表題　1	テレワークニーズに追いつかないセキュリティ対策
内容	新型コロナウィルスの影響で、テレワークが急速に普及している。VPN 接続、クラウドサービスの利用、遠隔会議システムなどを十分なリスク分析を経ずして導入した組織も多い。一時的措置として、従来のセキュリティポリシーから外れる施策を導入した組織もあるであろう。またコロナウィルスが収束したとしても、これらのシステムはニューノーマルの働き方として一定程度残ると考えられる。 急場しのぎで導入したシステムあるいはサービス利用が、組織の従来のセキュリティレベルを低下させていないか、インシデントハンドリングなどのセキュリティ運用業務がリモートでも行える準備ができているか、確認が必要である。
監査のポイント	・ テレワーク導入に伴い、ネットワークシステムや、データ保管の場所など、従来のセキュリティポリシーや社内ルールに違反している箇所はないか。 ・ テレワーク導入に際して、適切なリスク分析と対策がとられているか。特に、VPN 接続や、社外に分散するデータにアクセスする認証強度、自宅設置の PC のセキュリティ対策は十分か。 ・ テレワークを前提としたセキュリティ管理ができることを確認しているか。特に、PC やデータが自宅やクラウド上などの社外にあることのみならず、セキュリティ管理の担当社員も社外から適切なオペレーションを行うことが可能か。 ・ テレワーク環境を今後も定着させる場合、ネットワークや利用するクラウドサービス等の障害を想定した事業継続について検討し、対策がとられているか？
表題　2	**史上最悪の天災やパンデミックなどに対応できる IT-BCP へ**
内容	このところ毎年史上最大級の豪雨による大被害が発生している。環境省によれば、気候変動により今後さらなる大雨が予測され、災害が深刻化すると懸念されている。また、海溝型や直下型の地震は、ひとたび起きると甚大な被害をもたらすことになり、富士山噴火なども想定外においておくことはできない。さらに、今回の COVID-19 パンデミックでも、IT インフラの運用要員の確保などに多くの課題が露呈した。 デジタル化が進む中で、企業のみならず国民生活全般がサイバー空間に大きく依存するようになり、災害時においても IT インフラの機能確保が社会的要請になっている。企業や団体には、自組織の重要 IT インフラが利用できなくなるリスクの発生可能性と影響度を的確に把握できているか、そのようなリスクへの対策や業務継続の実効性確保ができているかなど IT-BCP の見直しニーズがさらに高まる。
監査のポイント	・ 史上最大級の天災や、COVID-19 などのパンデミックを想定したビジネスインパクト分析が行われ、経営陣に承認されたものとして IT-BCP への要求が明確になっているか ・ IoT やクラウドの利用、テレワークの推進などによる業務プロセスの IT 基盤への依存度の変化が的確に把握されているか ・ 上記 2 点の変化を踏まえた IT-BCP の要件の見直しが的確に行われているか ・ 要件の変化に応じたリスクの再評価が的確に行われ、その結果に基づいて、IT-BCP の見直しが行われているか ・ パンデミックを想定した IT 要員配置計画が組み込まれているか ・ IT-BCP の見直しに伴う教育や訓練が実施されているか。 ・ 全社 BCP との連携が的確に計画され、連携したテストや訓練が行われているか

表題　3	止まらない、安全なクラウドサービスへ広がる要求
内容	クラウドサービスはこれまで様々な課題が指摘されている。一方、システム構築や運用上のメリットは大きく、クラウドを利活用する流れは加速している。我が国の政府もクラウドバイデフォルトを掲げ、クラウドのセキュリティ評価制度（ISMAP）を立ち上げた。企業、個人、国家などの膨大なデータがクラウドに集約されるということは、それだけ攻撃者にとっても価値が高く、 クラウドに対する攻撃は、より狡猾にまた、激しさを増すと考えられる。 クラウドに関連するシステムだけでなく、サプライチェーン、組織、個人も含めて、ありとあらゆる構成要素がターゲットとなる。安全性に疑義がないことを多面的に証明、維持していくことが重要となるだろう。
監査のポイント	プロバイダのクラウドサービスについて、以下の観点での監査がポイントとなる。 ・ サービスの目的に合った適切な管理基準、管理策が選択されているか。 ・ 管理策の解釈に相違は無いか。管理策は適切に実装が行われているか。 ・ 言明されているサービスの適用範囲と実際の監査証跡は一致しているか。サプライチェーンの見逃しは無いか。 ・ サービス提供において、サービス提供用設備、利用する他社クラウド、提供先の顧客環境の責任分界点を明確にできているか。 ・ サービス約款、サービス内容、言明内容、管理策が整合しているか ・ 事故発生時の対応方針が明確か
