ICSCoE TLP: WHITE

セキュアな ICS クラウド導入指南書

～ データ利活用促進とセキュリティ向上の両立へ ～

2022 年 9 月

独立行政法人　情報処理推進機構

産業サイバーセキュリティセンター

中核人材育成プログラム　第 5 期受講生

ICS Cloud プロジェクト

目次

はじめに

昨今、新型コロナウイルス感染症（COVID-19）の蔓延や熟練技術者不足、国際情勢の変化などの影響により製造業の取り巻く環境は不確実性の高い状況が続いている。このような背景の中、企業が生き残るためには DX（デジタルトランスフォーメーション）の対応が必要であると言われている。

DX を実現する上ではデータの利活用が必要不可欠であり、データ利活用促進のためにクラウド、IoT、AI などの技術が活用されている。これらの技術は製造業においても IT 分野にとどまらず、製造現場の産業用制御システムなどの OT 分野にも導入が進んでいる。一方で、サイバー攻撃が高度化・巧妙化しており、これまで外部ネットワークから隔離されていた制御システムをクラウド、IoT 機器など外部に接続し、リスクに晒すことを敬遠する組織も少なくはない。しかし、サイバー攻撃を恐れるがあまり、データ利活用を推進しない場合、ビジネスチャンスを失い、事業成長のリスクが生じる可能性がある。つまり DX を実現する上では「データ利活用の促進」と「セキュリティの向上」は切っても切り離せない関係にあり、これらは両立する必要がある。

本書では製造現場の産業用制御システム環境へのクラウド活用にフォーカスを当て、クラウド導入時に発生する「データ利活用」と「セキュリティ」に関わる課題や乗り越え方などをまとめた。具体的な取り組みとして、事例調査、ヒアリング、製造現場の制御システム環境にクラウドを導入する上でのアーキテクチャ設計・脅威分析・セキュリティ対策検討の一連のプロセス、これらを実施した。

事例調査では国内外の製造現場へのクラウド導入事例を調査し、実施内容やそれぞれのメリットについてまとめた。またメリットだけではなく、リスクを正しく認識するために OT システム、クラウドに関わるセキュリティインシデント事例を調査し、インシデントの傾向や留意点をまとめた。

また製造現場にクラウドを導入するためには、導入に関する技術的な課題だけではなく、組織や人による課題が発生する。例えば、今まで外部ネットワークから隔離されていた制御システムのデータが、クラウド、IoT などにより外部に接続され、リスクに晒すのではないかという不安である。この不安に関する課題は Web や文献などには多くは載せられておらず、本書では製造現場におけるクラウド導入を果たした 8 組織にヒアリングを実施した。ヒアリングで判明した企画・導入・運用においての課題、解決策、そしてそれらを乗り越えて得られた効果をまとめた。

最後に、製造現場の制御システム環境とクラウドを両方のセキュリティを検討する上で、アーキテクチャの例を提示した。このアーキテクチャをもとに、制御システムとクラウドを融合させた脅威分析、セキュリティ対策の検討、これらについて一連のプロセスをまとめた。

製造現場の制御システムにクラウドを導入し「データ利活用の促進」とともに「セキュリティの向上」の手助けとなる「指南書」として本書をお読みいただき、少しでも参考になれば幸いである。

第1章　　本指南書について

1.1 本指南書の目的

本指南書では、製造業の DX を推進するための手段の一つとして、工場（製造現場）の産業用制御システム（ICS[1]/OT[2]）環境[3]へのクラウド導入にフォーカスを当てた。具体的にはクラウド導入時に発生する「データ利活用」と「セキュリティ」に関わる課題および乗り越え方を記載している。自社で導入を検討する各担当者に向けて、参考資料として活用していただくことを目的とする。

1.2 想定読者

本指南書の読者は、以下の部門の読者を想定している[4]。ただし、想定の読者以外にも知見を得られるような内容や表現としている。

- **情報セキュリティ部門**
  工場へのクラウドシステム導入の際に必要となるセキュリティ対策を検討する部門
- **DX 企画・導入推進部門（DX 推進部、情報システム部　など）**
  工場へのクラウドシステム導入を検討する部門
- **生産関連部門（生産技術部[5]　など）**
  工場へのクラウドシステム導入にあたり、工場側の立場で推進する部門

なお、本指南書の対象となる機器やシステムは、新設・既設によらず、製造現場における産業用制御システムとする。従って、事務系の情報システム（IT）への言及は最小限にとどめる。

---

[1] Industrial Control System：産業用制御システムの略称である。
[2] Operational Technology：運用・制御技術の略称である。
[3] 本指南書は FA（Factory Automation）システム、PA（Process Automation）システムのどちらに対しても適用可能な内容となっている。また制御システムプロトコルを直接利用するだけではなく、IoT などを用い間接的にデータを取得・活用するシーンも対象としている。
[4] 本指南書は実務者向けの資料ではあるが、実現に関してはトップマネジメントの CIO や CISO などの経営層の理解、並びに組織体制や予算に関する支援が必要である。
[5] 予知保全などの機能を実装する場合は保守部門も関わる。

1.3 本指南書の構成

本指南書は以下の章構成となっている。各章は「データ利活用」と「セキュリティ」の２つの観点で関連性がある。関係図を図 1-1 に示す。

第1章 「本指南書について」では、本指南書の目的、想定読者、免責事項について記載する。
第2章 「日本の製造業のデータ利活用における背景・課題」では、製造業の状況、製造現場におけるデータ利活用とセキュリティ対策の必要性を記載する。
第3章 「製造業における製造現場へのクラウド導入事例」では、実際に製造現場にクラウドを導入している事例を記載し、どのようなメリットを得ることができるのか記載する。
第4章 「セキュリティインシデント事例」では、製造現場にクラウド導入する際の関連する技術領域である OT システムとクラウドサービスのそれぞれで発生したセキュリティインシデント事例を記載する。
第5章 「クラウド導入における課題および乗り越え方」では、製造現場にクラウドを導入した企業にヒアリングした内容をまとめ、データ利活用並びにセキュリティへの課題・乗り越え方を記載する。
第6章 「セキュアな ICS クラウドアーキテクチャ」では、製造現場にクラウドを導入する際のアーキテクチャ並びにセキュリティ脅威・対策の例や考え方について記載する。
第7章 「おわりに」では、本指南書のまとめを記載する。

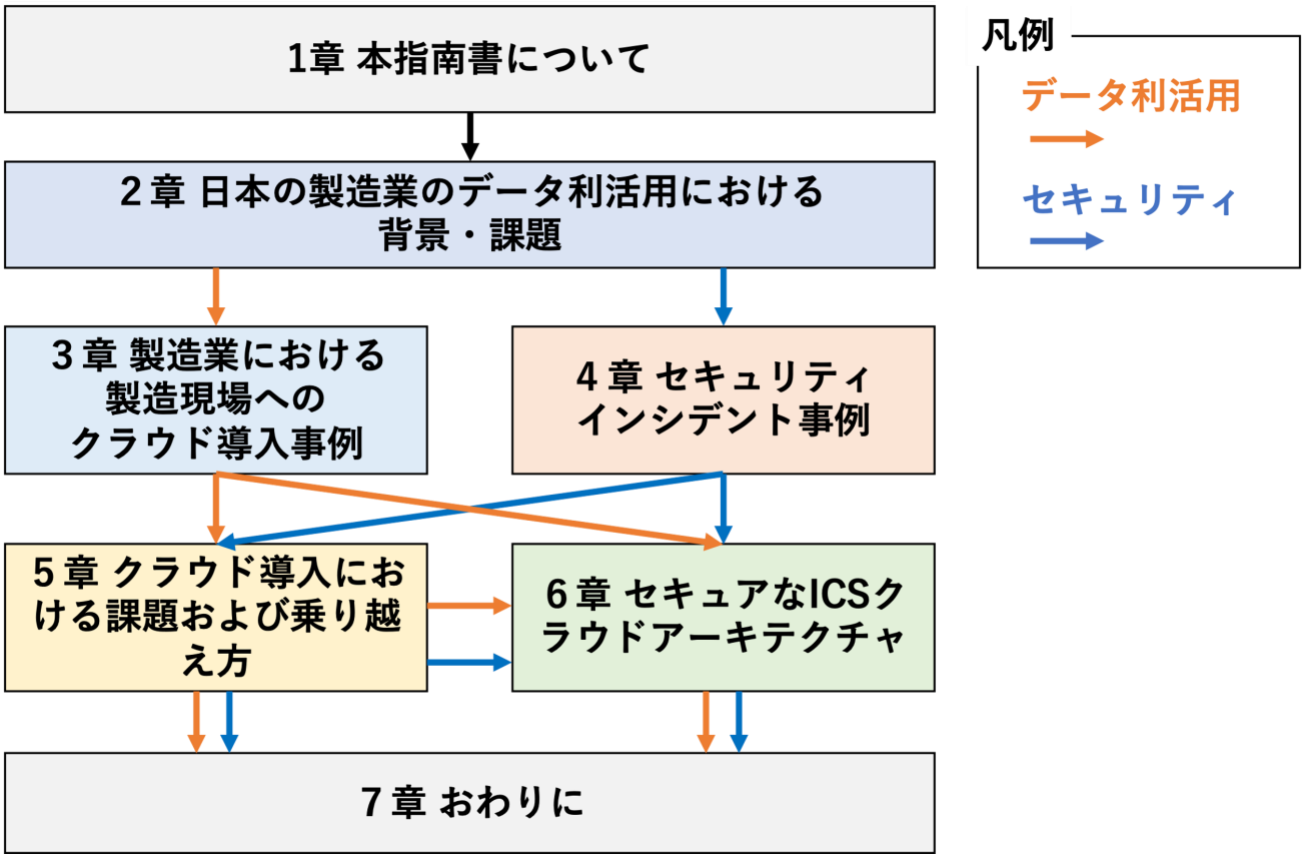


図 1-1 本指南書の構成

1.4 免責事項

- 本指南書は単に情報として提供され、内容は予告なしに変更される場合がある。
- 本指南書に誤りが無いことの保証や、商品性又は特定目的への適合性の黙示的な保証や条件を含め明示的又は黙示的な保証や条件は一切無いものとする。
- 本指南書に記載の内容は、独立行政法人 情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、作成者の見解に基づいている。
- 本指南書の利用によるトラブルに対し、本指南書作成者ならびに監修者は一切の責任を負わないものとする。
- 本指南書の有効期限は、発行日から 2 年間とする。

1.5 本指南書で使用する他企業の商標・登録商標について

- Microsoft、Windows、Azure、Azure AD、Azure Confidential Computing は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標である。
- AWS, AWS Nitro System は、米国 Amazon.com,Inc.の米国およびその他の国における商標または登録商標である。
- Google Cloud Platform、GCP、GCP confidential VMs は、米国 Google LLC の商標または登録商標である。

第2章　　日本の製造業のデータ利活用における背景・課題

本章では、製造業の DX を実現する上では「**データ利活用の促進**」と「**セキュリティの向上**」の**両立**が必要であることを認識していただく。

まず2.1 節にて日本の根幹の産業である製造業が DX を必要とする背景を記載する。また、製造業での DX を実現する上で必要不可欠である製造現場のデータ利活用動向を示し、工場におけるデータ利活用の形態としてのスマートファクトリーについて説明する。次に、2.2 節、2.3 節にてデータ利活用を促進する技術の 1 つであるクラウドサービスについて説明する。次に、2.4 節にてデータ利活用と同時に検討する必要があるサイバー攻撃情勢、セキュリティ対策状況についても言及する。最後に、2.5 節にて製造現場の制御システム環境へのセキュアなクラウドサービス活用について言及する。

図 2-1 にデータ利活用度とセキュリティ対応度の関係図を示す。データ利活用の促進のみを考え、セキュリティ対応が不十分であると、サイバー攻撃被害に遭いやすくなるなど、セキュリティ上のリスクが大きくなる。一方で、セキュリティのみを強化するあまり、データ利活用が阻害されてしまう場合も事業の成長を鈍化させ、競合他社へ競争に打ち勝てないなど、事業成長としてのリスクが大きくなる。つまり、あるべき姿として、**データ利活用の度合いによってセキュリティ対応の度合いも上げていき、これらを両立させる必要**がある。

本指南書では第 2 章から第 6 章にかけて、製造現場へクラウドサービスを導入し、データ利活用×セキュリティ両立企業となるために必要なことを記載している。それぞれの組織で導入する際に、参考にしていただければ幸いである。

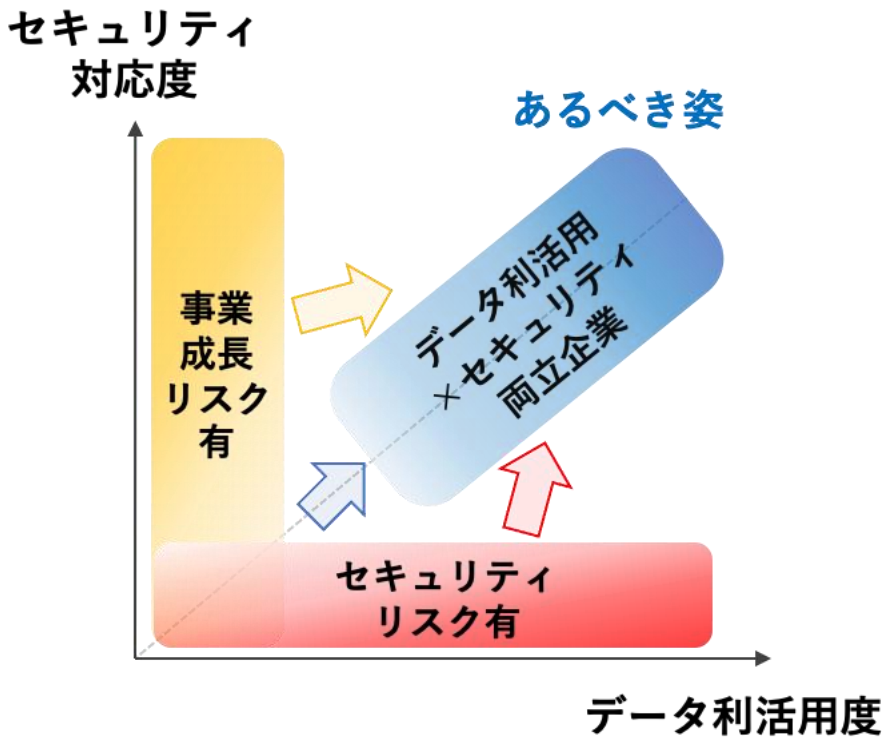


図 2-1 データ利活用度×セキュリティ対応度の関係図

2.1 製造業における DX

日本における製造業の位置付け、近年の動向や製造業における DX の必要性を述べる。また工場でのデータ利活用動向や、スマートファクトリーについて概要を記載する。

2.1.1 製造業における DX の必要性

日本における製造業は 2019 年業種別 GDP 比において第 2 位（20.5%）となっており、国の根幹となる産業である [1]。一方、昨今の COVID-19 の影響もあり、直近の製造業全体の売上高、営業利益は減少傾向が予想されている [2]。また、人口減少・高齢化が進み、製造業では特に熟練技術者の減少が問題視されている。COVID-19 のみならず、地震や洪水などの自然災害や、国際情勢などにも常に注視しなければならないなど、不確実性が高い世の中となっている。

世界各国に目を向けると IMF（国際通貨基金）では日本の国内総生産（GDP）は為替レート（米ドル）で換算した名目 GDP 規模では 2010 年に中国に追い抜かれ、米国、中国に次ぐ第 3 位となっている。また企業の世界時価総額ランキング TOP50 位以内に日本企業は過去（1989 年）には 32 社ランクインしていたが、2022 年 1 月には 1 社しかランクインしていないなどが実情である [3]。

このように不確実性が高まる中、企業が生き残るためには、DX に取り組む必要があることはよく言及されている。経済産業省、厚生労働省、文部科学省の「2021 年版 ものづくり白書」においても、製造業における製造業 DX（デジタルを用いた生産性の向上、新たな付加価値の創造）の推進が必要とされている。これらを実現させるためには「データ利活用の拡大・迅速化」が重要な要素の一つとされている [2]。

2.1.2 製造業におけるデータ利活用

情報処理推進機構の「DX 実践手引書 IT システム構築編 暫定 第 2.0 版」によると、“*市場動向に合わせて前例のない課題に取り組むにあたり、ビジネスのリアルタイムなデータをより的確に参照できるよう整備し、データを基軸とした判断根拠をもとに意思決定を行っていくような、データドリブン[6]企業となることが求められる*”とある [4]。不確実性の高い世の中において、データに基づいた分析・意思決定の重要度は非常に高く、データ利活用は DX と切っても切れない関係にある。

一方で、「2020 年版 ものづくり白書」によると生産プロセスに関する設備の稼働状況などのデータ取集を行なっている割合が、2017 年の 67.6%を基点として、2019 年に 51.0%と減少傾向となっている。また設計開発・生産・販売などの複数部門間での情報・データ共有について、販売後の製品の動向や顧客の声を設計開発や生産改善に活用している企業も 2019 年には 8.4%と多くないのが実情である [5]。

「2021 年版 ものづくり白書」では、ものづくりの工程・活動におけるデジタル技術の活用状況が掲載されている。2020 年の調査結果によると「活用している企業」は 54.0%、「活用を検討している企業」が 17.2%と全体の約 7 割の企業はデータ活用に前向きになりつつある [2]。

[6] 収集したデータに基づいた分析・予測の結果を踏まえてビジネスの意思決定や課題の解決を迅速に行っていくことをデータドリブン（Data Driven）と言う [4]。

2.1.3　　工場とデータ利活用

本項では前項のデータ利活用と工場との関係を記載する。ドイツから始まった第 4 次産業革命（Industry 4.0）を受け、日本でも 2016 年に内閣府の第 5 期科学技術基本計画より Society 5.0[7]が提唱された。続いて 2017 年より「モノづくりのスマート化」や「Connected Industries[8]」といった戦略が経済産業省主導で打ち出された。中でも工場のデータ利活用に関しては、品質の向上やコスト削減、生産性向上などを目指して「スマートファクトリー」というコンセプトが提唱された。

