表題 1	自然災害による IT 被害の拡大
内容	2018 年に大阪北部地震や西日本豪雨による広域災害、北海道胆振東部地震によるブラックアウト、2019 年には台風 15 号による千葉県南部の長期間停電や台風 19 号による広域水害が起きた。度重なる自然災害は物理的な被害を通じ、IT インフラに必須の電力インフラや地域のライフラインを傷つける。自社の重要 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見積もっているか、IT の自然災害リスクに対する対策や業務継続の実効性確保ができているかなどといったことに対する評価ニーズが高まる。
監査のポイント	・ 自社の IT インフラ環境の概要が情報として継続的に収集され、整理され管理される仕組みがあり、運用されているか。 ・ 上記 IT インフラの情報の中にクラウドを含む IT 委託先の情報も含まれており、情報が自社環境と同様に更新される仕組みが運用されているか。 ・ クラウドを利用している場合地理的冗長化が検討・実装されているか。 ・ 電気・水道等の公共サービスに関するリスクアセスメントが定期的に行われ、対象リスクの中に自然災害が含まれているか。含まれている場合、昨今の自然災害リスクの高まりを踏まえて前提条件が見直されているか。 ・ IT-BCP の見直しがリスクアセスメントの実施と連動して行われているか。また、その訓練は定期的に行われているか。 自社の評価に加えて、サプライチェーンの川上川下とも上記のような情報を連携し、チェーン全体での対策が一定水準になることまで確認できることが望ましい。
表題 2	**クラウド・バイ・デフォルト時代の新しい安全性評価制度の開始**
内容	政府機関においても「クラウド・バイ・デフォルト」が本格化し、日本版 FedRAMP ともいえるクラウドサービスの安全性評価制度が 2020 年秋からスタートする計画となっている。これまで統一指針のなかったクラウドサービスの採用に関する指標や管理策・監査基準が示されることで、政府機関のみならず民間企業においても、指針に則したクラウド・バイ・デフォルトの時代の情報セキュリティ対策実施が必要となってくる。
監査のポイント	【クラウド事業者】 ・ 政府のクラウド安全性評価の管理基準（2020 年春公開の見通し）にそった管理策の実装が行われているか。 ・ 経営者の言明のために、サプライチェーンを含む他のクラウドサービス及び利用者との責任分界点が明確になっているか。 【クラウド利用者】 ・ クラウド事業者の監査報告書を読み込める知識を持つ人材の育成がなされているか。 ・ クラウド利用のためのセキュリティ体制（クラウド事業者からの情報の確認や対応）が整備されているか。 ※政府の管理基準も ISO/IEC27017 ベースであるため、同規格に基づく監査が必要となる

表題 3	クラウドサービスの障害による大規模なビジネス影響
内容	黎明期には有象無象に存在したクラウドサービスたちも、競争を経て選択肢が上位サービスにシェアが集中する状況へと変化してきている。このような状況下でひとたびクラウドサービスのインフラに大規模障害が発生すると、連鎖して数多くのサービスが影響を受けてサービス停止する事象が既に発生している。直接契約しているサービスのみならず、サプライチェーンまでを含めた影響を検討することが必要な時代となった。
監査のポイント	【クラウド利用者】 本事象は可用性の確保をテーマとして、以下の観点から BC/DR や障害対策を、主には SLA の確認や実稼働データから確認する。 ・複数のデータセンター（DC）で稼働しているか否か ・DC の地域分散はなされているか ・主系従系への切り替えはどのように行われているか ・バックアップセンターは存在するかなど ・障害発生時の自らの対策が有効かということも確認する。
表題 4	DX 化の進展によりさらに加速するセキュリティ人材不足
