー・リスクに対する可視性や管理能力を最小化するような方法で構築され、保全されているのです。

このような特徴が企業に新たなリスクの高まりをもたらしています:

- **安全性が脅かされたデバイスによるデータ侵害:** ユーザーによるデバイスの脱獄やルート化で、デバイスのセキュリティーを揺るがす危険性があります。このように安全性の確保が損なわれたデバイスは、偽のゲーム、セキュリティー、バンキング他、一見安全なアプリケーションに組み込まれた高度なマルウェア経由で感染を起こしやすいといえます。このようなマルウェアは、デバイスの通信を改ざんし、攻撃者によるリモート・アクセスやデバイスの制御を可能にする恐れがあります[3]。
- **盗難デバイスによるデータ損失:** モバイル・デバイスは、私たちの多くが個人的に経験しているように、容易に忘れたり盗まれたりします。子供の写真は個人的に極めて重要ですが、顧客、競合、売上高に関するビジネス上の機密情報の損失は、企業をブランド、規制、財務リスクにさらしかねません。例えば、臨床試験中に使用し、タブレットに保管していた患者の記録をなくすことは、医療組織の HIPPA (医療保険の相互運用性と説明責任に関する法律) 準拠に違反する可能性があります。
- **不正な共有や不用意な共有によるデータ漏えい:** モバイル・デバイスへのデータ保管で、共有はかつてないほど容易になりました。しかし、企業は当然のことながら企業データの流れを懸念し、レガシーなエンドポイント上のこのようなデータの使用方法を管理しようとあらゆる努力を惜しみませんでした。モバイル・デバイスでは、データ共有に対する管理には限界があり、これが新たなビジネス・リスクを生み出しています。例えば、従業員が誤って SEC への提出書類のドラフトを公共の e-メールで共有したり、雇用主との諍いの果てに社内文書をソーシャル・ネットワークに投稿したらどうなるでしょうか。
- **知的財産の損失およびアプリケーション・レベルの攻撃:** 新たなモバイル機能を提供し利用する主要な方法は、モバイル・アプリケーションです。企業はアプリの開発に大金を投じ、一般公開されているアプリ・ストアから顧客に提供したり、企業のアプリ・ストアから従業員に提供したりしています。しかし、ソフトウェアの脆弱性により、アプリケーションはマルウェア攻撃にさらされます。リバース・エンジニアリングにより貴重な知的財産の抽出が可能になり、それがマルウェアを組み込んだ再パッケージ化を可能にします。このように、今や悪質なものになったアプリケーションは、サード・パーティーのアプリケーション・ストア経由で提供されたり、マルウェアと共にパッケージ化され、SMS メッセージ経由で被害者に導入されます[4]。マルウェアがインストールされると、認証情報などアカウントの乗っ取りに使用されるデータが盗み出されます。
- **犯罪行為としてのアクセスとトランザクション詐欺:** モバイル・デバイスは、顧客や従業員の認証という積年の課題をさらに拡大しています。フィッシングやマルウェア攻撃により認証情報を盗み出す際、犯罪者はモバイル・デバイスを使用して、機密情報を扱うアプリケーションにアクセスしますが、これはモバイル・デバイスは個別に「指紋採取」を行うことがより困難なためです[5]。企業は、「入り口に現れたユーザー」が真正な社員、パートナー、顧客なのか、それとも彼らを騙った犯罪者なのかを判断する必要があります。この真正性の評価は、特に顧客に対しては、煩わしさを最小限にとどめ、ユーザー・エクスペリエンスを維持する必要がありますが、従業員にとっても今後はこの点がますます重要になっていきます。

次の章では、この新たなリスクに対応するために求められる能力について検討します。

モバイル・セキュリティーに対する総合アプローチ: 要求される能力

モバイル・セキュリティー・リスクは、モバイル・エクスペリエンスのライフサイクルのあらゆる段階に存在します。このようなリスクは、モバイル・デバイス、モバイル・デバイスに保管されているコンテンツ、そのコンテンツへのアクセスに使用されるアプリケーション、企業ネットワークへのモバイル・アクセス、モバイル・デバイスで開始されるトランザクションに及びます。

