よろず相談会第2回

2024年10月18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	セキュリティ対策を進めたいが、専門知識のある人員確保が課題です。 費用をかけずに体制を構築する事例があれば教えてください。
2	事務所系と工場系などのネットワーク分離を、他社ではどのように実現しているのかを教えてください。
3	他社ではどのような体制や規定・ルール策定を行っているか知りたいです。 また、作成する上で参考となる資料があるか教えてください。
4	SaaSなど外部サービスの活用を進める場合、データバックアップなど自社対応すべき範囲を教えてください。
5	費用をかけずに、標的型メール訓練や内部侵入テストを実施したいです。 活用できるサービスや手法などがあれば教えてください。
6	社内には営業、技術、製造など様々な部署があるなかで、一律のセキュリティルールや設定を行うのは難しいです。 どのような考え方で取り組むのが良いか教えてください。

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。

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

セキュリティ対策を進めたいが、専門知識のある人員確保が課題です。費用をかけずに体制を構築する事例があれば教えてください。

回答：　各社様の規模により、専門の担当者の設定が困難な場合があることは理解しております。
そういった場合も兼任でも結構ですので情報セキュリティに関する役割と権限を持つ方をご指名頂き、

・自動車産業サイバーセキュリティガイドラインおよび同解説書をみる
・自己評価依頼説明会資料および同アーカイブ動画を見る
・自工会・部工会が開催する各種ウェビナー、よろず相談会に参画頂き情報を得る

ことから始めて頂きたいと思います。ただし、ゼロからのスタートの場合、上記資料も理解が困難かもしれません。
そのような場合には、独立行政法人 情報処理推進機構（通称IPA）の「中小企業の情報セキュリティ」が役に立つものと思います。以下のホームページから参照ください。

・ 中小企業の情報セキュリティHP　https://www.ipa.go.jp/security/sme/index.html

専門性の高いサイバー対応の体制として、中小企業向けに「見守り」「駆けつけ」「保険」のサービスをワンパッケージにした、「サイバーセキュリティお助け隊サービス」の利用を検討するのも一つの方法です。比較的利用しやすい安価なサービスとなっており、IT導入補助金による導入支援制度も用意されています。

・IPA　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/index.html

質問②

事務所系と工場系などのネットワーク分離を、他社ではどのように実現しているのかを教えてください。

回答：
【解説書より】

達成条件
“ネットワークを分離"とは、具体的にどう分離されていればよいか？

物理的な視点と論理的な視点の双方がある。
前者は、文字通り、ネットワーク回線が分かれていることである。
後者は、回線上は同一だったとしも、その中を流れるデータが仮想的に別区画として管理されている状態である。(以下例示)

＜物理的な分離＞
・産業用制御システムが存在する場合、そのネットワークを、情報システムのネットワークと切り離して構成する。

＜論理的な分離＞
・外部ネットワークに公開されるサーバーはDMZと呼ばれる仮想的な別セグメントに配置する。
・同一のハードディスクであっても、その中の区画を分けることで、仮想的な別空間の通信として管理する。

質問③-1

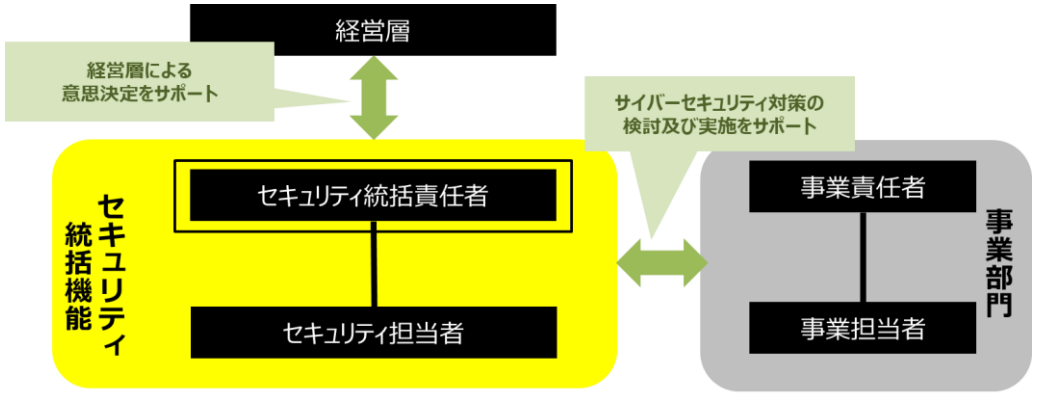
他社ではどのような体制や規定・ルール策定を行っているか知りたいです。
また、作成する上で参考となる資料があるか教えてください。

