2024 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	生成AIの悪用と誤用により増加するセキュリティ事故
内容	生成AIは攻撃者を利する手段に使われる。自然言語処理能力を活かしたフィッシング、ビジネスメール詐欺（BEC）、標的型攻撃のためのメール作成はもちろん、コンピュータ言語を駆使したプログラミングによるマルウェア攻撃の自動化と量産化を可能とした。 また、生成AIは攻撃対象ともなる。生成AIの指示文（プロンプト）に対する攻撃により、秘密であるべきマスタープロンプトを露出（プロンプトリーク）、プロンプトを上書きして禁則を破り情報を出力（ジェイルブレイク）させるなどの悪用手法が知られる。 さらには、生成AIの利用はリスクを伴うことを知らなければ誤用になりかねない。入力したデータは生成AI事業者のモデル学習に使われるとするならば、第三者と契約したNDA違反や個人情報の同意なき第三者提供、すなわち情報漏えいに該当する可能性がある。出力された生成物は、第三者の著作権、商標権を侵害する可能性もある。生成AIの利用にあたっては、特定利用者に閉じたデータ利用を保証する契約型と、不特定の利用者に広く開示される約款型の違いを踏まえた利用条件とリスクの正しい理解の普及が待たれる。
監査のポイント	生成 AI の利用者に対する監査の留意点は以下の通り。 ・利用する生成 AI は、指示文（プロンプト）への既知の攻撃に対する脆弱性がないか。 ・生成 AI へのアクセスの認証は、多要素認証等の強固な認証方式によって、なりすまし対策が施されているか。 ・入力したデータが生成 AI のモデル学習に使われる場合、当該データ及び学習したモデルの利用範囲は、当該利用者に限定されるか。または当該利用者以外に公開され共用されるか。 ・利用者が取得している個人情報を生成 AI に入力する場合、当該個人情報の取得時の利用目的を逸脱していないか。また、本人の同意のなく個人情報を生成 AI 事業者に提供することにならないか。 ・NDA（守秘義務契約）により利用者が他者から取得した情報を生成 AI に入力する場合、生成 AI 事業者への情報開示となり、守秘義務違反とならないか。 ・生成 AI が出力した結果を利用する場合、他者の知的財産権（著作権、商標権、意匠権、特許権等）の侵害に該当しないか。

第 2 位	他人事ではありません。日常化するランサムウェア被害
内容	ランサムウェアの被害報告件数は 2022 年には過去最多の 230 件、前年比で 57.5%増加している（出典：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」（PDF））。また、IPA が発表した「情報セキュリティ 10 大脅威 2023」では、3 年連続で組織部門における脅威度 1 位である。 ランサムウェアの被害は大企業だけではなく中小の組織にも及んでいる。中小組織が被災しても、社会的に無視できない影響が生じることがある。例えば、令和 5 年 7 月に生じた名古屋港港運協会の事案では、数日にわたりコンテナ船からの貨物の積み下ろしがストップし、大きな騒ぎとなった。 ランサムウェアの被害はもはや日常化しており他人事と見過ごすことはできない。どの組織でもランサムウェア対策を強化する必要がある。
監査のポイント	経営者がランサムウェア被害を自社の問題と捉えているか、そのリスクを十分理解しているかが、監査のポイントとなる。これは情報セキュリティ監査におけるガバナンス監査であるが、ガバナンス監査の基準は情報セキュリティ監査に含まれないため、ISO/IEC27014 などに基づいて、各々の組織で作成する必要がある。 また、ガバナンス監査は取締役が善管注意義務を果たしているかを対象とした監査であり、その実施者は監査役が望ましい。監査役にランサムウェアの被害の深刻さを理解していただき、取締役監査項目に追加されるようにするのがよいであろう。

第 3 位	国家支援型組織によるサイバー攻撃の深刻化
内容	分断が進む世界情勢の変化を受け、国家の支援を受けた高度なセキュリティスキルを持った組織による攻撃が発生している。これは政府機関や大企業だけを対象とするものではなく、これまで関係ないと思われていた中小企業や自治体なども対象となっている。 軍事的・外交的なプレゼンスを示すことを目的とした攻撃だけでなく、経済的打撃をも意図したサプライチェーンに対する攻撃も確認されている。今後の地政学的な状況の変化によってはさらに攻撃が激化・深化することも予想されるため、国家支援型組織による攻撃の動向を注視していく必要がある。
監査のポイント	国家支援型組織によるサイバー攻撃は、単なる金銭的動機による攻撃とは異なり、戦略的かつ計画的に行われることが多い。こうした攻撃に対しては防御側も戦略的かつ体系的な視点から防御体制を構築する必要があるが、我が国では政府機関においてもそうした体制が十分構築されているとは言えない状況にある。整備・運用状況を監査する立場からは、組織の規模の大小に関わらず高度なサイバー攻撃の対象となりうることを想定し、次のような観点を加味して監査を行うことが望まれる。 ・被監査組織の業務及び利用する情報資産が、サプライチェーン全体を考慮したときに安全保障面または国家戦略的観点からどのような重要性を持ちうるかを認識しているか、また要員に認識させているか。更に、その情報資産の重要性に応じたリスクを認識した上で、適切な管理が実施されているか。 ・攻撃者の利用するサイバーキルチェーンを想定したとき、被監査組織が各フェーズにおいてどのように攻撃を遮断しうるか、また各フェーズでどのようにインシデントレスポンスが可能であるか。 ・被監査組織単独では対処することが困難なサイバー攻撃事案について、外部からまたは公的な支援を受けるための体制が整っているか。

