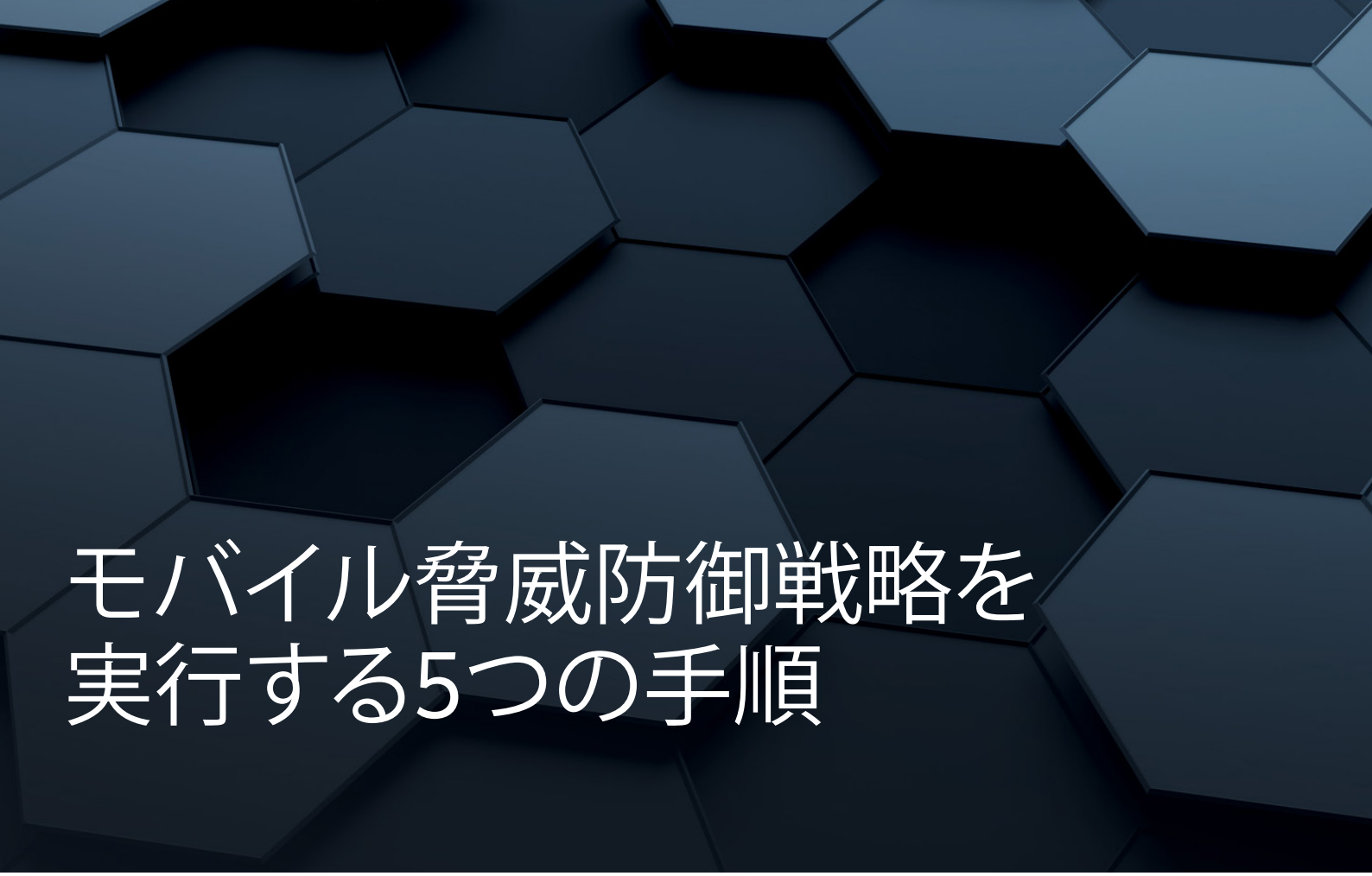


モバイル脅威防御戦略を実行する5つの手順

モバイル脅威に対する防御はスピード勝負。企業を攻撃から守るために全力を尽くしていますか？

従業員は、空港、ホテル、カフェの無料Wi-Fiをネットワークを利用していますか？USBポートは？従業員のデバイスは、中間者（MITM）攻撃や企業の認証情報を盗もうとするハッカーから保護されていますか？そのような攻撃を認識し、ブロックする戦略をお持ちですか？

