表題	1	仮想通貨の盗難、詐欺の拡大
内容		NEM盗難事件を端緒とした、仮想通貨交換業者の杜撰なセキュリティ管理による、仮想通貨の流出や盗難があとを絶たない。本人確認が不要な小口取引に分けられ、流出した仮想通貨がだれの手に渡ったかの捕捉が困難になっている。我が国のみならず海外でもセキュリティ管理が問われており、仮想通貨は2019年もリスクを含んだ展開になる。
監査のポイント		【仮想通貨の利用者】 ・通貨交換業者選定プロセスなど、取り扱いポリシーを定めているか。 ・ポリシーに従った運用をしているか。 【仮想通貨の交換事業者】 ・金融庁のガイドライン等に準拠しているか。
表題	2	巧妙化する標的型攻撃による被害の甚大化
内容		標的型攻撃による被害は勢いを衰えることなく発生している。海外では、情報の搾取のみならず工場や発電所のような生活インフラに係る施設の停止を目的とした攻撃が確認されており、国内でもプラント関連事業者を狙う攻撃メールも少なくない。また、仮想通貨流出事案のように「やりとり型」と呼ばれる手口も増えつつある。 これらのように、手口も巧妙化し、被害も生活インフラにまで及ぶ恐れがでている。
監査のポイント		・従業員への不審メールなど予兆への気づきに関する教育が徹底しているか。 ・マルウェアへの技術的な対策（予防、検出、分析等）が十分か（特に、検出や分析が確実か）。 ・メール等OA業務用ネットワークと、業務システムやプラント等事業系のネットワークをつなぐ場合、不用意に接続されていないか。 ・CSIRT等対応チームの組織化に加え、常に最新の攻撃手法について情報収集を行い、現状の対策ですり抜けられることがないか検討を行っているか。
表題	3	家庭用IoT機器のセキュリティ不備によるプライバシー侵害の更なる拡大
内容		家庭用IoT機器のうちグローバルIPアドレスを持つルータやカメラ等が先ず攻撃にさらされる。その一方で、ぜい弱性のあるファームウェアのアップデートは進まず、ID/PWはデフォルト設定のまま放置され続ける。 徐々に普及しているスマートスピーカーやコミュニケーションロボットなどもネットワークと接続できるため、セキュリティ管理が正しく行われていないと、外部からの乗っ取りやプライバシー情報の窃取等の被害が今後も拡大する恐れがある。
監査のポイント		【家庭用IoT製品の製造者やそれを用いるサービス提供者】 ・IoT製品のリスクアセスメントを実施しているか。 ・消費者・利用者への使用上の注意に過度に依存していないか。 ・消費者・利用者に対して、ID/PWを初期設定から変更するよう促しているか。 ・ファームウェアのアップデートをするよう促しているか。
表題	4	ビジネスメール詐欺被害の更なる深刻化
内容		日本語ビジネスメール詐欺で大きな被害がで始めている。対象は大企業から中小企業にひろがりつつある。 オレオレ詐欺より効率が良いここから、更なる拡大が予想される。
監査のポイント		・ビジネスメールが社外の人に読まれないような技術的な対策を行っているか。 ・メールを送付される対象（役員、財務・経理担当者等）を特定し、教育をしている。 ・ビジネスメール詐欺を想定した、送金の事務手続きが的確に運用されているか。

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		国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。生産年齢人口の減少に伴う人手不足が深刻になる中で、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現実的な解を求められており、働き方改革の流れはより一層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		・就業環境の変化に伴う新たなリスクの特定と、リスク対応の措置が取られているか。 ・二要素認証等の適切なアクセス制御や権限管理がなされているか。 ・ポリシーへの適合など適切な端末管理、アプリケーション管理が実施されているか。 ・従業員への情報セキュリティ教育が適正に行われているか。
表題	6	時代遅れとなりつつあるパスワード認証
内容		パスワードの定期変更は無意味であるとか、いや、やり方が悪いだけで意味があるとかの議論がある。パスワードなどの認証要素管理はセキュリティ対策の基礎であることは疑いようのない事実である。しかし、1人が使うパスワードが数十件を超えるといわれる現在※、もはや安全と言えるパスワード認証を運用するのは人の能力の限界を超えている。また、過去に決定した認証要素管理手法が脆弱になっている可能性もある。パスワード問題に端を発した認証要素管理は、認証要素の分類ごとにリスク評価を行った上でそれらに適した認証システムの導入を行うなど、見直しや再構築が行われる。 ※米国Security Magazineの調査ではビジネスマン1人の保有パスワード数は191と報告されている （2017.11：https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords）
