よろず相談会第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）-

2023年12月1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致します。
	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（1/3）

No.	質問
1	弊社には、専門（専任）組織として情報セキュリティを推進する組織が存在しません。また、情報セキュリティを専任で担当するメンバーも存在しません。（兼務にて対応中） ⇒このような会社において、**規定やルールの整備の主管部門をどこにし、どのような体制で進めるのが良いのか**、悩んでいます。また、**部門へ業務を依頼する際の、セキュリティ事務局の関わり方のアドバイス**をいただきたい。
2	万が一**サイバー攻撃にあった場合の社内体制を整備**したいですが、**外部への相談**は「誰に」「どのように」すべきか悩んでおります。
3	**規定やルールを作るにあたっての手順**が知りたいです。 また、規程を作成する上で、最終的なゴールはどのように定めているか。**「これでよし」とする基準の設定方法**について知見があれば知りたい。
4	**規定文章**系ですが、**どの程度のものを作成**する必要があるのでしょうか？ サンプルサイトがあれば、ご紹介いただけないでしょうか？
5	**規程やルールの事例**を知りたい。自社で既にあるルールなどをチェックシートの内容を充足するよう更新することの負荷が高く、他社では**どのように社内体制を整備し規程改定へ繋げているのか？**

本日取り上げさせて頂くご質問一覧（2/3）

No.	質問
6	社内への**持込み**＆社外への**持ち出し**、社内における**撮影、録音**に関する**ルール**の**作り方、運用の仕方**を知りたいです。 （自動車産業ガイドライン：No.91,94,95,96）
7	**情報資産管理台帳**の**作り方、運用の仕方**　（IPAリスク分析シート活用との関係を知りたい）
8	**情報流出対策**として、**USBメモリやSDカード等の機器使用ルール**の調整をしています。 設備やカメラ等からパソコンにデータを入れるといった使用用途がある為、暗号化や全面的禁止ができず、管理簿で管理をしていますが回数が多く手間が掛かります。他社では**どのように対応しているか**教えて頂けないでしょうか。
9	法令改正等をサーチする具体的な手段、参考にできるホームページなどがあれば教えていただきたい。 （自動車産業ガイドライン：No.12）
10	**情報セキュリティ対応方針(ポリシー)、規定、ルール**を作成したものの**社内浸透が不十分**だと感じています。 **浸透＆順守させるための取り組み**の例があればご紹介いただきたくお願い致します。

本日取り上げさせて頂くご質問一覧（3/3）

No.	質問
11	**規定やルールの適用状況の確認方法**や**頻度、改善に対する取り決め**など、具体的な事例をお聞きしたいです。
12	**社員教育の進め方**について教えてください。 （1）各部のセキュリティ管理者　（2）社員
13	**セキュリティ事故時**に関する下記項目について、[No.17]**予兆管理体制**、[No.18]**事故時の責任と役割**、 [23][24][26]**事故時の対応**について、**何を求められているのか**を教えてください。
14	セキュリティ事故発生時には**届け出や公表**することが必要と考えますが、いざセキュリティ事故が発生した際に、どのレベルで公表すべきなのか、また経営側との**基準設定**の際に、**どのように決めていくと良いのか**アドバイスいただけるとありがたいです
15	**自己評価の仕方**において、現状規程は策定できているが、守らせているか？等の実績の把握まで時間が掛かり、 **1点なのか2点なのか評価で迷っています**。（どの項目に対しても） また、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。

