よろず相談会 第８回

2025年2月7日 15：00～17：00

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
DX対応委員会　サイバーセキュリティ部会

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、個社の情報等を省き、一般化しております。
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させて頂く場合もございます。
	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。
	本資料は後日、メール、及び自工会HPにて展開いたします。ただし、本日の相談会の中で 個別にやり取りさせて頂いた内容は反映いたしませんので、ご注意ください。

本日取り上げさせて頂くご質問一覧

No.	質問
1	[No.1]どのようなセキュリティ体制を構築すれば達成になるのか、教えて欲しい。
2	[全般]セキュリティ対策の人員、費用を確保するのが困難であるが、どのように進めたら良いでしょうか。
3	機密書類の判定（極秘・秘・関係者外秘）について該当する情報を具体的に知りたい。
4	[No39]組織を跨いだ情報セキュリティ事件・事故の教育・訓練について、具体的な訓練の方法や事例（手順）を知りたい。
5	生体認証の利用に関して見解をお聞きしたいです。積極的に利用した方が良いのであれば、PCの入替やセキュリティゲートの検討の際に考慮したいと思っております。
6	情報セキュリティに関する法令対応についてどのようにすれば良いか知りたい。

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。
時間が余った場合は、その他の質問に対しても取り上げますので、ご発言頂ければ幸いです。
活発な議論の場としたく、ご理解の程よろしくお願い致します。

IPAセキュリティプレゼンター
自己紹介

田中 孝典　（たなか たかのり）

ITコーディネータ、情報処理安全確保支援士
特定非営利活動法人 ITCちば経営応援隊　理事
株式会社クロスウィズユー　代表取締役

第000537号
（情報処理安全確保支援士）

サイバーセキュリティ関連業務経験：20年以上

- 情報セキュリティマネジメントシステム（ISMS）構築支援事業の立ち上げ
- ファイル暗号、持ち出し制御パッケージの開発
- ネットワークセキュリティ機器のマーケティング
- 中小企業でISMS、プライバシーマークの運用
- 中小企業の情報セキュリティマネジメント指導
- 中小企業への技術情報管理認証制度導入支援

中小企業のDX推進・デジタル化支援

- 東京都 デジタル技術導入促進ナビゲーター事業
- 東京都 テレワークハンズオン支援コンサルティング事業

ほか

質疑応答

質問①

[No.1]どのようなセキュリティ体制を構築すれば達成になるのか、教えて欲しい。

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。

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)

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す。以下の手順で進めることを推奨します。
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）
③管轄部署にて自社の事情／環境を考慮し、自社の状況に合わせて修正する
（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）

質問①

[No.1]どのようなセキュリティ体制を構築すれば達成になるのか、教えて欲しい。

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です。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。

特にポイントとしては各部門に関連した役割を明確にすることで合意が得られやすくなるかと思います。
例：システム管理者⇒IT部門、教育責任者⇒総務部門
　　部門責任者⇒部門が保有している機密情報（顧客情報、図面・・・など）の管理

【表６】情報セキュリティ管理のための役割と責任分担（例）

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行います。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	情報セキュリティ対策が適切に実施されているか点検します。

参考
IPA 中小企業の情報セキュリティ対策ガイドライン
本編：第二部４　（１）管理体制の構築（P24）より

質問②

[全般]セキュリティ対策の人員、費用を確保するのが困難であるが、どのように進めたら良いでしょうか。

自社内に、セキュリティ対策の推進が出来る人員を確保するには、以下２つの方法があります。
・自社人員に対し、セキュリティ教育を行い育てる
・中途採用を活用し、即戦力の人員を確保する
但し、いずれの方法についてもそれなりの**費用、或いは費用に加えて時間がかかります**。

上記、人員確保を自社内のみで行うには限度があるため、３つ目の方法として「外部ベンダーを活用し、人員を確保する」手段があります。特に、IPAが提供している**「サイバーセキュリティお助け隊サービス」**は、「見守り」「駆付け」「保険」など**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サービス**です。（審査を経てIPAが要件を満たす事を確認したサービス）費用の確保が困難な状況であるならば、**比較的、低コストで利用出来る対策として有効**です。

IPA サイバーセキュリティお助け隊サービス：
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

費用の確保については、**経営陣に「セキュリティ対策の重要性」を理解して頂き、**企業戦略として事業活動に必要な投資として引き出すしか手はありません。一方で、「自動車産業サイバーセキュリティガイドライン」には、**費用を掛けずとも推進出来る対策も記載**しておりますので、**まずはその様な対策から進めて頂く事も非常に有効です。**

質問③

機密書類の判定（極秘・秘・関係者外秘）について該当する情報を具体的に知りたい。

機密書類の判定においては、機密区分の定義をきちんと行った上で、それに基づいて分類することが重要となります。以下はあくまで具体例となりますので、ご了承下さい。

もう少し細かい粒度で機密書類の判定を行う事例は下記を参照ください。
中小企業の情報セキュリティ対策ガイドライン第3.1版
P54～56

機密区分例	定義例（外部に漏洩した場合、会社の信頼や収益に）	具体例
極秘	極めて秘匿性の高い情報（著しい影響を及ぼす可能性がある）	企業の財務情報、新製品の設計図、研究データ、合弁情報など
秘	厳格に選定された関係者のみに共有すべき秘匿性の高い情報（影響を及ぼす可能性が高い）	規程、重要契約書、人事ファイルなど
関係者外秘	関係者間で業務に利活用する情報（影響を及ぼす可能性がある）	会議議事録、企画書、見積書など

