よろず相談会第11回

2025年3月21日 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	ガイドラインNo.31「標的型メール訓練を実施している」が実施出来ていない。どの様に実施すべきか手順を教えてほしい。
2	セキュリティ教育を実施しているが、成果の判断が難しい。どの様に評価を行えばよいのか教えてほしい。
3	セキュリティ対策の人員や費用を確保するのが困難なので良い方法があれば教えてほしい。
4	弊社ではセキュリティチェックシートLv2の達成に向けてSoCサービスの導入を検討していますが、どのSoCサービスを選定するかを悩んでいます。 SoCサービス選定に向けたポイントを教えてほしい。 また、SoCサービス導入にあたり、IT補助金を取得する情報があれば教えてほしい。
5	ガイドラインNo.151「重要なデータやシステムについてバックアップの復元(リストア)テストを実施している」について教えてほしい。 新規導入時には、導入前にリストアテストを必ず実施し手順書を作成していますが、大規模なシステム変更時以外には実施できていません。ただ、最低でも年一回以上は、手順書の机上確認を行っています。上記のような対応状況の場合でも、評価＝２、と判断してもよろしいでしょうか。
6	ガイドライン【No.136】「パソコン、サーバーには、マルウェア感染を検知・通報するソフトウエア(ウイルス対策ソフト)を導入している」について教えてほしい。弊社では、外部へのネットワーク通信できる端末のみウイルスソフトを導入しておりますが、社内のみでの利用や、スタンドアロンのPCにはウイルスソフトを導入しておりません。評価としては「２」なのか「１」なのかどちらになりますでしょうか。USBメモリを使用できる環境下の為、社内アクセス可能なPCにもライセンスを追加してインストールしたい旨を相談しましたが、許可はおりていない状況です。
7	海外拠点にて情報セキュリティ対応方針(ポリシー)や規程を作る必要がありますが、どのように進めればよいでしょうか。 日本と海外拠点では規模が異なる、法律が異なる等の理由により、日本で作成した規定を翻訳すれば足りるというわけにはまいりません。また、拠点ではスタッフの数も職種も限られているため対応が難しい状況です。
8	セキュリティ関連規程を設けましたが、どのように社員教員を進めていくのか決めかねております。第一歩として始めると良いことがあれば、教えてほしい。

質疑応答

質問①-1/4

ガイドラインNº31「標的型メール訓練を実施している」が実施出来ていない。どの様に実施すべきか手順を教えてほしい。

回答：
以下に、訓練の進め方を紹介します。あくまで一例となりますが、参考にしてみてください。

１．目的を明確にする
標的型攻撃メール訓練を実施するそもそもの目的は、従業員が訓練メールの受信や開封をリアルに体験し、自分ゴトとして捉えてセキュリティ意識を高めることにあります。**従業員が悪意あるメールを識別し、適切に対処できる能力を養うことがゴールです。**
自社の状況を踏まえて、「開封させない事」を目的とするのか、「適切に報告を挙げる事」を目的とするのか、目的によって手法や結果を刈り取る為の指標が変わってきます。

２．把握すべき数値を確認する
訓練の目的が決まれば次は取得・把握すべき数値を確認します。訓練実施後に「あの数値を取得していなかったから、効果が把握できない…」ということにならないために、目的に合わせた指標、数値目標を設定します。

質問①-2/4

ガイドラインNº31「標的型メール訓練を実施している」が実施出来ていない。どの様に実施すべきか手順を教えてほしい。

３．訓練の事前準備をする

3-1.事前教育を実施する

社員のセキュリティに対する意識を高め、標的型攻撃メールに対する注意喚起を行う為に必要です。通常は講義スタイルで、標的型攻撃メールの概要、その脅威、見分け方、発見した際の対応などに関する知識を伝えます。特に発見した場合に適切に報告を挙げるルートの確立や報告方法の周知は重要となります。

3-2.訓練の対象となる部署・社員を決定する

3-3.送付する文面を決定する

はじめは、見分けポイントが判別し易い一般的に世の中で出回っている文面で実施し、訓練の回数を重ね、開封率が下がって来た事を確認したのち、文面を高度化していくと良いでしょう。

3-4.訓練用のメール(仕組み)を準備し、事前にテストを行う

実際にPCやスマートフォンなどの端末にメールが届いているかを確認します。**その際、確実に受信フォルダに届くか、迷惑メールフォルダに振り分けられていないかもチェックします。**

