よろず相談会第５回

-技術対策について（ウイルス対策やセキュリティ監視、ランサム対策）-

2023年12月15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致します。
	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、 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、 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。 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（1/2）

No.	質問
1	エンドポイントの管理・監視体制を構築するためのアドバイスいただきたいです。また費用をかけずにできるかを知りたいです。
2	No133　メール監視について、社員に周知することを経営層と協議しましたが、社有メールを監視することは法律的は問題無いが、一部の社員からプライバシー侵害として苦情がでるリスクから周知を見送った経緯があります。 一般的に周知は行っているのでしょうか。
3	No143 の各項目のログ取得方法をどのようにすればよいかが分からないのでご教示頂きたいです。 保管方法についても、推奨されている方法がありましたら、合わせてご教示頂きたいです。
4	No145について、IDS/IPS, SOC について必ず導入しないといけないのでしょうか。
5	社内システムの都合で保守期限切れのOSの入替を速やかに適用できない場合、外部(Web)とは物理的に遮断した環境に移動し運用することは問題無いでしょうか。 ※使用者限定(ID/Pass)、物理媒体禁止(USBメモリ等)の管理等は実施。
6	VPN機能についてインターネットでウェブサイトを閲覧する際にも有効な手段となりえるのか分からず、ご教授いただきたくお願い致します。
7	標的型攻撃メール訓練についてどのように実施したら良いかアドバイスを頂きたい。

本日取り上げさせて頂くご質問一覧（2/2）

No.	質問
8	膨大な脆弱性情報に対する対応、運用についてどの様に進めていくのかアドバイスいただけるとありがたいです。
9	ランサムウェア・ウィルス等の対策を行う上で、一般ユーザーに向けた教育をどのようにしていけば良いのでしょうか。
10	ランサム対策でデータバックアップの保存先についてどのような方法があるのか教えていただきたい。
11	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。
12	No150について、システムがないと操業が難しい業務は、どのような対策案が考えられるか、ご教示頂きたいです。
13	使えるお金も人員も限られている中、どこからどのように手を付けたらよいのかわからないので、アドバイスいただきたい。
14	経営層の理解が得られ、必要な投資が行えるようにできるコツのようなものがございましたらご教授いただけますとありがたいです。
15	No131 メール送信による情報漏えいを防止するための対策について、いわゆるPPAPやそれを実現するシステムはセキュリティ上の問題があると聞きます。どういった対策を適用すれば良いでしょうか？

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。
時間に余裕があれば、ここに記載していない質問も用意しておりますので、引き続き取り上げさせて頂きます。
ご理解の程よろしくお願い致します。

質疑応答

質問①

エンドポイントの管理・監視体制を構築するためのアドバイスいただきたいです。また費用をかけずにできるかを知りたいです。

回答：
エンドポイントの監視体制としては①**２４ｈ３６５日の監視②インシデント発生時に対応する担当者を決めておくこと**の2点が必要です。自社で①の２４ｈ３６５日の監視を実施するのは困難なので、外部サービスの利用が一般的です。
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。また国のIT導入補助金の支援対象となる場合がありますので、併せてご確認ください
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
セキュリティ対策推進枠 ｜ IT導入補助金2023（後期事務局） (smrj.go.jp)
【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

情報交換例）　**・管理、監視体制の事例について可能な範囲でご紹介願います。**

質問②

No133　メール監視について、社員に周知することを経営層と協議しましたが、社有メールを監視することは法律的は問題無いが、一部の社員からプライバシー侵害として苦情がでるリスクから周知を見送った経緯があります。
一般的に周知は行っているのでしょうか。

回答：
No.133は内部不正に対するメール監視に関する設問です。
社員からのプライバシー侵害として苦情がでるリスクを避けるために、IPA「組織における内部不正防止ガイドライン日本語版第5版」のP75～77（21）従業員モニタリングの目的等の就業規則での周知　が参考になります。