モバイル・セキュリティーに総合的に取り組むことで、こうしたリスクすべてに対処し、リスク間に固有の相互依存性 (例: デバイス・リスクがどのようにコンテンツやアプリケーション・リスクに影響するか) に対応できると考えられます。以下に、モバイル企業のさまざまな経営資源を管理し保護するために求められる主な能力について検討します。

デバイスの保護

最初に対応すべき緊急課題は、モバイル・デバイスそのものです。企業は、自社ネットワークに接続するあらゆるデバイスに基本的なコントロールを実施する必要があります。規制に従っていないデバイスによる企業のデータやサービスへのアクセスは、一部またはすべて制限されます。例えば:

- **安全なデバイス登録:** 業務用に構成され、企業の資格情報で認証され、正当なユーザーに登録されたデバイスに限り、企業のコンテンツや e-メールなどのサービスを使用する資格があることを徹底する。
- **最適なデバイス・セキュリティー態勢:** デバイス・セキュリティー態勢が、確実に企業の基準を満たすようする。例えば、複雑なパスコード (または指紋認証) の存在、特定の OS レベルのセキュリティーおよびプライバシー設定、デバイス・データの暗号化など。

このような手順は、従業員のデバイスでは有効なソリューションですが、顧客のデバイスに対してはいずれも可能ではありません。このため、他の緊急課題 (特に、データおよびアプリケーション保護の緊急課題、アクセスや不正行為管理の緊急課題) が、顧客デバイスのリスクに対応するために必要となります。

コンテンツおよびコラボレーションの保護

第二の緊急課題は、従業員のモバイル・デバイスでアクセスされ保管される企業コンテンツの保護です。企業コンテンツには、業務メールと関連する添付ファイルが含まれます。また、Dropbox のようなクラウド・ストレージ・サービスに加え、Sharepoint、Documentum、Filenet[6] などの企業コンテンツ・リポジトリーの非構造化データも含まれます。いったんデバイスに保管されると、こうしたコンテンツは意図しないエクスポージャーから保護される必要があります。

コンテンツおよびコラボレーション・セキュリティーには、次のコア機能が含まれます:

- **選択的な企業コンテンツのワイプ:** デバイスの紛失や盗難に備え、企業がデバイス上の任意の業務コンテンツやプロファイル設定を削除できるようにしておくことは不可欠です。そこで必要になるのが、デバイス上のビジネス・コンテンツを分離 (コンテナー化) する能力で、最終的にデバイスが発見された場合に個人のコンテンツに影響が及ばないようにします。
- **企業コンテンツ共有の制限:** モバイル・コンテンツへとアクセスする主要な方法はアプリケーションです。特定の企業リスク分析に基づき、企業アプリケーション以外のもの (例えばコンシューマー・メールやソーシャル・ネットワーキング・アプリなど) によるビジネス・コンテンツの共有に制限を設ける必要があります。コンテンツ共有の管理は、企業データ全体として、あるいは特定のアプリケーションにおける文脈の中で適用可能です。

アプリケーションとデータの保護

第三の緊急課題は、モバイル・アプリケーションとデータの保護です。ユーザーによるコンテンツや企業サービスへのアクセスは、主にモバイル・アプリケーションを使用して行われます。メール、連絡先、カレンダーは、基本的でありながらも慎重な扱いが求められる同僚、パートナー、顧客との通信を可能にします。カスタムやサード・パーティー製のアプリケーションは、文書管理システムのコンテンツでのコラボレーションに加え、CRM や ERP システムへのアクセスを扱います。そのため、モバイル・アプリケーションは、犯罪者やハッカーの主な標的となります。

アプリケーション・セキュリティーには、次の機能が含まれます:

- **安全なコーディングと脆弱性の検出:** 企業アプリケーション同様、モバイル開発者は安全なコーディング手法とベスト・プラクティスに従う必要があります[7]。ソース・コードは、マルウェアの攻撃対象領域を拡張する脆弱性の検査[8]を開発段階で行う必要があります。実行ファイルとしてのみ提供されることも多い、サード・パーティー製のアプリケーションにも入念な検査が必要です。 修復は、本番環境展開前に行うのが理想的です。
- **アプリケーションの堅牢化:** 一般公開されているアプリ・ストアで提供されているアプリ (バンキングや e-コマース・アプリなど) には、リバース・エンジニアリングが行われる危険性があります。ハッカーは、アプリケーションのソース・コードを抽出し、ユーザーの認証情報やその他の個人情報を取り込むことを目的とした新たなコードでアプリを再コンパイルし、悪意のあるアプリをサード・パーティーのアプリ・ストアで再配置できます。これは理論上の問題ではありません - 最も人気がある iOS アプリがハッキングされています[9]。企業は、リバース・エンジニアリングに対するアプリの堅牢化を検討し、アカウント乗っ取り攻撃に対するエクスポージャーを減らす必要があります。

