よろず相談会第1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10月20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

No	質問
1	規程の作成の流れを教えて欲しい、具体的にどう整備していけばよいか迷っています。
2	「持込み・持出し物の制限を行っていること」「社内の撮影・録音において、セキュリティ事故(主に情報漏えい)を抑制する対策を行っていること」について、どの程度（網羅性等）まで実施すべきか
3	「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」の具体的な対象の法令が何かを知りたい。
4	社内体制を整備したいが、ITに詳しいメンバーが少なく、選任は難しい。どういった対応をしているのか知りたい。
5	サイバーセキュリティポリシーおよび手順の作成において、必要な工数および技能の見積もりはどの様に行えば良いのか。
6	小規模企業において、求められる全ての規程を満たすことが難しい。簡易的に対応する方法は無いのか？
7	規程内容の充実を図りたいが、専任者がいなくて整備が進みづらい。他社の意見を聞けると嬉しい。
8	規定・ルールを導入後、社員ひとりひとりに遵守させるために、どのような教育、社内へのアナウンス、周知を行えば良いのか。
9	情報セキュリティに関する意識を高めていく啓蒙活動のやり方に関して教えてほしい。
10	リスクアセスメントを各部署で実施してもらう為に、何を参考に具体的な進め方やガイドラインを決めれば良いのか。

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。

質問①

質問内容：規程の作成の流れを教えて欲しい、具体的にどう整備していけばよいか迷っています。ルールの基準のようなものをどこを参考にすると良いでしょうか。
大手企業向けのサンプルは入手したが、中小企業には厳しすぎる。 サンプルを参考に厳しく作って社内運用を規程に合わせた方が良いのか、それとも現運用に則った緩い規程にした方が良いのか。

回答：
企業規模等企業様毎の様々な事情により大手企業向けと同じ規程で運用することが難しいのは理解致します。
一方で単純に現運用に合わせた緩い規程を作ることも違うように思います。

重要なことは自社にとってのセキュリティリスクが何でその大きさがどの程度なのかを正しく理解すること。
そして、**そのリスクの大きさに見合った強度のセキュリティ施策を落とし込んだ規程・ルールにすること**です。

規程作成に関する考え方について、IPAの「中小企業の情報セキュリティガイドライン」に記載があり、規程のサンプルもありますので活用ください。

質問②

質問内容：No９１「持込み・持出し物の制限を行っていること」No９４～９６「社内の撮影・録音において、セキュリティ事故(主に情報漏えい)を抑制する対策を行っていること」について、どの程度（網羅性等）まで実施すべきかについてアドバイスいただきたい

回答：
物理セキュリティとして重要情報がある場所への情報盗難等につながる機器等の持込み・持ち出しをコントロールし、リスクを軽減することを目的としている項目になります。

自社サーバールーム等重要情報がある場所に対して、一般的には申請承認のプロセスを回して、許可を受けて持込み・持出しを行うということかと思います。 一方で、扱う情報の重要度・機密度によっては、申請というレベルだけではなく金属探知機等によるメディアの不正持込み・持出しの検査等が必要というケースもあるかもしれません。

いずれにしても、そこに保有す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。

質問③

質問内容：No9「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」の具体的な対象の法令が何かを知りたい。その際の法令は立地している国の法令に準拠する、で良いのか。

回答：
　内閣サイバーセキュリテイセンターが、サイバーセキュリティ対策において参照すべき関係法令をQ&A形式で解説する「サイバーセキュリテイ関係法令Ｑ＆Ａハンドブック」を作成公開しています。

サイバーセキュリティ基本法関連、会社法関連（内部統制システム等）、インシデント対応関連総論（当局等対応、関係者対応）、個人情報保護法関連、不正競争防止法関連、労働法関連（秘密保持・競業避止等）、情報通信ネットワーク関連（IoT関連等を含む）、契約関連（電子署名、システム開発、クラウド等）、資格等（情報処理安全確保支援士等）、その他各論（リバースエンジニアリング、暗号、情報共有、脅威インテリジェンス、データ消去等）、インシデント対応関連（事後的対応等）（ランサムウェア対応、デジタル・フォレンジック、サイバー保険等を含む）、民事訴訟手続、刑事法（サイバー犯罪等）、海外法令（GDPR等）