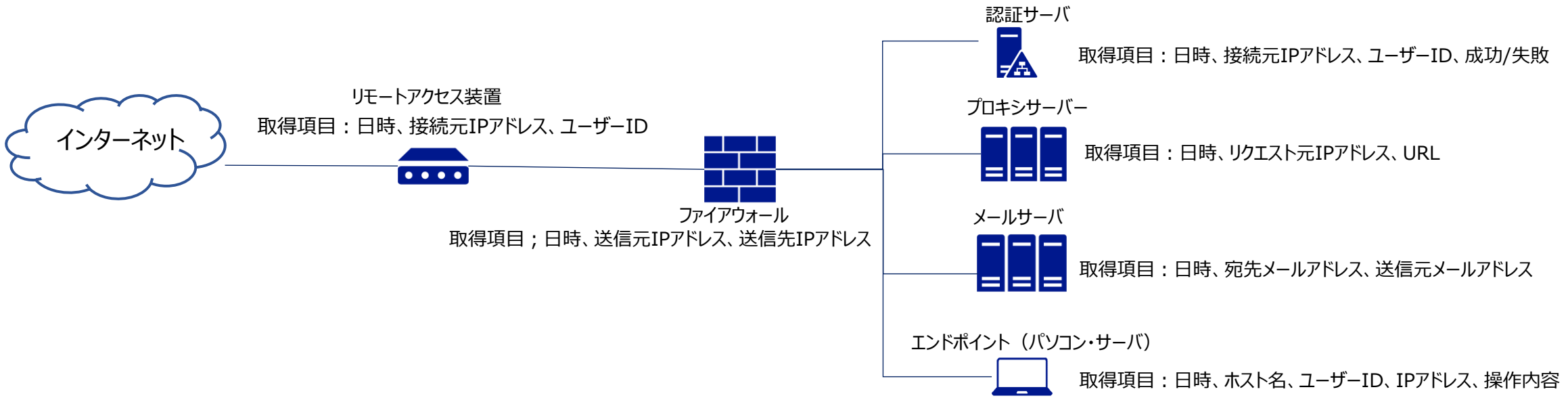
組織における内部不正防止ガイドライン | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

情報交換例）　**・各社様にて実践例がございましたら、ご紹介願います。**

質問③

No143 の各項目のログ取得方法をどのようにすればよいかが分からないのでご教示頂きたいです。
保管方法についても、推奨されている方法がありましたら、合わせてご教示頂きたいです。

回答：
事件・事故が発生した場合、侵入経路や漏えい経路（原因や影響）の調査を行うために、ログの取得が求められています。
下図の構成を例にご説明しすると、該当機器を利用していれば、**該当期間のログを出力する設定を有効にするとともに、**
そのログを以下の**リスクで該当機器が被災したとしても、ログを同時に失わないように保管しておくこと**が求められています。
想定リスクと対応例：機器故障・ランサム感染、紛失・盗難　→　**テープにログを出力し保存、金庫にそのテープを保管**など



質問④

No145について、IDS/IPS, SOC について必ず導入しないといけないのでしょうか。

回答：
No.145の達成条件は【ログを分析し、サイバー攻撃を検知する仕組みを導入している】となっています。
外部からの侵入を検知し、**サイバー攻撃を素早く検知・防止する**ことが必要です。
そのための手段として下記があります。
・IDS/IPS等を用いて侵入検知システムを構築する。
・SOCを設置して侵入の兆候が無いか監視・分析する。

