CONFIDENTIAL

よろず相談会 第10回

2025年2月26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。

Copyright© Japan Automobile Manufacturers Association, Inc.

本日取り上げさせて頂くご質問一覧

No.	質問
1	[No.42] サプライヤ各社様から受領したチェックシートの状況把握や点検まではメンバースキルや工数不足から実施できていません。そのような場合はどのように対応すればよいのか教えてください
2	[NO.55] 機密区分はルール化しているが、情報資産台帳まで作成できていない。全社対象だと範囲が大きすぎて全てを把握する事が困難であるが、どのような資料なのか、どのように取り扱うのか、どこに保管するのか、など具体的な方法を教えてください
3	[No.85/86] 執務室内に作業エリアとサーバー設置場所があるため、入場制限が難しく部屋単位での施錠対策が困難、サーバーラック設置も物理的な理由から困難な状況です。工数や費用を抑えて対策できる具体的な方法を教えてください
4	[No.150] システム利用不可能時の実施可能な代替手段の整備について、マニュアルで生産できる手順・体制は、どこまでの取組みを想定しているものであるか、具体的な事例を教えてください
5	セキュリティ組織体制の構築は、どのように進めたらよいか教えてください
6	脱PPAPにあたり、メールゲートウェイ上でウイルススキャンをしている場合、添付ファイルのリンク化をする必要があるのか教えてください

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。

Copyright© Japan Automobile Manufacturers Association, Inc.

回答者紹介

①自工会/部工会メンバーご挨拶
②IPAセキュリティプレゼンター/佐藤 裕一 様 ご紹介

佐藤　裕一

【経歴】

- 1981年 青山学院大学　経営学部経営学科
- 1981年 株式会社サンリオ
- 1986年 社団法人日本能率協会
- 2002年 リコーテクノシステムズ株式会社、リコー情報セキュリティ研究センター、株式会社リコー、リコーITソリューション株式　　会社
- 2011年 株式会社通信総研　代表取締役
- 2016年 独立行政法人情報処理推進機構（IPA）セキュリティセンター非常勤研究員（出向）

【主な実績】

- ＯＡ機器メーカーISMS統一認証取得支援
- システム開発販売会社　ISMS認証取得支援
- 国税庁事務管理センター及びバックアップセンター情報セキュリティ監査
- 国税庁事務管理センター及びバックアップセンターISMS認証取得支援
- 国税庁支所情報セキュリティ研修講師
- ISMS審査員研修コース講師（審査員資格取得JRCA承認研修）
- 防衛省ISMS審査員養成研修講師
- 総務省システム運用部署情報セキュリティ監査
- 自治体情報セキュリティ監査
- 情報セキュリティ関連公開セミナー講師
- Pマーク社内規程作成ツール開発
- 印刷会社Pマーク認定取得支援
- 放送業　J-SOX対応IT統制整備
- 自治体情報セキュリティポリシー策定
- 自治体マイナンバー監査
- 自治体マイナンバー保護評価
- 情報処理推進機構(IPA)研究員
  中小企業の情報セキュリティ対策ガイドライン作成、セミナー講師、
  SECURITY ACTION制度運用、セキュリティプレゼンター制度運用

【保有資格】

情報処理安全確保支援士（登録セキスペ）、システム監査技術者、情報セキュリティマネジメント試験、 ITコーディネータ、公認情報システム監査人(CISA)、ISMS審査員、

質疑応答

質問①

[No.42] サプライヤ各社様から受領したチェックシートの状況把握や点検まではメンバースキルや工数不足から実施できていません。そのような場合はどのように対応すればよいのか教えてください

➡ **まずはレベル1に相当する50問から状況把握、フィードバック、点検まで結び付けましょう。**

✓ セキュリティ推進担当者向け解説資料　・・・　推進担当者向け解説資料
状況把握の最優先は同書にて定めております。ぜひご活用をお願いします。

✓ 受領したチェックシートは**必ず提出元へフィードバック**をお願いします。その内容は推進担当者向け解説資料で定めた優先取り組み内容を活用頂いても問題ありません。

✓ スキルについて・・・ガイドラインに則った解説書を用意しており、これが答案用紙に相当しておりスキルを補います。
・・・ 自工会/部公開・サイバーセキュリティガイドラインV2.2 解説書

✓ 点検活動について・・・受領したチェックシート、状況把握の優先項目、解説書の3点を活用して推進をお願いします。
点検方法は証跡を元にオンラインでも、現地確認でも問題ありません。

Copyright© Japan Automobile Manufacturers Association, Inc.