スマートファクトリーでは IoT やビッグデータ、AI を活用して工場のスマート化の実現を目指している。経済産業省 中部経済産業局の「スマートファクトリーのロードマップ」では代表的な目的として「品質の向上」、「コストの削減」、「生産性の向上」、「製品化・量産化の期間短縮」、「人材不足・育成への対応」、「新たな付加価値の提供・提供価値の向上」、「リスク管理の強化」が 7 つ掲げられている［6］。

また、三菱総合研究所の「令和 2 年度スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査（経済産業省委託）」によると、工場におけるデータ利活用度合いによってレベル 0 から 4 まで定義されている。具体的には、レベル 0：データが活用されていない、レベル 1：データの収集・蓄積（・可視化）の実施、レベル 2：データによる事象のモデル化による分析・予測の実施、レベル 3：構築したモデルによる制御・最適化の実施、4：動的な自律制御または複数工場の連携の実施。このような 5 段階のレベル分けがされている（図 2-2）［7］。

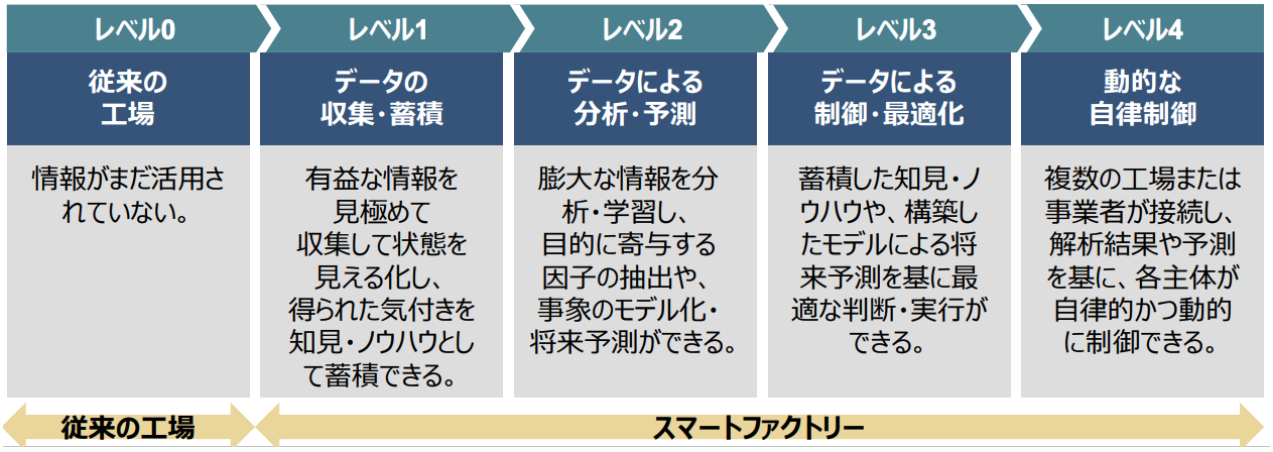


図 2-2 スマートファクトリーの段階（出展：三菱総合研究所 令和 2 年度スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査［7］）

[7] サイバー空間とフィジカル空間（現実世界）が高度に融合した「超スマート社会」を未来の姿として共有し、その実現に向けた一連の取り組み［26］。

[8] データを介して、機械、技術、人など様々なものがつながることで、新たな付加価値創出と社会課題の解決を目指す産業のあり方。

2.2 クラウドサービスについて

2.1.2 項で述べたように、製造業においてもデータ利活用が重要であることが認識されている。また、2.1.3 項で述べたように、工場のデータ利活用（スマート化）を促進するためにはまずデータを収集・蓄積し、それらを分析することが必要である。これらを実現する上で本指南書では後述するクラウドサービスの特性より、データ収集・分析基盤として「**クラウドサービスを活用することが有効である**」と考えた。本節では、まずクラウドという言葉の定義、そしてクラウドサービス活用する際の必須概念である責任共有モデルについて記載する。

2.2.1 クラウドの定義

まずクラウド（クラウドコンピューティング）の定義を行う。NIST[9]が 2011 年に *SP800-145 The NIST Definition of Cloud Computing* [8]を発行した。情報処理推進機構による同内容の翻訳となる、クラウドの定義を以下に示している。本指南書においても、この定義に則り記載していく。

“*クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルである。また利用者は最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ、提供されるものである。* [9]”

“*このクラウドモデルは 5 つの基本的な特徴（オンデマンド・セルフサービス、幅広いネットワークアクセス、リソースの共用、スピーディな拡張性、サービスが計測可能であること）がある。また、 3 つのサービスモデル（SaaS、PaaS、IaaS[10]）、および 4 つの実装モデル（プライベートクラウド、コミュニティクラウド、パブリッククラウド、ハイブリットクラウド）によって構成される。* [9]”

2.2.2 責任共有モデル

クラウドサービスを活用する場合、「責任共有モデル」の理解が大前提となる。これは、利用者とクラウド事業者が、責任分界点を定めるだけではなく、運用責任を共有しているという考え方である[10]。責任共有モデルの基本的な考え方の例を図 2-3 に示す。このようにオンプレミス型に比べ、クラウドサービスはクラウド事業者と運用責任を共有しており、IaaS、PaaS、SaaS ではクラウド事業者が管理する区分の運用責任の対象となる項目が異なる。なお「データ」と「ポリシー・設定・端末」においてはどのサービス形態においても利用者が対応・管理する項目であり、注意が必要である[11]。

---

[9] National Institute of Standards and Technology（米国立標準技術研究所）の略称。

[10] SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）の略称。

[11] SaaS であっても利用組織が設定ミスをすることでセキュリティインシデントにつながる可能性がある。

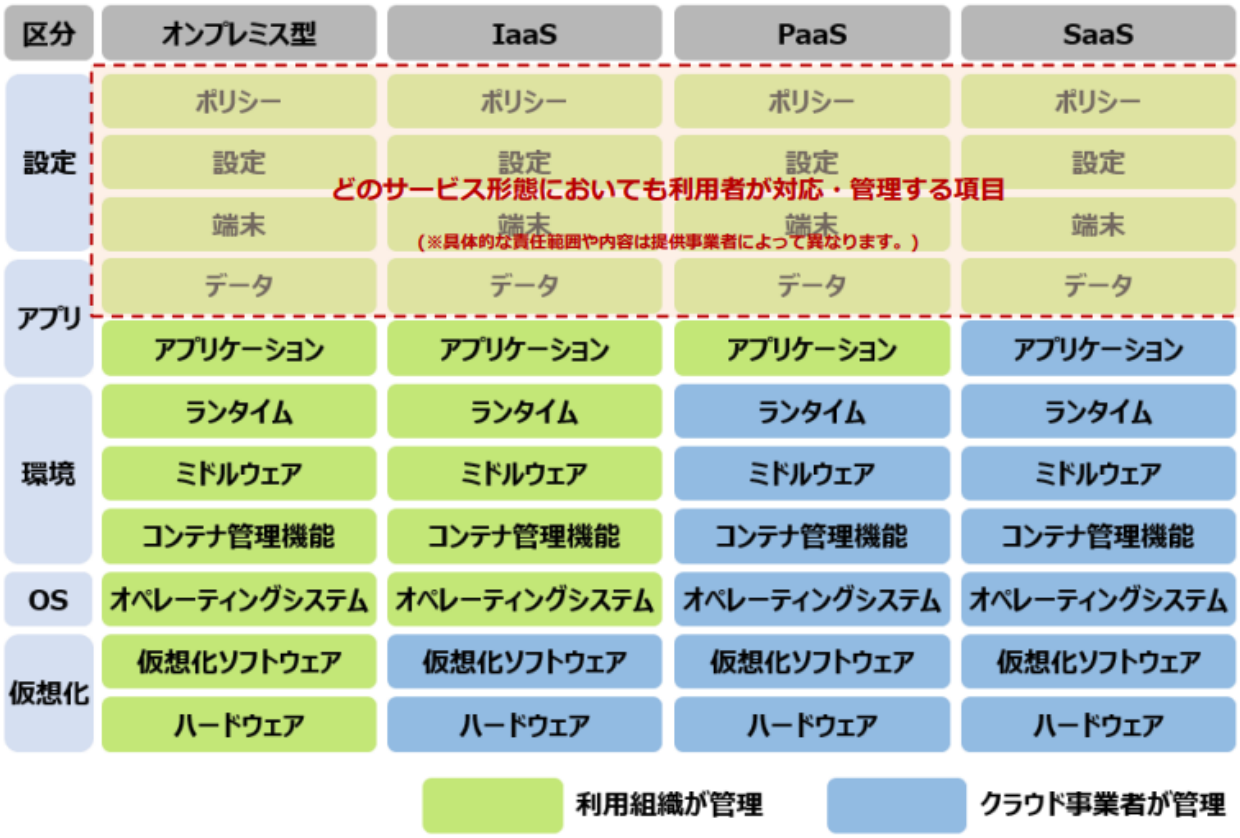


図 2-3 クラウドサービスの責任共有モデル（例）（出典：内閣官房内閣サイバーセキュリティセンター、クラウドを利用したシステム運用に関するガイダンス（詳細版）［10］）

2.3 クラウドサービスの活用

2.2 節に記載した通り、このようにクラウドサービスには従来のオンプレミスとは違う特徴、運用形態をとれるという特徴がある。本節では日本政府のクラウドサービス活用に関する方針、日本企業におけるクラウドサービス活用についての動向について記載する。またクラウドサービスを活用する上で認識する必要があるクラウドサービス特有のメリットや留意点を挙げる。

2.3.1 日本政府のクラウドサービス活用に関する方針

2021 年に各府省情報化統括責任者（ＣＩＯ）連絡会議決定より発行された「政府情報システムにおけるクラウドサービスの利用に係る基本方針」において、「クラウド・バイ・デフォルト原則」が掲げられた［11］。これは、政府情報システムはクラウドファースト（クラウドサービスの利用を第一候補としてその検討を行う）という方針が示されたものである。

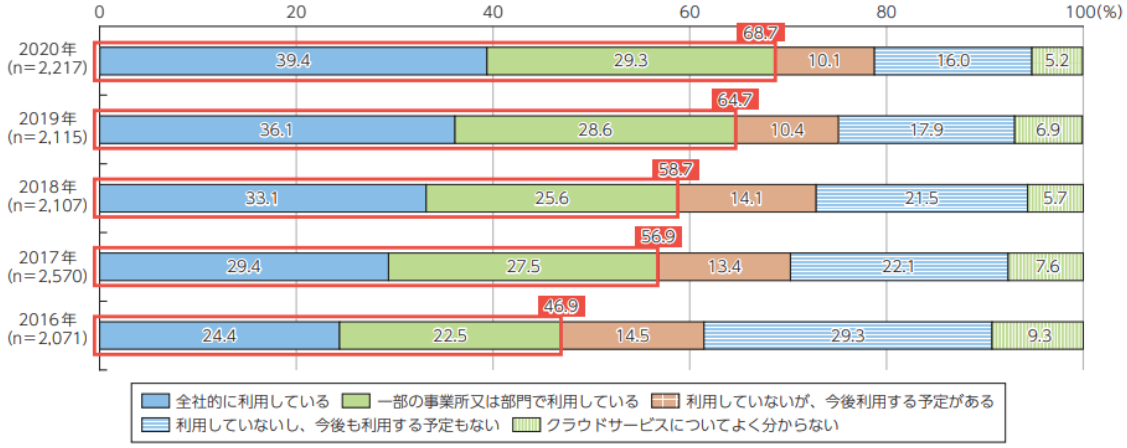
また 2022 年 5 月にはデジタル庁より「政府情報システムにおけるクラウドサービスの適切な利用に関わる基本方針の改定について」が発行され、「クラウドスマート」が新たに掲げられた［12］。旧方針では、クラウドファーストだったが、クラウドスマート（クラウドを賢く適切に利用すること）を方針として新たに定めた。スマートとはマネージドサービスや IaC（Infrastructure as Code）などを積極的に活用していくことである。これらを活用することで、運用負担を減らし、自社の競争領域となるコアビジネスに集中できるようにすることが期待できる。このことから、製造業のみならず、各産業においてクラウドサービス活用は益々推進されていくものと思われる。

2.3.2　日本企業におけるクラウドサービスの活用動向

まずは現状の日本企業でのクラウドサービス利用の動向を説明する。総務省の「令和 3 年版 情報通信白書」によると、2021 年の段階では、約 7 割の企業がクラウドサービスを利用しており、例年増加傾向となっている（図 **2-4**）。利用しているクラウドサービスは「ファイル保管・データ共有（2020 年割合 59.4%）」が最も多く使用されている一方で、「営業支援（17.6%）」や「生産管理、物流管理、店舗管理（10.2%）」など高度な利用は低水準に留まっている[12]。

また、総務省の「令和 2 年版 情報通信白書」によると、クラウドサービスを利用しない理由として、「情報漏洩などのセキュリティに不安がある（31.8%）」、「ネットワークの安定性に対する不安がある（14.6%）」、「クラウド導入によって自社コンプライアンスに支障をきたす（4.1%）」などの不安の声も挙げられている[13] [13]。経済産業省の「デジタル産業に関する現状と課題」によると、特に産業・政府・インフラ領域において主に信頼性（可用性など）の懸念からオンプレミスからクラウド移行は懸念があるとされている [14]。

上記より、ファイル保管、データ共有などの IT 分野に関してはクラウドサービスが広く活用されているが、産業・インフラなどの OT 分野に関してはまだ広く活用されていないと考えられる。



	集計企業数	比重調整後集計企業数	クラウドサービスの利用状況							
			利用している	全社的に利用している	一部の事業所又は部門で利用している	利用していない	利用していないが、今後利用する予定がある	利用していないし、今後も利用する予定もない	クラウドサービスについてよく分からない	無回答
全 体	2,223	2,223	1,522	873	649	580	225	355	114	7
[産業分類]										
建設業	340	96	73	48	25	21	13	8	2	-
製造業	372	590	401	223	178	167	72	94	20	3
運輸業・郵便業	352	203	116	57	59	67	23	44	19	1
卸売・小売業	338	475	340	191	150	107	41	66	24	3
金融・保険業	137	27	22	15	7	5	3	2	0	-
不動産業	134	32	28	19	9	4	2	3	0	-
情報通信業	254	110	101	74	27	8	6	3	-	0
サービス業、その他	296	690	442	246	196	200	66	134	48	-

図 2-4 クラウドサービスの利用動向（出典：総務省　令和 3 年版 情報通信白書 [15]）

12　（　）内の数値は 2020 年割合。

13　（　）内の数値は 2019 年割合。

2.3.3 クラウドサービスのメリット

2.3.1 項で述べた「政府情報システムにおけるクラウドサービスの利用に係る基本方針」では、クラウドサービス利用のメリットとして「効率性の向上」、「セキュリティ水準の向上」、「技術革新対応力の向上」、「柔軟性の向上」、「可用性の向上」の 5 つを挙げている [11]。

これらのメリットは、本指南書がフォーカスを当てた、製造業におけるデータ利活用においても享受できるものと考えられる。例えば、スマートファクトリー化した製造現場から生み出される大量のデータを蓄積し、可視化し、分析するためには、それに応じたコンピュータリソースが必要である。クラウドサービスでは、オンプレミスと比較して初期投資が少なく、リソースの利用状況に応じたスケールの変更が容易で、かつスケールアップに関しても安価に提供されている場合が多い。また仮想化技術などの利用により、個々のリソースの障害や大規模災害などに対しても可用性を確保できている。

2.2.2 項で述べた責任共有モデルや選択するクラウドサービスにもよるが、世界的に認知されたクラウドセキュリティ認証[14]を取得しているクラウドサービス事業者が存在する。第 4 章で挙げるようにクラウドサービスによるインシデントは存在している。しかし、近年のサービス普及に伴い、クラウドサービス事業者により高い頻度でセキュリティ機能が更新されている。近年では、クラウドサービス事業者はクラウドサービス普及に伴い、より高いセキュリティ要件について対策を講じている。例えば、近年、コンフィデンシャル・コンピューティング[15]という技術にクラウドサービス事業者が対応するようになった。この技術は、クラウド内にあるデータの保存時または転送時に暗号化されるだけではなく、データの処理中に、使用中のデータを暗号化できる技術のことである。この技術を活用することで、機密性の高い、個人を特定できる情報（PII[16]）や医療情報、金融データなどを扱う時に役立てられると考えられている。

クラウドサービスを活用することが、オンプレミスでセキュリティ機能を個々に構築するよりもセキュリティレベルを向上させる上で有利となる場合も多い。

---

[14] 例えば、ISO 27001, ISO 27018, ISO 27017, ISO 27701, FedRAMP, FISMA, HIPPA などがある。

[15] ハードウェアベースの高信頼性実行環境（Trusted Execution Environment）を使用して、メモリ内で使用されている間のデータも暗号化する技術。パブリッククラウド事業者のサービスでは AWS Nitro System, Azure Confidential Computing , GCP Confidential VMs などが挙げられる。

- AWS Nitro https://aws.amazon.com/jp/ec2/nitro/
- Azure Confidential Computing https://azure.microsoft.com/ja-jp/solutions/confidential-compute/
- GCP Confidential Computing https://cloud.google.com/confidential-computing?hl=ja

[16] Personally Identifiable Information の略称。個人情報や個人を特定できる情報のことを示す。

2.3.4　　クラウドサービス活用の留意点

2.3.3 項に挙げたようにクラウドサービスには多くのメリットがある一方で、クラウドサービスを活用する上でいくつかの留意点が存在する。以下にその留意点の例を述べる。

1. **サービス変更・廃止**

クラウドサービス事業者のサービス約款にサービス内容変更やサービス提供の廃止について明記されていることがある。大半は事前に利用者への通知はあるものの、自社で利用しているサービスが変更・廃止される可能性がある。変更・廃止の可能性とそれによるビジネス上の影響を認識し、代替策を事前に検討しておく必要がある。

