2020 年 10 月 15 日
モバイルアイアン・ジャパン

米英など 8 か国を対象に調査
労働者の 80%以上が「フルタイムでオフィスに戻りたくない」ことが判明。
～人々は近い将来、どこでも仕事ができるようになる～

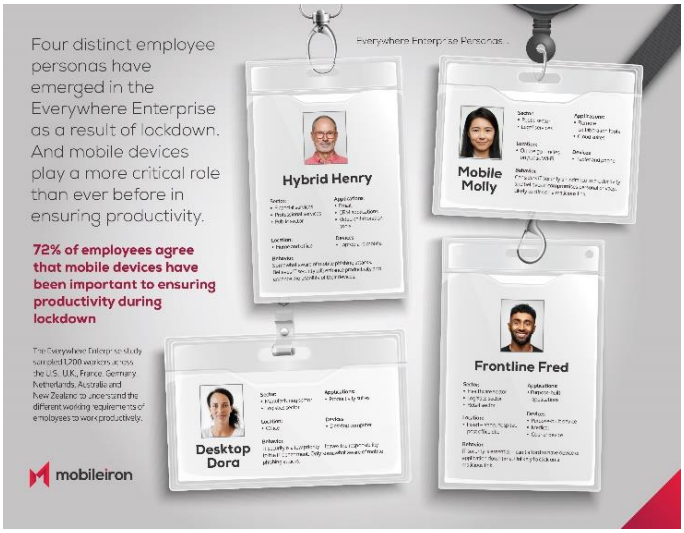
モバイルを中心とした分散型企業向けのセキュリティプラットフォームを提供する MobileIron（本社：カリフォルニア州マウンテンビュー、代表者：サイモン・ビディスコーム）は、2020 年 10 月 6 日に新型コロナウイルス感染症が働き方にどのような影響を与えているかという調査結果を発表しました。その結果、3 人に 1 人（30%）の労働者が、新型コロナウイルス感染症によるロックダウン中に、チームから孤立していることが生産性の最大の妨げになっていると主張しているにもかかわらず、80%以上の労働者がフルタイムでオフィスに戻ることを望んでいないことが明らかになりました。
※米国、英国、フランス、ドイツ、ベルギー、オランダ、オーストラリア、ニュージーランドの 1,200 人の労働者を対象に調査を実施。

新型コロナウイルス感染症の大流行は、人々の働き方を明らかに変え、すでに拡大しているリモートワークの傾向を加速させました。また、労働者が個人のデバイスを使用して企業のデータやサービスにアクセスする機会が増えているため、IT 部門に新たなセキュリティ上の課題が生じています。従業員、IT インフラ、顧客がどこにでも存在するという新しい「エブリウェア・エンタープライズ」がもたらす課題に加えて、労働者がセキュリティを優先していないという事実があります。この調査では、労働者の 3 分の 1（33%）が IT セキュリティを優先度の低いものと考えていることがわかりました。

現在の分散型リモートワーク環境では、悪質なサイバー犯罪者がフィッシング攻撃でモバイルデバイスを標的にするケースが増えており、新たな脅威が発生しています。これらの攻撃は基本的なものから巧妙なものまで様々で、成功する可能性が高く、多くの労働者はフィッシング攻撃の見分け方や回避方法を知りません。調査によると、全世界の労働者の 43%がフィッシング攻撃とは何かを理解していないことが明らかになりました。

MobileIron 製品管理担当シニアバイスプレジデントのブライアン・フォスターは、「モバイルデバイスはどこにでもあり、実質的にあらゆるものにアクセスできるようになっていますが、ほとんどの労働者はモバイルセキュリティ対策が不十分で、ハッカーにとって絶好な攻撃チャンスとなっています。ハッカーは、セキュリティが緩いモバイルデバイスを使って企業データにアクセスする機会が増えていることを理解しており、フィッシング攻撃で標的にするケースが増えています。すべての企業はユーザー体験を優先し、労働者が個人のプライバシーを損なうことなく、どこにいても、あらゆるデバイスで最大限の生産性を維持できるような、モバイル中心のセキュリティ戦略を導入する必要があります。」と述べています。

この調査では、ロックダウンの結果、働く場所にとらわれない「エブリウェア・エンタープライズ」では 4 つの異なる労働者のタイプが出現し、生産性を確保する上でモバイルデバイスがこれまで以上に重要な役割を果たしていることが明らかになりました。