このガイドの5つの手順では、モバイル従業員を標的とした高度なモバイル脅威に対して、有用な情報収集と迅速な保護を行う最善の戦略を策定します。オンデバイスのモバイル脅威対策で、最新のセキュリティリスクからデバイス、アプリ、データを保護する方法をお読みください。

MobileIron

MKT JA-A4 v1.0

モバイルデバイスに対する攻撃は急速に進化し、深刻化します。モバイル脅威防御（MTD）戦略は、そのスピードに勝てなければなりません。エクスプロイトを行う組織は、成功すれば多大な利益があるため、極めて意志が固く、巧妙です。2017年のPonemon Instituteのセキュリティレポートによれば、企業において消費者や顧客の個人情報（サイバー犯罪者にとって価値の高い情報）を含むレコード1,000件以上の情報漏洩が繰り返し生じる可能性は28%と推定されます[1]。このような攻撃は甚大な被害を及ぼします。情報の漏洩または侵害に加え、情報漏洩が報道されれば、顧客との関係や企業の評判に傷がつき、収益の喪失、罰金や法的費用が生じます。事態の収拾に貴重な時間やリソースも奪われます。

このようなリスクを防ぐためにあらゆる対策を講じていないなら、今こそ始めるべきです。ここでは、セキュリティの盲点を明確にし、場所や利用するネットワークを問わず、企業のアプリとデータにアクセスするすべてのモバイルデバイスを総合的に保護する5つのベストプラクティスをご紹介します。

モバイル脅威の現状

攻撃の75%
外部のハッカーによる侵入

ハッカー関連侵害の81%
盗んだパスワードの悪用

侵害の73%
動機は金銭的利益[2]

ICT Security Magazine, "2017 Data Breach Investigations Report, 10th Edition（2017年データ侵害調査レポート第10版）"

1 https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states

2 https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

MobileIron

ステップ1:
シームレスで目立たない脅威防御

一部のモバイルセキュリティソリューションは、モバイルデバイスのセキュリティに関してユーザーに依存しています。これは、不適切で効果の薄いMTD対策です。このような「ユーザーベースのセキュリティ」ソリューションの場合、モバイル従業員が自社のアプリストアを開き、クライアントをダウンロードした後、複数の手順を踏んでアプリをインストール、有効化、更新しなければなりません。さらに悪いことに、IT部門は、インストールされたクライアントをほとんどどうすることもできません。ユーザーがアプリを削除したり、無効化したり（スワイプオフ）すれば企業データは危険にさらされます。実際、ある調査によれば、3分の1以上の企業が、予算や人手不足のために最新のセキュリティを全社に適用し続けることができず、モバイルデバイスのセキュリティが十分ではありません。[3]

IT部門は、多くの場合、ユーザーが最新のセキュリティアプリをデバイスで使用することを期待しています。しかし、もしユーザーがデバイスを更新せず、すべてのエンドポイントがセキュリティポリシーに適合しなければ、企業は攻撃にさらされます。2017年のDimensional Researchのレポートに、次のように書かれているのも不思議ではありません。「調査参加者の3分の2は、自分の働く企業がモバイルサイバー攻撃を防ぐことができるかどうかに疑問を抱いていました。また、セキュリティ担当者ほぼ全員が、モバイル攻撃が急速に増加していると考えています。」[4]