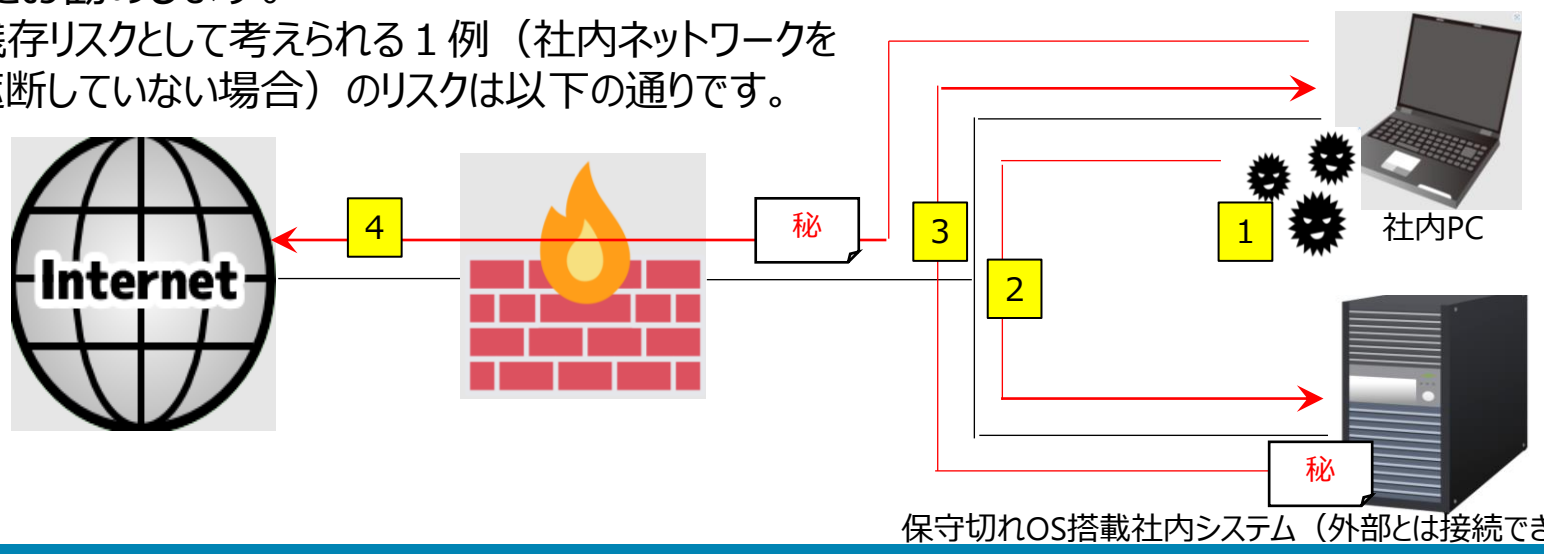
自社で検知・監視する体制を構築するのが困難な場合はIPA サイバーセキュリティお助け隊サービスの中にネットワーク監視型のサービスもありますので、合わせてご検討頂ければと思います。
サイバーセキュリティお助け隊サービス ユーザー向けサイト | IPA
ネットワーク監視型：企業のネットワーク構成にあわせ、適切な場所に設置し包括的に防御する働きをする

質問⑤

社内システムの都合で保守期限切れのOSの入替を速やかに適用できない場合、外部(Web)とは物理的に遮断した環境に移動し運用することは問題無いでしょうか。
※使用者限定(ID/Pass)、物理媒体禁止(USBメモリ等)の管理等は実施。

回答：
自動車産業ガイドラインNº123の達成基準が参考になり、「やむを得ずサポート切れのOS、ソフトウェアを利用する場合は、できる限り脆弱性悪用のリスクを低減すること」とあります。
外部ネットワーク（Web）と物理的に遮断（社外との通信ができない状態）であれば、外部からのマルウェアの混入や外部への情報漏洩リスクは低減されるかと思われますが、リスクは残存するため、OS更新計画を立案の上、計画的なOS更新を進めて下さい。また、OS更新が出来るまでの間は外部ネットワークとの遮断に加え、社内ネットワーク、外部記憶媒体からも遮断することをお勧めします。

