2023 年情報セキュリティ十大トレンド トピックス解説文、監査のポイント

第 1 位	大規模社会インフラシステム障害により増大するサイバーリスク
内容	わが国の重要インフラ分野として「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の 14 分野が指定されている。これらの分野の多くは制御システムによって動作するが、今やすべてのインフラは情報システムとは無縁ではなく、インターネットから隔離された完全な閉域システムは少ない。情報システムはネットワークでつながることにより障害が広域に展開し、大きな影響を与えることがある。社会インフラは今後も情報システム化、ネットワーク化が進み、ますます大きなサイバーリスクにさらされることとなるだろう。
監査のポイント	重要インフラ事業者及びその利用者に対する監査のそれぞれの留意点は以下の通り。 □重要インフラ事業者に対する監査のポイント ・重要インフラに関わる全ての情報系／制御系システムは、インターネットとの直接的な接続の有無にかかわりなく、サイバー攻撃の対象となり得ることを前提にリスクを評価し対策を実施しているか。 ・重要インフラに関わる全ての情報系／制御系システムは、他のシステムとのネットワーク接続・連携がされ得ることを前提に、攻撃・障害等の被害の波及範囲を評価し対策を実施しているか。 ・重要インフラ事業者の事業継続計画は、攻撃・障害等の被害の広域化・長期化を前提に立案され訓練されているか。 □重要インフラの利用者に対する監査のポイント ・重要インフラの利用にあたり、重要インフラ事業者のインフラ設備の高信頼設計方針（冗長化等）、サイバー攻撃等への防御対策及び事業継続計画を考慮して、重要インフラサービスの選択を実施しているか。 ・利用している重要インフラの代替サービス又は代替手段への切り替えが可能な対策を実施しているか。 ・重要インフラの利用者の事業継続計画は、重要インフラサービスが広域かつ長期に停止することを前提に立案され訓練されているか。

第 2 位	IT サプライチェーンの統制強化
内容	近年、委託先における情報漏洩のインシデント発生が後を絶たない。契約上で秘密保持の遵守や再々委託先の管理監督が示されているものの、実態として評価ができていない状況である。また、グループ会社や海外拠点への不正アクセスによって、国内の本社や生産拠点が影響を受ける事例も発生している。 自社だけでなくサプライチェーンに属するすべての企業を含めたセキュリティ対策を強化していく必要性の認識が広まり、技術的な観点、ルールの徹底や教育ならびに自動化を意識した管理・監督が加速する。また、委託先のチェーン全体を視野に入れて、システムとして情報漏洩が発生しにくい環境の構築も進む。
監査のポイント	ITサプライチェーンにはハードウェア、ソフトウェア、サービスに関わるものがあり、リスク対応も広範囲に及ぶが、主として下記の事項が監査すべきポイントとして挙げられる。 ・ システム開発やデータ処理の業務を委託する際に、委託先（さらに必要に応じてその先の再委託先）に対して要求するセキュリティ対策を明示し合意する手続きを定めているか。 ・ 社外からのソフトウェア（オープンソースソフトウェアやライブラリなども含む）の導入に際して、マルウェア混入や脆弱性の残存など、確認すべき項目が明確になっているか。 ・ オープンソースソフトウェアやICT製品、利用サービスについて脆弱性対応を迅速に行うための管理を行っているか。 ・ 社外の組織（業務委託先や子会社等）とのネットワーク接続（VPNを含む）の接続点で、接続先からの攻撃を想定したアクセス制御やマルウェア検知等の仕組みを導入しているか。 ・ 供給の途絶あるいは遅延を対応すべきリスクとして考慮しているか。 ・ クラウド型サービスやASP型サービスの利用の際に、セキュリティ管理状況やセキュリティ侵害発生時の対応レベルなどを確認しているか。 ・ 自社が業務委託先である、あるいは顧客向けにサービスを提供している場合、自社経由で顧客にセキュリティ攻撃が及ばないよう、納品物（開発委託を受けたソフトウェア等）や提供サービスのセキュリティ確認を行っているか。

