2025 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	組織化、ビジネス化するランサムウェア攻撃
内容	警察庁によると、令和 6 年上半期におけるランサムウェアの被害報告件数は昨年同期よりも高水準で推移している。この背景として、複数の関与者が役割を分担してサイバー攻撃を行うなど、RaaS（Ransomware as a Service）を中心とした攻撃者の裾野の広がりが指摘されている。情報処理サービス業の事例では、金融機関や地方自治体など、150 万件を超える個人情報を含む委託元の情報が流出したことが報告されている。また、KADOKAWA の事例では、25 万人分を超える個人情報や企業情報が流出し、提供するウェブサービスが広く停止したほか、書籍の流通等の事業にも影響が発生した。 ランサムウェアの被害は個別の事業者の被害にとどまらず、サービスの利用者や委託元にも広がる傾向にあり、被害による社会的影響はさらに拡大していくことが想定される。
監査のポイント	ランサムウェアについては攻撃側のエコシステムの変化や被害の拡大が指摘されているところであるが、攻撃自体の手口には大きな変化はない。監査においては攻守双方の視点をもって臨みたい。 一つは攻撃者のサイバーキルチェーンを想定した視点である。多様化するアタックサーフェスを想定した上で、偵察−侵攻−配置−悪用−侵入−潜伏−達成という攻撃のチェーンをどこで断ち切ることができるかが鍵となる。 もう一つは組織におけるインシデントレスポンスの視点である。準備−特定−封じ込め−根絶−復旧−学習という流れにおいて、事業継続の観点も含め、組織が各段階でどのような対応を取りうるか、または外部からの援助を得られるかを確認したい。 これらの二つの視点から、脆弱性やマルウェアへの対策、ログの保管、バックアップのような個々の取り組みの十分性、有効性について確認することがポイントとなる。 警察庁の調査では、ランサムウェア被害を受けた組織の半数弱で内部監査、外部監査いずれかによる情報セキュリティ監査を実施していたとされる。監査を通じたリスクの把握や改善提言の巧拙が被害状況に影響した可能性は否定できない。改めて監査人の役割の大きさ、監査の重要性を認識したい。

第 2 位	国際情勢の不安定化に伴い激化するサイバー攻撃
内容	ロシアによるウクライナへの軍事侵攻やイランとイスラエルの紛争、国際情勢が不安定な状況は今後も継続し、それに伴いサイバー攻撃も増加すると考えられる。2024 年 6 月に発生した JAXA への不正アクセスによる情報漏洩、8 月に発生した KADOKAWA へのランサムウェア攻撃は一例であるが、システム破壊や社会の混乱、金銭要求など、攻撃の目的は様々であり、あらゆる組織、あらゆるデバイスが標的となり得る。政府では「能動的サイバー防御」（アクティブ・サイバー・ディフェンス）の体制を導入する検討も始まっており、民間においてもあらためて組織が取るべき対策を見直す必要がある。
監査のポイント	サイバー空間では政治的、軍事的な活動が積極的に行われている。戦争行為などにも一定のルールが存在するが、サイバー空間の攻撃行為にはルールが存在しない無法地帯となっており、どのような組織であるかは関係なく、無差別に攻撃の標的となっている。また、攻撃の手段や目的も多様化するため、従来よりもリスクアセスメントの対象を広げて検討する必要がある。監査の立場としては、以下のような点について考慮が望まれる。 ・社会情勢の把握や関連組織との積極的な情報交換がなされているか ・情報資産の価値が経済安全保障の観点から検討されているか ・組織がサプライチェーン上どのような役割を持っているか明らかであるか ・破壊的な攻撃などが発生した時の事業継続計画が検討されているか ・重大事案発生時のインシデント対応体制が確立されているか

