ivanti

2021年
消費者セキュリティ
サイバーレポート

リモートワーカーによって
サイバー攻撃の
危機にさらされる企業

高リスクな消費者の振る舞いでサイバーセキュリティのギャップが拡大

2020年のパンデミックは、恐ろしい破壊的なウイルスを世界に広げただけでなく、日々の生活のあらゆる面で根本的な障壁となりました。働き方や働く場所も大きく影響を受けました。
あらゆる業種のあらゆる職種の従事者が、可能な限り在宅勤務をするようになりました。
リモートワーカーは重要なビジネス運用の継続に役立ちましたが、多くの企業は安全でない個人所有デバイスと従業員の高リスクな振る舞いの増加によってサイバー脅威の急増にさらされています。
パンデミックが始まって1年以上経過した今、脅威はどのような状況になっているでしょうか？

2021年の2月にIvantiは「2021年消費者セキュリティサイバーレポート」を発表し、ビジネスリスクとなる脅威について紹介しました。 このレポートは、2020年11月に実施した、米国と英国の18歳以上の労働者、2,000名以上を対象にした調査に基づいています。

企業は管理されていない従業員の私用デバイスやアプリが起こすセキュリティ問題を理解していますが、このレポートによると、従業員は会社支給のコンピューターを在宅勤務で使っている場合も、高リスクな振る舞いをしています。例えば、消費者の4人に1人が業務用のメールやパスワードを、食品のデリバリやオンラインショッピング、デートアプリなど、消費者用のウェブサイトやアプリのアクセスに使ったと回答しています。

企業セキュリティの複雑化
コロナ禍前の「ノーマル」な世界が戻ってきても、大規模なリモートワークは継続すると見られています。企業はリモートワーカーのセキュリティギャップを埋めるべく努力をしてきていますが、会社支給のハードウェアとソフトウェアを提供するだけでは不十分であることは明白です。このレポートを読むことで、企業はこの先の課題についてより良く知ることができます。

消費者の4人に1人

消費者の4人に1人が業務用のメールやパスワードを、食品のデリバリやオンラインショッピング、デートアプリなど、消費者用のウェブサイトやアプリのアクセスに使ったと回答。

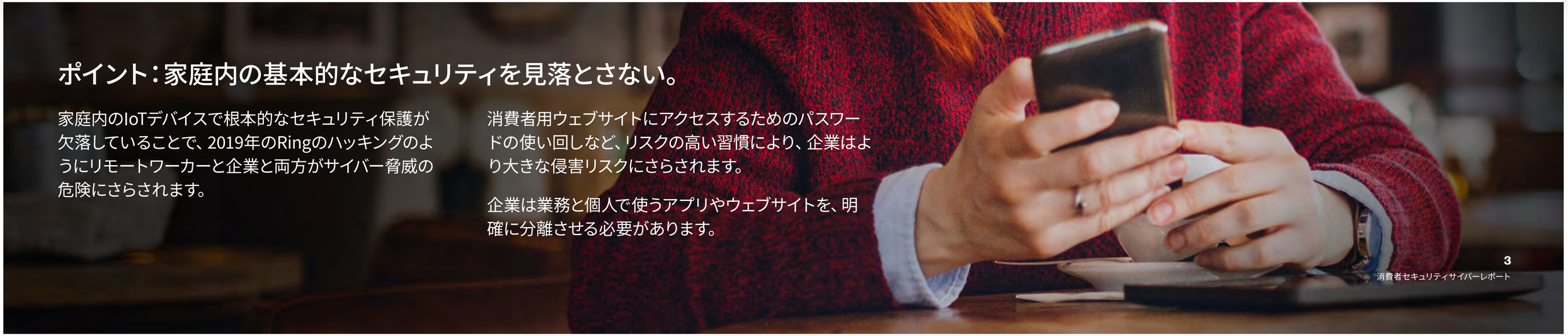
リモートワーカーのセキュリティ意識が企業のリスク要因に

平均的な在宅勤務環境のセキュリティレベルを理解するために、この調査では家庭のIoTデバイスを含むすべてのデバイスの使い方やセキュリティ意識について質問しました。

IDパスワードの使い回し
米国では25%、英国では20%が業務用メールや業務用のパスワードを消費者用のウェブサイトやアプリへのログインに使ったと回答。

私用デバイスの業務利用
米国では半数近く、英国では3分の1以上が、ノートパソコン、スマートフォン、タブレット、スマートウォッチといった私用デバイスを会社のアプリやネットワークへのアクセスで使うことが許されていると回答。

IoTデバイスの二要素認証
米国と英国の半数近くが自宅のスマートデバイスで二要素認証を設定していないと回答。



ポイント：家庭内の基本的なセキュリティを見落とさない。

家庭内のIoTデバイスで根本的なセキュリティ保護が欠落していることで、2019年のRingのハッキングのようにリモートワーカーと企業と両方がサイバー脅威の危険にさらされます。

