Deloitte.
デロイト トーマツ

安全神話の崩壊！

～甚大な被害をもたらす制御システムへのサイバー攻撃～

はじめに（制御システムのセキュリティに対する誤解）

これまでセキュリティといえば、情報の機密性、完全性、可用性の確保を目的として、主として情報システムを対象に対策を実施してきた。そんな中、昨今注目を集めているのが制御システムのセキュリティ（以下、制御セキュリティという。）である。

制御システムには、私たちの生活に欠かせない電化製品や自動車などで利用されている組み込み型の制御システムや、工場、プラント、発電所などで利用されている産業用制御システム（ICS：Industrial Control Systems）があるが、本稿における制御システムとは、後者を指す。

かつての制御システムは、インターネットや社内の情報システム環境とも切り離され、利用形態や稼働環境に応じた独自のハードウェア、ソフトウェア、通信プロトコルにより構成され、いわゆるクローズドな環境であった。そのため、ある企業のマネジメント層からは、工場のセキュリティ対策について次のような声が聞こえてくる。

担当役員

当社の工場はインターネットとはつながっていないから、セキュリティ対策は不要だ。

上記発言は、工場の“安全神話”を信じての発言と推察されるが、サイバー攻撃が高度化、巧妙化する時勢においてもその考えは通用するのだろうか。

本稿では、制御システムへのサイバー攻撃事例を紹介し、なぜ制御システムが狙われるようになったのか、その理由と共に、今後必要となる制御セキュリティ対策について解説する。

標的となった制御システム

前述のとおり、制御システムは工場、プラント、発電所など幅広い分野で利用されているが、制御システムに対するサイバー攻撃が行われた場合、その被害の大きさは計り知れない。従来の情報システムの場合、サイバー攻撃によるインシデント発生時の影響はプライバシーの侵害や経済的損失などにとどまっていた。一方で、制御システムに対するサイバー攻撃の場合には、経済的損失などに加えて環境汚染や最悪のケースでは、人命を脅かす危険性すらはらんでいる。

制御セキュリティの必要性が囁かれ始めたのは、2010 年頃のことである。制御システムを狙った初めてのマルウェアの登場により、国内外において制御セキュリティ対策が急務となった。以下では、過去実際に発生した制御システムに対するサイバー攻撃によるインシデント事例について、独立行政法人情報処理推進機構（以下、IPA という。）によって公開されている情報を基に紹介する。

事例 1）制御システムをターゲットにした初めてのマルウェア

2010 年 9 月、Stuxnet（スタックスネット）と呼ばれるマルウェアがイランの核燃料施設に持ち込まれ、遠隔監視制御用のコンピュータがこれに感染した。その結果、遠心分離機を制御する PLC（Programmable Logic Controller）の設定ロジックが改ざんされ、約 8,400 台の遠心分離機のうち約 1,000 台が稼働不能となり、一時操業が停止する事態となった。なお、当該 Stuxnet は、制御システムをターゲットにした初めてのマルウェアといわれている。

事例 2）エネルギーインフラ企業を襲うサイバー攻撃

2015 年 12 月、ウクライナの電力会社に対するサイバー攻撃では、大規模停電を引き起こし、発生から復旧までに最大で 6 時間を要し、およそ 22 万 5 千人の顧客に影響を与えた。また、翌 2016 年 12 月には別の電力会社に対するサイバー攻撃により、ウクライナ首都圏において、最大で 1 時間 15 分の停電が発生した。

事例 3）安全計装システム（SIS：Safety Instrumented System）※1 を狙った初めてのマルウェア

2017 年 12 月、Schneider Electric 社製の安全計装システム（Triconex）を狙った HATMAN（別名、TRITON あるいは TRISIS）と呼ばれるマルウェアにより、中東の石油化学プラントが緊急停止した。なお、当該 HATMAN は、安全計装システムを狙った初めてのマルウェアといわれている。

※1：プロセスの異常を検知した場合に安全かつ確実にプロセスを停止させることを目的とし、制御システムにおいて重要な役割を持つシステム。

事例 4）ランサムウェアによる操業停止

2019 年 3 月、ノルウェーに本社を置く世界有数のアルミニウム生産企業、Norsk Hydro が Locker Goga と呼ばれるランサムウェアにより、世界 40 か国 160 の拠点において、PC23,000 台のうち 11,000 台が感染、2,700 台が暗号化され、サーバ 3,000 台のうち 1,100 台が感染、500 台が暗号化された。これにより、長期間にわたる生産能力の低下、およそ 65 億円以上の損失を被ったと見積もられている。

