よろず相談会 第5回

2024年11月22日 10：00～12：00

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	対策内容について、達成レベルの判断基準と優先的に対策すべき項目があれば教えてください。
2	システムが停止した際の業務が遂行できる代替手段は、どのような対策をすればよいか教えてください。
3	ガイドライン[No.32] 「各部署の情報セキュリティ管理者に対して、組織内での対策とマネジメント手法に関する教育を実施している」について、マネジメント手法とは、どのようなことをするのか教えてください。
4	ガイドライン[No.37] 取引先の指導ができるようなセキュリティ教育の内容はどのようなものを行えばよいか教えてください。
5	セキュリティ対策の人員、費用を確保するのが困難です。どのように取り組みを進めればよいのか教えてください。
6	サイバー攻撃やその予兆を検知するためのログ監視・分析について、環境・頻度・方法について教えてください。

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

対策内容について、達成レベルの判断基準と優先的に対策すべき項目があれば教えてください。

回答：自動車産業サイバーセキュリティガイドラインでは達成レベルはLv1～Lv3で定義されています。Lv1から順にステップアップしていくようになっています。また判断基準については自社の取り扱う情報に応じて目標レベルを判断ください。
自工会・部工会ではLv2達成を推奨していますので、Lv1から順に進めて頂くようお願いします。

＜自動車産業サイバーセキュリティガイドラインのセキュリティレベル定義＞

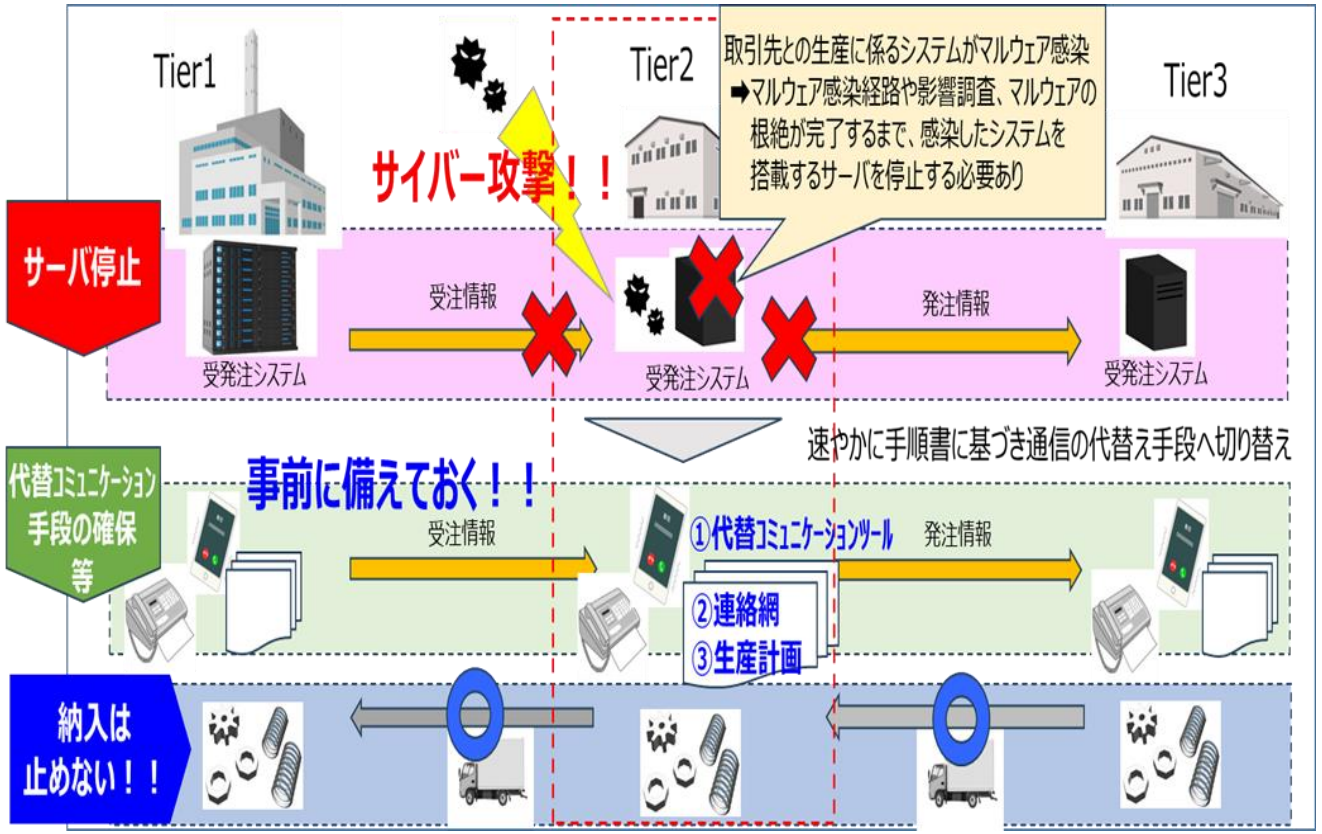
Lv. 3	⇦	**模範レベル（ベストプラクティス）**
Lv. 2	⇦	**顧客情報・取引先技術情報を取扱う会社が達成すべき項目**
Lv. 1	⇦	規模・扱っている情報に因らず**最低限必要な必須項目**

