よろず相談会 第７回

2025年2月7日 10：00～12：00

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	・初期教育をどのレベルで社内に展開すべきか　・情報セキュリティ体制の構築
2	弊社では経営層の理解はある程度得られているものの、予算や人員の確保に至っておりません。本業で手いっぱいな他部門を巻き込んで、積極的にセキュリティへの取り組みを実施するのは難しい状況ですが、良い進め方等あれば教えてください。
3	・ガイドライン[No.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 」について教えてほしい。　親会社とシステム統合することになりましたが、セキュリティポリシーがグループで統一されておりません。自社で定めたセキュリティポリシーがありますが、親会社で確認している状態であれば、「２.対応完了」としてよいのでしょうか？ ・ガイドライン[No.153]「事業継続上重要なシステムについては、重要度に応じて決められた各システムの復旧ポイント、復旧時間を満足するデータと手順が整備されている」について教えてほしい。社内にBCPとりまとめ部署が無いため、RTO・RPOの設定もございませんが、各事業部門の判断でベストエフォートでの復旧計画を立案している場合は「対応完了」としてよいでしょうか？
4	チェックシート及びお得意先様から本件に関して問い合わせがありますが、 秘密保持契約等なければ逆に内外に弱点等漏洩してしまう可能性があり、そこを懸念しております。
5	ガイドライン[No.21]　情報セキュリティ事件・事故を含めた自社の事業継続計画又は緊急時対応計画の作成について、参考及び雛形になるものはありますでしょうか。
6	・ガイドライン【No.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」について教えてほしい。サーバーの設置エリアに施錠が出来ません。専用ラックは必要でしょうか？ ・ガイドライン【No.99】「PCからのデータ書き出しを仕組みで制限している」について教えてほしい。USBの利用制限をかけた場合、従業員の業務効率の低下が懸念されますが、制限をかけるべきでしょうか？

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。

回答者紹介

①自工会/部工会メンバーご挨拶
②IPAセキュリティプレゼンター/進 京一様 ご紹介

IPAセキュリティプレゼンター

自己紹介

進　京一　SHIN Kyoichi, P. E. Jp

現職

- 進京一技術士事務所 代表
  - 技術士（電気電子部門、総合技術監理部門）
    専門：情報通信（光通信ネットワークシステム）
- 特定非営利活動法人　ＩＴＣちば経営応援隊 理事
- 法務省／防衛省デジタル統括アドバイザー

経歴

- 情報通信システムの開発・事業運営（30年間）
- 国内の情報通信ネットワークに関する標準化（7年間）

資格

- 情報処理安全確保支援士(RISS：000060号)
- 情報処理技術者試験(ST、SA、PM、SM、AU)
- 電気通信主任技術者、第三種電気主任技術者
- 公認システム監査人、ITコーディネータ、医療情報技師
- CISSP/CCSP、CISA、CIA、公認システム監査人

企業支援

- 独立行政法人情報処理推進機構(IPA)
  - 情報セキュリティプレゼンター
  - サイバーセキュリティお助け隊
- 経済産業省
  - 重要情報管理認証制度 支援/監査
  - 関東経済産業局 地域SECUNITY
- 全国中小企業団体中央会
  - 個別専門指導事業、情報セキュリティ研修
- 東京都中小企業振興公社 支援専門家

質疑応答

質問①

・初期教育をどのレベルで社内に展開すべきか
➡ (現役世代は、情報リテラシーの感覚が大きく違うため、社内展開が新入社員から幹部にまで必要になるので、レベル感の設定が難しい)
・情報セキュリティ体制の構築
➡ (MSを構築すれば簡単かもしれないが、まずは一般的な会社としてどの管理レベルを押さえるべきか)

✓**情報リテラシーの評価**:
➡各従業員の情報リテラシーのスキルレベルを評価するための基準を設けることが重要です。これにより、どのレベルの教育が必要かを判断できます。

✓**段階的なアプローチ**:
- **新入社員向け**: 基本的な情報リテラシーやデジタルツールの使い方、セキュリティ意識など、基礎的なトレーニングを提供する。
- **中堅社員向け**: より高度な分析スキルやプロジェクト管理ツールの使用方法を学ぶ機会を提供する。
- **幹部向け**: 戦略的意思決定やデータ活用に関する専門的な教育を行う。

✓**フィードバックの収集**: 教育プログラムの効果を評価し、必要に応じて内容や方法を改善するためのフィードバックを定期的に収集。

✓**継続的な支援**:
➡初期教育後も、オンラインリソースやワークショップを通じて、情報リテラシーを向上させるための継続的な学習環境を整える。

情報リテラシーの評価

自社の情報リテラシー(レベル)の評価(見極め)を行う事をお勧めします。可能な限り詳細であればあるほど良いと考えております。

1. **基本情報**
   年齢: 年代による情報リテラシーの差を分析するため。
   性別: 性別による傾向を把握するため。
   職業・業種: どの業種に属しているか、職務内容による差異を理解するため。