第 3 位	サイバーランサムによってあぶりだされる「怠け者システム管理者」や「ダメ経営者」
内容	システムに侵入し、情報窃取や暗号化を実施して脅迫をするサイバーランサムは、高度な攻撃技術を有するわけではなく、放置された脆弱性や、外部に公開していてはならないサービスを攻撃してくる。そのため、対策は特殊なものではなく、当たり前のセキュリティ確保ができていなかったことが原因と考えられる。 本来であれば防げていたはずの攻撃被害を防げなかった組織は、システム管理者が脅威を認識する手順を定めていないか、運用を怠っていたか、経営者がシステムのセキュア運用に理解がなく適切なサポートを契約しなかったか、適切なリソースを承認していなかったか等、「当たり前ができていなかった」ことがランサムウェアによってあぶりだされることになる。
監査のポイント	サイバーランサムの被害が世界的に後を絶たないが、その原因となる脆弱性は残念ながら管理者が適切に機器の設定を管理していなかったり、機器のセキュリティパッチを管理していなかったり、弱いパスワードを使っていたり、システム管理者・セキュリティ管理者の懈怠が起因であると指摘されても仕方がないものに起因することが多い。その中には、情報部門からのセキュリティリスクを経営層が軽視し、結果として被害に繋がったケースもあると考えられる。高度なサイバーセキュリティ対策でない「当たりまえ」がいかに実装できているか、監査において再度問い直すことが重要である。 □ システム ・保守切れ/保守未加入の機器・ソフトウェアがないか ・セキュリティパッチの必要性の判断と迅速な適用体制 ・インターネットからアクセス可能なサービスのモニタリング ・インターネットからアクセス可能な機器のセグメントアイランド化 ・セキュリティ機器のアラートの把握と対応方針の切り分け ・弱いパスワードを設定させないポリシーの徹底 ・管理者ログイン失敗のモニタリング ・管理者が異なるネットワークの接続点でのアクセス機能の最小化 □ 経営者 ・システム部門へのサイバーリスクの確認 ・システム部門による残存リスクに対する説明受領と内容による是正や承認の実施

第 4 位	クラウド障害による社会的影響の拡大
内容	クラウド・ファースト、クラウド・バイ・デフォルト、クラウドネイティブの考え方の普及に伴い、昨今特にデジタルビジネスにおいてクラウドサービスは社会的基盤となっている。 一方、メガクラウドであっても障害とは無縁ではなく、大規模データセンターにおける障害や、オンライン会議システムの世界的なサービス障害等、クラウドサービスの障害により多くの企業・組織の活動に影響が出てしまう事例が散見されている。 こうした障害への対応に加え、ビジネス要求への対応、ベンダーロックインからの防衛などの目的で複数のクラウドを利用する、いわゆるマルチクラウドを選択する企業が増えていく。マルチクラウドでは、セキュリティ統制が複雑になることから、統制不備に起因するセキュリティインシデントも散見されるようになる。
監査のポイント	クラウドサービスの利用に関して、特に可用性の観点からは次のポイントが重要である。 ・ クラウドサービスの利用の際に、可用性要件を定め、利用サービスの SLA(Service Level Agreement)や SLO(Service Level Objective)などで要求水準を満たしていることを確認しているか。 ・ クラウドサービスに障害が発生した際の確認手順、対応手順（顧客等ステークホルダへの連携を含む）が定められているか。 ・ クラウドサービスの障害を想定した対応訓練を行っているか。 ・ 複数のクラウドサービスを利用する場合（いわゆるマルチクラウド）、一方のクラウドサービスの設定や手順に変更があった際に他のクラウドサービスでも同様の変更が必要かどうかを確認しているか。

第 5 位	要注意！大事故につながるクラウドサービスのユーザ設定不備
内容	クラウドサービスの利用において、ユーザ側の仕様変更への対応の漏れや設定の不備による情報流出等の事故が多発したことから、2021 年 11 月末には NISC から「クラウドを利用したシステム運用に関するガイダンス」が、また 2022 年 10 月には総務省から「クラウドサービスの利用・提供における適切な設定のためのガイドライン」が発表されるなど、公的なガイドラインが発表されている。利用者側組織としてもクラウドサービス利用時に自らの組織におけるセキュリティ要求事項を定め、適切な対応ができているかどうかを確認する管理策の実装と、定期的な監査の必要性が高まっている。
監査のポイント	利用者組織にとっても、従来とは異なるマネジメントが必要となることから、妥当性のあるセキュリティ対策のベストプラクティスから管理策を実装しているかどうかがポイントとなる。米国では CIS ベンチマークとして公的に利用サービスごとの文書がリリースされており、日本政府などの公式文書でも参照されるようになってきている。 またクラウドサービス提供側では CIS ベンチマークに基づいた管理策が正しく運用されているかをダッシュボード等でリアルタイムに閲覧できるシステムが実装されているものも多いため、そのようなサービスを有効に活用しているか、またそのようなサービスを活用した監査手続も求められるところである。 ・ 妥当性のあるベンチマークに基づいた管理策が策定され実装されているか。 ・ 運用状況についてサービス機能などを用いて監視し、修正しているか。 ・ 常に最新の情報に基づいた対応が実施されているかを定期的にレビューし評価しているか。