第 3 位	野放しになっていませんか？急速に普及する AI 利活用
内容	生成 AI（Generative AI）を中心に技術は急速に発展し実社会への適用も進んできている。各組織は対策を実施しているものの、一般ユーザーレベルでも扱えるアウトプット作成の手軽さや適用範囲の拡大、専門家の不足により扱いは後手に回っている。取扱初期は慎重な取り扱いを求めていたマネジメント層も、ニュースでの取り扱いが減ったことにより目線が切られている傾向にある。このような中途半端に慣れた状況においては、誤設定や誤使用に基づく情報漏洩や、プライバシーの侵害、不十分な検証による低品質な製品・サービスが上市されることによるリスクが顕在化し、ブランドや企業に多大な影響を与える可能性がある。
監査のポイント	AI はその対象となる情報や利活用の方法などが日進月歩で移り変わっており、数年前の前提や知識、各種のルールが使えないばかりでなく、むしろ利用促進やセキュリティなどのリスクとなってしまう事すらある。総務省と経済産業省から AI 事業者ガイドライン（第 1.01 版）が令和 6 年 11 月に発出されたが、単にガイドラインの字面を追って形式美を整えているだけではなく、実際にリスクに対して機動的に対応できるよう体制、制度が整っているかを監査で確認する。 主なポイントとしては ・AI の活用により目指すべき社会及びそれを実現するための「基本理念」（why）、並びに原則及び各主体に共通する指針（what）は、関係者間で共有されているか。 ・関連するステークホルダーとの対話やアカウンタビリティを果たすためのプロセスが整備され、運用されているか。 ・組織内のガバナンス・マネジメント文書は、見直される基準が明確に定義され一定のイベントもしくは定期的に見直される運用が実施されているか。特に AI の活用方法の変化（開発者・提供者・利用者）を捉えられる作りになっているか ・「継続的改善に向けた評価の重要ポイントを、経営層が自らの言葉で明示」し、AI の活用と複雑性および組織内のスキルに応じた内部・外部の監査体制が整備運用されているか ・経営者から委託先まで、新規・既存の対象者に関わらず想定される関わり方に応じ、AI に関わる基本的な知識や考え方を最新の状況に維持するような仕組みが作られているか。

第 4 位	AI の攻撃への悪用
内容	かつては絶対に人間が優位だとされていた囲碁や将棋の世界でも今では AI に人間は勝つことができなくなってきた。このように生成 AI は私たちの生活や IT システムの中に組み込まれ、活用の幅が広がっている。サイバー攻撃の世界でもこれは同じであり、偽情報を生成するハルシネーションなど誤情報の拡散はもとより、ビジネスメール詐欺の巧妙化、脆弱性の探知の精緻化、エクスプロイトプログラミングの早期リリースなど悪用の対象は多岐に渡ることが想定される。既知のリスクであってもこれまでの常識だけで対応できるとは限らない世界になっているので、しっかりと最新の情報に基づいた対策が講じられているか監査することが求められる。
監査のポイント	AI に関する監査のポイントを考える際には 2 つの側面からの考慮が求められる。1 つは AI を活用する利用者としての側面、もう 1 つは AI を用いた高度な攻撃等に対応できているかという側面である。 ・利用者の側面では国際標準規格としてAIマネジメントシステム（ISO/IEC 42001）が発行されているため、品質マネジメントシステム（ISO9001）や情報セキュリティマネジメントシステム（ISO/IEC27001）と同様のアプローチによるマネジメントシステムの構築が考慮されているかを確認したい。 これらの規格を採用していない組織においては、2023 年の広島サミットで採択された AI の原則「広島 AI プロセス」の内容を参照できるので、自組織での利用方法や採用しているサービス・システムが広島 AI プロセスで採択された行動規範等に記載された事項に適合しているかなどを監査のポイントとして採用し確認したい。 （https://www.mofa.go.jp/ecm/ec/page5e_000076.html より） ・AI を用いた攻撃に対する対応の側面については、大きなポイントは従来に比べて攻撃側の目的達成までの速度が劇的に向上していることが挙げられる。たとえば Microsoft 社が公開している資料では攻撃者が何らかのアカウントを侵害してから、横移動攻撃により管理者アカウントを搾取、機密情報に到達するまでの時間が 2 時間を切っていると報告している。 （https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023 より） このような状況下では、人間が不審な兆候を探知し、ログを分析して原因を特定するなどといった従来型の対応で、攻撃に対抗する時間的猶予は存在しない。あらゆる機器やアカウントに関する脆弱性を常に監視し、すべてのパッチが適用されているかどうかをリアルタイムで把握するなど,平常時から基本的な所作を確認しておくことが大きなポイントといえよう。