2. **教育背景**
   最終学歴: 学位や専攻分野の情報。
   情報リテラシーに関する教育歴: 受講した研修やコース、資格など。

3. **スキル評価**
   デジタルスキル: 基本的なコンピュータ操作、ソフトウェアの使用能力。
   情報検索能力: インターネットやデータベースを使った情報収集の能力。
   データ分析能力: データを扱うスキルや分析ツールの使用経験。
   セキュリティ意識: サイバーセキュリティやプライバシーに対する理解。

4. **利用状況**
   インターネットの利用頻度: 日常的にどの程度インターネットを利用しているか。
   使用するデバイス: PC、スマートフォン、タブレットなどの利用状況。
   情報源の多様性: どのような情報源（ウェブサイト、SNS、書籍など）を使用しているか。

5. **行動特性**
   問題解決能力: 情報を使って問題を解決する能力。
   批判的思考: 情報の信頼性を評価する能力。
   コラボレーション能力: チームでの情報共有や共同作業の経験。

6. **自己評価**
   自己評価スコア: 自身の情報リテラシーに対する自己評価。
   自己改善の意欲: スキル向上に対する意欲や取り組み。

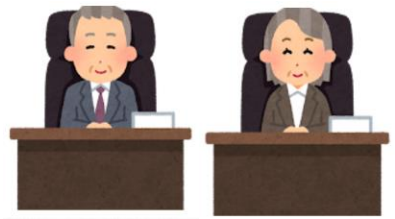
7. **組織内での役割**
   役職: 組織内での地位や役割。
   情報リテラシーに関する責任: 情報リテラシーに関する指導や教育を行っているかどうか。

これらの属性をデータ化することで、情報リテラシーの評価を行う際に、定量的かつ定性的な分析が可能になります。また、特定の属性間の相関関係を分析することで、情報リテラシーの向上に向けた具体的な施策を策定するための基礎データを得ることができます。

➡ まずは自社で分類できそうな属性から誰に、いつ、どのようなタイミングに教育を行う必要があるのかを可視化してみてください
「初期教育」が必ずしもタイミングを表す表現では無く、誰に何を伝えるかが重要であることに気づけます。

段階的アプローチ

自社なりに（一般論でも可）ターゲット（誰に何をどのように伝えたいのか）を定め教育を行いましょう。
以下は一般的なアプローチの考え方と方法になります。

	新入社員・若手社員	中堅社員	幹部・経営
ターゲット			
属性・人物像	デジタルネイティブ、リテラシーが高い。情報を自由に扱えるがビジネスでの実践経験が乏しく「情報漏洩」のリスクをはらんでいる。 デジタル媒体も問題なく使いこなし、インセンティブがあれば積極的な教育への参加もする	とにかく忙しい。積んできた経験で情報リテラシーが武器になる人もいれば、足枷になる人も。経営とも部下と会話する機会があり、上にも下にも毎日ギャップを感じている。	今更教育なんて・・・「サイバー」や「情報漏洩」が生産やステークホルダーに与える影響を頭では分かりつつも経験が無いので無関心。 デジタルは抵抗があるので、紙媒体や動画など視覚的な教育ならありがたい。
実施事項	教育：会社で得た情報とSNSとの付き合い方 方法：eラーニング	教育：デジタルの活用方法について 方法：長期社外教育プログラムなど	教育：情報漏洩のリスクについて 方法：集合研修、ワークショップなど

➡ 実行したら必ず定量的、定性的にフィードバック情報を収集し、仮説の検証、継続的な教育のためのPDCAを回してください。

ISMSの構築

機密区分を設け自社にとっての極秘に相当する区分の情報を抽出しましょう。そのステップとして、機密区分の定義（表1、＃54）、情報資産の一覧化（表2、＃56）を実施することでISMS構築の第一歩としてましょう。

１）機密区分を定義する ⇒ ２）高い機密区分の情報を抽出する ⇒ ３）情報資産 管理台帳に記入する

表１．達成条件No.54 機密区分の例

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）	取扱い方法例	台帳記載
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）	コピー、移動等 禁止	要
秘 （マル秘）	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）	コピー、移動は一定条件でのみ可。 保存時には暗号化	
関係者外秘 （社外秘）	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）	持ち出し時手続き要。保存時のアクセス制御、会社指定保管先のみ可	不要
（公開）	機密に当たらない情報（影響を及ぼさない）	ー	

IPA殿Webサイト上の 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　P54～58 リスク分析の【手順１】