第 4 位	重要インフラを支える供給網（中小企業）がサイバー攻撃ターゲットに
内容	経済安全保障推進法に基づき、2024 年より重要インフラの安定的な提供確保のための施策が本格化する。大手事業者を対象に重要インフラ設備に対する安全性の事前審査制度が開始され、重要インフラを担う大手各社のサイバーセキュリティ対策がさらに向上することが見込まれる。 大手事業者の防御が強化されれば、サイバー攻撃の矛先は大手事業者を支える供給網を構成していながら国から指定を受けなかった中小事業者に向けられ易くなるだろう。大手の重要インフラ事業者と取引のある中小事業者は、無名だから攻撃を免れるということはなく、むしろ攻撃者のターゲットリストの上位にランク入りする十分なリスクがあることを肝に銘じるべきである。
監査のポイント	重要インフラ事業者（大手事業者）及び重要インフラを支える供給者（中小企業等で、業務委託先、部品・材料等の製品、サービスの提供者）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（大手事業者）に対する監査のポイント ➢ 供給者との契約では、セキュリティに対する責任分界と役割が明確か。 ➢ 供給者からの製品・サービス供給停止を想定した BCP（事業継続計画）を策定し、訓練しているか。 ➢ 自社の IT/OT システムに外部から供給者がアクセスできる場合、外部接続のための装置等の脆弱性対策を施しているか、また、外部接続を常に監視し異常を検知できるか。 ➢ 供給者経由でサイバー攻撃を受け、内部に侵入されることを前提としたセキュリティ対策を実施しているか。 ・ 重要インフラを支える供給者（中小企業等）に対する監査のポイント ➢ 経営者は、自社が重要インフラに対するサイバー攻撃の経路であり、標的となりうることを十分自覚しているか。 ➢ 経営者は、サイバー攻撃を受けることを前提としたリスクアセスメントを実施しているか。 ➢ 経営者は、上記リスクアセスメントの結果に基づき、適切なセキュリティ投資を実施しているか。 ➢ 自社から重要インフラ事業者の IT/OT システムにアクセスできる場合、アクセス者の特定及びアクセス状況の監視を実施しているか。

第 5 位	重要性が高まる事前評価， 生成AIのリスク
内容	ChatGPT の利用拡大を契機に生成 AI の業務シーンへの利活用ニーズが急速に高まっている。これらの潮流に対応するため米国でも 2023 年 1 月 26 日に NIST AI リスク管理フレームワーク（AI RMF 1.0）も公開された。 急速に進歩する AI の技術環境や社会環境のなかで、AI を利用した際に発生するリスク評価をまだ正しく実行できていない組織が多く存在するのが実情であり、監査人は最新の正しい知識の下に利用動態から想定されるリスクを評価しなくてはならない。
監査のポイント	生成 AI に関する評価を実施する前にまず監査人は最先端の AI 技術に対する基礎的な知識を少なくとも利用者側と同等かそれ以上には身につけておかなくてはならない。その知識を前提として NIST AI リスク管理フレームワーク（AI RMF 1.0）など既に公開されている公的基準やガイドラインを活用して監査することが望まれる。 現在の状況は 2010 年代初頭におけるクラウドサービスの黎明期と似た状況であり、利用者側、管理者側ともに基礎的なアーキテクチャの理解などなしに利用が推し進められている場合もあるため、情報セキュリティの基本に立ち返った確認が必要である。 NIST AI RMF では AI のリスク管理における以下のようなポイントが定義されており、利用するサービス側の確認のみならず、自組織での利用目的やシステム構築の内容などについても同様に確認しておきたい。 ・客観的な指標を持った有効性と信頼性 ・責任ある設計開発運用や情報提供など安全な運用がなされているか ・セキュリティとレジリエンス ・信頼できる AI であるために説明可能で透明であること ・AI システムのメカニズムが説明可能で解釈可能であること ・プライバシーと個人情報がまもられているか ・有害な偏見や差別などの問題に対処するため公平性が担保されているか

