インダストリ4.0の加速：産業用制御システムのセキュア・エッジを拡張する

著者：Erik Halthen
Analog Devices, Inc.

産業用制御システムに求められるサイバー・セキュリティ

インダストリ4.0は、ある要因が理由となって普及が滞る可能性があります。その要因とは、産業用制御システム（ICS：Industrial Control System）のサイバー・セキュリティです。多くのビジネス・リーダーは、ICSのサイバー・セキュリティの複雑さが数多くの要素によってもたらされていることから、それに関する課題について理解するのは難しいと感じています。また、ICS向けソリューションの開発に携わっている技術者は、重要なサイバー・セキュリティの要件はデバイスのレベルで満たすべきだという意識に欠けているようです。従来は、ICSを保護するために、ネットワークやデバイスに対するアクセス制限と、ITソリューションを介したネットワーク上のトラフィックの監視を主要な方法として採用していました。また、工場でデバイスを扱っているプロダクト・リーダーは、サイバー・セキュリティはITに関する問題として容易に解決できるものだと考えています。しかし、ICSを保護するための従来の方法は、インダストリ4.0の導入が迫ってきている現在では、もはや十分なものだとは言えません。企業は、デバイスのセキュリティについてはエッジで対応するという戦略を持たなければならなくなっています。そうしなければ、ICSのサイバー・セキュリティという課題がインダストリ4.0の普及を遅らせることになるでしょう。インダストリ4.0を採用し、実際に活用するためには、サイバー・セキュリティをビジネス・プランの重要事項の1つとして位置づける必要があります。

アナログ・デバイセズは、インダストリ4.0によって市場にもたらされる課題について、既に認識しています。産業分野向けの市場は、従来から変化を受け入れるまでに大きな時間を要していました。しかし、インダストリ4.0の導入は、予想を超える記録的なペースで進んでいくはずです。このような大きな変化を迎えるなか、サイバー・セキュリティは、インダストリ4.0の普及を妨げかねない非常に高い障壁の1つとなっているのです。工場をセキュリティに関する危機から保護するために、ICSのサイバー・セキュリティに関する規格やガイドラインを整備したり、確立したりといったことが行われています。しかし、インダストリ4.0のイニシアティブの確立を加速させる方法についてのガイダンスは提供されていません。従来からのセキュア・エッジを拡張し、セキュリティを確保するための機能の実装を容易化して、顧客が速やかにインダストリ4.0に対応するソリューションを採用できるようにすることが当社の使命です。