第 6 位	働き方改革に追いつかない組織管理
内容	徳島県つるぎ町立半田病院のマルウェア感染事例でも明らかなように、現在のサイバー攻撃は複雑性を増しており、仮にインターネットから分離された環境においても、想定外の経路で侵入され、潜伏される事例も発生している。勤務場所の一つとなったホームエリアでのリモートワークにおいても、慣れてきた今だからこそ油断が生じ、そこにインシデントの原因が潜む可能性が高まっている。個人として Wi-Fi ルータをはじめとする家庭での情報通信機器に対する最新のアップデート適用や、家電や防犯設備、インテリア等の IoT 機器への対策等を行うだけでなく、組織としての総合的なセキュリティの監視と対策の仕組みづくりが望まれる。
監査のポイント	働き方の変革における主たる変化は、組織の管理外の「場所」と「デバイス」から業務を実施できるようになったことが最大のポイントであろう。したがって組織管理のネットワークの内と外といった境界を基準とした管理策ではなく、実施すべき対策が組織管理か否かに関わらず、同一に行われている状態が維持されていることを担保する管理策が策定・実装され、その運用が正しく行われているかを監査することが肝要である。そのうえで、最も大きな脅威であるランサムウェアなどに優先度を高めるなどの方針も必要である。 ランサムウェアは侵入・潜伏するプレランサム期と、実際に暗号化・脅迫を行うデプロイメント期に大きく動作が異なるため、いち早い検知とそのための常時監視が必要であり、同時に被害にあった端末やアカウント等からの横移動攻撃を防ぐ対策などもポイントとなる。 ・ 不要なポートは閉じているか（必要なポートが定義されているか）。 ・ アカウントの認証には多要素認証が実装されているか。 ・ アンチマルウェアは組織が定めたルール通りに、常に最新の定義ファイルで適用される状態となっているか。 ・ EDR などの導入により端末の利用状況を把握し、異常な利用を即時検知できる状態となっているか。 ・ デバイスやソフトウェアは常に最新のバージョン・パッチを適用しているか。 ・ セキュリティに関するログは取得するだけでなく、定期的に分析し、セキュリティポリシーに反する利用を即時修正できる体制となっているか。

第 7 位	待ったなし！中小企業のセキュリティ対策
内容	最近の新型コロナウイルス対策のために急速に進展したテレワークと、国を挙げてのデジタル化の推進に伴い、情報セキュリティ関連法規の改正や様々なクラウドサービスの提供が開始され、中小企業が IT 化を推進する動機と環境は急速に整いつつある。ただし、これらの進展に必要不可欠なのはこれらに即応したセキュリティ対策であることも明らかである。また、最近のサイバー攻撃対象となっているサプライチェーンでの対策も重要であり、組み込まれた中小企業においては外部から求められるセキュリティ対策にも応えなければならない。一方、人的資源や財務的資源に限りがある中で、置かれた環境に即したセキュリティ対策と監査をいかに柔軟かつ効率的に実現するかが大きな課題である。
監査のポイント	中小企業は「中小企業の情報セキュリティガイドライン」（独立行政法人情報処理推進機構）を評価の基準として自己評価し、自社がガイドラインのどのステップにあるかを把握することから始めることが望ましい。現状の把握と改善の段階であるステップ１、２の場合は、ガイドラインの項目の達成状況を評価し、達成が不十分な点を改善する。本格的な取り組みを行うステップ３の場合には、自己点検シートによって自らが定めた規定やルールを役職員が理解し・実施しているかを評価し、不十分な点について組織全体で認識し、改善に取り組む。より強固にする段階であるステップ４に達している場合には、必要に応じて専門家の支援や研修を受けて、内部監査人の育成を図り、内部監査体制を構築する必要がある。ステップ４の監査においては、その企業の規模や取引先、業務形態などに即した情報セキュリティ対策の監査がポイントとなる。 なお、「中小企業の情報セキュリティガイドライン」はテレワークの進展やインシデント対応に関する内容の充実など、サイバーセキュリティ環境の変化に対応するため、現在改訂作業中である。

