短期集中連載

はじめてのハードウェアセキュリティ活用法
～生産現場のIoT化のためのリスク対策～

第1回　IoT化に伴うセキュリティリスク

製造業の生産現場でIoT（モノのインターネット）化が進んでいる。システムは情報系と同様に標準化され、設備同士や外部ネットワークともつなぎやすくなった。半面、ハッキングによるデータの改ざんや破壊、IP（知的財産）の盗難などのセキュリティリスクも高まっている。これらのリスク対策としてよく知られるのが、ウィルス対策ソフトや不要な通信をブロックするファイアウォールなどのソフトウェアによる対策だが、ここにきて注目されているのが、生産設備や組込みシステムをより強固に守る「ハードウェア」による対策である。

本号から3回にわたり、生産現場のIoT化に伴うリスク問題とハードウェアセキュリティによる対策法を初心者向けに解説する。

ネットワーク化の加速とそこに潜むリスク

「日本の工場はすでにオートメーション化されているので、IoTなどは要らない」。ひと頃は製造業の管理職や生産現場の人たちの間で、そんな声さえ聞かれた。また、「サイバー攻撃や不正操作の標的とされるのは情報系のシステムだけ。インターネットにさえつながなければ、安全だ」と考える人は少なくなかった。そして、生産システムは外部ネットワークと接続されない閉ざされた環境で運用され、実際に外部からの被害に遭うことは少なかった。

しかし、日本の生産現場のようなシステムは、世界的に見れば異例であり、諸外国の企業では情報系のシステムだけでなく、工場の生産システムも早くからネットワークに接続して使用することで生産効率を高めていた。

国内で変化が現れたのは数年前のことだ。製造業の経営者たちが国際競争力の低下に危機感を持ち始めたのと同じ時期に、IoTやインダストリー4.0（IT導入による第4次産業革命）などの概念が紹介され、脚光を浴びるようになった。それを機にオープン化の流れが一気に加速し、情報系のシステムと同様、生産システムでも産業用PCをはじめ、生産設備を動かすためのPLC、さらにはロボットやセンサ、アクチュエータまで、組込みコンピューティング・システム（以下、組込みシステム）によって制御された多くのデバイスや装置がネットワーク化される時代となった。

ネットワーク化によって外部との接続が容易になり、ユーザーの利便性や快適性は高まり、生産現場の革新も始まっている。半面、接続が容易ということは、外部からの侵入も容易になるということである。実際に、生産システムを標的とした情報収集や不正操作を行う巧妙なマルウェア（悪意のあるソフト）が発見されるようになり、外部からの攻撃に対するセキュリティ対策の必要性が高まっている。

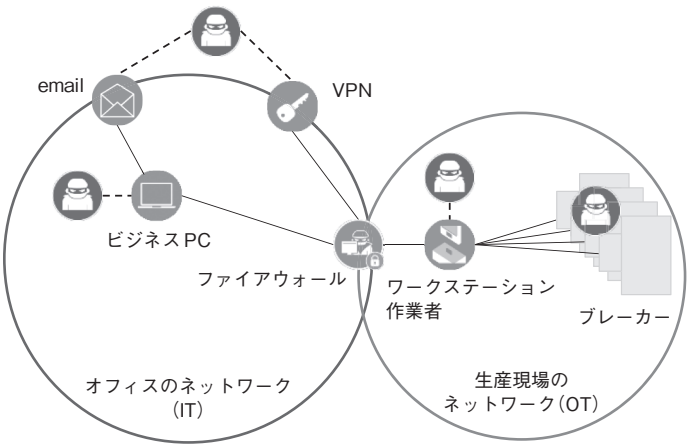
産業用設備が甚大な被害に

産業用設備がサイバー攻撃によって甚大な被害を受けた例として記憶に新しいのは、ウクライナのパワーグリッド（電力会社）が電力網のネットワークをハッキングされることによって、ブレーカーが落ち、大規模な停電が起きた事件である。こ

の施設では2015年暮れと16年暮れの2度にわたって被害に見舞われた。

この施設のシステムは、オフィスネットワーク(IT)と現場のネットワーク(OT)に分かれ、両者の間にはファイアウォール(システムを保護するソフト)が存在した(**図1**)。

図1　ウクライナの電力網がハッキングされた経路※



被害の発端は、オフィスのPCにウィルスソフトが添付されたEメールが送られてきて、それを開いたことでPCにマルウェアがインストールされてしまったことと考えられている。問題のウィルスは、キーストロークのログ(キーボード入力の記録)を読み取るマルウェアだった。キーストロークログを取ることでVPN(仮想専用ネットワーク)のIDパスワード、さらにはファイアウォールの設定変更などが行えるIDパスワードなどを取り、ファイアウォールをこじ開けた。ファイアウォールを開けることによって、現場のワークステーション上にあった機器を制御するプログラムを書き替え、ついにはブレーカーを落としたのである。

インターネットにつながってないにも関わらず、わずかなスキを突かれて工場全体がパニックに陥ったケースもある。2010年、イランの核燃料施設の制御システムがウィルス(スタックスネット)に攻撃され、8,000台以上の遠心分離機のすべてが稼働不能状態に陥った。この事件の原因として、最も可能性が高いと考えられているのがUSBメモリに仕込まれたウィルスソフトの仕業である。USBメモリから侵入したウィルスにPCが乗っ取られ、誤動作を起こすコマンドにより機器の破壊が実行されたとされている。

これらはいずれも海外で起こった例だが、国内も例外ではなく、多くの企業が生産システムでマルウェア感染を経験。中には操業停止に追い込まれたケースも出るなど、被害の件数や被害額は急激に増えている。

一般的なセキュリティ対策

生産設備や組込みシステムへの攻撃が成功すると、ノウハウ、IP(知的財産)、顧客データ、プロセス・インテリジェンスといった機密情報が洩れる恐れがある。また、攻撃によって業務が中断すれば、事業の継続性を損ない、企業のブランド・イメージや業績、存続そのものが危険に晒される。その対策として最も一般的なのが、ユーザー認証と鍵の管理、データの暗号化などを基本とするソフトウェア・ソリューションの導入であろう。

ただし侵入者によってさまざまな手口があるため、ソリューションといっても、1つのツールで完結するものではない。代表的なものに、管理用PCやPLCなどにインストールして、マルウェアの侵入を防御する制御PC向けウィルス対策ソフトや情報システム部門などで広く使われている不要な通信をブロックするファイアウォール、そして許可リスト以外のアプリケーションの起動を禁止する利用アプリケーション制御ソフトなどがあり、実際にはそれらを組み合わせて使用している企業が多い。

しかし、ソフトウェアは比較的容易に読み出して複製や配布ができるため、それだけでは組込みシステムを守るのは不十分である。実際に、ウクライナのパワーグリッドでもイランの核燃料施設の制御システムでも、ファイアウォールを使用し