紹介した事例はごく一部ではあるが、安全と考えられていた制御システムに対するサイバー攻撃は実際に発生している。では、なぜ制御セキュリティが脅かされる時代となったのか。その理由を紐解くカギは、上記 4 つの事例における制御システムへの侵入の手口にある。

キーワードは“制御システムのオープン化”

制御システムへの侵入の手口として、ある事例では標的型メール攻撃、またある事例では USB メモリ等の外部記憶媒体の利用など、いずれの事例においても制御システムへのサイバー攻撃の足掛かりとなったのは、本社で利用している業務用 PC や、制御システムと連携している生産管理システムなどの情報システムへのサイバー攻撃と考えられている。

クローズドな環境ということを最大の理由として工場は安全と考えられていたにも関わらず、その実態としては図 1 に示すように、様々な企業のニーズに外部環境の変化も相まって、制御システムはオープンな環境へと移り変わっていたのである。

1980 年代以降、UNIX サーバなどが普及した情報システムのオープン化に際し、様々なメリットを享受した一方で、セキュリティ面については大きなデメリットとなった。このことは制御システムについても同様であり、制御システムのオープン化が進むにつれ、それに伴うセキュリティリスクは増大している。要するに、制御システムの“安全神話”は既に崩壊しているのである。

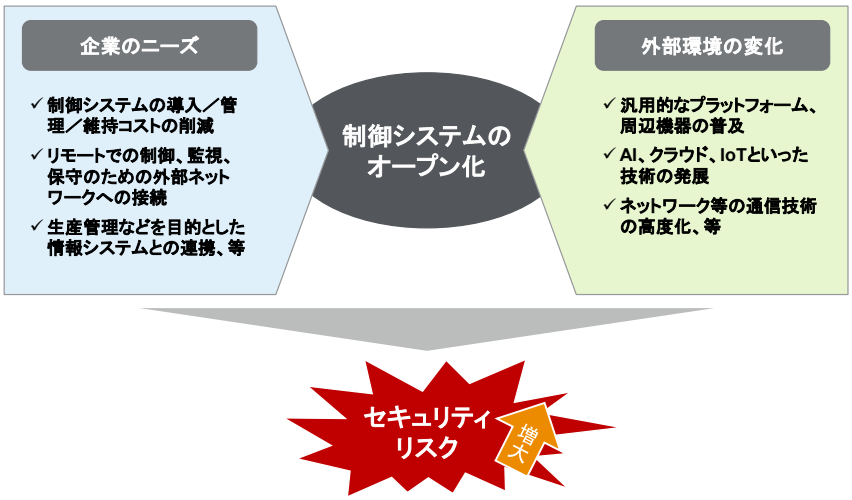

図 1 ：制御システムのオープン化とセキュリティリスクの増大

ここで、制御システムのどの部分でオープン化が進んでいるのか、IPA による情報を基に解説する。図 2 に示すように、一般的に制御システムは多段階の階層構造となっており、制御情報ネットワーク、コントロール（制御）ネットワーク、フィールドネットワークの 3 つのセグメントに分かれている。

