よろず相談会第4回

2024年11月6日(水) 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しないこと、ご承知おきください。

本日取り上げさせて頂くご質問一覧

No.	質問
1	会社規模が小さく、セキュリティの組織体制を構築するための知見がない。(知識不足、知見不足） 又、人員、費用を確保する事も困難である。そもそもセキュリティ対策は、どこまで行う必要があるのか、費用はどのくらい費やすのが良いのか、業務効率とセキュリティ対策とのバランス、最適解について知りたい。各社どのように構築されているのか?
2	インシデント発生時の初動対応について知りたい。又、インシデント対応訓練が未実施のため、机上訓練の事例を知りたい。
3	まずはマニュアルを作成してはいるが、ハードウェア対策や従業員への教育方法について、どの様に実施したら良いのかアドバイスが欲しい。
4	セキュリティ強化を推進する際に、経費負担をどの部署とすれば良いのか、決済をどう通せば良いのか悩んでいる。
5	EDR、SOC、UTM、サイバー保険等、他社は何をどこまで導入しているのか知りたい。又、最低限導入すべきなものは何かを知りたい。
6	ログ分析をサイバー攻撃検知につなげる場合、どこまで(どのログか、ログの内容や方法など)を対象とすれば良いのか知りたい。

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

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ｺｰﾃﾞｨﾈｰﾀ、医療情報技師
- CISSP@ISC2、CISA@ISACA、CIA@IIA

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 No. 1

会社規模が小さく、セキュリティの組織体制を構築するための知見がない。(知識不足、知見不足）又、人員、費用を確保する事も困難である。そもそもセキュリティ対策は、どこまで行う必要があるのか、費用はどのくらい費やすのが良いのか、業務効率とセキュリティ対策とのバランス、最適解について知りたい。各社どのように構築されているのか?

回答：最適解の考え方は、保有資産や業務体系により異なってくるため、情報の整理から始める必要があります。

・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把握する。
・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把握する。

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、把握することから始めましょう。

また、本年度、JAMA・JAPIAから、「セキュリティ推進担当者向け資料」という位置づけの、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。さらに、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。
最適解の考え方は難しく、環境や情勢により変化していくことを考えると、恒久的に模索していかなければならないところもございます。まずは、出来るところから手をつけて頂ければと思います。

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 No. 2

滝

インシデント発生時の初動対応について知りたい。
又、インシデント対応訓練が未実施のため、机上訓練の事例を知りたい。

回答：インシデント対応の目的は、インシデント発生による被害とその影響範囲を最小限に抑え、迅速に復旧し、再発を防止することで企業の事業継続を確保することです。
今回ご相談のインシデント発生時の初動対応としては、以下の通り実施いただくのが一般的です。

① インシデントが疑われる兆候や実際の発生を発見した場合、情報セキュリティ責任者に報告。情報セキュリティ責任者は、対応すべきインシデントであると判断した場合、速やかに経営者に報告。経営者は、速やかにインシデント対応のための体制を立ち上げ、あらかじめ策定している対応方針に従い、責任者と担当者を定めて、役割分担を明確にする。
② 担当者や情報セキュリティ責任者は、インシデント対象となる情報が外部からアクセスできる状態にある場合や、被害が広がる可能性がある場合は、ネットワークの遮断、情報や対象機器の隔離、システムやサービスの停止を行う。ただし、対象機器の電源を切る等、不用意な操作でシステム上に残された記 録を消さないようにする。

その後、報告・公表、復旧・再発防止のステップで対応を行います。詳細はIPAの「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」をご参照ください。

机上訓練は、様々な企業にて有料サービスを実施しておりますが、23年度IPAにて「経営者向けインシデント対応机上演習」が実施されています。全国15か所程度、3時間の集合研修で、参加費は1000円/1名でした。次回実施は未定ですが、IPAホームページを定期的にご確認いただくのが良いと思います。

質問 No. 3

伊

まずはマニュアルを作成してはいるが、ハードウェア対策や従業員への教育方法について、どの様に実施したら良いのかアドバイスが欲しい。

回答：

ハードウェア対策

パソコン、サーバー、スマートフォン、タブレットなどのハードウェア対策は、様々な対策が必要となりますが、その中から優先的に対応すべき項目として5点挙げます。こちらの対策を対応後、自動車産業サイバーセキュリティガイドラインに基づいて対策出来ていない項目を進めてください。

①OS、ソフトウェアの最新版へのアップデート　②ウィルス対策ソフトの導入　③パスワードの強化
④共有設定の見直し　⑤ネットワーク外でのバックアップ、データ保管

従業員への教育方法

従業員へのセキュリティ教育の主なポイントは以下になります。

・教育対象者：ITシステムを取り扱うすべての人員に実施（経営層、派遣社員、アルバイトも含みます）
・実施タイミング：単発にならないように定期的に開催する計画を準備
・効果確認とフォロー：教育実施が目的にならないようにテストやアンケートを実施し、その結果に対するフォローを実施