2. 障害に伴うサービス停止

クラウドサービスの多くはデータセンターの多重バックアップ体制、負荷分散技術を用い、耐障害性が優れていると言われている。しかし、システム障害を完全に無くすことはできず、サービス停止に陥る可能性がある。ビジネス要求をもとにオンプレミス型との可用性やコストなどの比較が重要である。

3. 利用者によるセキュリティ確保

クラウドサービスのメリットとして、セキュリティレベルを向上させる上で有利となることが挙げられる。一方で、利用者は責任共有モデルにおける自身の責任範囲において、セキュリティ対策を講じる必要がある。例えば、留意点 1 にも挙げたとおりサービス変更や機能拡張のたびに影響を受ける領域に対するレビューが必要になる点である。

クラウドサービスの急速な導入進展において、クラウドサービス利用者の設定の不備などによるセキュリティインシデント事例も発生している。なお具体的なクラウドサービスにおけるインシデント事例に関しては本指南書の第 4 章にて紹介する。クラウドサービスのインシデントを正しく恐れ、リスクとして認識するための参考にしていただきたい。

4. 専門知識を持った技術者の必要性

クラウドサービスのメリットとして「技術革新対応力の向上」がある。新たに提供される、もしくは改善されるクラウドサービスを適切に使用するためには専門知識をもつ技術者が必要となる。

5. サービス価格の上昇

クラウドサービスでは、クラウドサービス事業者の激しい競争や積極的な新技術採用により、サービス価格の値下げが行われている。その一方で、一部のサービスの価格が値上げに至った事例も存在する。利用しているサービスによっては、当初想定していたよりもコストが嵩む恐れがある。

また海外クラウド事業者のサービスを利用している場合、為替の影響でサービス料が上下する[17]恐れもある。

[17] サービス利用当初よりも円安となる場合、サービス料が想定より嵩む可能性がある。

6. 関連法規

クラウドサービスを利用する上では、「データの開示請求（CLOUD Act[18]など）」や「データ越境移転（GDPR、中国データセキュリティ法など）」などクラウドサービス事業者やサービス展開先の国ごとの法規に注意する必要がある。これらの問題は非常に複雑であり、各国の規則を継続的に監視する必要がある。また経済産業省主導のもと 2021 年 11 月よりデータ越境移転に関する研究会[19]が発足されており、動向を注視していく必要がある［16]。

[18] CLOUD Act（Clarifying Lawful Overseas Use of Data Act）は 2018 年 3 月 23 日、米国議会で可決した海外のデータの合法的使用を明確化する法案のこと。

[19] データ越境移転に関する研究会
https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/index.html

2.4 セキュリティ対策強化の必要性

冒頭で述べた通り、本指南書ではデータ利活用を進める上で、セキュリティも同時に検討していくことが必要であると考えている。そこで、2.4 節では、製造業においてのサイバー攻撃の動向、工場におけるセキュリティ対策状況及び、セキュリティ対策の必要性について記載する。また、データ利活用とセキュリティの関係性を述べ、セキュリティ一辺倒ではなく、データ利活用とセキュリティ双方の検討について言及する。

2.4.1 製造業へのサイバー攻撃の動向

IBM X-Force の「X-Force 脅威インテリジェンス・インデックス 2022[20]」にて、2021 年に世界でサイバー攻撃の標的とされた件数は製造業が最も多い業種であるという調査結果[21] [17]が公表された。2020 年に首位であった金融・保険業を抑えて製造業が首位に立ったという形である。この調査結果へ特に影響を与えた背景として、ランサムウェアという身代金要求型のコンピュータウイルスによる被害が増加していることが挙げられている。具体的な事例として、海外では 2021 年に米国のパイプライン企業に対して行われたサイバー攻撃により 5 日間も重要インフラの停止が発生した（このことに関しては、第 4 章にも事例として挙げている）。また日本企業においては、大手自動車製造会社に部品提供を行うサプライチェーン企業のランサムウェア被害、大手自動車部品会社の欧州子会社に対する不正アクセスが発生した。これらのように大手企業やその関連会社がサイバー攻撃の被害を受けたことが明らかになっている。被害を受けた企業では、復旧までの期間、生産停止を余儀なくされる事例も見られる。

産業用制御システムの変遷

これまで産業用制御システムはインターネットから切り離された環境で稼働し、サイバー攻撃とは無縁と考えられていた。しかし、1990 年代から産業用制御システムに使うマシンの OS に汎用 OS（Windows など）が採用され、生産管理・在庫管理など[22]のために、企業内の IT ネットワークと通信を行うようになった。

近年では、DX に伴い IoT やクラウドサービスの活用が始まり、産業用制御システムがインターネットと直接の通信を行う事例も増えてきた。具体的には、第 3 章に挙げるような製造現場のデータの利活用としてクラウドサービス活用事例を参照されたい。

一方で、新しい技術の採用に伴ってサイバー攻撃の対象は増えるため、技術の活用と並行してセキュリティを考慮し、安全性の確保を行う必要性が高まっている。

---

[20] IBM X-Force の「X-Force 脅威インテリジェンス・インデックス 2022」
https://www.ibm.com/security/jp-ja/data-breach/threat-intelligence/

[21] 調査結果によると、攻撃者に狙われる業種の世界で 1 位が製造業（アジアでは 2 位）となり、全業種の 23%を占めた。また、OT を標的とし不正アクセス被害のうち 61%が製造業であることも判明した。さらに、製造業を狙った攻撃のうち、1/3 はアジアで発生しておりこの比率は益々増加傾向にあり、その中でも日本への攻撃が最も多い国であった。これらより、日本における製造業のサイバーセキュリティ対策は喫緊の課題であることが分かる。

[22] 製造実行システム（MES：Manufacturing Execution System）なども該当する。

高まるサイバー攻撃の脅威

産業用制御システムにおいては、サイバー攻撃の対象が増加しているにもかかわらずシステムの欠陥（以下、脆弱性という）を残したまま維持運営せざるを得ない場合も多い。産業用制御システムは、可用性を担保するためにセキュリティ修正プログラムを適用することが難しいという特性や、特定の OS のバージョンでないと正常動作しないソフトウェアが存在するなどの事情があり、IT システムと比べセキュリティ対策の実行に障壁が多い。しかし、システムの脆弱性が残ったままのシステムでは、仮にサイバー攻撃を受けた時、いとも簡単に停止・誤作動を引き起こされてしまう。

加えて、サイバー攻撃が日々高度化しているという外部環境もあり、セキュリティ対策の必要性は高まっている。米国の非営利団体である MITRE 社は、システムの脆弱性に一意の値（CVE[23]）を採番するサービスを提供しており、2021 年に新たに採番された脆弱性は 2 万件に迫る勢いであった。新たなサイバー攻撃手法は日々開発されており、昨日まで問題のなかったシステムであっても、今日は侵害されてしまう可能性がある。

サイバー攻撃による影響

仮にサイバー攻撃が発生した場合、生産停止以外にも様々な危機が想定される。例えば化学プラントや産業ガスプラントを運営する企業の場合、原材料の配合や圧力データが改ざんされれば、工場の火災・爆発という人命に関わる甚大な災害も想定される。製品を作る工場であっても、自動制御の機器が誤作動し、そこで作業する従業員に危険が生じる。もちろん、こうした企業では重要度に応じて安全計装システムや異常に対する物理的な対策を施しているため、攻撃者が火災・爆発を起こすことは簡単なことではない。

一方で、IDC Japan の「2021 年 国内 IoT/OT セキュリティユーザー調査（N=443）」によると IoT/IIoT[24]/OT に関わるシステム特有のセキュリティの危険や事件・事故が 161 件ほど発生しているという調査結果も出ている。本調査によると生産、製造ラインやシステムの一時停止（一部停止）が 25.5%、工場やシステムの破壊・破損・故障が 18.6%、生産・製造ラインやシステムの完全停止が 18.0%など挙げられている [18]。これら調査結果から分かることは、火災・爆発の事例は出ていないものの、日本においてもサイバー攻撃が工場の操業停止などの現実世界に影響している事実があり、まだ被害が出ていない企業であっても他人事ではないということである。

[23] CVE（Common Vulnerabilities and Exposures）の略称。
[24] IIoT（Industrial Internet of Things）の略称。

2.4.2　工場のセキュリティ対策状況

2.4.1 項に挙げたようにサイバー攻撃に関しては工場においても例外ではない。一方で、工場における産業用制御システムのセキュリティ対策実施の動向はまだ発展途上である。経済産業省「2018 年版ものづくり白書」によると、工場においてセキュリティ対策の実施が進んでいない理由は、大きく 4 つに分けられる［19]。

① 中小企業を中心に工場の産業用制御システムや機器に対するサイバーセキュリティ対策の必要性を正しく認識、理解できていない企業が多い。
② どのような対策が必要なのかが分からない企業が多い。
③ 必要な対策を実施するためのスキルを有する人財や予算を確保できていない。
④ 実施した対策で十分なのかが分からない、実際にサイバー攻撃の被害にあった場合にどうすれば良いのかが分からない。

2.4.1 項や後述する第 4 章インシデント事例に挙げるように、一度サイバー攻撃における各社のリスクや万が一の被害に遭うと事業への影響は大きい。従って、サイバー攻撃の被害を想定したセキュリティ対策を講じることが望ましい。本指南書ではセキュリティ対策を講じる際の指針となる、脅威分析手法を第 6 章に記載しており、自社で検討する際に参考にされたい。

2.4.3　データ利活用とセキュリティの関係

2.4.1 項のようにセキュリティ対策が実施されないと、サイバー攻撃の被害に遭い、生産停止など事業に大きな被害を受ける可能性がある。一方で、セキュリティ対策を行うこと自体は重要であるが、サイバー攻撃を必要以上に恐れてやみくもにセキュリティを強化[25]すれば良いわけではない。利便性やコストとのバランスをとりながら、データ利活用の妨げとならないように気を付ける必要がある。

もちろん、データ利活用を促進したいがためにセキュリティ対策を緩くしすぎることで、サイバー攻撃の被害に遭うのは本末転倒である。従って、データ利活用とセキュリティはバランスが必要であり、双方の検討が必要不可欠である。

[25] 例えば、セキュリティを意識してデータへのアクセス権限を過剰に制限すると、データ共有の促進の弊害になる可能性がある。

2.5 製造現場におけるクラウドサービス活用

2.1.1 項で挙げたように、変化が激しく不確実な市場環境に俊敏に対応するためには、安全性や安定稼働のみならず、「スピード」・「アジリティ」に対応したシステム構成が求められる。そうしたシステム構成に寄与する観点として「マイクロサービスアーキテクチャ[26]」、「クラウドのような拡張（容易性）のある基盤」が挙げられる [4]。

クラウドサービスには2.3.4 項に挙げた留意点があるものの、スマートファクトリーに求められている、必要な大量のデータ収集・分析などを実現する上で、クラウドサービスは非常に適している。

一方で2.1.2 項や2.3.2 項で述べた通り、製造現場によるデータ利活用は思うように進んではいない。また産業分野でのクラウドサービス活用も敬遠されがちであり、これは2.4 節に挙げたように DX を進めることでセキュリティ上の脅威が増えており、サイバー攻撃への不安がデータ利活用を促進できない理由の一つでもある。

上記を踏まえ、本指南書では製造現場の制御システム環境へセキュアにクラウドサービスを導入・活用することで「データ利活用の促進」と「セキュリティの向上」の両立を実現できると考えた。クラウドサービスを導入・活用時の検討に必要と考えられる内容について、次章以降、以下のような構成をとっている。自社に必要とする内容をそれぞれ参照されたい。

- 第 3 章：製造現場へのクラウドサービス活用を取り入れている事例を挙げ、取り組み内容やそれぞれのメリットについて記載する。自組織に導入する際にユースケースの例として参考にされたい。
- 第 4 章：製造現場に関係が深い OT システムやクラウドサービスによるインシデント事例を挙げている。万が一被害が発生した場合のリスクを正しく認識する上で参考にされたい。
- 第 5 章：製造現場にクラウドサービス導入の際に企画・導入・運用においてよく発生する課題、そして解決策を記載している。製造現場へのクラウドサービス導入の際に参考にされたい。
- 第 6 章：製造現場にクラウドサービスを導入する上でセキュリティ上の脅威対策を講じたアーキテクチャについて提示する。脅威分析やセキュリティ対策の参考にされたい。

[26] 小さなサービス（マイクロサービス）を組み合わせることによってアプリケーションが開発・構成されるアーキテクチャ。メリットとして、各サービスが疎結合のため素早く開発・改修できたり、障害発生の影響を最小限にすることができたりすることが挙げられる。

第3章　　製造業における製造現場へのクラウド導入事例

データ利活用を行う上でクラウドサービスをどのように導入するのか、導入事例から活用形態を知ることは有用である。そこで、本章ではクラウドサービスが製造業で実際に活用されている事例を紹介する。実例を知ることで、クラウド活用のメリットを理解し、将来的に自社で既存ビジネスの効率化や新規事業を創出する際に役立てていただきたい。

次項からは具体的なデータ利活用事例について紹介する。

3.1 データ利活用事例（国内）

日本国内での製造現場におけるクラウドサービスを用いたデータ活用事例を表 3-1 に示す。本項では、三菱総合研究所の「令和 2 年度 スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査［7]」に記載されている、5 つのデータ利活用の目的（品質改善、機械化・自動化・最適配置、保守・保全の効率化、生産計画改善、工場外との情報連携）に基づき事例を整理した（図 3-1）。これらの企業は工場に限らず様々な物のデータを収集し、保守効率化や新規事業創出に役立てている。

あくまで事例の一部ではあるが、国内事例では製造現場のデータの収集・分析基盤としてのクラウド活用などが主な活用用途であることがわかる。工場においてもこれらのようなデータ利活用を促進することにより、人手不足や熟練工の技術の継承、事業創出など、データ利活用によってもたらされる恩恵は大いにあると考える。

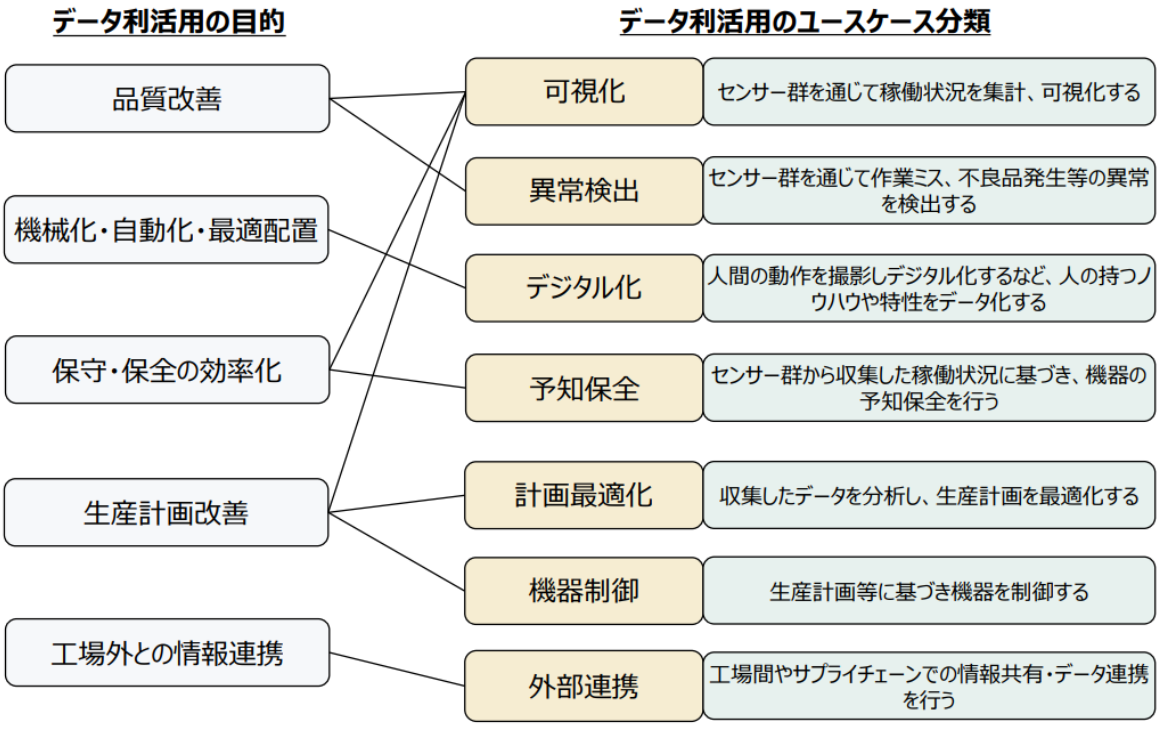


図 3-1 スマートファクトリーにおけるデータ利活用の目的と、それぞれの目的に対応するユースケース（出典：三菱総合研究所_令和 2 年度 スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査［7]）

表 3-1 クラウドサービスを用いたデータ利活用事例

#	対象企業（業界）	事例	着目したキーワード	参考・出典
1	DMG 森精機 （機械）	・ 制御システムのデータをクラウド基盤上に収集 ・ AI を活用してデータを分析することで、顧客に納入した工作機械の予防保全・工程の効率化、機材のメンテナンス性向上や不良率の削減	品質改善 保守・保全の効率化 工場外との情報連携	https://www.itmedia.co.jp/news/articles/1901/22/news116.html https://monoist.itmedia.co.jp/mn/articles/1901/23/news050.html
2	小松製作所 （機械）	・ 工作機械や溶接ロボットなどからデータ収集 ・ データの可視化、無駄なプロセスの削減し加工効率の改善 ・ 機械学習による溶接品質判定	品質改善 生産計画改善	https://www.itmedia.co.jp/news/articles/1904/09/news001.html https://monoist.itmedia.co.jp/mn/articles/2005/01/news034.html
3	ダイキン工業 （機械）	・ 工場内機器を IoT 化し、製造データを可視化、異常予測や作業の遅れを予測 ・ 可視化したデータを元に製造工程を改善し、2021 年度は 2019 年度と比較しロス 3 割減を達成	品質改善 機械化・自動化・最適配置 保守・保全の効率化	https://xtech.nikkei.com/atcl/nxt/column/18/01970/030200002/
4	牧野フライス製作所（機械）	・ 5G ネットワークを経由したクラウドからのロボット制御 ・ ロボット制御による工具搬送自動化およびモニタリング ・ 不具合発生時に遠隔地から調査・対処可能 ・ リアルタイムに詳細ログを確認可能	品質改善 保守・保全の効率化 生産計画の改善	https://www.makino.co.jp/ja-jp/press-release/5g-network https://pages.awscloud.com/rs/112-TZM-766/images/20220407-AWS_SmartFactory_3_MAKINO-Milling.pdf
5	ヤマザキマザック （機械）	・ 機械の稼働状況や操作データをクラウド上で管理・分析し故障予兆の効率化 ・ 工作機械の機能拡張におけるソフトウェアアップデート配信が可能	保守・保全の効率化 工場外との情報連携	https://xtech.nikkei.com/atcl/nxt/news/18/03232/

