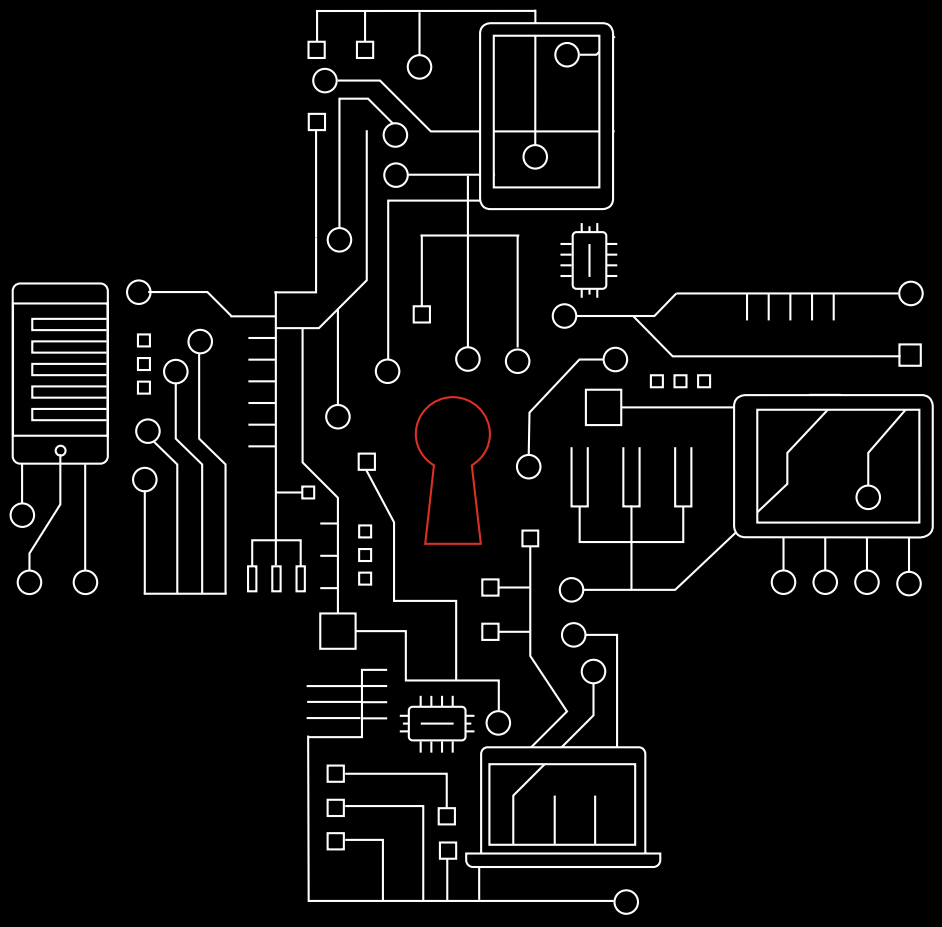
Mobile Security Index 2020

ヘルスケア業界における モバイルセキュリティの現状

医療センター、病院、救命サービス、看護施設、地域医療施設におけるモバイルセキュリティの現状を詳細に分析



verizon

モバイルデバイスのセキュリティは万全ですか

ヘルスケア業界はモバイルテクノロジーから大きな恩恵を受けています。同時に患者に関する膨大な量の個人情報を保有していることから、サイバー犯罪者にとっては実入りのいい標的の1つになっています。モバイルセキュリティを強化するための適切な措置を怠れば、これらのデータや重要なシステムがリスクにさらされる恐れがあります。

ヘルスケア業界では、モバイルが救命ツールとしての役割を担っています。モバイルの利用により、医療スタッフは即座に医療データを共有、利用できています。また、外来患者のモニタリングの質を高められるため、効果的なフォローアップのケアが実現し、患者の再診率を抑えることができています。さらにはデータに基づく適切な判断が可能なため、診断や治療の精度が向上しています。そしてクラウドベースのサービスと組み合わせれば、モバイルはさらに強力なツールになります。88%の組織が、クラウドに保存しているデータへの依存度が高くなっていると回答しています。

88%

88%の組織が、クラウドに保存しているデータへの依存度が高くなっていると回答しています。

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、9%が病院、医療センター、救命サービス、看護施設、地域医療施設で業務に従事するヘルスケア業界の回答者となっています。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

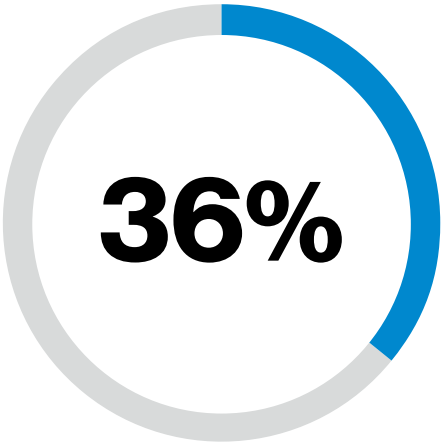
約40%の組織が侵害を受けている

ヘルスケア業界では、約5分の2の組織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おり、前回のレポートの25%と比較すると大きな増加となっています。