関係法令Q＆Aハンドブック – NISC（みんなで使おうサイバーセキュリティポータルサイト）

もちろん、立地している国の法令は必須かと思います。加えて、GDPR等海外の法令であっても立地によらず適用を受ける可能性のある法令がありますので、留意が必要です。

※「自工会・部工会サイバーセキュリティガイドライン解説書」にも記載がありますのでこちらも参照ください。

質問④

質問内容：社内体制を整備したいが、ITに詳しいメンバーが少なく、選任は難しい。
中小企業ではそういうケースも少なくないと思うが、どういった対応をしているのか知りたい。

回答：各社様の規模により、ITに詳しい方や専任の担当者の設定が困難な場合があることは理解しております。
そういった場合も兼任でも結構ですので情報セキュリティに関する役割と権限を持つ方をご指名頂き、

- 自動車産業サイバーセキュリティガイドラインおよび同解説書をみる
- 自己評価依頼説明会資料および同アーカイブ動画を見る
- 自工会・部工会が開催する各種ウェビナー、よろず相談会に参画頂き情報を得る

ことから始めて頂きたいと思います。ただし、ゼロからのスタートの場合、上記資料も理解が困難かもしれません。
そのような場合には、独立行政法人 情報処理推進機構（通称IPA）の「中小企業の情報セキュリティ」が役に立つものと思います。以下のホームページから参照ください。

- 中小企業の情報セキュリティHP　https://www.ipa.go.jp/security/sme/index.html

直ちに業界標準ガイドラインの要求事項を全件達成することは困難であっても、出来るところから少しずつでも実行頂くことにより、確実にセキュリティレベルは向上してまいります。
先ずは会社の経営課題として活動を開始してください。

質問⑤

質問内容：サイバーセキュリティポリシーおよび手順の作成において、必要な工数および技能の見積もりはどの様に行えば良いのか。

回答：サイバーセキュリティポリシーおよび手順については、IPA殿のWebサイトに掲載された「中小企業の情報セキュリティ対策ガイドライン」（以下リンク参照）等にその雛形となる情報が掲載されております。
これらを参考に、自社の状況に合致した形にアレンジすることにより、比較的容易に相応のポリシー／手順を作成することができますので、参考としてください。

但し、単純に会社名などを埋めていくのではなく、その記載内容を正しく理解・把握したうえで、実行可能なものを策定することは必要であり、これは各社様のセキュリティ対策の根幹となる部分でもありますので、経営トップも含めある程度の工数をかけて策定頂くことをお願い致します。

中小企業の情報セキュリティ対策ガイドライン | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

付録

- 付録2：情報セキュリティ基本方針（サンプル）（全1ページ）（Word:35 KB）
- 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）

質問⑥

質問内容：小規模企業では、求められる全ての達成条件を満たすことが難しい。簡易的に対応する方法は無いのか？

回答：自工会・部工会としては自動車産業のサプライチェーンに参加される全ての会社様に、その企業規模を問わずレベル２までの全項目を達成頂くことを希望しております。

但し、人員規模・予算上等の問題でそれが困難な会社様におかれましては、少なくとも23年度中にレベル1の全50項目の達成をお願いしたいと考えております。その上でレベル２の項目に関しても24年度末に向け、可能な項目から計画的に達成頂ければと存じます。

また、質問①④⑤で紹介させて頂いた様に、「IPAの規程類ひな型を利用する」「中小企業の情報セキュリティ」ホームページで紹介されている、例えば「お助け隊サービス」を活用する等も検討頂くと良いと考えます。

仮に24年度末までにレベル２を全件達成することは困難であっても、出来るところから少しずつでも実行頂くことにより、確実にセキュリティレベルは向上してまいりますので、よろしくお願い致します。

質問⑦

質問内容：規程内容の充実を図りたいが、専任者がいなくて整備が進みづらい。他社の意見を聞けると嬉しい。

回答：自工会・部工会あるいは公的機関が開催する各種ウェビナー等の場を通じ、他の会社様の活動内容や意見を共有する場を提供してまいりたいと考えています。

この「よろず相談会」を、そうした場にもしたい・・・という想いもございます。　折角ですので、主催者側からの回答だけでなく、ここに集まって頂いた方からの意見を出し合って頂けると嬉しく思います。
「専任者いなくて規程類の整備が進まない」というテーマについて、あるいは関連する事項について、意見を出して頂ける方は、いらっしゃいませんか？

質問⑧

質問内容：規定・ルールを導入後、社員ひとりひとりに遵守させるために、どのような教育、社内へのアナウンス、
周知を行えば良いのか

回答：IPA等の資料を活用しながら教育を実施頂ければと考えます。
教育実施のタイミングは社内環境変更時（新規受入時、昇格時、ルール変更時）に行うことが望ましいです。