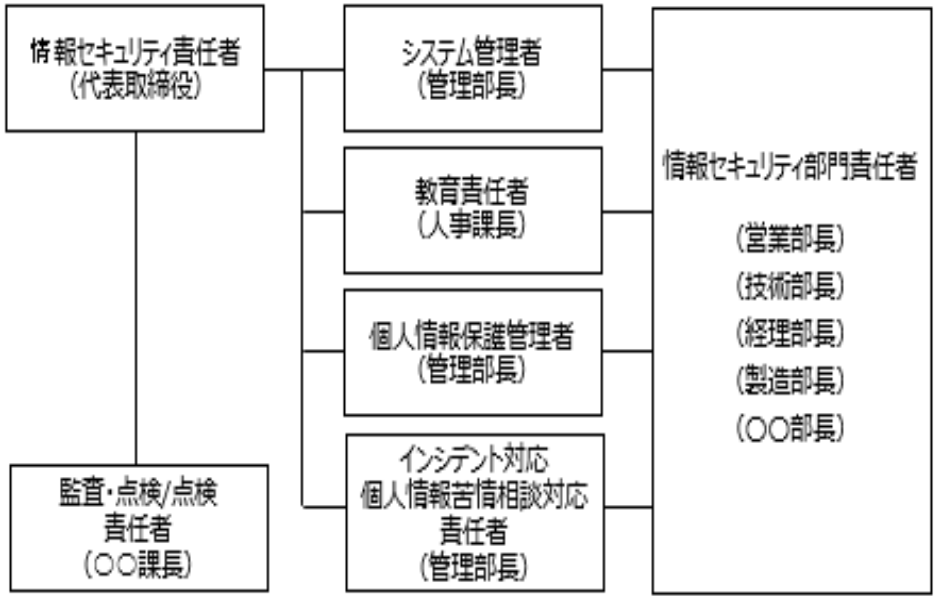
時間が足りない場合は、すべての質問に対してお話できない可能性がございます。
時間に余裕があれば、ここに記載していない質問も用意しておりますので、引き続き取り上げさせて頂きます。
ご理解の程よろしくお願い致します。

質疑応答

質問①

弊社には、専門（専任）組織として情報セキュリティを推進する組織・担当が存在しません。
このような会社において、規定やルールの整備の主管部門をどこにし、どのような体制で進めるのが良いか。
また、部門へ業務を依頼する際の、セキュリティ事務局の関わり方のアドバイスをいただきたい。

回答：
セキュリティの体制を整備にあたっては、IT部門のような特定の部門に特化せず、**全社横断的な体制を組むことが重要**と思います。
全社横断的な体制を構築し役割を明確にすることにより、**それぞれの部門が主管する範囲が明確**になり、**規定やルールの整備**や**セキュリティの実務**を行っていけるようになるかと思います。



・情報セキュリティ責任者（CISO)を任命する。
・情報セキュリティ責任者の元にセキュリティ委員会を設置する。
・情報セキュリティ部門責任者として各部門長を任命する。
・上記組織とは独立した監査機能を置く。

なお、この体制は各社様の組織・部門の役割等に合わせ、適切に設定頂ければと思います。

【ご参考】 中小企業の情報セキュリティ対策ガイドライン第3.1版　1 組織的対策　000055794.docx (live.com)

情報交換例）　**・各社様における体制構築の事例について可能な範囲でご紹介願います。**

質問②

万が一サイバー攻撃にあった場合の社内体制を整備したいですが、外部への相談は
「誰に」「どのように」すべきか悩んでおります。

回答：
サイバー攻撃に気づいたらまずは被害の拡大を抑える必要があります。被害の拡大を抑えるための助言をしてもらえるところに相談するのが良いと思います。早急な対処が必要ですので電話や対面など直接コミュニケーションがとれるところが望ましいです。
具体的には**有事の際に相談を受けるサービスなどを事前に契約した会社**の窓口であったり、**社内インフラや社内システムの運用保守を委託している会社**などに相談するのが現実的だと思います。サイバー保険などを契約すると有事の際に相談するサービスがセットになっている場合もあります。相談先に心当たりがない場合はこうしたサービスを利用できるように事前に準備しておくことをおすすめします。
取引先によっては発生を認知したタイミングで連絡して欲しいとの依頼を受けている場合があるかと思います。その場合はすみやかに連絡してください。連絡時に何を伝えるか事前に取り決めておくことが重要です。

その後、**各都道府県警察本部のサイバー事案相談窓口**などに相談してください。また、個人情報の漏洩などの可能性がある場合は**個人情報保護委員会**への報告も必要になります。相談や報告の仕方はそれぞれのHPに記載があります。
海外拠点の場合は拠点立地国の法律に従ってください。

質問③

規定やルールを作るにあたっての手順が知りたいです。また、規程を作成する上で、最終的なゴールはどのように定めているか。「これでよし」とする基準の設定方法について知見があれば知りたい。