表題　4	**標的型攻撃の侵入パターンが多様化**
内容	今までの標的型メールによるシステムへの侵入から、VPN や管理ソフトウェアなどの脆弱性や、海外拠点の弱いネットワークから本体に侵入する標的型攻撃にシフトが移っている。そのため、攻撃されていることを見つけづらく、何かのきっかけで異常が発見されるまで侵害に気づかないことが多い。 また、一般的なリモートデスクトップソフトなどを悪用し、普通の仕組みで浸透を継続することから、事案発覚後も侵害されつづけていることがある。
監査のポイント	・ 自システムに繋がるすべてのネットワーク(拠点間 NW・VPN 回線)からの通信において、不正な通信を監視し、発生時には自動的な検知と必要に応じた通信の遮断と発生理由を把握できる仕組みがあるか ・ クラウドサービスを含めすべての管理者アカウントの異常な利用(夜間等の通常利用されない時間帯・許可のない IP・ログイン失敗)を感知し、発生理由を把握できる仕組みがあるか ・ AD やファイルサーバなど重要なサーバで、異常な動作(イベントログの削除・タスクの登録)を検知し、確認する仕組みがあるか ・ サーバ内への許可外リモートデスクトップソフトウェアの導入を原則禁止し、その利用を管理しているか

表題　5	頻発する大規模システム障害への対応
内容	2020 年には2か月に1回程度の大規模システム障害が発生した。コンビニ決済、IC 乗車券、携帯電話ショップ、航空カウンター、そして証券取引システムなど、社会のインフラや人々の身近なサービスが長時間利用できなくなった。ネットワークが統合され、より便利になる一方で障害の影響も深刻化する。
監査のポイント	システムトラブルに関するセキュリティに関しては、2つの観点での監査が必要である。 ・ システムの開発保守におけるセキュリティ要求事項（ISO27002 の 14.1 及び 14.2）が実装され運用されているか ・ 情報セキュリティインシデント管理及び事業継続に関わる管理策が実装され運用されているか。 事業継続については、情報セキュリティの国際規格 ISO/IEC27000 の範囲外になるが、密接な関連があるため、組織として監査の範囲に取り込むことが望ましい。
表題　6	**在宅勤務のセキュリティ対策に求められる説明責任**
内容	新型コロナの影響により、政府の推進していた働き方改革が加速する形でテレワークが実施される状況となった。各社テレワークを行う場合の自宅環境や実施ルールなどは一通り決められているものの、研修が十分に行われていなかったり、自宅兼仕事環境の物理的なセキュリティや通信環境など本当にセキュリティが保たれていることを実際に確認されてなかったりするケースも多い。 新しい働き方が定着し、2021 年に東京オリンピックが開催される場合は自宅のテレワーク環境への注目が高まってくる。この流れの中で、自宅環境の説明責任の向上のため、企業側に対しても従業員に丸投げにさせないための支援が急務となる。
監査のポイント	可用性と機密性の確保を主目的として、以下の様な点に考慮して監査を実施しているか。 ・ 組織の情報セキュリティ責任者が、在宅勤務・リモートワークに関わる基本方針を定めているか ・ 在宅勤務・リモートワークに関わるリスクの洗い出しが行われているか ・ 在宅勤務・リモートワークに関わる既存契約の見直しが行われているか ・ 在宅勤務に必要な IT 環境や物理的セキュリティに対する要求事項を定め周知しているか ・ 上記要求事項に見合ったセキュリティアーキテクチャと管理策の実装をしているか ・ リモート会議に利用できるツールについて定義・限定しているか ・ リモート会議ツールのようなセキュリティアップデートが頻繁なサービスを継続的にモニタリングする体制が確立しているか。 ・ リモート会議の運用に関わる注意（無断参加者・録画・情報共有方法等）喚起を行っているか。 ・ 在宅勤務・リモートワークに関わる研修（リモート会議及びツールを含む）は必要なメンバーに対して実施されているか 必要な対策が確実に行われていることを検知・確認できる体制が確立しているか　（リアルタイムに近い頻度でログの確認ができているか等）

表題 7	手法の高度化が進む金銭目的のサイバー攻撃
