2026 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	ランサムウェア被害の広がりと深刻化
内容	警察庁によると、令和 7 年上半期におけるランサムウェアの被害報告件数は 116 件に上り、半期の件数としては令和 4 年下半期と並び最多となっている。 商品の流通に大きな影響が発生したこともあり、ビール・飲料会社やビジネス用品通販業者など大手企業の被害が記憶に新しいが、上半期の統計では中小企業の被害が 77 件と約 3 分の 2 を占めており件数・割合ともに過去最多となっていることにも留意したい。RaaS の利用や、複数の関与者が攻撃の役割を分担するなど攻撃実行者の裾野が広がっており、このことが、比較的対策が手薄な中小企業の被害増加につながっていると考えられる。 規模の大小を問わず、サプライチェーンリスクの観点からも、攻撃グループの増加、多重の脅迫やノーウェアランサムの増加など攻撃動向を引き続き注視していく必要がある。
監査のポイント	ランサムウェアの被害が依然として拡大しつつある中、監査には攻守双方の視点を持って臨みたいという点には変わりはないが、最近公表されたランサムウェアの被害事例からは、監査にも深い洞察と幅広い対応が求められているように思われる。 攻撃者のサイバーキルチェーンを想定した視点からは、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。単に EDR やゼロトラストといったソリューションを導入していればそれで良しとするのではなく、脆弱性対策、業務上のデータフロー、管理者権限の運用など、あらゆる視点からランサムウェアの被害につながる兆候がないかを確認することが求められる。 また、組織におけるインシデントレスポンスの視点においては、バックアップ・リストア及び BCP の有効性について確認することが望まれる。我々監査人の立場としても、組織が被害を受けた際、サプライチェーンに与える影響を最小化するための「復旧力（レジリエンス）」が問われていることを改めて認識しておきたい。

第2位	誤用から悪用へと広がる AI リスク
内容	生成 AI の利用が進む一方で、その誤用や悪用によるリスクも急拡大している。誤用によるリスクは、AI 技術の理解不足や不適切な運用により、意図せず誤って顕在化するリスクを指す。例えば、入力情報が再学習されることを理解せず、生成 AI に機密情報を入力した結果、第三者に機密情報が漏えいするリスクや、出力結果を検証せずに誤情報や著作権等の知財権侵害となる情報を用いるリスクなどが挙げられる。悪用によるリスクは、悪意をもって AI 技術が用いられ、不正な目的が達成されるリスクである。例えば、フィッシングメール作成やマルウェア開発、攻撃ターゲットの脆弱性探索などのサイバー攻撃プロセスの省力化・効率化・自動化、偽情報の生成・拡散、ディープフェイクによるなりすましによる被害拡大のリスクなどが挙げられる。
監査のポイント	生成 AI を利用する組織に対する監査のポイントは以下の通り。 - 生成 AI の利用に関する方針を定めているか。 - 生成 AI の利用に関するリスク評価を実施しているか。 - 生成 AI のリスク評価は、入力情報の機密性（組織外への漏洩など）に関わるリスクと出力情報の完全性（誤情報、他者の権利侵害など）に関わるリスクの双方を評価しているか。 - 生成 AI の利用に関する方針・リスク評価に基づき、リスク対応策を定めているか。 - 策定した生成 AI のリスク対応策は社会的に妥当と認められる基準に照らして適切か。 - 策定した生成 AI のリスク対応策は組織内で正しく実行されているかを確かめることが可能か。 一方、生成 AI を悪用され、サイバー攻撃のターゲットとなる側の組織にとっては、攻撃手段が生成 AI かどうかは本質的な課題ではない。従来通り、サイバー攻撃に対する管理策の整備・運用について監査することになる。ただし、これまで以上に攻撃の量・速度が増し、攻撃の質の高度化・巧妙化が進むことが予想されるため、防御する側の組織も対応の量や質を見直す必要がある。そのため、生成 AI を悪用され、攻撃対象となりうる組織に対する監査のポイントは以下の通り。 - サイバー攻撃が従来以上に激化することを想定したリスク評価の見直しをしているか。 - リスク評価の見直しに見合った、サイバー攻撃対策を策定し、必要な投資（人的・物的）をしているか。