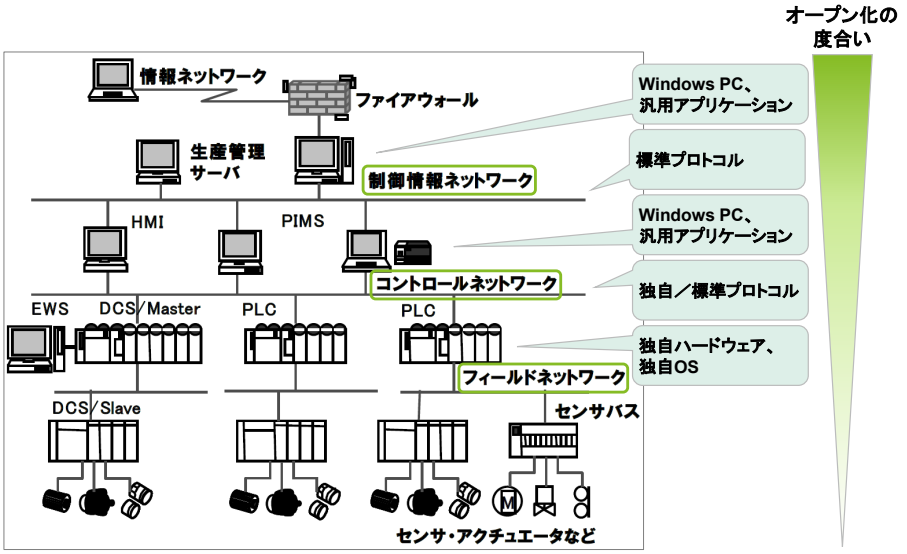

図 2：制御システムの構成例とオープン化の状況（IPA による情報を基に作成）

ポイントは、制御システムのネットワーク環境の 2 極化である。コントロール（制御）ネットワークを境として、これよりも上位のネットワークでは、Windows PC や汎用アプリケーション、標準プロトコルの利用など、オープン化が進んでいる一方で、下位のネットワークでは、未だ独自のハードウェア、OS 等が利用されていることが多い。

セキュリティの観点で考察すると、制御システムへのサイバー攻撃を成功させるための侵入の手口として、コントロール（制御）ネットワークよりも上位のネットワークが狙われやすい（リスクが高い）ということである。

このような状況を踏まえ、制御セキュリティではどのように対策を実施すべきか、対策を検討するにあたってのポイントと、具体的な対策実施にあたって参考とすべき規格、ガイドラインについて解説する。

情報セキュリティでの常識が通用しない制御セキュリティ

繰り返しになるが、これまでセキュリティといえば、主に情報システムを対象に対策が行われてきたこともあり、制御セキュリティについて前出の担当役員から、次のような声が聞こえてくる。

担当役員

工場のセキュリティ対策が必要なら、同じセキュリティなんだから、情報システムと同じ対策を適用すればいいじゃないか。

この意見は、半分正解で、半分間違いである。その理由は、制御システムのオープン化により、制御システムにおいても、OS として Windows や Linux 系が利用されていることや、インターネットや外部ネットワークへの接続が発生していることなど、これまで情報システムのセキュリティ対策で培ってきた知識や経験が活かせるという意味では正解。しかし、表 1 に示すように、情報システムと制御システムには相違点があることから、情報システムと全く同じセキュリティ対策ができるかというとそうではないため、間違いとなる。

表 1：情報システムと制御システムの相違点

	情報システム	制御システム
管理部門、主管部門	情報システム部門	製造部門、設備部門、技術部門
使用期間	3～5 年程度	10～20 年程度
システム構成	汎用プラットフォームを使用することがほとんど	専用プラットフォームを使用する場合が多い ※汎用プラットフォームの導入も増加
求められるセキュリティ要素 （表中の数字は優先順位を表す）	①機密性（Confidentiality） ②完全性（Integrity） ③可用性（Availability）	①可用性（Availability） ②完全性（Integrity） ③機密性（Confidentiality） 健康（Health）、安全（Safety）、環境（Environment）
通信	標準プロトコル	独自の専用プロトコル ※標準プロトコルの使用も増加
インシデント発生時の影響	経済的損失、信用損失	経済的損失、信用損失、 人的被害、環境破壊

例えば、セキュリティパッチの適用（更新プログラムの反映）を考えてみる。情報システムとは違い、制御システムで求められる最も重要なセキュリティ要素は可用性であり、通常 24 時間×365 日の稼働が求められている。

これにより制御システムでは OS の再起動ができず、情報セキュリティ対策としては一般的なセキュリティパッチの適用が難しくなる。これは一例ではあるものの、情報システムに対しては常識として考えられているセキュリティ対策であったとしても、制御システム特有の事情により、その常識が通用しないのである。

制御セキュリティ対策の検討を始める企業では、これまで情報セキュリティを担当していた人物を制御セキュリティの担当者として配置転換、あるいは兼務させるケースが多いと考えられる。そのような制御セキュリティの担当者は表 1 のような情報システムと制御システムの違いを念頭に置いたうえで検討を進めるとともに、次に紹介する規格、ガイドラインを参考に具体的な制御セキュリティ対策を実施することが望ましい。

制御セキュリティの代表規格「IEC 62443」

図 3 に示すように、制御システムに関するセキュリティ標準として、業種業界ごとに様々な規格、ガイドラインが存在する。これは、かつて制御システムが利用形態や稼働環境に応じた独自のハードウェア、ソフトウェア、通信プロトコルにより構成されていたことに起因していると考えられる。