質問④

[No39]組織を跨いだ情報セキュリティ事件・事故の教育・訓練について、具体的な訓練の方法や事例（手順）を知りたい。

回答：
自社でサイバーインシデントが発生した時に、どの様な行動が必要となるかを想定し、その内容を確認できるシナリオを作成するようにしてください。確認するポイントの例としては、以下の通りとなります。

- インシデント発生後、各部門からとりまとめ部門へ情報が適切に報告されるか。
- 上層部や他部門を巻き込んだ情報共有が出来るか。
- インシデント発生原因を切り分けられるか。
- 各部門はインシデント対応、復旧対応が出来るか（各部署が用意しているマニュアル通り動けるか）。
- 上層部で適切な対処判断ができるか。
- 社外（官公庁、メディア、警察、顧客等）への公表判断や報告を適切に出来るか。

参考資料：日本シーサート協議会　サイバー攻撃演習訓練実施マニュアル｜ワーキンググループについて｜公開資料一覧｜CSIRT - 日本シーサート協議会
JPCERT/CC　CSIRTマテリアル付録 - インシデント対応演習プログラム

参考ツール：IPA

ツール名	テーマ	リンク先
ABCSIRT	社内で発生したインシデントに限られた工数で立ち向かうCSIRTの１週間	ABCSIRT 30分で学ぶはじめてのインシデント対応 | デジタル人材の育成 | IPA 独立行政法人 情報処理推進機構
マルウェアスイーパー	国内拠点に次々と広がるマルウェアCSIRTが協力して、感染を封じ込めるか	マルウェアスイーパー ～協力と決断力でパンデミックを阻止せよ～ | デジタル人材の育成 | IPA 独立行政法人 情報処理推進機構
GAME　OF　CSIRT	自社を標的にしたサイバー攻撃から自社を守り、株価下落を防ごう	GAME OF CSIRT ～防ぐ、でもやられる、ならば対処する～ | デジタル人材の育成 | IPA 独立行政法人 情報処理推進機構

質問⑤

生体認証の利用に関して見解をお聞きしたいです。積極的に利用した方が良いのであれば、PCの入替やセキュリティゲートの検討の際に考慮したいと思っております。

■生体認証のメリット

セキュリティ向上：生体認証は、指紋、顔認証、虹彩認証などの身体的特徴を利用するため、他人によるなりすましや盗用が非常に困難になります。また、二要素認証や多要素認証と組み合わせることで、セキュリティが大幅に向上します。

利便性向上：認証デバイスに指をタッチする、カメラに顔を向けるなど、キーボードから文字列を入力するよりも手間が掛からないことが特徴です。

アカウント管理の省力化：生体認証であれば、ID・P/Wのようにユーザーが情報を覚える必要がありません。自分の身体さえあれば認証を行なうことができるため、ユーザーの負担削減とセキュアな認証を両立することができます。

■生体認証のデメリット

プライバシーの問題：生体認証に使用する身体情報は、個人情報に該当し、登録する事に抵抗を感じる人も少なくありません。生体認証によりセキュリティが強化される事は事実ですが、個人情報を管理すると言う事を理解しておく必要があります。

認証精度が完全ではない：指紋認証であれば指の汚れや乾燥、顔認証であれば認証時の光量や顔の角度など、認証時の状況は認証精度に影響を及ぼします。

コスト：生体認証システムの導入には、指紋認証スキャナーや顔認識カメラなどの認証機器、実際に認証を行なうシステムの導入が必要となるケースが一般的です。自組織にとって単純なコスト増にならないように注意することが大切です。

生体認証は、**上記メリット・デメリットを理解し**適切な利用を目指す事で、企業にとって**安全で効率の良い認証システムとして活用する事が可能です。**

質問⑥

情報セキュリティに関する法令対応についてどのようにすれば良いか知りたい。

法令を基に社内ルールを策定することが必要となります。また、策定した社内ルールに対して、教育・周知を合わせて行うことが必要です。（チェックシートNo.9の対応）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

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

情報セキュリティに関する法令の具体的な対象については、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ので、こちらを参照ください。

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）

参考情報

独立行政法人情報処理推進機構（IPA）
サイバーセキュリティに関する業務概要

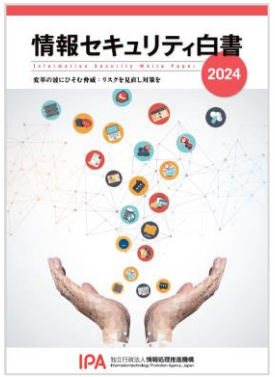
■ 平時からインシデント発生時まで、サイバーセキュリティのマネジメントからオペレーションまでトータルな施策・対応を実施。