アクセス管理と不正行為

第四の緊急課題は、デバイスから行われる企業のリソースへのモバイル・アクセスの管理と不正行為の検出です。モバイル認証は、変動しやすいモバイル・デバイスの性質 (アクセス時間やロケーション) およびログイン・プロセスにおける摩擦軽減の必要性に対応する一般的な要件です。認証以外にも、トランザクション活動は、特に顧客向けには、ユーザーのこれまでのアクティビティーという文脈 (コンテキスト) の中で検討し、犯罪行為や不正行為を検出する必要があります。

この緊急課題には次の機能が含まれます:

- **リスク・ベースの認証:** モバイル認証はコンテキストとリスクを意識したものでなければなりません。摩擦を減らし、ユーザー・エクスペリエンスを維持するためにも、ワンタイム・パスワードのような強力な認証手段は、アクセスのコンテキスト (新規デバイス、新規ロケーション、通常とは異なる時間帯、遠く離れたロケーションからの同時ログイン) により、リスク・プロファイルの上昇が示唆される場合のみ開始すべきです。
- **モバイル・シングル・サインオン:** モバイルのログイン操作は、フルサイズの PC キーボードよりもさらに厄介なため、企業のサービスに 1 回ログインすれば、その後は認証を受けた他のサービスにもシームレスにアクセス可能にすることはユーザーにとってメリットとなります。
- **トランザクション不正リスク検出:** 特定のユーザー・アカウントというコンテキストにおいては、アカウント履歴やアカウント・リスク指標 (マルウェアやフィッシング攻撃など) という軸で、入ってくるトランザクションを分析することで、犯罪行為としてのアクセスを検出し、企業とその顧客をアカウントの乗っ取りや不正行為から保護できるようになります。

セキュアな企業モビリティーのための堅固なプラットフォーム

前項では、真にセキュアなモバイル企業を確立するために対応するべき 4 つの緊急課題を検討しました。しかし、効果を最大化し維持するには、こうした能力をグローバル・セキュリティーと脅威インテリジェンスだけではなく、コンテキストとリスクを意識することで推進していく必要があります。

モバイル企業インフラストラクチャーにコンテキストとリスク意識を組み込む

従業員による企業コンテンツやアプリへのモバイル・アクセスを可能にしているため、根底となるデバイスのリスクを測定し、適切な管理を適用することは非常に重要です。例えば、高リスクのデバイスへの企業コンテンツの提供を防ぐ、規定に準拠していないデバイスからコンテンツを削除する、リスク・プロファイルに基づき企業リソースへのアクセスを制限するなどが考えられます。

デバイスが「高リスク」であるかどうかを判断するには、次の項目を検討します:

- **デバイスは脱獄やルート化されているか?** Apple や Google による検査を受けていないアプリのインストールを試みるユーザーは、多くの場合脱獄 (iOS) やルート化 (Android) として知られる処理をデバイスで実行します。この処理は、ハッカーにより開発され、新しい OS のバージョンが登場すると更新されます。この処理によりユーザーはどのようなアプリでも好きにインストールできるようになりますが、デバイスのセキュリティー・モデルが破られ、マルウェア攻撃を非常に受けやすくなります。このようなデバイスが企業ネットワークに入り込まないようにすることが非常に強く推奨されます。
- **デバイスはモバイル・マルウェアに感染しているか?** デバイスは、企業アクセスを要求した時にはすでにマルウェアに感染していたり、時間が経つうちに感染してしまうかもしれません。マルウェアは、SMS、連絡先、e-メールなどの重要なサービスを改ざんし、認証情報、通話記録、写真などの個人情報を取得する恐れがあります。デバイス・リスクを評価し、関連する企業ポリシーをデバイスに適用するには、マルウェアの存在をリアルタイムで検出することが極めて重要です。
- **デバイスは最新のソフトウェアとすべてのセキュリティー・パッチを適用しているか?** 他の企業プラットフォーム同様、ユーザーは最新のセキュリティー・パッチ (最新の OS ビルドに同梱) をデバイスに適用する必要があります。特に Android OS では、まったく更新されていないデバイスや、パッチが適用されていない重大な脆弱性が存在し、最新化されていないデバイスがあります。
- **デバイスが疑わしいコンテキストで使用されていないか?** 疑わしい使用は、コンテキストから導き出すことができます。デバイスはいつどこで使用されるでしょうか、新規デバイスなのかそれとも以前登録されたものなのでしょうか。例えば、以前のアクセスが常に米国西海岸から行われているにもかかわらず、米国以外の国からアカウントへのアクセスがあるなどです。

