TANIUM

世界がステイホームに移行したとき

グローバル ITリーダーの在宅勤務移行に伴い
サイバー攻撃が増加

エグゼクティブ・サマリー

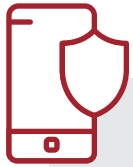
COVID-19は、これまでに経験したことのない未曾有の事態を引き起こしています。。経済危機と健康危機が一体となって発生したCOVID-19は、直接的な経済的影響だけでなく、事業運営の構造にも影響を与え、そして、多くの企業にとって広範囲な影響を及ぼしています。世界中で、雇用主は政府の命令に応じて、従業員に在宅勤務の厳格な命令を課し、前例のない規模で従業員を分散させました。ある推定によれば、パンデミックが収束した後も、5分の2もの従業員が在宅勤務を継続すると言われています。

ウイルスが出現する前から、IT責任者はすでにいくつかの課題について懸念していました。エンドポイントの可視性のギャップは非常に大きく、回答者のうち71%が、非管理のIT資産を毎週のように発見していると回答しています。ツールの氾濫、シャドーIT、サイロ化したITチーム、レガシー技術も主要な課題として挙げられています。大半(53%)のIT責任者は、このようなギャップが原因でサイバー攻撃にさらされる可能性があるだけでなく、ブランドにダメージを与え、コンプライアンス違反の罰金や顧客離れに悪影響を及ぼしたりすることを懸念していました。

危機がこのような課題をどの程度悪化させているのか、また、組織が次の事態に備えてどのような準備をしているのかを明らかにするために、タニウムは本グローバル調査を実施しました。

本レポートは、米国、英国、フランス、ドイツの1,004人のCXO(CEO、CIO、CTO)とVPへのインタビューをもとに編集されています。対象の組織はすべて、世界的なCOVID-19パンデミックの間に従業員を在宅勤務へと移行し、1000人以上の従業員を雇用しています。

調査結果から分かったこと



CXOとVPが、在宅勤務セキュリティの課題に直面：

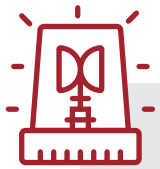
回答者の85%は、COVID-19パンデミック時に在宅勤務への迅速な移行を実施する際に準備ができていると感じていましたが[1]、その後98%がセキュリティ上の課題に直面したと回答しています。これは、2019年の同時期と比較すると、在宅勤務への移行のためにIT投資増額による恩恵を74%が受けていたにもかかわらずです。

問題解決先延ばしの組織の実態：

43%が組織をリスクにさらすことに繋がった個人用デバイスへのパッチ適用に苦労したと回答しており、93%が在宅勤務への移行に対応するために、他のセキュリティ優先事項を延期、またはキャンセルしていました。これら対策プロジェクトには、ID管理とアクセス管理（IAM）、そしてセキュリティ戦略の作業が含まれていました。

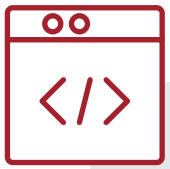
COVID-19で明らかになったエンタープライズ・セキュリティのギャップ：

90%が攻撃頻度の増加を報告しています。新しいデバイスの可視性、VPN要件によるIT容量の圧倒的な増大、ビデオ会議によるセキュリティリスクの増加がセキュリティ上の課題のトップ3でした。



これがニュー・ノーマルだ：

回答者の大半（85%）は、パンデミックの悪影響は数ヶ月に渡って組織におよぶと考えています。実際、回答者の大多数（70%）は、コンプライアンス規制（26%）、サイバーセキュリティリスクの管理（25%）、サイバーリスクと従業員のプライバシーのバランス（19%）などの複数の理由から、在宅ITの長期的な導入を成功させることは難しいと答えています。



可視化とコントロールが新しい現実における中心的な役割を担う：

回答者のほぼ半数（48%）が、社員の現場復帰に合わせて、IT資産の可視性を高めるエンドポイント管理への投資を計画しており、ほぼ同数（47%）がパッチ管理プロセスの改善を計画していると回答しています。