第3位	標的型攻撃の激化と被害拡大
内容	特定の組織を標的とし、その組織に適した攻撃手段を組み合わせ、内部情報の窃取などを行う標的型攻撃は現在も継続的に行われ、大きな脅威となっている。メールや VPN 装置が攻撃の入口となっており、侵入後も長期にわたって組織内に留まるため、外部との接続面が適切に運用されているか、内部システムの監視が行われているか、持続的に攻撃が行われていることを前提としたセキュリティ対策が行われているか、等を意識して監査を行う必要がある。
監査のポイント	標的型攻撃に用いられる攻撃手法は巧妙かつ複雑で、ゼロデイ攻撃などと組み合わされる場合、発見が困難な場合も多い。さらに、組織内部のシステムに侵入後、特殊なプログラムを動作させずとも、通常利用可能なコマンドなどを使用し一般的な操作を装う、一度に大量のデータを流さないなど、異常動作の検出を逃れるような手法も取られる。 検出は困難な場合も多いが、監査を行う場合は、以下の点に注意が必要と思われる。 - 外部からの攻撃面となりうる部分に対して適切なセキュリティ対策を行っているか。 - 内部システムを監視しているか。 - 異常動作や異常通信だけではなく、正常動作や正常通信について監視や記録の取得を行っているか。 - システムオペレーションの詳細な記録が行われているか。 - オペレーションの記録と、システムで記録されている内容の整合性を定期的にチェックしているか。 - 攻撃発生時に流出データや影響範囲の特定に寄与する仕組みが導入されている　　か。 - 攻撃発生時に適切に対処する体制が構築されているか。

第4位	サイバーセキュリティ対策への AI 活用の本格化
内容	サイバー攻撃において AI 技術の利用が進むことにより、攻撃は益々、増加し、かつ巧妙になっていく。一方、サイバー攻撃に対する防御側の対策にも AI 技術の活用は進み、今や欠かせないものになっている。例えば、システムの脆弱性検知、不正アクセス・ふるまい検知、ID・アカウント管理、インシデントレスポンスなど、従来はセキュリティ担当者が人手をかけて実施していた大量の業務が AI により自動化、高速化され、または高度セキュリティ技術者を適切に支援できるようになっている。情報セキュリティ監査においても生成 AI の利用が進み、監査業務の一部を担う、または監査人を支援するようになるだろう。
監査のポイント	監査人が注目すべきは「AI を導入しているか」ではなく、「AI が実際に検知・防御力向上に機能しているか」である。具体的には、 - AI が不審通信・挙動・IoC 等を常時分析し、従来見逃していた攻撃を検知できているか。 - ランサムウェアやフィッシング等への対応が AI により自動化・高速化されているか。 - 検知結果から封じ込め・遮断までの対応フローが自動連携されているか。 - 誤検知の頻度や分析精度がモニタリングされ、性能が継続的に改善されているか。 - 人手不足を補う形で運用負荷が軽減されているか。 を確認すべきである。 さらに、攻撃側の AI 活用を想定した高度な検知（多言語解析・行動分析等）が構成要件に含まれているか、既存対策と分断されず全体最適で運用されているかも重要な監査観点である。加えて経済安全保障の観点から脅威インテリジェンス等をサイバー防御にも適用していくことが政府からも示されている。したがって、AI を「導入目的の明確な検知・防衛手段」として統制下で活用できているかが評価の軸となる。

第5位	市場から締め出しの恐れ ～サプライチェーンセキュリティ対策の格付け開始
内容	サプライチェーンを対象としたサイバー攻撃の激化により、操業が停止するなど被害が拡大している。これに対応するため、2026 年度から経済産業省の「サプライチェーン企業のセキュリティ対策評価制度」が開始される。企業のサイバーセキュリティ対策を評価し、格付けする制度である。調達企業は新しい評価制度を生かしたサプライヤの選別を進めるため、サプライヤとして納品先の企業が求める格付けを取得しなければ取引ができなくなる恐れがある。
監査のポイント	サプライチェーン強化に向けたセキュリティ対策評価制度（中間報告）では、対策基準として Basic（★★★）25 項目、Standard（★★★★）44 項目が示されている。この基準に基づいて対策を実装し、運用しておくことが必要となる。その上で、Standard は外部機関の評価を受ける必要がある。この評価は費用が掛かると考えられるので、事前に自己評価で外部機関の評価で適合となるようにしておくことが望ましい。このために、内部監査で適合性を評価するとよい。Basic は Security Action（★、★★）の上に位置づく水準であり、自己評価で基準に準拠したことを表明できる。ただし、その評価が適正であることを説明できるようにするには、適切な内部監査を実施することが望ましい。

