# よろず相談会第2回

## - 技術対策（ウイルス対策,セキュリティ監視,ランサム対策） -

2023年11月1日

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
総合技術委員会 IT 対応委員会 CS 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します。 |
| | 事前に頂いたご質問につきまして、本日のテーマに沿ったものを選定し、<br>個社の情報等を省き、一般化しておりますので、予めご了承ください。 |
| 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、<br>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をさせて頂く場合もございます。<br>予めご了承ください。 |
| | 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。 |

# 本日取り上げさせて頂くご質問一覧

| No | 質問 |
|---|---|
| ① | 中小企業としてウィルス対策、セキュリティ監視、ランサム対策をどのレベルまで行えばいいか。 |
| ② | 電子メールによるマルウェア感染が流行する中メール訓練を実施したいが費用が掛かったりどのように実施して良いか決めかねている。毎年行う防災訓練のように自社で計画し訓練を行いたいがもし具体例があれば知りたい。 |
| ③ | メーカーに推奨された対策をしていますが、詳しい人もいません。そのような会社での対策や管理方法を教えて頂きたい.。 |
| ④ | VPNをOKとするか否とするか、OKの場合、どのような対策をすればよいか。 |
| ⑤ | No.96：具体的な盗聴による情報漏洩対策の手法、手順等の情報が知りたいです。 |
| ⑥ | ダークウェブへのアカウント情報流出状況や、流出時の具体的な対応についてご教示いただきたい。 |
| ⑦ | 通信内容の常時監視や不正攻撃への検知／遮断の仕組みで、投資をする場合どんな製品が必要か？<br>また、投資ができない場合は運用でカバーすることが可能か。 |
| ⑧ | ログの取得と監視24/365・SIEM機能を要請されていますが、自社で実施できるスキルが無いため、外部に依頼しようと相談したのですが、月額数千万円の概算見積りが届きました。Lv.2で100点満点を取るために必須と思われますが、全サプライヤが実現できるとは思えません。これについてどの様にお考えでしょうか？ |
| ⑨ | 相関分析（複合的なログなどで分析して情報セキュリティ事件・事故の予兆や痕跡を見つけ出す手法）とは、具体的に何を行っているのか。予兆という事なので常にチェックを行っているのか？ログの分析頻度など知りたい |
| ⑩ | VPNからの侵入事例をよく聞きますが、VPN機器の後に繋ぐ装置などで検出できるものでしょうか？ |

# 本日取り上げさせて頂くご質問一覧

| No | 質問 |
|---|---|
| ⑪ | 想定している技術対策をおしえてください |
| ⑫ | ランサムウエア対策としてのデータのオフライン保管用バックアップは、どの程度の期間保存しておくのが望ましいでしょうか。<br>（現状は、週に一回、３カ月分保存しています。） |
| ⑬ | サイバー攻撃模擬訓練を実施する際のポイントを教えていただきたいです。 |
| ⑭ | 低コスト(出来るだけ費用をかけずに)で出来る技術対策があれば教えて頂きたいです<br>※費用さえかけれるのであれば色々な対策ソフトを導入すれば良いと思いますので |
| ⑮ | No.31やNo.81など情報漏えい対策として自動検知する仕組みや標的型メール訓練を検討していますが、いずれも導入コストが高いと感じており、中々承認を得られない状況です。他社様は補助金制度等を利用してご承認およびご導入となっているのか、こちらも情報共有頂きたいです。また、そもそもどのぐらいのコスト感を持って取り組んでいるのかも知りたいです。 |

**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。**
**ご理解の程よろしくお願い致します。**

# 質問①

質問内容：中小企業としてウィルス対策、セキュリティ監視、ランサム対策をどのレベルまで行えばいいか。
また、各社の導入事例を参考にしたい。

回答：

サイバー攻撃におけるセキュリティリスクは、各社様の規模にかかわりませんので、基本的にはどの対策も会社規模にかかわらず全項目実施すべきものと考えます。

但し、各項目における達成手段については、各社様の状況に合わせ実施頂ければ結構ですので、IPAが発行する「中小企業の情報セキュリティガイドライン」等を参考に各社様に適合した手段／環境にて実施頂ければと存じます。

なお、各社様の導入事例については折角の機会ですので、本日ご参集の会社様からご紹介頂ければ幸いです。

情報交換項目例）

- **52 アクセス権の棚卸を定期的、または必要に応じて実施している（Lv1）**
- **117 ユーザーID 及びシステム管理者 ID は定期的または必要に応じて棚卸しを行い、不要な ID を削除している（Lv1）**
- **99 PC からのデータ書き出しを仕組みで制限している（Lv2）**