人物タイプ①ハイブリッドユーザー（Hybrid Henry）

一般的には金融サービス、専門サービス、または公共部門で働いており在宅勤務を好むが、チームメイトから孤立していることが生産性の最大の妨げになっている。生産性を維持するためには、ノートパソコンとモバイルデバイスに加え、E メール、CRM アプリケーション、ビデオコラボレーションツールへの安全なアクセスに依存している。IT セキュリティが生産性を確保し、デバイスの使いやすさを向上させると信じている一方で、この労働者は、フィッシング攻撃についてはある程度しか認識していない。

人物タイプ②モバイルユーザー（Mobile Molly）

タブレットや電話など様々なモバイルデバイスを使用して常に外出先で仕事をしており、公共の Wi-Fi ネットワークを利用することも多い。仕事を遂行するために、リモートワークを支援するツールやクラウド環境に頼っている。常に外出しておりモバイルデバイスに大きく依存しているため、信頼性の低いテクノロジーが生産性の最大の妨げになっていると考え、IT セキュリティが個人のプライバシーを侵害すると考えている。

人物タイプ③デスクトップユーザー（Desktop Dora）

チームメイトから離れていたり、自宅で仕事をしていることが生産性の妨げになり、オフィスに戻るのが待ち遠しい。モバイルデバイスよりも、固定された場所でデスクトップコンピュータを使って仕事をしたいと考えている。オフィス内外の同僚とのコミュニケーションのために、オフィスソフトに大きく依存している。IT セキュリティを優先度の低いものと考え、IT 部門に任せている。この労働者は、フィッシング攻撃についてもある程度しか認識していない。

人物タイプ④現場ユーザー（Frontline Fred）

医療、物流、小売などの現場で活躍しており、病院や小売店などの固定された特定の場所で仕事をするため、リモートワークができない。医療機器や宅配便の機器やアプリケーションなど、専用の機器やアプリケーションに頼って仕事をしているが、他のペルソナほど個人のモバイル機器に依存して生産性を上げることはない。生産性を高めるためには IT セキュリティが不可欠であることを認識している。

またフォスターは、「これまで以上に多くの労働者がモバイルデバイスを活用することで、どこからでも仕事ができるようにし、生産性を維持しているため、企業は信頼できるデバイス、アプリ、ユーザーだけが企業のリソースにアクセスできるようにすべく、ゼロトラスト・セキュリティのアプローチを採用する必要があります。サイバー犯罪者は、テキストメッセージや SMS メッセージ、ソーシャルメディア、フィッシング攻撃によってリンク共有を可能にするメッセージングアプリなどを標的にするケースが増えており、企業はモバイル脅威に対する防御力を強化する必要があります。企業データへの不正アクセスを防ぐためには、企業の電子メールだけにとどまらない総合的かつシームレスなフィッシング対策技術を提供し、ユーザーがどこで何のデバイスを使ってそのリソースにアクセスしても安全を確保できる必要があります。」と述べています。

◆モバイルアイアンについて

MobileIron は業界初のモバイルを中心とした分散型企業向けのセキュリティプラットフォームで企業セキュリティを再定義します。どこでも働くことのできる環境を持つ分散型企業では、企業データが複数のデバイスやクラウド内のサーバー間を自由に流れ、従業員はどこでも必要な場所で生産的に働くことができます。境界のない企業全体でアクセスのセキュリティを確保し、データを保護するため、MobileIron はゼロトラスト・アプローチ、すなわち攻撃者がすでにネットワーク内に存在することを想定し、「すべてを疑い、常に確認」という姿勢でアクセスのセキュリティを判断しています。

MobileIron のプラットフォームは、数々の受賞歴を誇る最先端の統合エンドポイント管理（UEM）機能に、パスワードレスの多要素認証（MFA）であるゼロ・サインオンとモバイル脅威防御（MTD）を組み合わせることで、デバイスの検証、ユーザー環境の検出、ネットワークの検証、脅威の検出と修復を実行し、許可されたユーザー、デバイス、アプリ、サービスのみがビジネス資産にアクセスできる、「どこでも働ける」環境を提供しています。世界大手の金融機関及び情報機関、また規制の厳しい企業など、20,000 社以上のお客さまが MobileIron を活用し、どこでも働くことのできるシームレスかつセキュアなユーザー体験を実現しています。

※MobileIron は、2020 年 9 月 28 日（米国時間）に Ivanti 社による買収に合意したことを発表しました。詳細は下記 URL をご参照ください。
https://www.mobileiron.com/ja/company/press-room/press-releases/mobileiron-research-reveals-the-future-of-work-is-everywhere-ja