[1] 「準備万端」と「十分に準備されている」を合わせた回答

厳しい現実を認識

大半（85%）のCXOとVPは、リモートワークへの移行の準備ができていると考えていました。大多数（74%）は、2019年の同時期と比較すると、分散型ワークフォースに移行するためのIT投資増額による恩恵さえ受けていました。回答者の38%が51%以上の投資増を主張していました。しかし、多くはサイバーセキュリティへの影響を過小評価しており、98%がCOVID-19の影響で分散型ワークフォースモデルに移行する際にセキュリティ上の課題に直面したことを認めています。

パッチ適用は、組織が不意を突かれたと思われる重要な分野の一つです。回答者の88%がこの重要な分野で問題を抱えていました。実際、回答者の43%がリモートワーカーの個人デバイスへのパッチ適用に困難を感じており、組織がリスクに晒されています。また、45%の回答者は、スキャンやパッチをあてることはできても、何台のデバイスが修正され、パッチがあてられたかを追跡することはできなかったと回答しています。

問題先送りの結果

一部のケースでは、セキュリティへの影響が劇的であり、組織が将来的に深刻なリスクにさらされる可能性がありました。

4分の1のCXOとVP（26%）にとって、パンデミックが始まって以来、パッチ適用や脆弱性スキャンなどの脆弱性管理の優先順位が低くなっています。回答者は、この期間にVPNに過負荷がかかり、エンドポイントへの可視性が不足していたために、脆弱性管理の優先順位を下げていたのです。この決定は、マイクロソフトが史上最大規模のパッチ・チューズデー・アップデートを含む、最も重いパッチ・チューズデー・アップデートを数ヶ月にわたって実施していた時期と重なりました。この間、サイバー犯罪者がVPNやその他のリモート作業ツールの脆弱性を探っていることを警告する複数の報告がありました。

回答者の93%が、リモートワークへの移行に対応するために、セキュリティの優先事項をキャンセルするか、延期しなければならなかったと答えています。IDとアクセス管理（39%）とセキュリティ戦略業務（40%）は、遅延やキャンセルの影響を受けていると回答した人が最も多くいました。

COVID-19で明らかになった
エンタープライズ・セキュリティのギャップ

同時に、日和見主義的（ご都合主義的・気ままな）なサイバー犯罪者や、セキュリティ態勢のギャップを探し求めている国家からのサイバー攻撃が大幅に急増しています。90%の企業が、パンデミックの影響で攻撃の頻度が増加したと回答しており[2]、通常より30%も脅威が増加したと報告しています。その中で最も多かったのは、データ漏洩を伴う攻撃（38%）、次いでビジネスメールの漏洩（侵害）やトランザクション詐欺（37%）、フィッシング攻撃（35%）でした。

CXOやVPにとって、分散型人材（分散型労働力/ワークフォース/在宅勤務）に移行する際のセキュリティ上の課題のトップ3（上位3つ）は、以下の通りです。

- **ネットワーク内の新しいパーソナル・コンピューティング・デバイスの特定**（27%）：可視性ギャップに関する問題が根強く存在することが確認されました。回答者の45%が、現場でのリスクを軽減するために、社内ネットワーク上での個人用デバイスの使用を禁止することで、組織を通常の状態に戻し、オンサイトでのリスクを軽減すると回答しています。
- **VPN要件によるIT容量の超過**（22%）：VPNに問題があると、パッチ適用に問題が生じ、ITチームは企業のセキュリティ管理を通じた従業員のトラフィックのルーティングを断念せざるを得なくなる可能性があります。
- **ビデオ会議によるセキュリティリスクの増大**（20%）：急遽導入したツールは、企業での使用には適さない場合があります。パンデミック・セキュリティ問題の真っただ中で、ポピュラーなプラットフォームにおいて、2つの重大な欠陥が発見されました。

現在、CXOやVPは、在宅勤務とそれに伴うデジタルトランスフォーメーションに対応する上での最大の課題として、予算や取締役会からのサポート、人材や専門知識よりも、セキュリティへの懸念（問題）を挙げています。近い将来、長期的にはほとんどのオフィスワーク（での業務）がリモートで行われると仮定した場合、管理されないままにしておくと、組織にとって大きな財務上及び風評被害のリスクになる可能性があります。