回答：**【体制】**情報セキュリティ体制は、平時の体制と、事件事故時の体制の**両方が必要**です。

平時の体制

会社として普段からセキュリティ意識を高め、
事件事故が発生しないための対策を行う体制
例）教育、リスクアセスメント

全社的なサイバーセキュリティ体制の構築のために、**「セキュリティ統括機能」**を設置します。

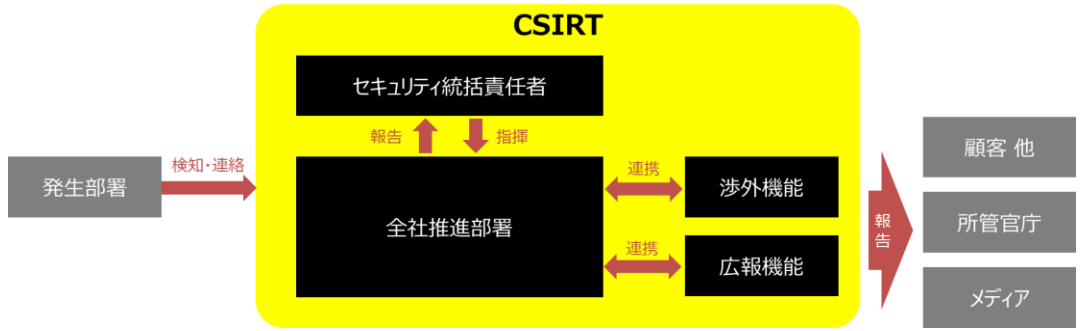


出典：経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」
参考：IPA 情報セキュリティ関連規定（サンプル）　（P.1-P.2）

事件・事故発生時の体制

事件事故発生してしまった場合に備え、
事業影響を最小限にとどめる体制
例）セキュリティ事件・事故対応、外部組織との連携

セキュリティ事件・事故対応への備えとして、一般的に**CSIRT**と呼ばれる機能を設置します。



参考：IPA 情報セキュリティ関連規定（サンプル）　（P.30-P.34）

質問③-2

他社ではどのような体制や規定・ルール策定を行っているか知りたいです。
また、作成する上で参考となる資料があるか教えてください。

回答：**【規定・ルール】**情報セキュリティに関する規定・ルールを策定し、策定した規定は、適宜見直しを行ってください

＜自動車産業ガイド Lv1 規定・ルール策定 関連項目 ＞

分類	規定・ルール	自動車産業ガイド **Lv1** 関連項目No.	達成条件
規定の策定	**法令順守**	9	情報セキュリティに関する法令を考慮し、ルールを策定、教育・周知している
		11	法令の変更に伴い、ルールを適宜見直ししている
	機密情報を扱うルール	4	社内に守秘義務を理解させ、守らせている
		8	業務で利用する情報機器の利用ルールを規定し、周知している
	社内接続ルール	79	業務で利用する情報機器の自社ネットワークへの接続ルールを定めている
	認証・認可	115	パスワード設定に関するルールを定め、周知している
	アクセス権	49	人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている
		51	管理ルールに沿ってアクセス権の発行、変更、無効化、削除を実施している
	情報資産の管理（情報）	54	機密区分に応じた情報の管理ルールを定めている
		58	情報資産(情報)は機密区分に応じた管理ルールに沿って管理している
	情報資産の管理（機器）	59	重要度に応じた情報機器、OS、ソフトウェアの管理ルールを定めている
		62	情報資産(機器)は重要度に応じた管理ルールに沿って管理している
	他社との情報セキュリティ要件	44	他社との間で、機密情報の取り扱い方法が明確になっている
		46	情報セキュリティ事件・事故時の他社との役割と責任が明確になっている
	取引内容・手段の把握	76	自組織の資産が接続している外部情報システムの利用ルールを定めている

