よろず相談会第3回

- セキュリティガイドラインに沿った自己評価の進め方 -

2023年11月17日

一般社団法人 日本自動車工業会
総合政策委員会 ICT 部会サイバーセキュリティ分科会

一般社団法人 日本自動車部品工業会
総合技術委員会 IT 対応委員会 CS 部会

本日の進行について

本日の進行	事前に頂いたご質問に対し、一問一答形式で進めさせて頂きます。
	一問一答の中で関連する質疑については口頭にてお願いします。
	事前に頂いたご質問につきまして、本日のテーマに沿ったものを選定し、 個社の情報等を省き、一般化しておりますので、予めご了承ください。
注意事項	進行上マイクとカメラは必ずオフにしてください。
	発言される際には挙手ボタンを押していただき、指名されましたら、 マイクをオンにして発言をお願いします。発言が終わりましたら必ずマイクをオフにしてください。
	話しの流れによっては個社ごとの状況を回答をさせて頂く場合もございます。 予めご了承ください。
	運営管理上、本日の会議はレコーディングさせて頂きます。

本日取り上げさせて頂くご質問一覧

No	質問
①	小規模子会社での自己評価が上ぶれする傾向が確認できています。１人情シスレベルの子会社での上振れ是正について良いアドバイス等ありましたらご教示いただけると幸いです。
②	達成基準に対して、どこまでやれば完了か判断しにくい項目がある。他社事例に記載されている内容の一部だけでも実施して達成基準が満たされたと自分が判断した場合に対策完了として良いでしょうか。
③	会社として１つの評価結果を求められておりますが、部門ごとに状況に差があるために、どのようにまとめて良いかがわかりません。まとめ方についてのアドバイスや、他社様における事例等あればお願いします。
④	「評価の根拠記入欄」について、どの程度具体的に記載すればよいのでしょうか？参考とすべき見本回答等はございますでしょうか？
⑤	自己評価の進め方や考え方について教えてください。他社がどのように対応したかの事例があれば知りたいです。
⑥	弊社はISO27001を取得しておりませんが認証を取得できるレベルにはなりたいと考えています。このセキュリティチェックシートはISO27001に関連性がある項目となっているでしょうか？ISO27001との関連性を考慮しつつ評価を進められますでしょうか？
⑦	弊社での現状の取り組み段階は、規程の策定までは完了している状況です。しかしながら規定に基づいた実績の把握までは時間が掛かっている状況で、1点なのか2点なのかで迷ってしまいます。評価方法についてアドバイスをお願いします。
⑧	対象カテゴリーにある「パートナー企業のリスク管理」の項目において、パートナー企業の数が多数に及ぶため、各社ごとの内容協議、調整に非常に手間がかかり、短期間での対応が困難です。効率の良い評価の進め方はありますでしょうか？
⑨	規定やルール等を明確化した文書の策定を求める項目が複数ありますが、どの程度のものを作成する必要があるのでしょうか？他社事例の模範解答の選択肢のうち１つでも当てはまるものがあれば、達成を考えてよいのでしょうか？
⑩	自己評価の進め方や考え方について教えてください。他社がどのように対応したかの事例があれば知りたいです。

本日取り上げさせて頂くご質問一覧

No	質問
⑪	ガイドラインの自己評価を進めるにあたり、実施している対応が問題無いかの判断が難しいと感じています。F/Wやサーバー、クライアントのセキュリティ的な設定や、ログ取得の項目及び設定方法など、推奨設定などご提示頂けますと幸いです。
⑫	社内教育・訓練の実施と内容見直しについて、自己評価をどう進めていいのかわかりません。
⑬	No.16「サイバー攻撃や情報漏えいの新たな手口を知り、対策を社内部署へ共有している」ですが、自己評価を進めるにあたって、全社員に分かり易く説明することと、理解度の確認方法を知りたいです。
⑭	No.90「不正侵入や不正行動を監視している」に対して、社内のすべての重要な場所の監視ができた時点で達成とすべきなのか、すべての重要な場所のうち1つでも監視ができた時点で達成としていいのでしょうか。
⑮	No.150「システムが停止した際も業務が遂行できる代替手段を用意している」に対して、どのくらいの期間システムが停止することを想定した代替手段の検討が必要でしょうか。