企業リソースにアクセスするすべてのモバイルデバイスのセキュリティを即座に100%確保するには、ユーザーに最新版のインストールを任せてはなりません。Gartnerは、高度なモバイルセキュリティをシームレスに導入するために、「MTDソリューションとエンタープライズモビリティ管理（EMM）ツールの統合」を企業に推奨しています[5]。これならIT管理者は、セキュリティ保護と更新をEMM経由で直接デバイスに適用できます。つまりユーザーが最新のセキュリティ更新をダウンロードしたり、有効化したりする必要はありません。プライバシーポリシーも適用されます。EMMとMTDを統合したソリューションにより、IT部門はユーザーのデバイスがコンプライアンス違反でないか世話を焼く必要がなくなり、経費を削減して長期的な優先事項に集中することができます。

「調査参加者の3分の2は、自分の働く企業がモバイルサイバー攻撃を防ぐことができるかどうかに疑問を抱いていました。また、セキュリティ担当者ほぼ全員が、モバイル攻撃が急速に増加していると考えています。」

— Dimensional Research
"The Growing Threat of Mobile Security Breaches: A Global Survey of Security Professionals
（モバイルセキュリティ侵害の脅威が増加：セキュリティプロフェッショナル世界調査）"

3 https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
4 https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
5 https://www.gartner.com/doc/3789664/market-guide-mobile-threat-defense

ステップ2：
すべての種類のサイバー攻撃を把握

モバイル脅威の可視化不足は、現代の企業が直面する重大なモバイルセキュリティ問題です。事実、調査した企業の半数以上（51%）が、従業員が仕事に使用しているモバイルデバイスにマルウェアがダウンロードされてもわからないと回答しました[6]。アプリレベルの脅威にのみ重点を置き、可視化不足に拍車をかけているモバイルセキュリティソリューションもあります。しかし、すべてのサイバー攻撃が同じではありません。攻撃の経路には複数あり、他の方法で関門を突破するものもあります。したがって、1つの層だけに注目していてはなりません。完全に統合された包括的なモバイルセキュリティで、デバイス、ネットワーク、アプリケーション（DNA）攻撃を防ぐ必要があります。

- **デバイスレベルの攻撃：**エクスプロイトが成功すれば、デバイスを完全に制御し、暗号化されたコンテンツを削除できるため、極めて深刻な被害を与える可能性があります。デバイスレベルの攻撃は一般に、ダウンロードした無料アプリや、開くと同時にマルウェアに感染するSMSメッセージを通じて実行されます。
- **ネットワークレベルの攻撃：**パブリックネットワークは便利ですが、モバイルデバイスにエクスプロイトを引き込む経路ともなります。たとえば、ホテルやカフェの無料Wi-Fiを不正アクセスポイントとして、MITM攻撃が実行されたり、デバイスと企業ネットワークの通信を傍受されたりすることもあります。攻撃者はデバイスへの侵入に悪用できる既知の脆弱性を短時間で探し出し、ユーザー名、パスワード、企業の機密データを抽出した後、企業リソースへのアクセスに利用します。
- **アプリレベルの攻撃：**通常、ユーザーが不注意に第三者のアプリストアからアプリをダウンロードすることで生じます。アプリに含まれるマルウェアが、許可の取得、デバイスへのエクスプロイト、社内ネットワークへの侵入によって企業データを詐取します。

高度な機械学習アルゴリズムと挙動ベースの検出機能を持つソリューションがあれば、企業は、このような既知および未知（ゼロデイ）の攻撃をブロックできます。機械学習ツールは、シングルアプリベースの脅威に狭く焦点を絞るのではなく、無許可のVPN構成、無料アプリダウンロードなど、すべてのタイプの異常動作を即座に認識します。

「調査した企業の半数以上（51%）が、従業員が仕事に使用しているモバイルデバイスにマルウェアがダウンロードされてもわからないと回答しました。」

— Zimperium
"Mobile Security 2017 Spotlight Report（モバイルセキュリティ2017年スポットライトレポート）"