このようなリスクが検出され、分析されれば、さまざまな修復措置を取ることができます。例えば、企業モビリティー管理システムは、安全が損なわれたデバイスから任意の企業コンテンツを消去し、新たなコンテンツの提供を防ぎ、悪意のあるアプリを削除できます。企業リソースへのアクセスは、デバイスのリスクが修復されるまで制限することができます。モバイル・アプリケーションは、デバイス・リスクに基づき機密情報に関わる機能を無効にしたり制限をかけたりできます。アクセス管理レイヤーは、リスク・ベースの認証により脆弱なデバイス・アクセスを制限できます (そのため、強力な認証は、本当に高リスクの状況でのみ使用されます)。

モバイル・セキュリティー・フレームワークをコンテキストとリスク意識の高いものにすることで、モバイル・チャネル固有のリスクに対応する、よりスマートな方法を採用できます。

エキスパートによる調査と脅威インテリジェンスによるモバイル・セキュリティー・コントロールの維持

セキュリティー・コントロールが直面する課題のひとつに、新たに出現する脅威に常に適応し続けることがあります。モバイル・セキュリティー・コントロールも例外ではありません。例えば、脱獄検出ロジックは、デバイスが脱獄済みであるという事実を覆い隠し、高リスクのデバイスであるとしてフラグを立てられないようにする「*Jailbreak hider*」[10] の進化に対応する必要があります。同様に、行動やコンテキストに関するコントロールが増えるにつれ、ハッカーは被害者を綿密に模倣し検出を逃れようとします。

全体として、モバイル・セキュリティー・コントロールを実行可能にしておくには、専用の調査チームと、脅威に対するグローバル・インテリジェンスをリアルタイムで提供する信頼性の高いソースが求められます。

より幅広い企業のセキュリティー・コンテキストへのモバイル・セキュリティーの統合

モバイル・デバイスは、新たな企業アクセス・チャネルを創出します。そのため、モバイル・セキュリティー・イベントは、全社的なセキュリティー・コンテキストの一環として管理する必要があります。モバイル・セキュリティー・イベントを企業の SIEM 製品 (セキュリティー情報およびイベント管理システム) と連携することで、モバイルを中心とした脅威および攻撃のベクトル (経路情報) を企業のインシデント対応プロセスに組み込むことができます。

IBM Mobile Security Framework

IBM Mobile Security Framework は、すべての緊急課題においてモバイル企業の安全を確保する IBM の総合ソリューションです。
特定のセキュアなモビリティー・ニーズに対応するベスト・オブ・ブリードの製品を集約・統合することで、影響力を最大化し、迅速に価値を実現します。

フレームワークの構成要素を、2 つの一般的なモビリティー構想を詳しく説明することで紹介していきます。

モバイル・ワークフォースの安全確保と BYOD プログラムの実施 (B2E)

企業は、従業員が安全に企業リソースへモバイルからアクセスできるようにしたいと考えています。BYOD プログラムがモビリティー・プロジェクトを開始する必要最小要件になりつつある中、IT 部門のコントロール外にあるデバイスを管理し安全を確保する必要性があります。デバイス・リスク以外にも、個人データとビジネス・データの共存は、IT 部門のセキュリティー・チームやモビリティー・チームにさらなる複雑さをもたらしています。