ISMSの構築

１）機密区分を定義する ⇒ ２）高い機密区分の情報を抽出する ⇒ **３）情報資産 管理台帳に記入する**

表２．達成条件No.56 情報資産(情報)一覧化の例

No.	対象情報	個人情報有無	管理者	部署	保管場所	保管期限	開示先（メールアドレス）	棚卸日	備考
1									
2									
3									
4									

極秘情報の例：人事情報、給与情報、企業競争力に直結する情報、etc.
個人情報は含まれているか、極秘情報の管理者、保管場所、保管期限、管理者連絡先、定期的な棚卸を実施してください。

付録7：リスク分析シート（全7シート）(Excel:98 KB)　情報資産管理台帳Sheetが参考になります。
「リスク分析シート」は、自社の情報資産に想定されるリスクを特定し、対策を検討するために利用します。

質問②

弊社では経営層の理解はある程度得られているものの、予算や人員の確保に至っておりません。本業で手いっぱいな他部門を巻き込んで、積極的にセキュリティへの取り組みを実施するのは難しい状況ですが、良い進め方等あれば教えてください。

回答：予算・人員の確保や他部門を巻き込んでの推進活動は、多くの中小企業が直面している共通の課題です。
一方で、サイバー攻撃の脅威は日々高まっているのも事実で、優先度をつけて取り組みを始める必要があります。

そのような背景を受け、JAMA・JAPIAでは2024年11月に、８つの優先項目を取り上げたセキュリティ推進担当者向け解説資料を公開させていただいております。これらの項目のうち、社内で進めやすいものから着手いただければと考えます。

なお、既に社内に存在している情報やプロセスを活用するのが有効な場合もあります。特にサイバー対応は災害復旧対応と類似している部分もあります。例えば、「緊急時の連絡体制」については、地震やパンデミックなどを想定して人事部門が管理している連絡網や、安否確認システムは無いでしょうか。
一から準備するのではなく、それらの活用を検討することで、サイバー有事の備えを進めることも検討ください。

＜８つの優先項目（解説資料より抜粋）＞

分類	優先項目	目的
セキュリティ事故発生時の構え	緊急時の対応手順や連絡体制の再確認	セキュリティ事故発生時に早期に対応して、被害を最小化する
	ネットワーク外でのバックアップ、データ保管	被害を受けた際でも重要データは消失させない
	サーバーダウン時の生産継続方法の検討	システムが利用出来なくても生産／納入を継続させる
侵入・拡散させない対策	脅威や攻撃手口の情報収集	脅威や攻撃手口の最新情報を知り、対策を検討する
	OS、ソフトウェアの最新版へのアップデート	脆弱性を悪用した不正侵入を防止する
	ウィルス対策ソフトの導入	ウィルス感染によるデータ暗号化、不正侵入を防止する
	パスワードの強化	パスワード推測、解析、窃取による不正アクセスを防止する
	共有設定の見直し	誤設定による情報漏えいを防止する

質問③

・ガイドライン[No.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」について教えてほしい。 親会社とシステム統合することになりましたが、セキュリティポリシーがグループで統一されておりません。自社で定めたセキュリティポリシーがありますが、親会社で確認している状態であれば、「２.対応完了」としてよいのでしょうか？

・ガイドライン[No.153]「事業継続上重要なシステムについては、重要度に応じて決められた各システムの復旧ポイント、復旧時間を満足するデータと手順が整備されている」について教えてほしい。社内にBCPとりまとめ部署が無いため、RTO・RPOの設定もございませんが、各事業部門の判断でベストエフォートでの復旧計画を立案している場合は「２.対応完了」としてよいのでしょうか？

回答[No.1] ： 自工会/部工会・サイバーセキュリティガイドラインV2.2解説書のP9に記載の通り、ガイドラインへの回答は個社毎にご回答いただくことになります。自社で定めたセキュリティポリシーがあるとの事ですので、その内容がセキュリティを確保するための基本方針となっているかをご確認の上、自己評価ください。解説書P10にポリシーのサンプルが掲載されておりますので、自社のセキュリティポリシー内容が十分なものとなっているのか、比較いただくのも良いと思います。
参考 「情報セキュリティポリシーサンプル 1.0 版」(JNSA, 2016 年)
「情報セキュリティ対応方針(サンプル)」(IPA, 2019 年)

回答[No.153]：ガイドラインで達成基準として定めている通り、事業継続上重要なシステムに対し、「バックアップ及びトランザクションデータログの保管」「手順書の整備」が、各事業部門の復旧計画に含まれているかをご確認いただき、会社として評価ください。本自己評価は自社の状況を確認し、弱点を把握するためですので、現時点の点数を気にする必要はありません。