6 http://go.zimperium.com/2017-mobile-security-report

ステップ3:
実用的な脅威情報の提供

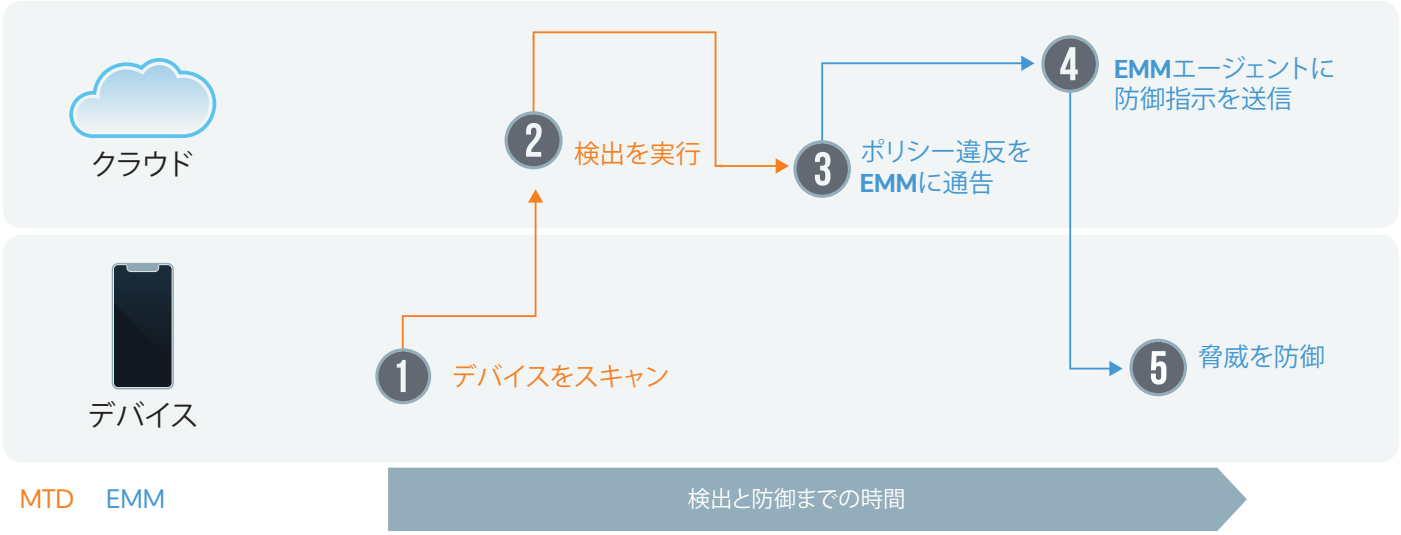
可視化不足もセキュリティの盲点を作りますが、すべての脅威に同じ優先度で対処する大量のアラートもセキュリティの低下を招きます。モバイルセキュリティ管理者が「アラート慣れ」し、根拠に基づく決断を速やかに下せなくなるためです。

MTDソリューションが有用な脅威情報を提供するには、機械学習アルゴリズムを利用した分析エンジンを組み込み、デバイス自体の上で悪意ある行為と正常な行為を区別する必要があります。機械学習アルゴリズムは、モバイルデバイスのOS統計データ、メモリ、CPU、その他のシステムパラメータの微妙な変化を分析することにより、攻撃の種類を正確に特定するだけでなく、誰が、何を、どこで、いつ、どのように攻撃したかの詳細な解析を提供します。

機械学習をベースとするオンデバイスのソリューションは、ユーザーがネットワークに接続していないとき、または未知のマルウェア、新しい脅威、ゼロデイ攻撃に遭遇したときでも攻撃を検出します。このタイプのソリューションは、クラウドにトラフィックをトンネリングする必要がないため、クラウドベースのソリューションより速度でも優れています。モバイルセキュリティの専門家は、差し迫った脅威を迅速に特定し、優先度を付け、深刻な攻撃が企業リソースに影響を与える前に即座に行動を取ることができます。

