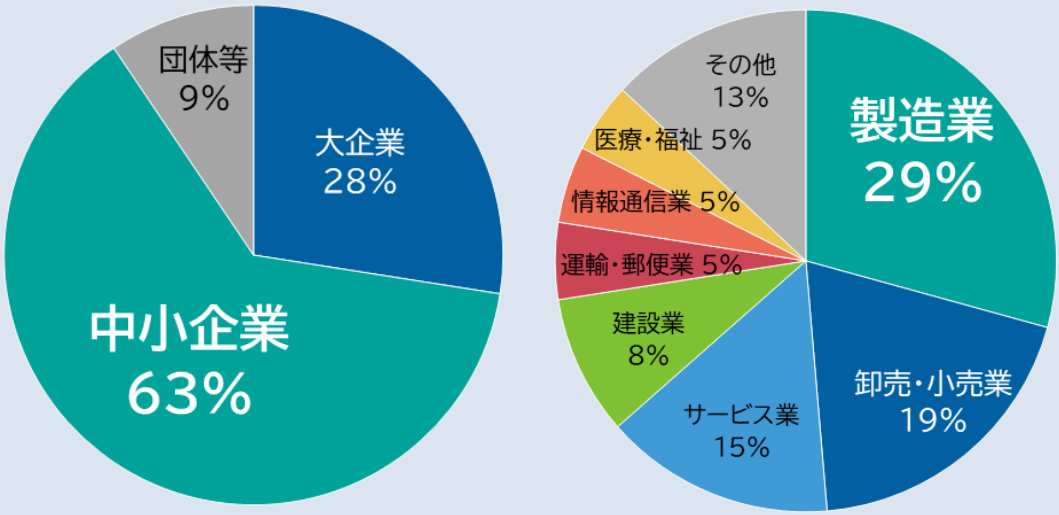
工場におけるサイバーセキュリティ
～平素の備えが工場を守ります～

サイバー攻撃の一つであるランサムウェアによる被害は、
大企業より中小企業で多く発生しています。
また、業種別では製造業が最も多くなっています。

ランサムウェア被害企業等の規模・業種別割合



警察庁:「令和6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」に基づき作成

工場を有する中小規模の製造事業者の経営層や、工場のセキュリティ担当者を対象に、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の解説書として、

Appendix【工場セキュリティの重要性と始め方】

を作成しました。

Appendix【工場セキュリティの重要性と始め方】はこちら

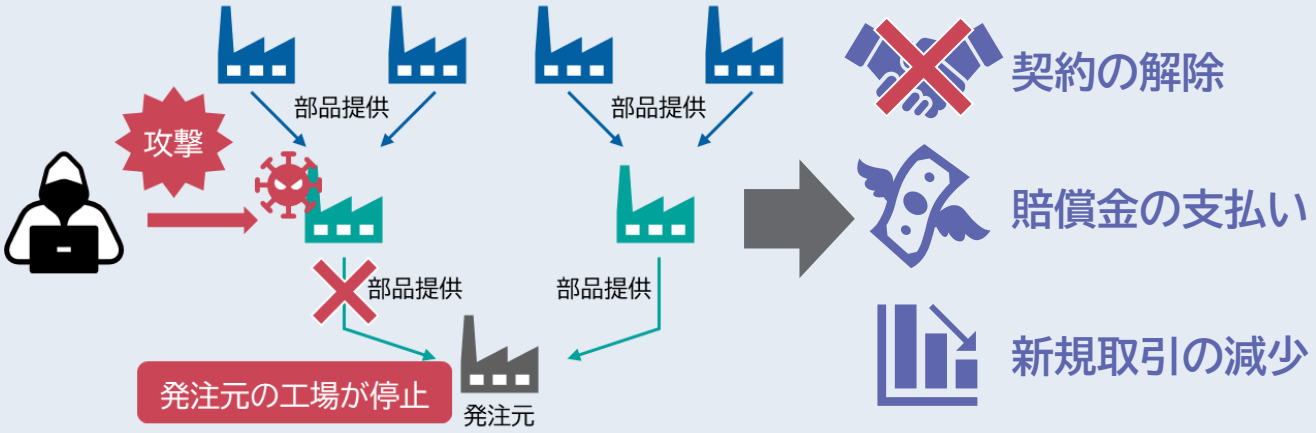
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_appendix02.pdf

経済産業省
Ministry of Economy, Trade and Industry
商務情報政策局　サイバーセキュリティ課

工場に対するサイバー攻撃は、甚大な被害を及ぼします！

製造業全体を守るためには、サプライチェーンを構成する全ての企業において、セキュリティ対策を実施する必要があります。

サイバー攻撃は、自社だけでなく発注元へも甚大な被害を及ぼします！



コストをかけずとも実施できる対策から始めましょう！

サイバー攻撃を受けても業務を継続できるよう、事前に準備をしておくことが大切です。

チェック	事前準備の例
✓	被害発生時の役割分担をあらかじめ決めていますか。
✓	サイバー攻撃を受けた際に支援を求める外部の連携先（情報システム・工場システムを委託しているベンダなど）を整理していますか。
✓	一部設備・機器が停止した場合のバックアッププランを用意し、生産現場担当者に対して訓練を行っていますか。
✓	工場のネットワーク構成図や製造設備を把握できていますか。

「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」
& Appendix【スマート化を進める上でのポイント】はこちら

https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

経済産業省
Ministry of Economy, Trade and Industry
商務情報政策局　サイバーセキュリティ課