内容	セキュリティ人材の不足が叫ばれて久しい。各種の調査でもこれを課題とする組織が多い状況が続いており、人材不足は一向に改善しない。特にビジネスの IT 化、DX（デジタルトランスフォーメーション）化が進む中では、セキュリティ人材は情報セキュリティ部門、情報システム部門だけではなく、ビジネスを企画し運営する事業部門にも必要とされている。事業部門においても必須の人材としてセキュリティ人材を位置づけ、戦略的、集中的に育成しなければ、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	・DX 事業を推進する事業部門側で、必要とする情報セキュリティ人材の人材像（スキル、人数等）が定義にされているか。 ・定義された人材像の人材を確保できているか。 ・確保できていない場合、体制整備の計画（外部研修の受講、採用等）が立てられているか。また体制が整備されるまでの間の暫定的な措置が講じられているか。
表題 5	働き方改革の推進普及による新たな脅威の発生
内容	政府の推進する働き方改革は先鋭的な企業のみならず、多くの企業において制度化され、裁量労働の拡大やテレワークなどが実施される環境となった。地震や洪水被害など自然災害による出社困難時の対応も大きな課題となる中で、2020 年には東京オリンピックの開催本番となり、より一層この流れは加速するものと考えられる。この流れの中で、情報漏洩への対策や端末管理などの情報セキュリティ対策や従業員教育など、情報が物理的境界に閉じない新しい時代に即した規範や情報セキュリティ管理策モデルの構築が急務となっている。
監査のポイント	・テレワーク等に適したセキュリティアーキテクチャの実装とそれに見合った管理策の実装がなされているか（境界型防御からゼロトラストセキュリティへの対応等）。 ・必要な対策が確実に行われていることをできるだけリアルタイムに検知確認できる体制が確立しているか（厖大化するログの確認ができているか等）

表題 6	プライバシー保護の国際標準化に乗り遅れる日本企業
内容	個人情報、プライバシー保護に関して 2019 年 8 月に ISO/IEC27701 が国際標準化され、公開された。ISMS の延長線でも個人データ保護の管理が行えるようになることから、この標準規格の実装による監査ニーズが高まると予想される。一方で肝心の GDPR をはじめとする各国法規制に対する日本企業の動きは遅く、今後強化されるこれら対策への遅れから、制裁金を科される企業が発生する懸念がある。また、日本独自規格であるプライバシーマーク制度も含めた関連認証制度の動向も注目される。
監査のポイント	・進出先各国、グループ本社は法規制動向の把握を継続的に行う体制を構築し、運用しているか。 ・各国拠点、地域中核拠点、グループ本社のいずれかに、各国現地法対応としてのデータ保護管理方針、体制、規程、手順は策定され、適時に改訂される仕組みがあるか。また運用されているか。 ・グループ横断的なデータ保護管理方針、体制、規程、手順が、地域中核拠点、あるいはグループ本社において、グローバルの動向を加味して、作成され適時に改訂され運用されているか。 ・プライバシー情報の洗い出しはサプライチェーンを意識した形で行われているか。 ・適切な運用がされていることを担保するモニタリングの取り組みは有効に機能しているか。 ※全体的な取り組みの監査に加えて、上記のような重要な領域に関しては個別の対策が十分に整備・運用されていることの確認が求められる。
表題 7	サプライチェーンの透明化で求められるセキュリティ対策の強化
内容	標的とする企業よりもセキュリティレベルの低い取引先、関係会社等に侵入し、情報を窃取してから標的企業を攻撃する「サプライチェーン攻撃」が増えている。その一方で、BCP やサプライチェーン管理の観点からサプライチェーン全体の透明性が求められる。サプライチェーンの実態が明確になり、公にでもなれば、それは攻撃者にとっても有用な情報となり、サプライチェーン攻撃を助長しかねない。より巧妙さを増す攻撃に備えるためのセキュリティ対策がさらに求められるようになる。