監査のポイント		・組織として認証システムのリスク評価が行われ、見直しがなされているか。 ・パスワード認証は機能しているか（ユーザが管理できているかなど）。 ・利用中の認証要素管理手法のぜい弱性は管理されているか。
表題	7	GDPRを乗り越えても残る諸外国のプライバシー規制リスク
内容		2018年5月25日にEUにおいてGDPR（General Data Protection Regulation:一般データ保護規則）が施行された。日本は十分性認定の対象国とされたものの、これだけを以って安心している企業が見られるなど本質的な対応ができていないケースもある。また、中国において施行されているサイバーセキュリティ法をはじめとして、各国のプライバシー関連の法規制が強化されていく中、海外進出している日本企業のリスク認識と対策の遅れ、及びそれらの不十分性によるリスクが高まる。
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 ・各国の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運用されているか。 ・自社グループ横断的なデータ保護管理方針、体制、規程、手順は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。 ・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。
表題	8	高度化するランサムウェアによる被害拡大
内容		身代金要求型ウイルス（ランサムウェア）は、2017年の「WannaCry」の大流行のようなものは発生していないが、日本語を含む多言語化が進む一方で金銭窃取を目的とはしないものがで始めるなど、高度化、多様化が進んでる。RaaS（Ransomware-as-a-Service）の普及、高度化も相まって、従来の対策が対応する前に急速に被害が拡大する事案が発生する恐れがある。
監査のポイント		・従業員への不審メールに関する教育が徹底しているか。 ・ぜい弱性対策・マルウェア対策（予防、検出、分析等）の実施が十分か。 ・情報のバックアップ及びリカバリーテストの実施がされているか。 ・内部ネットワークでのマルウェアの感染拡大に対する局所化対策ができているか。 ・感染経路や原因を追究できる体制や仕組みを整えているか。

表題	9	問われるサイバーセキュリティ経営の責任体制
内容		サイバー空間の利用そのものが企業のビジネス戦略に不可欠なものとなる中で、「経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要」とされているが、その責任をだれが担っているのかの説明を求められる時代になる。 ビジネス戦略等のリスクの統括は取締役会にあるとの認識は一般的であるが、その部分であるサイバーリスクの統括の責任は、委員会等設置会社では監査委員会にあるとの見方が有力であり、各企業において取締役や監査役がどのような責任分担をするのか、その責任を負うだけの準備ができているのかが問われることになる。
監査のポイント		・企業あるいは企業グループの情報セキュリティへの取り組みの基本方針や取り組み体制が経営トップから明確に示されているか。 ・組織が明確に定めた情報セキュリティへの取り組みへの責任者のもとで、必要に応じてモニタリングや対応策の検討が行われている記録があるか。 ・情報セキュリティ対策の評価と報告が、適切なレベルの経営会議に報告されているか、また利害関係者に適切に開示されているか。 ・監査役あるいは監査委員会が、取締役や執行役員の情報セキュリティ対策に係る活動の的確性を評価した記録があるか。
表題	10	クラウドバイデフォルトの情報セキュリティ体系化
内容		政府機関においても「クラウドバイデフォルト」が提唱され、金融業界においてもFISC「安全対策基準」でクラウド項目が明記されるなど、もはやクラウドはITインフラにおいて第一選択肢となっている。利用企業においては、情報セキュリティ基準や管理策がオンプレミス時代のままでは実態との間に齟齬が生じ、ビジネス拡大の阻害やコストの増大など、本来クラウドで得られる便益を損なうことから、時代に即したクラウドバイデフォルトの情報セキュリティ体系化が求められる。
監査のポイント		・利用するクラウドサービスが事業活動に及ぼすリスク評価を実施しているか。 ・クラウド事業者との責任範囲の境界（責任分界点）を明確にしているか。 ・サービスのSLAは適切に設定されているか。 ・データの配置場所、準拠法など法的なリスクは存在しないか。 ・各種規制ガイドラインの準拠に必要な第三者監査報告書やセキュリティホワイトペーパーなどの情報が公開されているか、また適宜更新されているか。