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

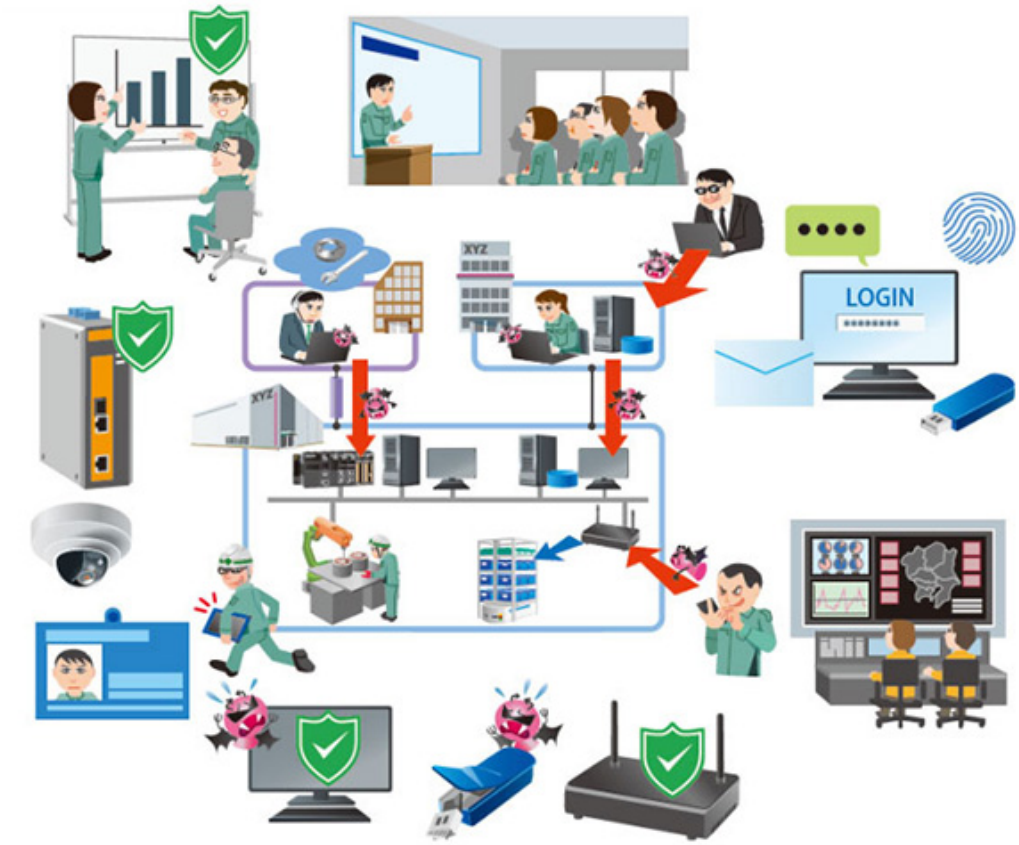
製造業の中には、自社の工場を「スマート工場（スマートファクトリー）」化した、もしくはこれからスマート工場化を検討している企業は多いかもしれません。

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？

資料によると、工場をスマート化する際、大きく3点の課題が発生するといいます。

まず1点目が「IoT機器の導入に伴う課題」です。工場のスマート化に伴い、工場内には多くのIoT機器が導入されることになります。そのため、IoT機器の入れ替わりや追加も度々発生することになりますが、一部のIoT機器には暗号化などのセキュリティ機能を持たないものもあるため、セキュリティ対策が必要になるといいます。

具体的な対策としては、無線の届く範囲を制限するなど、無線回線を秘匿化すること、利用可能な機器を一覧化し、許可された機器以外の通信を拒否するなど、利用機器を制限すること、強固なパスワードを使用し、危殆化（きたいか：安全だったものが危険にさらされること）されたアルゴリズムやプロトコルは利用できないよう通信を保護することが挙げられています。

パスワードについては、悪意のある第三者に推測されにくいよう、大文字と小文字の英字、数字、記号を必ず含めて8文字以上にするなど、一定以上の複雑さが求められます。パスワードを設定・入力する際は、入力する人間の背後にいる人間に入力内容を読み取られないよう、画面上に入力文字を表示させないなどの配慮も必要といいます。

IoT機器は、従来のパソコンやサーバーと比べ消耗が早く、交換のスパンが短い場合が多いため、資産管理の情報に、機器の借用期間や借用元、交換時期といった情報も記載することが望ましいとのことです。こうしたIoT機器の管理のためには、自動化ツールの導入が必要になる場合もあるとしています。

【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？

2点目が「複雑かつオープンな通信の増加に伴う課題」です。スマート工場内では、タブレットやノートパソコンのようなリモート端末を無線接続したり、クラウドに接続する機器を使用したりするため、ネットワークの構成はどんどん複雑化していきます。

これらリモート端末を利用する際は、ユーザーが正しい利用者であることをシステム上で証明するため、多要素認証を必ず実施し、一定回数認証に失敗した場合は、アカウントロックを行うことが推奨されています。加えて、一定時間操作されていないリモート接続についてもロックを掛け、再度認証しないと操作ができないようにすべきとしています。

工場内で定常的に稼働しない端末がある場合、その端末の存在を見落としてしまうことで、データの改ざんなどのサイバー攻撃に悪用される恐れもあるといいます。端末の管理は特に注意して行うべきといいます。

【課題3】委託先のセキュリティ対策にも要注意

3点目が「新たな脅威の増加」という課題です。

ここでいう“新たな脅威”とは、IoT機器を狙った脅威だけでなく、委託先など外部企業への業務委託が増えることによるサプライチェーンの脅威も含まれます。対策としては、業務委託先の企業と交わす契約書に、セキュリティに関してどのように取り組むのか、具体的な内容を記載する必要があるといいます。

その内容としては、委託に利用する機器一覧の提示、委託に利用する機器のマルウエアスキャンの実施やスキャン結果の提示、情報の機密保持や目的外使用の禁止といったセキュリティ上の責務や、その責務に違反した場合の罰則事項などが挙げられます。作業時における留意事項の周知といった内容も、契約書に記載すべきとしています。

資料ではその一方で、「すべての取引先や製品・サービスに完全な要求や検証を求めることは現実的ではなくなる」ともしており、こうしたサプライチェーンに対するセキュリティの内容は業務の重要度を加味して設定すべきともしています。

スマート工場は、十分なセキュリティ対策の上においてはじめて成り立つものです。セキュリティ対策がおろそかなままでは、工場のあらゆるポイントが悪意のある第三者の攻撃にさらされることになります。

すでにスマート工場化に成功した企業も、まだこれから取り組みを始めるという企業も、IPAが発表したこの報告書に目を通しておくことで、サイバー攻撃の被害を未然に防ぐことができるでしょう。