よろず相談会第1回

2024年10月18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	情報セキュリティ関連規程を発行したが、その通りの運用はできていない。今後の進め方についてアドバイスがほしい
2	レベル１を目指していますが、何から手を付けていいか分からない状態です。ご相談をお願い致します。
3	ガイドライン[No.32]「各部署の情報セキュリティ管理者に対して、組織内での対策とマネジメント手法に関する教育を実施している」について教えてほしい。 管理者にマネジメント手法による教育を実施とありますが、具体的な事例をご教示下さい。
4	知識がなく、チェックシートに記載されている文言が分からないことが多い。
5	ガイドライン[No.37]「情報システムの調達に係る要員に対して、取引先の指導ができるようセキュリティ教育を実施している」について教えてほしい。 情報システムの調達に係る要員が、誰に何を指導する必要があるのか。取引先への指導とは、どのような内容を指すのか
6	セキュリティ対策の専任者を置くことは難しく、また社外で任せるにあたっての費用が大きすぎるので、もっと簡易な方法があれば教えて欲しい。

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

情報セキュリティ関連規程を発行したが、その通りの運用はできていない。今後の進め方についてアドバイスがほしい。

回答：
下記のような対応が考えられます。
①規定やルールの責任者の決定や見直し
⇒内容を鑑みて適切な管轄部署（所管部門）を責任者とし、運用の徹底含めて責任者にお願いする。
（例：「情報機器の利用ルール」では、情報提供/管理を行うIT部門長　など）
②規程の周知
⇒情報セキュリティ関連規程が社内へ浸透されるよう、いろいろな周知を行う。
（例：ポイントを簡潔に記載した配布物を用意、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で
定期的に流す、全パソコン利用者（役員・協力会社社員も含む）へ理解度アンケートを実施、など）
③社員の教育・意識向上
⇒社員ひとりひとりが規程を理解して遵守する必要があります。教育や意識向上のための啓発活動が有効です。
IPA等に教育向けの充実した資料がありますので、これらを活用頂ければと思います。
（例：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②

レベル１を目指していますが、何から手を付けていいか分からない状態です。
ご相談をお願い致します。

回答：
自社にとって何が大事か定義し、リスクを把握したうえで、そのリスクに見合ったセキュリティ施策を行うことが大事です。

・自社にどんな情報資産、ヒトモノカネに関する情報やデータがあるのかを書き出す。
・会社にとって、またはお客様にとっての「価値」をランク付けしてみる。
・その情報が漏えい、破壊、紛失、事故が起きた場合のリスクをランク付けしてみる。

会社の資産は、それぞれのステークホルダーが存在しますので、それぞれの目線に立ったうえで
何の資産が、どのように侵害されたときに、どのようなリスクがあるのか、まずは把握することから始めましょう。
そうすると、どのような体制が必要か、システムが必要か、ルールが必要か、といったことを考えることが出来るようになります。

本年度、JAMA・JAPIAから、「セキュリティ推進担当者向け解説資料」とし、何から対策をスタートするとよいか、ご参考となる資料を展開する予定です。また、下記のようなガイドラインもございますので、是非ご参考ください。

ガイドライン：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③

ガイドライン[No.32]「各部署の情報セキュリティ管理者に対して、組織内での対策とマネジメント手法に関する教育を実施している」について教えてほしい。管理者にマネジメント手法による教育を実施とありますが、具体的な事例をご教示下さい。

回答：
マネジメント層が理解しておかなければならない内容としてはまずは「世の中にはどのようなリスクがあるか」、「対策しないとどのような影響が出るか」を理解することです。各種資料が公開されいますが、読み解くのに時間が掛かったり理解するのが困難な場合も多いかと思います。HPに掲載されている動画の場合は時間に余裕がある時に視聴可能かと思いますので、下記にご紹介します。

自工会・部工会においては説明会を実施しており、その中でマネジメント層向けに上記の内容を説明しています。
下記に説明会の資料及び説明動画を掲載しております。
自動車産業サプライチェーンへの推進活動 | JAMA - 一般社団法人日本自動車工業会

またIPAのサイトに各種セキュリティ事例・対策事例の動画が掲載されています。
こちらの動画を使用した教育も手段の一つとなるかと思います。
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

参考資料：マネジメント層が知っておくべきリスク、取り組みの事例が記載されています。
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

質問④

知識がなく、チェックシートに記載されている文言が分からないことが多い。

回答：
【是非お願いしたいこと】

「わかるところから少しでもよいのでまず始める」ことが大切で、わからないところは一旦置いておいて、始めていただくというのが重要です。

活用できそうな資料をご紹介いたします。

①解説書資料

⇒自工会HPにチェックシートの主要項目の解説資料をご準備しております。

cyb_sec_guideline_manual_v02_02.pdf (jama.or.jp)

②セキュリティ推進担当者向け解説資料

⇒チェックシートのレベル1の中でも優先項目に絞った解説資料となります。

現在整備中ですが、今月～来月にかけて、自工会HPへ掲載予定です。

③セキュリティ教育資料

⇒セキュリティ知識の向上として、IPA等の教育資料の活用も有効です。

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⑤

ガイドライン[No.37]「情報システムの調達に係る要員に対して、取引先の指導ができるようセキュリティ教育を実施している」について教えてほしい。情報システムの調達に係る要員が、誰に何を指導する必要があるのか。取引先への指導とは、どのような内容を指すのか

回答：

誰に？→　情報システムの調達を行い、セキュリティ要件の仕様出し、及び受け入れテストを行う部署
何を？→　調達する情報システムのセキュリティ品質が確保するための、基礎知識や確認ポイント

例えば、外部から接続が出来るリモート機器を調達するとしたとき、

- ISO等の認証が取れている仕入先か、製品か
- パッチのアップデートが行えるシステムか、体制となっているか
- ログがきちんと残る仕様となっているかどうか
- 調達後の保守契約は適切か（何かあったとき仕入先のサポートはあるのか）

上記は一例に留まりますが、外部から侵害されるリスクのある情報システムを調達するためには、調達担当者がきちんとセキュリティ要件を把握したうえで調達することが肝要です。教育資料の作成の際には、以下の経産省やIPAのガイドライン等が活用できると思いますので、是非ご参照ください。

ガイドライン：IT製品の調達におけるセキュリティ要件リスト活用ガイドブック | 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⑥

セキュリティ対策の専任者を置くことは難しく、また社外で任せるにあたっての費用が大きすぎるので、もっと簡易な方法があれば教えて欲しい。

回答：
社内の人員で行う対策としては下記に掲載されている内容を確認し、自社で使用している機器・ソフトウエアが掲載されているか確認し、対策を実施することが考えられます。
JPCERT/CC 脆弱性関連情報　　JPCERT コーディネーションセンター
IPA 重要なセキュリティ情報　　重要なセキュリティ情報 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

また下記ガイドラインの第 2 部　実践編にその他の対策方法について記載されています。
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

全ての対策を自社のみで行うには工数が掛りますし、専門知識が必要な場合があります。以下に記載したIPAの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**民間サービスです。（審査を経てIPAが要件を満たすことを確認したサービス）
「見守り」機能としてUTM等によるネットワーク監視型、EDR等による端末監視型、併用型のいずれかを選択できます。
低コストでの対策としてご検討ください

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

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＞

JC-STAR

- 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

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。

サイバーセキュリティ お助け隊

「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。

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

IPA

・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 CSお助け隊

マーク付きの民間サービス

中小企業

E N D