[2] 回答者には以下のリストが表示されました：データ漏洩、ビジネスメールの漏洩（侵害）/トランザクション詐欺、フィッシング、分散/サービス拒否攻撃、パスワード漏洩（侵害）、ランサムウェア攻撃、その他のマルウェア攻撃。

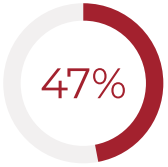
次に起こることは？

大半（85%）のCXOとVPは、パンデミック期間中の運用による悪影響が少なくとも3ヶ月以上続くと考えており、また、3分の1近く（33%）が、6ヶ月から12ヶ月間続くと予測しています。したがって、組織が最も深刻なリモートワークの課題に早急に取り組むことがますます重要になっています。

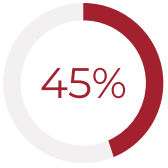
幸いなことに、ほとんどの企業がまさにこれを実行しようと計画しているということです。CXOやVPの70%が、コンプライアンス要件を満たし（26%）、サイバーリスクを管理し（25%）、サイバーリスクと従業員のプライバシーのバランスを取る（19%）ことで、サイバーセキュリティをリモートワークの最優先事項にすると回答しています。

これらの回答者のほぼ全員（96%）が、従業員がオフィスに戻る際にリスクを減らすための変更を計画していると回答しています。彼らは、主に次のものに投資を行うことでこれを実行しようと考えています。

IT資産の可視性を高めるエンドポイント管理（48%）



パッチ管理の改善（47%）



ITを分散化するためのクラウドコンピューティング（45%）

ゼロトラストモデル、VPNへの依存を軽減（38%）

可視性とコントロールが新しい現実における中心的な役割を果たす

今日、ITおよびビジネスのリーダーたちは、自分たちがある種の特別な瞬間を迎えていることに気づきます。多くの組織は、2020年スタート時に目の前に突きつけられた前例のない課題に見事に驚くほどうまく適応しましたが、従業員の生産性をサポートするだけでは十分ではありません。どこでも仕事ができる新しい時代に、継続的なサイバーリスクの軽減に十分な注意と注意を払わない限り、同じ組織が深刻な財務上の損害や風評被害にさらされることになるかもしれません。

重要なのは、現在多くの企業が抱えているパッチ未処理による脆弱性の潜在的な脅威に対処し、大幅に拡大した企業の攻撃対象リスクを軽減することです。これを実現する最善の方法は、多くの人が認識しているように、オンプレミス環境とクラウドベースの環境をまたいでITエンドポイントの可視性と制御を改善することです。これにより、より生産性が高く柔軟な作業形態、分散化されたクラウドコンピューティングモデル、セキュリティに対するよりアジャイルなゼロトラストアプローチ推進が可能になるだけでなく、遅れていたセキュリティプロジェクトを軌道に戻すこともできるのです。

破壊的な世界的危機から浮かび上がってくるのは、エンドポイントの一元管理とセキュリティを軸に、ビジネスを支えるITの強化に向けた新たな決意かもしれません。

この調査は、Censuswideが Taniumの委託を受けて実施したもので、2020年5月29日から2020年6月6日までの間に、米国、英国、フランス、ドイツの従業員数1,000人以上の企業のCXOおよびVP（CEO、CIO、CTO）1,004人を対象に世論調査を実施したものです。Censuswideは、ESOMARの原則に基づくMarket Research Societyに準拠し、メンバーを採用しています。

TANIUM

タニウムは世界で最も要求の厳しいIT環境向けに構築できる統合されたエンドポイント管理とセキュリティのプラットフォームを提供している、Fortune100に名を連ねる過半数、大手小売店、金融機関や米国軍の４軍を含む、大規模かつ先進的な組織や企業にご使用いただいております。これらのお客様は、タニウムを使うことで確実な判断を下すことができ、効果的に業務を遂行し、起こりうる障害に対する耐性を高めることが出来ています。タニウムは、米国フォーブス誌「2019年クラウドコンピューティングTop100」で7位に、フォーチュン誌「働き甲斐のある中小規模企業ベスト100」で10位にランクされました。さらにタニウムのことを知りたい方は、タニウムのウェブサイトをご覧いただくか、LinkedInやTwitterでフォローしていただければ幸いです。

tanium.jp

@Tanium

jpmarketing@tanium.com