回答：
規定やルールの作成手順は一般的に以下が良いと考えます。
①公開されているテンプレートを入手する
　（例：「情報機器の利用ルール」では規定サンプル「IT機器利用」（※）を活用）
②テンプレートに従い、自社の事情／環境を考慮し、該当部分を修正する
　（例：情報機器では、どんな端末／ソフトウェアを支給しているか）
③内容を鑑みて適切な管轄部署（所管部門）を検討し、規定やルールの責任者を決定する
　（例：「情報機器の利用ルール」では、機器提供／管理を行うIT部門長）
④全社員に対して周知・公開を行う
　（例：社内ポータルサイトへ掲載する、社内報で周知する、メールで展開する）

最初から完璧な基準を作るのは難しく、まず一度作成し周知したうえで、利用者からの意見（〇〇については記載がないのか？ ××の部分が不明確、など）や、規定があるにもかかわらず社内で起こってしまったセキュリティ事故への振り返りなどを参考に見直しをかけながら、**より良い規定・ルールに育てていく**のが良いと考えます。

（※）IPAの「中小企業の情報セキュリティガイドライン」の付録５の６

質問④

規定文章系ですが、どの程度のものを作成する必要があるのでしょうか？
サンプルサイトがあれば、ご紹介いただけないでしょうか？

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

また自工会/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）

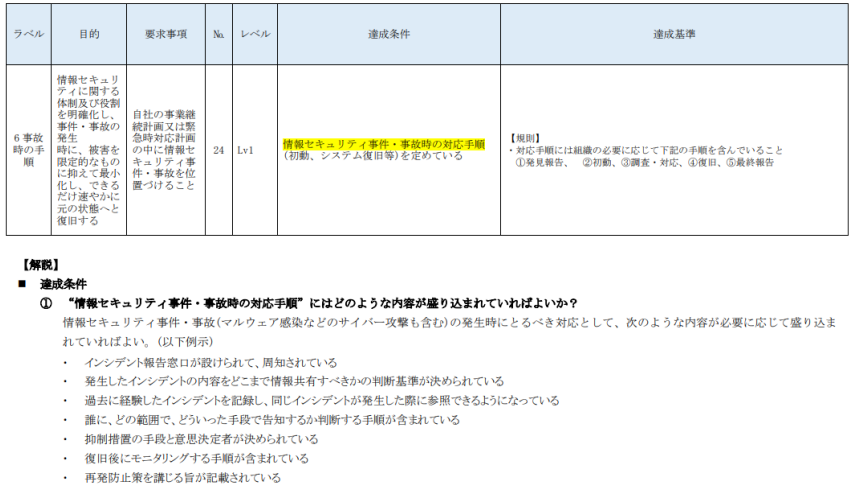
中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。
※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。
※青字箇所は、自社の事情に応じた文言を選択してください。

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	№	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）**その他に良いサンプルをご存じの会社様がおられましたらご紹介願います。**

質問⑤

規程やルールの事例を知りたい。
自社で既にあるルールにチェックシートの内容を充足するよう更新することの負荷が高く、他社ではどのように社内体制を整備し規程改定へ繋げているのか？

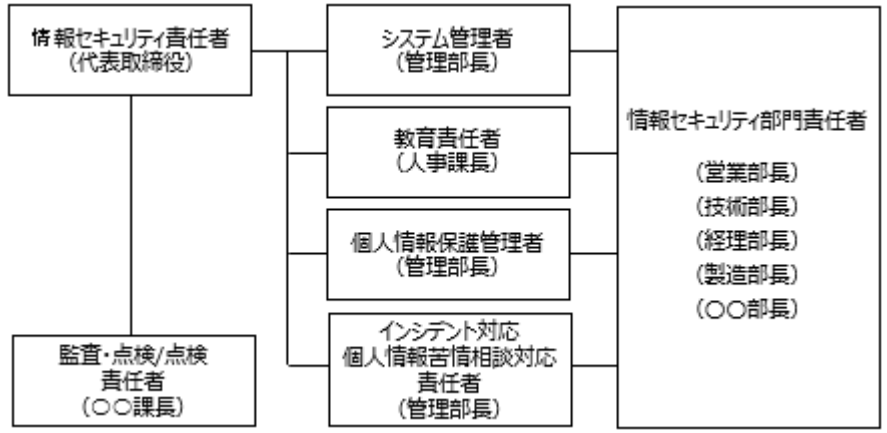
回答：
質問①で回答と重複する部分もありますが、まずは社内の様々な部門を入れた体制構築を行います。