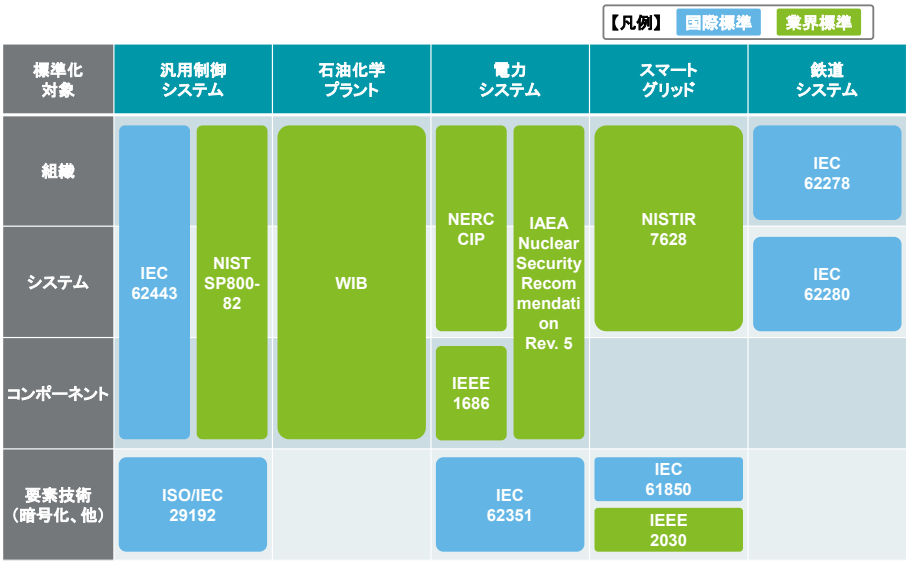

図 3： 制御システムに関するセキュリティ標準

そんな中、制御セキュリティの代表的な国際標準規格として知られているのが、IEC 62443 である。この規格は、制御システムのすべての機器、装置を対象にし、4 つのシリーズで構成されている。中でも特筆すべきはシリーズ 2 である。ここでは、産業用オートメーション及び制御システム（IACS：Industrial Automation and Control System）を対象としたサイバーセキュリティマネジメントシステム（CSMS：Cyber Security Management System）確立の要件が定められており、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）確立の要件を定めた ISO/IEC 27001 をベースに作成されている。加えて、IACS 分野では、CSMS 認証の仕組みが整備されており、その認証基準のベースとしても採用されている。そのため、全ての制御セキュリティ担当者が最初に手に取り、理解すべき規格として推奨したい。

以上、制御セキュリティ対策の必要性と対策実施にあたっての考え方について解説してきた。これらを踏まえて、冒頭の担当役員には次のような発言を期待したい。

担当役員

当社の工場はオープン化の波の中、サイバー攻撃のリスクにさらされており、セキュリティ対策が必要である。対策にあたっては情報セキュリティに関する知識・経験と工場の現場の理解をうまく掛け合わせることが肝要だ！

企業ニーズの多様化と技術革新などにより、制御システムオープン化の流れは今後ますます発展、加速することが予想され、当然それに伴う制御セキュリティも重要になる。

セキュアなスマートファクトリーを目指して！

スマートファクトリーをご存じだろうか。スマートファクトリーが注目を集めた契機は、ドイツが産学官一体となって推進している国家プロジェクト Industrie 4.0（第 4 次産業革命）である。簡単に説明すると、スマートファクトリーとは、生産能力の向上、コスト削減、品質向上などを目的として、AI やクラウド、IoT、ロボットなどの先端技術、ビッグデータなどを活用することにより最適化された工場をいう。

現在、日本では、人口の減少、超高齢社会による労働力の低下が深刻化しており、これは日本経済を支えてきたモノづくり産業にとっても大きな課題である。この課題を解決し、国際競争力を強化するためにも工場のスマート化は重要な経営戦略として考えられているが、忘れてはならないのが、セキュリティである。

工場に対するサイバー攻撃の被害が甚大であることを考慮すると、ともすれば、一瞬にして経営破綻を招くおそれもあり、工場のセキュリティ対策が十分でないにも関わらず、工場のスマート化を推進することは、そのリスクを軽視または無視しているとも受け取られかねない。

したがって、工場のスマート化に際して、セキュリティ対策を後回しにするのではなく優先検討事項とした上で、十分なセキュリティ対策が行われていることを前提に、セキュアなスマートファクトリーを目指していただきたい。

デロイト トーマツ サイバー合同会社
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】　東京・名古屋・福岡

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス　内容がご提供できない可能性があります。詳細はお問合せください。