#	対象企業（業界）	事例	着目したキーワード	参考・出典
6	アイシン （輸送用機器）	・ 生産ラインで状態監視システムを稼働 ・ エッジ、クラウド形式をとり、学習モデルを設備に設置したエッジデバイスに配信 ・ IoT や AI を使って自動化、可視化することで省力化を図り、生産性を向上	品質改善 機械化・自動化・最適配置 保守・保全の効率化	https://aws.amazon.com/jp/solutions/case-studies/aisinaw-brainstech/
7	デンソー （輸送用機器）	・ 全世界 130 カ国にまたがる工場データを集約 ・ 収集したデータを分析、設備稼働、品質管理などに利用 ・ 海外工場のデータもリアルタイムで活用	品質改善 生産計画改善 工場外との情報連携	https://www.denso.com/jp/ja/news/newsroom/2020/20201005-01/
8	豊田自動織機 （輸送用機器）	・ 製造設備を IoT 化し稼働情報・品質情報の可視化 ・ エッジ、フォグ、クラウドの 3 レイヤーを設け検証負荷低減、可用性確保 ・ AI で製造設備、環境パラメータ変更の自動算出 ・ 熟練作業員の知見や作業をシステム化して不良品、品質確認工数の削減	品質改善 機械化・自動化・最適配置 保守・保全の効率化 生産計画改善	https://monoist.itmedia.co.jp/mn/articles/2102/19/news003.html
9	アズビル （電気機器）	・ 工場内に設置したバルブの稼働データを情報収集 ・ 稼働状況を可視化してバルブの故障予兆診断の実施 ・ 稼働テストをシステムから一括に実施し、点検工数の削減	品質改善 機械化・自動化・最適配置 保守・保全の効率化	https://www.azbil.com/jp/product/factory/support-training/lifecycle-support/control-valve-solution/services/index.html
10	ファナック （電気機器）	・ 工場内の様々なデータや作業時の人的データ、マニュアルなどの資料データをクラウド上に収集 ・ 工作機械業界内の重複している業務の効率化や工数削減	機械化・自動化・最適配置 工場外との情報連携 生産計画改善	https://www.fanuc.co.jp/ja/profile/pr/newsrelease/2019/news20190912.html

#	対象企業（業界）	事例	着目したキーワード	参考・出典
11	旭化成 （化学）	・ 製造 IoT プラットフォーム（IPF）の構築 ・ 「製造現場データの分析・見える化基盤」と「アドホック・データ分析基盤」を構築 ・ 機械学習により、製造機器の故障予測の高度化（20 日前予測を 5 ヶ月先予測に改善）によるロス削減	品質改善 機械化・自動化・最適配置 保守・保全の効率化 生産計画改善	https://aws.amazon.com/jp/solutions/case-studies/asahi-kasei/
12	三井化学 （化学）	・ 国内主要拠点で IoT デバイスを導入 ・ プライベートクラウド構築によるリアルタイム分析 ・ エッジコンピューティング化による BCP 向上	品質改善 生産計画改善	https://jp.mitsuichemicals.com/jp/release/2021/2021_0826.htm
13	キリンホールディングス （飲料品）	・ 生産データを蓄積・分析する IoT 基盤を工場内に導入 ・ データ収集、連携・蓄積、加工・分析、可視化を実現	品質改善 生産計画改善	https://news.mynavi.jp/techplus/article/20201125-1527425/
14	JFE エンジニアリング （建設）	・ AI やビッグデータを活用したプラントの異常検知のため、クラウドを活用したデータ解析プラットフォームを構築 ・ プラント異常予兆検知の早期化により、運転障害の未然防止・トラブル時の迅速な正常化対応を実現 ・ ビッグデータ蓄積による、AI を活用した異常予兆検知や最適制御の実現	品質改善 機械化・自動化・最適配置 保守・保全の効率化	https://www.brains-tech.co.jp/case/case10-jfee/ https://www.jfe-holdings.co.jp/investor/library/dxreport/2021/pdf/all.pdf

表 3-1 の事例のように工場内のデータの可視化・分析基盤としてクラウドを利用し、データの可視化・予知保全など、機器などの制御に直接影響しない用途で使用されることが多く見られた。一方で、少数ではあるが、制御までクラウドを活用しているところもある。これらは制御システムで特に気にされている可用性やレイテンシを考慮した結果であると考えられる。今後、可用性やレイテンシなどを考慮できれば、5G や MEC などの技術を活用することで、制御に利用することも増えてくる可能性も考えらえる。

上記の活用形態を鑑み図 3-2 に活用事例を抽象化したモデルを示す。パターン 1 は判断を人・機械共存しているパターンである。このパターンが一番多く、データをクラウドに集約し可視化によって人が分析、または機械（AI モデル）による分析を行い、最終的には人が判断して製造現場の制御システム環境（ICS 環境）の設備に対して操作を実施する。

パターン 2 は分析・操作を機械（AI モデル）が担うパターンである。ICS 環境で設備の操作を行う AI モデルを「高速応答に特化したエッジ側モデル」、「モデル構築（学習）に特化したクラウド側モデル」の 2 つに機能分離をしている。パターン 1 と同様にクラウド側にモデルが存在するメリットとして、データがクラウド側に保管されており、モデル構築・更新する際に現場に行く必要がない点である。また実際に AI モデルが制御（推論）する場合はエッジ側モデルを利用する。このメリットとしては制御が現地で完結しているため、レイテンシの問題の解決はもちろん、クラウドの障害によってクラウド側にアクセスできなくとも継続可能な点である。一方で、エッジ側のモデルを搭載する機器の設置や管理が必要になる。

パターン 3 は分析・操作を機械（制御ロジック）が担うパターンである。パターン 2 との違いとしては操作をクラウド単独（制御ロジック）で実現している場合である。可用性やレイテンシの課題をクリアする必要はあるが、課題を解決できるのであれば現地に行かずして制御ロジックの変更はもちろん、他拠点への展開も容易となる。

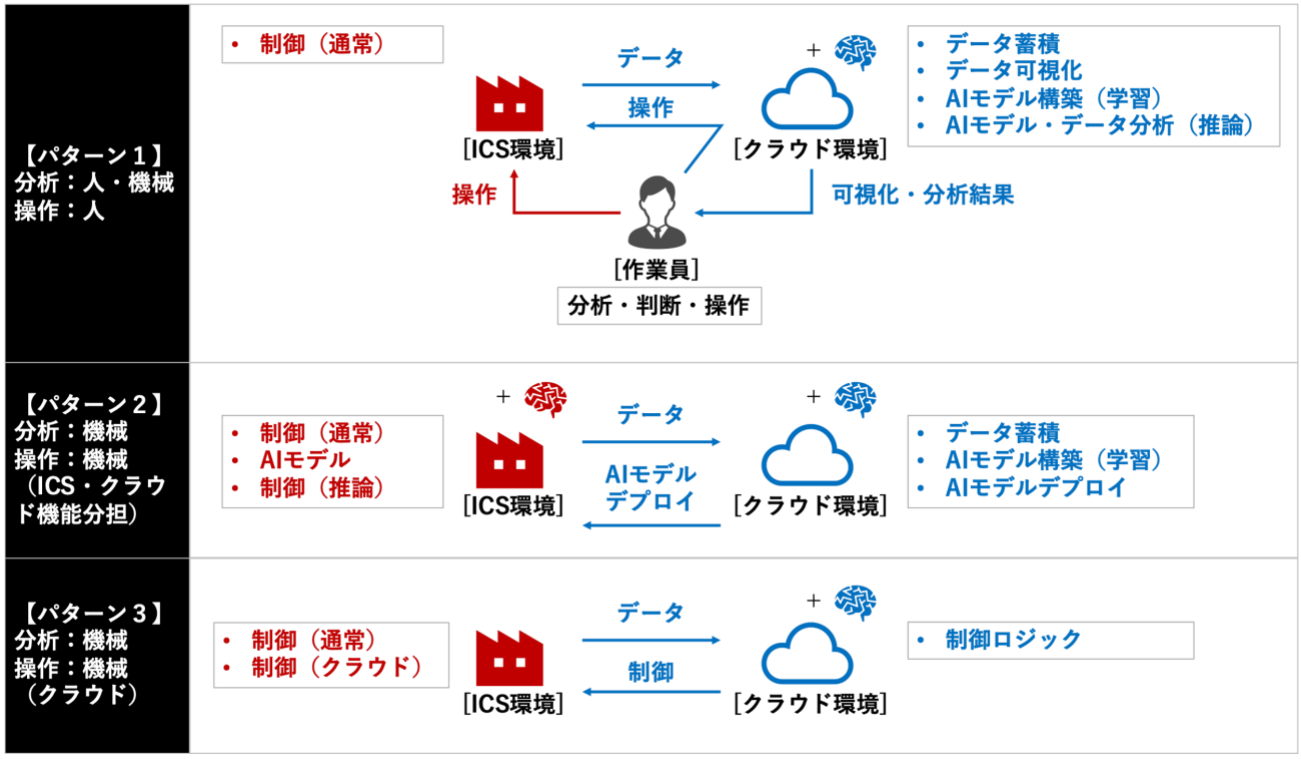


図 3-2 ICS 環境におけるクラウド活用パターン

3.2 データ利活用事例（国外）

国外事例の一例として IT ベンダー企業の取り組みである Cognite 社、ユーザー企業の取り組みである Moderna 社の 2 社を取り挙げる。

Cognite 社

Cognite 社は国内事例のようにデータ収集・分析基盤の用途として、DataOps プラットフォームを SaaS/PaaS として展開している[27]。

プラットフォームでは従来の IT データ（装置データ・作業指示など）、OT データ（時系列・イベントデータなど）、エンジニアリングデータ（文章、シミュレーションデータ、3D データなど）を集約できるようにしている。これらの膨大なデータは従来多くの部門毎に異なるフォーマットや管理システムで情報を管理しているケースが多く、プラットフォームで全てのデータの一元管理を可能としている。加えて、これらデータを用いてデジタル空間にリアルタイムの現場環境を再現するデジタルツインを実現している。デジタルツインを構築することにより、新たな試みへの着手や、問題発生時の原因追求・再現などがデジタル上で実現可能となっている。

なおサイバーセキュリティのサポート組織管理に関しては、各種規制や基準に準拠できるよう設計するなど力を入れている。

Moderna 社

COVID–19 のワクチン開発でも有名な米 Moderna 社は国内事例のようなデータ収集・分析基盤としての用途のみならず、製造プロセス自体をクラウド移行している。

Moderna 社 CDO の Damiani 氏によると、Moderna 社はほぼ完全にクラウドベースで事業をおこなっている [20]。作業者はクラウド上にある専用ポータルを介して、ワクチンの製造に必要なタンパク質の情報と研究データにアクセスできる。その後、専用ポータルから指示を出すだけで自動化された製造プロセスによって、すべてのステップでデータを収集しながらワクチンを生成する。データサイエンティストは、タンパク質からワクチンを効率的に作成するアルゴリズムを構築し、そのアルゴリズムはクラウドサービスの AI などを活用して研究を推進している。さらには製造側でもデジタル化を進めており、ペーパーレスかつ、製造プロセスにおいて必要なシステムもクラウド上に存在している。

上記のように Moderna 社はデータの利活用によって迅速に COVID–19 に対応するワクチンを製造し、かつ製造プロセスを構築、自動化することによって世界中の人々にワクチンを提供出来た。このように迅速に顧客へのサービスを提供することできたことで、市場でも評価された[28]。これは、研究と工場のクラウド化とデータ利活用が大きな要因の一つであると考える。

---

[27] Cognite 社 https://www.cognite.com/ja-jp/

[28] COVID-19 が流行し始めた 2019 年 12 上旬（2019 年 12 月 2 日時点）の株価は 15.33 米ドルであったが、1 年後の 2020 年 12 月 1 日は 141.01 米ドルと 1 年間で約 9.2 倍となった。執筆当時の 2022 年 6 月 1 日時点では 143.40 米ドルであったが、2021 年 8 月 10 日は 456.76 米ドルとなり、2019 年 12 月 2 日比で約 30 倍となった。もちろん、外部環境（景気や為替など）によっても株価は変動するため参考までの数値とされたい（株価は全て終値）。

製造プロセスなど企業において機密とされている部分に関しても、クラウドサービスを活用している事例は日本企業ではほぼ見受けられない。適切なセキュリティの管理を行い、クラウドサービスを十分に活用することで Moderna 社のような恩恵も日本企業でも享受できるものと考えられる。

3.3 データ利活用事例まとめ

本章で紹介して来たように、データ利活用の一手法としてクラウドサービスを積極的に活用することで、既存ビジネスの効率化や新規事業の創出といったメリットを享受できる。

一方で、それに伴いリスク・懸案事項が増加している。様々な要素に起因し発生するセキュリティインシデントの動向や実事例について、次の第 4 章で述べる。

第4章　　セキュリティインシデント事例

本章では、サイバー攻撃への考慮・対策が不十分であったために発生したインシデント事例を取り上げる。ICS に関係の深い OT セキュリティインシデント事例（4.1 節）並びにクラウドセキュリティインシデント事例（4.2 節）について記載する。

4.1 OT セキュリティインシデント事例

OT 環境におけるセキュリティインシデント事例を表 4-1 に示す。

従来の OT 環境に関しては、IT と物理的・論理的に切り離されていたことから安全に関する議論こそあったものの、サイバーセキュリティへの関心は薄かった。しかし、2010 年にイランの核燃料施設を操業停止に追い込んだ「Stuxnet」が OT 環境を標的とした世界初のマルウェアとして話題を呼んだことを皮切りに、OT セキュリティインシデントのインパクトの大きさに注目が高まっている。セキュリティインシデントに関しては、インターネットや USB メモリなどのリムーバブルメディア、電子メールなど様々なマルウェアや攻撃者の侵入経路が考えられる。しかし、「OT 環境は IT 環境と比較して、設備が長期稼働していること」、「OT 環境と IT 環境の境界が曖昧になってきたこと」、これらのことから脆弱性への対応の困難さや侵入経路の増加を考慮し、環境に応じた対策を講じていく必要がある。

なお、本節で取り上げた事例は「重要インフラに関わる製造業」という観点で調査・整理したセキュリティインシデントのごく一部であり、業界・年代に関して網羅的にまとめたものではないことに留意されたい。

表 4-1 OT セキュリティインシデント事例

#	対象	業界	発生国	発生年月	内容・原因	参考・出典
1	核開発施設	電力	イラン	2010 年	・核施設における遠心分離機の設定が改ざんされ、操業が一時停止した。 ・施設内に持ち込まれた USB メモリからマルウェアが制御ネットワーク内に感染拡大した可能性が高い。	https://www.ipa.go.jp/files/000080701.pdf
2	製鉄所	製造(鉄鋼)	ドイツ	2014 年 12 月	・溶鉱炉が正常にシャットダウンできず、装置及び製鉄システム（操業）に大きな損害が生じた。 ・標的型攻撃メールにより制御システムの操作権限を奪取された。	https://www.ipa.go.jp/files/000080712.pdf
3	ウクライナ電力網	電力	ウクライナ	2015 年 12 月	・社内での不審メール開封により PC がウイルスに感染した。 ・SCADA 制御の掌握により変電所の電源をリモートで切断された。 ・IT インフラのコンポーネント無効化やコールセンターへの DoS 攻撃も並行して実施されていた。 ・最大 6 時間の間、40～70 万人程度に影響を与えた。 ・2016 年にもマルウェア（「Industroyer」と呼ばれるマルウェアの亜種）による ICS への攻撃が確認され、同様のインシデントが発生した。	https://www.ipa.go.jp/files/000076755.pdf https://www.ipa.go.jp/files/000080712.pdf https://www.jpcert.or.jp/present/2016/20160217_CSC-JPCERT01.pdf
4	TSMC	製造(半導体)	台湾	2018 年 8 月	・各 PC のデータが暗号化されて開けなくなり、生産が停止した。 ・製造用ツールをインストールした PC がランサムウェア（「WannaCry」と呼ばれるマルウェアの亜種)に感染しており、ネットワーク内に拡大した。	https://japan.cnet.com/article/35123656/ https://www.ipa.go.jp/files/000080712.pdf
5	ASCO	製造(航空)	ベルギー	2019 年 6 月	・ベルギーの工場がランサムウェアに感染し、ドイツ、カナダ、米国の工場の操業を停止。従業員 1000 人が影響を受けた。	https://ics-cert.kaspersky.com/publications/news/2019/06/14/asco-ransomware/

