よろず相談会 第９回

2025年2月26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	EDRの導入効果を知りたい
2	No80.「許可された機器以外は社内ネットワークに接続できないよう、システムで制限している」に関して、 他社ではどのように展開を行っているか知りたい。同規模程度の会社にて、 どの程度（社内関係会社、小規模拠点、 外注拠点でも実施？等々）、どのように（L2SW側の設定にて.1X認証を実施？等々） 具体的に
3	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
4	ルール作成のようなものは有るか無いかと言うことで回答しやすいが、周知しているというような運用面については回答が難しい（Ex. No 3、8、23、82 etc）。どのように判断すれば良いか
5	サーバーの管理などをお願いしている外部業者とセキュリティ対策に関する契約ができないか協議する場合、どのような点に注意すれば良いか？
6	Windows、グループウェア、基幹システムのパスワード設定や、UTMの設定について、どのような点に注意すれば良いか？

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。

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

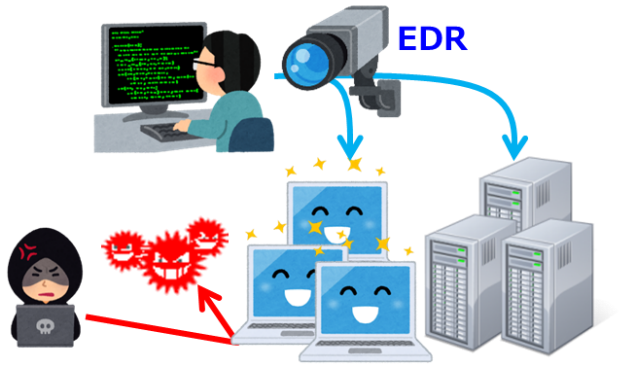
質問①

EDRの導入効果を知りたいです

回答：EDR製品を導入することにより期待されることは、主に以下の３つがあります。

①サイバー攻撃被害から守る

エンドポイントのログを収集・分析し、怪しい挙動や攻撃を
検知＆隔離して脅威を除去
※未知ウィルスにも対抗



②マルウェア被害範囲の特定

万が一侵入を許してしまった場合においても、
被害端末を一台ずつ通信ログを分析せずに、
統合管理的に被害範囲を把握可能

③セキュリティ事故復旧対応時、
クリーンなサーバ・端末であることを判別

※第３回 よろず相談会
資料より抜粋

上記から、見える化できる効果としては、以下のような項目が挙げられます。
1．インシデント数・・・未知のウィルスにも対応できるため、被害につながるインシデント数が減少する
2．インシデント対応時間・・・被害範囲の特定が可能で、復旧対応がスムーズになり、対応する時間が短くなる

なお、IPAサイバーセキュリティお助け隊のサービス導入実績でも、インシデント数の減少につながったと読み取れる報告がされております。（サイト／報告書 ※P16）

質問②

・№80.「許可された機器以外は社内ネットワークに接続できないよう、システムで制限している」に関して、他社ではどのように展開を行っているか知りたい。
同規模程度の会社にて、
　－どの程度（社内関係会社、小規模拠点、外注拠点でも実施？等々）
　－どのように（L2SW側の設定にて.1X認証を実施？等々）　具体的に

回答：【どの程度】について：対象としては自社の機密情報が存在する拠点が対象となります。特に社内ネットワークに接続されている拠点は対策が必要かと思います。
【どのように】：実施方法例
・ネットワークアクセス制御システム（NAC等）を利用した認証
　⇒規模が大きく複数拠点を持つような会社向け
・L2SW等のネットワーク機器によるMACアドレスフィルタリング、証明書による認証等
　⇒拠点や端末が少ない会社向け。原則拠点内管理なので、複数拠点を持つ場合は管理工数が増大
・DHCP認証
　⇒DHCPサーバでMAC認証でIPアドレスを付与。IPレンジが知られた場合は接続が可能
・物理的な対策
　⇒入室制限、持ち込み品検査、ネットワーク機器の施錠、物理的なポート閉塞等
在宅勤務も一般化している現在では機器の接続制限だけでセキュリティを担保するのは困難となりつつあります。アカウント認証（システムやVPNの認証）やネットワーク分離による通信制限、SASE等とも組み合わせて総合的な対策でセキュリティを向上させていくのが重要と思います。

質問③

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。

【人員】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３つの方法が考えられます。

１）**自社人員を推進者に指名**し育てる：まずは兼任でも指名、当該チェックシート評価や関連資料の勉強から始める

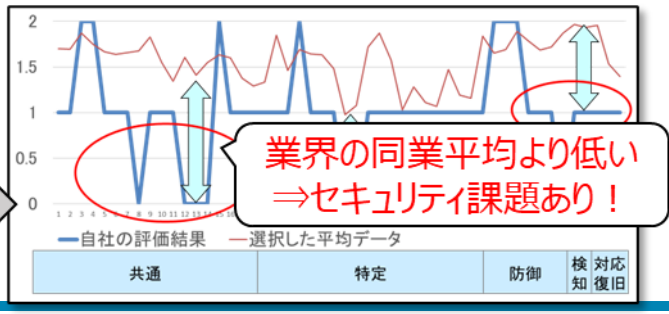
２）**中途採用**を活用し、即戦力の人員を確保する

３）**外部ベンダーを活用**し人員を確保：自社担当者で不足する人工や専門知識を補強します

但し、いずれの方法についてもそれなりの費用がかかります。

【費用】サイバーセキュリティ対策費用は勿論、上記の人員確保にも費用がかかります。 まずは、**経営陣に「サイバーセキュリティは経営課題」であることを理解頂く**こと、そして必要な投資を引き出すことしか手はありません。
理解を得る方法は多々あると思いますが、JAMA/JAPIAで推進している施策から紹介します。

