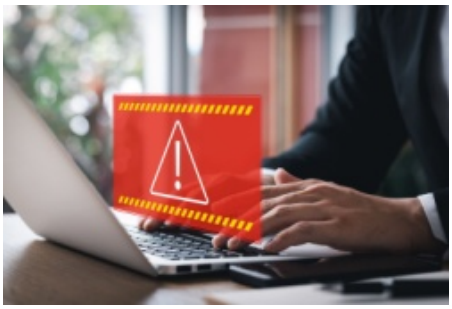
事例で学ぶセキュリティインシデント（第13回）

# 対策が脆弱な業務委託先が狙われるサプライチェーン攻撃

2024.06.17



工作機械部品を製造するM社。大阪工場の製造課長が出社後、いつものように生産管理システムを立ち上げようとしたところ、パソコンがなかなか起動しない動作異常のトラブルに見舞われた。本社のIT担当者に連絡したところ「ウイルス感染かもしれません……。そちらに伺いますのでパソコンの電源を切り、社内ネットワークから切り離してください」と告げられ、電話が終わった。そして、IT担当者は工場へ向かう社用車のハンドルを握りながら、サプライチェーンを構成する取引先にウイルス感染が広がっていないことを祈った。

## サプライチェーン攻撃が2位にランク

M社は大手工作機械メーカーのサプライチェーンを構成する1社として、長年、工作機械の部品を製造してきた。サプライチェーンでは、製品の企画・開発から部材の調達、製造、物流、販売、決済まで企業の枠を超えて連携。大手から中堅・中小企業まで、さまざまな企業が自社の技術力や得意分野を生かしながらチェーンの一端を担う。

そのサプライチェーンを狙った攻撃が深刻になっている。IPA(独立行政法人情報処理推進機構セキュリティセンター)が公表している「情報セキュリティ10大脅威2024」(組織)では、1位の「ランサムウェアによる被害」に続き、「サプライチェーンの弱点を悪用した攻撃」が2位にランクされている。これは攻撃者が標的とする企業・組織のセキュリティ対策が強固で直接的な攻撃が難しくなり、対策が脆弱な企業を踏み台にして間接的に標的の企業を狙うものだ。サイバー攻撃の踏み台となった企業は、サプライチェーンを構成する他の企業にもウイルス感染や機密情報の窃取といった被害を広げるなど、意図せずに加害者となる恐れがある。

攻撃者はセキュリティ対策が脆弱な企業を狙い、ターゲットとする企業の機密情報を盗み取るケースもある。例えば、顧客企業のWebサイトのコンテンツ制作・運営を担う業務委託先のセキュリティ対策が脆弱だったことから、委託元のWebサイトのシステムが不正アクセスされ、顧客情報が流出。顧客の個人情報がフィッシングサイトやマルウエア攻撃に悪用されるといった事案もある。業務委託先のセキュリティ対策の不備は業務委託元の企業のみならず、顧客にも被害が及ぶことになる。

## 委託元の要請に応えられない企業は取引停止も… 続きを読む