#	対象	業界	発生国	発生年月	内容・原因	参考・出典
6	本田技研工業	製造(自動車)	日本他	2020 年 6 月	・サイバー攻撃により北米、インドなどを含めた国内外拠点が生産停止に陥った。 ・詳細は非公開。ランサムウェアの可能性が高いと指摘されている。	https://piyolog.hatenadiary.jp/entry/2020/06/10/030123
7	Tesla	自製造(自動車)	米国	2020 年 8 月	・従業員が成功報酬 100 万ドルでマルウェアを社内システムに仕込むよう、容疑者から持ちかけられた。 ・買収された社員はテスラに報告し、容疑者は逮捕。被害を受けずに済んだ。	https://www.dnp.co.jp/biz/column/detail/10161903_2781.html
8	Colonial Pipeline	石油	米国	2021 年 5 月	・サイバー攻撃を受け 100GB のデータが窃取された。 ・OT 領域への被害を防ぐためにパイプラインの操業を停止、米国国内ではガソリン供給に大きな影響が出た。 ・身代金を支払ったものの復旧には時間を要した。 ・攻撃にはランサムウェアが使用された。 ・VPN を通じ社内システムに侵入された。VPN のパスワードは単純ではなかったが既に侵害されたパスワードであった。また多要素認証を使用していなかった。	https://piyolog.hatenadiary.jp/entry/2021/05/12/051650
9	小島プレス工業	製造(自動車)	日本	2022 年 2 月	・サイバー攻撃により社内システムに不具合が発生、生産が困難となった。 ・取引先のトヨタが生産への影響を考慮し、全拠点の生産を停止(翌日には生産再開)した。 ・特定外部企業との通信に使用していたネットワーク機器の脆弱性を利用した攻撃が実施された（詳細は開示されていない）。 ・社内ネットワークに侵入後、ランサムウェアにてデータを暗号化された。	https://www.chunichi.co.jp/article/445050

これらの OT セキュリティインシデントから、以下のような点が読み取れる。

① 業界を問わずセキュリティインシデントが発生している。また、米国 ICS-CERT が公表した ICSA（ICS 用機器)、ICSMA（医療用機器）の脆弱性が年々増加傾向にある [21]。
② 自社のセキュリティインシデントがサプライチェーンを通じて他社に影響を与える。
③ 人（内部不正）を狙った攻撃経路もあり、入退室管理などの物理セキュリティ、IT セキュリティ、エアギャップ[29]による対策が通用しない場合がある。
④ 電力や石油などの重要インフラ業種が攻撃を受けると社会・経済に大きな影響があるだけでなく、直接的または間接的に人命に関わる場合がある。
⑤ 標的型攻撃メールなど IT 環境への攻撃に起因し、OT 環境が操業停止にまで陥る事態が多数報告されている。このことから IT・OT 環境が繋がっている事例が増えていることや、境界での対策が不十分なまま接続されている危険な環境が少なからず存在していることが読み取れる。
⑥ 企業の事前の対策や対応力によってセキュリティインシデントが長期化する恐れがある。
⑦ 多要素認証に対応していないレガシーな VPN 装置（Colonial Pipeline などの事例）や既知の脆弱性への対応ができていない機器を侵入されるケースが見られる。侵入後、（パッチ適応など）対応不十分な機器を WannaCry（TSMC の事例）などに感染させ、影響拡大させている。
⑧ Stuxnet や Industroyer と言った ICS 製品の脆弱性を悪用した攻撃が発生している。

これまで紹介した事例からわかるように、サイバー攻撃による被害は、業種や企業の規模とは関係なく発生していることがわかる。事業内容によっては情報の漏えいに留まらず、特に製造業においてのサイバー攻撃は生産停止など物理的な影響が発生している。またウクライナのような停電発生など、社会インフラにサイバー攻撃を受けると間接的に人命に関わる被害に至る事態も発生している。

また、サイバー攻撃による被害は自社だけに留まらず、製品供給の遅滞やマルウェアの感染拡大などにより、取引先に影響を及ぼす事例も見られる。取引先に影響を及ぼさないよう、自社のセキュリティ対策推進と並行し、取引先が被害に合わないよう企業間で連携したセキュリティ対策の検討も望まれる。

さらに、被害の起点となるのはインターネットを経由したサイバー攻撃だけでなく、組織内の従事者が内的/外的要因により不正を働くケースもある。

OT に関わるサイバーセキュリティは従事する社員一人ひとりのセキュリティに対する意識の向上はもちろんだが、物理侵入の対策や分離した LAN への不正接続などを検出し対応する体制など、OT・IT 部門が協働し取り組んでいく必要がある。

[29] 機器やシステムをインターネットなど安全でなはないネットワークから物理的に切り離すこと。

4.2 クラウドセキュリティインシデント事例

クラウドでのセキュリティインシデント事例を表 4-2 に示す。

オンプレミスの設備と比較し、クラウドは管理できる範囲（裁量）が狭く、場合によっては、組織のニーズに応じた検知・対応のためのソリューションを導入できない。そのため、セキュリティインシデントの検知・対応が困難になる場合がある。従って、クラウドにアップロードするプロセスやデータの熟考はもちろん、設定の管理や暗号化・冗長化など、様々な面からセキュリティリスクを洗い出し、対応を検討する必要がある。また、自社での運用・設定ミスに起因したセキュリティインシデントのみならず、自社が攻撃を受けずともクラウド事業者が受けたサイバー攻撃・起こした障害によってサービス影響が発生し得ることも忘れてはならない。なお、4.1 節と同様、本節で取り上げたセキュリティインシデントは世界中で発生しているもののごく一部であり、クラウド利用企業で発生した著名なセキュリティインシデント・各クラウド事業者で発生したセキュリティインシデントの一例を挙げたものに過ぎない。

表 4-2 クラウドインシデント事例

#	対象	業界	発生国	発生年月	影響・原因	参考・出典など
1	Uber Technologies	運輸	米国	2016 年 10 月	・クラウド(AWS)上に保存していた全世界の Uber 登録ユーザー5700 万人の個人情報が漏洩した。 ・同社は漏洩したデータ削除のため、攻撃者に 10 万ドルを支払った。 ・GitHub への不正アクセスが行われ、そこで得た認証情報から AWS のアカウントに侵入された。	https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data
2	ソフトバンク	情報通信	日本	2020 年 2 月	・社員が退職する際に私物 PC からソフトバンクの利用するクラウドサーバーへ接続、営業秘密情報を持ち出した ・データへのアクセス権限の最小化、退職者の振る舞いに問題があった。	https://www.softbank.jp/corp/news/press/sbkk/2021/20210112_01/ https://piyolog.hatenadiary.jp/entry/2021/01/13/181011
3	Salesforce	情報通信(クラウド事業者)	米国	2020 年 12 月	・2016 年にリリースされた Web サービス機能において、（設定値を変更していない場合）外部から認証無しで情報を参照出来る状態になっていた。結果、当該クラウドサービスを利用していた数多くの企業から情報漏洩が発生した。 ・利用企業側で設定に関する確認を徹底することで、情報漏洩を防げていた可能性がある。	https://piyolog.hatenadiary.jp/entry/2020/12/28/060000
4	Microsoft	情報通信(クラウド事業者)	米国	2021 年 3 月	・認証を Azure AD に依存している Microsoft やサードパーティーのサービスが約 14 時間程度接続しにくくなった。 ・Azure AD のセキュリティ対応などの業務プロセスに不備があった。	https://japan.zdnet.com/article/35167925/

#	対象	業界	発生国	発生年月	影響・原因	参考・出典など
5	Atlassian	情報通信	オーストラリア	2021 年 4 月	・同社が提供するタスク管理サービス「Trello」にて、一部ユーザーの公開設定不備により、ボード内の情報がインターネット上に公開されている事象が発生した。 ・個人情報や機密情報の流出が相次いで発覚したため、国内でも NISC が公式 Twitter 上でプライバシー設定を確認するよう呼びかけた。	https://www.atlassian.com/ja/blog/trello-public-board https://twitter.com/nisc_forecast/status/1379309590081236993
6	Amazon Web Services	情報通信(クラウド事業者)	米国	2021 年 9 月	・企業のデータセンターなどから AWS へ専用線で接続するためのネットワークサービスで障害が発生した。 ・銀行のスマートフォンアプリ、空港でのチェックインシステムに影響が出るなど、幅広い社会サービスが影響を受けた。 ・AWS 側のネットワーク機器に関する障害が原因であった。	https://www.itmedia.co.jp/news/articles/2109/08/news091.html
7	富士通クラウドテクノロジーズ	情報通信(クラウド事業者)	日本	2022 年 5 月	・一部のロードバランサーの脆弱性を悪用され、不正アクセスが行われた ・当該ロードバランサー上の証明書データや、当該ロードバランサーを通過した通信を窃取された可能性がある。	https://pfs.nifcloud.com/cs/catalog/cloud_news/catalog_20220516100 0_1.htm

これらのクラウドセキュリティインシデントから、以下のような点が読み取れる。

① 設定ミスによりサービスが社外からアクセス可能な状態になってしまうなど、運用の不手際による情報漏えいのリスクが高まる。
② 各社が契約したサービスの運用に関わる過失だけでなく、クラウド事業者の過失に起因したセキュリティインシデントによりサービス影響が発生する場合がある。
③ クラウドサービスの仕様変更により、新たなリスクが生まれる場合がある。
④ 個人情報保護に関する検討は特に重要である。例えば設定ミスや不正アクセスにより万が一個人情報を窃取された場合を想定して、仮名化・匿名化などの処理は行われているか、データの暗号化や別の管理者による鍵管理はされているか、などが検討例として挙げられる。
⑤ ソースコードに認証情報を直接記載してはいけない。
⑥ 仮に認証情報が窃取されたとしても被害が最小限に留まるよう、アカウントの権限分離をすべきである。

4.3 セキュリティインシデント事例まとめ

本章では OT やクラウドにおけるインシデントについて紹介した。

JPCERT/CC によると ICS 環境の一層のオープン化の副作用として、サイバー攻撃の対象の拡大があると言われている。具体的には ERP や MES がクラウドに移行、クラウドと連携して稼働する IIoT 機器の導入、IT システムと OT システムの融合、などクラウドサービスの利用の拡大について記載されている [21]。なお Trend Micro 社の 2022 年 2 月～3 月における「産業制御システムのサイバーセキュリティ実態調査」によると、ICS 環境でも業務効率化のためにクラウドサービス利用に起因したサイバー攻撃被害が発生していると判明した。調査項目の一つである「産業制御システムが攻撃を受けたサイバー攻撃の種類」についての質問では、回答者の約半数がクラウドサービスに起因していると結果が出ている。具体的には、「クラウドサービスの脆弱性を利用したサイバー攻撃（53.3%）」、と「クラウドサービスの設定間違いを悪用した攻撃（48.7%）」の被害にあったと回答している[30] [22]。

このようにサイバー攻撃の高度化やクラウド導入によるリスクの増加に伴い、セキュリティ対策の必要性も高まる。しかし、導入技術の幅を広げデータ利活用を推進しない場合は DX に乗り遅れ、ビジネスチャンスを失いかねない。従って、リスクを正しく認識し、適切にセキュリティ対策を講じることで、ビジネスメリットを享受しながらリスク低減を実施することが必要である。

[30] 調査対象：アメリカ（300 名）・ドイツ（300 名）・日本（300 名）の従業員 1,000 人以上の製造・電力・石油/ガス産業の企業に所属する産業制御システムのサイバーセキュリティ対策を決める意思決定者 900 名が対象。

これらのインシデントの傾向から、少なくとも以下のような点には注意を払うべきであると言える。

① 物理的なセキュリティ（入退室管理、USB メモリの管理など）の強化
② IT-OT 間のネットワーク境界防御の強化
③ VPN 端末におけるセキュリティの強化（パッチ適用、多要素認証など）
④ クラウド上に保存しているデータの公開範囲/アクセス権設定など、設定内容の管理（デフォルトの設定のみならず、サービスの機能拡張や仕様変更への追従も重要）
⑤ クラウド事業者側で障害が発生した際の運用方針の策定

また、ICS 環境とクラウド環境を接続するが故に、企画・導入・運用においての課題が生じることがある。直近で ICS 環境にクラウドサービスを導入した各企業の取り組みについて、調査した結果を次の第 5 章にて述べる。また、実際にセキュリティ対策を講じる上での脅威分析やセキュリティ対策については第 6 章にて述べる。自社に導入にする際にそれぞれ参考にされたい。

第5章　　クラウド導入における課題および乗り越え方

本章では、実際に制御システム環境にクラウドを導入した組織にヒアリングを行い、その分析をした結果を述べる。「中核人材育成プログラム」[31]の広い人脈を活かし、8 組織にヒアリングを実施し、「データ利活用」と「セキュリティ」に対してどのような課題があり、それをどのように乗り越えたか伺うことができた。これからクラウド導入に挑戦する企業でも同様の課題に直面することが想定されるため、課題解決にあたり参考にされたい。

5.1 節で、ヒアリング結果から得られた課題とその乗り越え方をプロセスと観点で整理する。5.2 節から5.4 節で、各プロセスでの課題とその乗り越え方を述べる。

5.1 クラウド導入のロードマップ

多くの組織では、クラウドを導入するまでに、企画、導入、運用の順にプロセスを進めていた。企画フェーズでは、自組織が解決すべき課題を抽出、解決するためのソリューション検討、人員の確保並びに組織文化の醸成などを行う。導入フェーズでは、開発、試験導入を経て、クラウドサービスが実稼働するまでの導入作業を担う。運用フェーズでは、システムの維持、人材の確保・育成、セキュリティの確保などを行う。各フェーズに考慮すべき課題があり、組織ごとに様々な方法で乗り越え、成果（導入効果）を出していることが分かった。

本指南書では、それらの考慮すべき課題を「組織」「人」「技術」の観点で整理した（図 5-1）。

図 5-1 ヒアリング結果で明らかになったクラウド導入の課題、導入効果、残課題（n=8）

[31] 独立行政法人 情報処理推進機構 産業サイバーセキュリティセンターが取り組んでいるセキュリティの観点から企業などの経営層と現場担当者を繋ぐ人材（中核人材）を対象とした教育プログラムのこと。社会インフラ・産業基盤のサイバーセキュリティ対策の強化をテーマに、テクノロジー（OT・IT）、マネジメント、ビジネス分野を総合的に学ぶ 1 年間程度のトレーニング内容となっている。

5.2 企画

クラウド導入を企画するフェーズにおいて以下の課題が明らかになった。

[#01] 組織的な課題１：迅速な意思決定の実現

クラウド導入では迅速な意思決定が欠かせない。タイムリーに成果（導入効果）を出し、経営層やユーザーの期待に応えることは、クラウド導入を進めるにあたり重要である。また、企画から導入までに時間がかかってしまうと、事業部門が独自にクラウドを導入して、統制が取れず失敗してしまうこともある。

ある企業では、参考となる情報が得られない中でクラウド導入に取り組んだ。PDCA の”Do”、”Act” に重点を置き、”Plan”、”Check”には時間をかけないことを意識し、早期に成果を出すことに注力していた。アウトソーシングを活用しつつも早々に内製化することを重点課題と設定し、自社にノウハウを蓄えることで管理可能な領域を増やし、組織的な知見を蓄え、継続的にスピード感を持った対応を実現していた。

別の組織では、クラウド導入の背景としてオンプレミストと比較して開発環境を即時立ち上げられるなど、スピード感を持って開発を行える「開発のしやすさ」を挙げている。また、オンプレミスなどでは機器を所有すると老朽化への対応が必要となるため、「維持運用の手間が少ない」点も、クラウド導入を後押しする理由となった。

別のある組織では、「後からスケールを変更できる」点を挙げている。必要最小限のシステム構成でクラウド導入し、うまくいかなければ最小限のコストで撤退が可能である。コストに関心の高い関係者には有効な訴求方法と言える。

[#02] 組織的な課題２：クラウド導入に対する反発への対応

制御システム環境へのクラウドの導入を企画すると、外部とデータが送受信されることや業務環境の変化を嫌った関係部門からの反発を経験し、導入に苦労した組織は多かった。こうした反発に関しては関係者の不安を取り除く活動や、理解者を増やす活動が有効であった。

ある組織では、操業への影響に関する不安に対し、操業へ影響させないクラウドの構成にすることを工場関係者へ丁寧に説明することで不安を取り除いていた。またクラウド導入時の構成に関しては企画段階からセキュリティ部門と一緒に検討を取り組むなどの工夫を行なっていた。

別の組織では、デジタル技術により生産プロセスを改善していきたい前向きな人を巻き込みながらクラウド導入に着手することで社内での理解者を増やす活動を行なっていた。着手する対象に関しても理解を得られやすい工場からスモールスタートで取り組み、成果を上げていた。また得られた成果を社内展示会に出展することで、クラウド導入に関わる取り組みを広めることができた。

[#03] 組織的な課題３：全体最適化

企業全体を俯瞰した最適化を行うには、関係部門に協力を仰ぎ、統制を取る必要がある。システム運用の一元管理によるコスト低減や、一括契約による単価の引き下げが期待できる。

ある組織では、各部門の裁量でシステムを導入してきた経緯があり、部署ごとで個別最適された状態となっており、類似のシステムを重複して開発しているなど、非効率であった。そこで、クラウド導入に伴い経営トップから号令をかけることで、全社最適を意識する風土が芽生えてきた。

[#04] 人的な課題１：クラウド導入を担う人材の確保

クラウド導入に限らず、DX は専門に特化した人材が担うことが望ましい。そのため、自組織にとってどのような人材が必要であるか定義することが重要である。

ある組織では、DX 人材に求めるスキルを、テクノロジーごとに整理していた。例えば、データサイエンティストであれば画像系処理や時系列系処理のどちらを得意とするか、クラウドエンジニアであれば、フロントエンド系なのかバックエンド系なのか、幅広い対称を得意とする人材が必要なのか、一つのことに特化した人材が必要なのか、などの様々な観点から求める人材を明確にする事で、DX 推進を円滑に進める土台を構築していた。その結果、組織的に DX を進める体制が整い、専門知識を生かした迅速な意思決定を実現していた。

[#05] 技術的な課題１：安全性の確保

クラウド導入においては、少なからず生産設備に対し変更を加える場合がある。多くの組織では、クラウド導入に伴うシステムや設備の構成変更が生産業務に与える影響を懸念され、関係者から可用性や機密性の確保を求められていた。

ある組織では、生産業務における安全面をローカル機器で保証するとともに、実験が許される範囲を模索していた。具体的には、制御システムのうち一部の機能はクラウド上で動作するが、リアルタイム性が求められる機能はローカルに残していた。クラウドとローカルの役割分担を見定めようとする活動により、仮にクラウドとの通信断やクラウド自体の障害が発生しても操業に影響しない範囲を考察し、安全性を考慮したクラウド活用計画を策定していた。