■残存リスクとして考えられる１例（社内ネットワークを遮断していない場合）のリスクは以下の通りです。



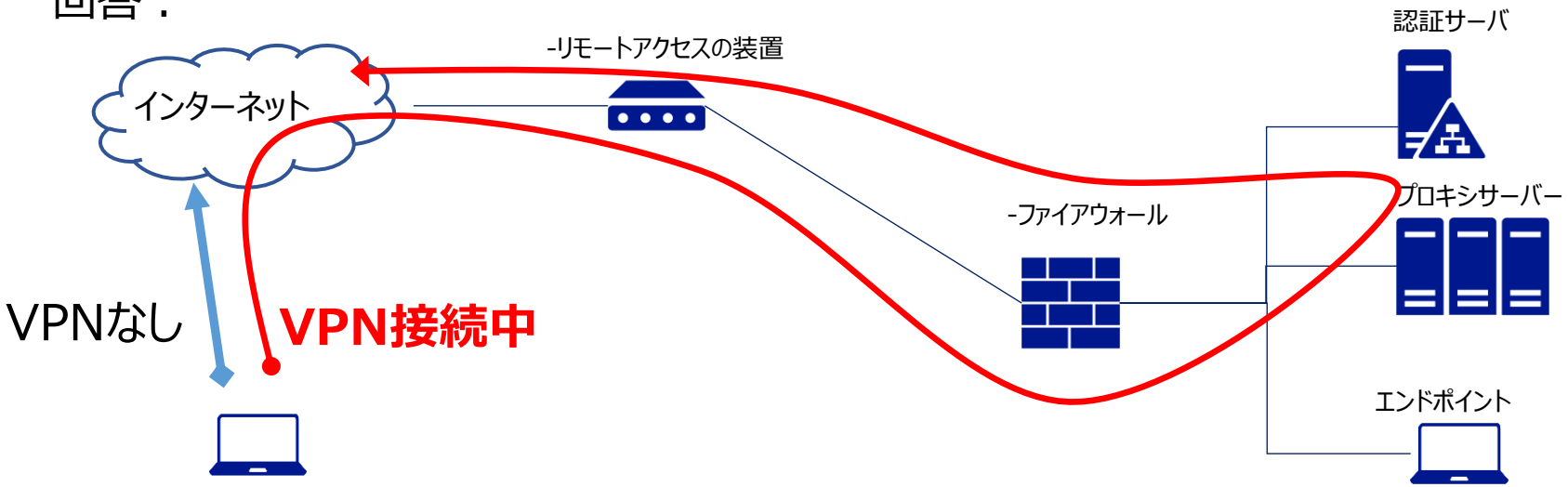
1 社内PCがマルウェア感染
2 社内PCからサーバへ侵入
3 保守切れOS搭載の社内システムの脆弱性から情報搾取
4 社外へ情報流出

保守切れOS搭載の社内システムを社内ネットワークから切り離す方が賢明

質問⑥

VPN機能についてインターネットでウェブサイトを閲覧する際にも有効な手段となりえるのか分からず、ご教授いただきたくお願い致します。

回答：



VPN接続中は社内と同様のセキュリティ対策が適用できるため、通信の暗号化、認証、アクセス制御が可能となります。
社外でもインターネットを安全に利用することにつながります。それ以外にも働く場所を問わずに、社内ネットワーク・サーバにアクセスできるので、**リモートワークを安全に実現することができます。**（端末やリモートアクセス装置のセキュリティ対策は必須）

質問⑦

標的型攻撃メール訓練についてどのように実施したら良いかアドバイスを頂きたい。

回答：
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することが重要です。
開封率を下げたり、受信時の報告が適切に行われたりすることを確認することなどがあります。
実施方法としてはセキュリティ企業が提供している“標的型攻撃メール訓練”サービスを利用したり、自前でシステム管理部門等が中心となって同様の訓練を実施したりする方法があります。
また訓練メールを送付して開封状況・対応状況を確認するたけではなく、実施後に教育も合わせて実施することでより効果的な訓練にすることが出来ると思います。
教育サンプル：そのメール本当に信用してもいいんですか？　-標的型サイバー攻撃メールの手口と対策-（IPA)