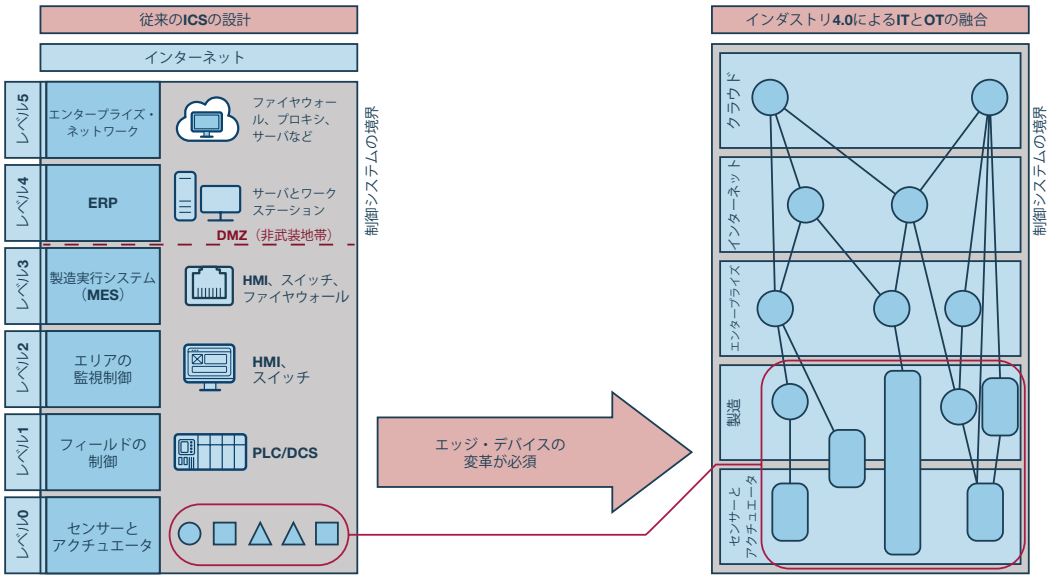

図1. インダストリ4.0の導入前後。
インダストリ4.0を採用するためにはエッジ・デバイスの変革が必要になります。

インダストリ4.0がICSのサイバー・セキュリティにもたらす変化

インダストリ4.0により、ICSのサイバー・セキュリティに変化が求められることには理由があります。インダストリ4.0の本質は、工場においてアクセスの対象となり得るデバイスを増やし、制御に対するアクセシビリティを高めることです。つまり、データへのアクセスを増やすことによって、透過性を高め、ネットワークに関する計画の必要性を軽減し、CapEx（設備投資費）やOpEx（運営費）を削減し、帯域幅を改善し、マシンの相互作用を最適化するということです。そのような手法によって、制御に対するアクセシビリティを高めるということは、工場のシステムに対するサイバー・セキュリティのリスク・アセスメントに変化が生じるということを意味します。ICS向けのサイバー・セキュリティ・ソリューションは、変化するリスクに適応できるものでなければなりません。システムにファイヤウォールを適用したり、施錠した部屋にデバイスを設置したりといった従来の対策は、インダストリ4.0の目的とは相容れないものであるように感じられます。言い換えると、セキュアな方法で機能を増やすことができるようにするために、より厳しいセキュリティ対策を施したデバイスを選択する必要があるということです。データの信頼性を高め、セキュアな運用を可能にするためには、現場のあらゆるデバイスにおいて、アイデンティティと完全性（インテグリティ）を中核的な存在として位置づける必要があります。

産業分野の市場に向けて、ICSにセキュリティ関連の機能を実装する際のガイダンスとなる様々な規格が定められています。例えば、米国では、NIST（米国立標準技術研究所）からセキュリティ機能に関するガイダンスが提供されています。欧州の管理下では、国際市場に向けたセキュリティ向けの規格として、IEC 62443が策定されています。これら2つが最も有力な規格です。いずれも、ICSにセキュリティ機能を実装したり、セキュリティに対応するための体制を評価したりする際に役立つガイドラインとなっています。但し、インダストリ4.0の採用を加速させる方法についてのガイダンスは提供されていません。現在、IEC 62443には、PLC（Programmable Logic Controller）より下位のレベルを対象としたセキュリティ機能の実装に関するガイドラインが存在しません。そこで、IEC 62443の枠組みの中で、工場の最下位のレイヤにおけるサイバー・セキュリティに対応することを目的とし、ISA99に作業部会が設立されました。システムに必要なセキュリティ体制を構築するうえで、十分なセキュリティ・レベルに達していないデバイスがあれば、対策を講じなければなりません。一般に、そうした対策は、アクセスを制限したり、脆弱なデバイスを分離／隔離するファイヤウォールを使用したりする方法に依存しています。将来、インダストリ4.0に移行できるように、デバイスのセキュリティ・レベルをより高いレベルに引き上げる必要があります。

ICS向けのセキュア・エッジを拡張するアナログ・デバイセズ

アナログ・デバイセズは、独自の立場からセキュア・エッジの拡張に取り組んでいます。これまで、当社は、現実世界の情報をデジタル・データに変換する物理エッジを主な対象領域としてきました。このことから、当社であれば、アイデンティティと完全性を、シグナル・チェーンのかなり早い段階で提供することによって、データの信頼性を確立するということを実現できます。つまり、当社は、セキュア・エッジの新たな定義を確立するチャンスを手にしているということです。従来のセキュア・エッジは、ICSでセキュリティに対応するための枠組みに含まれるゲートウェイやPLC、サーバを起点にしていました。

このような視点は、従来の工場に配備されていたITシステムのサイバー・セキュリティに関する視点を思い起こさせます。実際、このような視点は業界全体に根強く残っています。シグナル・チェーンの中で、セキュア・エッジを下位のレイヤに設けることには、大きな魅力があります。データを基にして行われる意思決定の信頼性を高めることができるからです。アイデンティティと完全性の確立がシグナル・チェーンのなるべく早い段階で行われるほど、意思決定を後押しするデータの信頼性と確実性が高まります。

ICSのサイバー・セキュリティに対応可能な万能のソリューションというものは存在しません。システムのリスク・アセスメントに基づき、きめ細かなアプローチを採用／適用する必要があります。多くの場合、エッジではイーサネットが採用されることになります。この点に注目し、アナログ・デバイセズは、ICSのサイバー・セキュリティをより高度に拡張するための戦略を構築しています。