質問④

チェックシート及びお得意先様から本件に関して問い合わせがありますが、
秘密保持契約等なければ逆に内外に弱点等漏洩してしまう可能性があり、そこを懸念しております。

- **業界の標準化**: サイバーセキュリティに関する基準やガイドラインを策定し、それに従うことで、業界全体のセキュリティレベルを向上させることができます。標準化は、共通の問題に対処するための効果的な手段です。
- **リスク管理の強化**: サイバー攻撃や情報漏洩のリスクを軽減するために、企業がどのような対策を講じているかを示すことができます。ガイドラインに沿った取り組みを行うことで、リスク管理の強化につながります。
- **顧客や取引先への信頼の向上**: サイバーセキュリティ対策を適切に実施していることを示すことで、顧客や取引先からの信頼を得ることができます。特に、取引先がセキュリティを重視する場合、これに従うことは重要です。
- **法令遵守**: サイバーセキュリティに関する法令や規制が存在する場合、これに従うことで法令遵守を示すことができます。特に個人情報や重要情報を扱う場合、適切な対策が求められます。
- **インシデント対応の準備**: ガイドラインに基づいて事前に準備をすることで、万が一のインシデント発生時に迅速かつ適切に対応するための土台を築くことができます。
- **継続的な改善**: 定期的にガイドラインを見直し、提出することで、企業のセキュリティ対策を継続的に改善する機会を得ることができます。

質問⑤

ガイドライン[No.21]　情報セキュリティ事件・事故を含めた自社の事業継続計画又は緊急時対応計画の作成について、参考及び雛形になるものはありますでしょうか。

回答：参考になりそうな情報を以下に列挙しました。

●内閣府：「事業継続ガイドライン」
- ・事業継続計画（BCP）の基本的な考え方や計画策定方法について網羅的に記載されています
- ・文書の最後に添えてあるチェックリストで、事業継続の取組みに何が必要かを俯瞰できます

●中小企業庁：「中小企業BCP策定運用方針」
- ・組織の現在の事業継続能力を簡単な質問からチェックしたり、BCP様式などがダウンロードできたりします

＜BCP取組状況チェック（一部抜粋）＞

物的資源(情報)	情報のコピーまたはバックアップをとっていますか?
	あなたの会社のオフィス以外の場所に情報のコピーまたはバックアップを保管していますか？
	主要顧客や各種公共機関の連絡先リストを作成する等、緊急時に情報を発信・収集する手段を準備していますか?
	操業に不可欠なIT機器システムが故障等で使用できない場合の代替方法がありますか？
体制等	あなたの会社が自然災害や人的災害に遭遇した場合、 会社の事業活動がどうなりそうかを考えたことがありますか?
	緊急事態に遭遇した場合、あなたの会社のどの事業を優先的に継続・復旧すべきであり、 そのためには何をすべきか考え、実際に何らかの対策を打っていますか?
	社長であるあなたが出張中だったり、負傷したりした場合、 代わりの者が指揮をとる体制が整っていますか?
	取引先及び同業者等と災害発生時の相互支援について取り決めていますか？

●厚生労働省：「サイバー攻撃を想定した 事業継続計画（BCP）策定の確認表」
- ・医療機関向けですが、最低限の確認しておくべき項目に絞ってまとめており、一部読み替えての活用は可能です

質問⑥

・ガイドライン【No.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」について教えてほしい。サーバーの設置エリアに施錠が出来ません。専用ラックは必要でしょうか？
・ガイドライン【No.99】「PCからのデータ書き出しを仕組みで制限している」について教えてほしい。USBの利用制限をかけた場合、従業員の業務効率の低下が懸念されますが、制限をかけるべきでしょうか？

回答[No.85] ：サーバーを隔離できない場合、物理的なアクセスが容易になるため、サーバーへの不正アクセスやデータ漏洩のリスクが高まります。鍵付きの専用ラック使用や、サーバーが設置されているエリアの施錠化、施錠できるエリアへのサーバー移転など、サーバーへの物理的なアクセスを制限できる様対策を検討してください。

回答[No.153]：情報漏洩の主な原因の一つに、従業員による情報の不正持ち出し、紛失、盗難があり、USBデバイスの利用は、これらインシデントを引き起こす要因になる場合があります。個人情報や秘密情報の漏洩は企業経営に大きなダメージを与える可能性があるため、優先して対応する必要があります。USBデバイス一律禁止とすると従業員の業務効率低下が懸念されますので、業務効率を考慮しながら、自社に適した対策を複数取り入れて対応するのが良いと考えます。
《対策例》
・特定のUSBデバイスのみを許可するソフトウェアを導入し、会社が承認したデバイスのみ利用可能とする。
・USBポートの利用を一律不可とし、USBデバイスを利用したいユーザーが個別に利用承認を得る。
・USBデバイスの接続やデータ転送のログを監視し、不審な活動が検出された際にアラートを発出する仕組みを導入する。
・USBデバイスの使用に関するポリシーを定め、従業員へ定期的に教育を行う。
・USBデバイスへのデータ転送等は常時監視されていることを従業員へ周知し、悪事ができない事を認識させる。

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