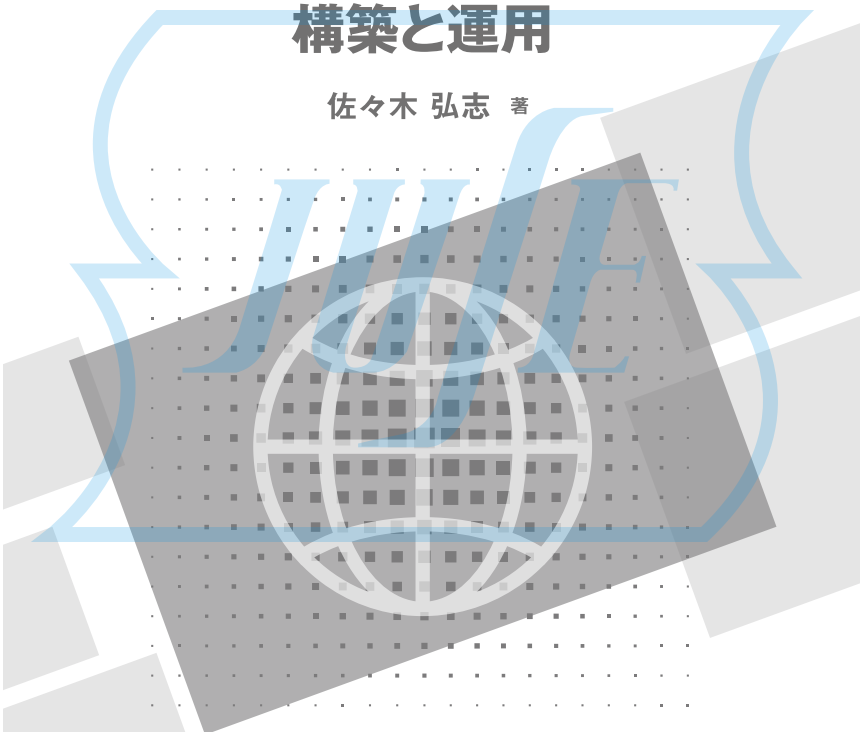
製造業のサイバーセキュリティ

産業サイバーセキュリティ体制の構築と運用

佐々木 弘志 著



日科技連

はじめに

世界的な新型コロナウイルス感染症拡大を受けて、ビジネス環境が激変する中で、製造業におけるデジタルトランスフォーメーション(Digital Transformation、以下 DX)の流れが加速している。製造事業者の情報システムは、これまでの自社でのデータ管理・開発を中心とした自前主義の考え方から、環境変化に機敏に対応できるように、クラウドサービスの活用へと移行しつつあるが、この大きな構造変化に伴い、クラウド上の重要データの保護などの新たなサイバーセキュリティの課題が生まれている。

また、一方で、工場やプラントの運用制御技術(Operational Technology、以下 OT[1])における IT 技術の活用が進み(OT の IT 化)、AI、IoT といった最新技術を活用することで、予知保全・歩留まり向上といった付加価値が生まれている。同時に、OT と IT の技術的、物理的なつながりが深まることによって、制御システムに対するサイバー攻撃の脅威が高まっている。

加えて、製造業が生み出す製品・サービスにおいても、単に製品を売るという一方向のビジネスではなく、顧客や異業種との双方向のつながりから生まれる価値をビジネスとする流れが進むことにより、多様なステークホルダーやシステムが、サイバー空間で相互につながることによって生まれる新たなサイバーセキュリティリスクや、サプライチェーンリスクの問題が顕在化してきている。

このように、サイバー空間上の組織やシステムを超えた「つながり」が、組織内の情報システムに留まらず、事業者のビジネス全体に拡大する中で、製造業のサイバーセキュリティ課題は、従来の「情報システム部門を中心としたセキュリティ体制」ではカバーしきれない事態となっている。

本書は、近年のビジネス環境変化に即した製造業のサイバーセキュリティ対策の全体像とそれを推進するための包括的・体系的な方法論、及び具体的な例

1) 運用制御技術(OT は IT との対比で制御システムの意で用いることが多い)

を示すことで、セキュリティ担当者が、場当たり的な対応から脱却し、経営層の理解や社内の関係者とともに、中長期的な対策へと転換を図るための指南書となることを目的とする。