教育コンテンツを自作することが難しい場合は、IPAが提供している動画や教育資料を活用することをお勧めします。

参考サイト：映像で知る情報セキュリティ 、5分でできる！情報セキュリティポイント学習

質問 No. 4

セキュリティ強化を推進する際に、経費負担をどの部署とすれば良いのか、決済をどう通せば良いのか悩んでいる。

回答：経費負担の考えは各社によって異なりますので、以下検討材料として情報を提供いたします。

①全社的に使用する機器／サービスについてはIT部門（情報セキュリティ部門）が負担
②ルールに基づいて、各部署が購入する機器／サービスについては各部署で負担

①については、例えば「会社⇔インターネット 間のFW」や、「IT部門が配布しているPCへのセキュリティ施策」については一元的にIT部門が経費を負担するという考えです。全社施策については、IT部門で事前に予算計画を立てることが可能だという考えの前提です。
②では、例えば各部署が外部に公開するサービス（クラウド環境等）を使用するとした際に、ルールに基づいて実施する各種セキュリティ施策（アンチウイルスソフト、脆弱性診断サービス等）については、各部署が負担します。これは各部署が独自に予算計画を立てる必要があるため、各部署での負担とするという考えです。

上記の考えが全てではなく、会社規模によっては一律情報セキュリティ部門が経費負担するというのも一つの考え方ですので、実運用を回すにあたってどの部署が適切なのかは、関係部署を巻き込みながら調整をお願いいたします。

質問 No. 5

滝

EDR、SOC、UTM、サイバー保険等、他社は何をどこまで導入しているのか知りたい。
又、最低限導入すべきなものは何かを知りたい。

回答：情報セキュリティにおいて、EDR（Endpoint Detection and Response）、SOC（Security Operations Center）、UTM（Unified Threat Management）、サイバー保険はそれぞれ異なる役割を果たしており、どの機器やサービスを導入するかは、組織の規模、既存のセキュリティ体制、予算規模等によるため、一般的に何をどこまで導入しているかのご回答は難しいです。本日ご出席の会社様におかれましては、自社の導入事例を共有いただけるとありがたいです。

組織規模やセキュリティ体制などによりますが、最低限導入すべき対策としては、以下をご検討ください。これらは「セキュリティ推進担当者向け資料」として、近日自工会HPに掲載予定の資料に含まれています。HP掲載後ご利用ください。

- ✓ ネットワーク外でのバックアップ、データ保管：サイバー攻撃を受けた際に素早く復旧できる様にバックアップしましょう。
- ✓ 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ぐためアップデートしましょう
- ✓ ウィルス対策ソフトの導入：ランサムウェア攻撃等から情報資産を守るために導入しましょう
- ✓ 共有設定の見直し：システムの共有設定が正しいか、不要なアカウントがないか確認しましょう。

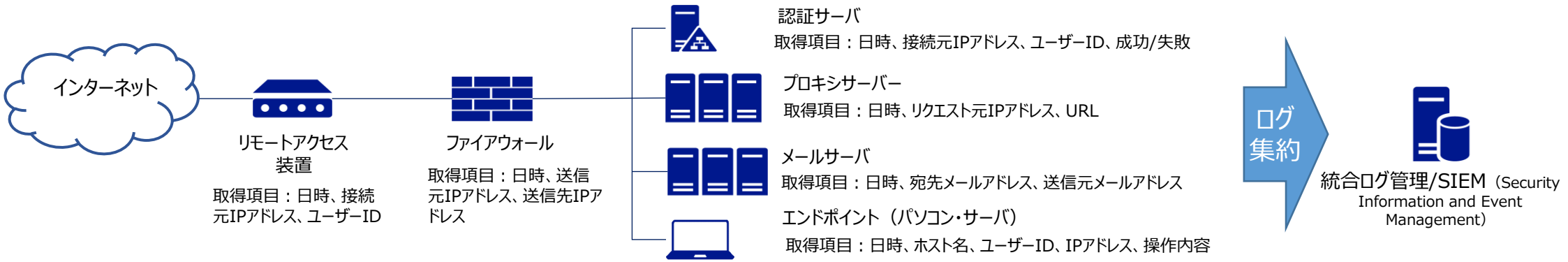
十分な投資が出来ない場合や自社で機器を運用する要員確保が厳しい場合は、IPAが認定する「サイバーセキュリティお助け隊サービス」の利用を検討することも一つの方法です。「見守り」「駆付け」「保険」などセキュリティ対策に不可欠なサービスをワンパッケージで安価に提供する民間サービスで、社内ネットワークにUTM等を設置して通信を監視するサービス、PCへEDR等をインストールし、個々のPCの通信や挙動を監視するサービスなどを選ぶことができます。

質問 No. 6

伊

ログ分析をサイバー攻撃検知につなげる場合、どこまで(どのログか、ログの内容や方法など)を対象とすれば良いのか知りたい。

回答：
サイバー攻撃が発生した場合、侵入・拡散経路を考慮したログの取得が必要となります。
下図の対象や内容でログを取得することが一般的ですが、各社の環境に合わせて対象を検討してください。
また、個別の機器でのログから、サイバー攻撃を検知することも可能ですが、ログを統合管理することで相関分析（異なる複数のログやイベントの関係性を特定し、異常性や攻撃の兆候を検出する）が可能となり、攻撃全体のパターンや攻撃経路を把握し、より効果的な検知、対応が可能となります。



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。

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。

◇「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