従業員のデバイスと重要なビジネス・コンテンツの保護

IBM MobileFirst Protect (MaaS360) は、迅速なデバイスの登録を可能にし、きめ細かいポリシーを企業所有デバイスおよび管理された従業員所有のデバイスに無線で適用できます。こうしたポリシーにより、適切な*デバイス・セキュリティー態勢と安全なデバイスの登録* を確保できます。

IBM MobileFirst Protect は、コンテナー化技術とアプリケーション・ラッピング技術を使用して、モバイル・デバイス上の企業データを分離し管理します。これにより、写真などの個人情報に影響を及ぼすことなく、業務データを*選択的に消去* できます。コンテンツの漏えいを確実に防ぐため、MobileFirst Protect は、安全なブラウザーや企業ネットワークへの安全な接続を提供するゲートウェイだけではなく、e-メール、連絡先、カレンダー、コンテンツ・エディターといった、*安全な生産性アプリケーション* を備えた、個別のワークスペースを提供します。これにより、企業資産は管理された方法によってのみアクセスされ、コンテンツ共有はビジネス・リスクおよび企業ポリシーに基づき制限されるようになります。

IBM MobileFirst Protect Threat Management は、IBM Security Trusteer を搭載しており、独自のリスク認識機能を加えたうえで、デバイス・リスクに基づく動的なポリシー施行を企業が行えるようにします。これは、従業員により脆弱な、または侵害されたデバイスが企業環境へと持ち込まれる可能性があるため、BYOD プログラムでは特に重要です。例えば、マルウェアに感染したデバイスによる社内 Web アプリケーションやコンテンツ・リポジトリーへのアクセスを制限し、データ・エクスポージャーやネットワーク侵害のリスクを緩和できます。

カスタム・ビルドの企業アプリケーションの保護

IBM MobileFirst Platform Foundation (別称 Worklight) は、ネイティブおよびハイブリッドのモバイル・アプリケーション向けに統合された開発/ランタイム環境を提供します。

IBM MobileFirst Platform には、根底にあるデバイス・リスクと他のコンテキスト・パラメーターに基づき、特定アプリケーション向けの規則を施行して、アプリケーションの使用方法と機能を制御するセキュリティー・エンジンが含まれます。これは、モバイル・セキュリティー要件が特定のアプリケーションと結びつけられ、本書で検討した、より包括的なインフラストラクチャーに対し重み付けを行う必要がある場合に役立ちます。**IBM MobileFirst Platform Application Scanning** は、ソース・コードの脆弱性をスキャンすることでシームレスにこの環境を強化します。これにより、安全な開発ライフサイクルと、マルウェア攻撃によるリスクの低減が可能になります。実行ファイルとしてサード・パーティーから入手可能なアプリケーションは、**IBM Security Appscan Mobile Analyzer** を使用して分析できます。これは、クラウド・ベースのモバイル・アプリケーション・セキュリティー・サービスです。Mobile Analyzer は、アプリをスキャンしてクロスサイト・スクリプティングや破綻した暗号化処理など、潜在的なコードの脆弱性についてレポートします。

IT セキュリティーは、セキュリティー・リスクに基づき、社内アプリ・ストアへのモバイル・アプリの追加を許可または禁止できます。

また、Trusteer Mobile SDK を使用することで、自社アプリケーションをリスク意識の高いものにできます。Trusteer Mobile SDK は、IBM MobileFirst Platform Foundation にあらかじめ統合されており、アプリケーションが侵害されたデバイスや脆弱性のあるデバイスで実行されると、アプリケーションのセキュリティー・ポリシーを実行時に適用できます。また、このリスク認識は任意のモバイル・アプリに直接組み込むこともでき、デバイス・リスク・データを活用して、デバイス・リスクに基づきアプリケーションのビジネス・ロジックを適応させることができます。例えば、モバイル ERP アプリで、リスクの高いデバイスでの発注の承認を無効にできます。

従業員による企業ネットワークやリソースへのアクセス管理

従業員がモバイル・デバイスから企業ネットワークやリソースへと接続すると、**IBM Security Access Manager (ISAM)** は、接続要求を分析します。アクセス時間、デバイスのロケーション、デバイス ID、デバイス・リスク要因など、さまざまな領域でコンテキストを認識して、接続にアクセス・コントロール・ポリシーを適用します。