2021 年 3 月

佐々木 弘志

製造業のサイバーセキュリティ
産業サイバーセキュリティ体制の構築と運用

目　次

装丁・本文デザイン＝さおとめの事務所

第1章

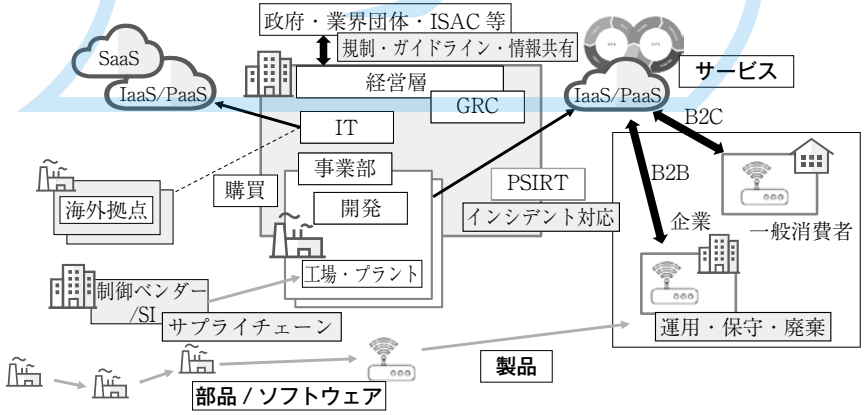
製造業のサイバーセキュリティ脅威

1.1　製造業のサイバーセキュリティ脅威の全体像

1.1.1　サイバーセキュリティ管理範囲の増大

本節では、製造業のサイバーセキュリティ脅威が、DX(Digital Transformation)の進展に伴い、情報システムだけではなく、ビジネス全体に広がっていることを示す。

一般的な製造事業者は、家電、産業機械、車載、化成品のような各事業分野に対応する事業部門を有しており、それぞれの事業部門に開発部門と、製品を製造する工場・プラントがある(図 1.1)。「IT(Information Technology)」はメール、Web アクセス管理、業務管理などの情報システムを表しており、IT 部門配下のセキュリティ部門が主管となっている。



GRC：Governance Risk Compliance(ガバナンス・リスク・コンプライアンス)
PSIRT：Product Security Incident Response Team(ピーサート)

図 1.1　製造業を取り巻くサイバーセキュリティ管理範囲の拡大

また、海外拠点(営業所・生産拠点など)も、WAN(Wide Area Network)で本社 IT とネットワーク接続していることが多いため、セキュリティ部門の管理対象であるが、拠点の端末などのセキュリティ管理は、現地法人任せになっている場合が多く、十分なガバナンスが効いているとはいえないことが多い。最近は、海外拠点の侵入をきっかけにサイバー攻撃の被害に遭う事案が増えており、経済産業省からの注意喚起が出される事態となっている[1]。

ひと昔前の製造業が管理すべきセキュリティ対象といえば、この「IT」と「海外拠点」がメインであり、経営層が、事業者全体のセキュリティリスクを知りたければ、セキュリティ部門に聞けばよかった。しかし、DX 推進やビジネス環境の変化に伴い、従来のセキュリティ部門の管轄外のセキュリティ脅威が増えてきており、リスク管理対象も拡大している。

1.1.2　実際に起こったサイバー攻撃

「工場・プラント」の制御システム(OT：Operational Technology)は、省人化、歩留まり向上、予知保全[2]などの目的で、IoT、AI の導入が進み、これまで、ほとんど外部ネットワークと接続していなかった工場・プラントがサイバー攻撃にさらされる機会が増えてきた。

工場やプラントで用いられている産業制御システムは、専用機器や通信プロトコルを用いており、サイバー攻撃を受けにくいとされていたが、2010 年にイランの原子力施設の遠心分離機を破壊するマルウェアが登場して以降、制御システムを対象とした実被害を伴うサイバー攻撃が発生するようになった。その代表的な例としては、2015 年、2016 年に発生したウクライナにおける電力設備へのサイバー攻撃による停電があげられる。

また、2019 年にノルウェーのアルミ製造会社がランサムウェアの被害に遭った際には、制御システムへの感染はなかったものの、生産にかかわる情報システムがマルウェア感染した結果、生産に影響が出ており、OT が IT に依存する度合いが高まっていることの証左といえる。

さらに、製造事業者が製造する製品そのものにも DX 推進の波は押し寄せている。製造事業者は、グローバルの激しい競争にさらされる中で、単なる「モノ」売りではなく、「コト」売り(サービスや体験を売る)にビジネスモデル

