

ニューノーマル処方箋(第43回)

自動車産業がサイバー攻撃に狙われている！？どう防ぐ？

2024.06.28



<目次>

- ・自動車部品の工場が、サイバー攻撃に狙われている
- ・なぜ自動車産業は、サイバー攻撃に狙われるのか？
- ・どうすればサイバー攻撃を防げるのか？業界団体がガイドラインを策定
- ・自動車を造るように、産業全体のセキュリティも力を合わせて守ろう！

自動車部品の工場が、サイバー攻撃に狙われている

サイバー攻撃は年々増加しており、ターゲットも多様化しています。大企業だけでなく、サプライチェーンや中小企業にまで被害が及んでいます。

特に日本の経済を支える重要な産業である自動車産業は、広いサプライチェーンやITを活用した技術革新が進む中で、サイバー攻撃のターゲットになりやすい産業の1つといえるでしょう。

実際に自動車産業を狙った事件も多数発生しています。例えば2023年9月には、ある自動車メーカーのサーバー機器が外部からの不正アクセスを受け、個人情報の一部が外部へ流出した可能性があると発表。件数は10万件に及びました。

2022年3月には、自動車部品を製造するメーカーの海外グループ会社が、第三者による不正アクセスを受けたことを確認したと発表しました。同社では不正アクセスを受けた機器のネットワークを速やかに遮断し、他拠点への影響がないことを確認。生産活動への悪影響はなかったといえます。

同年3月には、別の自動車部品メーカーも第三者による不正アクセスを受けたと発表しています。同社から部品を仕入れていた自動車メーカーは、安全のため国内全工場の製造ラインをストップする事態に追い込まれました。調査の結果、同社の情報が外部へ持ち出された形跡はなく、情報漏えいの事実も確認されなかったといえます。

なぜ自動車産業は、サイバー攻撃に狙われるのか？

自動車産業がサイバー攻撃の標的とされるのには、さまざまな理由が考えられます。例えば自動車産業は、オフィスだけでなく製造工場の情報システムもインターネットにつながっています。サイバー攻撃が成功した際のインパクトが大きいことも理由の1つでしょう。

産業自体の規模が大きく、「サプライチェーン攻撃」がしやすいということも考えられます。サプライチェーンとは、原材料の調達や部品の製造から製品の完成、販売に至るまでの一連の流れをさします。この中で、セキュリティ対策が手薄な企業を狙うのが、サプライチェーン攻撃です。

多くの場合、大企業であればあるほどサイバー攻撃の標的になりやすいのですが、大企業のセキュリティ対策はレベルが高くなりがちです。そんな大企業でも、サプライチェーンをたどれば、セキュリティ対策が甘い中小企業が存在するかもしれません。サプライチェーン攻撃は、そうした企業にサイバー攻撃を仕掛け、踏み台として利用することで、最終的に大企業を攻撃します。

自動車産業は、自動車を組み立てて完成させる工場だけではなく、その自動車に使用する部品の工場、さらにその部品を作るための工場……と、サプライチェーンの裾野が広い業界です。そのため、サプライチェーンの“源流”に位置する企業が狙われがちです。先に挙げた3つのサイバー攻撃の例も、2件は部品メーカーをターゲットとしたものでした。

どうすればサイバー攻撃を防げるのか？業界団体がガイドラインを策定… 続きを読む