第 8 位	ディープフェイク等高度化する虚偽情報を使ったネット詐欺に要注意
内容	インターネット上には元々真偽が定かでない情報が飛び交っているが、テクノロジーの進化に伴い、AI を用いて作成した画像や、動画を使ったフェイクニュースが多数作成されるようになってきている。ロシアのウクライナ侵攻や台風災害時においても、多数の偽動画・画像により、誤った情報が広まってしまっている。今後、標的型メール攻撃等でも、今までのような添付ファイルではなく、リンク先の動画やより騙しやすい画像を参照させて、詐欺に繋げる手口が出てくる可能性があり、組織内における抑止（心理的対策）と防止（物理的対策）両面の対策が求められる。
監査のポイント	・ 従業員に対して不審メールの手口や種類が拡大しており、過去にない種類の詐欺に利用されるケースが有ることを教育しているか。 ・ フィッシングメールの訓練や事例の研修を行うにあたっては、既知の情報だけでなくサッカーワールドカップの様な、多くの人の関心が高いトレンドの情報も用いているか。 ・ 常に最新の攻撃手法について情報収集を行い、海外の最新情報などを取り入れ、現状の対策で対応できていないことがないかどうかの検討を組織的に行っているか。 ・ SNS などで情報発信する際や、通常業務においても特別な対応を実施する場合には、元となる情報の正確性について一次情報に当たることの重要性を教育研修で伝えているか。 ・ （他のサイバーセキュリティ対策と同様）技術的な対策とモニタリング等の検知が実効性をもっていることを検証しているか。

第 9 位	経済安全保障上の観点からも重要なサイバー攻撃対策
内容	経済安全保障推進法が 2022 年 5 月に成立した。半導体など重要物資のサプライチェーンの確保、基幹インフラ設備の事前審査、先端技術開発、特許の非公開の 4 本柱を中心に、具体的な政策が推進されていく。国会審議で岸田総理がサプライチェーンに対するサイバー攻撃対策の重要性に言及している。この発言は重要物資のサプライチェーンの確保のみを念頭に置いたものではなく、4 本柱のいずれでもサイバー攻撃対策の視点が問われると解釈すべきであり、それぞれの分野での対策が急務である。
監査のポイント	経済安全保障に関しては、経済安全保障推進法（以下、「法律」という）を受けて関係省庁で政省令の整備が進められている。サイバーセキュリティにおけるコンプライアンスの観点から、これらの政省令の内容の把握が組織で系統的に行われ、関連部署にその内容が周知徹底されるかが監査の第一のポイントとなる。第二には法律に準拠するための技術的な対策とその実施状況の点検が行われる体制が整備されているかが監査の対象となる。体制整備のために、必要に応じて社内ルールの整備も行われる。この社内ルールに従った体制の運用が的確にできているかが、今後、重要な監査対象となると予想される。

第 10 位	オープンソースソフトウェアの脆弱性懸念に対する SBOM 普及の期待
内容	Log4j の脆弱性の露呈により、多くのソフトウェアがオープンソースソフトウェアを利用している実態と、オープンソースソフトウェアで脆弱性が発見された時の危険性が強く認識されることになった。そのため米国政府機関では、SBOM（Software Bill Of Materials：ソフトウェア部品表）と呼ばれる制度を導入し、ベンダーが提供するソフトウェアの構成状況を明らかにする取り組みが進行している。 日本でも同様の動きが求められ、ソフトウェア開発や製品ベンダーが自らのソフトウェアの依存関係を明らかにしていくことが想定される。ただし、ソフトウェアのパーツは複雑な依存関係があり、フリーライダーである利用者がその依存関係の開示をオープンソースの作者に要求しても、回答には限界があり混乱を招くことも懸念される。
監査のポイント	Log4j のような汎用のソフトウェアの脆弱性は、多くのユーザが（そしてベンダーが）、自分たちが使っている（開発している）ソフトウェアの構成に無知であることを洗い出した。このような教訓から、自らが扱うソフトウェア資産を把握するために、SBOM という制度が有効とされ、その導入を推進する組織もあると想定されるが、期待されるような成果をあげられるかについては監査する必要がある。 ・ SBOM の仕組みを理解し、その限界を見極めた現実的な使い方が想定されているか。 ・ 開発と運用と脆弱性を理解した SBOM をメンテナンスする要員がアサインされているか。 ・ 実際の脆弱性の発現と、脆弱性の存在とは異なることであることを切り分け、脆弱性評価をする運用の体制があるか。