質問②

[NO.55] 機密区分はルール化しているが、情報資産台帳まで作成できていない。全社対象だと範囲が大きすぎて全てを把握する事が困難であるが、どのような資料なのか、どのように取り扱うのか、どこに保管するのか、など具体的な方法を教えてください

1）機密区分を定義する ⇒ 2）高い機密区分の情報を抽出する ⇒ 3）情報資産 管理台帳に記入する

➡ **社内各部署への機密区分の教育や共有などを通じて台帳への記載をお勧めします。**
機密区分を定義するまでをセンター部署の役割とし、情報資産がどの機密区分に該当するのか、判断ができる部署に一任しましょう。

表１． 達成条件No.54 機密区分の例

機密区分例	定義例（外部に漏洩した場合、会社の信頼や収益に）	取扱い方法例	台帳記載
極秘	極めて秘匿性の高い情報（著しい影響を及ぼす可能性がある）	コピー、移動等 禁止	要
秘 （マル秘）	厳格に選定された関係者のみに共有すべき秘匿性の高い情報 （影響を及ぼす可能性が高い）	コピー、移動は一定条件でのみ可。 保存時には暗号化	
関係者外秘 （社外秘）	関係者間で業務に利活用する情報 （影響を及ぼす可能性がある）	持ち出し時手続き要。保存時のアクセス制御、会社指定保管先のみ可	不要
（公開）	機密に当たらない情報（影響を及ぼさない）	ー	

Copyright© Japan Automobile Manufacturers Association, Inc.

質問②

１）機密区分を定義する ⇒ ２）高い機密区分の情報を抽出する ⇒ ３）情報資産 管理台帳に記入する

➡ **機密区分より情報資産の重要性を見極め、情報漏洩した場合のリスク値を具体的に想定しましょう。**

リスク値（例）

【極秘】
・国家機密：軍事作戦計画、国家安全保障に関する情報
・企業の最重要情報：大規模なM&A計画、長期的な経営戦略、特許出願
・研究開発データ：画期的な技術や製品の開発に関する情報、
・顧客の個人情報：特にセンシティブな情報（健康情報、金融情報など）

→ 操業停止、業績悪化、Yahooニュース、ブランド失墜、社長に叱られる、懲戒など

【秘】
・経営情報：経営会議の議事録、業績予測、予算案
・人事情報：従業員の給与情報、評価データ、雇用契約
・契約書：重要な取引先との契約内容、守秘義務契約
・顧客リスト：特定の顧客情報や取引履歴

→ 競争力損失、信頼関係悪化、法的責任、評判悪影響など

【関係者外秘】
・プロジェクト情報：パートナー企業との共同プロジェクトに関する情報
・サプライヤー情報：特定のサプライヤーとの契約内容や条件
・社外向け資料：社外向けのプレゼンテーション資料（特定の関係者にのみ配布）
・市場調査データ：競争相手の分析結果や市場動向に関する内部データ

→ 取引先やパートナーとの関係性悪化、契約違反など

Copyright© Japan Automobile Manufacturers Association, Inc.

質問②

１）機密区分を定義する ⇒ ２）高い機密区分の情報を抽出する ⇒ **３）情報資産 管理台帳に記入する**

表２．達成条件No.56 情報資産(情報)一覧化の例

No.	対象情報	個人情報有無	管理者	部署	保管場所	保管期限	開示先（メールアドレス）	棚卸日	備考
1									
2									
3									
4									

極秘情報の例：人事情報、給与情報、企業競争力に直結する情報、etc.
個人情報は含まれているか、極秘情報の管理者、保管場所、保管期限、管理者連絡先、定期的な棚卸を実施してください。

付録7：リスク分析シート（全7シート）(Excel:98 KB)　情報資産管理台帳Sheetが参考になります。
「リスク分析シート」は、自社の情報資産に想定されるリスクを特定し、対策を検討するために利用します。

Copyright© Japan Automobile Manufacturers Association, Inc.