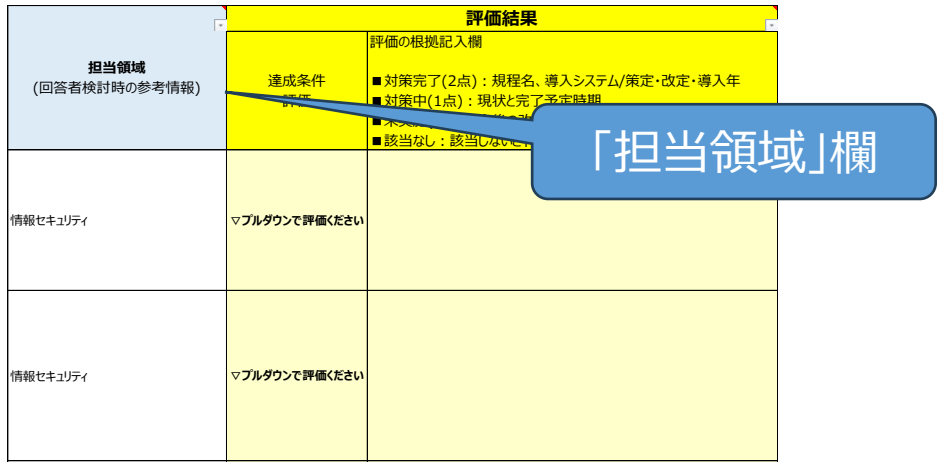
経営トップを入れた体制を構築することで各部門が管掌する業務が分類されていき、**それぞれの管掌する部門でルールを整備**していくことが出来るかと思います。
なおセキュリティチェックシートの担当領域欄に参考として一般的な主管部門を掲載しています。こちらもご参考にして改訂して頂ければと思います。

また初回以降は自工会HPに掲載しているガイドラインの変更点を確認して修正頂くことで毎回全体を見直さなくても良くなるかと思います。

情報交換例）

・各社様における規則改定の事例について可能な範囲でご紹介願います。





質問⑥

社内への持込み＆社外への持ち出し、社内における撮影、録音に関する
ルールの作り方、運用の仕方を知りたいです。

回答：
PCの持ち込み、持ち出しについてはIPAなどがルールのサンプルを公開していますのでそれを参考にするのが良いと思います。
撮影、録音についてはまずは社内のどこで制限するか、許可するかなどの検討が必要です。社内一律禁止が現実的ではない場合もありますので必要になった場合どのようなルールで許可するか、録音や撮影データの扱いをどのようにするかなどを検討し各社様でリスクを検討いただくのが良いと思います。
盗聴対策に関しては盗聴されると経営上リスクとなる会議、会話が行われる場所を限定するなどリスクを局所化した上で専門業者などに対策を依頼するのが良いと思います。
PC持ち込み＆持ち出し、撮影、録音いずれの場合もそれぞれに関わる**情報資産に対するリスクの大きさ**によって自社が**どのようにそれを守るべきなのかという視点**で考えることが重要です。
参考：
IPA 中小企業の情報セキュリティ対策ガイドライン
付録5：情報セキュリティ関連規程（サンプル）（全45ページ）(Word:167 KB)
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

情報交換例）**各社様においてルールの作り方や運用の仕方の事例がありましたらご紹介願います。**

質問⑦

情報資産管理台帳の作り方、運用の仕方。IPAリスク分析シート活用との関係を知りたい。

回答：
会社の情報資産台帳を作成するには、規模にもよりますが、特定の部署の担当者だけで資産洗い出しを実施するのは非現実的だと考えます。部門／事業部ごとに窓口となっていただける担当者を選出いただき、**各組織の業務内容を理解している人に協力いただける体制を作る**ことから始めるのが良いと考えます。

窓口が決まれば、ご認識いただいている**IPAリスク分析シート（※）を活用**し、記入例を参考にしながら情報資産台帳の作成依頼を各窓口の方にお願いします。規模に応じて、例えば部署ごとの記入シートをそれぞれ用意するなど、記入者が作業をしやすい方法を検討しても良いと思います。会社によっては、部署レベルで業務処理基準書や業務マニュアル、予算管理台帳、個人情報を含む人事情報などの情報資産をたくさん保持している場合もあると考えます。

