第 1 位	**緊急コロナ対策から With コロナへ　業務優先で後回しにしたセキュリティの再点検**
内容	コロナ対策として緊急避難的にリモートワークを推進した結果、セキュリティ対策がセキュリティリスクに対して十分ではない例が散見される。 具体的には、クラウドの安易な利用による情報セキュリティ対策漏れ（特に、資産管理されず組織として管理権を有しないクラウドの利用など）、リモートワーク環境で後手に回る脆弱性管理の不備を狙った標的型攻撃、そして、内部不正を誘発しかねない甘いアクセス制御とルールの不備などである。ファイルサーバや重要システムへのリモートアクセスやコラボレーションツール利用など、非常事態宣言に一旦はリスクを許容して許可したことを、今一度リスク評価し、セキュリティ対策全体を再点検すべき時期である。 働き方改革としても今後定常化していくと思われるリモートワークの有効な恒久的サイバーセキュリティ対策の実装が求められる。
監査のポイント	・ コロナ禍を踏まえた新しい働き方を前提とした情報セキュリティのリスク分析が適正に行われ、リスクに対応した管理策が選択され、実装されているか（マネジメント監査における対応）。 ・ 上記のリスク分析結果に基づき、個別管理策の内容見直しがなされているか。 （例えばオフィスから持ち出せる情報であるか否かという観点で情報の分類が見直されているかなど） ・ リモートワークなどへの個別方針がない場合にも、新しい働き方に対応した体系的な方針が設定されているか。 ・ リモートワークのリスク対応として、技術的・物理的対策が十分に行われているか。 （例えば在宅環境やリモートアクセス環境など、従来と異なる技術的対策に関して、着実な実装と運用がなされているか。） ・ 技術的対策を補完する人的対策・物理的対策が有効に機能しているか。 ・ リモートワークとオフィスワークが併用される環境でのハイブリッドな働き方に対するリスク評価・管理策の選定がなされているか。
第 2 位	**多様化するワークスペースに対応するセキュリティ対策**
内容	リモートワークが増加する中、在宅勤務だけでなく、貸し作業スペースによる勤務も増加している。ニーズに合わせ個室型、共同スペース型など多様な形態のサービスが提供されている。多くの貸し作業スペースはセキュリティ対策が行われているが、共有設備ならではののぞき見や無線 LAN 盗聴、紙媒体の裁断処理など、設備内で提供されているセキュリティ対策が自社で定めている水準に合致しているとは限らない。 こうした共用サービスの仕組みが、自社のセキュリティの水準を下げるものとなっていないかの確認が必要となる。
監査のポイント	・ リモートワークの実施を許可するワークスペースについて、社内規程等でルール化されているか。 ・ リモートワークの実施場所を許可する際には、自社のセキュリティ要求に合致しているか、セキュリティの観点による確認が行われているか。 ・ 上記の確認には、無線 LAN に関するセキュリティ、他人ののぞき見、盗難など自社社員以外が共同利用する際のセキュリティ要求事項が盛り込まれているか。 ・ リモートワークの実施場所に関するセキュリティリスクの受容は、セキュリティの責任者を含めて判断を行っているか。

第 3 位	ICT サプライチェーンにおける情報セキュリティリスクの増大
内容	近年、情報セキュリティが強固でない中小企業や海外子会社、業務委託先、ASP 型サービスへのサイバー攻撃が増加し続けている。攻撃の方法もより巧妙さを増しており、自社だけでなくサプライチェーンに属する全ての企業を含めてセキュリティ対策を強化していく必要がある。また、委託先に対するルールの徹底・教育とともに、システムとして情報漏洩が発生しにくい環境を構築することも重要である。 一方、システム開発において OSS（オープンソースソフトウェア）を利用して、開発工数を削減するいわゆるノーコード・ローコードの動きも進んでおり、経済産業省のサイバーフィジカルのセキュリティの検討においても、OSS の利用時のセキュリティ対策として「ソフトウェア部品表(SBOM)」の作成が重要視されている。 このように、自社だけでなくサプライチェーンに属する全ての企業を含めてセキュリティ対策を強化していく必要性の認識が広まり、委託先に対するルールの徹底や教育、導入・調達する ICT 製品、サービスのセキュリティ管理が進む。
監査のポイント	サプライチェーンリスクに対する対策は広範囲に及ぶが、主として下記の事項が監査すべきポイントとして挙げられる。 ・ システム開発やデータ処理の業務を委託する際に、委託先（さらに必要に応じてその先の再委託先）に対して要求するセキュリティ対策を明示し合意する手続きを定めているか。 ・ 社外からのソフトウェア（オープンソースソフトウェアやライブラリなども含む）の導入に際して、マルウェア混入や脆弱性の残存など、確認すべき項目が明確になっているか。 ・ オープンソースソフトウェアや ICT 製品、利用サービスについて脆弱性対応を迅速に行うための管理を行っているか。 ・ 社外の組織（業務委託先や子会社等）とのネットワーク接続（VPN を含む）の接続点で、接続先からの攻撃を想定したアクセス制御やマルウェア検知等の仕組みを導入しているか。 ・ クラウド型サービスや ASP 型サービスの利用の際に、セキュリティ管理状況やセキュリティ侵害発生時の対応レベルなどを確認しているか。 ・ 自社が業務委託先である、あるいは顧客向けにサービスを提供している場合、自社経由で顧客にセキュリティ攻撃が及ばないよう、納品物（開発委託を受けたソフトウェア等）や提供サービスのセキュリティ確認を行っているか。

