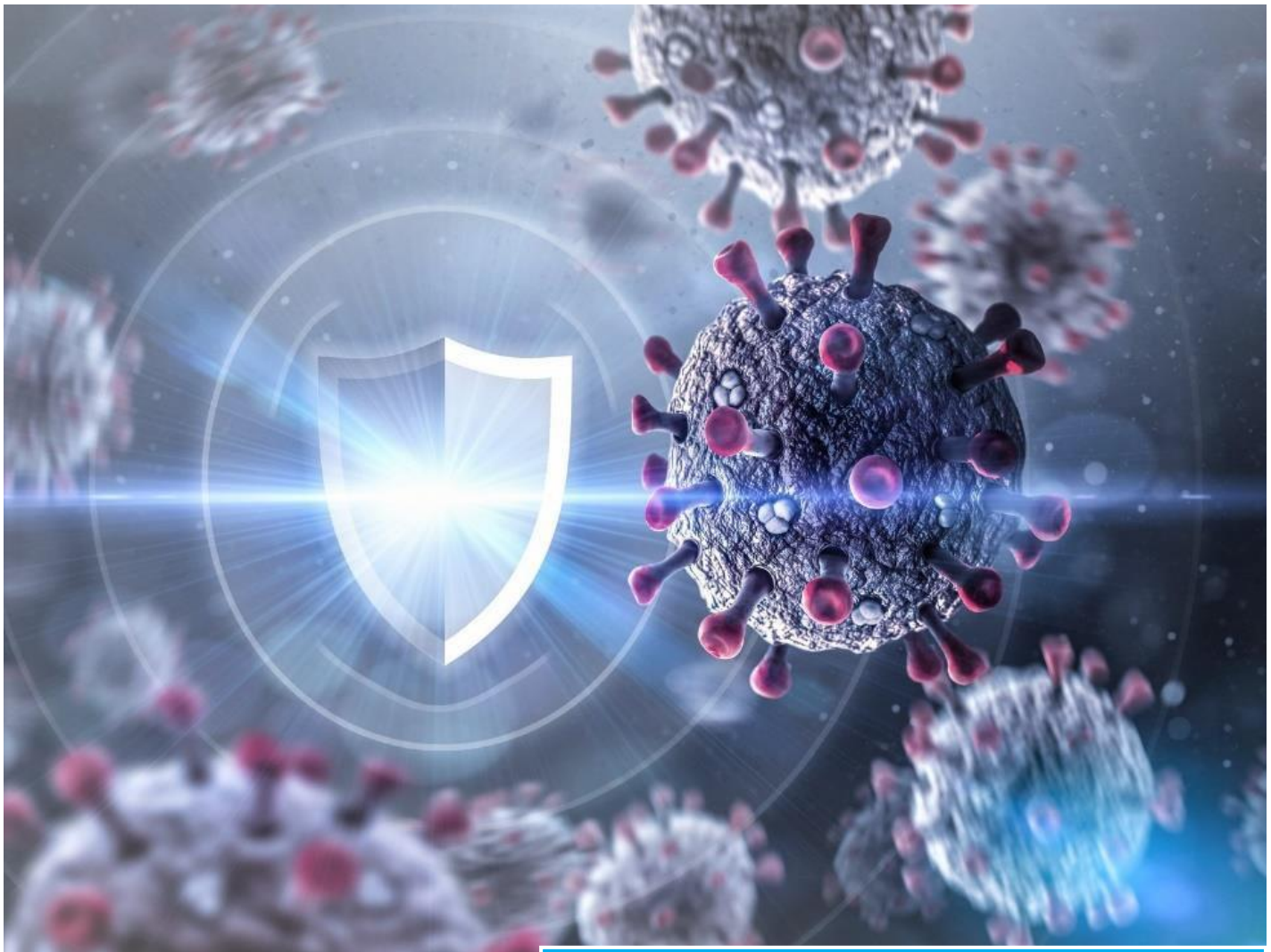

新型コロナウイルス感染症コンテンツシリーズ

新型コロナウイルス感染症の世の中で進化するサイバーリスク

著者：トビー・デロッシュ、CIA、CCSA、CRMA、CICA、CFE

The Institute of Internal Auditors
INTERNAL AUDIT FOUNDATION
Wolters Kluwer

目次

専門家について

トビー・デロッシュ、CIA、CCSA、CRMA、CICA、CFE

トビー・デロッシュ氏（CIA、CCSA、CRMA、CICA、CFE）は、Wolters Kluwer社のソリューション・コンサルタントである。ビジネスリスクを高める弱点を特定し文書化するとともに、そのような状況へのソリューションを推奨する専門家としての経歴がある。これまで数多くの内部監査部門を支援し、財務、業務、コンプライアンス監査を実施・監督し、コントロール・フレームワーク、財務システム、業務手順を評価してきた。

はじめに

新型コロナウイルス感染症パンデミックは、新たなサイバーリスクと非定型のサイバーリスクの両方に対する脆弱性に組織体を曝すという、最悪の事態を引き起こした。従業員は、自分自身と家族の安全に配慮しながら、職務をこなしている。従業員は、ほとんど、あるいはまったく準備や研修をしない状態で、リモートワークに移行した。組織体は、大幅な減収と世界経済の激変のせいで、生き残りに焦点を当てている。このような大混乱の中で、ハッカーをはじめとするサイバー犯罪者は、脆弱性を悪用する機会を手にしている。リスクの増大が著しいため、米国連邦捜査局（FBI）や国防総省（DoD）でさえ、リモートワーカーに警告を発している。

本稿では、新型コロナウイルス感染症パンデミックの最中とその後も、内部監査人がサイバーリスクへの警戒心を持ち続けるようにするために、認識を高める必要がある多くの状況について検討する。これは決して網羅的なリストではなく、むしろ現在の環境下でサイバーリスク評価を促し、パンデミック後の世の中を考え始めるための取り組みである。