運用については、例えば「毎年〇月までに更新」など事前に実施時期を決めておき、各窓口の方に記載内容の確認と更新をお願いする、といった定例業務にしてしまうと、毎年忘れずに最新化ができるかと思います。

（※）IPAの「中小企業の情報セキュリティガイドライン」の付録７

情報交換例）**各社様における情報資産管理台帳に関する事例がありましたらご紹介願います。**

質問⑧

情報流出対策としてUSBメモリやSDカード等の機器使用ルールの調整をしています。
設備やカメラ等からパソコンにデータを入れるといった使用用途がある為暗号化や全面的禁止ができず、管理簿で管理をしていますが回数が多く手間が掛かります。どのように実施しているか参考までに教えて頂けないでしょうか。

回答：
外部記憶媒体の利用においては**許可された物のみ業務で利用**することや**利用履歴を管理**することで、**情報漏洩やウイルス感染を防止することが重要**になるかと思います。まずは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。またWindowsの機能としては下記のような物もあります。
・外部記憶媒体の利用を禁止したり許可された媒体のみ利用可能とする。
・イベントログに利用履歴を保管する。

※上記機能は使用しているWindowsのエディションにより利用可・不可がありますので、MicrosoftのHP等をご確認ください。
上記以外でも使用しているウイルス対策ソフトや資産管理ツールによっては事前に許可された機器しか使えないようにしたり使用記録を保管する機能を持ったものがあります。自社で利用しているツールで実現出来ないかご確認ください。

暗号化については**社外持ち出し用**として暗号化機能を持ったUSBを用意し、**許可制**にしておくことで対応する方法もあります。

情報交換例）　**・各社様における実施事例がありましたらご紹介願います。**

質問⑨

法令改正等をサーチする具体的な手段、参考にできるホームページなどがあれば教えていただきたい。
（弊社では法務部がありません。総務省の情報セキュリティ関連の法律・ガイドラインがあるのは知っていますが、
実務運用がうまくできず、困っています。）

回答：
情報セキュリティの関連法に限らず、企業活動を行う上で関係する法律があるかと思います。まずはそれらの法律の改正を現状どのように把握する社内体制なのかをご確認いただき、すでに把握する体制があればそれの運用に情報セキュリティの関連法も併せて運用頂くのが良いと思います。
もし、現状そういった運用がないのであれば企業活動に必要な関連法まとめて改正を把握する方法を各社様の顧問弁護士にご相談いただくのが良いと思います。

参考：
内閣サイバーセキュリティセンター(NISC) 関係法令Q＆Aハンドブック
https://security-portal.nisc.go.jp/guidance/law_handbook.html

情報交換例）　**・各社様における情報収集の事例について可能な範囲でご紹介願います。**

質問⑩

情報セキュリティ対応方針(ポリシー)、規定、ルールを作成したものの社内浸透が不十分だと感じています。
浸透＆順守させるための取り組みの例があればご紹介いただきたくお願い致します。

回答：
あくまで弊社の一例ですが、以下にご紹介します。
・ポイントを簡潔に記載した配布物を用意（パソコンに設定できる壁紙、紙のリーフレット、パソコン等に貼れるシールなど）
・各事業所の掲示板に、情報セキュリティの注意喚起を行うためのポスターを作成し掲示（数か月に一度、張り替え）
・啓発動画を作成し、事業所に設置されている社内放映テレビにて定期的に流す
・月１回の頻度で、全パソコン利用者（役員・協力会社社員も含む）へ情報セキュリティメールマガジンを送付
・年１回の頻度で、情報セキュリティe-learningを全パソコン利用者に実施。受講が確認できない場合、一部システム利用の停止を行うなど罰則付きで行うことで、情報機器を扱う方へ漏れなく浸透させている
・年１回の頻度で、全パソコン利用者（役員・協力会社社員も含む）へ情報セキュリティの理解度アンケートを実施

情報交換例）

各社様における社内浸透＆順守させるための取組の事例がありましたらご紹介願います。

質問⑪

規定やルールの適用状況の確認方法や頻度、改善に対する取り決めなど、具体的な事例をお聞きしたいです。

回答：

状況の確認としては各部門の役割に応じて定期的に確認を実施し、不足事項の改善を進めることが一般的かと思います。
確認方法は結果の正確性、自律的な改善を行うことが重要と思います。