3-5.事前の共有先、訓練日時を決定する

訓練実施には、社内の理解と協力が重要です。係長・主任など現場のリーダー層にまで訓練の意義や必要性を周知する事で、より効果的な訓練が実施できます。又、**情報システム部門には、メール訓練が円滑に実施できるよう連携**し、特にセキュリティ対策製品により訓練メールが届かない場合もある為、送信元IPアドレスや送信メールドメイン等の情報を準備し調整しておきましょう。尚、訓練メールを一度に大量に送信すると、サイバー攻撃と判断され送信や受信が停止する場合もある為、**通数と送信完了時間も考慮しながら複数回に分けた日時を検討しましょう。**

質問①-3/4

ガイドラインNº31「標的型メール訓練を実施している」が実施出来ていない。どの様に実施すべきか手順を教えてほしい。

４．訓練をして検証をする

事前準備は以上で、次はいよいよ訓練用メールを実際に送信して、訓練実施のステップを進めます。その後、結果を分析して報告します。

4-1.訓練を実施する

訓練対象者に対し、**それが訓練用であることは明かさず、用意したメールを送信します。**

4-2.アンケートなどで成果を検証する

訓練用メールを送信した対象者にタネを明かしてアンケートをとります。アンケート内容は不審なメールだと気づいたか、どこで気づいたか、或いは、なぜ気付かなかったのか、添付ファイルの開封やURLリンクのクリックをした理由、もしくはしなかった理由などで構成されます。更に、不審なメールだと気付いた後の初動対応はどうしたかも調査します。メールに集計機能を設定していた場合はそれによる計測データも集計します。集計したデータは分析後、訓練結果レポートとしてまとめます。**課題や改善点が見付かった場合は、分かり易くポイントをまとめて従業員にしっかりとフィードバックする事も重要です。**

５．事後教育で成果につなげる

これが最も重要です。標的型攻撃メール訓練が「訓練しっぱなし」になってしまわないよう、しっかり成果につなげます。具体的には、

①対応・報告フローの再確認
②見破り方の再確認
③セキュリティ意識維持のための定期教育

を行うと良いでしょう。

質問①-4/4

ガイドラインNº31「標的型メール訓練を実施している」が実施出来ていない。どの様に実施すべきか手順を教えてほしい。

６．その他補足

以前は、「開封率」で訓練の結果を刈り取る事がトレンドとなっていましたが、最近ではより実践的な「不審メールを発見した後の行動」に焦点を当てて訓練の成果を刈り取る事が重要だとされています。**「従業員が適切な知識で訓練メールを識別し、適切な対処を取れたかどうか」が成否の指標となるよう**に、開封率自体も見ておくべきではありますが、あくまでも目安程度にとどめておきましょう。

７．最後に

・適切な報告ルートを設置する
・最低限の根回し・事前周知はしておく
・事後教育で成果につなげる

といったことに注意して、自社に適した訓練方法を検討してください。

参考資料

一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会　メール訓練手法検討サブWG作成
メール訓練手引書一般公開版 v1.0
https://www.nca.gr.jp/activity/nca-mail-exercise-swg.html

質問②

セキュリティ教育を実施しているが、成果の判断が難しい。どの様に評価を行えばよいのか教えてほしい。

回答：
セキュリティに限らず教育に対する成果の測定は難しい課題かと思いますが、いくつか評価方法の例を挙げさせてもらいます。

テストによる測定: 教育プログラムの前後で、参加者に対してテストやクイズを実施し、知識の向上を測定します。

アンケートの収集: 教育後にアンケートを用いて理解度や満足度を収集し評価します。

行動の観察: 教育後の行動変化を観察します。例えば、セキュリティポリシーの遵守状況や、フィッシングメールへの対応など、実際の業務における行動をヒアリング等によりチェックします。

事故の発生率: 教育前後でのセキュリティインシデントの発生率を比較します。教育が効果的であれば、インシデントの発生が減少することが期待されます。

シミュレーション: フィッシング攻撃等のシミュレーションを行い、参加者がどのように対応するかを評価します。実践的な演習を通じて、知識の定着度を測ることができます。

フォローアップ: 教育後、数ヶ月後に再度テストやアンケートを実施し、知識や意識の持続性を確認します。

質問③

セキュリティ対策の人員や費用を確保するのが困難なので良い方法があれば教えてほしい

回答： ガイドラインの「自動車業界として最低限実装すべき項目」を通じて1人でも出来ることを実践し、
STEP 1・・・できていること、出来ていない事を可視化しましょう。
STEP 2・・・できていないことから起きえる事象のインパクトを可視化して経営などの判断を取りましょう。