リモートワークのリスク

組織体は多大な労力を費やして、ネットワークとデータを保護するために安全なIT環境を構築している。従業員が仕事の場を会社から自宅に移した途端に、安全策を講じた環境が迂回されて、新たなリスクとの接点が多数生じた。典型的な3人家族の家庭では、複数のデスクトップ・コンピュータ、ノートパソコン、プリンター、タブレット端末、携帯電話や他のモバイルデバイス、ゲームシステム、住宅用警報装置、サーモスタット、スマートスピーカー、その他のデバイスなど、驚くほど複雑なネットワークが存在する可能性がある。リモートワークの導入で、ノートパソコンや仕事用の携帯電話が追加され、このネットワークは拡大する。米国国防総省のエッシー・ミラー最高情報責任者（CIO）代理は、「テレワーク機能の向上に伴い、敵にとって攻撃対象領域が拡大している。攻撃者は、すでに手元にある状況や環境を悪用している」と述べた[1]。組織体の観点からいうと、デジタルフットプリント[a]がまさに指数関数的に拡大し、サイバーリスクも拡大した。

ネットワーク・セキュリティ

最初に、全従業員は自宅のネットワークを保護しなければならない。Wi-Fiを保護すると、悪意のあるユーザーがネットワークトラフィックをのぞき見することが、より難しくなる。ネットワークパスワードを見直して、複雑さの指針を満たすようにすべきである。なぜならば、ネットワークパスワードの多くは、インターネットのサービスプロバイダーの技術者が電話番号やアドレスとして設定してから変更されていないためである。基本的な家庭内ネットワークでは、リモートワーカーは会社にあるファイアウォール、セキュリティパッチ、およびバックアップから遮断されたままである。

従業員が組織体のデータにアクセスするためには、多要素認証（MFA)を使用する仮想プライベート・ネットワーク（VPN） を使用するよう義務付けるべきである。リモートデスクトップを使用して組織体のデータにアクセスする場合、IT部門は特定のIPアドレスのみをホワイトリストに登録すべきである。