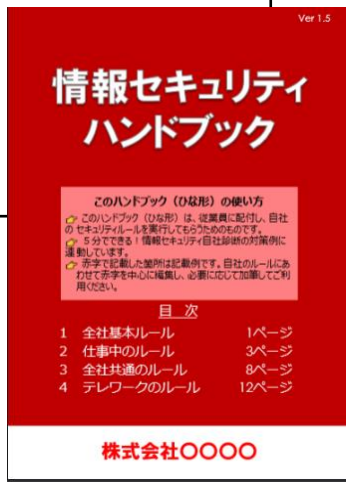
参考資料
■IPA：ここからセキュリティ ①特集　新入社員向け ・電子メール、インターネット接続について：新入社員等研修向け情報セキュリティマニュアル Rev3 ②中小企業向け ・情報管理について：【てびき】情報管理も企業力～秘密情報の保護と活用～（経産省） 教育・学習（企業・組織向け）｜ここからセキュリティ！ 情報セキュリティ・ポータルサイト (ipa.go.jp)

質問⑨

質問内容：情報セキュリティに関する意識を高めていく啓蒙活動のやり方に関して教えてほしい

回答：情報セキュリティに関する意識を高めていく啓蒙活動のやり方としてはIPA「中小企業の情報セキュリティ対策ガイドライン」P20（2）、22（3）、付録4を活用してご検討頂ければと考えます。

参考資料
■IPA：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　P20（2）、22（3） ■IPA：中小企業の情報セキュリティ対策ガイドライン 付録4：情報セキュリティハンドブック（ひな形） 中小企業の情報セキュリティ対策ガイドライン	情報セキュリティ	IPA 独立行政法人 情報処理推進機構



質問⑩

質問内容：リスクアセスメントを各部署で実施してもらう為に、何を参考に具体的な進め方やガイドラインを決めれば良いのか

回答：リスクアセスメントを進めるにあたり、IPA「中小企業の情報セキュリティ対策ガイドライン」P54～64、付録7を活用してご検討頂ければと考えます。

参考資料
■IPA：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　P54～64 ①手順１（P54～58）：リスク特定 ②手順２（P59～61）：リスク分析 ③手順３（P62～64）：リスク評価 ■IPA：中小企業の情報セキュリティ対策ガイドライン 付録7：リスク分析シート（全7シート） 中小企業の情報セキュリティ対策ガイドライン	情報セキュリティ	IPA 独立行政法人 情報処理推進機構

質問⑪

質問内容：No17「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。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」において、SOCサービスに加入する以外の手段はあるか？整備の為の要件を知りたい。

回答：
もちろん、自社でネットワークやセキュリティデバイスを監視し、サイバー攻撃の検出や分析を行う企業も多数存在します。専門人員を配置するだけではなく、一定程度のセキュリティ知見を持つネットワーク担当やシステム担当がその役割を担っているケースは多いかと思います。

自社で体制を整備する場合の肝となる部分は、昨今の高度化するサイバーリスク等に対応し、自社の求めるレベルの対応ができる人材を確保・育成し運用体制を維持していくことにあるかと思います。

自社で運営する場合、サイバー攻撃等の新たな手口を知り共有するために、JPCERT/CC や IPA 等の注意喚起や脆弱性関連情報を活用することができます。また、サイバー攻撃等の監視・分析を効果的に行うための基盤としてSIEM(System Information and Event Management）等を活用する方法もあります。

JPCERT/CC 緊急情報を確認する　https://www.jpcert.or.jp/menu_alertsandadvisories.html
IPA 重要なセキュリティ情報　https://www.ipa.go.jp/security/security-alert/index.html