2)　予知保全：工場のラインの機器が壊れる前に、機器にセンサーを取り付けて振る舞いを監視することで、不具合を予見して故障する前に対応すること

をシフトすることが急務となっている。そうでなければ、クラウドサービスを提供するGAFA[3]などのプラットフォーマーにビジネス価値の大半を支配され、「モノ」である製品は単なるサービス実現のための従属物として、コスト競争にさらされることが目に見えているからだ。

したがって、IoT家電のように、「モノ」を売ったあとに、どれだけビジネスを生み出せるかが鍵となっており、そのため製品自身がインターネット接続して自社管理のWebやスマートフォンのアプリと連携したり、他社サービスと連携したりすることで、新たな価値を生み出している。

しかし、このようなIoT機器がクラウド上のサービスと連携することで、機器・クラウドに対するハッキングからの情報漏えいや、機器が攻撃者に乗っ取られてDDoS[4]攻撃の拠点とされるなどの事案が発生している。

1.1.3　サプライチェーンの脅威

また、このような“つながる社会”が進む過程で、製造事業者にかかわる「サプライチェーン」のセキュリティ脅威が増大しており、重要なセキュリティの管理領域として注目されている。

製造事業者におけるサプライチェーンのセキュリティ管理は、自社のビジネス活動に利用するリソースの調達である「サプライチェーン上流」と、自社の製品・サービスの顧客向けのセキュリティ対応である「サプライチェーン下流」に分けられる。このうち「サプライチェーン上流」に関していえば、さらに、社内システム(IT/OT)向けのサーバ、ルーター、業務アプリケーション、制御機器などの調達と、自社の製品・サービス向けに組み込んで利用するソフトウェア・クラウド基盤などの調達に分けられる。これらの調達物にバックドアが仕掛けられ、社内の機密情報や、顧客の重要情報が漏えいするといった脅威への対応が、国際的な課題にまで発展している。

例えば、米国を始めとした国々が、中国製の通信機器の政府調達を禁止するといった動きや、EUにおいては、製品・サービスにおけるセキュリティの製品認証の枠組みが検討されるなどの規制的な動きが進んでいる。

一方、「サプライチェーン下流」のセキュリティ管理とは、顧客からのセ

3)　GAFA：Google、Amazon、Facebook、Appleに代表される米国の巨大IT企業の総称
4)　DDoS(ディードス、Distributed Denial of Service)：分散サービス拒否攻撃。大量の拠点から1つのサービスに、一斉にサービス要求を行い、サービスをダウンさせるサイバー攻撃

キュリティに関する要求や問合せ・インシデント発生に対応することである。自社の製品・サービスがネットワークにつながることによって、セキュリティインシデント発生のリスクが高まるため、必然的に、顧客へのセキュリティ対応体制の重要性が増すことになる。

このように、製造業のサイバーセキュリティ脅威が、組織内外での広がりを見せるなかで、特に、制御システムに対するセキュリティ脅威は、情報システムとは異なる特徴をもっているため、独自の経緯をもって発展してきた。次節以降は、「制御システム」に関するセキュリティ脅威について詳しく説明する。

1.2　制御システム

1.2.1　制御システムの環境変化

産業制御システムは、古くは、リレー回路やタイマー回路といった、いわゆるアナログ回路で構成されていたが、1960 年代頃から、デジタルコンピュータや PLC（Programable Logic Controller）が登場し、アナログ回路をデジタル化することによって進化を遂げてきた。この頃には、まだ情報システムとの境界もあいまいであり、もちろんマルウェア[5]も存在していなかった。

しかし、1990 年代以降、情報システムが、個人向けのデスクトップパソコン（Windows シリーズ）、インターネットを活用した Web、メールシステムなどの広がりにより急速に発展を遂げる中で、制御システムを取り巻く環境も大きく変化してきた。それは、以下の 3 点に集約できる。

① 制御システム間の通信インタフェースのイーサネット化
② 制御システムの汎用 OS 化（Windows Embedded、Linux などの利用）
③ 制御システムとインターネットとの接続

「制御システム間の通信インタフェースのイーサネット化」による環境変化については、多くの制御システム技術者が肌で感じているところだろう。15 年前は、RS-232C、RS-422/485 といったシリアル通信インタフェースが一般的だったが、工場やプラントの LAN（Local Area Network）化に伴い制御システ

