事例で学ぶセキュリティインシデント（第1回）

端末の隔離など的確な対応でランサムウエア感染拡大を防ぐ

2023.06.27

「あれっ、おかしいな。パソコンが動かない。フリーズでもしたのかな」

出社後、パソコンの異変に遭遇したのは、西日本に工場がある自動車部品メーカーA社の設計担当者だ。程なくその理由が分かった。パソコン画面に「ロックを解除してほしければ指定の宛先に暗号資産のビットコインで振り込め」と表示されたからだ。設計担当者はすぐに本社の情報システム担当者に電話をかけて状況を説明した。情報システム担当者はそのパソコン画面を確認しなくても、ランサムウエアに感染したことを理解した。

「対岸の火事」では済まされない―ランサムウエアの感染被害

ランサムウエアはパソコンやサーバーにウイルスを感染させ、端末のロックや、端末内のデータ、ファイルを暗号化して使えなくするサイバー攻撃だ。攻撃者はロックの解除やデータの復号化と引き換えに暗号資産などの金銭を要求することから、身代金要求型ウイルスとも呼ばれる。攻撃者の手口も巧妙化しており、企業・組織の機密データを盗み取った後に暗号化し、身代金を支払わないと機密データをネット上に公開すると脅迫するケースもある。

国内でもランサムウエアの感染被害は後を絶たず、「対岸の火事」とは言っていられない状況だ。医療機関のシステムがランサムウエアに感染し、患者の電子カルテが暗号化され、診療業務に支障を来すといった例も報告されている。

インシデント対応で重要な初動対応… 続きを読む