別の組織では、心理的な不安を取り除くために片方向通信ゲートウェイを採用した。クラウドを活用しても外部から侵入されない構成であることをシンプルに説明でき、現場が抱える心理的な不安を取り除くことに成功した。また、構成がシンプルになったことで、関係者に対して説明しやすいといった副次的メリットも得ることができた。

5.3 導入

導入フェーズにおいては、多くの組織が、開発、試験導入、本番導入の順でプロセスを実行し、一定の安全性を担保しながら導入する事例が多かった。

[#06] 組織的な課題１：導入をやり切る情熱

制御システム環境へのクラウド導入においては、実証実験から本番導入へ移る際、大きな障壁があることを理解したうえで取り組む必要がある。例えば、本番導入時に実証実験では判明しなかった様々な課題が発生して挫折した事例や、本番導入が進む過程で制御システムの改修や設備の増強などが必要となり、実証実験段階で想定した 10 倍以上の費用がかかった事例もある。このように、実証実験から本番導入へ進む過程では様々な困難やリスクが発生する可能性を認識し、それでも最後までやり遂げようとする気持ちをしっかり持ち続けることが重要な成功要因となる。また、うまく推進できそうにない場合は、最小の失敗で撤退を判断するなどの判断基準とそれを容認する環境づくりも重要である。

ある組織では、今後のクラウド活用拡大を見据えて、本番導入時の安全性やセキュリティ対策が課題となった。同組織の情報システム部門が主体となり、セキュリティも含めてクラウド導入を推進していた。ネットワークレイヤーのセキュリティ対策状況のアセスメントを行い、一部の機能をあえてクラウドで実装せずローカルで実装させるなどの工夫を凝らし、関係部門を巻き込み、安全性を担保した形で導入に踏み切り、クラウドの導入を実現した。

[#07] 人的な課題１：ノウハウの蓄積

クラウド導入には、クラウドに関する技術を持った人材が社内に必要不可欠である。導入や運用のプロセスを経てノウハウを蓄えることにより、迅速な開発や、他拠点への迅速な展開を実現できる。

ある組織では、クラウドの知見を持った技術者がいなかったため、クラウドの導入に苦労していた。クラウドのノウハウを蓄えるため、社内勉強会の開催やクラウド事業者からの技術援助をもらいながら社内人材の育成に取り掛かった。

[#08] 人的な課題２：ベテラン社員によるデータの分類

データを利活用するには、データを分類し分析可能な状態にする必要がある。分類作業を行う際は、現場エンジニアに対し、どのデータにどのような意味があるかを確認し、部門を超えた協力体制で進めることが望ましい。

ある組織では、システムを設計する IT エンジニアが、製造ライン異常予測を実現するためにどのようなデータを収集すれば異常を判別できるか把握していなかった。集まるデータを正常な値と異常な値に分類し異常データにラベリングを施すため、製造ラインの保守に関するベテランエンジニアをクラウド導入の検討に参画してもらうことにした。部門を超えた協力体制をとることで、データ分類やノウハウの共有を行い、データ分析が可能な体制の構築に成功していた。

[#09] 技術的な課題１：機密性の確保

クラウドでデータを分析するには、オンプレミスのデータをクラウドにアップロードする必要がある。通信経路を流れるデータの盗聴や、クラウドとの接続箇所から不正アクセスを受ける事態を想定し、セキュリティ対策を行う必要がある。

ある組織では、クラウド活用による新たなリスクとして、工場とクラウドサービス間の通信経路でデータが盗聴されることを懸念していた。そこで、システムを構築する基盤を厳選し、クラウド事業者と基盤の間で専用線が整備されている社外設備を活用することにした。社外設備には社内 LAN 経由でしかアクセスできない設定とした。その結果、工場から基盤を介してクラウドサービスに至るまでの一連の通信経路において、社内 LAN と同等のセキュリティ水準を確保することができ、不安を払拭できた。

別の組織では、制御システム環境のデータを取得し、クラウドに蓄積して分析する方法をとっていた。この際、データの機密性に関する課題が生じた。OT 領域と IT 領域では潜在的なセキュリティリスクが異なるため、セキュリティ対策も異なっている。元々分かれていたこれらの領域をネットワークで接続することは、機密性の低下（機密性が低い方の領域の水準となってしまう状態）を引き起こす原因となると考えた。そこで、データを蓄えるデータレイクと呼ばれる専用領域を用意し、OT および IT 領域から一方通行でデータを蓄積する構造とした。OT・IT 間で直接的にデータが行き来しない構造に加え、データレイク領域は API 経由のアクセスのみを許可する技術的対策も施し、組織として一定のセキュリティを担保できる構成を実現していた。

別のある組織では、製造業であるが故に自組織だけではソフトウェア開発が難しいという課題があった。PaaS や SaaS を活用し、使い分けることによって課題を乗り越えていた。また、さまざまな形態のクラウドサービス活用に伴い責任分界点を明確化したことは、セキュリティ対策への不安低減にも繋がっていた。

[#10] 技術的な課題２：可用性の確保

クラウド導入によってデータがクラウドに集約されるようになり、通信経路を流れるデータの欠損や、クラウド自体が停止するなど、オンプレミスでは発生しなかった可用性に関する懸念事項が生じる。万が一にクラウドとの通信断が発生した場合でも、事業を継続できるようなシステム構成を導入フェーズで検討することが重要である。

ある組織では、通信経路のどこかで障害が発生してデータの欠損が発生する可能性が高まる点を懸念していた。工場でのクラウド活用では、工場 LAN からクラウド基盤まで長距離のデータ伝送が発生するため、データ欠損の問題が生じる。そこで、オンプレミスのサーバにマスターデータを管理し、クラウドにはマスターデータのコピーのみを送信する構成を取っていた。これにより万が一の際に復旧する手段を確保することができ、データ欠損のリスクを許容した上で、クラウドによるデータ利活用の取り組みに着手できていた。

別の組織では、サーバレスという技術を用いて、アプリケーションだけを動作させる環境を整えていた。クラウドにデータを送りサーバレスで処理したり、分散データベースで保管を行ったり、など障害の影響を減らすための工夫を行なっていた。さらに、サーバ OS を維持する運用負担の減少や、サーバ OS を狙うサイバー攻撃に強い環境の実現といった副次的な効果も現れていた。ただし、サーバレス構成においてもアプリケーション自体の欠陥があれば可用性や機密性を損なう原因となる。システム構成によってはクラウドを通じて社内のデータを抜き取られる可能性もある。たとえサーバレスの技術を活用したとしても、アプリケーションレイヤのセキュリティリスクに対策を施す必要がある。

5.4 運用

クラウドを含め、システムは導入して終わるものではなく、継続的な運用が発生する。運用はシステムのライフサイクルで最も長い期間を占めるため、企画フェーズから運用フェーズを意識した検討を行うことが重要である。また、アウトソーシングを活用する場合は自社にノウハウが残らない点やアウトソーシング先のセキュリティの水準が異なる点も熟考し、予算や組織体制を鑑みた最適な運用方法を検討されたい。

[#11] 組織的な課題１：内製とアウトソーシングの選択

運用には専門のノウハウが必要であり、長期間にわたって運用を担う人員の確保が必要である。どの組織でも人的リソースが限られているため、運用を内製で行うか、あるいはアウトソーシングを活用するかを検討する必要性が生じる。

ある組織では、システムの運用を戦略的観点で内製化していた。想定した運用業務は運用変更が発生する頻度が高いため、アウトソーシングすると運用変更時に調整の負担が大きくなると考えた。社内の人員で運用を担い、ノウハウを組織内に蓄えることで変化に強い組織を作り上げていた。

一方、ある組織では、将来的なセキュリティ維持管理の運用負担増を考慮して、外部サービスの活用を選択していた。クラウド事業者が提供するサポートサービスを有効活用し、セキュリティやパフォーマンスの状況を監視してもらうことで、提供される機能を効率的に使い、自社の運用負担の軽減を図っていた。

[#12] 組織的な課題２：データ管理体制

クラウド導入に伴い、工場内のデータはクラウドにアップロードされる。データの通信経路やインターネットとの接続箇所など、サイバー攻撃の起点となり得る箇所に対し、情報漏えい対策や不正アクセス対策といったセキュリティが求められる。

ある組織では、工場と IT 領域のネットワークを分離し、その間を通過するデータを監視する組織を設けていた。万が一に重要な情報が漏えいしたとしても、早期に検知し、被害を最小限に抑えるための体制を整えていた。

別の組織では、システムに使用するアカウントや、データ単位でアクセス可能な範囲を定め、日常的なモニタリングや定期的な棚卸を行なっていた。これにより、アカウント不正利用の早期検出や、情報公開範囲の適正化を実現し、一定の機密性確保に成功していた。

[#13] 組織的な課題３：セキュリティ体制の構築

サイバー攻撃が日々高度化する点を踏まえると、全ての攻撃から自社の資産を守り切ることは難しい。そのため、攻撃者が侵入してきた後の対応フローや復旧手順を確立しておき、対応可能な体制を整えておくことが重要である。

クラウドの運用においては、業界標準のガイドラインへの準拠を検討するケースが多い。加えて、自組織の状況に合わせ、OT セキュリティ規程の明文化、CSIRT というセキュリティ対応体制を構築する組織も多く見られた。また、CSIRT を IT 領域のセキュリティ対応体制と位置付け、工場セキュリティを担う FSIRT や、制御システムセキュリティ担う OTSIRT などを立ち上げ、CSIRT と連携する手続きを定める事例もある。

運用体制の立ち上げは、組織的・人的・技術的に様々な課題が生じるが、OT 部門の技術者が積極的に参画し、IT セキュリティの技術を身につけてもらうことで、全社的な組織体制の構築に成功する事例が多く見られた。

[#14] 人的な課題１：人材の継続的な育成

クラウドの運用が始まると、運用の効率化や運用ノウハウの蓄積などのアクションが求められる。多くの組織では、クラウドやデータ活用といった技術に詳しい人材を確保するため、人材育成の方法に工夫が見られた。

ある組織では、クラウド事業者と連携し、クラウドサービスに関するハンズオン形式の研修を開催していた。さらに、クラウド事業者との定期的な打ち合わせで課題を共有することにより、ユーザー側の不安解消に努めている。

別の組織では、工場の人材を対象とした半年間の教育プログラムを展開していた。ただし、データサイエンスに関するスペシャリストを育てるのではなく、各工場がデータを使って意思決定できる最低限度の教育に留めていた。教育内容を絞ることにより、多くの対象者に対しスピーディに教育プログラムを展開することに成功し、工場の人材だけでデータを使った意思決定できる体制が整いつつあった。

別の組織では、工場セキュリティを推進するチームを結成していた。情報システム部門の担当が主となり、各工場の総務部門と連携して 1 工場ずつセキュリティ教育に関する説明会を実施していた。

[#15] 人的な課題２：人材の士気向上

関係部門との衝突や利害対立など、次々に現れる課題への対応で担当者の士気が低下してしまうケースも見られた。働きやすい環境の整備や挑戦する機会を提供することで、担当者の士気向上に取り組む組織もあった。

ある組織では、人材を育てた結果、高い技術力を持った人材が転職市場に流れてしまうという新たな課題が生じた。そこで、高度人材を定着させるために、自社の職場環境を改善することで乗り越えようとしていた。具体的には、データ分析を行う担当者が豊富なデータを利用できるようにし、分析の自由度を高めることで担当者の探究心を満たそうとしていた。また、アジャイル開発などの取り組みにより短期的に結果を出しやすい環境を整えるなどの工夫をしていた。

[#16] 技術的な課題１：セキュリティ規定に則った対策

セキュリティは導入して終わりではなく、人手を介した監視・運用体制が伴うことで効果が持続する。

ある組織では、以前よりオンプレミスの制御システムに対して、セキュリティに考慮した構成をとっていた。これらのシステムをクラウド環境へ移行するにあたり、インターネットから自組織以外のメンバーがアクセス可能になる点が課題となった。クラウドを遠隔管理する WEB システムの認証においては、外部からの不正アクセスを防ぐため、多要素認証を導入している。また WAF と呼ばれる WEB アプリケーション保護に特化したセキュリティ対策製品を導入し、サイバー攻撃の対策としている。さらに、クラウドに関連したセキュリティ規格（ISO27017 など）を導入し、それに準じた様々な対策を施している。

別の組織では、クラウドの設定変更時は、事前に申請が必要な社内フローとし、変更前のリスク分析を必須とした。また、クラウドに対して行う作業は録画し、クラウドへ接続する際の作業場所も指定するなどの徹底したセキュリティ対策を行っている。

[#17] 技術的な課題２：工場ごとのアクセス権管理

ある組織では、工場から得られたデータを、他の工場から参照できないよう工場ごとに分離して管理する必要があった。そこで、各工場が使用するアカウントに必要最低限のアクセス権限を設定し、人員の異動などに応じて設定作業を都度実施する運用を定義することで、情報の機密性を確保していた。

[#18] 技術的な課題３：変動コストの低減

ある組織では、クラウドの稼働状況をモニタリングし、リソース利用量を調整することでコストの低減を実現していた。クラウドはオンプレミスと異なり、使用した分だけコストが掛かる契約形態となることが多い。そのため、リソース利用量を監視し、動かす必要のない時間はリソースを停止するなどの運用でコスト低減に努めていた。

5.5 導入効果

クラウドを導入した結果、DX を進めやすい組織文化の醸成を実感している組織や、既存業務の効率化を通じて定量的な効果を得られた組織があり、多くの組織がクラウドの更なる活用に意欲的であった。

[#19] 効果１：データを基にした（データドリブンな）意思決定の実行

クラウドを活用することにより、現場の意思決定方法が勘や経験によるものではなく、具体的なデータを用いた判断ができるようになったという効果を挙げる組織が多く見られた。判断に必要なデータが集約されて分析可能となったことに加え、データを扱う能力を身につけたことが、データドリブンな組織文化の醸成に貢献していると考えられる。

[#20]効果２：横展開の効率向上

クラウドで新規にサーバを構築する際、オンプレミスと比べて少ない手間で迅速に立ち上げることができるようになったという効果を挙げる組織が多く見られた。設定済みのマシンに関する設定情報をあらかじめ保管しておけば、クラウド上ですぐに全く同じ設定のサーバを起動することができる。工場ごとにサーバを構築するケースでは、わずかなカスタマイズのみで利用を開始できることもあり、横展開がスピーディに実現されていた。

[#21] 効果３：責任分担の明確化による経営資源の有効活用

クラウド導入によって、運用負担が軽減され、自組織の事業にリソースを集中できるという効果を挙げる組織が多く見られた。使用するクラウドサービスの形態によっては、ネットワークの管理、データベースやストレージの維持管理、マシン OS のパッチ適用などの業務をクラウド事業者が一元管理している。ただし、クラウド事業者の責任範囲は、クラウドサービスの形態や企業間の契約に依存するため、運用負担の軽減効果を十分に得るには両者の責任分界点を明らかにすることが前提条件となる。

[#22] 効果４：生産設備故障の早期予兆検知

生産設備の故障が発生する前に予兆を検知し、予知保全の精度を高めることに成功している組織が多く見られた。元々、定期的な保全活動や担当者の経験を元に異常検知や機器の交換を行なっていたところ、クラウドに集めたデータを使い、設備が故障する予兆を前もって見つけることができるようになった。また、不具合箇所の原因特定もデータに基づいた調査が可能となり、1 週間かかっていた調査が 1 日足らずで原因特定できたという組織もあった。

5.6 残課題

グローバル対応におけるデータ越境に伴う法規制

グローバルを前提とした制御システム環境へのクラウド導入は、自社とクラウド事業者の両方で共通の課題がある。特に産業機器データが国をまたいで移動しなければならない場合、データ越境に関するルールが国によって異なる点は具体的な解決策の提示が難しい。企業体力のある組織では、各海外支店に法務担当者を設置して対応しているケースもあるが、多くの組織では、都度法律や国の文化を調査する対応が求められている。日本の行政ではある程度規定を定める動きが見られるため、その動向を受けて各組織が対応方針を定めることが今後期待される。

制御システム環境における適切なセキュリティ対策の水準

ヒアリングの中でも、どの程度のセキュリティ対策をしていれば十分か悩む組織が複数見られた。しかし、組織ごとに行なっている事業や考え方が異なる点や、デジタル技術の高度化に伴い日々新たなセキュリティリスクが発生することを考えると、具体的な水準を示すことは難しい。事業環境の変化に応じてセキュリティ対策を継続的に見直すことが重要であり、安定生産や高品質な生産活動を支えることができれば、組織を持続的な競争優位へ導く源泉となる。

一方、セキュリティ対策費用がクラウド導入によって得られる利潤を超えてしまっては本末転倒である。また、考えうる全ての対策を完璧にすることは難しい。そこで、例えば、既存のセキュリティ対策をすり抜けることを前提として考え、問題が起きても被害を最小限に抑えるような対策方針とすることは有効な方法である。被害を最小限に抑えるためには、異常があったことを早期に検知し、被害拡大を防ぐ組織的な対応体制をあらかじめ用意し、最低限業務が継続できる復旧地点まで戻せるようなバックアップを確保するなどの事後対策を拡充することが望ましい。

第6章　　セキュアな ICS クラウドアーキテクチャ

第 3 章や第 5 章に記載した通り、製造現場の制御システム（以下、本章では ICS という）にクラウドサービスを活用することは、ICS のデータ利活用を促進するための戦術として極めて有効である。一方で、第 4 章で述べたように、OT 固有のインシデント（4.1 節）、クラウドサービス固有のインシデント（4.2 節）がある。従って、ICS でクラウドサービスを利用する際には、OT・クラウド各々の固有のリスクを検討した上で、ICS とクラウドを接続することにより発生する新たなリスクを検討する必要がある（図 6-1）。しかし、ICS とクラウドを接続した際に発生しうるリスクやそれに対応する対策を示しているドキュメントは多くない[32]。