検出と防御

その他のMTD/EMMソリューション



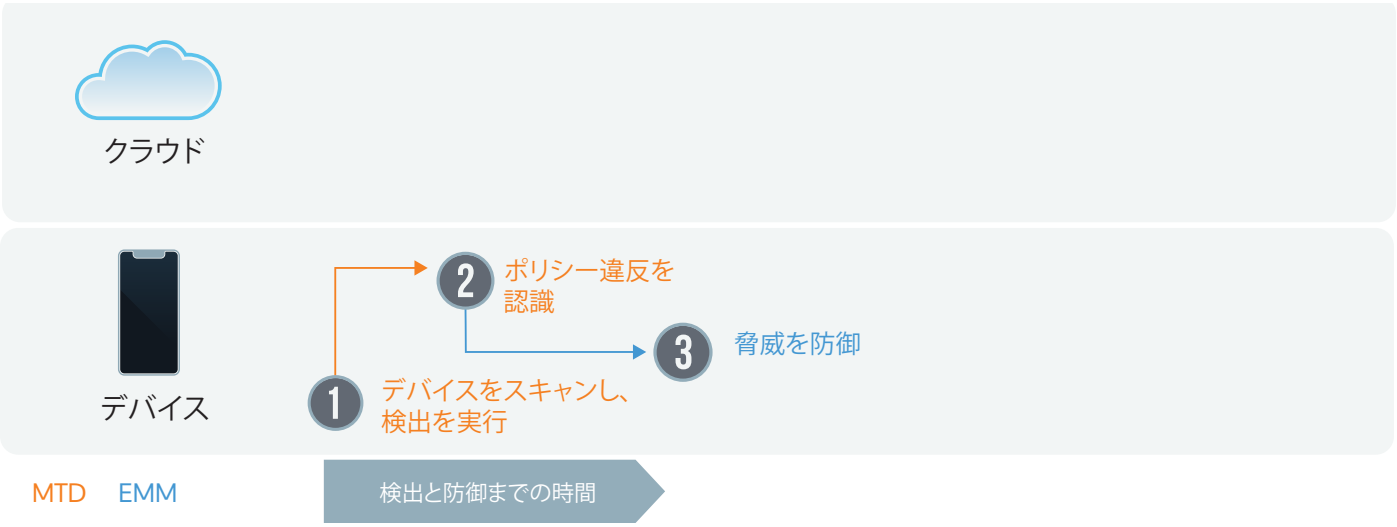
ステップ4:
機械速度でデバイスを脅威から防御

攻撃は機械速度で生じるため、オンデバイスのセキュリティも機械速度で対応する必要があります。クラウドだけのMTDソリューションは、オンデバイスのモバイル脅威の検出と防御を遅らせることがあります。デバイスをスキャンし、いったんクラウドにアラートを送ってから、EMMにセキュリティ侵害を伝えるためです。これにより、無料Wi-Fiを通じてデバイスを攻撃するMITMのように、甚大な被害を与える攻撃への対処が遅れるかもしれません。このタイプの攻撃では、ハッカーがモバイルデバイスに侵入し、ユーザーより強い制御力を発揮します。そして、ユーザーの連絡先すべてをダウンロードする、メールを盗む、ユーザーとしてログインしてCEOにフィッシングメールを送るなども可能です。これによって、企業全体に多大なセキュリティ侵害が生じる恐れがあります。

オンデバイスのMTDソリューションは、脅威の検出と防御に余計な手順がないため、機械速度で脅威に対応します。情報はデバイス上にあるため、即座にポリシー違反を検出し、MITMを含めた脅威をデバイス上でブロックできます。スピード勝負のハッカーとの戦いにおいて、これは決定的な利点であり、以降の多くの頭痛の種を省くことになります。