消費者用ウェブサイトにアクセスするためのパスワードの使い回しなど、リスクの高い習慣により、企業はより大きな侵害リスクにさらされます。

企業は業務と個人で使うアプリやウェブサイトを、明確に分離させる必要があります。

リモートワーカー保護するために企業セキュリティの改善も必要

パンデミックが始まってから、セキュアでない個人用デバイスや家庭のIoTデバイスへのサイバーセキュリティ攻撃が激増しています。

エンドユーザーの弱いセキュリティ対策も一因ですが、企業もいくつかの重要な局面でセキュリティを改善しなければならないことが、今回の調査で判明しました。

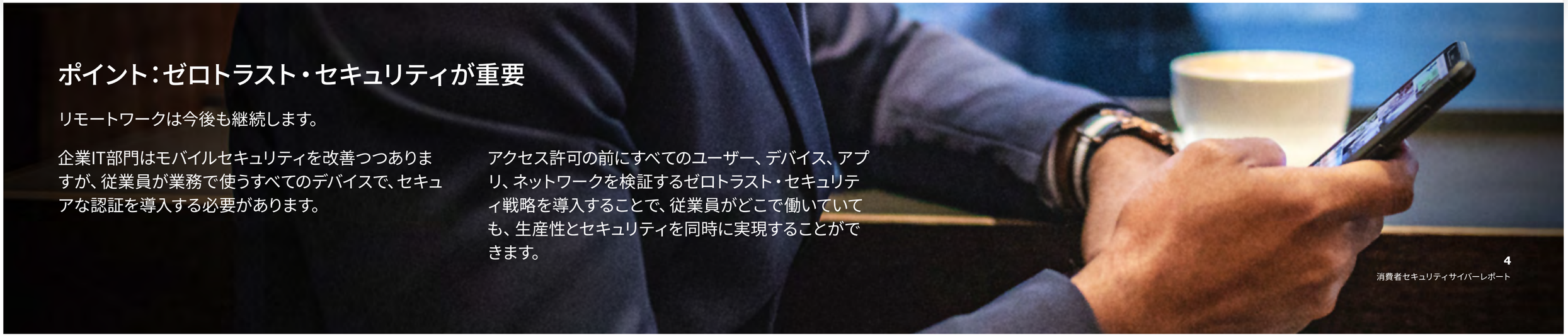
25%

セキュリティソフトウェア
25%以上が、リモートワーク中に特定のアプリにアクセスするためにセキュリティソフトウェアをインストールする必要はないと回答。

パスワード更新
米国と英国の約25%のリモートワーカーが、会社は6ヶ月ごとのパスワード更新やワンタイムパスワードの利用を義務付けていないと回答。

30%

安全なアクセスツール
米国と英国の回答者の30%近くが、VPNなどの安全なアクセスツールを使うことを会社はリモートワーカーに義務付けていないと回答。



ポイント：ゼロトラスト・セキュリティが重要

リモートワークは今後も継続します。

企業IT部門はモバイルセキュリティを改善つつありますが、従業員が業務で使うすべてのデバイスで、セキュアな認証を導入する必要があります。

アクセス許可の前にすべてのユーザー、デバイス、アプリ、ネットワークを検証するゼロトラスト・セキュリティ戦略を導入することで、従業員がどこで働いていても、生産性とセキュリティを同時に実現することができます。

セキュアな消費者が企業をセキュアに

これまでになく多くの従業員がリモートで働いている現在、サイバー脅威も急速に増加しています。企業には家庭でのIoTセキュリティと消費者のセキュリティ意識の欠如の中で、ビジネスアプリやデータを保護する戦略が必要です。消費者向けのデバイスが激増する中、高度なセキュリティ設定を導入、維持することはリモートワーカーには困難です。そして、サイバー犯罪者はそれを知っています。結果として、新型コロナウイルスのパンデミックは健康への大きな脅威となっただけでなく、セキュリティ対策のできていない企業やユーザーを利用するサイバー犯罪者が簡単に攻撃を仕掛けられる環境を作っています。

有効な対策：

今すぐゼロトラスト・セキュリティの導入を

リモートワーカー全体にゼロトラストを導入しましょう。
ゼロトラスト・モデルが導入されると、企業の情報、アプリ、ネットワークにアクセスするのが信頼されたデバイスやアプリであることを確認することで、企業はパスワード盗難などのリスクを回避することができます。

さらに、リモートワークが継続し、デバイスが増えるほどに、多要素認証の利用、デバイス保護、セキュアなネットワーク接続などのポリシーを適用することが、ゼロトラスト・セキュリティの導入でより簡単になります。

調査方法

消費者セキュリティサイバーレポートは2020年11月に実施された調査に基づいています。この調査は、パンデミックの間に消費者と企業のサイバーセキュリティがどのように変わったかを調べることを目的としています。米国と英国で会社支給のパソコンを使って在宅勤務をしている18歳以上の人、2000人を調査対象としました。

Ivantiについて

Ivantiの自動化プラットフォームは、すべてのIT接続をあらゆるデバイス、インフラ、ユーザーでよりスマートかつセキュアにします。Ivantiは、PCやモバイルデバイスから仮想デスクトップインフラストラクチャやデータセンターに至るまで、場所にとらわれないEverywhere Workplaceのクラウドからエッジまでで IT資産を検出、管理、防御し、パーソナライズされたユーザー体験を従業員に提供します。場所にとらわれないEverywhere Workplaceでは、企業データはデバイスやサーバー間を自由に流れ、どこでどのように仕事をしていても、従業員の生産性を高めます。Ivantiは、米国ユタ州のソルトレイクシティに本社を置き、各国にオフィスを有します。
詳細については、ivanti.co.jp ご確認ください。

ivanti

ivanti.co.jp
03-5226-5960
contact@ivanti.co.jp