1. 経営層向け説明会は正に、経営陣に「サイバーセキュリティは経営課題」であることを理解頂くことを狙っています。聴講した経営者の６割以上が、自社の「リソーセス確保」が最重点課題だと認識して頂けました。
2. 動機付・攻め所の一助：自動車業界平均比較テンプレート（自己評価提出会社へ送付）



質問④

ルール作成のようなものは有るか無いかと言うことで回答しやすいが、周知しているというような運用面については回答が難しい。（Ex.　項目番号 No.3、No.8、No.23、No.82）

回答：周知している、という項目については、「どの程度の周知が実施できていれば達成基準を満たしていると判断してよいのだろうか？」と迷ってしまう方もいるかと思います。大多数の周知対象者に認知される可能性の高い施策を行っているかどうかがポイントになります。周知対象者は組織によって異なるため、あくまでも一例とはなりますが、表にまとめました。参考にしながら評価いただくことで、本ガイドラインの意図に沿った評価に近づけることが出来るかと考えます。

周知したい内容	周知対象者	十分に周知できていると判断できる例	これだけでは周知が不十分な例
[No.3] 情報セキュリティ対応方針（ポリシー） [No.23] 情報セキュリティ事件・事故の対象範囲	全従業員、派遣社員	・全拠点において壁にポスター等で掲示 ・毎日閲覧がされると考えらえる組織内ポータルサイトに目立つ形でリンクを掲載	・新卒社員の入社時研修で教育を実施（派遣社員や中途社員は存在を知らない、勤続年数の長い社員の多くは存在を忘れてしまっている）
[No.8] 業務で扱う情報機器の利用ルール	PC、スマホ利用者	・年1回の従業員向け情報セキュリティ研修で利用ルールについて教育を実施（周知対象者以上に実施している）	・PCについては配布時に、PC利用ルールの載ったリーフレットを配布（スマホ配布時に未対応）
[No.82] リモートワークの機器利用ルール	リモートワーク対象者	・リモートワーク申請サイトに掲示 ・リモートワーク対象者の教育資料に掲載	・組織内ポータルサイトの階層深くに掲載（多くの人は存在を知らない、容易に探せない）

質問⑤

サーバーの管理などをお願いしている外部業者とセキュリティ対策に関する契約ができないか協議する場合、どのような点に注意すれば良いか？

外部業者と契約する上では下記点を踏まえて自社に最適なサービスを検討する必要があるかと思います。

1．自社と同程度の規模の会社へサポートした実績があるか？
それぞれの外部業者のサポートメニューで想定している規模が違います。
自社に合った内容を提案頂く上で規模感を確認した方が良いと思います。

2．機密情報の取り扱いは適正か？
セキュリティ業務委託する場合取り扱う情報は機密度が高く、漏れた場合に外部からサイバー攻撃を受ける可能性が出てきます。そのため委託先のセキュリティ評価が必要となります。
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　P28（4）委託時の対策
付録5：情報セキュリティ関連規程（サンプル）（全42ページ）（Word:167 KB）　P27～委託管理

3．必要なコストが自社の予算と合っているか？
1番とも関連しますが、想定される規模感で提案されるソリューション・コストが変わってきます。
運用費用、ソリューション導入費用等を考慮し、決定する必要があります。

4．サーバ導入後の運用面での取り決め
自社と外部業者の責任範囲（有事の対応責任、セキュリティパッチ適用運用など）について、
事前に外部業者と合意して契約書等に記載すると良いと思います

質問⑥

Windows、グループウェア、基幹システムのパスワード設定や、UTMの設定について、どのような点に注意すれば良いか？

グループウェア：複数のユーザーが共同で作業を行うためのソフトウェアツール、例えばTeams。
UTM：Unified Threat Management 統合脅威管理、複数のセキュリティ機能を持ち、包括的に社内ネットワークを保護するシステム。

【パスワード設定の注意点】 当該**チェックシートのNo.115、116、120**にパスワード設定の注意点が記載されています。
・桁数・組合せ文字・有効期限を定める（8桁以上、英大文字・小文字・記号・数字のうち、3種類以上を組合せる等）
・英字や数字の連続など容易に推測されるものを避ける（NG：IDと同じ、名前・電話番号・生年月日、辞書にある単語 等）
・パスワードの使い回しをしない　・デフォルトパスワードは変更　　・リスクが高いシステムには多要素認証を実装　etc

【UTM設定の注意点】「自社環境に適した機器や設定」を信頼できるセキュリティベンダー等に相談する方が良いでしょう。
・導入時：**処理能力**、**セキュリティ機能**(ファイヤーウォール、侵入防御IPS、アンチウィルス、URLフィルタリング、アンチボット、サンドボックス等)、**通信速度**などを検討して自社に適した機種を選択
・設定時：初期設定(機器設置、N/W設定等)、セキュリティ機能有効化、**UTM監視・アラート処理の実施** 有無判断

（※１）**お助け隊サービス**のネットワーク監視はUTMを設置し見守り・駆付けを廉価に行うサービス！ 検討下さい。
（※２）実は私、自らUTMを設置した事が無く、上記の記述は一般論です。経験者 居られましたら、是非お話をお願いします。

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