サイバー攻撃を受けたら・・・

生産停止する工場ですか？
生産継続できる工場ですか？

サイバー
セキュリティ
×BCP

工場の緊急時生産管理体制を共に考える！

「中小製造業向け体験型演習」
開催に向けた事前説明セミナー

令和５年 **２月１日(水)**	**15:00～ 17:00**	**オンライン** **(Microsoft Teams)**

参加費無料

【プログラム】

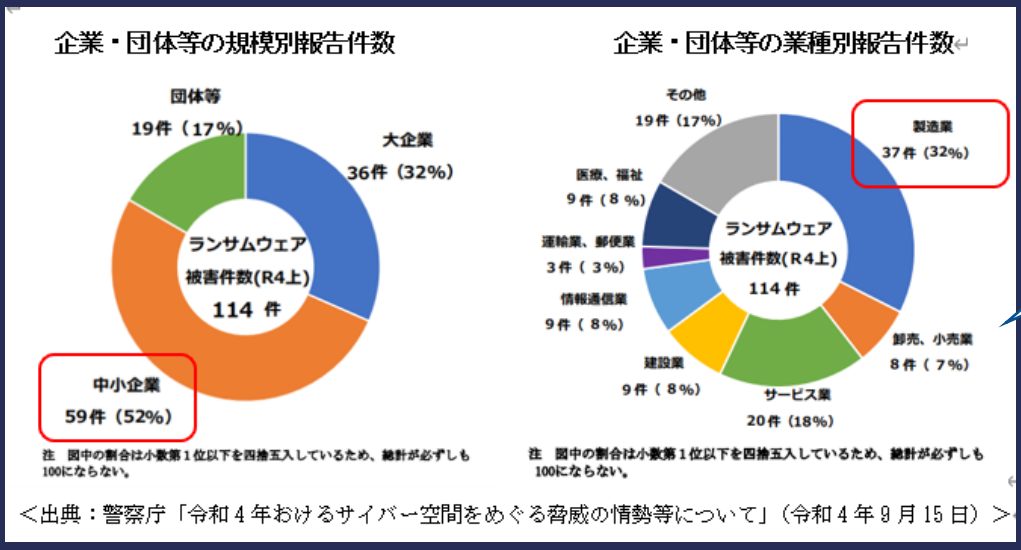
1　中小製造業を巡る情勢とセキュリティ・BCP関連施策のご紹介　【九州経済産業局】

2　中小製造業向け体験型演習の概要紹介　【九州大学】

3　工場セキュリティハンドブックのご紹介と演習との相乗効果について　【日本ネットワークセキュリティ協会】

4　パネルセッション　【九州大学、マツダ(株)、(株)安川電機】

主催：経済産業省九州経済産業局、九州大学サイバーセキュリティセンター、一般財団法人九州オープンイノベーションセンター
後援（予定）：JNSA（NPO法人日本ネットワークセキュリティ協会）



＜出典：警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」（令和４年９月15日）＞

警察へのランサムウェア**被害報告件数の52%が中小企業**、業種別では**製造業が最多**。

不正アクセスといったサイバー攻撃が**“引き金事象”**となって工場が機能不全に陥り、生産停止や保安事故などが起こると、製品の生産・出荷に支障をきたし、取引先との関係のみならずサプライチェーン全体にも影響が出ることが昨今強く懸念されています。

とはいえ、日々攻撃の手口が巧妙化するなか、工場へのサイバー攻撃による生産への影響を完全にゼロにすることはできませんが、**自然災害による被害と同様に、重要視すべきは“生産の継続（BCP）”ができるように備えること**です。

今回実施する演習は、九州大学が社会人向け実践教育プログラムの一つとして実施されていたプログラムを、**“中小製造業向け”にアレンジし提供する“全国初”の取組**となります。

サイバー攻撃による生産設備等の機器障害発生時における対策本部活動、緊急生産管理体制等を予め検討し訓練を行い、影響を最小限にするための**課題・対応を共に考えませんか？」**

九州大学
KYUSHU UNIVERSITY

SECKUN
「サイバーセキュリティインシデント対応机上演習」
実施イメージ

○申し込み方法

下記フォームよりお申し込みください。入力できない場合はメールで、
①企業・団体名、②所属部署、③役職、④氏名、⑤メールアドレスを
九州経済産業局デジタル経済室（kyushu-iot@meti.go.jp ）までご連絡ください。

URL：https://mm-enquete-cnt.meti.go.jp/form/pub/kyusyu-johoseisaku/ttx-seminar

○申込締切：令和５年１月３０日（月）１８：００

○登壇者等詳細はこちら：https://www.kyushu.meti.go.jp/event/2301/230110_2.html

○お問い合わせ先：経済産業省　九州経済産業局　デジタル経済室　担当：春口、横尾
TEL：092-482-5552　E-mail：kyushu-iot@meti.go.jp