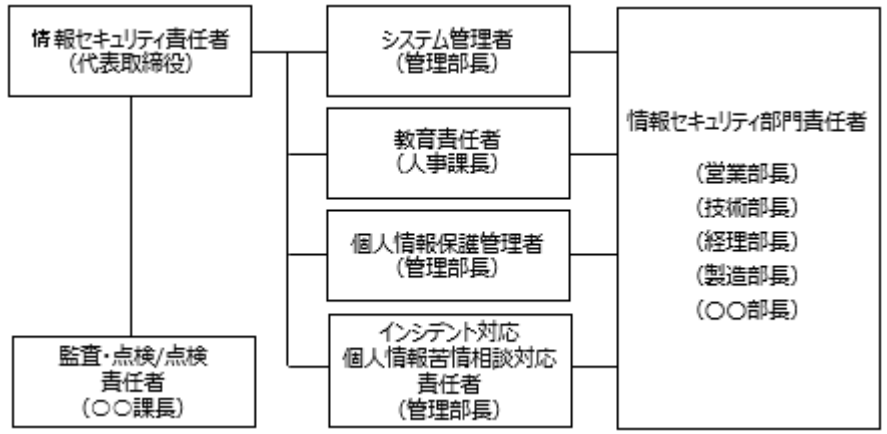
質問⑫

質問内容：セキュリティの体制を整備するにあたり、IT以外のどういった部署を巻き込んでいけば立ち上げがうまくいくかが知りたい。

回答：セキュリティの体制を整備にあたっては、IT部門に特化せず、全社横断的な体制を組むことが肝要かと存じます。
一例として、IPAの関連規程サンプルから引用します。

- 会社全体のセキュリティを統括し責任を持つ立場として情報セキュリティ責任者：CISO（ Chief Information Security Officer ）を設定する。
- CISOのもと関連部門からなる情報セキュリティ委員会を設置する。
- 情報セキュリティ委員会の配下に情報セキュリティ部門責任者（営業・技術・経理・製造などの部門長）を置く。
- 上記組織とは独立した監査機能を置く。

【参考】IPA中小企業の情報セキュリティ対策ガイドライン
記載の情報セキュリティ委員会体制図サンプル



なお、この体制は各社様の規模・機能配置等に合わせ、適切に設定頂ければと存じます。

【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　付録5：情報セキュリティ関連規程（サンプル）１ 組織的対策
000055794.docx (live.com)

質問⑬

質問内容：No.30「機密区分に応じた情報の取り扱いに関する教育を行っている」に関して機密区分とはどのような定義が一般的なのか

回答：機密区分の定義についてはIPA「中小企業の情報セキュリティ対策ガイドライン」P55（機密性）を参考にし、自社内で定義して頂ければと考えます。

自動車産業サイバーセキュリティガイドライン			参考資料
No.	内容	解説書	
30	機密区分に応じた情報の取り扱いに関する教育を行っている	－	■IPA：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　P55　（機密性） 中小企業の情報セキュリティ対策ガイドライン	情報セキュリティ	IPA 独立行政法人 情報処理推進機構

評価値		評価基準	該当する情報の例
機密性 アクセスを許可された者だけが情報にアクセスできる	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データ[24]として指定されている 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	●自社の独自技術・ノウハウ ●取引先リスト ●特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	●自社製品カタログ ●ホームページ掲載情報