第6位	組織が本腰を入れて取り組むべき AI ガバナンスの確立と対外公表
内容	AI は組織の意思決定や業務に広く使われ、今や組織活動に欠かせないものになった。その一方で、特に LLM の出力に誤り、差別、バイアスなどが含まれたまま出力結果を利用すると倫理や法上の問題を惹き起こし、組織の信用失墜や係争に発展しかねないリスクをはらんでいる。こうした AI 利用に関わる組織のリスクに対応するため、国内外の AI 関連法規制（AI 推進法、EU AI Act など）・ガイドライン（AI 事業者ガイドライン、NIST AI RM など）や国際規格（ISO/IEC 42001）の制定が相次いでいる。AI を利活用する事業者は自組織の AI ガバナンスの確立と説明責任をはたす対外公表のために、これら法規制の遵守、国際規格等への準拠が益々、求められるようになる。
監査のポイント	AI を利活用する事業者に対する監査のポイントは以下の通り。 - 事業領域（国内外のすべて）において遵守すべき AI 関連の法令、規制及び契約上の要求事項、並びに倫理上の要請を特定しているか。 - 特定された要求事項、倫理上の要請を考慮して、必要な管理策を整備・運用しているか。 - 整備・運用する管理策は、AI 関連の国際規格や公的なガイドラインに準拠するなど、社会的に妥当と認められるか。 - 経営者は AI 利活用に対する自らの姿勢を、利害関係者または社会に対して説明する責任を自覚しているか。 - 利害関係者または社会に対する説明責任を果たすための対外公表の在り方・手段は適切かつ十分か。

第7位	国家レベルの攻撃者が事業者にサイバー攻撃を仕掛ける時代の到来
内容	地政学リスクにかかわる安全保障分野は国際経済とそれを支えるサイバー空間へ広がり、ついに能動的サイバー防御法が 2025 年 5 月 16 日に成立した。奇しくも同日、昨年公布された重要経済安保情報保護活用法の施行を迎えた。これにより既に施行済みの経済安全保障推進法と合わせ、経済安全保障関連の重要 3 法令が出揃った。2025 年 7 月 31 日現在、15 分野の指定済み基幹インフラ事業者数は既に 257（自治体を含む）にも及ぶ。指定事業者にはセキュリティ管理措置が要求されるだけでなく、政府から機微な情報共有を受ける場合にはさらにセキュリティ・クリアランスも実施される。国の要求は指定事業者のみならず、当該事業者から業務を請負う委託先、再委託先、再々委託先といった裾野の広がるサプライチェーン全体に及び得る。これらサプライチェーンを担う事業者は、国の要求に応じたセキュリティ管理、クリアランス、情報提供体制の整備等の取組みをしなければならない。これを裏返せば、国家レベルの攻撃者が一事業者にサイバー攻撃を仕掛ける時代が到来しており、個々の事業者のサイバーセキュリティがナショナルセキュリティ（国家安全保障）に直結することを意味する。
監査のポイント	経済安全保障関連 3 法の成立を受け、サイバーセキュリティは国家安全保障に直結する重要課題となった。これに伴い、情報セキュリティ監査人は以下の点に注目していく必要がある。 第一にサプライチェーン全体の防御力が保たれているかを確認したい。国家が支援する攻撃者は、最も脆弱な委託先や内部者を侵入口とする場合が多い。そのため、社内を含めたサプライチェーン全体のリスク評価と管理体制を監査の重点対象とする。物流のみならず情報流や金流にも留意するとともに、誰がチェーンそのものを管理し、チェーンを構成している各社はそれぞれが担う役割を全うしているかといった 組織を跨いだマネジメントの面で問題ないかの検証も有用である。 第二に実践的攻撃に対する「実効性」を検証したい。特に、未知の脆弱性を突くゼロデイ攻撃や巧妙な標的型攻撃を想定した攻撃演習（レッドチーム演習）が行われているか、その結果を可能な範囲で独立評価する。規程遵守などの形式美を整えるだけでなく、実際に攻撃を検知・防御し、国の能動的サイバー防御と迅速に連携できているかを厳しく検証することが重要である。