時間が足りない場合は、すべての質問に対してお話できない可能性がございます。
ご理解の程よろしくお願い致します。

質問①

質問内容：小規模子会社での自己評価が上ぶれする傾向が確認できています。1 人情シスレベルの子会社での上振れ是正について良いアドバイス等ありましたらご教示いただけると幸いです。

回答：

貴社子会社にて自己評価を行った際の結果に対し、評価結果が貴社の認識と比べて上振れして困っていると読み取りました。

そもそも本ガイドラインは監査目的や第三者認証を求めるものではなく、評価結果に対して自工会/部工会から何らかのチェックや是正を行う事もありません。あくまでもセルフチェックの形をとっており、評価者の解釈で回答いただいて問題なく、評価者が異なれば結果が多少変わってしまう事も認識しております。回答方法が良くわからず入力されているケースや、評価結果を良くしたいとの気持ち等が、上振れに繋がっていると思います。

貴社におかれましては、多少の上振れはあるものと認識の上で、親会社として評価結果をチェックをお願いいたします。サプライチェーン全体のセキュリティ向上のため、各社ごとにリスクを明確化し、計画的な対策を実施いただく事を目的とした活動であることを改めてお伝えいただき、今後改善いただければと思います。

情報交換例）

・各社様における子会社からの評価報告に対する対応事例があればご紹介願います。

質問②

質問内容：　達成基準に対して、どこまでやれば完了か判断しにくい項目がある。
他社事例に記載されている内容の一部だけでも実施して達成基準が満たされたと
自分が判断した場合に対策完了として良いでしょうか。

回答：

対策完了とご判断いただくには、**「目的」**項目に書かれた**“何のために対応するのか？”**を認識いただいた上で、**“何を？”（「達成条件」の内容）**、**“どれだけ対応するのか？”（「達成基準」の内容、対象、時期、頻度）**の**全て**が満たせているのかをチェックいただきます。

「他社事例」には、お取組みいただき易いように、具体的な対応方法の例を記載していますが、自社の取組みが「他社事例」に記載の一部だけで良いのか？他にも対応が必要なのか？を、**各社におけるリスク（被害の影響の大きさ）を考慮し、ご判断いただければと思います。**

参考

分類	ラベル	目的	要求事項	No.	レベル	達成条件	達成基準	他社事例 (参考事例を列記しており、 すべての遵守を求めているものではありません)
共通	1方針	会社として、セキュリティに対する基本的な考え方や方針を示し、社内の情報セキュリティ意識を向上させる	自社の情報セキュリティ対応方針を策定し自組織内に周知していること	1	Lv1	**自社の情報セキュリティ対応方針(ポリシー)を策定している**	・自社の情報セキュリティ対応方針を策定し、文書化すること	【情報セキュリティ対応方針の記載事項の例】 ・経営者の責任：当社は、情報セキュリティを確保・維持、改善するための活動を、経営者主導で推進します ・法令遵守： 当社は、情報セキュリティに関連する法令を遵守します 【策定・文書化の責任者の例】 ・経営者 ・取締役会
				2	Lv2	**自社の情報セキュリティ対応方針(ポリシー)の内容を確認し、必要に応じて見直ししている**	【規則】 ・社内外の環境変化を踏まえて、内容を確認し、適宜見直ししていること 【頻度】 ・情報セキュリティ対応方針(ポリシー)の内容を確認、改善 -1回以上/年 ※別途、重大な変化が発生した場合には迅速に対応すること	【見直しの例】 ・会社規則に見直しについて規定している ・定期的にセキュリティ委員会で規定見直し状況を報告施している 【社内外の環境変化の例】 ・自社体制の変更 ・対象となる情報資産の変更 ・新たな脅威の検知・管理対象の変更時 ・情報セキュリティ事件・事故発生後
例えば	3法令遵守	会社として、情報セキュリティに関する法令を遵守する	情報セキュリティに関する法令を考慮し、社内ルールを策定すること (法令例：個人情報保護法、不正競争防止法)	9	Lv1	**情報セキュリティに関する法令を考慮し、ルールを策定、教育・周知している**	【規則】 ・情報セキュリティに関連する法令を守るための社内ルールを策定すること ・策定した社内ルールを教育・周知すること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 （教育） ・新規受け入れ時、かつ、１回／年 （周知） ・定常的に、かつ、ルールの改正時に周知すること	【規則改定の例】 ・個人情報保護法、GDPR、不正競争防止法等の情報セキュリティに関する法令・規則の情報収集をを行い必要に応じ規則改定を行っている ・法令の変更内容がルールに則っているか関係部署で確認している（１回／年） ・策定したルールに、見直す頻度を記載している 【教育・周知の例】 ・策定したルールに、教育・周知頻度を織り込んでいる ・eラーニングで教育を実施している（年1回）