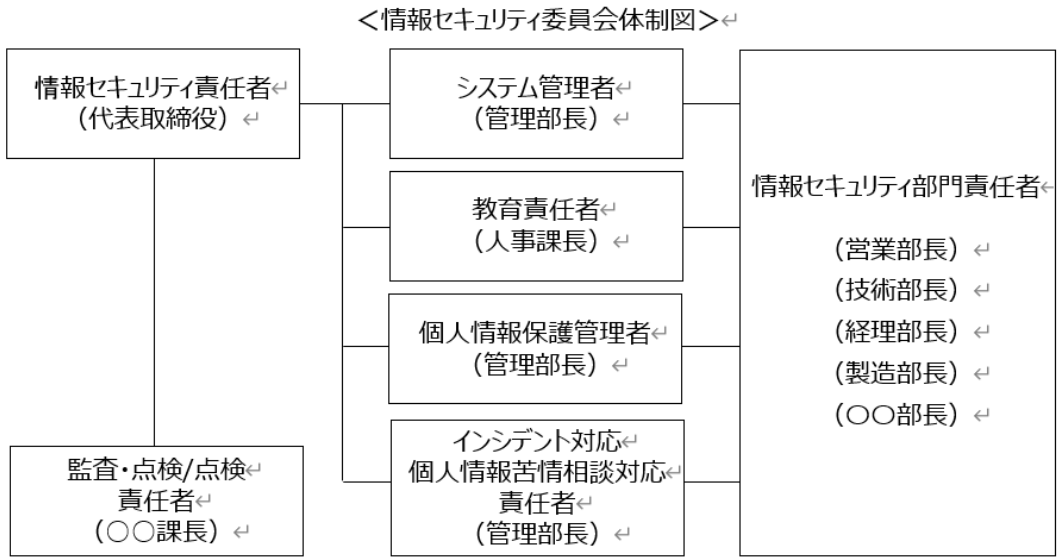
－IPA「中小企業の情報ｾｷｭﾘﾃｨ対策ｶﾞｲﾄﾞﾗｲﾝ」P55（機密性）－

評価値３、２、１のランクに応じて
極秘、秘 等、各社にて表記をご検討して
頂くのが一般的となります。

質問⑭

質問内容：No.13「情報セキュリティ責任者を含む、平時の体制と責任と役割を明確化している」において、情報セキュリティの体制とは、どのような役割や責任があり、どのような活動を行うべきか。

回答：
セキュリティの体制は企業における**情報セキュリティを推進・実現するための管理体制**になります。
具体的には、「情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する」役割・責任を持ちます（IPA 中小企業の情報セキュリティ対策ガイドライン　関連規程サンプルより）



出典: IPA 情報セキュリティ関連規程サンプル　https://www.ipa.go.jp/security/guide/sme/about.html

活動の例
- 情報セキュリティ指針・計画(対策・教育)
- 情報セキュリティ定例(情報共有)
- 情報セキュリティ監査・評価
- 情報セキュリティ改善方針策定

IPA 中小企業の情報セキュリティ対策ガイドライン
本編：第二部４　（１）管理体制の構築

質問⑮

質問内容：No76「自組織の資産が接続している外部情報システムの利用ルールを定めている」外部サービスを利用する際のセキュリティ基準の具体例はありませんか。 IPA等の資料等も参考にさせていただいていますが、どのような基準にすればよいか決めかねている。

回答：他の質問の回答にも引用しています「IPA 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」のP28には「委託時の対策」として、契約書や覚書を交わす事、先方のセキュリティ対応方針を確認する事等の記述があります。
＜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 (ipa.go.jp)

もう少し具体的な参考事例として、会員企業様にて設定していますセキュリティ基準の概要を以下に提示します。

＜点検項目＞ ※以下の項目の実施状況を利用部門が申請し、情報セキュリティ部門／IT部門が確認

①外部からの不正侵入・攻撃の防止
・ネットワークへのアクセス管理 ・ 不正通信の検知 ・重要データの隔離と暗号化 ・ウイルス対策 ・脆弱性点検 など
②内部からの情報の不正利用の防止
・サービス利用ID／特権IDの管理 ・利用環境による制限 など
③サービス申込部署・共同使用部署の運用に関する要求事項
・利用する情報の明確化 ・利用者の承認と記録 など
④サービス提供事業者の運用に関する要求事項
・サービス提供事業者の不正利用禁止 ・ログ・バックアップの取得など
⑤契約・資格・ファシリティ
・公的資格、第三者機関による評価 ・第三者への業務委託先管理 ・知的財産権の保護 など

質問⑯

質問内容：No18「情報セキュリティ事件・事故発生時の対応　体制と責任と役割を明確化している」
何が事件で何が事故等かの具体的な事例が知りたい

回答：セキュリティインシデント（事件・事故）の定義はIPA「中小企業のためのセキュリティインシデント対応の手引き」P2、
また具体的な事例はIPA「情報セキュリティ10大脅威2023」に掲載されておりますので、ご参考にして頂ければと考えます。

自動車産業サイバーセキュリティガイドライン			参考資料
No.	内容	解説書	
18	情報セキュリティ事件・事故発生時の 対応体制と責任と役割を明確化している	－	■IPA：中小企業の情報セキュリティ対策ガイドライン 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の手引き P2 セキュリティインシデントの必要性 中小企業の情報セキュリティ対策ガイドライン	情報セキュリティ	IPA 独立行政法人 情報処理推進機構 ■IPA：情報セキュリティ10大脅威2023　組織編85ページ 情報セキュリティ10大脅威 2023	情報セキュリティ	IPA 独立行政法人 情報処理推進機構

セキュリティインシデント対応の必要性

セキュリティインシデントとは、セキュリティの事故・出来事のことです。単に「インシデント」とも呼ばれます。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象等がインシデントに該当します。
インシデント対応は、これらの被害を想定し、あらかじめ準備することで被害や影響範囲を最小限に抑えます。また、自社だけではなく、顧客、取引先、株主、従業員等の関係者へ被害が拡大しないようにします。