第 6 位	クラウド設定不備によるセキュリティ事故の多発
内容	クラウドサービスの利用の際に各種の設定を誤ることにより情報が外部流出する事故は組織規模の大小を問わず世界中でいまだ数多くのインシデントが報告されている。 クラウドサービスの利用がより拡大する中で、基本的な設定事項が適切に行われているかを定期的に確認することは極めて基本的だが重要な要素である。今日では各プロバイダーからの設定ベストプラクティスはもとより、総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン」や NISC「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル　別冊. クラウド設計・開発編」など公的なドキュメントも公開されており、適切な対応を怠ることは善管注意義務違反規範に問われる可能性も否定できない。
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。ベストプラクティスを提示した公的なドキュメントも公開文書として参照できるようになっているため、これらの文書群の内容への準拠状況の確認と、クラウドサービス提供側で提供されている 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、確認する。監査の実施にあたっては、サービスダッシュボードでリアルタイムに閲覧できるシステムなどを有効に活用し監査手続にも応用することで、公平性や信頼性を高めることができる。監査人は被監査主体が利用するサービスの機能やベストプラクティスを確認し監査を進めたい。 なお、監査のポイントとしては以下の通りである。 ・ 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 7 位	人材の流動化に伴う営業機密の流出増加
内容	人材が流動化し転職することは現在当たり前のこととなっており、競合他社に直接、間接的に移動するようなケースも今や珍しくはない。その際に機密情報を持ち出し利用したことが明るみになることで、転職元企業だけでなく転職先企業にも多大なダメージを与えるようなケースも見られている。 これらの転職先に情報を持ち出すケースは、役職の上下に関わらず、また対象となる情報も、営業・研究開発・生産・顧客情報など多岐にわたる。 対応策として、システム上のアクセス管理を適切に設定するとともに対象となる機密度の高い情報に関してはアクセス履歴も継続的にモニタリングする、退職予定者に対しては特にこのルールを厳格に適用するという事前・事後両面からの対策の徹底が求められる。また従業員自身がどのような場合に罪に問われるか、人生を賭けてまで行うメリットがないことなど研修を通じて周知する意識面からのアプローチも有用である。
監査のポイント	情報セキュリティ監査の観点からは、人材が流動化し入退社が継続的に行われるのは恒常的であることから、全ての人材が機密情報への接触や持ち出しを定常的に制限されているという当然の前提を確認することが求められる。情報の持ち出しは必ずしも退社時の直前に行われるものでないからである。その上での退職時の追加的な対応がなされているかの確認に進むことがよい。 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。 ・ 社内研修や秘密保持誓約書で実効性のある意識付けが行われているか、その際に以下のような観点が含まれていると良い ➢ 機密情報管理の必要性、定義、分類、管理方法 ➢ 罪の意識がないまま行為に至らせない具体的な方法の例示 ➢ 得られるメリットと多額の損害賠償や刑事罰の比較 ➢ 常に見られていることを意識づけるコントロールの例示 ・ 研修の対象者は業務委託、派遣、役員等全ての人材となっているか ・ 機密情報の定義、分類、管理方法が明文化し周知されているか ・ 退職者を含むIDの変更・削除管理が適切にかつ「適時に」行われているか ・ 機密情報へのアクセス権は必要最低限に設定されているか ・ 機密情報へのアクセスログは定期的に監視し、問題のないことを確認しているか