# 質問②

質問内容：電子メールによるマルウェア感染が流行する中、メール訓練を実施したいが費用が掛かったり、どのように実施して良いか決めかねている。毎年行う防災訓練のように、自社で計画し訓練を行いたいが、もし具体例があれば知りたい。

回答：

自社による標的型メール訓練を計画される場合、先ずは

・IPA「組織における標的型攻撃メール訓練は実施目的を明確に」
・NISC「攻撃メール訓練の目的や方法を見直すヒント」

などの信頼できるサイト等を参考に、自社におけるメール訓練の目的・対象者・効果的な文面例などを検討してください。そのうえで訓練環境を設定頂くことになりますが、ITに詳しい社員様がおられる場合は、市販のキットを購入することにより、廉価での実施も可能と考えます。自社での実施が難しい場合は、多くのベンダー様より実施サービスが提供されておりますので、そちらもご検討願います。対象者の規模・仕様により価格も多岐に渡りますので、各社様の状況に合致したものを選定頂ければと存じます。

情報交換例）

**・各社様のメール訓練実施状況／実施環境／費用規模（差支えない範囲で）**

# 質問③

質問内容：メーカーに推奨された対策をしていますが、IT部門もなく詳しい人もいません。そのような会社での対策や管理方法が有れば教えて頂きたいです。

回答：

中小企業様など、現実的にIT人員がおらず、活動が進まない会社様も多いかと思います。脅威が高度化する一方、ITセキュリティ関連人員の確保は困難かと思いますが、技術的な側面が強く専門性も高いSOCなどの機能については、IPAの認定する中小企業に向けたサービス等もありますので、外部のSOCサービス等の利用を検討することも一つの方法かと思います。

IPA サイバーセキュリティお助け隊サービス：

「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（審査を経てIPAが要件を満たすことを確認したサービス）
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

情報交換例）

**・不足するIT人材に対する各社様の取り組み**

# 質問④

質問内容：VPNをOKとするか否とするか、OKの場合、どのような対策をすればよいか。

回答：

特に若い世代を中心とする昨今の働き方から見て、在宅勤務をはじめとするテレワーク環境の整備は避けて通れないものと考えております。会社構外での業務においては、情報漏洩リスクの高まりは避けられませんが、それを低減する有効な手段としてVPNは広く普及しており、各企業様におかれましても導入は不可避と考えます。

VPN環境における情報漏洩対策としては、利用端末からの情報持出し機能を遮断する（シンクライアント化または書き出し制限機能の実装）が有効なものと考えております。
また、それを補完する牽制手段として

- **情報持出しの禁止に関し利用者と合意し、署名を取得する。**
- **データの持出し状況を常にモニタリングし、異常を検出する環境を構築する**
- **万一の不正に対する厳格な処分に関しルール化し周知する**

等が考えられます。

情報交換例）

- **テレワークにおける各社様の情報漏洩対策**
- **VPNの脆弱性に対する各社様の取り組み状況**

# 質問⑤

質問内容：No.96：具体的な盗聴による情報漏洩対策の手法、手順等の情報が知りたいです。

回答：

先ずは物理セキュリティ対策として、重要機密を扱う会議室等への無関係者（社員を含む）への侵入手段を制限すること（二要素認証等による入室管理・監視カメラの設置・建物最上階への会議室配置など）。

次に会議でのプレゼン環境への配慮（アナログマイクの使用禁止・プロジェクタではなく、個人ごとに資料表示など）

更には定期的な点検（電波漏洩チェックによる盗聴器の調査／駆除、目視による盗聴器・隠しカメラ等の駆除など）

などが考えられます。これらに関する責任部門を明確にし、定期的に状況をトップに報告する運用を確立頂ければ、本項目は達成とお考え頂いて差支えないものと考えます。

情報交換例）

**・各社様の盗聴による情報漏洩対策があればご紹介願います。**

# 質問⑥

質問内容：ダークウェブへのアカウント情報流出状況や、流出時の具体的な対応についてご教示いただきたい。

回答：
ダークウェブは一般的な検索エンジンでは表示されることがなく、専用のツールやブラウザを必要とするウェブサイトのことです。
非常に匿名性が高いことから、違法な取引（ハッキング等で入手したアカウント情報/個人情報、ハッキングを行うツールやマルウェア自体、等）で利用されることが多く、一般人が触れることはありません。
実はダークウェブの方が、インターネット上では圧倒的に数が多いとされています。

