表題	1	多様化・巧妙化するランサムウェアの被害拡大
説明		身代金を要求するランサムウェアが急増し、2017年前半にはWannaCryなどが世界中で猛威を振るった。十分に儲かると味をしめた攻撃者は、2018年には更に高度化、巧妙化したランサムウェアを開発すると予想される。大企業でも思わぬ被害が生じる恐れがある。
解説		感染したPCのファイルを暗号化するなど利用不能とし、その回復のために金銭を要求するマルウェアをランサムウェアと呼ぶ。感染経路は電子メールやWebサイトを介するものが多いが、感染したPCにとどまらず、共用フォルダにあるファイルも暗号化し組織の業務を止めたり、ぜい弱性未対策の機器を狙いネットワークを介して広範囲に感染を広げるなど手口が巧妙化しており、その被害が急増、重大化している。
監査のポイント		・従業員への不審メール教育が徹底しているか。 ・ぜい弱性対策・マルウェア対策の実施が十分か。 ・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による感染拡大活動に対する局所化対策ができているか。

表題	2	最新の対策もすり抜ける標的型攻撃による甚大な被害の発生
説明		ふるまい検知やサンドボックスはセキュリティ対策に必須だが、2018年には攻撃が更なる進化をする可能性が高い。ファイルレスマルウェアや、攻略した通常サイトをC＆Cサーバにするマルウェアが端末ごとに埋め込まれるなど、攻撃者は最新検知技術を回避する攻撃を仕掛けはじめている。高度な対応に安心していると、甚大な被害発生が露見して初めて攻撃に気づく恐れがある。
解説		標的型攻撃は特定の対象を標的として、目的を達成するまで様々な手段を講じ、執拗に攻撃するサイバー攻撃を指す。標的型攻撃の多くは、何らかの方法でマルウェアと呼ばれる不正ソフトを対象組織の内部システムに送り込み、感染させ、それを起点に様々な攻撃ソフトをダウンロードし、目的を達成しようとする。 このマルウェアの大部分は新種のものなので、ウィルスソフトが検知できない。マルウェアの検知には、他のシステムに影響を与えないサンドボックスと呼ばれる環境で感染したと思われるファイル等を動かし、そのふるまいを確認する方法がとられる。ところが、攻撃者はファイルが開かれた環境がサンドボックスなどの検知のための環境であるかを探る仕組みを装着し始めている。 また、通常はマルウェアがソフトウェアとしてインストールされるので、検知ができるが、それをしないファイルレスマルウェアも開発されており、検知システムが乗り越えられるリスクが高まっている。
監査のポイント		・サンドボックス製品を超えるマルウェアへの対応がされているか。 ・常に最新の攻撃手法について情報収集を行い、今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。 ・ファイアウォールやプロキシログの分析による「異常」の検知の実施がされているか。

表題	3	セキュリティ機能が乏しいIoT製品への攻撃による社会的混乱
説明		消費者向け電化製品の多くがネットにつながり、IoT製品の便利さが見えるようになった。しかし、2018年にはセキュリティ対策の制約がクローズアップされると予想される。IoT製品の多くが専用機器として作られるため、マルウェア対策機能などを実装するリソースが限られるのだ。セキュリティ機能の乏しいIoT製品への攻撃や攻撃予告で、リコールや風評被害などの社会的混乱の懸念が高まってくる。
解説		IoT機器はビデオなどの家電製品をインターネットに接続し、遠隔操作や自動操作を行うことで、利用者に便利な機能を提供する機器である。IoT機器ではマイクロコンピュータ（マイコン）が情報処理や通信処理を行う。IoT機器のセキュリティ上の弱点として以下のような点が挙げられる。 ・マイクロコンピュータの容量が限られているため、例えばウィルスソフトなどのセキュリティソフトを入れる余地がほとんどないこと ・通常の情報処理機器と比較して製品寿命が長いため、古くなると攻撃技術の進歩に対応した対策が取りにくいこと ・数量が多く、一般の人が触れない構造のため、ぜい弱性対策のためのアップデートが行いにくいこと ・管理者が不明確、あるいは知識の乏しい管理者であることが多く、セキュリティ対策が浸透しにくいこと
監査のポイント		・IoT製品やIoTを活用したサービスにおけるリスクアセスメントの状況 ・IoT製品のセキュリティ対策の実装状況 ・消費者・利用者への注意喚起 ・消費者対応窓口の教育・訓練状況