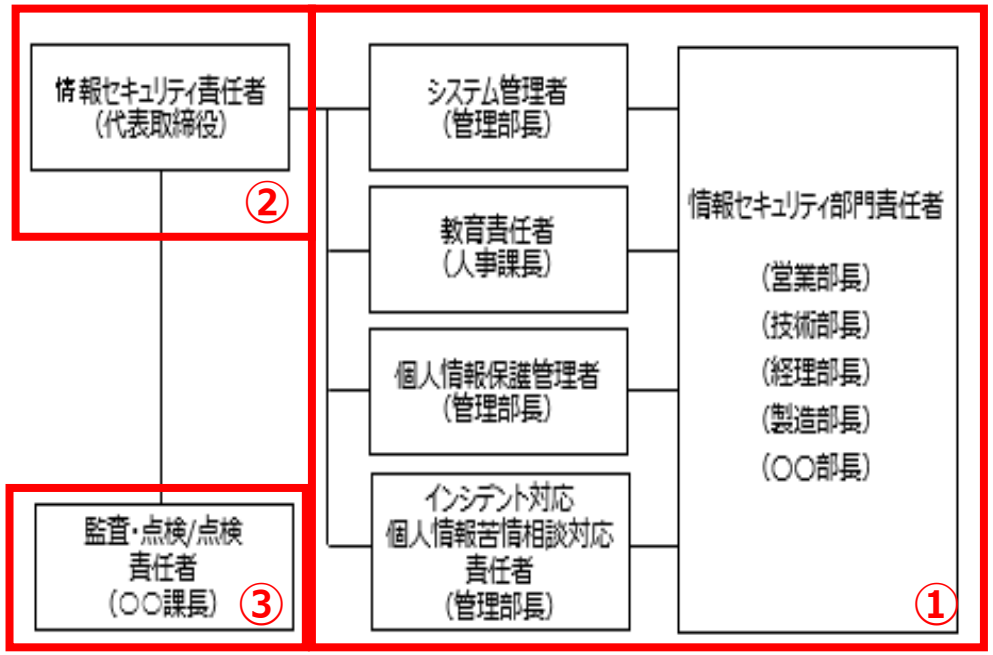
下記に体制の所で例示した体制で実施する場合の事例を紹介します。

①：各部門で確認を実施し、不足している内容を明確にし
　　改善計画の立案・実施を行う。

②：全体を統括する部門が各部門の実施、改善方法・状況の
　　確認・アドバイスを行う。

③：独立した監査部門による監査を実施する。
　　（外部コンサルタント等による監査でも可）

※①、②は年一回程度、③は２，３年に一回程度でも可



情報交換例）　**・各社様における体制整備の事例がありましたらご紹介願います。**

質問⑫

社内教育の進め方について、教えてください。
（1）各部のセキュリティ管理者　（2）社員

回答：

（1）各部のセキュリティ責任者

まずはセキュリティ規定に明示されている役割を周知、理解してもらうための教育が必要になります。次の段階では実践のための考え方や事例などの理解、グループワークなどを通じて日々の活動で必要な知識を習得することとなります。
具体的にはIPAが公開している「サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集」を活用した社内教育や「情報セキュリティ管理者育成コース」などのセキュリティ教育サービスを行う会社などに委託するのが良いと思います。
参考：IPA サイバーセキュリティ経営ガイドライン Ver 3.0実践のためのプラクティス集
https://www.ipa.go.jp/security/economics/csm-practice.html

（２）社員

最初に行うのは情報セキュリティのポリシーやルールなど各社様で作成したものを周知、理解してもらう教育が必要です。ルールが定着してきたらセキュリティ教育を内製してもよいですし、セキュリティ教育サービスを提供する会社に委託しても良いと思います。教育を内製する場合の参考資料としてはIPAの情報セキュリティ・ポータルサイト「ここからセキュリティ」などを活用していただくのが良いと思います。
参考：IPA ここからセキュリティ
https://www.ipa.go.jp/security/kokokara/

情報交換例）　**・各社様で実施している教育の事例がありましたらご紹介願います。**

質問⑬

セキュリティ事故時に関する下記項目について、
[17]予兆管理体制、[18]事故時の責任と役割、[23][24][26]事故時の対応について、何を求められているのかを教えてください。