本指南書では、ICS でクラウドサービスを利用する際のリスクを検討するにあたり、OT・クラウドそれぞれ個別の検討だけではなく、**ICS とクラウドサービスを融合させた総合的な「アーキテクチャ」の検討が必要**と考えた。各種の文献調査、事例調査、および、第 4 章での個別ヒアリングを行い、その検討結果を、ICS のデータ利活用を促進するために必要な機能として一つのアーキテクチャ図にまとめた。加えて、アーキテクチャの作成にあたり実施した、脅威分析、セキュリティ対策の検討結果についても記載する。

なお脅威分析やセキュリティ対策については、ICS 固有領域にも触れるが、なるべくクラウド固有領域や ICS とクラウドの混合領域を中心に検討を行う。なおこの混合領域とは、ICS を起点としクラウドサービスを導入する際に増える要素を示す[33]。

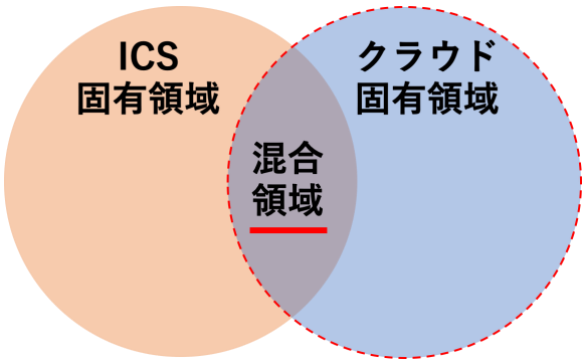


図 6-1 ICS へのクラウドサービス導入時のセキュリティ検討範囲

＜留意点＞

本章で説明するアーキテクチャ、脅威分析、セキュリティ対策の内容は、筆者らがこれまでに調査した事例や知識を元に作成したものであり、**唯一絶対の正解ではない。**これらは検討を行う組織の状況によって異なる検討結果となるのが通常であるため、あくまで一つの参考例であることに留意いただきたい。

上記を踏まえ、本章で記載している**アーキテクチャ（の考え方）、脅威分析の手法、セキュリティ対策例、そしてこれら検討の手順**について、自社に適応する際に参考にできれば幸いである。

---

[32] クラウド事業者固有のアーキテクチャは存在するが、クラウド事業者のサービスに依存しないドキュメントは現時点では極めて少ない。

[33] 例：クラウドサービスにデータを転送するための機器や増設した IoT 関連機器、ICS―クラウド間の通信接続、クラウド領域に用意する ICS 環境のデータ保管、分析・解析機能など。

6.1 アーキテクチャ設計・脅威分析・セキュリティ対策の流れ

ICS へのクラウドサービス導入の脅威分析、セキュリティ対策を講じるためには、まず分析対象が必要である。本指南書ではアーキテクチャを分析対象として設定した。前述した通り、ICS とクラウドサービスを融合させたアーキテクチャは多くなく、汎用性を考え[34]、筆者らが設計する必要があった。またアーキテクチャを設計する上で必要なる要件については第 3 章で調査した事例や、第 5 章に挙げたヒアリングをもとに定義した。

本指南書における、ICS とクラウドサービスを接続した際の、リスク分析やセキュリティ対策を講じるための手順をまとめたものが図 6-2 のようになる。

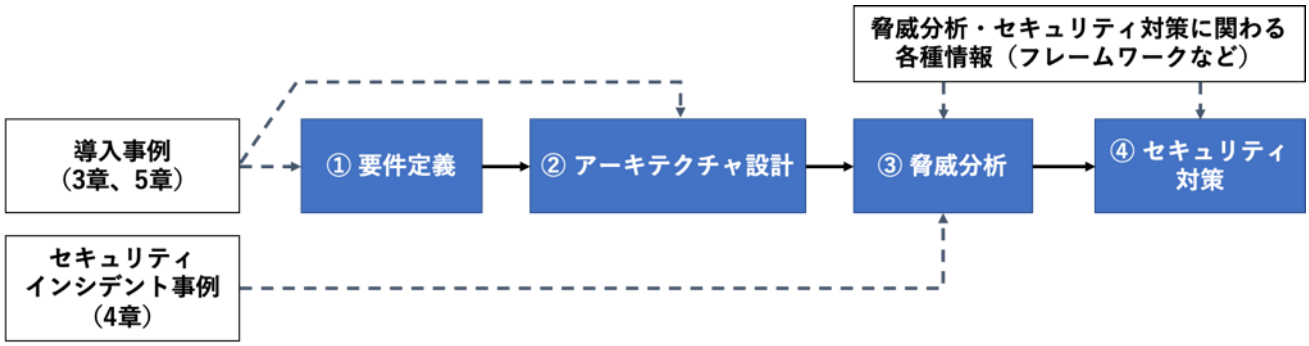


図 6-2 要件定義～セキュリティ対策までの流れ[35]

なお各項目の内容は以下の通りである。

① **要件定義：** 第 3 章や第 5 章で挙げた事例（以下、導入事例という）をもとに、よく利用されている要件を抽出し、データ利活用要件として定義する。 … 詳細は6.2 節に記載

② **アーキテクチャ設計：**①要件定義に基づいて、必要な機能を導出し、整理・分類し、データ連携などの、各機能間の関係の検討を行う。なお、本指南書では汎用性を高めるために製品固有の表現は避け、抽象的な表現としている。 … 詳細は6.3 節に記載

③ **脅威分析：**②で設計された抽象度の高いアーキテクチャに対し、シナリオベースによる脅威分析を行う。なお脅威分析に第 4 章のセキュリティインシデントや脅威分析に関わる各種情報（フレームワークなど）を参考とする。 … 詳細は6.4 節に記載

④ **セキュリティ対策：**③脅威分析で明らかになった脅威に対し、セキュリティ対策を検討し、記載する。 … 詳細は6.5 節に記載

次節より、各項目について説明する。

[34] 製品固有の表現をなくすことで、汎用性を高めることを目指した。

[35] 図の波線は参考関係を示している（矢印の始点が参考元）。

6.2 要件定義

6.1 節の通り、アーキテクチャを検討する上で、導入事例を参考に、クラウドサービス活用事例の要件として「データ可視化」、「予知保全」、「最適設定演算」、「データ連携」[36]を取り込むことにした。本導入事例の調査では FA（Factory Automation）が多く、本要件に関しても FA を想定した[37]。それぞれの要件の内容を以下に示す。なお、要件の（　）に含まれているレベルはスマートファクトリーの段階（図 6-3）を参考にする。

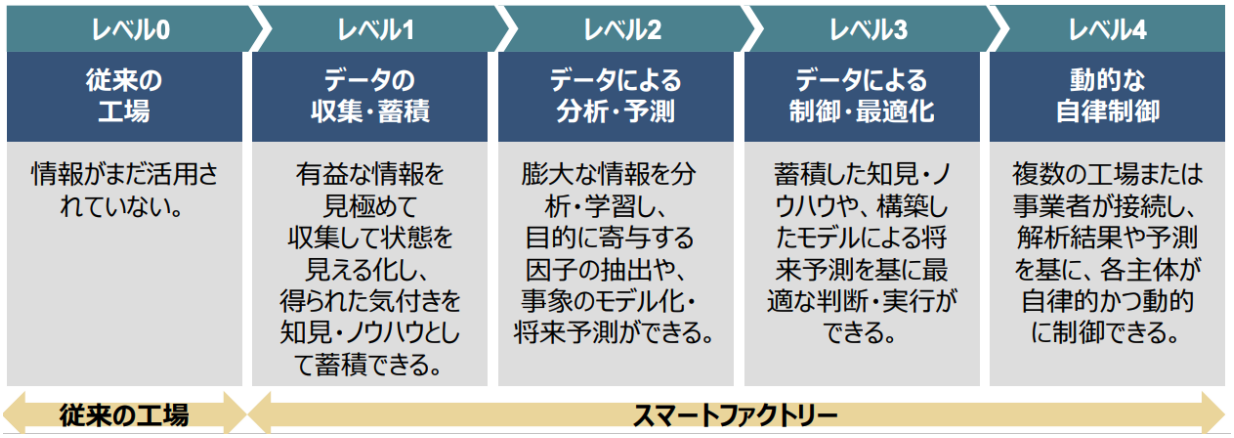


図 6-3 （再掲）スマートファクトリーの段階（出展：三菱総合研究所 令和２年度スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査［7］）

1 データ可視化（レベル 1）

設備からの時系列のデータ（設備稼働状況、温度など）を、時系列（秒単位）毎にリアルタイム（遅延 1 分以内）で確認したい。またデータの傾向が変わっていないかトレンド分析をしたい。

2 予知保全（レベル 2）

機械学習によって設備の状態データから、設備保全のタイミングを適切に判断したい。設備の稼働状況などを WebGUI 経由で表示したい。本機能より CBM[38]が実現でき、メンテナンスの効率化を可能とする。

3 最適設定演算（独自レベル 2.5[39]）

従来、熟練作業員が経験と勘をもとに、設備異常が発生する前に設備の設定値を適宜変更していた。これらに対し設備データ（IoT/PLC）を利用して機械学習を用いた設備の最適な設定値（推奨値）[40]を演算したい。演算された推奨値は ICS のダッシュボードに表示され、その推奨値を人手によって HMI に入力

---

[36] これら要件内容は独自のものであり、実際の事例ではない。
[37] 第 1 章でも述べたとおり、FA（Factory Automation）システム、PA（Process Automation）システムのどちらに対しても適用可能な内容となっている。ここでは具体例として FA を想定しているが、検討の流れや検討方法はもちろん PA にも適用可能である。
[38] CBM：Condition Based Maintenance の略称。設備の稼働状況によって劣化状況を判断する。
[39] 完全な自動制御ではなく、推奨値をダッシュボードに表示することで人を介入させるため 2.5 とした
[40] この最適値とは「このまま稼働を続けたら不良品を作る恐れがある」と判断した際に、正常値に戻すための推奨値のことである。

する。熟練作業員の負担減や、この推奨値をもとに運転を継続することで機器寿命の延長が期待できる。

4　**データ連携（レベル 2）**

クラウドに収集したデータを、様々なアプリケーションに連携させたい。部門間（IT 系ーICS 系部門間含む）や組織を跨いだデータ連携（利用・提供・共有）が想定される。そのため、アプリケーションや部門ごとに個別にデータ連携の仕組みを構築するより、集中的にその仕組みを構築した方が効率良く、ガバナンス面でも有利である。

6.3 ICS クラウドアーキテクチャの設計

6.3.1 アーキテクチャの全体構成と前提

前節の要件を元に作成したアーキテクチャを提示する前に、理解しやすくするためにアーキテクチャの全体構成と前提について記載する。

全体構成

アーキテクチャは、図 **6-4** に示すオンプレミス領域（左）、クラウド領域（右）で構成される。

オンプレミス領域は、制御セキュリティ検討におけるデファクトスタンダードである Purdue モデル[41]に基づいた 4 階層＋DMZ の構成とした。クラウド領域は、IT クラウド基盤と ICS クラウド基盤の 2 つの構成とした。ICS クラウド基盤の可用性の観点から、IT クラウド基盤における設定ミスなどの影響を最小限にできるように、クラウドサービスにおける何らかの方法（アカウントや仮想ネットワークなど）により分離されていることを仮定した。

企業 IT エリアや IT クラウド基盤では、財務、人事、経営管理などの、いわゆる IT 系システムが稼働することを想定した。ただし、それらのシステムは本指南書の主なフォーカスではないため、記述は最小限としている。工場や ICS クラウド基盤では、工場向けのアプリケーション（例：製造プロセスや製品に特化した検査システムなど）が稼働することを想定した。ICS に関する要件が適用されることと、アプリケーションの応答性などの観点で機能を分担して配置することが重要となる。

アーキテクチャをこのような領域に分けて考えることで、各領域に適したフレームワークが利用しやすくなるとともに、必要とされる技術要素や組織内の責任分界を大まかに捉えることができる。

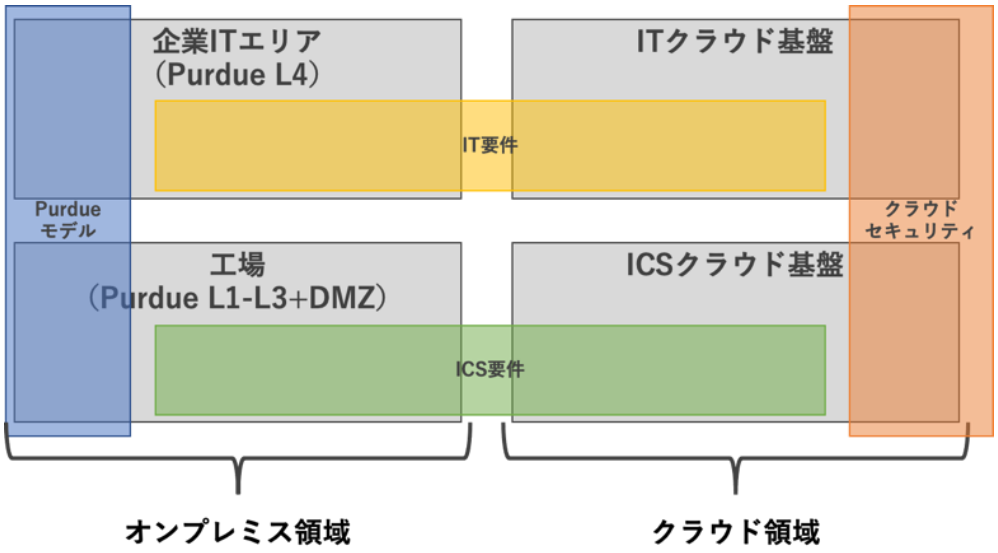


図 6-4 アーキテクチャ構成要素

[41] 正式名称は Purdue Enterprise Reference Architecture。Theodore J.Williams と Industry-Purdue University Consortium for Computer Integrated Manufacturing によって開発された。Level0：物理プロセス、Level1：インテリジェントデバイス（プロセスセンサー、アクチュエータなど）、Level2：制御システム（DCS、PLC、HMI、SCADA など）、Level3：製造業務システム（MES やデータヒストリアン）、Level4：ビジネスシステム（ERP など）、DMZ：ビジネスシステム（Level4）からのデータトラフィックを管理し、Level 3 以下の制御システムのレベルを守る。

前提

提示するアーキテクチャの前提を以下に示す。

1. 本章で提示するアーキテクチャは、第 3 章や第 5 章の事例調査を経て得た知見を元に我々が作成している。従って、提示したアーキテクチャが唯一絶対の正解というわけではない。想定した要件に対する一つの例として参考にしていただきたい。

2. 汎用性を持たせるために、組織やユースケースに固有となってしまうような要素を抽象化して記載している。機能を実現する固有の製品名も排除してある。そのため、このアーキテクチャだけを以て、機能や製品の実装には至らない。

3. アーキテクチャの実際の利用にあたっては、各現場や各組織の実態に沿ってアーキテクチャを適合するように変更した上で、機能、製品などの実装が必要である。「自組織の場合ならば」という目線を持ちつつ説明を読んでいただくことが望ましい。

以上の前提の元、次項以降のアーキテクチャを参照いただきたい。

6.3.2　ICS×クラウドアーキテクチャ

本項では、前節で求めた要件からアーキテクチャを提示する前に、要件によらない抽象度の高いアーキテクチャを図 6-5 に示す。このアーキテクチャは、汎用性が高く、各種要件に柔軟に適用できる。

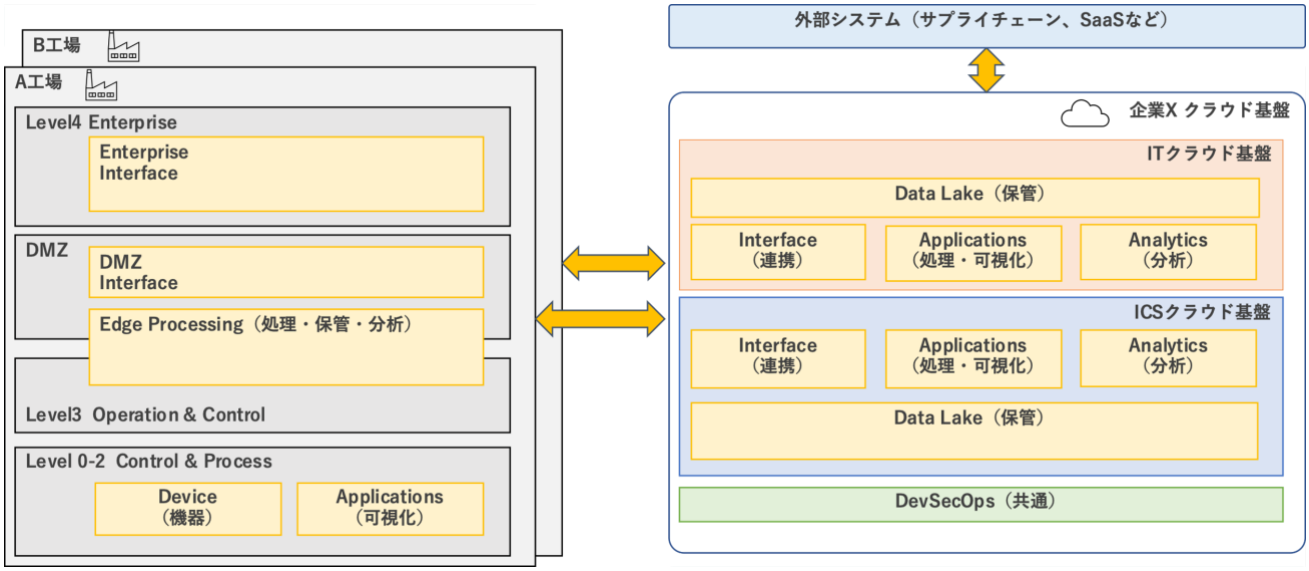


図 6-5 ICS×クラウドアーキテクチャ

【「工場」の機能】

- **Purdue Level 0 – 2（Device）**
  ICS クラウド基盤で保管・分析するための元データとなる機器（例：PLC や IoT 機器など）のことを指す。
- **Purdue Level 0 – 2（Applications）**
  ICS クラウド基盤で処理・分析された内容を現地（製造現場）で可視化するための機器（例：ダッシュボードや HMI など）のことを指す。
- **Purdue Level 3 – DMZ（Edge Processing：データ処理・保管・分析）**
  工場からクラウド基盤へデータの送受信を行う上で必要な機能を保有する機器・システムのことを指す。
  データ処理（データ圧縮・データ変換・転送処理）
  「データ圧縮」では、設備情報のデータ量が多い場合や、データサイズが大きい場合、**通信帯域を圧迫する可能性があり、圧縮処理が必要**となる場合がある。「データ変換」では、クラウド基盤への通信を行う上で、状況に応じて**通信プロトコルの変換**が必要となる可能性がある。「転送処理」では、工場からクラウド基盤への転送を実施する上で、可用性の観点からクラウド基盤が利用できない場合を考え、必要に応じて**再送処理を保有**することが望ましい。
  データ保管
  データ保管では前述した Device にある機器の生データ及びデータ変換されたデータを保管する。保管容量や保管期間に関しては、将来のシステムの拡大や、Device にある機器の数・種類や、クラウド基盤が障害などで停止した際に業務上必要なデータを利用することができる期間などを加味して決定する。