また本年度、JAMA・JAPIAから、「セキュリティ推進担当者向け解説資料」とし、何から対策をスタートするとよいか、ご参考となる資料を展開する予定です。また、下記のようなガイドラインもございますので、是非ご参考ください。
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
P19.できるところから始める

質問②

システムが停止した際の業務が遂行できる代替手段は、どのような対策をすればよいか教えてください。

回答：



自動車産業サイバーセキュリティガイドライン | JAMA - 一般社団法人日本自動車工業会

左図にある通り、Tier2企業がサイバー攻撃を受けて、生産に係るシステムがマルウェア感染した場合を想定します。

その場合、Tier2企業は、感染したシステムを搭載するサーバに対する、**「マルウェアの感染経路や影響調査」、「マルウェアの根絶」が完了するまで、感染サーバを停止しなければなりません。**また、その間はシステムによる受発注情報の授受が出来ない状態に陥り、**その状態が長期化すると、顧客への納入停止や、仕入先からの部品手配停止リスクが発生します。**

そのような場合に備えて、会社における**事業継続計画の策定が必要**になります。

生産業務であれば、

①電話やFAX、代替えによるコミュニケーション手段確保
②受発注業務が出来る様に社内外の連絡網整備
③手動での生産計画策定

等の事前準備が必要となります。

いざという時のために、これらの対応が速やかに出来る様に、日ごろから準備や訓練をしておきましょう。

質問③

ガイドライン[No.32] 「各部署の情報セキュリティ管理者に対して、組織内での対策とマネジメント手法に関する教育を実施している」について、マネジメント手法とは、どのようなことをするのか教えてください。

回答：
一般的には、各部署の情報セキュリティ管理者は、情報セキュリティ確保のために多くのマネージメント活動を実施し、これによりセキュリティの強化とリスク低減を行います

部門ごとのマネージメント活動例

- ポリシーの理解浸透　組織全体のセキュリティポリシーを理解し、部門内での適用を促進する
- リスクアセスメント　部門内の情報資産に対するリスクを特定し評価する
- リスク対策の実施　部門内の特定されたリスクに対して適切な対策を講じる
- 教育・訓練　部門の従業員に対して情報セキュリティに関する教育や訓練を実施し、意識を向上する
- インシデント報告対応　セキュリティインシデントが発生した場合の部内の報告体制を整備し迅速に対応する
- 法令・規制の遵守　情報セキュリティに関連する法令や規制を遵守するための活動をする
- 内部監査の実施　定期的に部門内のセキュリティ対策が適切に実施されているかを監査し改善点を特定する
- 対策のレビュー　自部門でのセキュリティ対策の効果を定期的に評価し、必要に応じて改善策を講じる
- セキュリティ部門との調整　セキュリティ部門との連携・調整を図る。

質問④

ガイドライン[No.37]　取引先の指導ができるようなセキュリティ教育の内容はどのようなものを行えばよいか教えてください。

回答：ガイドライン[No.37]の設問は【**情報システムの調達**に係る要員に対して、取引先の指導ができるようセキュリティ教育を実施している】となっています。取引先に関係する情報システムの調達としては下記が挙げられます。

代表的な外部サービス利用例
- ・システム開発の外部委託
- ・クラウドサービスの利用

上記のような外部サービスを利用する場合に該当サービスでセキュリティ対策が正しく行われていて情報漏洩等のリスクが無いか確認することが必要です。そのためのどのような対策が必要なのかを知るための教育が必要となります。

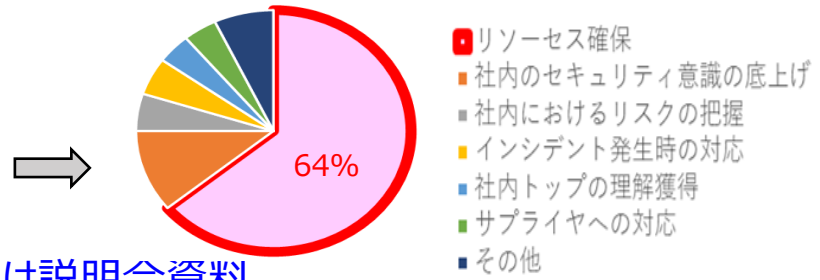
中小企業の情報セキュリティ対策ガイドライン第3.1版　P28（4）委託時の対策
付録5：情報セキュリティ関連規程（サンプル）（全42ページ）（Word:167 KB）
P29 9-1 委託先情報セキュリティ対策状況確認リスト
中小企業のためのクラウドサービス安全利用の手引き

