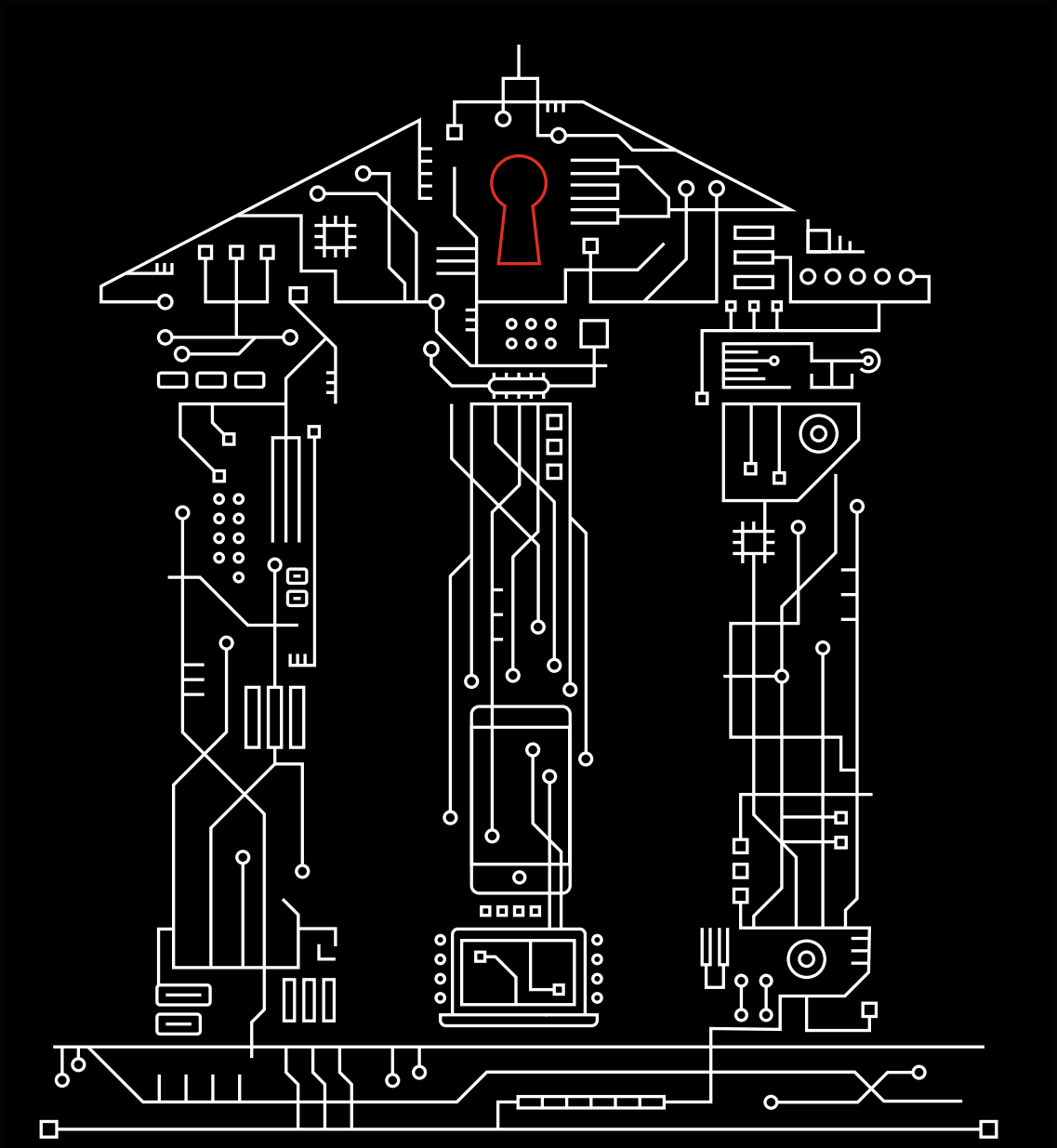
# Mobile Security Index 2020

## 金融サービス業界における モバイルセキュリティの現状

銀行、保険、クレジットカードなどの
金融サービス業界におけるモバイル
セキュリティの現状を詳細に分析



verizon

# モバイルデバイスがサイバー犯罪者につけ入る隙を与えていませんか

**金融サービス業界で成功するには顧客の信頼を築き、それを維持できるかどうかにかかっています。一方で、この業界の企業は性質上、サイバー犯罪者にとって実入りのいい標的の1つになっています。そのため、これらの企業ではモバイルセキュリティを強化する対策を早急に講じなければ、顧客を失ってしまう恐れがあります。**