第 5 位	急がれるサプライチェーンセキュリティ対応 ～上流から下流まで一体となって守る取り組み～
内容	昨今の組織的な活動（企業のみならず官公庁も）において、ヒト・モノ・カネ・情報の経営要素に外部委託先やサプライチェーンを使わないケースはほぼ皆無になってきている。また、自動運転やスマートフォンを使ったサービスなどそのチェーンは更に長く複雑になってきている サプライチェーンの中心となる組織が適切にセキュリティ対策を行ったとしても、委託先やサプライチェーンの先でのサイバーインシデントなどが発端となり、サプライチェーン全体に直接・間接的な影響がおよぶことも多い。特に、サプライチェーンの多くを占める中小企業においては、過度なダイエットを行い筋肉量の減った手足のごとく、セキュリティの取り組みに出せるリソースが枯渇しており対応が待ったなしの状況に有る。海外・国内関わらず、情報セキュリティのみならずコンプライアンス的な面でもリスクが高まっている。 社会全体、あるいはサプライチェーンの中核を占める企業が積極的に旗を振りリソースを優先的に配分し、セキュリティレベルを高める取り組みをおこなっていかないと、社会やチェーンが「千丈の堤も螻蟻の穴を以て潰ゆ」ことに繋がってしまう。
監査のポイント	千丈の堤にも例えられるサプライチェーンリスクへの対策については、個社としての取り組みと、サプライチェーン全体を考えた場合の中核となる組織としての取り組みに分け、主に以下の点を監査のポイントとして考えたい。 個社としての取り組みとしては以下の点を中心に確認しておきたい ・サプライチェーンで適用されるガイドラインや法令等を理解し、組織としての対応ができているか。 ・情報資産が棄損された場合を想定したシナリオが検討され、訓練・演習はされているか ・自社のリスク管理の状況は客観的にモニタリングされているか。 ・制度対応や利害関係者への説明責任を果たせるようモニタリング内容の文書化はされているか。 ・委託・提携の終了時点で情報資産の廃棄が行われていることを確認しているか。 サプライチェーンの中核となる組織においては以下の点も含め確認しておきたい ・サプライチェーンを通じたリスク管理をサポートする共通の情報インフラは整備、若しくは計画がされているか ・サプライチェーンを構成する企業間で、取扱い上想定されるリスクなどの認識を合わせるプロセスが整備、若しくは計画がされているか

第 6 位	クラウドサービスに起因した大規模障害によるビジネスリスク
内容	CrowdStrike Falcon に起因する世界規模での障害が発生し、クラウドサービスおよびその関連サービスの障害が全世界に深刻な影響を及ぼすことが明らかになった。外部からのサイバー攻撃、利用しているネットワークの障害、ベンダのアップデートモジュールの不具合など様々な要因により事故は発生する。事業基盤が単一のクラウドサービスに依存してしまうと、サービスの障害発生時において事業継続に大きな影響が出る恐れがあり、マルチクラウドやハイブリッドクラウドの活用も進むと考えられる。システムの複雑性が増す中でクラウド利用者として責任を明確にし、統制の取れた状態でクラウドサービスを利用していくために、より一層監査が重要となる。
監査のポイント	ネットの普及によって、クラウドサービス利用は一般的なものとなった。さらに利用者が意図していなくても他のクラウドサービスが無意識のうちに連携して使われているケースもある。クラウドを使ったシステムの責任範囲はクラウドサービス提供者とクラウドサービス利用者に分かれている。クラウドサービスの障害に対して、利用者が出来ること・やるべきことを認識し、適切に行うことが重要である。監査の立場としては、以下のような点について考慮が望まれる。 ・クラウドサービス提供者の責任範囲を明確に理解しているか ・クラウドサービスの障害などにおける事業継続計画が検討されているか ・クラウドサービスの利用状況について継続的な監視を行っているか ・システム障害時の影響範囲を明確にできているか ・ベンダーロックインに対する対策が検討されているか

