

ニューノーマル処方箋(第26回)

「スマート工場」でセキュリティ事故を防ぐためにはどうすれば良いか？

2024.01.19



< 目次 >

- ・スマート工場に求められるセキュリティ対策とは
- ・【課題1】工場の各地に配置されたIoT機器の安全をどうやって守る？
- ・【課題2】端末の利用者が「正しい」ことを、どうやって証明する？
- ・【課題3】委託先のセキュリティ対策にも要注意

スマート工場に求められるセキュリティ対策とは

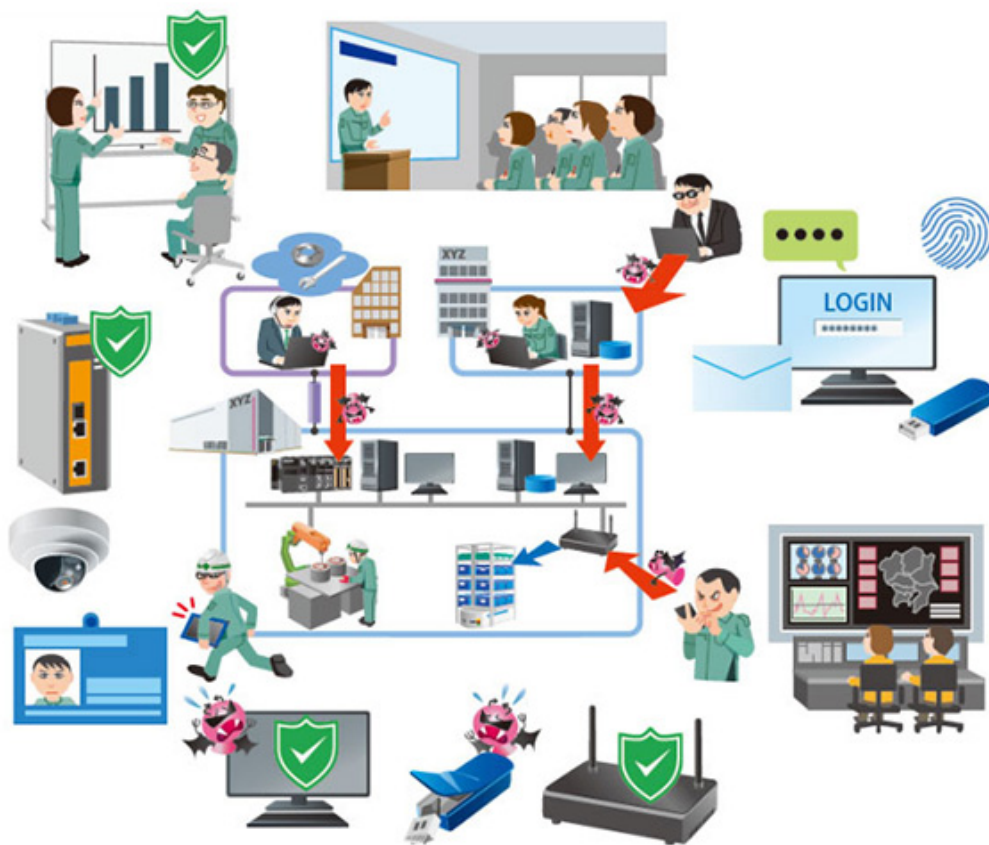
製造業の中には、自社の工場を「スマート工場(スマートファクトリー)」化した、もしくはこれからスマート工場化を検討している企業は多いかもしれません。

スマート工場とは、工場内の設備や機器にIoTやAI、クラウドサービスなどのデジタル技術を導入し、ネットワーク化した工場のことです。生産性の向上や省力化、設備管理の効率化が期待できるなどのメリットがあります。

しかし、工場のさまざまな機器がネットワークに接続されることで、従来では起こりえなかったセキュリティ事故が発生する恐れがあります。例えば、スマート工場内の機器が悪意のある第三者によるサイバー攻撃の被害に遭い、工場の操業がストップしたり、機密情報が盗まれたりする事態も起こりえます。スマート工場を安全に運営するためには、工場全体でセキュリティ対策を行っていく必要があります。

こうした事態に備え、経済産業省のIT政策実施機関であるIPA(独立行政法人情報処理推進機構)は2023年7月、「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」という資料を公開しました。IPAは本資料について、実際に先進的なスマート工場を運営しているある国内企業1社のセキュリティ対策を、IPAが“モデル事業者”として調査し、そのうえでモデル事業者“以外”の国内企業8社との差分や適合性を加味することで、より多くの企業が活用できるよう利便性を高めたもの、としています。

スマート工場に求められるセキュリティ対策とは、どのようなものなのでしょうか？同資料から読み解きます。



スマート工場に必要なセキュリティ対策のイメージ図(IPA「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」PDFより)

【課題1】工場の各地に配置されたIoT機器の安全をどうやって守る？… 続きを読む