参考：IPA 情報セキュリティ関連規定（サンプル）
：JNSA　情報セキュリティポリシーサンプル改版

質問④

SaaSなど外部サービスの活用を進める場合、データバックアップなど自社対応すべき範囲を教えてください。

回答：基本的なSaaSの責任共有モデルは右図の通りで、アプリケーションまでをSaaS事業者が責任を持つモデルになります
バックアップの自社対応についてはケースバイケースなのかと思いますが、次のような視点で考えるとよいかと思います

SaaS事業者のバックアップポリシー
- バックアップ頻度: プロバイダーがどのくらいの頻度でデータをバックアップしているか
- 保持期間: バックアップデータがどのくらいの期間保持されるのか
- 復元単位: 全体を復元、機能ごとに復元、個別データ単位で復元
- 復元手順: データの復元がどのように行われるのか（手順や時間についても）
- 複製条件: 同一センター内複製、同一地域内DCへの複製、遠隔地複製なのか

災害復旧計画
- SaaSプロバイダの災害復旧計画はどうなっているのか

契約で提供されるSLA
- データの可用性やバックアップに関するSLAから、期待されるサービスレベルを確認

自社でのバックアップ手段
- 自社でバックアップする場合のバックアップ方法、費用

質問⑤

費用をかけずに、標的型メール訓練や内部侵入テストを実施したいです。
活用できるサービスや手法などがあれば教えてください。

回答：

標的型メール訓練

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、実施前、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ます。
参考サイト：「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」

内部侵入テスト　（出典　総務省　国民のためのサイバーセキュリティサイト）

攻撃者と同じ視点で攻撃を行い、実際に攻撃が成功するかをリスクベースで確認する検査をペネトレーションテストと言います。
脆弱性診断やペネトレーションテストを行い、WebアプリケーションのSQLインジェクションの脆弱性や、セッションハイジャックの
脆弱性の有無などを診断することで、設置したサーバのセキュリティ強度が確認でき、さらに強化すべきポイントを明確に
することができます。これらのセキュリティ診断は一般的には有料のサービスとして提供されていますが、
インターネットで公開されているフリーウェアの診断ツールを入手して、自分である程度のチェックを試みる方法もあります。
参考サイト：脆弱性診断・ペネトレーションテスト実施 | 国民のためのサイバーセキュリティサイト (soumu.go.jp)

質問⑥

社内には営業、技術、製造など様々な部署があるなかで、一律のセキュリティルールや設定を行うのは難しいです。
どのような考え方で取り組むのが良いか教えてください。

回答：

エンタープライズ領域（会社全体のベースとなる OA 環境）については、**会社として一律のセキュリティルール**としながらも、**生産に影響を与えない設備制御システムの護り方**や、**お客様情報/技術情報をもっと厳格に護りたい**という業務ニーズ等に合わせて、部署毎にセキュリティ基準を検討ください。

各社によって、様々な部署があると思いますが、まずは、何を護らないといけないのか？、どの様な対策があるのか？、対策する上でどのような課題があるのか？をご検討ください。

課題がある場合、100点の対策でなくても、セキュリティリスク低減のために80点の対策で進めないといけない実態もあるのだと思います。（例：生産設備において、タイムリーにOSのVerUpができないため、ネットワーク対策で代替 等）

自動車産業ガイドでは、特定の業務領域によらず
全体の業務に共通する
エンタープライズ領域（業務基盤となる OA 環境）が対象範囲です。

参考情報

参考資料URL

No.	参考資料URL
1	IPA 情報処理技術者試験　情報セキュリティマネジメント試験とは https://www.ipa.go.jp/shiken/kubun/sg/about.html
2	IPA プラクティス5-1　多層防御の実施 https://www.ipa.go.jp/security/economics/practice/practices/Practice214/
3	IPA 中小企業の情報セキュリティ対策ガイドライン https://www.ipa.go.jp/security/guide/sme/about.html
4	IPA 中小企業のためのクラウドサービス安全利用の手引き https://www.ipa.go.jp/security/sme/f55m8k0000001wcf-att/000072150.pdf
5	徳丸浩のウェブセキュリティ講座　Nessusの無料版(Nessus Essentials)をインストールしてみよう https://www.eg-secure.co.jp/tokumaru/youtube/17
6	IPA 中小企業の情報セキュリティ対策ガイドライン　P.54（8）詳細リスク分析の実施方法 https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

E N D