質問②

（ご参考）機密情報の保管方法について

➡ 情報や資産の形態に応じて適切な保管方法を選択しましょう。

物理的な保管方法

施錠されたキャビネット
（紙媒体、USBなど）

セキュリティルーム

デジタルな保管方法

暗号化

クラウドストレージ

Copyright© Japan Automobile Manufacturers Association, Inc.

質問③

[No.85/86]　執務室内に作業エリアとサーバー設置場所があるため、入場制限が難しく部屋単位での施錠対策が困難、サーバーラック設置も物理的な理由から困難な状況です。工数や費用を抑えて対策できる具体的な方法を教えてください

人の作業エリアに対する要件とサーバー設置エリアに対する要件は全く異なる為、結論から申し上げると、同一エリア内への設置を前提とした対策は推奨出来ません。端的に云うと、**作業エリアに対しては、人が快適に効率的に業務を行えることを狙いにした環境整備が必要**となります。一方で、サーバー設置エリアには、セキュリティの確保と運用のし易さを念頭に、サーバー管理以外の業務ができないよう、必要のないものは極力置かないように意識する事と、特に**一番重要な要素は「空調」です。**サーバーは常に稼働し続けるため、熱がこもってしまったり、高熱状態が続いてしまったりすることでマシントラブルの原因となってしまうのです。そのようなトラブルを防ぐために、24時間365日にわたって適切な温度や湿度管理をしなければなりません。具体的には、**室温は人が快適に過ごせる温度よりもかなり低く設定する必要があり、かつサーバーの発熱部分には直接冷却するなどの工夫が必要です。また、サーバーの熱がこもらないように設置場所も気を配らなければなりません。**

限られたオフィススペースにサーバールームを設けることに消極的なオフィスや事務所は少なくありませんが、セキュリティ面や運用面の観点からも、サーバールームはなくてはならない設備だと言えるでしょう。スペースが限られたオフィスでも、適切にオフィスのゾーニングを行うことでサーバールームの設置が可能となります。**オフィスの広さに関係なく、オフィスレイアウトを考える際はゾーニングの計画が重要です。社員の動線はもちろん、使い勝手やセキュリティ性など、様々な観点からオフィスにとって最適なゾーニングを検討してください。ゾーニングの詳細や費用については、**それぞれのオフィスの状況によって異なる為、**自社の状況を踏まえてベンダーに相談する事をお勧めします。**

Copyright© Japan Automobile Manufacturers Association, Inc.

質問④

[No.150]　システム利用不可能時の実施可能な代替手段の整備について、マニュアルで生産できる手順・体制は、どこまでの取組みを想定しているものであるか、具体的な事例を教えてください

システム利用不可能時の代替手段の目的は、「ビジネスを止めない事」です。
特に、取引先ビスネスへの影響を出さない事が、最重要事項となります。

この「ビジネスを止めない事」を念頭に、システムがなくとも取引が出来る手順の整備と、その手順を実行するための体制を想定してください。代替手法は、当該システムから物理的または論理的に分離された手法を選定することが望ましく、システムの停止時に備え、下記のような検討が求められます。

- 人手による業務継続方法の検討　（例：発注システム停止時に、電話や FAX で注文を受ける）
- システム継続手法の検討　（例：メインシステム停止時に、バックアップシステムに切り替える）
- コミュニケーションに関わる代替手法の検討　（例：予め複数の通話手段を確保しておく

関連ページ：　自工会/部工会・サイバーセキュリティガイドラインV2.2解説書（日本語版）　(127ページ)

本件に関する実例は沢山ありますが、いずれも企業のビジネスに関わる話となる為、実際にシステム停止を経験した企業の皆様から事例としてご紹介頂けますと幸いです。

Copyright© Japan Automobile Manufacturers Association, Inc.

