最新セキュリティマネジメント（第27回）

工場のスマート化に潜むセキュリティリスク

2023.08.21

製造業におけるDXの目玉の一つは工場のスマート化だろう。これにより生産性を上げた工場は「スマートファクトリー（工場）」と呼ばれる。具体的にはIoTやAIを駆使して、生産ラインや品質管理システムをネットワークで結び、生産業務の指標となる各種データの管理を効率化し、生産性を向上させていく。

しかし、スマート化と同時にセキュリティリスクも意識しなければならない。独立行政法人情報処理推進機構（IPA）では「スマート工場化でのシステムセキュリティ対策事例調査報告書」を公開し、リスクとその対策についての指針を示している。生産現場のスマート化を考える上で参考になるはずだ。

スマート化による潜在的なリスクを知る

IoTやAIといった新しいテクノロジーは生産現場を大きく変えようとしている。実際に、多くのIoT機器を導入し収集したデータをAIで分析、生産ラインの効率化を実現して大きな成果を上げている中小企業も次々と登場している。

だが、工場のスマート化は新たなリスクをもたらす可能性がある。その代表がセキュリティリスクだ。ネットワーク化を進め、自社の事業所や取引先などとも情報のやり取りを緊密にするようになれば、悪意を持った攻撃者に狙われやすくなる。万一、システムを乗っ取られたりデータを盗み出されたりすれば、大きな損害につながる恐れがある。

安心して利用できる情報化を支援するIPAでは、スマート化した工場である“スマート工場”におけるセキュリティについて具体的な対策への指針を提供するために、先進的なスマート工場の事例を調査して、セキュリティ対策の項目を整理した「スマート工場化でのシステムセキュリティ対策事例調査報告書」を2023年7月に公開した。

報告書の特徴は、国内のモデル事業者1社の実施内容を整理した上で、モデル事業者以外の国内企業8社の現状との差分などを踏まえて、観点や対策を追加して汎用性が高められている点にある。工場のスマート化を考える多くの製造業にとって、自社のリスクを洗い出すためのガイドラインとして活用できるだろう。

実施例などを参考に独自のガイドラインを作成

モデル事業者となっているのは、プリント基板を製造する事業部門があり、スマート化した専用の工場を保有している企業だ。報告書では、この事業部門におけるスマート工場の生産システムの設計開発から廃棄に至る各フェーズで、想定されるリスク、実施しているセキュリティ対策、効果などが項目別に述べられている。

モデル事業者の工場におけるスマート化の取り組みは以下の6つ。①RFIDによる部品管理、②3Dデータを用いた作業指示、③作業記録画像を用いた工程・作業改善、④モジュラー設計へのデータ活用、⑤工場シミュレーターを活用した生産計画最適化、⑥ロボットの活用だ。

こうした手段の活用を前提として報告書では、全体概要、企画、設計・開発、運転・運用、保守、廃棄といったフェーズごとに、実施例、関連帳票、必要度、脅威、実施例により低減されるリスクと残留リスク、スマート化に際しての考慮事項などが述べられている。

メインとなるのは設計・開発、運転・運用だが、実施例は細部にわたっている。例えば設計・開発の部分は、リスクやネットワーク、外部機器、計算機、制御機器などに分けられ、さらに「ネットワークへの対策」は「ゾーン分割と監視」「ネットワーク境界の保護」「無線LANへの対策」「不正機器接続への対策」にブレークダウンされている。

不正機器接続への対策では、実施例として「正規の機器と不正機器の識別」と「不正機器の排除や接続防止」の内容が述べられ、実施例によって「不正機器を経由した攻撃のリスクが低減できる」とする一方で、正規機器自体を踏み台にした攻撃を防ぐために「正規機器自体を堅牢化」する必要性を述べている。

さらに、「スマート化に際しての考慮事項」としては、IoT機器では不正な機器の入れ替えや内部ソフトウエアの書き換えが攻撃者によって容易に行われうるため、対策として「電子証明書等を利用した真正性の検証」などの実施が「有効である」など、スマート化に際して留意すべきポイントが述べられている。

報告書は項目数が多く記述内容も詳細だが、網羅性は高い。項目ごとに記載されている実施例やリスク、考慮事項などから自社に該当する部分を取り出せば、独自のセキュリティ対策ガイドラインを作成できる。せっかく生産性を向上させようと工場のスマート化を図ったのに、それがインシデントの発生要因になり経営に悪影響を及ぼしては意味がない。工場のスマート化に取り組むに当たって、事前にチェックして参考にしてほしい。