最新セキュリティマネジメント（第42回）

# スマート工場のセキュリティリスク

2024.11.18

2024年10月15日、独立行政法人情報処理推進機構（以下：IPA）は「スマート工場のセキュリティリスク分析調査」報告書第2版を公開した。スマート工場が持つセキュリティリスクの把握と対策を目的として2022年6月に公開した第1版に、制御システムの新たな課題を追記したものだ。本連載ではスマート工場のセキュリティリスクについて初めて取り上げるので、まずは初歩的なセキュリティリスクを紹介する。

## 設備のデジタル化はセキュリティリスクを伴う

生産現場をスマート工場に進化させていくのは、深刻な人手不足が避けられない日本の製造業にとって、競争力を左右する大きなテーマだ。スマート工場では品質向上、コスト削減、生産性向上などの目的を達成するために、IoT機器やセンサーなどから収集した情報を活用していく。

データの用途としては工場の見える化、分析や予測、遠隔制御などが想定され、今後はリアルと同じ状況をサイバー上に展開するデジタルツインや、AIによる自動運転などの高度化が進むと考えられる。しかし、そこにはデジタルだからこそのセキュリティリスクも潜んでいる。

スマート工場にはどんなリスクがあり、どんな対策を講じていくのかを解説した「スマート工場のセキュリティリスク分析調査」報告書第2版では、スマート工場の7つの実装モデルを提示し、それぞれについて検討するべき被害や脅威、対策、そして対策の実装例を解説している。

実装モデルとして、単一工場モデル、複数工場モデル、遠隔からのシステム監視と制御、遠隔からの設備の保守、遠隔からのソフトウエア更新、ロボットの利用、ドローンの利用という7つが設定されている。

現在スマート化されていない工場であれば、一足飛びに遠隔操作をめざすのは難しいだろう。ここでは単一工場モデルとロボットの利用の2つの実装モデルに絞り、想定されるセキュリティリスクと対策について紹介する。

## オフィスのICT環境と同レベルのセキュリティ対策が必要… 続きを読む