第 4 位	広がる Web 会議利用の盲点－データ漏洩に注意
内容	通常のビジネスとしてすっかり定着した Web 会議だが、相手が限定された単なる TV 会議との意識だと危険だ。セキュリティが確かなサービスを選ぶことは常識だが、参加者が適正か、公開の場や公共の Wi-Fi を使っている場合でも盗聴の恐れはない仕組みか、議論の録音や共有資料の管理はできているかなど、考慮すべきことは多い。Web 会議の場合、異なるポリシーや異なる利用環境の組織間でのコミュニケーションツールであるというるリスクを考慮する必要がある。
監査のポイント	・ クラウドサービスとして提供されている Web 会議システムの利用が組織のクラウドサービス利用方針に従っているか。 ・ Web 会議システムの利用に伴うリスク分析が行われ、リスクが体系的に把握されているか。 ・ 組織的対策として、Web 会議システムの管理責任者が任命され、その責任者が Web 会議サービスプロバイダーの提供するセキュリティに関する情報の内容を理解し、それを踏まえたリスクとその対応について理解しているか。 ・ 当該責任者から各々のユーザに情報セキュリティ対策に関する指示が適切に行われているか。
第 5 位	**ISMS からサイバーセキュリティ対策マネジメントへ**
内容	多くの企業が ISMS を実装し、情報セキュリティ対策を行っている。サイバーセキュリティは情報セキュリティが侵害された時の実空間の被害を軽減するための活動であり、情報セキュリティ対策の延長上にある。このため、ISMS を生かしたサイバーセキュリティ対策のマネジメントが可能となる。 ISMS はセキュリティ対策のうちの予防に重点がある。現在では予防策のみでは不正侵入は防げない。このため、予防が効かなかったとき、すなわち情報セキュリティインシデントが生じているときの検知や対処などを補強する必要がある。現状では米国 NIST のサイバーセキュリティフレームワーク等を参照して、ISMS を補強することが望ましい。
監査のポイント	・ サイバーセキュリティの監査を行うためのサイバーセキュリティ固有の管理基準が、米国 NIST のサイバーセキュリティフレームワーク等を参考にして、作成されているか。 ・ サイバーセキュリティ監査の範囲をどこまでとするかについて、経営者の承認がとれているか。 ・ 事業継続に関して、IT 部門と事業部門が適切に連携できるルールが整備され、訓練等が実施されているか。

第 6 位	個人データ活用におけるビジネスとプライバシーの対立
内容	様々な場面で個人データを活用したビジネスが提供されようとしている。サービスの提供企業はビジネスや情報セキュリティが成り立つことだけではなく、個人データにおける法規制をクリアしていることを説明できる必要がある。その際、ビジネス部門が解釈するだけでなく、リスク管理部門や法務部門など多面的な観点からの確認を経るとともに、マネジメントが意思決定に必要な情報を基に十分な確認をして判断していることが求められる。
監査のポイント	・ プロジェクトの組成時（取り組みの開始前）に個人データを活用するビジネスであるという前提のもとに、メンバー選定やコストやスケジュールの検討が開始されているか。 ・ チーフプライバシーオフィサー（CPO）などプライバシーに関する専門性と権限を持つメンバーが関与しているか。 （特に法務、リスク管理部門など社内の専門家の意見を聴ける体制になっているか。） ・ 計画段階でプロジェクトリスクとしてプライバシーが識別され対応案が検討されているか。 ・ 計画段階で、単に自社の業務のみならず委託先・サプライチェーン先を含む関連業務全体を、一気通貫でプライバシーの観点から検証しているか。その際、検討は自社だけで行われておらず適切なメンバーが関与していたか。 ・ 計画段階で外部有識者の客観的な目線で課題やグレーゾーンを洗い出しているか。また有識者による継続的なサポートを得られているか。 ・ フェーズの完了、業務の開始等プロジェクトの重要な意思決定タイミングでプライバシーの観点からの致命的な課題が無いことを確認しているか。課題の対応方針が定まっていないものはないか。
第 7 位	**クラウドの仕様変更への対応不備によるセキュリティ事故**
内容	クラウドサービスは仕様変更が高い頻度で実施されており、利用者が設定に処すべき事項が複雑化し、結果として事故が生じる事態が発生した。提供者側による情報の提供やより良い UI/UX の提供が求められる一方、利用者もクラウドサービスを常に勉強し、リスク回避を行う必要がある。クラウドサービス提供者、SIer、利用者による責任分担が明確でないと障害発生時の対応も迅速に行うことができず、思わぬ事態を招く恐れがある。
監査のポイント	・ クラウドサービス提供者（CSP）、SIer、利用者（CSC）による明確な責任分担が約款や契約により明確となっているのか、その責任分担が適切に運用され機能しているかといった、マネジメント監査、ガバナンス監査が重要。 （具体的には CSP、SIer、CSC による協調的管理が行われ、定期的に三者間で合意された手順に対するレビュー等が実施されているかどうか。） ・ 利用者（CSC）のスキルアップによるリスク回避が有効に機能しているかどうか。 （具体的には研修状況の管理の他、例えば資格取得や更新等について可視化できる指標を用いて管理しているか、適正なスキル保有者が適正なポジションに配置されているかモニタリングできる仕組みの確認など）