「日本のメーカーは狙われやすい」 ダークウェブ情報流出、主要30社で確認（出典：ITmedia NEWS）

| 区分 | 製造業 | 行政・自治体 | 金融業 |
|---|---|---|---|
| 1000件以上 | 8社 | 3社 | 6社 |
| 500～999件 | 4社 | 3社 | 4社 |
| 100～499件 | 4社 | 11社 | 9社 |
| 1～100件 | 14社 | 6社 | 11社 |
| 流出件数 | 28,983件 | 11,622件 | 15,202件 |

アカウント情報が流出した場合、アカウントの停止やアカウントパスワードの変更が必要となります。
また、外部サービスで利用しているアカウント情報が漏えいする可能性もあるため、アカウント情報（ID/PW）の使いまわしは避けることが重要です。

# 質問⑦

質問内容：通信内容の常時監視や不正攻撃への検知／遮断の仕組みで、投資をする場合どんな製品が必要か？
また、投資ができない場合は運用でカバーすることが可能か。

回答：
ファイアウォール、IDS/IPS、Webフィルタ、アンチウィルス、等のセキュリティ機能を1台で対策できるUTM（統合脅威管理）機器・サービスをご検討頂ければと思います。

常時監視、不正攻撃の検知／遮断は、技術的な機能が必要となってくるため、運用のみで対応する事は難しいと思います。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が認定する中小企業向けサービスもありますので、サービス利用を検討することも一つの方法かと思います。

IPA サイバーセキュリティお助け隊サービス：
「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（審査を経てIPAが要件を満たすことを確認したサービス）
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

# 質問⑧

質問内容：ログの取得と監視24/365・SIEM機能を要請されていますが、自社で実施できるスキルが無いため、外部に依頼しようと相談したのですが、月額数千万円の概算見積りが届きました。Lv.2で100点満点を取るために必須と思われますが、全サプライヤが実現できるとは思えません。これについてどの様にお考えでしょうか？

回答：
自工会・部工会としては自動車産業のサプライチェーンに参加される全ての会社様に、その企業規模を問わず、レベル２までの全項目を達成頂くことを希望しております。
但し、人員スキル・規模・予算上等の問題でそれが困難な会社様におかれましては、現時点ではレベル２を全件達成することは困難であっても、まずは達成出来る項目から取り組んで頂き、達成項目を増やしてから人員や予算の配分を考えていただければと思います。

また、比較的安価でサービス利用料がIT導入補助金の支援対象となるIPAが認定する中小企業に向けたサービスを検討することをお勧めします。

IPA サイバーセキュリティお助け隊サービス：
「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（審査を経てIPAが要件を満たすことを確認したサービス）
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

# 質問⑨

質問内容：相関分析（複合的なログなどで分析して情報セキュリティ事件・事故の予兆や痕跡を見つけ出す手法）とは、具体的に何を行っているのか。予兆という事なので常にチェックを行っているのか？ログの分析頻度など知りたい

回答：
様々な分析例がありますが、一例を紹介いたします。

以下のログが取得されていた場合、①～③のログ単体だけでは、怪しいとは言えないが、複合的に実行されている場合は、システムへの侵入を疑うことができます。

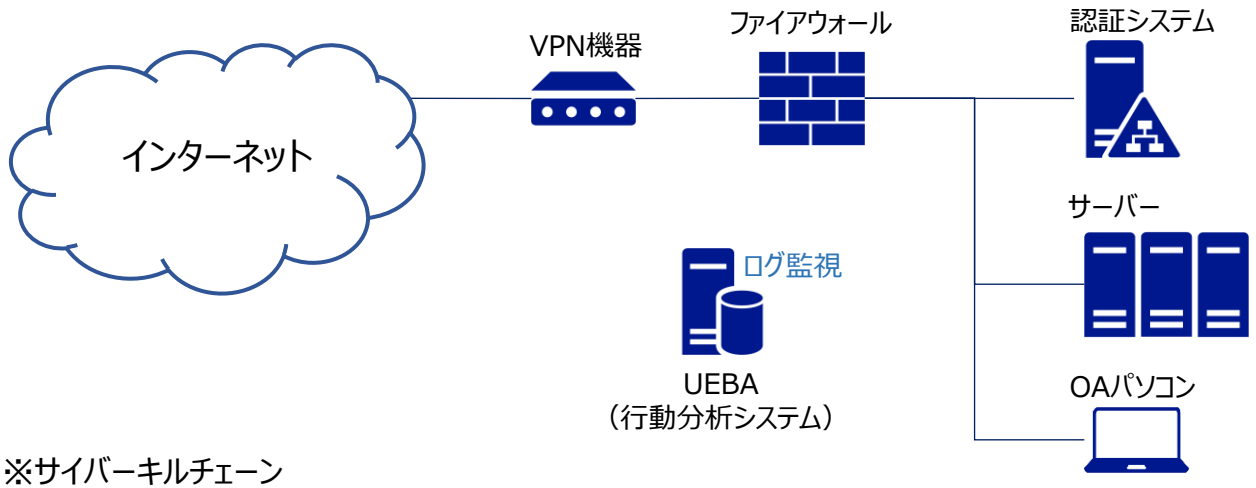
① ログインに10回連続で失敗したあと、ログイン成功した
② 海外からログインした
③ 管理者コマンドを実行した