ネットワーク・セキュリティに対する脅威の1つは、サードパーティ製[b]のソフトウェアをダウンロードすることである。リモートワーカーは、会社で使っていたツールや接続手段から遮断されたとわかると、悪戦苦闘することが多い。このような制約をなくそうとして、フリーのソフトウェアを使おうとする可能性がある。例えば、会社にいる時のような対面の会話をしたくて、ZoomやBluejeansのようなウェブ会議ツールをダウンロードするかもしれない。残念ながら、これらのプラットフォームの一部はハッキングされることがあり[2]、組織体をサイバー犯罪者に曝す可能性がある。コミュニケーションツールは、IT部門が承認したものに限定すべきである。

個人所有のデバイス

場合によっては、リモートワークへの移行を迅速に決定しなければならない。故意に、あるいは必要に迫ら

[1] DOD Warns of Cyber Risks as Employees Work From Home (https://www.databreachtoday.com/dod-warns-cyber-risks-as-employees-work-from-home-a-13960)
[2] Zoom Meetings Keep Getting Hacked. Here's How to Prevent 'Zoom Bombing' on Your Video Chats(https://fortune.com/2020/04/02/zoom-bombing-what-is-meeting-hacked-how-to-prevent-vulnerability-is-zoom-safe-video-chats/)
訳注a. デジタルフットプリントとは、インターネットを利用したときに残る記録の総称。作成したアカウント、ソーシャルメディアへの記事やメッセージの投稿、電子メールの送受信、ウェブサイトの閲覧履歴など。
訳注b. サードパーティ製品とは、その製品の開発・販売元ではない企業が提供する製品。互換性のある関連製品。

れて、従業員は個人所有のデバイスを使用して業務を遂行することがある。これらのデバイスは、特に従業員や顧客からの機密データや個人を特定できる情報（PII）を処理する場合、セキュリティ対策を満たしていない可能性がある。組織体に個人所有のデバイスの持ち込み（BYOD）方針[3]がない場合は、直ちに方針を確立すべきである。この方針は、使用を許可するデバイスの種類、VPNの使用、エンドポイント・コントロール[c]、データのリモートワイプ[d]、受けられるサポート、パスワード規則、および暗号化について取り上げるべきである。従業員の多くは、個人所有のモバイルデバイスを業務に使用してから退職する場合、個人所有のモバイルデバイスのデータをリモートワイプする権利を会社が留保していることが多いと知って驚いている。BYOD方針が非常に明確で全員が理解していることを、確認すべきである。

フィッシング詐欺

従業員が個人所有のデバイスを使用する場合や、仕事用のノートパソコンでネットワークにアクセスできない場合、セキュリティパッチの適用やアップデートには限界がある。このような場合は、ITセキュリティチームと協力して、個人所有のデバイスの使用を禁止したり、組織体が管理するデバイスの使用を強制したりする方法について話し合うこと。

さらに悪いことに、リモートワーカーを標的にしたフィッシング詐欺が大幅に増加している。これらの多くは、マスクやフェイスシールドなどの個人用保護具があると宣伝する電子メールである。在宅勤務の従業員が仕事用のノートパソコンで個人の電子メールをチェックしている場合、フィッシング攻撃からネットワークを悪質なコードに簡単に曝してしまう可能性がある。在宅勤務に伴って従業員宅に持ち帰るすべてのノートパソコンは、ファイアウォールと強力なウイルス対策機能を備えるべきであり、ウイルスがシステムに侵入するのを防ぎ、最終的に侵入してしまったものを検知し、削除することが望ましい。

最近のフィッシング攻撃は、新型コロナウイルス感染症に対する恐怖に付け込んで、無防備な被害者を誘い込んでいる[4]。ムスタングパンダと自称するグループは、ベトナム首相からのパンデミックに関する声明と称して、圧縮したWindowsアーカイブファイルを添付したフィッシングメールを送り付けた。ファイルが開かれたとき、コマンド＆コントロール攻撃を開始するためにバックグラウンドで実際にマクロを実行していたのは、無害に見えるWord文書であった。コンピュータはネットワークのファイアウォールの後ろにある場合があるため、攻撃者はネットワークデータにアクセスしたり、ネットワークを完全に遮断したりすることができる。