✓「自動車業界として最低限実装すべき項目」・・・ 推進担当者向け解説資料
状況把握の最優先は同書（pg3～6）にて定めております。ぜひご活用をお願いします。

リスク	インパクト	取組み優先位	経営目線影響
情報漏洩	セキュリティ対策が不十分な場合、顧客情報や企業の機密情報が漏洩するリスク、信頼の失墜や法的な問題が発生		
業務の中断	サイバー攻撃（ランサムウェアなど）やその他のセキュリティインシデントにより、業務が中断。 これにより、収益の損失や顧客へのサービス提供の遅延	自社の目線で 価値の重みづけを 検討お願いします	
経済的損失	セキュリティインシデントが発生した場合、被害の修復や法的費用、罰金、賠償金など、経済的な損失が発生。 また、ブランドイメージの損失も長期的な影響		
信頼性の低下	顧客やパートナーからの信頼喪失、特に、データ漏洩やインシデントが公表による企業の評判が悪化し顧客離れ。		
法的責任	業界や地域の法律に基づくコンプライアンス要件を満たさない場合、法的な責任を問われる。罰金や制裁が伴う可能性		
競争力の低下	セキュリティ対策が不足している企業は、競合他社に対して劣位に立つ可能性があります。顧客はセキュリティがしっかりしている企業を選ぶ傾向があるため、ビジネスチャンスを失う。		
内部統制の欠如	セキュリティ対策が不十分な場合、内部統制が欠如し、従業員による不正行為やミスが発生するリスク		

質問④

弊社ではセキュリティチェックシートLv2の達成に向けてSoCサービスの導入を検討していますが、どのSoCサービスを選定するかを悩んでいます。SoCサービス選定に向けたポイントを教えてほしい。
また、SoCサービス導入にあたり、IT補助金を取得する情報があれば教えてほしい。

回答：

■SOCサービスの選び方（※引用・・・SOC（Security Operation Center）とは？運用の基本と企業における必要性 | LAC WATCH）

SOCサービスの選び方として次の4つのポイントが挙げられます。

・運用対象が明確
・監視・連絡体制が充実
・実績がある
・サービス提供者の技術に問題がない

まずは、自社が求める運用対象と、サービス提供事業者の運用対象でミスマッチがないか確認することが重要です。そのためには、自社内でのSOCに対する要件定義がされていなければなりません。

■SOCサービス・・・ サイバーセキュリティお助け隊サービス 比較| IPA

■IT補助金・・・ トップページ ｜ IT導入補助金2025

上記サイバーセキュリティお助け隊サービスであれば
こちらのIT導入補助金の対象となります。

補助額、補助率及び補助対象経費

枠	セキュリティ対策推進枠
補助額	5万円～150万円
機能要件	独立行政法人情報処理推進機構が「サイバーセキュリティお助け隊サービスリスト」に掲載しているいずれかのサービス
補助率	1／2以内 ※小規模事業者は2／3以内
補助対象経費	サービス利用料（最大2年分）

質問⑤

ガイドラインNo.151「重要なデータやシステムについてバックアップの復元(リストア)テストを実施している」について教えてほしい。新規導入時には、導入前にリストアテストを必ず実施し手順書を作成していますが、大規模なシステム変更時以外には実施できていません。ただ、最低でも年一回以上は、手順書の机上確認を行っています。上記のような対応状況の場合でも、評価＝２、と判断してもよろしいでしょうか。

回答：
「大規模なシステム変更時以外にはリストアテストを実施できていない」「リストア手順書の机上確認しか行っていない」と云う事であれば、厳密には評価は「１」となります。

本項番No.151の目的には、「システム停止、データ消失による業務影響を極小化するとともに、早期の業務復旧を実現する」と定義されていますので、**万が一のインシデント発生時に「用意している手順書に従ってリストアを実行したが、上手くリストアが出来ない」などのトラブルが発生する可能性がある**状況では、**「対策完了(評価＝2)」とは言えません。**

リストア作業では、**手順書(机上確認)だけでは確認し切れない対応やノウハウが隠れている事が多々あります。**
新規導入時の１パターンだけでなく、**システム更新都度の実機テストや定期的な実機テスト**を重ねる事により、いざインシデントが発生した時にも慌てる事なく、落ち着いて対処出来る様になり、又、ノウハウも蓄積する事が出来ます。

ガイドライン全体を通して、評価の点数を取る事が目的ではなく、**万が一のインシデント発生に実践的に備える事が目的**となりますので、各項番の目的・狙いを踏まえた「実践的な準備・対応」が出来るように進めて頂けると良いと思います。

質問⑥

ガイドライン【No.136】「パソコン、サーバーには、マルウェア感染を検知・通報するソフトウエア(ウイルス対策ソフト)を導入している」について教えてほしい。弊社では、外部へのネットワーク通信できる端末のみウイルスソフトを導入しておりますが、社内のみでの利用や、スタンドアロンのPCにはウイルスソフトを導入しておりません。評価としては「２」なのか「１」なのかどちらになりますでしょうか。USBメモリを使用できる環境下の為、社内アクセス可能なPCにもライセンスを追加してインストールしたい旨を相談しましたが、許可はおりていない状況です。