5）マルウェア（malware）：悪意ある不正なソフトウェアという意味で、マリシャス（malicious：悪意ある）とソフトウェア（software）を合わせた造語。一般的にはウイルスという言葉が使われることが多いが、攻撃が多様化する中で、ウイルスの定義にそぐわないワームやボット、スパイウェアなどが登場したため、セキュリティ業界では、それらを総称してマルウェアという言葉を用いることが多い。

おわりに

本書は、製造事業者のサイバーセキュリティ対策を、セキュリティ担当者が、経営層の理解を得て、包括的・体系的に進めるための考え方や、具体的な実践例を示した。

新型コロナウイルス感染拡大に限らず、革新的な技術の登場など、製造事業者にとってのビジネス環境が大きく変わるようなできごとがこれからも発生すると考えた場合、環境変化に柔軟に対応するために、これまでの常識にとらわれない対象の捉え方が必要となる。

ここで示した製造業のセキュリティ対策の基本概念である「5つのセキュリティ領域と4P」は、製造事業者のビジネス環境変化によって生じたセキュリティ管理対象の拡大を包括的に捉えるための「新しい共通言語」である。

すなわち、セキュリティ担当者が、経営層、リスク管理、法務、工場・プラント、製品・サービス開発、購買、顧客対応のそれぞれの部門の責任者や担当者など、これまでは、自身のビジネスにおいてサイバーセキュリティの比重が低かった人たちに対して、各セキュリティ課題を共有し、経営目標に沿ったセキュリティ対策を推進するための武器である。本書で例示した個別のセキュリティ対策の陳腐化は避けられないが、基本概念である「5つのセキュリティ領域と4P」については、しばらくの間使えるものであると考える。

DXは先進的なプラットフォームの導入だけではなく、同時に社内文化の変革を指す概念でもある。第5章の仮想企業例でも示したように、DX推進により拡大したセキュリティ管理領域をカバーするためには、CSIRTのようなセキュリティ担当者が、経営層の理解を得て、部門間の壁を超え、他部門のことに無関心な社内文化、風土の変革を伴いながら主導していく必要がある。

セキュリティ担当者が、その難題に立ち向かうときに、本書が少しでも役に立てば幸いである。

2012年に、製造業の制御システム機器の開発者から、制御システムセキュリティ業界のエバンジェリストに転身して以降、私は、「産業サイバーセキュ

リティの文化醸成」すなわち、産業システムに関するセキュリティ業界において、「ヒト・モノ・カネ」が健全に回る状態をつくることを使命として、多くの人たちの協力を得て、さまざまな啓発・コンサルティング活動を行ってきた。本書は、その集大成ともいうべきものである。

本書を執筆・出版するにあたって、さまざまな公開情報に加えて、私がビジネス上かかわったすべての人達から得た助言や知見の積み重ねを活用させていただいた。この場を借りて感謝申し上げたい。また、構想から1年半もの間、辛抱強く完成を待ち続けてくれた日科技連出版社の木村修氏、支えてくれた家族や友人にも改めて感謝を伝えたい。

本書を手に取っていただいたみなさまとともに、これからも「産業サイバーセキュリティの文化醸成」に尽力したい。

2021年3月

佐々木 弘志

著者紹介

佐々木 弘志（ささき　ひろし）

国内製造企業にて、制御システム機器の開発者として14年間従事した後、セキュリティベンダーであるマカフィー株式会社に2012年12月に入社。制御システム開発の経験をもつセキュリティ専門家として、産業サイバーセキュリティの文化醸成（ビジネス化）をめざし、国内外の講演、執筆などの啓発及びコンサルティングサービスを提供している。

2012年12月～2021年3月現在	マカフィー株式会社　サイバー戦略室 シニア・セキュリティ・アドバイザー、 CISSP
2017年7月～2021年3月現在	独立行政法人 情報処理推進機構（IPA） 産業サイバーセキュリティセンター（ICSCoE） 専門委員（非常勤）
2016年5月～2020年12月	経済産業省 商務情報政策局 情報セキュリティ対策専門官（非常勤）

製造業のサイバーセキュリティ
産業サイバーセキュリティ体制の構築と運用

2021年4月26日　第1刷発行

著　者　佐々木弘志
発行人　戸羽節文

検　印
省　略

発行所　株式会社 日科技連出版社
〒151－0051　東京都渋谷区千駄ヶ谷5-15-5
DSビル
電　話　出版 03-5379-1244
営業 03-5379-1238

Printed in Japan　　印刷・製本　株式会社三秀舎

ISBN 978-4-8171-9734-4
URL https://www.juse-p.co.jp/