ファイル共有サイト

従業員が会社のネットワークから離れて働いていると、トラブルが起こることがある。例えば、共有ドライブ、SharePoint、またはTeamsにアクセスできない場合、同僚とファイルを共有することが難しくなる。そういう場合、人々は大抵クリエイティブになり、自宅で行っているのと同じ方法を使おうとする。しかし、組織体のITセキュリティチームは、DropboxやGoogleドライブなどのサイトを使用してファイルを共有することを認めていない可能性が非常に高い。

---

[3] Create a mobile BYOD policy for the coronavirus pandemic (https://searchmobilecomputing.techtarget.com/tip/Create-a-mobile-BYOD-policy-for-the-coronavirus-pandemic)

[4] Nation-State Hackers Using COVID-19 Fears to Spread Malware (https://www.bankinfosecurity.com/nation-state-hackers-using-covid-19-fears-to-spread-malware-a-13951)

訳注c. エンドポイント・コントロールとは、サーバー、パソコン、あるいはスマートフォンのような末端に接続されたデバイスや端末を、サイバー攻撃から守るためのセキュリティ対策。

訳注d. リモートワイプとは、携帯電話やスマートフォン、ノートパソコンなど持ち運び型の情報端末に記録されているデータを、通信回線を通じた遠隔地からの指示により消去すること。また、端末の持つそのような機能。

プライバシー保護法

リモートワークの増加により、組織体は、欧州の「一般データ保護規則（GDPR）」や米国の「医療保険の相互運用性と責任に関する法律（HIPAA）」などのプライバシー保護法に違反するリスクにも曝されている。再度、よくある状況をじっくり考えると、従業員の自宅にはリモートワーク専用のスペースがないかもしれない。このような場合、従業員は家族と一緒にダイニングルームやリビングルームで業務を行う可能性がある。この従業員が機密データを日常的に取り扱う場合、特に、その業務が機密情報を電話で話す必要がある場合、HIPAAの物理的保護セクションに違反するリスクが極めて高くなる[5]。

トラブルシューティングのためにクライアントシステムにアクセスする可能性のあるITサポート担当者がリモートワーカーに含まれている場合、機密データ漏洩のリスクはさらに複雑になる。トラブルシューティングでは、クライアントのデスクトップをリモートで表示したり、スクリーンプリントを共有したりする必要がよくある。これらの作業は、意図せぬデータ漏洩を容易に引き起こす可能性があり、リモートワーカーが個人所有のデバイスを使用している場合、データ漏洩リスクの影響度は、より重大になる可能性がある。

HIPAAのような法令では、内部監査は、日常的な監査とインシデントベースの監査の両方を実施する義務がある。内部監査人は、リモートワーカーの作業環境を再検討し、適切なセキュリティレベルを確保するために、迅速に行動する準備が必要である。

[5] Meeting HIPAA Requirements When Working Remotely (https://www.totalhipaa.com/hipaa-compliance-working-remotely/)

ベンダーのコントロールとSOCレポート

自身が所属する組織体の外で、第三者のサイバーリスクの増大に直面する可能性もある。サービス型ソフトウェア[e]（SaaS）については、通常は業務受託会社のコントロール（SOC）レポートに依拠して、テクノロジー・ベンダーのコントロール・フレームワークを検証している。ベンダーも従業員をリモート環境に移しているならば、ベンダーのコントロールに依拠する場合は、ベンダーの統制環境が基準に達していることを確認する必要がある。

物理的な警備のような、基本的なコントロールを考えてみよう。

サービスプロバイダーは、以下を対象とする警備の方針と手続を策定しているべきである。

- 従業員、ベンダー、訪問者による、施設への、および施設内の物理的な出入りの警備
- 受付場所、敷地の境界、監視、警備員、巡回警備の基準
- 特定の種類の場所と資産を警備するための基準
- 鍵と物理的な保安装置の基準
- 従業員、採用候補者、取引先従業員の経歴調査
- 施設へ出入りするためのアクセスカードやIDカードの発行
- 退職した従業員やベンダー担当者の出入りを禁止する措置
- 物理的安全対策違反の調査
- 資産の移動