このように収集したログに異常があるかどうか、相関関係を活用して分析することで、リアルタイムで異常を検知することができます。
このような分析ルールに基づいた分析を手動で実施することは困難であるため、様々な分析ルールに基づいて自動検知を行う、SIEM（Security Information and Event Management）システムを活用することで効率良くログ分析が可能となります。

# 質問⑩

質問内容：VPNからの侵入事例をよく聞きますが、VPN機器の後に繋ぐ装置などで検出できるものでしょうか？

回答：
各種機器のログやエンドポイントセキュリティ製品で検出することは可能です。
社内への侵入を防ぐためにVPN機器の対策（脆弱性対応、パスワード管理、等）を確実に実施することが重要ですが、単一の技術要素や攻撃局面のみで対策しようとするのではなく、サイバーキルチェーン(※)に対応した多層対策を行うことが重要です。




※サイバーキルチェーン
サイバー攻撃が行われる過程を7段階の行動にモデル化したもの。軍事分野で敵を攻撃する過程を4段階に分類した「キルチェーン」（kill chain）概念をサイバー攻撃に応用したもの。
サイバーキルチェーンとは - 意味をわかりやすく - IT用語辞典 e-Words

- ファイアウォール
  通信ログから不審通信、不審挙動を検知
- 認証システム
  認証失敗ログや認証時間ログから不審挙動を検知
  （多要素認証を採用することで、アカウントを窃取されても不正アクセスを防ぐことは有効な対策）
- サーバー
  EDRによる振舞い検知
- OAパソコン
  EDRによる振舞い検知
  操作ログから不審挙動を検知
- UEBA
  上記ログを統合監視し、不審挙動を検知

# 質問⑪

質問内容：想定している技術対策をおしえてください

| 名称 | 機能 | ガイドライン番号 |
|---|---|---|
| ウィルス対策ソフト | パソコン等へのウィルス侵入を検知・ブロック | 136 |
| メールゲートウェイ | ウィルスメールや迷惑メールなどをブロック | 139 |
| EDR | パソコンやサーバーを監視し、不審な挙動・異常を検知 | 130、138、145 |
| ファイアウォール | ネットワークの境界に設置し、外部からの攻撃や不正アクセスを防止 | 103、145 |
| IDS/IPS | 外部や内部からの不正疑いのある通信を検知 | 110、142、145 |
| UTM | ファイアウォール、IPS等の複数のセキュリティ機能を一つの機器で統合したもの | 108 |
| WAF | Webアプリケーションを守ることに特化したファイアウォール | 109 |
| Web改ざん検知 | Webサイトの不正な書き換え、改ざんを検知 | 147 |
| SIEM/SOC | セキュリティアラートを検知し、分析対応するツール/体制 | 145 |

技術対策には費用がかかるため、全てを一度に実施するのは難しいと思われます。予算と会社の状況に応じて導入いただきたくお願いいたします

# 質問⑫

質問内容：ランサムウエア対策としてのデータのオフライン保管用バックアップは、どの程度の期間保存しておくのが望ましいでしょうか。（現状は、週に一回、３カ月分保存しています。）

回答：
ランサムウェアに感染した際の対策としてデータバックアップを行ってください。
ご質問にあるように、週１回、３カ月＝12世代のバックアップを行っていれば、世代管理しているデータの中からデータを復元する時点を選択できます。バックアップの頻度が多ければ安全性は増しますが、一方手間がかかり運用の費用は大きくなります。また、データ量が多ければ保存先のデータ容量も消費してしまいます
バックアップはシステムのバックアップとデータのバックアップで分けるのが良いと思います。