ISAM は、IBM MobileFirst Platform、IBM MobileFirst Protect、Trusteer Mobile Browser と統合され、ポリシー・エンジンに特定のデバイス・リスクやコンテキスト指標に関する情報を提供します。例えば、マルウェアに感染したデバイスによるネットワークへの接続を防いだり、新たなデバイスやロケーションから行われるアクセスに *2 要素認証* の使用を開始したり、特定のリソースへのアクセスに、*セキュアなブラウザー* の使用を強制したりできます。

さらに、ISAM は IBM MobileFirst Protect と統合して、モバイル・デバイスから企業アプリケーションへの *シングル・サインオン* を提供します。

モバイルでの顧客やパートナーのトランザクションの保護 (B2C および B2P)

モバイルの顧客を保護することには、モバイル・ワークフォースの安全保護への対応とは異なる課題があります。モバイルの顧客やパートナーの場合、こうしたデバイス(管理されていないデバイス) に対して、企業は何らコントロールを行うことができず、またそのユーザーが自分たちのデバイスに対し、そうしたコントロールを提供することに同意することはまずあり得ません。そのため、企業は管理されていないデバイスには侵害されている可能性があるものとして、機密性の高い企業コンテンツを絶対にそのデバイスに配置しないようにする必要があります。安全性を確保する必要があるタッチ・ポイントは、顧客のログインおよびトランザクションと、顧客に対応するアプリケーションです。

外部向けのアプリケーションの保護

企業は、一般公開されているモバイル・アプリケーションで顧客やパートナーと関わります。このモバイル・アプリケーションは、すでに述べたようにソース・コード開発段階で、または実行ファイルとして、脆弱性について詳細な検査を行う必要があります。しかし、こうしたアプリケーションは一般公開されているため、企業はまた Arxan Application Protection for IBM Solutions のようなソリューションで*アプリケーションを堅牢化*することも検討する必要があります。アプリケーションを堅牢化することで、ハッカーがモバイル・アプリにリバース・エンジニアリングを施し、悪意あるコードを組み込み、サード・パーティーのアプリ・ストアで再配信して、何も知らない顧客をおびき寄せることを防ぎます。このようなアプリがインストールされ、起動されると、多くの場合顧客の認証情報を取得したり、詐欺を開始したりします。

さらに、管理されていないデバイスのセキュリティー態勢は弱いことが多いため、外部に対応するアプリに Trusteer Mobile SDK を組み込み、基盤となるデバイスのリスクを動的に評価する必要があります。例えば、モバイル・バンキング・アプリで、脆弱なデバイス上の取り引き活動を無効にできます。

クロスチャネル攻撃の検出: 犯罪行為としてのアクセスと不正なトランザクション

顧客は、モバイル・アプリケーションやブラウザーを使用して、モバイル・バンキングやモバイル・コマースなどのサービスにアクセスします。顧客の認証情報が、モバイル・デバイスやパーソナル・コンピューター上でフィッシングやマルウェア攻撃による流出の危険にさらされることも珍しくありません。犯罪者はこうした認証情報を使用して、自身のモバイル・デバイスから顧客のアカウントを乗っ取り、このようなインシデントを特定するという困難な任務がセキュリティー・チームやリスク対策チームに課せられます。**IBM Security Trusteer Pinpoint Criminal Detection** は、アカウント・ログインとトランザクション・アクティビティーに関連する膨大なリスク要因を相関分析し、高リスクのアクセスに正確にフラグを立てます。考慮されるリスク要因には、強力なデバイス ID、デバイスの使用パターン、これまでにデスクトップ、ノート PC、モバイルなどあらゆるチャネルで、マルウェアやフィッシング攻撃により改ざんされたインシデントなどがあります。独自の動的なリスク・データをリアルタイムで活用することで、犯罪行為にただちに対応することが可能になり、誤検出を最小化できます。