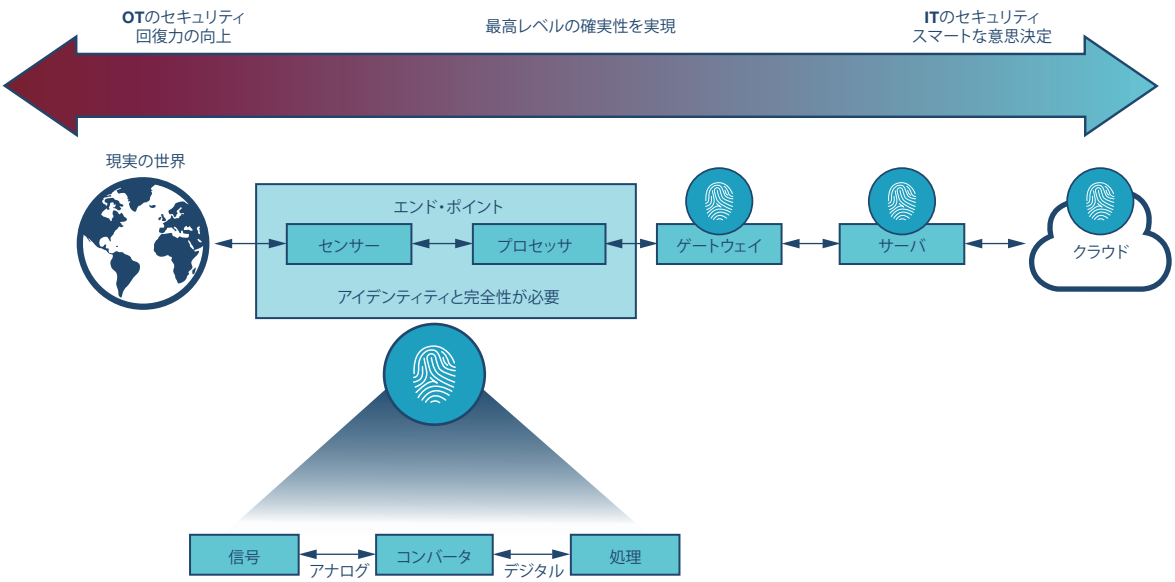

図2. 物理的な情報からデジタル・データへの変換が発生する場。
意思決定において最高の確実性を得ることが可能になります。

インダストリ4.0の導入を可能にするには、工場に新しい接続方法を導入する必要があります。このことは、ICSにおいて大きな役割を担っているイーサネットが、今後もそうした役割を担い続けるということを意味します。アナログ・デバイセズのセキュリティ戦略は、イーサネットによる接続に重点を置いています。その理由は、通信プロトコルによって、ネットワーク上のすべてのデバイスがシステムに対して及ぼす影響が大きく変化するからです。当社の既存の産業用イーサネット・ソリューションや、IEEE 802.1 TSN（Time Sensitive Networking）ベースのソリューションは、セキュリティに関する開発に重点を置いて構築されています。そうした製品ファミリの1つに、2ポートでマルチプロトコルの接続に対応するRapID®ベースのプラットフォーム「fido5000」があります。この製品ファミリは、ネットワーク経由の攻撃からの防御を実現するために、キーの生成／管理、セキュア・ブート、セキュア・アップデート、セキュア・メモリ・アクセスといったセキュリティ機能を提供します。その開発ロードマップには、ハードウェアの「信頼の基点（Root of Trust）」、セキュア・デバイスのライフサイクル管理、セキュアな通信と相互認証、タンパ・プロテクションを備えた、シングルチップのソリューションが含まれています。産業界では、今後もインテリジェント化されたセンサーの採用が続くでしょう。そのため、工場の下位のレベルまで接続性が拡張され、デバイスのレベルでのセキュリティ要件が更に追加されていきます。アナログ・デバイセズは、インダストリ4.0の普及を加速するために、ICSで活用するためのセキュリティ・ソリューションを容易に採用でき、エッジでの信頼性を確立することが可能なセキュアなポートフォリオの開発に取り組んでいきます。

著者について

Erik Halthen（erik.halthen@analog.com）は、2016年にアナログ・デバイセズがSypris Electronics社のサイバー・セキュリティ・ソリューション事業部門を買収したことに伴い転籍しました。アナログ・デバイセズのサイバー・セキュリティ・ソリューションの開発に対し、広範な知識を基に大きな成果をもたらしています。具体的には、アナログ・デバイセズでサイバー・セキュリティを担当する中心人物の1人として、産業用ソリューション向けのセキュリティ・システム・マネージャを務めています。特に、防衛業界におけるサイバー・セキュリティ・プログラム・マネージャとしての経験を活かし、最新のセキュリティ・ソリューションの開発や、インダストリアルIoTに対する市場の主要な要求を満たすべく取り組みを行っています。

オンライン・サポート・コミュニティ

EngineerZone™ SUPPORT COMMUNITY

アナログ・デバイセズのオンライン・サポート・コミュニティに参加すれば、各種の分野を専門とする技術者との連携を図ることができます。難易度の高い設計上の問題について問い合わせを行ったり、FAQ を参照したり、ディスカッションに参加したりすることが可能です。

ez.analog.com にアクセス

＊英語版技術記事はこちらよりご覧いただけます。

アナログ・デバイセズ株式会社
本　　社 〒105-6891　東京都港区海岸1-16-1　ニューピア竹芝サウスタワービル10F
大阪営業所 〒532-0003　大阪府大阪市淀川区宮原3-5-36　新大阪トラストタワー10F
名古屋営業所 〒451-6040　愛知県名古屋市西区牛島町6-1　名古屋ルーセントタワー38F

TA20848-0-12/18

www.analog.com/jp

ANALOG DEVICES
想像を超える可能性を
AHEAD OF WHAT'S POSSIBLE™