第 8 位	脆弱性管理体制の再検討の加速
内容	セキュリティパッチの適切な適用など基本的な対策の不備による事故が増加しており、脆弱性対策の不備が懸念されている。 深刻な影響が懸念される脆弱性が公表されても、自組織のシステムのどこに該当するソフトが内在されているかが把握できていない、あるいは脆弱性スキャンの結果多くの脆弱性が見つかるがどの脆弱性に重点的に対応すべきかの評価・判断が難しく的確に対応できない、さらには、深刻な脆弱性に対するパッチを当てる作業が業務プロセスに影響を与える恐れがあるのにリスク判断と意思決定の権限と責任の体制が機能しないなど、多くの課題を抱えており迅速な脆弱性対策が取れない組織が増加している。 サイバー攻撃の激化を見込まなければならない中で、脆弱性の報告は増加し続けている。DX が進む中、的確な脆弱性管理の確立に向けて、体制やプロセスの見直しが急務である。
監査のポイント	技術的脆弱性の管理はセキュリティ対策の基本に位置づけられるが、実効性のある管理の仕組みを構築するのが難しいのもまた事実である。この難しさを克服し有効な体制を築くためには、経営者がこの重要性を的確に理解し、自社に必要な管理体制に応分の資源を配分する意思を持たなければならない。そのためには、監査により管理体制の再検討の切り口を明らかにすることが望まれる。 脆弱性管理の監査においては、①現状の脆弱性管理にかかわる規程類の記述と②実際の脆弱性対応の記録とをもとに、関係者のヒアリング等をとおして自社の脆弱性対策としてうまくいっている点と課題点を明らかにするのが望ましいであろう。 その際のポイントに以下の項目が挙げられる。 ・ 定常的な脆弱性管理プロセスが規定され、その権限と責任の所在が明示されているか。各責任者には、その権限と責任の認識があるか ・ 権限と責任の分担がシステム部門やセキュリティ部門だけに偏っていないか、事業部門がリスク判断やその結果責任に的確に関与できているか ・ 緊急性の高い脆弱性への対応に柔軟に対応できる体制になっているか ・ 脆弱性への対応は規定されたプロセスに沿っているか、その対応の記録が整然と保存されているか ・ 認識され高リスクと評価されたが、パッチ適用ができず代替策で乗り切る決定をした未対応の脆弱性が、その後適切にフォローされているか ・ 脆弱性管理プロセスの見直しをするトリガーが決まっているか ・ 脆弱性検査ツールや脆弱性の影響評価手法、脆弱性情報の入手ルートなどが適切に見直されているか

第 9 位	止まらないランサムウェアの進化
内容	攻撃手法としてのランサムウェアは進化し続けており、アンダーグラウンドで提供されている RaaS(Ransomware as a service)やいわゆるノーウェア(非暗号型)ランサムなど、攻撃の手口に変化が見られるようになっている。この背景として、前者は開発者と攻撃者の分業によるビジネスツールとしてのランサムウェアの事業体制が確立していること、後者は暗号化を行わないことで感染を認知されにくいようにすることなどが指摘されている。ランサムウェアに限らず攻撃の脅威は進化していることから、ISO/IEC 27001:2022 でも新たに管理策として加えられた脅威インテリジェンスを活用するなど、組織としていかに脅威に立ち向かうかを考えていく必要がある。
監査のポイント	ランサムウェアの進化に対する監査のポイントは、組織が攻撃手法の変化に追従しうるかを確認するということに他ならない。これに加え、攻撃の対象となりうる機器を把握しているか、攻撃を受けた場合に組織が十分に対応しうるかといった観点についても考慮する必要がある。具体的なポイントには次のようなものがある。 ・脅威及び脆弱性に関する情報を収集し、具体的なセキュリティ対策へのインプットとしているか。 ・アタックサーフェスについて組織としてどのように把握し、攻撃対象となりうる要因を低減しているか。 ・攻撃の兆候をどのように収集し、検知しているか。 ・通常のパターンマッチングでは検知が難しいマルウェアに対し、どのような防御策を講じているか。 ・攻撃を受けた際の復旧策について、事業継続の観点から十分であるか。特にバックアップデータは適時にリストア可能であるか。

第 10 位	経営課題として浮上，サイバー人材育成
内容	各種証明書のコンビニ交付における誤発行など、システム設計のミスによる情報流出事故が相次いでいる。行政サービスの IT 化やビジネスの DX 推進の陰で、IT 人材、セキュリティ人材が慢性的に不足している。システムを設計、構築する IT 業界はもちろん、システム開発を外部に委託する企業側でも、セキュリティを考慮した設計レビューや検収など、一定レベルのセキュリティ知識が必須である。サイバー攻撃への対応などの専門的な人材にとどまらず、セキュリティに素養のある IT 人材も今後ますます重要な存在となっていく。 人材はすぐには育たない。企業経営者がセキュリティ人材を必須の経営資源と捉え計画的に育成しなければ、引き続きセキュリティ考慮不足のサービスやシステムが生み出される恐れがある。
監査のポイント	IT 人材、セキュリティ人材などのサイバー人材は今後も不足する状況が続くと予想される。こうした環境の中でも人材確保を行うためには、経営層も関与した具体的なアクションが必要である。監査のポイントとしては下記がある。 ・ 自社あるいは部門において必要とされるサイバー人材の人材像（職種、スキル定義、人数など）が明確になっているか。 ・ サイバー人材を確保するための具体的な計画（採用、育成、外部委託等）と予算措置がとられているか。また、これらの計画は人事部門、研修部門も関与し、経営層からの支持も得られているか。 ・ システムの設計や開発を外部に委託する場合でも、最低限社内に確保すべきサイバー人材の人材像が明確になっているか。 ・ 自社内で育成する場合には、研修計画、目標とする資格などが明確にされ、また社員自らがサイバー人材を目指すインセンティブの制度（研修費や資格の取得、維持の費用負担、処遇）など、具体的な社内制度が作られているか。