参考サイト
・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」

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⑧

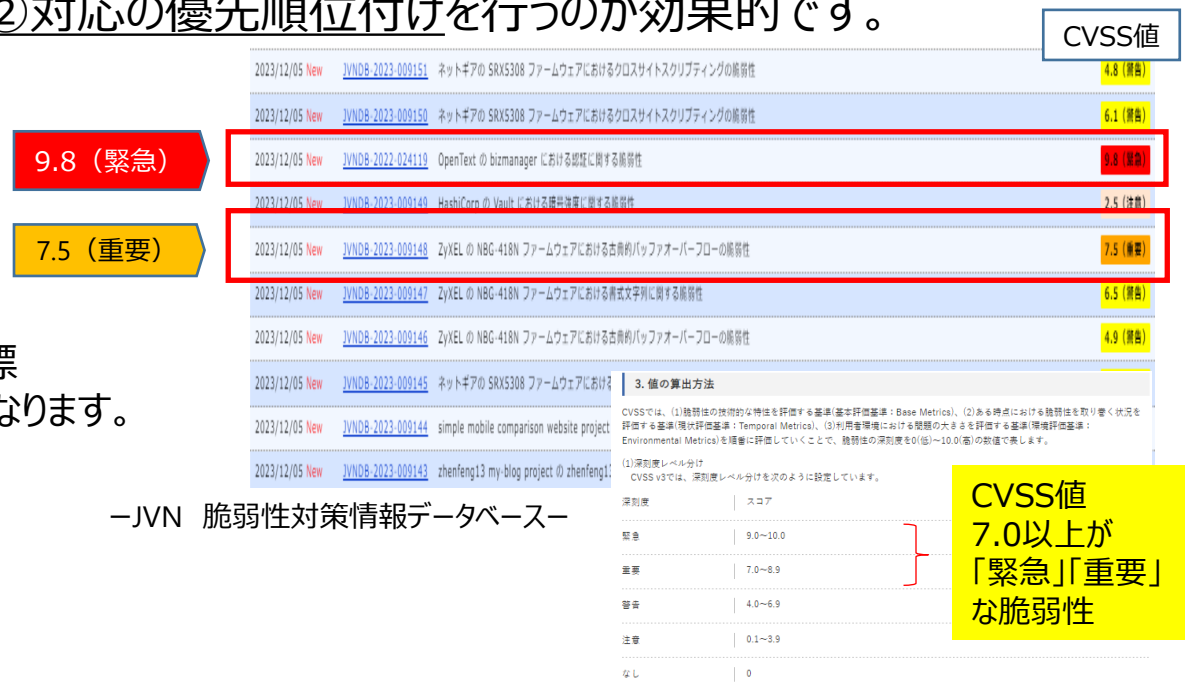
膨大な脆弱性情報に対する対応、運用についてどの様に進めていくのかアドバイスいただけるとありがたいです。

回答：
脆弱性対策を進める上で、脆弱性の優先順位付けが必要になります。
その上で、参考になるのが、自動車産業ガイドラインNº124の他社事例のセキュリティパッチアップデートの適用基準例、および適用期間例です。対応すべき脆弱性情報の①絞り込み、②対応の優先順位付けを行うのが効果的です。

①脆弱性情報の絞り込む

【セキュリティパッチ・アップデート適用基準例】
- Microsoft「緊急」レベル
- **IPA、JPCERTの「緊急」および「重要」レベル**
  - **➡ ここを解説（CVSS値7.0以上のこと）**

JVN脆弱性管理サイト： JVN iPedia - 脆弱性対策情報データベース
CVSS値：脆弱性の深刻度を同一の基準の下で定量的に比較できる指標
IPAのサイトで公開されている、CVSS値の「３.値の算出方法」が参考になります。
共通脆弱性評価システムCVSS v3概説 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構



－JVN　脆弱性対策情報データベース－
－IPA　共通脆弱性評価システムCVSSV3解説－ ３．値の算出方法

②脆弱性対策の優先順位を付ける

【セキュリティパッチ・アップデート適用期限例】
- 公開後１ヶ月以内に適用している
- 「緊急」レベルは２週間以内、「重要」レベルは１ヶ月以内に適用している
- 期限内に適用できなかったセキュリティパッチは管理表作成のうえ、記録している