第 8 位	管理機能が攻撃対象に　社外端末によるシステム管理に潜む重大脆弱性
内容	コロナ以前、社内システムの管理は社内からのアクセスを前提に管理機能を実装することが多かった。昨今、システム管理者もリモートワークをするために社外から管理系ソフトウェアにアクセスできるようになると、それまで外部にさらされることのなかった脆弱性が露見する。そこに攻撃を受ければ、一気に管理者権限を奪われかねない。
監査のポイント	社内システムの管理者がリモートワークできるように、システムの管理機能へ社外からアクセスさせる場合、当該管理ソフトウェアに関して以下に留意して監査する必要がある。 ・ 管理ソフトウェアのパッチやバージョンは最新のものを使用しているか。 ・ 管理ソフトウェアに既知の脆弱性がないかを確かめているか。 ・ 管理ソフトウェアに存在する既知の脆弱性への対処をしているか。 ・ 管理ソフトウェアの不正使用を検知するための監視をしているか。 ・ 管理ソフトウェアのアクセスログ及び動作ログを残し、保全しているか。 ・ 管理ソフトウェアに対して社外からのアクセスを拒否する手段が別途用意されているか。 ・ 管理ソフトウェアの機能を停止させる又はそのソフトウェアから社内システムへのアクセスを拒否する手段が別途用意されているか。
第 9 位	**クラウド相互乗り入れ問題　バタフライエフェクトで自社の業務が停止する**
内容	クラウドサービスの機能の多様化や細分化、API による連携が容易に実装可能となっていることなどを背景とし、あるクラウドサービスに障害が生じた際などに、連携して幅広いサービスが障害に巻き込まれる事案が拡大している。 利用しているシステムやサービスが、そのバックエンドでどのようなクラウドサービスの機能を利用しているか、また、その機能はどのようなサービスを利用しているかなど多段的な「ピアクラウド」のサプライチェーン管理や、その接続にかかる API 等の安全性の確認も必要になってくる。
監査のポイント	・ クラウド利用者にとっては利用しているシステムやサービスの全体像をしっかりと把握した上で、リスク評価を実施することが重要なポイントとなる。 ・ 監査においては、管理策は、利用しているクラウドサービス全体のシステムアーキテクチャ及び業務システムの全体構成に対応して策定されているため、それらを理解した上で監査手続を実施することが必要となる。 ・ 特に緊急時の連絡体制の整備、リカバリの手順など可用性への対応を行うための体制整備がされているかどうかは監査の重点ポイントとして検討する。 （機密性に重点を置くばかりでなく、乗り入れている部分のどこか一部の停止が全体業務の停止につながる恐れもあり、その要因の除去を自力で行うことは難しいため）

第 10 位	気を付けよう外部サービスの穴
内容	インターネット上の外部サービスを利用することで、情報共有や顧客へのサービス提供を効率的に行える時代になった。一方で外部サービスサイトに脆弱性があり、そこを突かれて重要な情報が漏洩するという被害が少なくない。 ID とパスワードのみの認証であったり、提供されている API から大量の情報が照会可能であったり、サービス自体がセキュリティを意識していない場合もある。 また、ID 連携を行っている場合、連携をおこなっているすべてのアプリケーションで不正利用の恐れがあるので、被害が深刻となりやすい。
監査のポイント	・ 組織ガバナンスの問題として、組織がインターネット上の外部サービス利用のすべてを把握し管理しているか。また外部サービスの利用ルールが確立しているか。 ・ ルールが確立していない場合、インターネット上の外部サービスのほとんどはクラウドサービスであるため、これらのサービスが組織のクラウドサービス利用の個別方針に基づき適正に利用されているか。 ・ 特に、新たに利用を開始したサービスについては、リスク分析が行われ、情報セキュリティのための利用ルールの策定とそれに基づく利用がなされているか。 ・ ID 連携を行っている場合には、リスク分析にその点が考慮されているか。