質問③

質問内容：会社として１つの評価結果を求められておりますが、部門ごとに状況に差があるために、どのようにまとめて良いかがわかりません。まとめ方についてのアドバイスや、他社様における事例等あればお願いします。

回答：IT部門とユーザー部門で対応状況に差がある場合などは、各項目を実施する主たる部門での対応状況を基にご回答頂くのも良いかと存じます。

一方で、サイバーセキュリティの観点では、攻撃者は侵入可能なところ(脆弱なところ)を狙うという傾向があります。

例えばIT部門の中でも対応状況に差があり、ある部署は対応できていて、ある部署は未達成などといった場合には、低い方に合わせて頂くと、現状のセキュリティリスクを正しく反映できるのではないかと存じます。

情報交換例)**各社様にて部門ごとの対応状況まとめに関する事例があればご紹介願います。**

質問④

質問内容：「評価の根拠記入欄」について、どの程度具体的に記載すればよいのでしょうか？
参考とすべき見本回答等はございますでしょうか？

回答：記入いただいた「達成条件評価」や「評価の根拠記入欄」に対して、自工会/部工会から何らかのチェックや是正を行う事はありません。貴社内や評価結果を共有したい会社様が、評価した理由を把握できるレベルで記入いただければ結構です。チェックシートの「他社事例」を参考に記入いただくのが良いですが、細かく記載するのが難しい場合は、規則やシステムの制定/導入有無や、今後の予定等を簡潔に記載いただければ結構です。

《入力例》

No.	達成条件	評価の根拠記入欄
1	自社の情報セキュリティ対応方針(ポリシー)を策定している	情報セキュリティポリシーとして『情報セキュリティ規則』を〇〇年〇月に制定済み
17	サイバー攻撃や予兆を監視・分析をする体制を整備している	現状実施できていない。今年度中にSOCを設置し、予兆検知等を実施予定
28	電子メールのマルウェア感染に関する社内への教育を行っている	標的型攻撃メール訓練を年2回、イントラでの注意喚起を適宜実施
85	サーバー等の設置エリアは、施錠等で入場を制限している	サーバー設置場所にICカードによる入退場認証システムを設置済
103	インターネットと社内ネットワークとの境界にファイアウォールを設置し、通信を制限している	ファイアウォールを設置して通信を制限済

質問⑤

質問内容：　自己評価の進め方や考え方について教えてください。
他社がどのように対応したかの事例があれば知りたいです。

回答：

＜自己評価の進め方や考え方＞
自動車産業ガイドの自己評価は、**自己評価の点数アップが目的ではありません。**
是非、**セキュリティレベルアップが必要なポイントの点検（気づき）**と**セキュリティレベルアップ**に繋げて
いただけますと幸いです。

＜他社の取組み事例＞
自動車産業ガイドの「他社事例」の内容を参考にしていただければと思います。
また、複数のITベンダー様やセキュリティベンダー様へご相談いただいたり、
本活動（自工会・部工会の「よろず相談会」）の場を活用いただき、参加会社様から教えていただけそうでしたら、
情報共有いただくことも良いと思います。

＜参考：今後のよろず相談会開催予定＞　※申込期限/人数制限にご注意ください
・12/1　：第4回　日常運営について（規定やルールの整備、社内体制の整備）
・12/15　：第5回　技術対策について（ウイルス対策、セキュリティ監視、ランサム対策）

質問⑥

質問内容：弊社はISO27001を取得しておりませんが認証を取得できるレベルにはなりたいと考えています。このセキュリティチェックシートはISO27001に関連性がある項目となっているでしょうか？ISO27001との関連性を考慮しつつ評価を進められますでしょうか？

回答：自工会/部工会サイバーセキュリティガイドラインは特定の認証等に準拠して作成されているわけではない為、

本チェックシート内容を達成したからISO27001を取得できる、取得できるレベルになるといったことはございません。

ISO27001では体制の確立やリスクアセスメントの実施、セキュリティポリシーの策定や対策の実施、セキュリティトレーニングへの取り組み等が求めらます。本セルフチェック活動での評価結果への取り組みと、ISO27001認証取得レベルを目指す取り組みを予め比較しながら対応を進めることで、効率よく対応ができるのではないかと考えます。