**80%**

**モバイルデバイスはビジネスに不可欠であると、80%の金融サービス企業が回答しています。**

モバイルテクノロジーは、金融サービス企業がより良いカスタマーエクスペリエンスを実現し、革新的な新商品を提供するうえで欠かせません。そしてクラウドベースのサービスと組み合わせると、モバイルは強力な武器になります。大手の銀行や決済サービス企業、新興の金融テクノロジー企業など、この業界ではあらゆる規模の企業がモバイルテクノロジーの恩恵を受けています。

**ベライゾンは独立系調査会社に依頼し、モバイルデバイスの調達、管理、セキュリティを担当するシニアプロフェッショナルにアンケート調査を実施しました。合計876人の回答者のうち、金融サービス業界の回答者は12%を占めています。特に断りのない限り、本レポートのデータは、このアンケート調査によるものです。**

verizon

## 約半数の企業が侵害を受けている

金融サービス企業の約半数（47%）が、昨年モバイルデバイスに関係した侵害を受けたと認めています。これは前回のレポートの42%を上回る数字です。事業を継続していくためにはブランドイメージの維持が欠かせないことを理解していながら、これらの企業では十分なセキュリティ対策が実施されていません。

顧客が財産や資金、資産、機密データ、認証情報の管理を金融サービス事業者に任せているのは、これら事業者が十分に信頼できると顧客が考えているためです。しかしそこには、金銭目当てのハッカーが集まってきます。この業界は、サイバー犯罪者にとって大きな利益を期待できる標的なのです。そして数字が示すように、多くのケースでは、サイバー犯罪者が攻撃に成功しているのです。

**データというまさに宝の山が、危険にさらされています。2019年には、ある大手の銀行持ち株会社が侵害に遭っています。ハッカーは構成に不備のあったWebアプリケーションファイアウォールを通じてこの企業の内部に侵入し、1億を超える利用者の口座番号や社会保障番号、クレジットカード情報を盗み出していました[1]。**

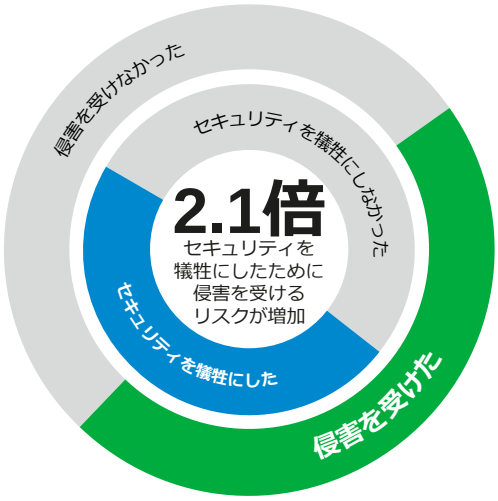
顧客ロイヤリティやブランドの価値がダメージを受ける恐れがあるにもかかわらず、48%の金融サービス企業が、「業務を遂行」するためにモバイルセキュリティを犠牲にしたと認めています。他の業界と同様に、その結果は明らかです。モバイルセキュリティを犠牲にしたと述べた金融サービス企業は、そうでない同業他社と比較して2.1倍、侵害を受けるリスクが高くなっています。

