

■ デジタルものづくり対応支援事業

情報セキュリティ対策基礎講座（会員限定）

― 自動車業界の標準「自工会／部工会サイバーセキュリティガイドライン」から導き出した中小企業のための情報セキュリティ強化の進め方 ―

近年、デジタル化の進展に伴って、サイバー攻撃による工場の操業停止や個人情報の流出などの被害が急増しており、企業におけるサイバーセキュリティを含む情報セキュリティ対策の強化が急務となっています。

このような状況の中、2020年3月に「日本自動車工業会」と「日本自動車部品工業会」が共同で、自動車業界全体の標準・指針となる「サイバーセキュリティガイドライン」を策定しました。

次世代自動車センター浜松では、会員企業の皆様が、自工会／部工会「サイバーセキュリティガイドライン」をもとに情報セキュリティ対策に取り組んでいただくよう、当センターの仲元技術コーディネーターが講師となって、情報セキュリティの強化に取り組む際の考え方や具体的な取り組みの進め方などについての基礎的な情報を提供する講座を開催しました。

■ 日 時：令和6年10月16日（水）13時30分～15時

■ 場 所：Web形式

■ 参加者：49社／230名

公益財団法人 浜松地域イノベーション推進機構
Hamamatsu Agency for Innovation

次世代自動車センター

情報セキュリティ対策 基礎講座

自動車業界の標準
「自工会／部工会 サイバーセキュリティガイドライン」から
導き出した中小企業のための情報セキュリティ強化の進め方

2024年10月16日
次世代自動車センター浜松

© 2024 公益財団法人浜松地域イノベーション推進機構 次世代自動車センター (1)



8 サプライチェーン全体に求められる「情報セキュリティ」への対応

- 近年では、サプライチェーンの最上流に位置する大手企業が
傘下の取引先企業に情報セキュリティの強化を要請するケースが増加
- その理由は
「1つの企業のレベルの低さ」が「サプライチェーン全体」の弱みになるから。
- 1社でもレベルの低い企業があると、
すべての関係企業に被害がおよぶ。
(操業停止・風評被害などの連鎖)
- 今後は、「Q：品質、C：コスト、D：納期」と
同じレベルで「S：セキュリティ」の強化に対応することが、
サプライチェーンの企業間での「信用維持・事業継続」の重要な要素になる。

14 「情報セキュリティ」に関する事件・事故を防ぐために、何をすればよいのか

- 自工会／部工会「サイバーセキュリティガイドライン」を
もとに、情報セキュリティの強化の取り組むことが効果的
- 自工会（日本自動車工業会）／部工会（日本自動車部品工業会）
「サイバーセキュリティガイドライン」とは
 - ・自動車業界の標準として、具体的な取り組み方法を示したもの。
 - ・2020年3月に完成車メーカーの業界団体「日本自動車工業会」と
部品メーカーの業界団体「日本自動車部品工業会」が共同で策定。
 - ・目的は、業界共通のサイバーセキュリティ対策基準を共有して活動する
ことで、サプライチェーン全体のセキュリティレベルを向上させること。
 - ・内容はサイバーセキュリティだけでなく**情報セキュリティ全般（故意や
過誤による情報漏洩など）**をカバーしている。

23 自工会／部工会「サイバーセキュリティガイドライン」対応（現状の見える化 1/3）

1. 現状の見える化：ガイドラインと自社の現状とのギャップを確認する。

- 「見える化」のためのツール（例）
- 1. 「自工会／部工会サイバーセキュリティガイドライン チェックシート」
https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html
- 2. 本講座で提供する「情報セキュリティ対応状況チェックシート」（次世代自動車センターが独自に作成）
上記1.のチェックシートの超簡易版（Lv1のうち、最初に着手してほしい17項目のみチェック）
- 3. IPA（情報処理推進機構）「5分でできる！情報セキュリティ自社診断」
<https://www.ipa.go.jp/security/guide/sme/5minutes.html>

分類（シブ）	No.	内容（調査項目）	評価基準	達成状況（自己申告）
1. 経営者・役員	1.1	経営者・役員がサイバーセキュリティの重要性を認識し、推進している。	経営者・役員がサイバーセキュリティの重要性を認識し、推進している。	達成状況（自己申告）
2. 体制（組織）	2.1	経営者・役員がサイバーセキュリティ推進の責任を負っている。	経営者・役員がサイバーセキュリティ推進の責任を負っている。	達成状況（自己申告）
3. 体制（組織）	3.1	経営者・役員がサイバーセキュリティ推進の責任を負っている。	経営者・役員がサイバーセキュリティ推進の責任を負っている。	達成状況（自己申告）