このようなコントロールをベンダーの施設用に完璧に設計することは可能かもしれないが、従業員がリモートで働いている場合には、同じ水準のコントロールを保証することは断じてできない。友人、家族、修理工などが従業員の家に出入りするはずだから。

訳注e. サービス型ソフトウェアとは、ソフトウェアをインターネットを通じて遠隔から利用者に提供する方式。

そこで、次のようなベストプラクティスを期待すべきである[6]。

1. セキュリティ意識を向上させる研修の積極的な実施
2. リモートワーク方針の策定
3. パスワードの強化のような、エンドユーザーに対するコントロールの要求
4. ネットワークトラフィックの監視

目標とするのは、ベンダー側がリスクを確実に軽減することで、そうなればベンダーのコントロール・フレームワークに依拠し続けられる。

2020年のトップリスクの1つとして、既に特定されていたサイバーセキュリティ

新型コロナウイルス感染症流行前に内部監査人協会（IIA）が公表したレポート「OnRisk 2020」は、サイバーセキュリティが2020年に組織体に影響を及ぼす可能性のあるトップ11のリスクの1つであると指摘した。同レポートの主な発見事項は、サイバーセキュリティが「知識が著しく不足している分野」であると言及した。取締役、経営陣、および内部監査部門長(CAE)は、サイバーセキュリティについて知識が不足している点と、このリスクが組織体に強く関連しているという点で、一致した見解を示した。同レポートは、「リスク・マネジメントの担当者は、サイバー知識を優先的に身につけるべきである」と提言している。

出典：*OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk.* Lake Mary, FL: The Institute of Internal Auditors, 2019.

[6] SOC 2 Academy: Access Controls for Remote Employees (https://kirkpatrickprice.com/video/soc-2-academy-access-controls-remote-employees/)

パンデミックがサイバー問題に及ぼす影響

サイバーリスクに対する関心の低下

リモートワーカーは、業務を続けるために最善を尽くしているが、家族と自分自身の健康と幸福が常に優先する。食料品を見つけること、リモート授業中の子供たちと一緒に仕事をすること、生活の中で増えるストレスに対処することなどを親が心配している場合、望ましいサイバー慣行に従うことは最優先ではないかもしれない。

一方で、企業は大幅な減収に対処して、生き残ろうとしている。多くの企業が、すべてのサポート機能を停止し、一握りの従業員を除いて全員を一時帰休とし、残った従業員の賃金を引き下げている。当面の間、採用と支出は全面的に凍結される。財務リスクが最も高い場合、サイバーリスクの評価は相対的に低くなる。ITセキュリティチームは、最小限の人員で作業をしていることが多いため、どこに時間を割くかを優先順位付けしているが、新たなリモートワーカーのセキュリティ対策でパンク寸前である。

ニューノーマルにおけるサイバーセキュリティ

新型コロナウイルス感染症パンデミックは、サイバーリスクに曝される可能性に直接影響を及ぼしてきたが、このリスクは今も続いている。世界中でリモートワークが指示されていることによる長引く影響は、いつまでも印象に残りそうである。良い影響としては、交通量、燃料消費量、汚染、および多くの事務所運営費が減少している。あまり外食しないので、食費が抑えられる。家族で一緒に過ごす時間が増えている。人々は歩いたり、自転車に乗ったりしている。

これらをすべて勘案すると、誰もが今回のように行動したことは今までなかったが、新型コロナウイルス感染症パンデミック発生前のような通常業務に戻ることは想像し難い。内部監査人としては、経営陣に対してリスクの増大を指摘する義務がある。今後の業務環境は、出社とリモートワークを組み合わせたものになるだろう。サイバーセキュリティのコントロールについては、現状を踏まえて改訂を行い、将来に備えなければならない。

32%

のCAEは、内部監査資源をサイバーセキュリティに**割り当てていない**と回答した。

出典：2020 North American Pulse of Internal Audit. Lake Mary, FL: The Institute of Internal Auditors, 2020.