情報交換例)**各社様にてISO27001と関連した評価の事例があればご紹介願います。**

質問⑦

質問内容：弊社での現状の取り組み段階は、規程の策定までは完了している状況です。しかしながら規定に基づいた実績の把握までは時間が掛かっている状況で、1点なのか2点なのかで迷ってしまいます。評価方法についてアドバイスをお願いします。

回答：

ご質問は、達成条件に「規定の策定」とはべつに達成基準が設定されているケースに関してと思われます。基本的に、複数の達成基準が設定されている場合、すべての基準が満たされている場合に「対策完了（2点）」となります。

例えば、No.9「情報セキュリティに関する法令を考慮し、**ルールを策定**、**教育・周知している**」との達成条件の場合、「**ルールを策定**」と「**教育・周知している**」の二つが設定されていますが、ルールを策定し、教育・周知も実施できている場合は２点、ルール策定のみ実施できていて、教育・周知ができていない場合は「対策中（1点）」となります。「実績の把握」ということですが、必ずしも従来よりレベルが上がっている必要はなく、現状に合わせた点数をつけてください。

ただし、本ガイドラインは監査目的や第三者認証を求めるものではなく、あくまでもセルフチェックの形をとっております。評価結果に対して自工会/部工会から何らかのチェックや是正を行う事もありませんので、評価者の解釈で回答いただいて問題ありません。

質問⑧

質問内容：　対象カテゴリーにある「パートナー企業のリスク管理」の項目において、パートナー企業の数が多数に及ぶため、各社ごとの内容協議、調整に非常に手間がかかり、短期間での対応が困難です。
効率の良い評価の進め方はありますでしょうか？

回答：

全てのパートナー企業を一律に進めることは大変という困りごとと理解いたしました。
自社のビジネス影響の大きな企業から優先して、計画的に、取り組みを始めていただくことが大切と思います。

まずは、協力いただける取引先様１社に協力いただいて、進め方の雛形を作り、それから拡大いただけると進めやすいと思います。

また、No.42「重要な機密情報を取扱うパートナー企業のセキュリティ対策状況を把握している」の項目など、自工会・部工会の本活動「セキュリティ対策状況の自己評価」をご活用いただくことで、個社が個別で実施されるよりも、効率的に実施いただけると考えます。（自己評価結果を取引元へ共有）

情報交換項目例）

・各社様で工夫されているの取組みがございましたら、ご紹介いただけますでしょうか？

質問⑨

質問内容：規定やルール等を明確化した文書の策定を求める項目が複数ありますが、どの程度のものを作成する必要があるのでしょうか？他社事例の模範解答の選択肢のうち１つでも当てはまるものがあれば、達成を考えてよいのでしょうか？

回答：他社事例はあくまで例となりますので、達成基準を基に、対応状況をご判断ください。

IPAの「中小企業の情報セキュリティガイドライン」に、規程のサンプルもありますので活用ください。

自工会/部工会・サイバーセキュリティガイドラインV2.1解説書（日本語版）にも、どういった内容を記載すればよいのかを記載しておりますので、ご活用ください。

中小企業の情報セキュリティ対策ガイドライン 付録2

情報セキュリティ基本方針（サンプル）

中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。

情報セキュリティ基本方針

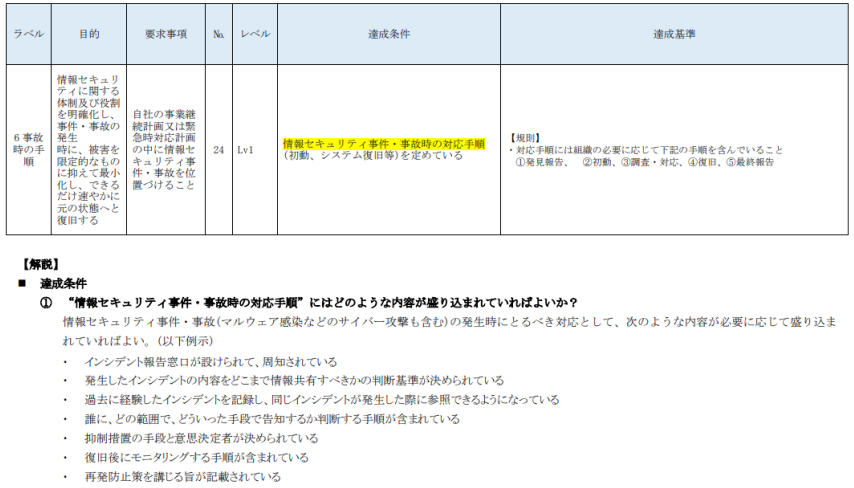
株式会社○○○○（以下、当社）は、お客様からお預かりした当社の情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1.経営者の責任