✓ システムバックアップ　　：長期間
✓ データバックアップ　　：短期間

会社の状況や予算に応じてバックアップ期間や頻度を決めてください。
ガイドラインでは、頻度は1回/日、過去3世代以上を要求しています。

情報交換例）

**・各社様のバックアップ期間や頻度があればご紹介願います。**

# 質問⑬

質問内容：サイバー攻撃模擬訓練を実施する際のポイントを教えていただきたいです。

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。
- インシデントの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

情報交換例）

**・各社様のサイバー攻撃模擬訓練の事例があればご紹介願います。**

# 質問⑭

質問内容：低コスト(出来るだけ費用をかけずに)で出来る技術対策があれば教えて頂きたいです
※費用さえかけれるのであれば色々な対策ソフトを導入すれば良いと思いますので

回答：
セキュリティ対策ツールの導入には費用がかかり、運用にも工数がかかるため、様々なツール導入は容易ではないと思われます。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

【価格表】
- ネットワーク監視型：企業のネットワーク構成にあわせ、適切な場所に設置し包括的に防御する働きをする
- 端末監視型：ユーザーが利用する各端末に導入し、不審な挙動を検知し、迅速な対応につなげる働きをする
- 併用型：ネットワーク監視型と端末監視型の両方を導入

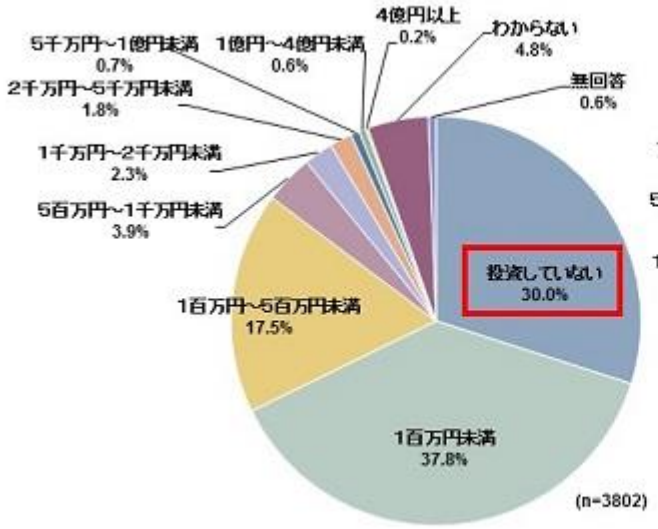
# 質問⑮

質問内容：No.31やNo.81など情報漏えい対策として自動検知する仕組みや標的型メール訓練を検討していますが、
いずれも導入コストが高いと感じており、中々承認を得られない状況です。他社様は補助金制度等を
利用してご承認およびご導入となっているのか、こちらも情報共有頂きたいです。
また、そもそもどのぐらいのコスト感を持って取り組んでいるのかも知りたいです。

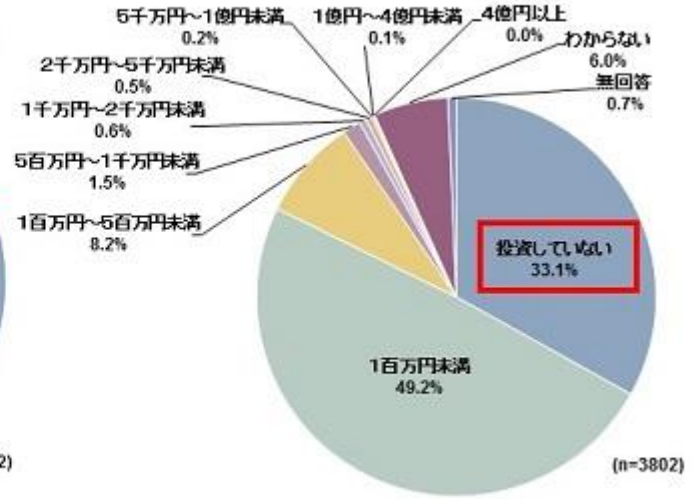
回答：
技術的な対策の仕組みを導入するには費用がかかるため、社内承認を得るのが容易でないことは多くの会社様で共通の悩みと思われます。
しかしながら、万が一情報漏えいが発生した場合、どのようなセキュリティ体制であったのかを問われることになります。対策が不十分であった場合、企業としての信頼を失ってしまいますので、経営幹部の理解を得て、予算確保をお願いいたします。

右図はIPAが2021年度に実施した中小企業における「IT投資」「情報セキュリティ投資」の調査結果です。
IT投資は100万円未満が37.8%、100～500万円未満が17.5%となっています。

【IT投資】




【情報セキュリティ投資】




参照：IPA「2021年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について
https://www.ipa.go.jp/security/reports/sme/about.html