**87%**

**87%の金融サービス企業が、この業界は他の業界より利益の期待できる標的であるとサイバー犯罪者に見なされていると回答しています。**

**91%**

**91%の金融サービス企業が、自社のサイバーセキュリティが強固なものであると外部に示すことができれば、新たな顧客を獲得しやすくなると回答しています。**




**48%**

**48%の組織がセキュリティを犠牲にしたことがあると回答しています。**

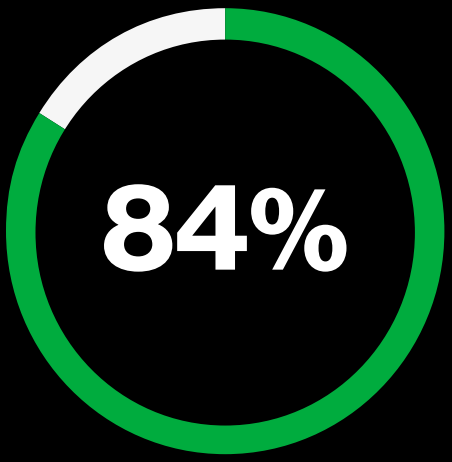
**47%**

**47%の組織がセキュリティ侵害を受けたと認めています。**

図1：モバイルデバイスやIoTデバイスに関連したセキュリティ侵害を昨年受けた割合。業務を遂行するためにIoTデバイスを含むモバイルデバイスのセキュリティを犠牲にした割合。

# モバイルが金融業界を変革

モバイルテクノロジーは金融サービス業界で重要な役割を果たしています。この点に異論をはさむ人はいないでしょう。モバイルテクノロジーにより、金融サービス企業はモバイル決済アプリやeウォレット、高度にカスタマイズされた保険証券などを通じ、カスタマーエクスペリエンスの変革を成し遂げています。顧客対応に必要なデータを大いに活用できるようになり、融資や利息、住宅ローンの金利などを容易に比較して顧客に提示できるようになりました。また、2要素認証を使用すれば、重要な情報を扱うサービスも安全に利用できます。




84%の金融サービス企業が、今後5年以内にモバイルがクラウドベースのサービスにアクセスするための主な手段になると回答しています。

## モバイルとクラウドのリスク

モバイルとクラウドがこれまでより密接に関係しあうようになっています。それどころか84%の企業が、今後5年以内にモバイルがクラウドベースのサービスにアクセスするための主な手段になると回答しています。アプリを開発、実行する場合、ほとんどのケースにおいて、まずはクラウドが選択されます。68%の企業が、新たに作成したビジネス情報の半分以上をクラウドに保管していると回答しています。

ほとんどの金融サービス企業が、自社の組織内で使用されているアプリの数を著しく少なめに計算しており、38%の組織がその数は100未満であろうと回答しています。1,000を超えるアプリを使用していると回答した組織はわずか8%にとどまりました。しかし実際のアプリの平均数は、もっと大きな数字になっています。

## ランサムウェアに対する懸念

金融サービス企業はモバイルデバイスによって生じる脅威に懸念を示しており、85%の回答者がそのビジネスリスクの高さを「中」から「高」と位置付けています。また「クリプトジャッキング」をはじめとする新たな脅威も含め、さまざまな脅威の存在が気がかりであると述べています。しかし、最も対策が遅れていると感じている脅威はランサムウェアであり、23%がそのように回答しています。ランサムウェアが確認されるようになったのはここ数年ですが、この攻撃は巧妙さを増し続けています。また、金融サービス企業は、アダルトコンテンツや違法なコンテンツへのアクセスなどの、従業員の行動に関係する脅威に対しても備えができていないと感じており、そのような回答が20%見られました。

金融サービス企業が懸念を示している、セキュリティ侵害がもたらす損害のリスクは多岐にわたり、知的財産の消失（57%）、ブランドイメージの失墜（56%）、罰金の支払い（53%）などがあります。しかし最大の懸念事項は、データの漏洩や窃取のリスク（60%）であり、特に顧客の個人情報や銀行の口座情報が心配であると回答しています。