当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2.社内体制の整備

当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。



ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
6 事故時の手順	情報セキュリティに関する体制及び役割を明確化し、事件・事故の発生時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する	自社の事業継続計画又は緊急時対応計画の中に情報セキュリティ事件・事故を位置づけること	24	Lv1	情報セキュリティ事件・事故時の対応手順（初動、システム復旧等）を定めている	【規則】 ・対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、　②初動、③調査・対応、④復旧、⑤最終報告

【解説】

■ 達成条件

① “情報セキュリティ事件・事故時の対応手順”にはどのような内容が盛り込まれていればよいか？

情報セキュリティ事件・事故(マルウェア感染などのサイバー攻撃も含む)の発生時にとるべき対応として、次のような内容が必要に応じて盛り込まれていればよい。(以下例示)

- インシデント報告窓口が設けられて、周知されている
- 発生したインシデントの内容をどこまで情報共有すべきかの判断基準が決められている
- 過去に経験したインシデントを記録し、同じインシデントが発生した際に参照できるようになっている
- 誰に、どの範囲で、どういった手段で告知するか判断する手順が含まれている
- 抑制措置の手段と意思決定者が決められている
- 復旧後にモニタリングする手順が含まれている
- 再発防止策を講じる旨が記載されている

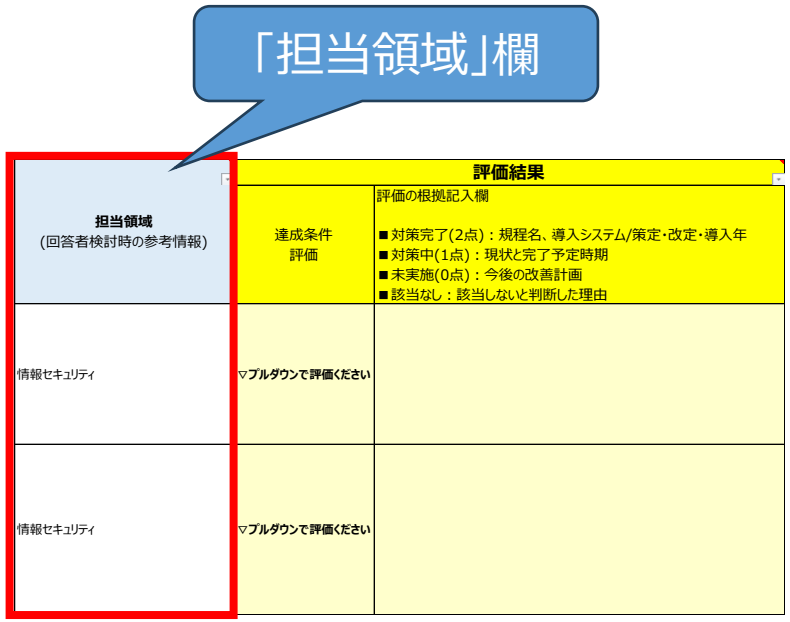
情報交換例)**各社様にて規程やルール策定の事例があればご紹介願います。**

質問⑩

質問内容：自部署だけでは全ての項目に対して回答ができず、関係する他部署に回答をお願いしないと評価が進められない状況です。他部署と連携して進めるにあたってのやり方、アドバイスなどを教えていただけないでしょうか。

回答：チェックシートのL列に「担当領域」という欄を設けています。これは、自組織内で回答を担当する方が不明確な場合に、参考としていただく為の欄です。各要求事項に対し、実施責任を持つと考えれる担当領域名（機能）を記載しております。個社毎に状況は異なると思いますが、参考に担当部署へ入力依頼いただくのが良いと思います。依頼の際、N列の「評価の根拠記入欄」に評価の根拠を入力いただく事により、次年度自身がどのように評価を行ったのか把握できたり、他部署の考え方を把握することができます。