質問⑨

ランサムウェア・ウィルス等の対策を行う上で、一般ユーザーに向けた教育をどのようにしていけば良いのでしょうか。

回答：
有効活用できるコンテンツとして、**「IPAのランサムウェア対策特設ページ」**があります。ランサムウェアの感染事例や、感染した場合の対処方法などがまとめられており、感染防止や被害低減のために役立つ情報が公開されています。また、同ページには、教育のための映像コンテンツが用意されており、ランサムウェアに対して、経営者・管理者・システム担当者、従業員、それぞれが行うべき対策の解説がなされています。
ランサムウェア対策特設ページ | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

このコンテンツを活用の上、以下チェックシートNoごとの活動を推進する中で、教育を進めていただければ良いと思います。
- No26：自社の中で、マルウェア感染時の対応手順を定めること
- No28：電子メールのマルウェア感染に関する社内への教育を行うこと
- No29：インターネットへの接続に関する社内への教育を行うこと
- No31：標的型メール訓練を実施すること
- No34：全社で啓発活動を実施すること
- No38：情報セキュリティ事件・事故発生時の対応について、教育・訓練を実施すること
- No40：教育・訓練の内容を必要に応じて見直すこと

質問⑩

ランサム対策でデータバックアップの保存先についてどのような方法があるのか教えていただきたい。

回答：
ランサムウエア対策としてバックアップを取得し、万一感染した時に戻せるようにすることは重要です。ランサムウエアは感染端末に接続する全ての機器に影響を及ぼす可能性があるため、下記を考慮する必要があります。
・バックアップ媒体、環境へは必要な時だけ接続する
・バックアップは複数用意する。
・バックアップから戻せるか定期的に確認する。

バックアップ保存先としては外部記憶媒体、クラウドバックアップシステム等の社内端末・ネットワークとは別の環境に保存することで、感染時にバックアップも被害を受けないようにすることが重要です。

参考事例
ランサムウェアの脅威と対策（IPA） 3.4. バックアップにおける留意事項

情報交換例）**その他に良いサンプルをご存じの会社様がおられましたらご紹介願います。**

質問⑪

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。

参考教材：IPAから提供されている３種類の訓練ツールを活用すると良いかと考えます。

ツール名	テーマ	リンク先
ABCSIRT	社内で発生したインシデントに限られた工数で立ち向かうCSIRTの１週間	ABCSIRT 30分で学ぶはじめてのインシデント対応 | デジタル人材の育成 | IPA 独立行政法人 情報処理推進機構
マルウェアスイーパー	国内拠点に次々と広がるマルウェアCSIRTが協力して、感染を封じ込めるか	マルウェアスイーパー ～協力と決断力でパンデミックを阻止せよ～ | デジタル人材の育成 | IPA 独立行政法人 情報処理推進機構
GAME OF CSIRT	自社を標的にしたサイバー攻撃から自社を守り、株価下落を防ごう	GAME OF CSIRT ～防ぐ、でもやられる、ならば対処する～ | デジタル人材の育成 | IPA 独立行政法人 情報処理推進機構

情報交換例）　**・各社様にて実施例がございましたら、ご紹介願います。**

質問⑫

No150について、システムがないと操業が難しい業務は、どのような対策案が考えられるか、ご教示頂きたいです。

回答：中核システム（会社の存続に関わる最も重要性（または緊急性）の高い設備やシステムの代替確保方針は各社次第ですが、一般的に製造業の場合、以下のようなものとなります。

・同一の機能をもつ施設を協力会社等に所有し、併行で操業しておく
・バックアップ用の作業施設と設備類を保持する
・バックアップ用の作業場所のみ確保（または、確保すべき場所を具体的に想定）しておき、設備は購入やリース等により確保する
・他製品の製造施設・設備を一時的に転用する
・バックアップ用の作業場所（場合によっては設備も含む）を、同業組合等を通して、他社と提供し合えるように協定を締結しておく
・違う場所において新たに施設を建設する