モバイル・セキュリティーの強固な基盤

IBM のモバイル・セキュリティー向けの基盤は、IBM の全体的なソリューションをより強固かつより効果的なものにします。

リスク認識: Trusteer Mobile SDK

Trusteer Mobile SDK は、以下のような侵害された脆弱なデバイスを正確に検出します。

- **ルート化されたデバイスおよび脱獄済みのデバイス** (デバイスがもはや安全とはいえない事実を隠すことを意図した方法で脱獄されたものを含む)。
- **マルウェアに感染したデバイス** (金銭目的の脅威および一般的な企業脅威)
- **古いモバイル OS** および適用されていないセキュリティー・パッチ

さらに、Trusteer Mobile SDK は、*強力なデバイス* ID を提供し、各デバイスを明確に特定します。

Trusteer Mobile SDK は、複数の IBM オファリングにあらかじめ組み込まれており、リスク認識をもたらすことでよりスマートなポリシー適用に必要な情報を提供します:

- **IBM MobileFirst Protect Threat Management (Maas360):** この統合により、マルウェアの影響を受けたデバイスからデバイス・リスクがなくなるまで企業コンテンツを削除するなど、特定の軽減措置を取ることができます。
- **IBM MobileFirst Platform (Worklight):** アプリケーション開発/ランタイム・プラットフォームとの統合により、開発者はコーディングを一切行うことなく直接アプリケーションにリスク認識を組み込むことができます。アプリケーション・ランタイム・エンジンは、セキュリティー・ポリシーを適用して、根底にあるデバイス・リスクの種類およびスコープに応じてアプリケーションの使用を制限します。
- **IBM Security Access Manager:** ISAM は、MobileFirst Platform、MobileFirst Protect Threat Management、Trusteer Mobile Browser により受け渡されたデバイス・リスク特性を取り込みます。ルール・ベースのポリシー・エンジンは、このリアルタイムで提供される動的な属性に基づき、企業リソースへのアクセス・コントロールを適用できます。

このようなあらかじめ組み込まれた統合に加え、アプリケーション開発者は Trusteer Mobile SDK をどのアプリケーションにも組み込むことができます。SDK を呼び出すことで、リアルタイムでデバイス・リスクが検出され、アプリのコードへと提供されます。例えばモバイル・バンキング・アプリは、マルウェア感染など、根底にあるデバイス・リスクに基づいて送金を制限し、強力なデバイス ID およびこのアプリで生成された各トランザクションを関連づけることができます。

グローバルな脅威インテリジェンス: X-Force および Trusteer Research

犯罪者やハッカーはセキュリティー・コントロールを突破したり回避したりする新たな方法を探しているため、脅威の様相は常に変化しています。IBM はグローバルな調査活動を行い、脅威の様相を常時監視し、最新の技術と対抗手段でセキュリティー防衛策を適応させます。

IBM リサーチは、新たに登場したモバイル・マルウェア、新たなルート化や脱獄手法、犯罪者が顧客や従業員のアカウントへの侵入に使用する新たな戦術を追跡します。調査結果は、正確な検出とモバイル脅威の防止を維持するために、モバイル・セキュリティー・コントロール全体でポリシー・ルールおよびコード堅牢化として適用されます [11]。

セキュリティー情報およびイベント管理: IBM Security QRadar

さまざまなモバイルセキュリティー製品が、IBM Security QRadar と (適用可能な場合に) 統合されています。IBM Security QRadar は、全社的にあらゆるセキュリティー関連イベントを集約し相関分析します。モバイル・セキュリティー・イベントを組み込むことで、モバイル・チャネルを使用した高度な攻撃に対して適切な企業対応を構築できます。

モバイル・セキュリティー成熟への道筋: 行動喚起

2014 年後半、IBM は企業が現在どのような能力を開発し、IBM Security Framework の緊急課題と向き合っているかを探る調査を開始しました。また、「モバイル・セキュリティー成熟への道筋」において、こうした能力を拡張する短中期計画についても検討しました。

その結果、企業は「まだ道半ば」であることが示されました。当然ながら、デバイスおよびコンテンツのセキュリティーに対する基本的な緊急課題には、継続的な注意が注がれています。それでも、企業はデバイス盗難によるデータ損失の危機に直面しており、企業モビリティー管理 (EMM) 製品群の使用がこのシナリオへの対応として有効です。近い将来、実質的にあらゆる企業が何らかの形の EMM を導入し、企業リソースへのアクセスを許可する前に、ポリシーへの確実な準拠をモバイル・デバイスに課すようになると予想します。また、デバイスが紛失や盗難にあった場合、企業コンテンツは選択的に消去されるか保護されるようになると予想します。