担当領域	機能
情報セキュリティ	組織全体でのセキュリティ活動を推進するための方針とセキュリティ各種ルールの策定や周知を行う役割を担う
IT	情報機器や情報システムを管理し、それらに対する適切なセキュリティ対策実施や運用の役割を担う
法務	機密情報や個人情報に関する法令に基づき、組織内のルールを策定し、パートナー企業との各種契約締結を管理する役割を担う
購買・調達	自組織の守るべき資産のサプライチェーンにおける流れを把握し、パートナー企業のセキュリティ対策状況を管理する役割を担う
人事	入社や退職、契約期間満了に伴う様々なセキュリティ対策を実施する役割を担う
リスク	組織全体のセキュリティに関連するリスクを評価し、事業継続計画の策定や見直しを行う役割を担う
総務	自社拠点への入退場ルールや拠点内でのセキュリティルールの策定や運用を行う役割を担う



質問⑪

質問内容：　ガイドラインの自己評価を進めるにあたり、実施している対応が問題無いかの判断が難しいと感じています。
F/Wやサーバー、クライアントのセキュリティ的な設定や、ログ取得の項目及び設定方法など、推奨設定などご提示頂けますと幸いです。

回答：

F/W(Fire Wall: ネットワーク通信を制御する仕組み)やサーバ、クライアント端末の**購入先であるITベンダー様**や**セキュリティベンダー様**へご相談いただくと良いと思います。

基本的には、使用していない通信や機能を塞ぐことで、攻撃者に利用させないようにするなどの工夫をされる事例をお聞きします。

また、一度対策されていても、**あらたな脆弱性や攻撃手法へ対応できているかを確認**する「セキュリティ診断」を定期的に実施することも、対応が必要な箇所を見つけるためには重要になります。

＜参考：セキュリティ診断の事例＞

・N/W機器やサーバ機器 の脆弱性を診断する　　：プラットフォーム診断（サーバ/ネットワーク機器/OS/ミドルウェアなど）
・作成したアプリケーションに設定や脆弱性を診断する　：アプリケーション診断

質問⑫

質問内容：社内教育・訓練の実施と内容見直しについて、自己評価をどう進めていいのかわかりません。

回答：自工会/部工会・サイバーセキュリティガイドラインV2.1解説書（日本語版）にて、教育に何を盛り込むのか、訓練で何を実施するのかといった解説を掲載しておりますので、ご活用ください。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
3 法令順守	会社として、情報セキュリティに関する法令を順守する	情報セキュリティに関する法令を考慮し、社内ルールを策定すること (法令例：個人情報保護法、不正競争防止法)	9	Lv1	情報セキュリティに関する法令を考慮し、ルールを策定、教育・周知している	【規則】 ・情報セキュリティに関連する法令を守るための社内ルールを策定すること ・策定した社内ルールを教育・周知すること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 (教育) ・新規受け入れ時、かつ、1回／年 (周知) ・定常的に、かつ、ルールの改正時に周知すること

【解説】

■ 達成条件

① ルール策定・教育実施・周知の3つの観点があるが、情報セキュリティに関する法令の教育にはどのような内容を盛り込むべきか？

法令そのものの詳細や解釈を教育するのではなく、法令を基に策定した社内ルールに対しての教育を行うことが重要である。社内ルールの遵守、理解度向上が目的となるため、遵守すべき事項、遵守できない場合の組織としてのリスクの説明が盛り込まれていればよい。

② 教育効果の確認まで実施するべきか？

当要求事項においては、教育効果の確認までは含まない。ただし、投資対効果の明確化や今後の改善のためには実施する方が望ましい。

■ 達成基準

④ "定常的"な周知の具体的な頻度や方法は何か？

例えば、1回／年 の頻度で、メールやチャット・資料配布という方法がある。従業員が、法令違反しないための周知方法であれば、どのような方法でも良い。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
7 日常の教育	マルウェアや機密情報についてリスクや正しい取り扱いを理解させ、情報セキュリティ事件・事故を予防する	従業員として注意することを教育していること	31	Lv2	標的型メール訓練を実施している	【規則】 ・標的型メール訓練を実施すること ・万が一開封した時の対応も訓練内容に含めること ・訓練内容や方法を振返り、次回の訓練を改善すること 【対象】 ・電子メールの利用者 【頻度】 ・1回以上／年