質問⑤

セキュリティ組織体制の構築は、どのように進めたらよいか教えてください

回答：
セキュリティの体制を整備にあたっては、IT部門のような特定の部門に特化せず、全社横断的な体制を組むことが重要です。全社横断的な体制を構築し役割を明確にすることにより、それぞれの部門が主管する範囲が明確になり、規定やルールの整備やセキュリティの実務を行っていけるようになるかと思います。

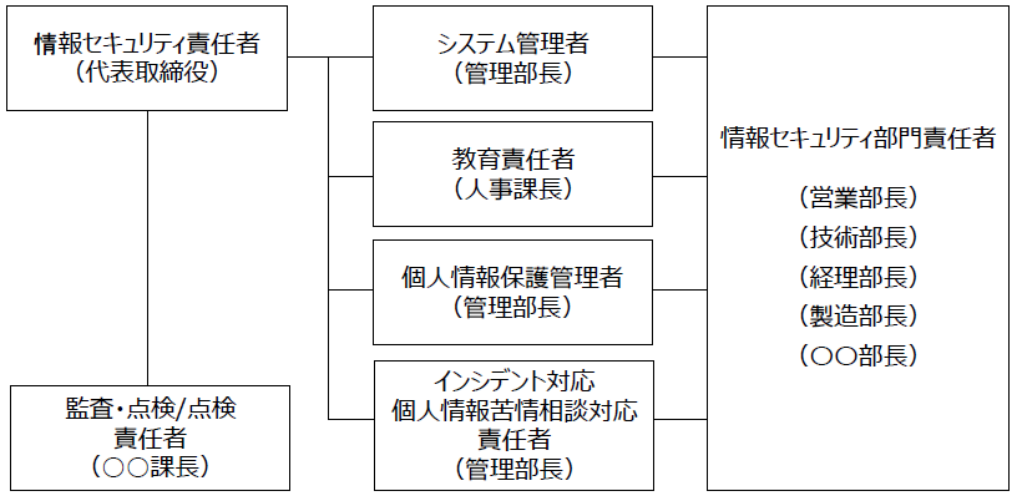
組織の規模によっては、情報セキュリティ委員会の設置を検討すると良いと考えます。委員会として活動計画を立て、定期的に開催する委員会の中でその進捗をレビューし改善を図っていくことで、セキュリティを全社的に浸透させることにもつながります。

【表６】情報セキュリティ管理のための役割と責任分担（例）

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行います。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	情報セキュリティ対策が適切に実施されているか点検します。

【参考】IPA 中小企業の情報セキュリティ対策ガイドライン
本編：第二部４　（１）管理体制の構築（P24）より

<情報セキュリティ委員会体制図>



付録5：情報セキュリティ関連規程（サンプル）（P1）より

Copyright© Japan Automobile Manufacturers Association, Inc.

質問⑥

脱PPAPにあたり、メールゲートウェイ上でウイルススキャンをしている場合、添付ファイルのリンク化をする必要があるのか教えてください

回答：

PPAPは、ファイルをパスワード付きZIPファイルで圧縮しメール添付で共有する方法ですが、パスワードを同一経路で共有する場合はセキュリティ施策として適さないです。むしろ、ZIPファイルで共有するため、メール送受信時にウィルススキャンを行っていたとしてもファイルの中身を確認することができないため、セキュアでなくなります。このため、PPAPをやめる企業が増えています。

おススメの代替策は、会社で許可されている外部共有用クラウドストレージを活用し、ファイル自体はクラウドストレージ上に格納して、そのファイルへの共有リンクを作成し、そのリンクのみメールで送付する方法です。この場合、メールゲートウェイ上のウィルススキャンは実施できませんが、クラウドストレージ側でも同等のウィルススキャン機能を提供しているものが多いため、その場合のリスクはほぼ変わりません。むしろ、ファイルに対してアクセス権限を付与して共有することになるため、もしメール誤送信が発生しても、後からアクセス権限を変更することもできるため、よりセキュアな手法だと考えます。

以上から、安全なクラウドストレージが用意できない等の事情がある場合を除き、添付ファイルのリンク化が推奨されます。ただ、ご質問にある「添付ファイルのリンク化が脱PPAPに必要か」に対しては、必ずしも必要ではないと考えます。どういう攻撃や人為ミスによる情報漏洩を想定するか次第ですが、**ファイルをZIP化しないでそのままメール添付するほうが、PPAPより安全なことが多い**です。

【ご参考】IPAサイトに掲載されている過去セミナー「脱PPAPの歩き方」の資料

Copyright© Japan Automobile Manufacturers Association, Inc.

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