結論

世界中の内部監査部門が機敏性を示し、リスク評価を更新し、監査計画を見直すにつれて、サイバーリスクに対する関心が高まり、より高い価値が生み出せる。

まさに今、監査で検討すべき分野

リモートワーカーが及ぼす影響を検討する監査人には、以下の分野を勧める。

- 在宅勤務方針をレビューして、組織体が所有し管理するデバイスの使用を義務付ける。
- 個人所有のデバイス、すなわちBYOD方針をレビューして、ホワイトリストに登録されていないデバイスによる組織体ネットワークおよびデータへのアクセスを禁止する。
- 個人所有のデバイスの使用を許可する場合は、ハードウェアに適切なセキュリティ・コントロールがあり、このコントロールがBYOD方針で裏付けられていることを確認する。
- 会社のネットワークにアクセスする際、MFAを使用しているVPN を使用するよう義務付ける。
- デバイスの保護やパスワードの複雑さなど、一般的なセキュリティ対策に関する研修を義務付ける。
- 従業員と顧客の個人情報を取り扱うための研修を義務付ける。
- 方針をレビューして、承認されたウェブ会議やデータ交換サイトのみを使用することになっているかを確認する。
- 重要なSaaSベンダーをベンダーリスク・マネジメント担当者とレビューして、最新の業務環境下でSOC
レポートが依然として有効であることを確認する。
- 組織体内外のリモートワーカーによるデータ漏洩が発生した場合の、事業継続計画をレビューする。
- リスク・マネジメントチームに問い合わせて、エクスポージャーがある場合、サイバーセキュリティ賠償責任保険をかけていることを確認する。
- ITセキュリティ部門とサポート部門の人員配置に関して、人員配置と意思決定のレベルをレビューする。

参考文献

- The Future of Cyber Security in Internal Audit
- OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk
- Privacy and Data Protection Part 1: Internal Audit's Role in Establishing a Resilient Framework
- 2020 North American Pulse of Internal Audit

内部監査財団について

内部監査財団は、内部監査専門職を進展させるために必要不可欠なグローバル・リソースであることを目指している。当財団の調査・教育商品は、内部監査の実務家やステークホルダーに対して、新たな話題に関する洞察を提供し、内部監査専門職の価値を世界的に推進・向上させている。また、学術基金を通じて、内部監査人協会(IIA)の内部監査教育パートナーシップ・プログラムに参加する学生と教育者に助成金を支給することにより、専門職の将来を支援している。詳しくはwww.theiia.org/Foundation を参照。

内部監査人協会(IIA)について

内部監査人協会(IIA)は、内部監査専門職に関する提唱者、教育機関、ならびに基準、ガイダンスおよび各種認定資格の提供者として、世界で最も広く認識されている。1941年に設立され、現在、世界170以上の国と地域に20万人以上の会員がいる。国際本部は、米国フロリダ州レイクメリーにある。詳しくは、www.theiia.org を参照。

TeamMateについて

TeamMateは、Wolters Kluwerの税務・会計部門の一部として、的を絞った設定可能で効率的なソフトウェア・ソリューションを提供することで、世界中の全業界の組織体の専門家が監査・コンプライアンスリスク、およびビジネスの諸問題を管理できるよう支援している。
ソリューションには、TeamMate+ Audit、TeamMate+ Audit Public Sector、TeamMate+ Controls、TeamMate Analyticsなどがある。これらのソリューションは、リスクの識別と評価、電子監査調書の作成と管理、コントロール・フレームワークの管理、データ分析のすべての側面を組織体が管理するために必要な、統合されたアシュアランスを提供する。詳しくは、www.teammatesolutions.comを参照、またはTwitter、Facebook、Linkedin、YouTubeをフォロー。

免責事項

内部監査財団(IAF)および内部監査人協会(IIA)は、情報および教育目的のために本レポートを発行している。本レポートは、個別具体的な状況に対する確答を提供することを目的とするものではなく、あくまでも指針としてご使用いただくものである。特定の状況については、関連する独立した専門家に直接助言を求めることをお勧めする。IAFおよびIIAは、本レポートのみに依拠する人に対して一切の責任を負わない。

著作権