時系列に従って、適当な代替方針を組み合わせていくことが重要となります。
回答にあたり、以下の中小企業庁のホームページを参考としております
3.2.1 事業継続のための代替策の特定と選択をする (meti.go.jp)

質問⑬

使えるお金も人員も限られている中、どこからどのように手を付けたらよいのかわからないので、アドバイスいただきたい。

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、**少なくとも23年度中にレベル1の全50項目の達成をお願いしたい**と考えております。その上でレベル２の項目に関しても24年度末に向け、可能な項目から計画的に達成頂ければと存じます。IPAのガイドライン・規程サンプルを参考にしたり、お助け隊サービスを活用する等も検討頂くと良いと考えます。

24年度末までにレベル２を全件達成することは困難であっても、出来るところから少しずつでも実行頂くことにより、確実にセキュリティレベルは向上してまいりますので、よろしくお願い致します。

参考：
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
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⑭

経営層の理解が得られ、必要な投資が行えるようにできるコツのようなものがございましたらご教授いただけますとありがたいです。

まず、必要な投資を行える様にするためには、経営層と絶えずコミュニケーションをとれる環境をつくることが大切です。
その上で、①経営者自体がやるべきこと、②自社の業界内での対策レベルの立ち位置をしっかり経営者に伝えていくことが効果的です。

①経営者自体がやるべきこと

IPA「中小企業の情報セキュリティ対策ガイドライン」第1部経営者層（P5～12）が参考になります。また、この中には中小企業における事例も掲載されておりますので、こういった世の中の被害事例を活用し、自社にあてはめて危機感をしっかり経営層に効果的だと考えます。

資料	リンク先
中小企業情報セキュリティ対策ガイドライン	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

②自社の業界内での対策レベルの立ち位置を知る

日本自動車工業会より「自動車産業ガイドラインの集計結果」「自動車産業平均比較テンプレート」が提供されておりますのでご活用下さい。

資料	リンク先
集計データ最終結果公表	自動車産業サプライチェーンへの推進活動	JAMA - 一般社団法人日本自動車工業会
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）	活用方法は以下に記載 自動車産業サプライチェーンへの推進活動	JAMA - 一般社団法人日本自動車工業会

情報交換例）　**・各社様にて実施例がございましたら、ご紹介願います。**

質問⑮

チェックシートNo131 メール送信による情報漏えいを防止するための対策について、添付ファイルをZIP化してメールを送り、その後パスワードメールを別送する、いわゆるPPAPや、それを実現するシステムは、セキュリティ上の問題があると聞きます。
それら問題点ふまえ、どういった対策を適用すれば良いでしょうか？

回答：
PPAPは主にメールの通信経路上での盗聴防止を目的に日本で広く普及しましたが、**常にPPAPをすることに対し、現在では以下の弊害がある**と言われています。

1. パスワードがついた添付ファイルはウィルスチェックができない
2. （結局、次のメールでパスワードを送付しているため）誤送信対策にならない
3. パスワード解除の手間（添付ファイルのダウンロード→拡張子変更→解凍）、スマホでは作業できない

PPAP以外の盗聴対策として、メールサーバをTLS暗号化に対応させ配信経路を暗号化する方法や、ストレージサービスに添付ファイルを保存・リンクを案内しブラウザでダウンロードしてもらう方法などがあります。

また、メール送信時の情報漏えいを防止するためには他にも、「**誤送信対策**」や「**機密として管理していることを示しておく**」ことも有効です。
・メールに機密が含まれている旨や、転送禁止などの注記を記載する
・メール送信前に上司の事前承認を得る、CCに上司を含める
・メーリングリストには送付しない、送信前にポップアップを出す　など
情報交換例）　**各社様にて実践例がございましたら、ご紹介願います。**

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