第8位	クラウドサービスの大規模障害は社会的混乱につながるおそれ
内容	クラウドサービスは最早社会インフラといっても良いほど普及し、企業内外のコラボレーションや基幹業務まで多岐に及ぶ領域で使用されている。その反面、データセンタやリージョン単位などの大規模障害の際には、被害の当事者だけではなく、その取引先など幅広い範囲に影響を及ぼし、広範囲でのビジネスの中断といった社会的混乱につながる場合がある。
監査のポイント	クラウドサービスはビジネスにおけるライフラインであり、さらにはクラウドサービスのサプライチェーンにより、認識していなかったクラウドサービスの障害が利用中のクラウドサービスに影響を及ぼす場合もある。また、SLA に規定された稼働率を超えていた場合でも、障害発生のタイミングによって組織に与える実際の影響は大きく変動する。監査のポイントとしては以下のような点を考慮することが望ましい。 - ビジネス上の要求に基づき、Availability Zone の利用、複数リージョンへのデータ分散やフェイルオーバー設計を含んだ可用性の確保ができているか。 - 障害発生時の切り分け及びクラウド事業者の責任範囲を踏まえた運用体制になっているか。 - システム障害時の影響範囲を取引先への影響含め明確にできているか。 - クラウドサービスの利用状況を継続的に監視しているか。 - 事業継続計画（BCP）：クラウドの障害が長期にわたる際の業務継続手順が BCP に含まれているか。

第9位	サイバーセキュリティ人材の不足がもたらす事故の多発
内容	サイバーセキュリティ人材が不足する状況が続いている。DX の推進や情報システムのクラウド化の推進に伴い、情報システムの開発を情報システム部門ではなく、ビジネス部門で行うことも増えている。クラウドシステムの適切なセキュリティ機能の利用、サイバー空間における脅威の変化、AI 活用のリスクなどビジネス部門で求められるセキュリティ人材を計画的に育成していないことにより、脆弱なシステムが乱造されセキュリティ事故が多発する。
監査のポイント	サイバーセキュリティ人材の育成は、この十大トレンドで継続的に課題となっているトピックである。特に、情報システムの開発をビジネス部門が主体となって行う企業においては、ビジネス部門においてもサイバーリスクに精通した人材が必要となる。監査人は下記のポイントを押さえ必要な助言を行うべきである。 - サイバーセキュリティ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。 - 情報システム部門、情報セキュリティ部門のみならず、ビジネス部門においても必要とされる人材像が定義され、人材育成計画が策定されているか。 - その人材像にはDX、クラウド、AI利活用、個人情報保護やその他の制度の変更など、進展するサイバー空間上のリスクへの対応が考慮されているか。 - 人材を確保するための具体的な計画（育成、採用、外部委託等）があり、必要な予算措置がとられているか。 - 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、具体的な社内制度（研修費や資格の取得、維持の費用負担、処遇など）が作られているか。 また、監査人においても昨今のサイバーリスクに対応できるよう、自らスキル向上の機会を獲得する必要がある。

第10位	利用者の知識不足が生み出すクラウドサービス利用インシデント
内容	クラウドサービスも生成 AI も、その便利さゆえに市場が急激に拡大している。安易な禁止はかえってシャドーIT による様々なリスクを引き起こす。また、利用に際して、適切なセキュリティ設定ができていないことで、意図しない情報公開による機微情報の漏洩も継続的に発生している。 組織としては、契約したサービスについてどのような利用を許容するか適切なガイドラインの整備が求められる。それは情報の取り扱いやユースケースだけではなく、適切なセキュリティ設定を含む構成管理や継続的な態勢管理が求められる。
監査のポイント	外部サービスのための導入・利用に関するガイドラインが整備されているか。また、利用にあたっては、サービスを安全に利用するために、構成管理の不備を引き起こさないための仕組みが整備・運用されているかを確認する必要がある。 また、組織の機密情報および、自社又は第三者の権利を侵害する情報の意図しない処理を行わないために、情報の適切なラベリングの実施および、適切な権限を有していないユーザーによる処理を抑止することが望ましい。監査においてはポリシー・ルール有無だけではなく、従業員への教育、技術的対策も含めた有効性の評価が必要になると考えられる。