## リスクはハッカーだけではない

金融サービス企業は、短期間で金銭を稼ごうとするサイバー犯罪者の標的になっていると認識しています。しかし、ハッカーに加えて「内部の脅威」も大きな懸念事項の1つになっています。79%の金融サービス企業が、モバイルデバイスに限って従業員が最大のリスクであると述べています。それにもかかわらず、ITのセキュリティに関する従業員向けのトレーニングを継続的に実施していると回答した金融サービス企業はわずか41%にとどまっています。

不注意によるものであっても、従業員の行動が企業を大きな危険にさらす恐れがあるのは間違いありません。許可されていないアプリのインストールや安全でない公衆Wi-Fiのホットスポットへの接続など、その行動の種類は様々です。しかし多くの企業がリスクを意識していながらセキュリティを犠牲にしており、モバイルのポリシーの設定担当者自らがルールを破っているのが現状です。このような状況で従業員に適正な行動を期待するのは筋違いであり、果たして適切なリスク管理と言えるでしょうか。

## 金融サービス企業のセキュリティ対策には改善の余地がある

大きなリスクが存在するにもかかわらず、金融サービス企業の多くは基本的な予防措置を講じていません。デフォルトのパスワードやベンダー提供のパスワードを全て変更していると回答したのは半数未満（49%）にとどまっています。データアクセスの権限を必要最小限に限定している組織はわずか46%に過ぎません。この2つは、定期的なセキュリティテストや公衆ネットワークで送信するデータの暗号化と同様、極めて基本的なセキュリティ対策に位置付けられるものです。この4つの基本的な予防措置をすべて実施している金融サービス企業の割合はわずか16%に過ぎません。

そしてクラウドの利用が増加しているにもかかわらず、金融サービス企業の多くはクラウドベースのアプリやサービスのセキュリティ対策を怠っており、セキュリティの強度を事前に検証することなくクラウドアプリを使用しないよう制限をしていると回答した組織は、半数未満（48%）にとどまっています。未知のネットワークやロケーションからアクセスがあったときにクラウドアプリの機能を制限していると回答したのは、わずか51%でした。このような基本的な予防措置を怠っていると、顧客や従業員、ビジネスデータがさらに大きなリスクにさらされる危険があります。

**1,300**

**Netskopeによれば、組織では平均約1,300のアプリとクラウドサービスを利用していますが、そのうちの95%が管理されていない状態にあり、IT部門はこれらのアプリやサービスに対する管理権限を持たず、その状態を把握すらしていません[2]。**