56 「事故時の対応の優先度」と「システム・設備等が使えない場合の代替手段」の決定

- 取り組みの進め方
- ① 全社の情報資産（情報、製品、設備など）を棚卸し
・社内各部門及び 全社で使用している業務システムなどを調査し列記する。
・システムだけでなく、コンピュータを制御に使っている設備・機器も、
各部門に依頼して、もれなく洗い出す。
- ② 停止した場合の影響・その理由・現時点での代替手段の有無、を調査する。
- ③ 上記をもとに、
「事故時の対応の優先度」「システム・設備等が使えない場合の代替手段」
および、整備の進めかた（着手順・予算など）を決定する。
- ④ 上記③の内容を対策強化の取り組み計画として立案し、順次実施する。

【参加者の声】

- ・自工会チェックシートの中でもさらに絞り込んだ最初の一步のチェックシートなどは、実戦的で非常に参考になった。
- ・具体的な進め方がわかった。特に詳細なルール（セキュリティ規程）について、どのような項目を盛り込んでよいのかわからなかった部分が明確になった。
- ・費用を掛けずにできる対策の紹介が大変参考になった。仕組み作りとインシデント発生時の訓練を早急に行っていこうと思った。
- ・サイバーセキュリティを強化していく目的と手順・注意事項等を丁寧に説明いただき、サイバーセキュリティの今後の重要性を改めて勉強させていただいたこと、情報資産（情報・製品・設備）の非常事態時の優先度決定の内容及び事業継続の為の代替手段の決定について、近年の「防御」から「回復力」の強化の重要性が大変参考になった。
- ・これまでにない切り口で、今すぐにも取り組める内容が具体的に紹介され、大変勉強になった。情報セキュリティ対策の基本的な考え方、ルールづくり、体制づくりを認識することができた。
- ・自動車業界には、チェック項目が既に存在していることを学んだ。全く対策に着手していない中小企業は、チェック項目を全てクリアすることは非常に大変だと感じた。しかし、その分、自動車業界は、関係企業の隅々までセキュリティ面に対して厳しく対策を打つ必要があると改めて学んだ。
- ・情報セキュリティを守るためにはガチガチのルールを作ってはだめで、業務との兼ね合いも見ながら、策定・運用・改善が欠かせないと経営層に訴える内容だった。
- ・基本的なところを再度確認することができた。完璧な対策が無い中で、チェックシートで“完了”評価を判断するのが難しいと感じた。
- ・当社に抜けている箇所が明確になった。セキュリティ対策の考え方、進め方など基本がよくわかった。「守れないルールは作らない」など、大事な点だと感じた。
- ・QCDSの概念を知ることができた。ルール運用の確認という点で監査などの具体的対応策や、規定において法令と行為をセットとするなど実務的な対応を知ることができた。
- ・Lv1の中の最低限実施すべき基礎的な項目について、丁寧に説明していただいたので参考になった。
- ・企業のセキュリティ対策の一環として、企業の価値・資産を守る活動としての「情報セキュリティ」について、わかりやすく体系化されていたことと、昨今のサイバー攻撃事例の知見が深まり、情報セキュリティに対する必要性を痛感した。また、会社としてどのように取り組むべきかの方向性も理解した。特にルール化の中の情報資産の管理は、部門内でも議論していきたい。
- ・現在のセキュリティリスクの状況や、攻撃を全て防ぐことは不可能なので、ウイルス対策と同じように代替手段の構築が必要不可欠であるとの考え方が参考になった。
- ・自工会チェックシートに基づいた自己評価は行っているが、ルールの作成方法について確認ができた。経営層や全社に対してセキュリティの重要性を訴求する参考になった。
- ・「自工会/部工会サイバーセキュリティガイドライン」は項目が多すぎるのと専門語や内容が理解しづらかったので、簡易的な「情報セキュリティ対応状況」チェックシートを使用するなど進め方が参考になった。
- ・情報セキュリティ、サイバーセキュリティについてガイドラインがあることは心強く、「防御力」だけでなく「回復力」も重要ということは学びになった。
- ・1つの企業のサーバーセキュリティへのレベルの低さが全体に影響を及ぼすことを改めて理解し、対策の重要性を学べた。