ヘルスケア業界には、数多くのセキュリティリスクが存在します。ヘルスケア業界の組織は患者やスタッフに関する極めて機密性の高い情報を保有しています。サイバー犯罪者はこれらの情報を狙っており、情報を盗み出してブラックマーケットで販売したり、脅迫や恐喝に利用したりしようとしています。

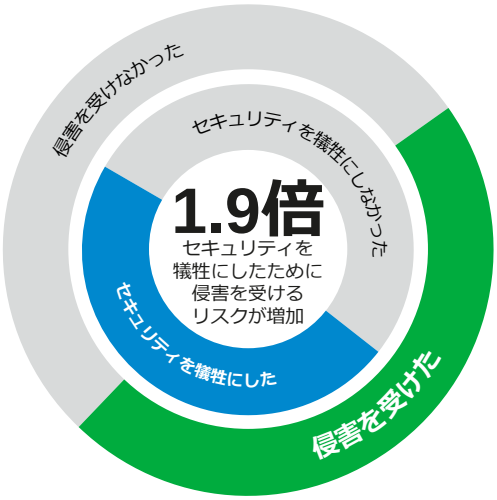
2017年には英国のNational Health Service（NHS）がランサムウェア攻撃を受け、その結果英国全土の病院に混乱が生じ、数千に上る診察の予約や手術をキャンセルしたり、別の病院で対応したりしなければならなくなりました[1]。そしてセキュリティ侵害の影響は、長期間にわたり続く可能性があります。2019年には米国のある医療費回収代行業者が大規模なデータ侵害を受け、クリニックや診断ラボなどの20を超える医療機関に支障が生じ、最終的には約2,500万人が影響を受けました[2]。

患者やスタッフが被害を受ける恐れがあるにもかかわらず、37%の組織が「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組織は、そうでない組織と比較して1.9倍、侵害を受けるリスクが高くなっています。



モバイル関連の侵害に遭った組織の36%が大きな被害を受けたと回答しています。

クラウドのリスク



37%

37%の組織がセキュリティを犠牲にしたと回答しています。

38%

38%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。

71%

ヘルスケア業界の71%の組織が、新たな法規制に照らしてモバイルデバイス関連のリスクを再評価しています。

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[3]。

ヘルスケア業界が最大の脅威と考えるモバイルセキュリティ上の問題

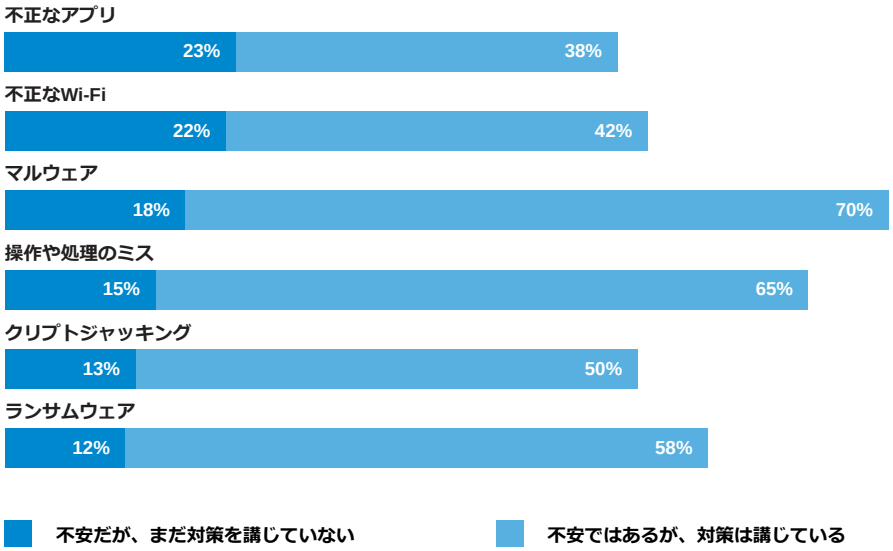


図2：脅威や脆弱性の問題をどう捉えているか

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85%の組織が、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。44%の組織が、新たに作成した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。

ヘルスケア業界のほとんどの回答者が、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、65%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4%でした。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。

既知の脅威

ヘルスケア業界はモバイルデバイスを狙う脅威に不安を抱いており、73%の回答者がそのリスクの高さを「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、様々な脅威の存在が気がかりであると回答しています。しかし、ほとんどのヘルスケア業界の組織が、対応の準備ができていないと感じている脅威は、既知の脅威であり、具体的には未承認のアプリケーションの利用による脅威（23%）、不正なWi-Fiホットスポットや安全でないWi-Fiホットスポットの利用による脅威（22%）、マルウェア（18%）などが挙げられます。

ヘルスケア業界が懸念している、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、信用の失墜（50%）、法規制の罰則（32%）などがあります。しかし最大の懸念事項はデータの流出（62%）であり、特に医療記録の窃取や漏洩が心配であると回答しています。しかし、患者情報だけがリスクにさらされているわけではありません。51%がスタッフの個人情報の漏洩を懸念しています。ヘルスケア業界のスタッフは税金など、高度に標的を絞ったフィッシング詐欺の主な標的になっています。