**95%**

**95%の金融サービス企業が、数分間サービスが停止しただけでも長期間にわたってブランドイメージに悪影響を及ぼす恐れがあると述べています。**

**79%**

**79%が公衆Wi-Fiを個人的に業務に利用していると回答しており、このうち32%の企業では、その業務利用がポリシーで明確に禁じられているにもかかわらず、公衆Wi-Fiが利用されていました。**

# 92%

**92%の金融サービス企業が、組織はモバイルデバイスのセキュリティをもっと真剣に考える必要があると述べています。**

# 20%

**NetMotionによれば、モバイルワーカーの20%がITのセキュリティポリシーの制約が業務上最も煩わしい問題であると回答しています。この「煩雑な認証手続き」が全体で5番目に煩わしい問題として挙がっています[3]。**

# 43%

**侵害に遭った金融サービス企業の43%が、過去1年でモバイルセキュリティの投資が大幅に増加したと回答しています。**

# 91%

**モバイル関連の侵害に遭った金融サービス企業の91%が大きな被害を受けたと回答しており、51%がその影響が長引いていると回答しています。**

## 金融サービス企業が最大の脅威と考えるモバイルセキュリティ上の問題

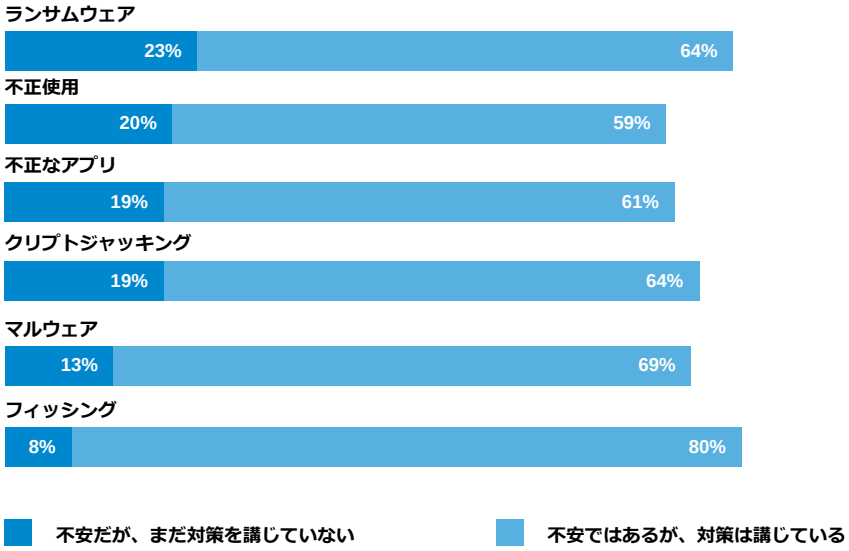



図2：脅威や脆弱性の問題をどう捉えているか

### なぜ対応を誤ってしまうのか

セキュリティを犠牲にしてしまう理由として、便宜性（69%）、収益目標達成の圧力（47%）、利便性（42%）の3つが上位に挙げられています。つまり、金融サービス企業のセキュリティ対策を妨げているのは、予算上の問題だけではないということです。意思決定者が、セキュリティ対策が効率に及ぼす影響を懸念していることも関係しているのです。

セキュリティポリシーの設計や導入に問題があると、従業員のエクスペリエンスや企業のパフォーマンスに悪影響を及ぼすことになります。パスワードポリシーのような単純なものでも、従業員の生産性の低下につながる恐れがあります。リセットする回数が増えれば、サポートのコストが増える可能性もあります。従業員がルールの抜け道を利用するようになるとリスクが増大する可能性も生じます。

### セキュリティが負荷になってはならない

一方で、セキュリティソリューションを適切に導入すれば、ソリューションの存在をほとんどユーザーに意識させることなくリスクを大幅に抑制できます。例えば、セキュアなモバイルゲートウェイや適応型の認証、ゼロトラストサービスを導入している環境では、不正ログインの試行件数が減少しており、システムやデータが大きなリスクにさらされなくなっています。

また、効果の高いツールを使用すれば、ITチームの負荷が軽減され、レポートの質が向上するほか、可視性も高まります。

# 脅威は増加しているのか

ワイヤレス接続するデバイスの数や種類が大幅に増加しており、スマートIoTデバイスが金融業界や保険業界のビジネスに変革をもたらしています。そして86%が、IoTデバイスはデジタルトランスフォーメーションに不可欠であると回答しています。

金融サービス企業では、IoTデバイスを設備の状態や生産性の監視（82%）、建物の物理的なセキュリティの監視（68%）、人や車両、他の資産の位置の監視（61%）に利用しており、例えば、IoT対応の監視システムはATMやCD、銀行の支店のセキュリティの維持に貢献しています。また、家庭や車両に設置されたIoTセンサーにより、保険の外交員は保険の手続きを正確に処理できるようになり、高度にカスタマイズされた保険証券の提供を可能にしています。

IoTによって生じるセキュリティのリスクの調査では、これらデバイスの調達や管理、セキュリティ担当者のグループに対してもインタビューを実施しましたが、回答者の75%がIoTデバイスを標的にした攻撃のリスクにさらされていると回答しており、リスクの高さを「中」から「高」と位置付けています。そして29%が、すでにIoTデバイスに関連する侵害を受けていると回答しています。

このようにIoTデバイスのセキュリティリスクが認識されているにもかかわらず、54%の回答者が「業務を遂行」するためにそのデバイスのセキュリティを犠牲にしたと回答しています。なぜそうなってしまうのでしょうか。原因としては便宜的な理由が挙げられます。53%は、その決定の背後には時間的なプレッシャーがあると言います。多くの場合、市場にいち早く商品を投入しようとするあまり、セキュリティを二の次にしてしまうのです。そして27%が、IoTデバイスのセキュリティを最優先として考えるべきものではなく「後回し」にできると回答しています。

