

## ■ デジタルものづくり対応支援事業 第2回サイバーセキュリティ対策ワークショップ（会員限定）

近年のデジタル化の進展に伴って、外部からのサイバー攻撃による工場の操業停止や個人情報流出などの被害が急増しています。

特に最近では、仕入先の部品メーカーが被害を受けたことにより、大手完成車メーカーの生産が停止するなど、サプライチェーン全体に影響する事例も発生しており、製造業にとってもサイバーセキュリティ対策の強化が急務となっていますが、多くの中小企業では「自社のような規模の企業は大丈夫」「具体的に何をしたらよいかわからない」などの理由で、対策・対応が遅れています。

次世代自動車センター浜松では、今回、サイバー攻撃対応の机上演習やサイバーセキュリティBCPの模擬策定演習を内容として、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、「サイバー攻撃が発生した場合にどのような対応を迫られるか」や「サイバー攻撃の被害の低減や復旧の迅速化のための対策の立て方」などについて、参加企業の皆様が自ら考えながら学ぶ「サイバーセキュリティ対策ワークショップ」を開催しました。

■ 日 時 : 令和7年3月12日（水）13時30分～16時30分

■ 場 所 : グランドホテル浜松

■ 参加者 : 20社 / 39名

### <開会・挨拶>



### <グループワーク 1：サイバー攻撃対応の机上演習>



### <グループワーク 2：サイバーセキュリティBCPの策定演習>



### <質疑感想>



### <総括>



## 【参加者の声】

(全体)

- ・ITセキュリティについて取り組む気持ちが高まった。
- ・緊急時対応と同じで、迅速な対応が必要ということがわかった。
- ・非常時に被害を最小化となるような判断・対応ができるよう平時に準備をしておくことの大切さが学べた。
- ・改めて自社の課題点を見つめ直すいい機会となった。
- ・実際にケーススタディを通して具体的な取り組み内容をイメージできた。
- ・サイバーセキュリティBCPの策定をしたかったが、作り方が判らなかつた中、大変判りやすい説明と自社の実情に基づいて記入ができたから参考になった。また、2人で参加できて良かった。
- ・BCPとしてサイバーセキュリティの投資をしていく必要性を感じた。事前の対応マニュアルを整備するのも専門的な知識になるため、人にかかるコストが発生するが、必要な投資だと感じた。また、今日の研修で作成したBCPは経営状況や人の変化に合わせてアップデートすることが重要だと感じました。
- ・他社との会話で今まで気付かなかつたことに気付けた。
- ・組織としての対策が必要だと考えさせられた。
- ・グループワークすることにより、さまざまな考えが聞くことができよかつた。

(グループワーク1)

- ・被害のケースは知っていたが、攻撃されたらどう進んでいくのかと具体的に考えることができ参考になった。
- ・準備していたとしてもできることは半分以下、準備していなかつたら何も動けないことがよくわかつた。
- ・連絡網や初期対応の手順書の必要性がわかつた。
- ・初動の対応の仕方がわからなかつたので参考になった。
- ・システムの見える化がまず必要であり、体制作りも早急に必要。
- ・業務システム構成図や社内体制づくりの重要性を再認識した。現場での確認と迅速な初動の重要性を感じた。
- ・ケーススタディにより、異常発生から初動対応における正確な対応手順を理解し、事前に非常時対応のマニュアルを整備することが重要だと感じた。
- ・対応手順の作り方・進め方が参考になった。
- ・サイバー攻撃を受けたあとの初動は訓練しているが、その後は限られた人のみしか対応できない現状がわかつた。

(グループワーク2)

- ・重要度の決め方や進め方が参考になった。担当者が社内だけでなく社外もあるので、そちらの優先度も気づくことができた。
- ・評価表を作成することで進め方のイメージがよくわかつた。
- ・自社に置き換えて考えることができたので、良いきっかけとなった。
- ・サイバーセキュリティの全社訓練が重要だと感じた。
- ・何からやったらいいかわからなかつたので、サンプルを出してくれてイメージが沸いた。
- ・BCPを作るための順番で模擬体験ができて、作る上で参考になった。
- ・システムのBCPを策定すべく、自社のシステムに関わる設備を洗い出し、どの部門が管理しているか、停止したときの影響度を見える化し、復旧の際の優先順位をつけることが重要だと学んだ。