検出と防御

MobileIron Threat Defenseソリューション



ステップ5：
詳細なレポートが
コンプライアンス要件を簡素化

世界規模の企業が規制に適合するには、明確な監査と報告のプロセスによって、一般データ保護規則（GDPR）、決済カード業界データセキュリティ規格（PCI-DSS）、医療保険の相互運用性と説明責任に関する法律（HIPAA）、Notifiable Data Breaches（NDB）など多くの規制に適合する必要があります。

モバイル企業では、IT部門の管理するデスクトップにユーザーがつながっていないため、これがさらに難しくなります。従業員は、複数のネットワークを介して、さまざまな個人/企業所有のデバイスでビジネスアプリやデータにアクセスします。あるレポートによれば、「GDPRコンプライアンスを達成する上での難関の1つは、ノートPCや他のモバイルデバイス上にある個人を特定できる情報（PII）を保護することです。これは企業のファイアウォールの中にないため、追跡が難しく、侵害される大きなリスクがあります。」[7]

モバイル脅威やリスクの状況を明確に把握し、コンプライアンスの要件を満たすには、すべてのデバイスとアプリを追跡/管理できる必要があります。監査レポートの迅速な生成、脅威のログ、アクセスと利用の詳細な履歴があれば、管理者は速やかに脆弱性を特定し、すべてのユーザー、デバイス、アプリのコンプライアンスを確保できます。企業は、コンプライアンスの指針に従い、ビジネスをモバイルリスクから守るよう最善を尽くすことができます。

「GDPRコンプライアンスを達成する上での難関の1つは、ノートPCや他のモバイルデバイス上にある個人情報（PII）を保護することです。これは企業のファイアウォールの中にないため、追跡が難しく、侵害される大きなリスクがあります。」

GDPR：レポート
"GDPR Compliance for Mobile Workers（モバイルワーカーのGDPRコンプライアンス）"、2017年10月

7 https://gdpr.report/news/2017/10/13/gdpr-compliance-mobile-workers

MobileIron THREAT DEFENSE

MobileIron Threat Defense：オンデバイスモバイルセキュリティが少ない労力で有用な情報を提供

MobileIronは、サイバー犯罪者が常に高度な方法を編み出し、あらゆる手段を使ってデータを抜き取ろうとしていることを知っています。このため常に革新を続け、お客様が最新のモバイルセキュリティ脅威に先手を打てるような新しいソリューションを発表しています。この取り組みの一環として、MobileIron Threat Defenseは、高度なオンデバイスモバイルセキュリティ導入の5段階をサポートします。当社のソリューションは、1つの総合的なアプリで複数の大きな利点を提供します。

- EMMと完全に統合した1つの脅威防御アプリ
- オンデバイスセキュリティの有効化や更新にユーザーの操作不要
- 高度なモバイルセキュリティが、インターネット接続なしでもiOS/Androidデバイスの既知およびゼロデイ脅威をブロック
- 機械学習アルゴリズムがオンデバイスのDNA脅威を即座に検出/防御

この結果、実用的な情報を提供し、モバイル従業員全員をDNA脅威から即座に保護する手軽なオンデバイスセキュリティが実現します。既存のEMMの強力な基盤の上で現代のモバイルセキュリティ戦略を実行し、モバイル脅威に対する保護を強化することにもなります。企業は、モバイル従業員の生産性を維持し、革新力と競争力を確保するという最重要事項に集中できるのです。

完全に統合された当社のモバイル脅威検出/防御ソリューションの詳細は以下をご覧ください。
www.mobileiron.com/threatdefense

MobileIron

〒106-0041
東京都港区麻布台1-11-10
日総第22ビル3階
japan@mobileiron.com
www.mobileiron.com
Tel: +81.3.6426.5301
Fax: +81.3.6426.5302