# IoTデバイスを安全に利用する

IoTのセキュリティを強化する方法は数多くあります。すべてのモバイルデバイスを対象に弊社のアドバイスに従って対処を行い、以下に示すIoT固有の4つのベストプラクティスを実行すれば、セキュリティを確保できます。

**1. ソリューションやコンポーネントを購入する前に、そのセキュリティをチェックする**
市販のソリューションを購入する場合であれ、既成のコンポーネントを調達して独自のIoTデバイスを構築する場合であれ、ソリューションやコンポーネントの提供元のベンダーにセキュリティ対策の詳細を確認し、セキュリティの強度をチェックします。認証や暗号化の機能、パッチのポリシーについては特に重点的に確認します。76%が、IoTデバイスをリモートで使用している、またはアクセスが難しい場所に設置していると回答していますが、そのような場合は、無線通信（OTA）でアップデートをすれば、デバイスをセキュアな状態に維持できます。

**2. ネットワークに接続するデバイスのセキュリティを事前に強化する**
まずはデバイス自体に改ざん防止機能や改善検出機能があることを確認します。次に、デフォルトのパスワードやベンダー提供のパスワードをすべて変更します。また、必要のない機能などは無効にして、極力ハッカーに隙を見せないようにします。使用していないポートやプロトコルがあればブロックします。

**3. 移動時も保存時もデータを暗号化する**
83%の回答者が個人情報（PII）を収集していると回答していますが、このうちの25%がそのデータを暗号化していませんでした。データを暗号化すれば、ハッカーはそのデータを悪用できなくなるため、ブランドイメージの失墜につながるデータ侵害のリスクを抑えることができます。

**4. IoTプラットフォームを使用する**
すべてのデバイスを簡単に監視および管理できるIoTプラットフォームを選択します。このプラットフォームでは、デジタル証明書などのセキュリティ機能を実装して、脆弱性を減らすことができます。また、IoTプラットフォームはSIMをデバイスにバインドするため、SIMが盗難にあった際の被害を抑えてサイバー攻撃の影響を緩和できます。

# 72%

**72%が、IoTデバイスは組織にとっての最大のセキュリティリスク要因であると回答しています。**

# 64%

**64%が、IoTデバイスに関連したリスクが過去1年で増加したと考えていると回答しています。**

# 43%

**IoT デバイスを使用している 43% が、 全社的に展開している IoT デバイスが少なくとも 1 種類はあると回答しています。**

verizon

## 攻撃を受ける前に行動しなければならない

侵害に遭った金融サービス企業の43%が、過去1年でモバイルセキュリティの投資が大幅に増加したと回答しており、また、侵害を受けた57%の組織が、今後1年でモバイルセキュリティの投資を大幅に増やすと回答しています。一方、侵害に遭っていない組織の場合、同じ回答をした組織の割合はそれぞれ、わずか28%と20%になっています。

モバイルのセキュリティの問題を是正しようとする動きが企業に見られるのは良い傾向です。しかし、自身が被害を受けるまでは行動を起こさない企業があまりに多い点は気がかりです。

このような状況では、モバイルに関連したセキュリティ侵害が発生した場合、その影響は深刻なものとなり、影響が長引くことになります。そして金融サービス業界の企業は特に大きな影響を受けることが少なくありません。侵害に遭った組織の91%が大きな被害を受けたと回答しており、この割合は調査対象の他のどの業種よりも大きな数字となっています。さらに40%の組織が、問題への対応は困難で多額のコストを要したと回答しています。

侵害を受けたことに気付いてからモバイルのセキュリティを見直すのではなく、今こそ行動を起こさねばなりません。

# 次のステップ


**MSI 2020のメインレポート**
完全版のMobile Security Index 2020レポートには、モバイルデバイスが直面している脅威についてのさらに詳細な統計情報と分析が記載されています。FBIの主任捜査官やベライゾンの最高情報セキュリティ責任者（CISO）をはじめとするセキュリティエキスパートへのインタビューも掲載しています。


