

サイバー対策4割危険性

大企業、システム更新遅れ

日本を代表する大企業の多くが、サイバーセキュリティ対策が不十分であることが分かった。日本経済新聞が診断ツールで日経平均を構成する225社を調べたところ、サイバー攻撃（3面きょうのことば）を受ける危険性がある企業は4割弱に上り、米国の主要500社より高かった。自動車や機械など大規模製造業が低評価を受けた。工場などの製造現場に残る古いシステムのネットワーク環境や情報端末が弱点となる場合が多く、早期の改善が求められる。

車や機械目立つ

調査には米スタートアップのセキュリティ・スコアカード（SSC）が、年だけで世界の10000社以上を調査した実績を持つ。仏アクサやフィンランドのノキア、日本企業でも多くの業種で自社や取引先のサイバー対策を

把握するために利用して、SSCは2021年だけで世界の10000社以上を調査した実績を持つ。今回、4月1日時点の日経225の企業に対して、保有するウェブサイトを調査し、保有するウェブサイトを「一定の防衛ができていない」とする最上位のA評価は30%（68社）、課題がある「Bは33%（74社）」とされた。危険性がある「C以下は、Cが25%（57社）で、「高い危険性がある（D）」や、「早急に対応すべき（F）」もそれぞれ8%（19社）、3%（7社）と合計で4割弱あった。SSCによると、過去に最低のF評価を受けた企業は、実際にサイバー被害を受けた割合がA評価企業より7・7倍も高いという。危険性が高いと評価されたDやF評価の企業は、自動車や機械などの製造業で8割近くを占め

た。製造現場ではあらゆるモノがネットにつながる「IoT」が急速に普及し外部からの通信にさらされる一方、更新が難しいことから古いシステムを使い続ける場合が多くセキュリティ上の穴になりやすい。同様の調査を米国の主要株価指数「S&P500」に採用される500社で実施したところ、C評価以下が3割と、日本の大企業より少なかった。一方、日本企業が製造を委託することもあるタイの証券取引所の主要指数「SET100」の企業ではC評価以下が6割弱に上り、国ごに防衛力の差が出た。

サイバー攻撃者はこうした企業が抱える弱点を外部から収集した情報を基に標的を決める。セキュリティ監査に詳しい情報セキュリティ大学院大学の与儀大輔客員研究員は「露出している弱点を解消すれば攻撃に狙われにくくなり、取引企業からの安心感も確保できる。目に見える部分だけでも自社の対策を再点検すべきだ」と話している。（サイバーセキュリティエディター 岩沢明信）

許諾番号30088124 日本経済新聞社が記事利用を許諾しています。
2022年06月05日 日本経済新聞 朝刊 001ページ
©日本経済新聞社 無断複製転載を禁じます。