回答：
ウイルス感染経路を考えますと、外部へのネットワーク通信を通じてというのは一つの感染経路ではありますが、それ以外にも、様々なケースが考えられます。
感染経路の例）

- 内部ネットワークを介しての感染リスク：　感染したデバイスがネットワーク内で他のデバイスに感染を広げる等。
- 外付けデバイスのリスク:　USBメモリや外部ストレージデバイスを使用することで、インターネットに接続していないPCやサーバー　にマルウェアが持ち込まれる可能性があります。
- ドキュメントファイル等からの感染リスク：　社内共有したドキュメントファイル等を通じてウイルスに感染するなど。

過去の事例等からも、社内ネットワークを通じた横感染ややUSB等の使用によりウイルス感染するというのは必ず考慮する必要のあるリスクです。従いまして、外部との通信ができる端末に絞った対策というのは「１」と考えていただき、その他の端末の対策も検討いただくのが良いかと思います。
もちろんスタンドアロンでUSB等の使用が全くない・物理的に制限している等でリスクは十分に低いとの判断、あるいは別の対策をしている等の理由でウイルス対策ソフトを導入しないという選択があっても全く問題はありません。

質問⑦

海外拠点にて情報セキュリティ対応方針(ポリシー)や規程を作る必要がありますが、どのように進めればよいでしょうか。
日本と海外拠点では規模が異なる、法律が異なる等の理由により、日本で作成した規定を翻訳すれば足りるというわけにはまいりません。また、拠点ではスタッフの数も職種も限られているため対応が難しい状況です。

回答：　国にもよりますが、現地法律事務所、情報セキュリティ特化コンサル、業界団体などに相談して進めて頂く事が情報セキュリティポリシー策定に必要な相談先となります。

但し、上記に伴う莫大な費用使わず自社内で完結する方法もあり下記のステップをご参照ください。

ステップ1 現状の把握

- ✓ 現在の日本の情報セキュリティポリシーを確認し、海外拠点に適用できるかを評価する
- ✓ 海外拠点の業務内容、従業員スキル、既存のセキュリティ対策や業務プロセスを理解する
- ✓ 想定されるリスクの洗い出しを行う

➡ 情報セキュリティ対応方針の最小限を可視化し、出来ること出来ないことを見極める事。出来ることは計画に織り込み、出来ないことは出来るように計画（プロセスの見直し、人員確保、システム導入など）を策定する事。

ステップ2 ステークホルダーとの協議

- ✓ 現地チームとの対話：海外拠点のスタッフと話し合い、実務に即したセキュリティ要件や懸念点を把握する。
- ✓ 経営層との合意形成：経営層と協議し、ポリシーの方向性や必要なリソースについて合意を得ること。

➡ 経営の理解を得るためには投資ありきではなく、リスクの可視化とリスクのインパクトを示すこと。

質問⑦

ステップ3　トレーニングと周知

✓ トレーニングの実施：新たなポリシーや規程に対する定期的な教育・トレーニングを行い、スタッフの理解を深める。（集合研修やeラーニングなど）
✓ 周知徹底：ポリシーを文書化し、スタッフに配布することで周知。

➡ 教育・トレーニングを体系化し、コーポレート目標としてデフォルト化し、中長期的な理解の深化を目指す。

ステップ4 定期的な見直し

✓ 定期的なレビュー：ポリシーの実施状況や効果を定期的に評価し、必要に応じて更新

情報セキュリティ海外展開でよく聞こえてくる困りごと

✓ コミュニケーションルートや窓口が無い、もしくはあるが普段から会話していない、英語ができないなど
✓ セキュリティ推進　＜ 利便性が優先される

まずは簡単な情報交換（会話やガイドライン共有など）を行いニーズの違いを感じ取ってみではいかがでしょうか。
ガイドラインはグローバルスタンダードで展開しておりますが、必ずしも全ての会社に適用する必要はありません。

➡ 海外拠点のニーズに沿ったセキュリティーポリシー策定に向けた支援を行うスタンスで進める事をお勧めします。
これを経て上述のSTEP1からPDCAを回しながら推進して頂ければと存じます。

質問⑧

セキュリティ関連規程を設けましたが、どのように社員教育を進めていくのか決めかねております。第一歩として始めると良いことがあれば、教えてほしい。

回答：
まずは、規程の周知を実施するのがよいと考えます。
規程の周知の手段としては、以下の例を挙げます。
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

平行して社員教育を実施する。社員教育においては、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) ）

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