**MSI 2020のセキュリティ評価ツール**
ベライゾンのモバイルセキュリティ評価ツールでは、MSI 2020レポートのデータとお客様のセキュリティの状況を理解、リスクの認知、リスクの度合い、備えの4分野で比較して、カスタムレポートを作成できます。レポートにはお客様のセキュリティを強化するための指針が記載されます。


**MSI 2020の利用規定ガイド**
このインタラクティブガイドでは、強固なAUPを構成する要素についてご説明するとともに、お客様がご自身でAUPの作成と改善をし、マルウェアやフィッシングなどのリスクを軽減をするためのヒントをご紹介しています。

# アドバイス

### ユーザー

- 正式なAUPを定め、個人所有デバイスの業務利用に関する責任や使用できるネットワーク、ユーザーがインストールできるアプリを規定
- セキュリティファーストの視点に重点を置き、すべての従業員に定期的なトレーニングを施し、疑わしい事象を報告するための手順を周知
- パスワードの強度や再利用、2要素認証について規定したパスワードのポリシーを定めて周知

### アプリ

- データアクセスの権限を必要最小限に限定
- 従業員がインストールできるアプリを出所の明確なソースから入手したアプリのみに制限し、インターネットからダウンロードしたアプリはブロック
- すべてのパッチを迅速にインストール

### デバイス

- ベンダーから提供されたデフォルトのパスワードをすべて変更し、同じパスワードを再利用しない
- 脆弱性のあるデバイスやマルウェアに感染したデバイス、紛失したデバイスや盗まれたデバイスを対象としてデバイスのロックダウンや隔離を行うよう、各種のポリシーを導入
- モバイルデバイス管理（MDM）ソリューションにより、パッチの管理を簡素化し、認証ポリシーなどのAUPを適用
- モバイル上の脅威を検知するソフトウェアを導入し、デバイスを定期的にスキャンして脆弱性の有無を確認

### ネットワーク

- セキュアでないネットワークを介して送信するデータはすべて暗号化
- 公衆Wi-Fiの危険性をユーザーに周知し、未知のWi-Fiネットワークや安全でないWi-Fiネットワークの使用をブロック
- ゼロトラストアプローチの採用を検討

### クラウドサービス

- 特にファイル共有アプリなどで、出所の怪しいクラウドアプリの使用を制限
- 信頼できるネットワークやVPNを使用しているデバイスのみにクラウドサービスへのアクセスを許可

**詳細は、enterprise.verizon.com/msiをご覧ください。**

# Verizon Mobile Security Index について

本年の報告が第3版となるMobile Security Indexは、モバイルのセキュリティに関する主要な情報ソースの1つとなっています。本年のMSIでは、独立の調査機関に委託し、組織においてモバイルデバイスとIoTデバイスの調達、管理、セキュリティを担当している876人のプロフェッショナルに調査を実施しました。このレポートでは、Asavie、IBM、Lookout、MobileIron、NetMotion、Netskope、Symantec、VMware、Wanderaといったモバイルデバイスのセキュリティ分野を牽引する企業の協力も得ながら、さらに詳しい調査を実施しており、これらの企業からはインシデントやデバイスの利用状況に関する追加情報をご提供いただきました。さらに今回は、FBIと米国のシークレットサービスからも協力を得られました。モバイルデバイスを脅かす脅威の全容とその対策を明らかにするうえで、皆様には多大なご尽力をいただきました。厚く御礼申し上げます。

verizon

1 CNN、「A hacker gained access to 100 million Capital One credit card applications and accounts」、2019年、7月30日
2 Netskope、『Netskope Cloud Report』（https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019）、2019年8月
3 NetMotion、「The Mobile Frustration Index」（北米の様々な年齢層と各種のデバイスを対象として285人に調査を実施）（https://www.netmotionsoftware.com/blog/connectivity/mobile-frustration-index）、2019年9月