第 7 位	サイバー人材不足が引き起こす経営リスクの増加
内容	サイバー人材、とりわけサイバーセキュリティの人材不足が深刻化している。経済産業省の「DX レポート」で述べられた「2025 年の崖」の年を迎え、レガシーシステムの刷新も急務となる。また複雑化する脅威に対抗するためには複数の製品・サービスを多層に組み合わせる必要がある。しかしながら現実には、隙のないセキュアなシステムの設計や実装運用を行える人材が確保できず、万が一を想定していないシステムが乱造され、またサイバー攻撃の被害に遭った際の対応に手間取ることで、企業経営にまで影響する事案が増え、ネット社会全体のサイバーリスクが増大する。
監査のポイント	サイバー人材育成は昨年度の十大トレンドでもトピックに取り上げられているテーマであり、継続して改善が求められている状況にある。人材育成は短期で解決できるものではなく中長期の経営課題として本腰を入れて取り組むべきテーマである。監査のポイントとしては下記がある。 ・サイバー人材の育成が経営課題として位置づけられ、育成計画が立案されているか。 ・サイバー人材育成計画には、目標とする人材像（職種、スキル定義、人数など）が明確になっているか。 ・目標を達成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。 ・情報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。

第 8 位	進まない DX 化　～「2025 年の崖」から転落するリスク～
内容	経済産業省は 2018 年 DX レポートで、2025 年までに DX を推進しない場合、わが国全体で最大年 12 兆円の損失が生じる「2025 年の崖」を指摘した。DX に失敗した企業は、デジタル競争の敗者、技術的負債の増加、サイバーセキュリティの3つのリスクを負う。セキュリティを含む IT 人材不足や、重要なプログラムのサポート終了などが背景にあり、システムの脆弱性対策が困難になるのだ。 2025 年 10 月に Windows10 の一般的なサポート終了を控えている中で、DX に乗り遅れた企業は「2025 年の崖」から転落し、企業の衰退とそれを助長するサイバーリスクにさらされる。
監査のポイント	2025 年の崖への対応について、企業の状況について、情報セキュリティ監査としては二つの局面に分けて監査主題を設定する必要がある。 ・DX に取り組んでいる、あるいはこれから取り組むという局面においては、DX の前提となる基盤やアプリケーションの選択が適切であるかが監査主題となる。DX においてはクラウドサービスの利用が一般的であるので、安全性の高いクラウドサービスを選択すると共に、選択したクラウドサービスを前提とした組織のセキュリティ対策が想定されるリスクに対応できるかを監査する必要がある。監査の基準としては、情報セキュリティ管理基準に加えて、ISO/IEC27017 に基づく「クラウド情報セキュリティ管理基準」や ISO/IEC27036-4 を参照基準として用いることができる。 ・DX に対応できていない場合には、レガシーのまま運用せざるを得ないシステム、サポート切れのシステムに対する安全対策が有効かを監査する必要がある。具体的には、当該システムに係るネットワークセキュリティやモニタリング、及びインシデント対応などが重点となる。