回答：

セキュリティ事故発生時は素早い対応により被害の最小化が必要になります。

①検知・初動対応②報告・公表③復旧・再発防止等の観点で平時から体制・手順を整備し、備えておくことで素早い対応を行うことにより事故の影響を最小限に抑えることが重要となります。

[17]予兆管理体制：サイバー攻撃やの予兆を検知し、対応する体制を構築する。

検知は外部の監視サービスを利用し検知に対応する体制を自社で構築しておく場合が多いです。

サイバーセキュリティお助け隊サービス ユーザー向けサイト | IPA

[18]事故時の責任と役割：情報セキュリティ事件・事故の発生に備えて役割・責任範囲、連絡先、報告ルートを整備しておくことが重要です。

[23][24][26]事故時の対応：事件・事故として扱う事象、事件・事故の重要度を決めておき、下記手順を事前に文書化することが必要です。①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告
付録8：中小企業のためのセキュリティインシデント対応手引き（全8ページ）（PDF:1.2 MB）

情報交換例） **・各社様における実施事例がありましたらご紹介願います。**

質問⑭

セキュリティ事故発生時には届け出や公表することが必要と考えますが、いざセキュリティ事故が発生した際に、
どのレベルで公表すべきなのか、また経営側との基準設定の際に、どのように決めていくと良いのかアドバイスいただけるとありがたいです。

回答：
セキュリティ事故の手口や被害によって公表するかを判断する必要があります。
各社での判断は経済産業省が公表している「サイバー攻撃被害に係る情報の共有・公表ガイダンス」が参考になります。
情報共有・被害公表の意義や判断について記載されていますので参考にしてご判断いただければと思います。

参考：
経済産業省 サイバー攻撃被害に係る情報の共有・公表ガイダンス
【別添2】サイバー攻撃被害に係る情報の共有・公表ガイダンス（PDF形式：5,613KB）
https://www.meti.go.jp/press/2022/03/20230308006/20230308006-2.pdf
【別添3】サイバー攻撃被害に係る情報の共有・公表ガイダンス（概要）（PDF形式：1,188KB）
https://www.meti.go.jp/press/2022/03/20230308006/20230308006-3.pdf

質問⑮

自己評価の仕方において、現状規程は策定できているが、守らせているか？等の実績の把握まで時間が掛かり、1点なのか2点なのか評価で迷っています。（どの項目に対しても）また、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：
「守らせている」という表現については、例えばNo.4の**達成条件**に記載があります。ご質問のとおり、厳密には何をもって「守らせている」ことが出来ているかの判断は難しいと思います。そのため、このような表現は**達成基準**には記載しないように努めております。より判断しやすい**達成基準**に記載の内容が全て出来ていると判断できた時点で、2点をつけていただければと思います。例えば、「守秘義務を説明すること」とある場合、説明することが社内で実施できているのであれば、その説明を聞いた人が理解し、期待通りの行動をして守っているかどうかまでの確認が出来ていなくても2点としていただいて構いません。

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)
4	Lv1	**自社の守秘義務のルールを規定し、守らせている**	【規則】 ・自社の守秘義務を策定し、文書化すること ・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること ・退職もしくは期間満了時に会社の機密情報を持ち出さないこと 【対象】 ・役員、従業員、社外要員（派遣社員等）	【守秘義務の記載例】 ・在籍中は、業務上の必要がない限り、会社の情報を他者に伝えない ・社外に機密情報を取り扱う業務を委託する場合、必ず機密保持契約をする ・退職もしくは期間満了時に会社PCや会社の資料を返却させる 【理解させ、守らせることの例】 ・退職もしくは期間満了時の機密情報の回収、退職後の義務の書面または対面での説明をしている ・守秘義務の誓約書の雛型を作成し、入社時に署名している ・従業員の就業規則により、機密情報の守秘義務が明記されている ・守秘義務違反時の罰則を規則に記載している ・退職時マニュアルに守秘義務事項を確認する手順を記載している ・機密管理月間を設けて、守秘義務に関する職場自主点検を実施している

本資料は、別途メールで
送付させていただきます。

アンケートへのご協力、
よろしくお願いいたします。

※ＵＲＬは、チャット欄＆資料送付時のメールへ
掲載させていただきます。

E N D