内容	技術的なスキルが高いとされていた標的型攻撃の手法を取り込み、ランサムウェア・情報暴露・暗号通貨窃取・BEC を狙う攻撃者は、様々な手法によって組織を狙い、時には国家が背景にあると推定されるサイバー攻撃者グループよりも技術的に高度な手法を使ってくることも少なくない。すでに、標的型攻撃と金銭目的の攻撃の技術レベルは区別できず、より広汎で大量で高度な攻撃に組織はさらされることになる。
監査のポイント	· 自組織のセキュリティ対策が、上記内容のようなサイバー攻撃を想定して対策を行っているか。 · 金銭目的でのサイバー攻撃を想定した業務フローの更新を行っているか。例えば、振込先口座の変更依頼があった場合、真偽を電話で確認するなど。 · セキュリティ担当、IT 担当の社員のみならず、一般の従業員に対しても研修や訓練等を行っているか。 · 新たなサービスを立ち上げる場合に、なりすましによる金銭搾取などの詐欺行為を想定した脅威の分析と対策を行っているか。また、そうした検討を行えるよう社内体制を整備しているか。
表題 8	在宅勤務者を踏み台に組織を狙うフィッシング詐欺の横行
内容	リモートワークの増加や、ニューノーマルな働き方の一環による在宅増加に伴うウェブサービスの拡充により、ID/パスワードの利用シーンが増え、かつ、アクセスできるリソースや価値が増えたことから、相対的にアカウント情報を狙うフィッシングも増えている。さらに構築スピードと利便性を重視して乱立したサービスではセキュリティデザインもされておらず、被害範囲を拡大させる一因となっている。
監査のポイント	· フィッシングメールについて在宅勤務者に教育し、誤って入力してしまった際にとるべき措置について教育されているか · メール容量警告やパスワード期限切れ警告など、システムからの通知を装ったフィッシングメールを隔離できる仕組みがあるか · 在宅勤務者の端末からのインターネット通信もセキュリティが確保される仕組みがあるか · 異常なログイン動作(間隔の短い複数国からのログイン)を検知し、異常でないか確認する仕組みがあるか

表題　9	Easy なネットサービスの Easy な拡大がなりすましの温床に
内容	ネットサービス、とりわけスマホによる決済サービス分野は顧客獲得競争が激化している。シェア拡大のため利便性を追求する一方でセキュリティが甘くなり、犯罪者によるなりすましと換金・送金手段も容易になった。また、行政も消費の活性化と官民キャッシュレス決済基盤の構築を目的にマイナポイント事業を展開し、マイナンバーカードの普及を促進している。 リテラシーの低い消費者とサービス拡大路線を進む事業者、マイナンバーカードを普及させたい行政の三位一体が、深刻ななりすまし犯罪の温床になるおそれがある。
監査のポイント	・ サービス登録時の本人確認は、決済・送金額と扱うデータのリスクに応じた手段と証拠に基づいて行っているか。 ・ サービス利用時の本人認証は、なりすましを防止できるか。 ・ 送金・決済の指示が本人によるものかを事前又は事後速やかに確認できるか。 ・ QR コードをモバイルデバイスで扱う場合、決済要求が利用者のモバイルデバイスから発信されたこと、QR コードの真正性及び有効性を確認できるか。 ・ クレジットカード番号を扱う場合、カード会員のデータセキュリティ基準を満たしているか。 ・ マイナンバーを扱う場合、特定個人情報に関する安全管理措置を講じているか。
表題　10	**ニューノーマルに対応した新たな情報セキュリティ監査**
内容	コロナ禍で監査に支障が生じている。三密の回避を理由に現場への立ち入りや担当者への質問ができないことがある。一方でリモートワーク中の社員たちへの監査は実質的に不可能である。これらの結果、監査手続きが不十分となり、脆弱性がとらえにくくなっている。 このような状況が続くと情報セキュリティマネジメントが行き届かなくなり、情報セキュリティ事故につながりかねない。ニューノーマルに対応した情報セキュリティ監査のあり方が問われている。
監査のポイント	・ リモート監査といわれる Web 会議等を通じた質問やビデオ撮影等の間接的な手段など、様々な工夫で監査の努力が行われている。これらの手段を通じても、短期的には監査リスクが増えることは避けられない。このため、管理策がより確実に実施されるような取り組みが必要である。自主点検の強化、管理手順に確認やモニタリングのプロセスを加えるなど、ミスを減らす工夫が必要である。 ・ 中長期的には、モニタリング等を含めてシステム化を推進することが必要である。情報セキュリティ監査の DX を検討するよい契機にしたい。