表題	4	クラウドなど集中管理による社会的規模の被害発生
説明		クラウドサービスなどを利用した一元管理でガバナンスを高める一方で、設定ミスなどによる情報の大量消去、意図しない書き換えなどが発生する可能性がある。2017年に大手クラウドベンダーの設定ミスが世界の通信に大きな影響を与えたように、集中化したシステムのエラーが社会的な影響を及ぼす可能性がある。
解説		クラウドサービスが浸透するにつれて、利用者がクラウドと知らないでクラウドサービスを使っているケースが少なくない。クラウドサービスの中には認証など特定の機能を提供するサービスがあり、そのサービスを他のクラウドプロバイダが利用するなど、相互に複雑に交わった構造の上で、サービスが提供される例が少なくない。機能を集約して特化したサービスを利用することで、より安く、柔軟なサービスを提供することができる。しかし、一方で特定のクラウドサービスに事故が生じた場合に、関連する無数のサービスに影響することおそれがある。
監査のポイント		・構築やメンテナンス手順が明確にされているか。 ・チェックリストなどが整備され、運用されているか。 ・二重チェックなどを行うようにし、事故を未然に防ぐ対策ができているか。 ・万が一、事故が発生した時に備えて、被害が最小化できる仕組みがあるか。

表題	5	考慮不足の働き方改革に起因する事故の発生
説明		「働き方改革」が国主導で広がりを見せ、2018年には本格的な改革が進む。改革手法の一つがITを活用したテレワークの推進である。BYODなど私有端末の業務利用などの拡大も予想される中、十分なセキュリティが保たれない作業環境下での事故が懸念される。
解説		2017年3月29日に政府の主導する働き方改革実現会議から、働き方改革実行計画が発表されたことにより本年の大きなトピックの1つとなった。 いつでもどこでも働ける環境としてテレワークに取り組む企業が増えている。テレワークでは操作端末等のIT環境が「境界」の外に出ることから、従来の境界防御型のセキュリティ対策からテレワーク環境に適した環境への変更がシステム上もポリシー上も必要となってくる。環境整備を終えた企業はテレワークを本格化する前に、セキュリティポリシーを含めた対策が必要となる。
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。 ・重要情報の流出防止のためのアクセス制御や権限管理がなされているか。 ・従業員教育が適正に行われているか。

表題	6	日本語ビジネスメール詐欺被害の拡大
説明		国外では大きな被害が報告されていたビジネスメール詐欺が国内でも発生し始めている。2018年には、日本語の詐欺メールがより一層広がり、更なる被害の拡大が予想される。
解説		ビジネスメール詐欺とは、会社の役員を装ったメールを送ったり、ウェブメール等に不正アクセスして取引メールの間に入り込んで口座を偽ったメールを送ったりし、巧みに企業や組織の担当者をだまして金銭を詐取する、メールを利用した詐欺行為である。 BEC(Business E-mail Compromise)とも呼ばれる。会社の合併・買収に絡む送金詐欺の場合には被害額が高額になることもある。
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おこなっているか。 ・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、教育をしているか。 ・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	7	ガバナンス欠如のIT投資による重大インシデントの発生
説明		サイバーセキュリティ経営ガイドラインが公表されて一年経っているが、依然として、不明瞭な責任体制や経営陣の認識不足など、ガバナンスの不備が残っているケースがみられる。現場まかせでセキュリティレベルの検討や確認が不十分なまま、IT化やクラウドサービス利用が進んだ結果、事業中断に及ぶなどの重大インシデントが懸念される。
解説		情報セキュリティガバナンスとは、経営者のリーダーシップにより企業や団体の情報セキュリティへの取り組みを適切に機能させることを意味する。情報セキュリティ対策は、経営者の定める目的や目標に沿って体系的に取り組んでいくことが肝要である。ガバナンスが機能しないと、部門独自のリスク判断で対策よりも利益優先になりかねず、防げるはずの重大なインシデントが発生してしまうことが懸念される。
監査のポイント		・情報セキュリティについての責任体制が明確か。 ・情報セキュリティ方針が周知・徹底されているか。 ・IT投資の計画／導入／運用開始の各段階での責任者レビューの徹底がされているか。 ・監査役等による経営陣のガバナンス姿勢の検証がされているか。