監査のポイント	標的型攻撃に対する監査のポイントに加えて、さらに以下の確認が求められる。 ・サプライチェーンを形成する取引先、関係会社等の情報が公になっているか。 ・取引先、関係会社等と自社とが連絡を取り合う互いの担当部署がどこか、第三者が容易に推知できる状態か。 ・取引先、関係会社等に対して自社の情報システム及びセキュリティ対策に関わる情報が不必要に開示されていないか。 ・取引先、関係会社等との情報のやり取りに関わる合意した取決めはあるか。 ・その取決めは、取引先、関係会社等のセキュリティレベルが自社よりも低いことを前提としているか。 ・取引先、関係会社等との情報のやり取りにおいて、なりすましへの対策（予防、検知）等の情報セキュリティへの配慮は十分か。 ・取引先、関係会社等と自社を直接接続する通信経路がある場合、悪意の第三者が当該通信経路を使用することを前提にセキュリティ対策を立てているか。

表題 8	標的型ランサムウェアで倒産危機？ システム全てが人質に
内容	従来型のランサムウェアとは異なり、システムに侵入後にビジネス上重要なサーバを狙ってランサムウェアを仕掛け、ビジネス全体を「人質」にとる標的型ランサムウェアが世界中で増加している。もし狙われて攻撃されたら、被害を受けた複数台のサーバの復元コストや、ビジネスの停止による損失など、その被害の甚大さに倒産してしまう企業も出てくるかもしれない。
監査のポイント	· ウイルス対策の基本的な設定(最低限週に一回のフルスキャンの実施・毎日のシステムスキャンの実施・適切なパターンの更新)と、基本的な運用(スキャン結果の解析によるリスクの分析)が行われているか。 · サーバに端末よりレベルの高いウイルス対策を行っているか。 · サーバはリアルタイムで異常監視を行っているか。 · 拡散に使われる脆弱性(SMB の脆弱性や、管理共有)は対策されているか。 · 侵入・改ざんされない方法でバックアップが取得されているか。
表題 9	**クラウドサービスの管理・設定ミスによる情報漏洩**
内容	2019 年にも広くビジネスシーンで利用されていたクラウドサービスにおいて、設定ミスにより情報が大量に流出する事案が発生した。各ビジネス部門が各々でクラウドサービスを契約し利用する形態が広まっていることから、組織全体での情報セキュリティに関するポリシーやガバナンスの徹底などが課題となってくる。
監査のポイント	· 組織の情報セキュリティ責任者が、組織内で利用している全てのクラウドサービス資源の状況を把握できている体制になっているか。 · クラウド利用ポリシーやクラウドサービスに適したセキュリティポリシーが定められているか。 · 組織のポリシーが全ての資源に対して適用されているかを確実に確認できるシステム体制がとられているか。 · クラウドサービスプロバイダーが提供するポリシー管理ツール（ポリシーの一律適用やポリシー違反の資源利用を警告する仕組み）が適切に活用されているか。

表題　10	安易なアジャイル開発による脆弱なシステムの氾濫
内容	ビジネスのアジリティを推進するため、アジャイル開発が導入され、また開発と運用のギャップを埋めるために DevOps を導入する企業が増えている。一方、これらの開発・運用方法論に対しては、従来とは異なるセキュリティの考え方も必要となる。開発ルールやチェックリスト、リリース前のセキュリティ診断では開発やリリースのスピードに対応できず、設計思想としてのセキュリティの導入、セキュリティの自動化、DevOps サイクルの各所へのセキュリティの導入などいわゆる DevSecOps の考え方が必要となる。 こうしたセキュリティへの取り組みを怠ると、脆弱性を抱えたサービスあるいはシステムが氾濫する。
監査のポイント	· 情報システムの設計の際に、必要なセキュリティ要件を盛り込むための制度が整備されているか。 · 開発/運用の担当者に必要なセキュリティスキルが定義され、十分な力量を持った者がアサインされているか。 · セキュアな開発/運用を行うための支援ツールや環境（SAST/DAST/IAST/RASP、セキュアライブラリ、プロジェクト・課題管理ツール、バグ・脆弱性・バージョン管理ツール、CSPM、情報共有ツール等）が整備されているか。