【解説】

■ 達成基準

① "標的型メール訓練"として行うべき訓練内容は何か？

実践形式の訓練が求められる。具体的には、自社のビジネスを模倣したダミーのメールを従業員に対して一斉配信し、そのメール内のリンクをクリックしたかどうかを確認する形式が一般的には多く見られる。自組織の業務に関連がある件名や本文だとしても、不審なファイル・リンクが含まれたメールに対しては、不用意に反応しないことを啓発する上でこのような方法が効果的である。

※「メール訓練手引書」（日本CSIRT，2022年）が標的型メール訓練の計画から改善までの手引きとして使用することができる。
参考：https://www.nca.gr.jp/activity/imgs/nca-mail-exercise-guidebook-v1.0.pdf

質問⑬

質問内容：No.16「サイバー攻撃や情報漏えいの新たな手口を知り、対策を社内部署へ共有している」ですが、自己評価を進めるにあたって、全社員に分かり易く説明することと、理解度の確認方法を知りたいです。

回答：まずは、情報を集めるところから始めてください。例えば、IPAの「コンピュータウィルス・不正アクセスに関する届け出について」や「ビジネスメール詐欺の事例集」では、関連する資料がダウンロード可能です。
コンピュータウイルス・不正アクセスに関する届出について | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
ビジネスメール詐欺の事例集を見る | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

また、一般社団法人 JPCERT コーディネーションセンター （JPCERT/CC） では、国内外で発生するコンピューターセキュリティインシデントの報告を受け付けていて、統計や特筆すべき事例などのレポートをダウンロード可能です。
JPCERT コーディネーションセンター インシデント報告対応レポート

IPAでは、動画での教育コンテンツも公開しております。
映像コンテンツ一覧 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

これらの情報の中から、従業員向けに動画の視聴を案内したり、事例や対策を**簡単に取りまとめ**、イントラや情報セキュリティに関する説明会で社内周知を行うのが良いと思います。ただ、上記の資料やレポートをそのまま従業員に展開してもなかなか読んでもらえませんので、ポイントを絞って、重要な点を伝えるのが良いと思います。その後E-Learning等で従業員の理解度を定期的にチェックし、結果が悪い点については、後日社内へ周知を行い改善につなげるのが良いと思います。

情報交換例）　**・各社様における情報収集の手段やご紹介願います。**

質問⑭

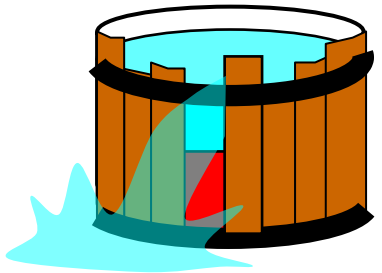
質問内容：　No.90「不正侵入や不正行動を監視している」に対して、社内のすべての重要な場所の監視ができた時点で達成とすべきなのか、すべての重要な場所のうち1つでも監視ができた時点で達成としていいのでしょうか。

回答：

・No.90の＜目的＞、＜要求事項＞を考慮いただき、対応できている所を見つけるのではなく、**セキュリティレベルアップが必要なポイントの点検（気づき）とセキュリティレベルアップに繋げていただければと思います。**

＜目的＞　**サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ**
＜要求事項＞ 社内への入退場において、**セキュリティ事故(主に不正侵入、不正持ち出し、情報漏えい、不審行動)を抑制する対策を行っていること**

・セキュリティは「桶の理論」で説明されることがあります。
一番弱い所から破られるという理論です。
１つでも監視ができた時点で達成とするより、すべての重要な場所の監視ができた時点で達成としていただく必要があります。



質問⑮

質問内容：No.150「システムが停止した際も業務が遂行できる代替手段を用意している」に対して、どのくらいの期間システムが停止することを想定した代替手段の検討が必要でしょうか。

回答：どの様なリスクを想定するかによって変わってきます。

例えば地震等の災害によって電源が喪失した場合、一般的には3日間程度復旧に時間がかかると言われています。

サイバー攻撃の場合、システムをバックアップから復旧することができる時間を考慮する必要があります。

自社のビジネスがどれくらい停止することが許容できるのか検討し、その中でどのくらいの操業レベルまで復旧するか、

取引先とも相談の上検討を進めて頂くのが良いかと存じます。

情報交換例)**各社様にてシステム停止時の代替手段、停止期間の想定の事例があればご紹介願います。**