質問⑤

セキュリティ対策の人員、費用を確保するのが困難です。どのように取り組みを進めればよいのか教えてください。

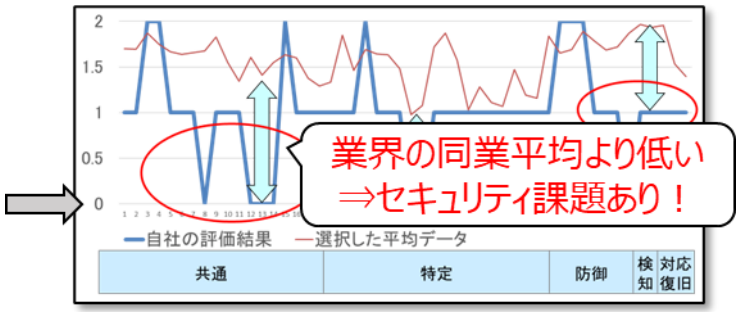
回答：
サイバーセキュリティ対策は、経営課題です。
まずは自社の経営者が、リソーセス確保に関して、どの様に認識されているか
ご確認頂ければと思います。ちなみに先日実施されました経営層向け説明会を
聴講して頂きました経営者の方は、自社の「リソーセス確保」が最重点課題と認識して
頂けている会社様が多数おられました。 2024年度 自己評価の実施・展開及び経営層向け説明会資料

アンケートQ4：具体的に自社で対策を進める上での課題は何ですか



その上で、JAMA・JAPIAから、「セキュリティ推進担当者向け解説資料（自動車産業サイバーセキュリティガイドラインの
優先項目の解説）」が自工会HPに公開されておりますので、ご参考にして下さい。
自動車産業サイバーセキュリティガイドライン | JAMA - 一般社団法人日本自動車工業会

また、セキュリティ対策予算の確保の取組み例としては、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）を活用し、他社の対策状況と自社の対策状況とのギャップから、
強化対策計画を作成して、優先付けを行い対応されている会社もあります。

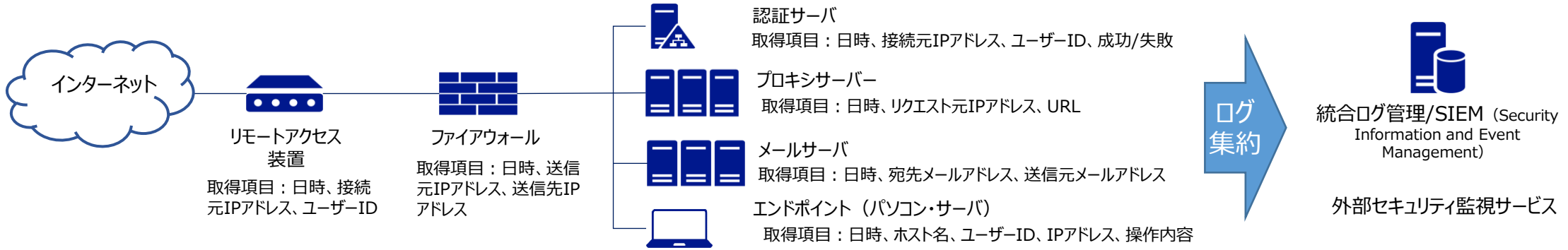


参考資料
・IPA　ガイドライン第2部実践編：中小企業の情報セキュリティ対策ガイドライン | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
・IPA　サイバーセキュリティお助け隊サービス制度：サイバーセキュリティお助け隊サービス制度 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

質問⑥

サイバー攻撃やその予兆を検知するためのログ監視・分析について、環境・頻度・方法について教えてください。

回答：
昨今の高度化するサイバー攻撃対応として、様々なログを総合的に監視することが重要となっています。サーバー環境、ネットワーク機器、エンドポイント、セキュリティデバイス等組織のIT環境全体をカバーすることが理想的です。



方法としては、統合ログ管理(SIEM)を導入し自社で監視する方法と、外部のセキュリティ監視サービスを使う方法がある。
自社で監視する場合は、即時対応性、カスタマイズ性、知識の蓄積などがメリットなる一方、コスト、人材確保、24/365の運用、技術進化への対応などが、負担となる可能性があります。
攻撃者は人の目が届きにくい週末や夜間を狙ってくるケースも多く発生しており、基本的には24時間365日リアルタイムの監視を行うことが重要になります。また、週次・月次などでレビューを行い通常と違うトレンド・パターンを確認することも重要です

E N D