－IPA「中小企業の情報ｾｷｭﾘﾃｨ対策ｶﾞｲﾄﾞﾗｲﾝ」付録8：中小企業のためのｾｷｭﾘﾃｨｲﾝｼﾃﾞﾝﾄ対応の手引き（P2抜粋）－

（補足）
事故：偶然などが原因でだれも悪い出来事を起こそうとせずに起きた悪い出来事
事件：故意に起こした悪い出来事

質問⑰

質問内容：社内人員の都合で、情報セキュリティ委員会、CSIRT、SOCの全てに所属することは問題無いでしょうか。

回答：
中小企業様など、現実的にセキュリティ専任の人員はおらず数名のIT人員がセキュリティも兼務している企業様も多いかと思います。情報セキュリティ員会、CSIRT、SOCでそれぞれ求められる役割が異なる中で、その機能を果たせる形で兼任することに何ら問題はないと思いますし、大きな企業であっても兼務しているケースは多いかと思います。

脅威が高度化する一方セキュリティ人材が不足する中、セキュリティ人員の維持・育成は苦労が多いかと思います。技術的な側面が強く専門性も高いSOCなどの機能については、IPAの認定する中小企業に向けたサービス等もありますので、外部のSOCサービス等の利用を検討することも一つの方法かと思います。

IPA サイバーセキュリティお助け隊サービス：
「見守り」「駆付け」「保険」など中小企業のセキュリティ対策に不可欠なサービスをワンパッケージで安価に提供する民間サービス（審査を経てIPAが要件を満たすことを確認したサービス）
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

質問⑱

質問内容：CSIRTの具体的な要件についてご教示いただきたい

回答：CSIRTの要件はIPA「プラクティスナビ」、「中小企業のためのセキュリティインシデント対応の手引き」を参考にして下さい。

参考資料
【平時】 ■IPA：脆弱性情報　（JVN） 脆弱性対策情報 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 【有時】 ■IPA：プラクティス・ナビ　指示7 プラクティス・ナビ IPA 情報処理推進機構 ■中小企業の情報セキュリティ対策ガイドライン　　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の手引き 中小企業の情報セキュリティ対策ガイドライン | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

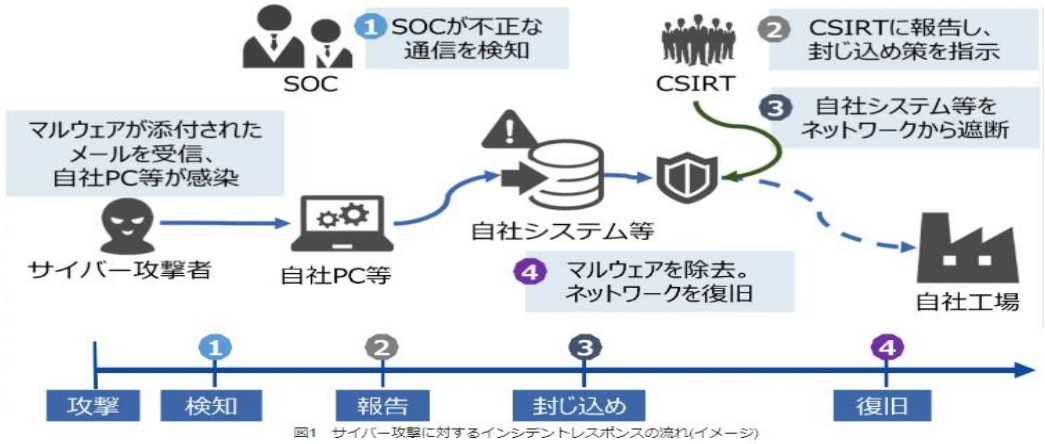


図1　サイバー攻撃に対するインシデントレスポンスの流れ(イメージ)

表1　インシデント対応の流れとCSIRTの主な活動の例

インシデント対応の流れ	CSIRTの主な活動例
①検知	• Webサイトの改ざんやシステムの停止、また標的型メール等に関する外部組織や社内、顧客からの通報を受領 • ログ監視等からC&Cサーバ等との不正な通信を発見
②報告	• 発生事象に応じた組織内外との連携（システム運用の委託先や専門ベンダを含む）
③封じ込め	• インシデントの影響分析・対応優先度の判断 • 被害極小化のための暫定対応の実施（システム停止・ネットワーク遮断など）
④復旧	• 恒久対応を実施し、サービスやシステムを復旧

ーIPA　プラクティスナビ　指示7　インシデント発生時の緊急対応体制の整備　抜粋ー