企業が抱える次の大きな課題は、セキュアな企業アプリケーションの開発です。安全なアプリケーション開発ライフサイクルを確立する必要性は、安全な Web 開発という既存のパラダイムから引き継がれています。
一部の対応要員は、アプリのソース・コードで脆弱性スキャン・ツールを使用していますが、バイナリーで (サード・パーティーまたは公式アプリでさえ) 行う集団はさらに少ないといえます。こうしたビジネス・アプリケーションから確実に脆弱性をなくすことは、マルウェアや他の攻撃にさらされる危機を低減させながら、モビリティーのメリットを実現したいと考えるあらゆる企業にとって、非常に重要なポイントです。

最後に、アクセスとトランザクション詐欺のリスクを管理することは、新たに考慮すべきポイントです。トランザクション・リスクは、ネットワークへのアクセス、ログイン、データやサービスへのアクセスなど、モバイル・デバイスとバックエンド・システム間のあらゆるインタラクションに関係します。効果的にトランザクションを保護するには、企業は根底にあるデバイス・リスクとユーザーのアクセス・パターンを検討して、特定のセッションやインタラクションに関連するセキュリティー・リスクの高いトランザクションを判断する必要があるでしょう。これにより、アカウントの乗っ取りや不正なトランザクションを、企業データや顧客の資産が危険にさらされる前に、検出できるようになります。

IBM Mobile Security Framework は、モバイル企業を保護する総合ソリューションと包括的なロードマップを提供します。リスクの最小化とコストや複雑さの低減を行いながら、従業員、お客様の両者に対するモビリティーのメリットを企業が取り入れられるようになります。

詳細情報

モバイル・エンタープライズの保護に関する詳細については、IBM 営業担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。
https://www.ibm.com/mobilefirst/jp/ja/mobile-security.html
さらに、IBM グローバル・ファイナンシングは、企業が必要とする IT ソリューションを最もコスト効果に優れた、戦略的な方法で獲得できるよう支援します。IBM の信用審査の承認を受けたお客様については、お客様の事業目標に合わせて IT ファイナンシング・ソリューションをカスタマイズして、効果的なキャッシュ管理と総所有コストの改善を実現できます。IBM グローバル・ファイナンシングは、重要な IT 投資の資金を調達し、ビジネスを推進させる最も賢明な選択肢です。詳細については、次の Web サイトをご覧ください。**ibm.com**/financing/jp

[1] IBM/Apple のモバイル・エンタープライズ提携は、バーチカル・モバイル・アプリケーションをいかに構築し提供するかに対して高まる期待に対応するものです。

[2] https://www.cmocouncil.org/facts-stats-categories.php?view=all&category=mobile-marketing

[3] https://www.lacoon.com/lacoon-discovers-xsser-mrat-first-advanced-ios-trojan/

[4] https://www.fireeye.com/blog/threat-research/2015/02/ios_masque_attackre.html

[5] http://securityintelligence.com/can-you-trust-it-mobile-authentication-must-become-context-and-risk-aware

[6] IBM エンタープライズ・コンテンツ管理ソリューションについては、次の Web サイトをご覧ください: http://www-03.ibm.com/software/products/en/category/enterprise-content-management

[7] https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Home

[8] Gartner Hype Cycle for Enterprise Mobile Security 2014 では、「…企業にますますモバイル・デバイスが浸透しているなか、モバイル・アプリケーションとデータのセキュリティー検証と保護は、攻撃に対する予防措置として必須になりつつある」と示しています。

[9] https://www.arxan.com/arxan-annual-report-state-of-mobile-app-security-reveals-an-increase-in-app-hacks-for-top-100-mobile-apps/

[10] http://lifehacker.com/5864300/xcon-unblocks-iphone-apps-with-jailbreak-detection

[11] IBM X-Force は、グローバルなサイバー犯罪の脅威の様相における主な発展をまとめた 4 半期レポートを発行しています。最新のレポートについては、次の Web サイトをご覧ください: http://www-03.ibm.com/security/xforce/#quarterly

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
May 2015

WGW03121-JPJA-00