普及啓発・リテラシー向上支援

- 情報セキュリティ10大脅威、情報セキュリティ白書
- 経営者、社内担当者向け各種ガイドライン・教育コンテンツ
- 地域・中小企業支援
- 情報セキュリティ安心相談窓口
  10,923件（2023年）

SECURITY ACTION
セキュリティ対策自己宣言
累計宣言数約30万者（2023年10月）

サイバーセキュリティお助け隊



サイバー事案対応（検知・分析・対処調整）

- サイバー情勢分析
- 国家支援型サイバー事案対策
- 情報共有（サイバー攻撃情報・脆弱性）
- セキュリティ監視（独法等）
- サイバー事故原因究明

IPA J-CRAT
2011年創立　341件支援（2023年）

J-CSIP Initiative for Cyber Security Information sharing Partnership of Japan

JVN iPedia
脆弱性データベース
約20万件登録（2024年3月）

セキュリティ基準・評価認証

＜製品・サービスのセキュリティ評価・認証＞

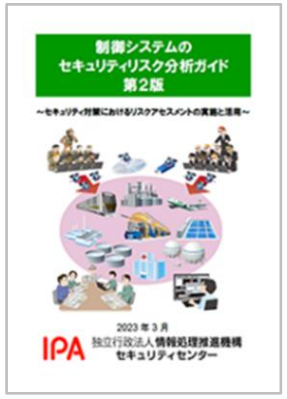
CRYPTREC Cryptography Research and Evaluation Committees

- 暗号技術調査/IT製品ISOセキュリティ認証
- IoT製品セキュリティラベリング（JC-STAR）
- クラウドサービスセキュリティ評価（ISMAP）

＜セキュリティ基準・分析・監査等＞

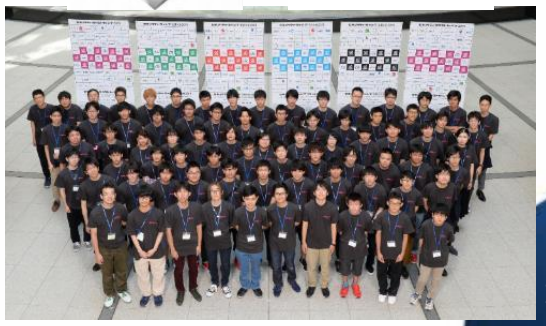
- 制御システムセキュリティリスク分析
- サプライチェーンセキュリティ評価
- 独法等情報セキュリティ監査、政府システム監査

JC-STAR



人材育成

- 国家資格「情報処理安全確保支援士」
  登録者数21,727名（2023年10月1日時点）
- 中核人材育成プログラム
  累計435名受講（2017年～）
- 若手人材発掘（セキュリティ・キャンプ）
  累計1,073名受講（2004年度～）
- 情報セキュリティコンクール
  応募約５万点（2023年度）



サイバーセキュリティお助け隊サービスの活用を！

IPA

手遅れになるまえに、手を打つ。

「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

見守り
（異常の監視）
24 時間 365 日監視
挙動や問題のある攻撃を検知し
あなたの PC と
ネットワークを守ります。

駆付け
問題が発生したときに、
地域の IT 事業者等が
駆付け対応します。
（リモート支援の場合あり）

保　険
簡易サイバー保険で、
駆付け支援等インシデント対応時に
突発的に発生する各種コストが
補償されます。

ワンパッケージで安価に!

サイバーセキュリティお助け隊サービス制度

https://www.ipa.go.jp/security/sme/otasuketai-about.html

- 中小企業に対するサイバー攻撃への対処として不可欠なサービス要件を、ワンパッケージとしてサービス基準にまとめ、これを満たすことが所定の審査機関により確認された民間サービスをIPAが「**サイバーセキュリティお助け隊サービス**」として登録・公表する制度。

◇「サイバーセキュリティお助け隊サービス基準」の主な内容

主な要件	概要
相談窓口	ユーザーからの**相談を受け付ける窓口**を設置／案内
異常の監視の仕組み	ネットワーク又は端末を**24時間見守る仕組み**を提供
緊急時の対応支援	インシデント発生などの**緊急時には駆け付け支援**
中小企業でも導入・維持できる価格	・ネットワーク一括監視型：**月額１万円以下（税抜き）** ・端末監視型：**月額2,000円以下／台（税抜き）**
簡易サイバー保険	インシデント対応時に突発的に発生する駆付け費用等を補償する**サイバー保険を付帯**

相談窓口、緊急時の対応支援、簡易サイバー保険などを**ワンパッケージで提供**

本サービスを採用することを通じて、取引先企業に対する**自社の信頼性をアピール**

・ワンパッケージのサービスとして登録

・マーク提供
・ブランド管理・普及促進

➢ 各地域の「サイバーセキュリティお助け隊サービス」として**40事業者**が**57サービス**を登録。（2024年4月時点）

サイバーセキュリティ お助け隊

マーク付きの民間サービス

中小企業

E N D