悪意のない脅威

医療記録は、サイバー犯罪者にとって常に実入りのいい標的となるでしょう。一方でこの業界では、「内部の脅威」も依然として大きな懸念事項の1つになっています。ヘルスケア業界の75%の組織が、モバイルデバイスに限ってスタッフが最大のリスクであると回答しています。それにもかかわらず、ITのセキュリティに関するスタッフ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組織はわずか52%にとどまっています。

不注意によるものであっても、スタッフの行動が組織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、その行動の種類はさまざまです。しかし多くの組織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。このような状況でスタッフ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。

ヘルスケア業界のセキュリティ対策には改善の余地がある

あらゆるところにリスクが存在しているにもかかわらず、ヘルスケア業界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すべて変更している、あるいは公衆ネットワークで機密データを送信するときにデータを暗号化していると回答したのは半数未満（43%）にとどまっています。この2つは、定期的なセキュリティテストやデータアクセスの権限を必要最小限に限定する措置と同様、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組織の割合はわずか12%にすぎません。

そしてクラウドの利用が増加しているにもかかわらず、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、わずか35%でした。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アプリの機能を制限していると回答したのは49%でした。このような予防措置を怠っていると、データや患者、スタッフがリスクにさらされる危険があります。

なぜそうなってしまうのか

セキュリティを犠牲にしてしまう理由として、便宜性（64%）や利便性（46%）が上位に挙げられています。これは、セキュリティ対策が生産性や効率に及ぼす影響を意思決定者が懸念していることを示しています。データを利用して即座に判断を下す必要のある医療の現場では、当然のことと言えるでしょう。

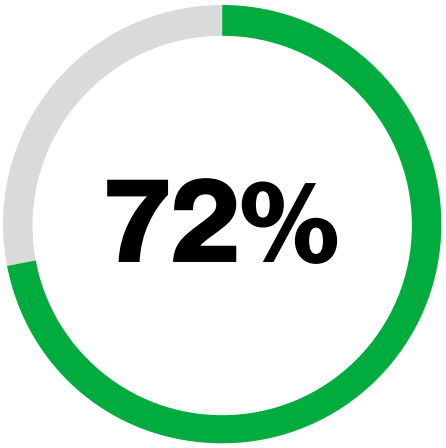
セキュリティポリシーの設計や導入に問題があると、スタッフや患者ともに悪影響を及ぼすことになります。パスワードポリシーのような単純なものでも、スタッフの生産性の低下につながる恐れがあります。リセットする回数が増えればサポートのコストが増える可能性もあります。スタッフがルールの抜け道を利用するようになるとリスクが増大する可能性も生じます。救急医療の現場では特にこれが顕著です。

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。

65%

65%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23%の組織では、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。



ヘルスケア業界の72%の組織が、スタッフが素早くデータにアクセスできるようにする必要があるために、効果的なセキュリティ対策を実施するのが難しくなってきていると回答しています。

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[4]。

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デバイスが医療サービスに変革をもたらしています。そして94%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。

カプセル剤のスマートパッキングなどのイノベーションにより、患者は用法を守って正しく薬を服用できるようになりました。また救急車に取り付けられたセンサーにより、救命隊員は患者を搬送中に患者の診断データを病院に送ることができます。ヘルスケア業界では、IoTを機器や作業効率の監視（77%）、建物の物理的なセキュリティの監視（71%）、患者の容体の監視（59%）に利用しています。

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77%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35%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、35%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。その要因の1つとして、回答者全員が時間的なプレッシャーを挙げています。多くの場合、イノベーションを急ぐあまり、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。

44%

IoTを組み込んだ製品を開発している企業の44%が、デジタル証明書を使用してセキュリティを強化しています。

71%

71%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。

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。全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ざん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。

93%

93%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回答しています。

攻撃を受ける前に行動しなければならない

93%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回答しています。そして77%が、モバイルデバイスを標的にする脅威が他のデバイスよりも速く迫ってきていると回答しています。

セキュリティ侵害に遭ったヘルスケア業界の組織の30%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が、そうでない組織では、この割合はわずか16%にとどまりました。

問題を認識している組織がこの業界に見られるのは良い傾向ですが、より具体的な行動を起こしていない点は気がかりです。

このような状況でモバイルに関連したセキュリティインシデントが発生すると、多くの場合、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。侵害を受けた組織のうち、約半数（48%）が攻撃によりサービスが停止しており、39%がデータの消失や漏洩に対処しなければならなくなっています。修復の作業には長い時間を要し、作業は困難でコストもかかります。

侵害を受けたことに気付いてからモバイル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 BBC、「NHS ‘could have prevented’ WannaCry ransomware attack」、2017年10月27日
2 HIPAA Journal、『AMCA Data Breach Total Nears 25M as Wisconsin Diagnostic Laboratories Confirms 115K Record Breach』、2019年8月28日
3 Netskope、『Netskope Cloud Report』（https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019）、2019年8月
4 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