表題	8	成長しないマネジメントシステムによる組織活力の低下
説明		ISMSやプライバシーマーク等の情報セキュリティ関連マネジメントシステムが導入されて10数年が経った。本来はPDCAサイクルでセキュリティ対策が向上しているはずだが、認証取得組織においても情報セキュリティ事故が発生している。認証取得で安穏とした組織では、高度化、巧妙化する脅威に対応した議論がなされないままに終わる懸念がある。
解説		個人情報の取扱いの適切性を評価するプライバシーマーク制度は1998年、情報セキュリティへの態勢を評価するISMS適合性評価制度は2002年にそれぞれスタートし、多くの事業者が認定、認証を受けている。いずれの制度もマネジメントシステムを評価するものであり、組織が計画-実行-評価-改善のプロセス（PDCAサイクル）により、継続的な維持、向上を図ることが背景思想として盛り込まれている。長年にわたり継続して認定、認証を受けている組織は、マネジメントシステムが硬直化、マンネリ化し、それぞれの基準が企図する維持、改善が疎かになり新たなリスクに対応できていない可能性がある。 【参考】https://isms.jp/about/index.html ISMS適合性評価制度は、わが国全体の情報セキュリティ強化のため、また安対制度廃止後の受け皿として、2002年4月から本格運用を開始した。 https://www.jipdec.or.jp/project/pmark.html 1998年よりJIPDECが運営する「プライバシーマーク®制度」は、事業者の個人情報の取扱いが適切であるかを評価し、審査基準に適合した事業者にプライバシーマークの使用を認める制度。
監査のポイント		・組織のマネジメントシステムが、脅威、事業、情報システム、制度等の変化に対応したセキュリティ対策のレベルとなるよう必要な施策を盛り込んでいるか。 　特に、内部監査の品質向上や経営陣の理解の促進が行われているか。 ・プライバシーマークの認証要求事項の改訂への対応が行われているか。

表題	9	形だけCSIRT/名ばかりセキュリティ人材による弊害の発生
説明		CSIRTを社内で組織化する企業が急増しているが、中には形だけのものもある。セキュリティ人材不足が叫ばれる中、セキュリティを勉強したばかりの担当者が専門家として任用される例もみられる。こうした例では、インシデントに繋がる兆候の見過しやインシデント対応時のミスなどにより、被害が深刻化する可能性がある。
解説		CSIRTとはコンピュータ・セキュリティ・インシデント対応チーム（Computer Security Incident Response Team）の略語である。近年のサイバー攻撃激化に対応して、組織内にCSIRTを設ける企業や機関が増えている。CSIRTが本来の機能を発揮できるために、日ごろからインシデント管理を怠らず、また関係機関との連携を保ち攻撃や防御に関する最新情報を入手しておくなど、インシデントが生じる前から適切な活動をしておく必要がある。また、インシデントか否かを適切に判断し、インシデントと認定された場合には、刻々と変化する状況に応じて、経営者を含む組織構成員と連携し、被害を最小化できるようにしておかなければならない。このためには、適切なスキルと組織を動かせる権限を有する人材がリーダシップを発揮し、日ごろから訓練などを通じて組織の対応力を高めておくことが不可欠である。しかし、技術知識や権限のないリーダが任用されたり、マニュアルのみで訓練がなされていないなどの例が少なくない。こうしたCSIRTでは、いざという時に役に立たない恐れがある。
監査のポイント		・自社のCSIRTに必要なスキルが特定され、そのスキルを獲得する計画が策定されているか。 ・人員のセキュリティに対する理解度の確認がされているか。 ・契約しているサービスの品質の確認(レポート等の評価)がされているか。

表題	10	GDPR違反の摘発
説明		2018年5月25日にEUにおいてGDPR（General Data Protection Reguration:一般データ保護規則）が施行予定である。EU域内の個人の情報を扱う場合、欧州拠点及び域外移転の可能性が有る各国で諸対応が求められる。日本企業には、対策開始の遅れや駆け込み対策による対応漏れで摘発されるリスクが高まる。
解説		EU域内の個人情報を取り扱うにあたって、1995年から実施されていたEUデータ保護指令が強化されたものがGDPRである。個人情報の取り扱いや個人の権利の明確化など、要求事項がより厳格化され、違反した際の制裁金も高額化（最大で全世界の売上の4%）している。 本来EUデータ保護指令への対応が十分に機能していれば、ルールの厳格化に対する追加対応で済むところであるものの、現実的には情報資産の漏れやセキュリティの追加対応など、対応自体も小規模で済まないケースが多く見受けられる。日本企業の出遅れが他国企業の対応と比べ目立っている状況にある。
監査のポイント		全体的な取り組みの監査に加えて、下記の様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。 -データ保護管理方針、体制 -個人情報取扱いに係る規程、手順 -個人情報収集/取得に際しての同意取得 -国外移転に係る手続き(SCC等)