第 9 位	急がれるサイバー安全保障への備え ～ 指定事業者の委託先も無縁ではいられない ～
内容	サイバー安全保障分野における法制度の整備、運用強化が進む。既に経済安全保障推進法は 2024 年 5 月に施行され、特定重要設備のセキュリティ等のリスク管理措置は特定社会基盤事業者のみならず、委託の相手方及び再委託の相手方にも及んでいる。重要経済安保情報保護活用法は 2025 年 5 月までに施行予定であり、民間事業者に政府から機微な情報が共有される場合には、民間事業者に対する情報保全体制の確認（セキュリティ・クリアランス）も実施される。さらにサイバー安全保障分野における情報収集・分析能力の強化、能動的サイバー防御のための体制整備に向けた検討が進んでおり、民間事業者がサイバー攻撃を受けた場合の政府への情報提供を求める立法化が議論されている。民間事業者は、サプライチェーンセキュリティの強化、従業員個人と事業施設のクリアランス対応、サイバー攻撃に関する情報提供等の法的義務への備えが急がれる。
監査のポイント	サイバー安全保障の対象となる民間事業者に特定社会基盤事業者を含む重要インフラ事業者が指定されるとするならば、政府が示した特定重要設備に対するリスク管理措置の考え方が参考になる。特定重要設備（以下、「設備」という）の重要維持管理（以下、「管理」という）を委託する場合の監査のポイントは以下の通り。 （ https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_setsumeikai.pdf より） ・委託された管理等の実施に当たり、委託（再委託を含む）先によって、設備について事業者が意図しない変更が加えられることを防止するために必要な管理等がなされ、その管理等に関する事項を指定事業者が確認できることを契約等により担保しているか。 ・管理等の再委託が行われる場合においては、再委託先のサイバーセキュリティ対策の実施状況を確認するために必要な情報が、再委託先を通じて指定事業者に提供され、また、再委託を行うことについてあらかじめ指定事業者の承認を受けることが契約等により担保されているか。 ・指定事業者が、委託先が契約に反して管理等の役務の提供を中断又は停止するおそれがないかを確認しているか。 ・指定事業者が、設備の供給者や委託（再委託を含む）先について、過去の実績を含め、我が国の法令や国際的に受け入れられた基準等の遵守状況を確認しているか。 ・指定事業者が、設備の供給や委託（再委託を含む）した管理等の適切性について、国際的な法的環境等により影響を受けるものではないことを確認しているか。 ・指定事業者が、設備の供給者や委託（再委託を含む）先に関して、国際的な影響を判断するに資する情報の提供が受けられることを契約等により担保しているか。また、契約締結後も当該情報について変更があった場合に、適時に情報提供を受けられることを契約等により担保しているか。

第 10 位	急速な ID の集約化がもたらす被害拡大
内容	マイナ保険証のように、複数の ID が1つの ID に集約される動きが進む。ビジネスにおいても、ユーザの利便性向上や顧客の囲い込みのため、「ポイント経済圏」に象徴されるような各種会員 ID の統合やフェデレーションが加速する。反面、1つの識別・認証情報が漏れると芋づる式に被害が拡大するリスクもある。多要素認証など強固な認証手段を用いないシステムで被害が広範囲に及ぶセキュリティ事故が増加する。
監査のポイント	識別・認証のためのデータの保護を強化することに加え、強固な認証方式をユーザに提供する必要がある。監査のポイントとしては下記がある。 ・ユーザ ID としてメールアドレス等推測されやすいものを用いていないか。 ・パスワードを平文で保存せず、安全な方式でハッシュ化されているか。 ・パスワードとしてパスフレーズを用いるユーザのために、十分な長さのパスワードを設定できる仕様としているか。 ・ユーザが脆弱なパスワード（ID と同じ文字列など）を設定しないようガイドする仕組みを設けているか。 ・多要素認証など、より強固な認証手段を提供しているか。 ・複数システム間での認証連携の仕組みとして要求されるレベルの安全性が確認されている方式を導入しているか。 ・ネットワークを流れる識別・認証情報は全て暗号化された通信で行われる仕様となっているか。 ・識別・認証情報が保存されているデータベースへの不正なアクセス（内部者を含む）を検知する仕組みが講じられているか。 ・ログイン通知をユーザに送付する、リスクベースで認証を行うなど、不正な利用に気付ける仕組みを設けているか。