データ分析

ICS クラウド基盤で構築した分析機能（例：機械学習モデルなど）を工場側に実装する。機械学習の推論[42]を工場側で行えるようにすることで、**レイテンシを求められる要件**[43]、**可用性を求められる要件**[44]などに適している。なお機械学習は使用している間に予測性能が時間経過とともに劣化していく事象（ドリフト）が発生する可能性がある。機械学習モデルを更新する必要があるが、学習自体は ICS クラウド基盤で実施し、学習した機械学習モデルを ICS クラウド基盤から ICS 側へデプロイし、モデルを更新することができる。

- **Purdue DMZ（DMZ Interface）**
  ICS クラウド基盤と接続するためのインターフェースを設ける。機器の認証や通信の暗号・復号処理を実施する。
- **Purdue Level4（Enterprise Interface）**
  全社 IT クラウド基盤と接続するためのインターフェースを設ける。機器の認証や通信の暗号・復号処理を実施する。

【「ICS クラウド基盤」の機能】

- **Interface（連携）**
  工場側や IT クラウド基盤や外部（サプライチェーン企業、SaaS など）と接続するためのインターフェースを設ける。機器の認証や通信の暗号・復号処理を実施する。
- **Data Lake[45]（保管）**
  工場側の Device の機器で取得した生データや、その生データを処理したデータ、ICS クラウド基盤で分析した結果のデータなどを保管する。
- **Applications（処理・可視化）**
  ICS クラウド基盤の分析で使用するために、データを処理（データ変換、画像文字認識など）したり、データの可視化（ダッシュボードなど）したりする。
- **Analytics（分析）**
  工場でのデータを分析するための機能（例：機械学習による予知保全、最適運転など）を要する。なお Data Lake で保管されているデータを用いて、機械学習モデルを学習することができる。

---

[42] 機械学習モデルが、パターンやルールを新たなデータに当てはめることで、新たなデータに関する分析や予測などを可能とするプロセスのことを示す。

[43] 例えば画像処理による不良品判断などが考えられる。クラウド基盤側で機械学習モデルの推論を実施する場合、工場⇆クラウド基盤の通信遅延が発生し、処理要求時間を満足しない（レイテンシが大きくなる）可能性がある。

[44] クラウド基盤がサービス停止したとしても機械学習モデルが工場側に存在するため、モデルの入出力が工場側で完結する場合、処理を継続することができる。

[45] Data Lake（データレイク）：すべての構造化データと非構造化データを保存できる一元的に格納することができる基盤のこと。

【「IT クラウド基盤」の機能】

- **Interface（連携）**
  工場の Enterprise や ICS クラウド基盤や外部（サプライチェーン企業、SaaS など）と接続するためのインターフェースを設ける。機器の認証や通信の暗号・復号処理を実施する。
- **Data Lake（保管）**
  Applications や Analytics で生成されたデータを保管する。Interface を経由することで工場の Enterprise からもデータにアクセスすることができる。
- **Applications（処理・可視化）**
  管理系アプリケーション（生産管理、ERP など）がある。生産状況や ERP データを処理したり、データを可視化したりする。
- **Analytics（分析）**
  分析機能（経営管理や受発注など）がある。Applications で処理されたデータを元に最適な受発注数などを分析し、効率的な生産を促す。

【共通】

- **DevSecOps**
  クラウド基盤（ICS クラウド基盤、IT クラウド基盤）共通の項目。クラウド基盤内のアプリケーションを開発・検証するための機能、ID、権限管理などのセキュリティ機能、ログ取得・分析、コスト管理などの運用機能を要する。

【外部システム】

- **サプライチェーン企業、SaaS など**
  サプライチェーン企業や、他社 SaaS との情報連携を行う。

以上までが ICS クラウドアーキテクチャについての説明である。

6.3.3　　要件に基づくアーキテクチャと各機能

6.2 節に挙げた要件を ICS クラウドアーキテクチャ（図 6-5）に反映したアーキテクチャを図 6-6 に示す。ここに記述されている各要素の説明を、次ページ以降の表 6-1 および表 6-2 に示す。大きく「工場群[46]」、「クラウド基盤」、「外部システム」の 3 つで構成されており、「工場群」⇆「クラウド基盤」、「クラウド基盤」⇆「外部システム」間で連携される。なおアーキテクチャ内の各要素のデータ連携は複雑になるためここには示さない。

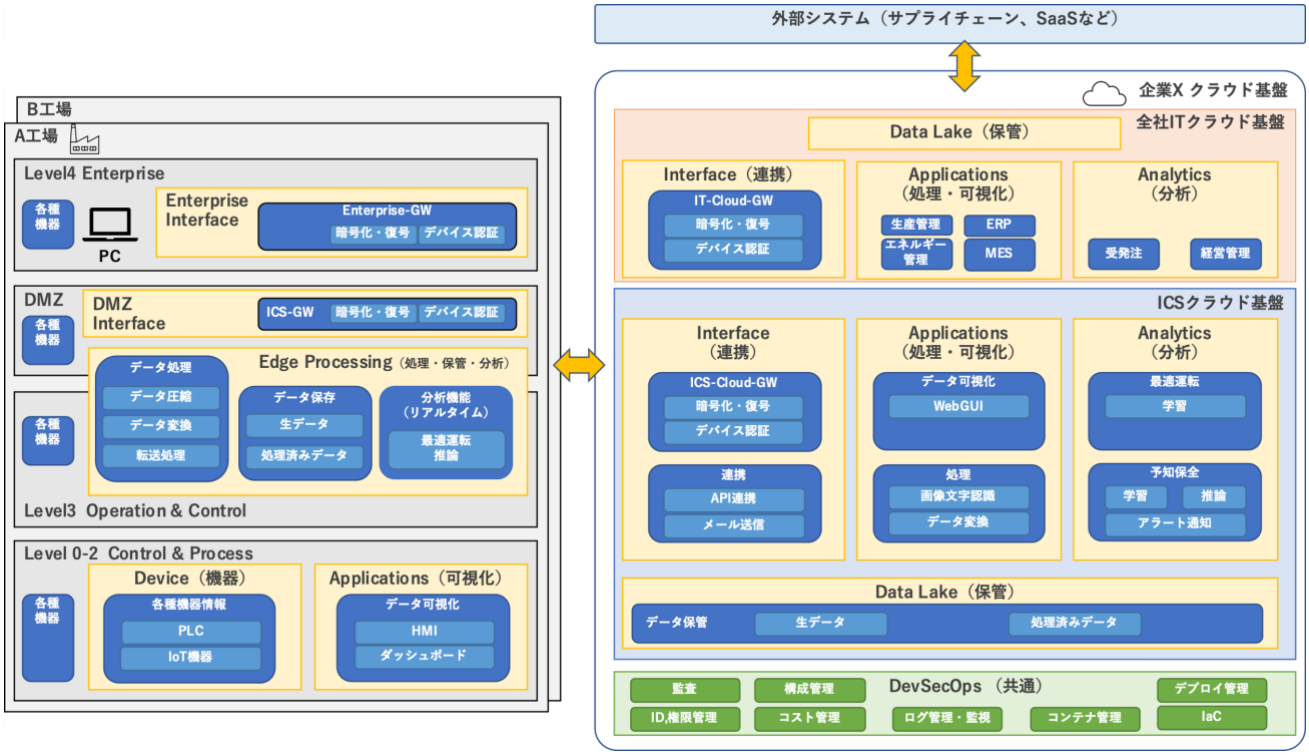


図 6-6 要件を反映したアーキテクチャ

[46] ここでは複数の工場をクラウド基盤に接続することを想定して「工場群」としている。各工場は前項で示したアーキテクチャを持つ。

【利用シーン：予知保全】

一例として予知保全の利用シーンに関係する要素をピックアップした図を図 6-7 に示す。大きく「ICS クラウド基盤の Analytics の予知保全機能にデータを入力するフェーズ」、「分析したデータを利用するフェーズ」、「モデルを更新する学習フェーズ」の 3 つがある。

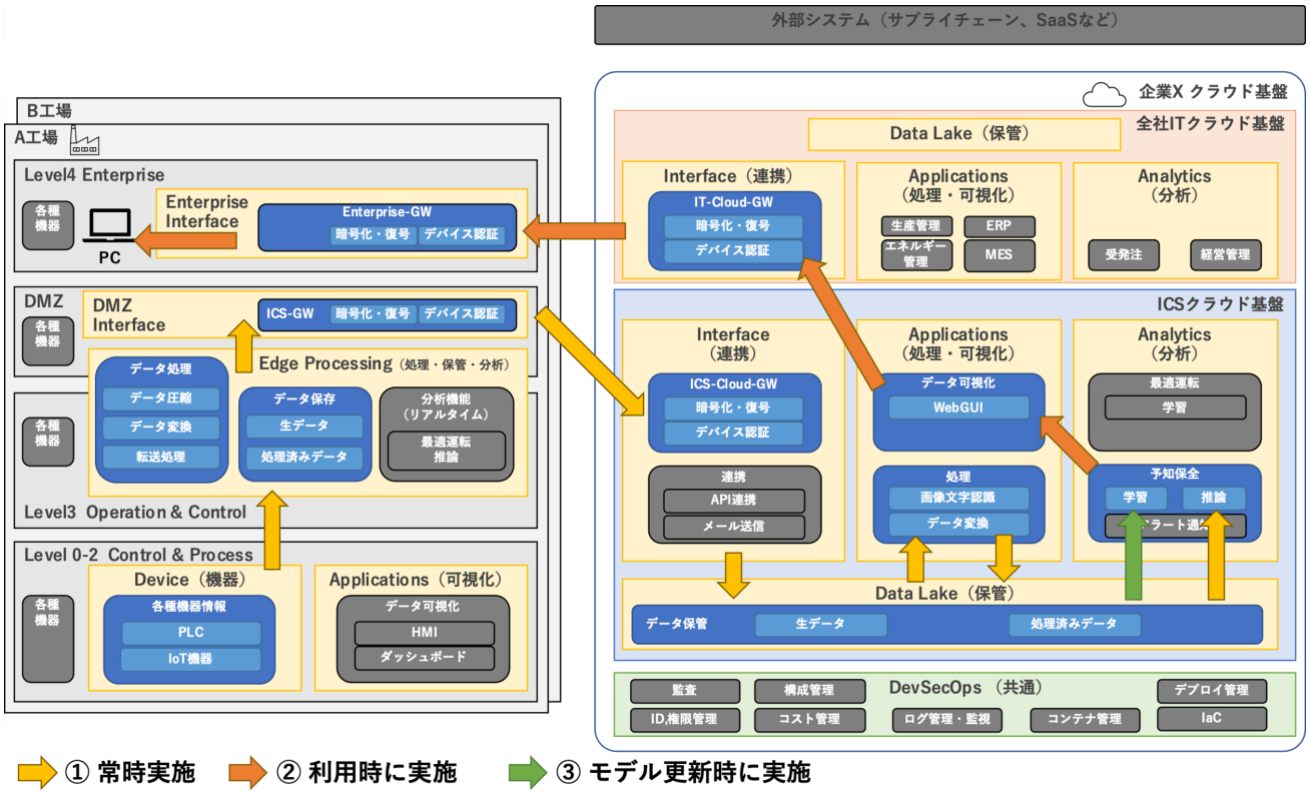


図 6-7 予知保全機能利用シーン

＜① 予知保全機能にデータを入力するフェーズ＞

PLC や IoT 機器から取得するデータ（時系列・画像データ）を Edge Processing にて必要に応じてデータ変換・圧縮を実施し、工場側に一時的にデータ保管する。また、状況に応じてデータの圧縮やプロトコル変換を実施し、ICS-GW、ICS クラウド基盤の Interface を通じて Data Lake に生データを保管する。もしデータが IoT カメラなどで取得した画像データであれば ICS クラウド基盤の画像文字処理を通じて画像で取得した値を数値化し、Data Lake の処理済みデータに保管する。生データ及び処理済みデータを予知保全機能に入力し、分析を可能とする。

＜② 予知保全の分析結果を利用＞

予知保全モデルで分析（推論）した結果を Level4 Enterprise にある業務用 PC から、Enterprise-GW、IT-Cloud-GW を通じて ICS クラウド基盤の WebGUI にて分析結果を確認し、保全作業に活かす。

＜③ 予知保全モデルの更新＞

Data Lake に保管されているデータを用い、学習モデルの更新（再学習）を行う。**この際、現場に出向かなくて済む（クラウドで作業が完結する）面もクラウドを利用する一つのメリットである。**

表 6-1 工場アーキテクチャの機能

レベル分類	機能大分類	機能中分類	機能小分類	内容
Level 4/5	Enterprise Interface	Enterprise-GW	暗号化・復号	通信を暗号化、復号する。
			デバイス認証	デバイスが正規のデバイスであるかを認証する。
		—	PC	社員が使用する各種 PC。
DMZ	DMZ Interface	ICS-GW	暗号化・復号	通信を暗号化、復号する。
			デバイス認証	デバイスが正規デバイスであるかを認証する。
Level3	Edge Processing	データ処理	データ変換	生データを整形しデータ保存の加工済みデータに保存する。
			転送処理	データ保管にあるデータを ICS-GW へ転送する。なお可用性を加味して、クラウド通信障害などが発生した場合などを考慮し、再送機能を保有する。
			データ圧縮	大容量のデータを可逆/非可逆圧縮し、通信負荷を低減する。
		データ保管	生データ	Devices から受信したデータを保管する。なお保管期間は転送処理に耐えうる必要期間とする。
			加工済みデータ	生データから加工されたデータを保管する。なお保管期間は転送処理に耐えうる必要期間とする。
		分析機能（リアルタイム）	最適運転推論	収集した PLC、 IoT センサーデータや IoT カメラの画像データから、生産品質の異常とならないような制御設定値を表示する。モデルはクラウドから展開される。
Level 0-2	Devices（機器）	各種機器	PLC	工場内機器を制御する機器。
			IoT 機器	温度・湿度や画像を取得する機器。
	Applications（可視化）	データ可視化	HMI	端末で機器パラメータ設定や機器状態を表示することができる。最適運転推論の結果は人を介在し、HMI にパラメータを設定する。
			ダッシュボード	最適運転推論の運転推奨値の結果ダッシュボードを表示する。

表 6-2 クラウドアーキテクチャの機能

基盤分類	機能大分類	機能中分類	機能小分類	内容
全社 IT クラウド基盤	Interface（連携）	IT-Cloud-GW	暗号化・復号	通信を暗号化、復号する。
			デバイス認証	デバイスが正規のデバイスであるかを認証する。
	Applications（処理・可視化）	—	ERP	企業資源計画。経営のヒト・モノ・カネ・情報を一元的に管理する機能（アプリ）である。具体的には勤怠、営業、在庫、調達、経理・財務など。 経理・財務を例に取ると、従来はデータの手動入力や csv ファイルによるデータ連携が主なデータ登録方法だったが、クラウド上で様々なシステムと連携させることでデータ登録の自動化が進み、決算対応時間の短縮や、管理会計のメッシュの詳細化（週次→日時、工場単位→ライン単位、など）が実現されている。
		—	MES	製造実行システム。製造工程の状況把握、作業のスケジューリング、生産資源の配分、品質管理、作業者への指示などを行う機能（アプリ）である。生産管理システムと連携し、管理システムの生産計画を元に、各製造工程における作業指示を表示する。
		—	エネルギー管理	ICS 環境のセンサーから取得した消費電力量などを、省エネ法や IR、経営管理の観点で算出が必要なエネルギー消費量に換算・集約し、可視化、レポート作成を行うための機能（アプリ）である。予知保全に基づいて停止される設備の停止時間は、クラウドを通してアプリによるエネルギー消費量換算の際に反映される。 基本的には工場ごとに算出されるものだが、本社機構（総務部など）による全社分析のニーズや、応答速度が不要であること、市販 SaaS との連携を考え全社 IT クラウド基盤に設置する。
		—	生産管理	生産管理システム。需要計画、生産計画、調達計画、在庫管理、工程管理、原価管理といった情報を一元的に管理する機能（アプリ）である。部門横断のリアルタイムな情報閲覧や、原価計算などの負担軽減に役立つ。受発注システムの情報を元に、生産計画を立て、MES に連携する。

基盤分類	機能大分類	機能中分類	機能小分類	内容
	Analytics（分析）	―	経営管理	設備の稼働時間やエネルギー消費量などから人/設備/工場単位での運営効率（生産量、加工時間、不良品率など）を分析し、予実管理、計画策定のための計数を算出する機能（アプリ）である。クラウドの処理能力と IoT 機器による秒オーダーでの情報収集が可能なったことから、AI による高精度な予測値の算出が可能となっている。
		―	受発注	設備の稼働効率などを元に（BOM などとも連携し）発注が必要な部品の種類と数を自動算出する機能（アプリ）である。AI による発注タイミングの算出も行う。 将来的には、営業管理システムと生産管理システムと連携し、受注情報の受領と同時に最適な設備の稼働を AI で提案する。 また、会計システムとも連携し、管理会計、財務会計両面のオペレーションを効率化する。
ICS クラウド基盤	Interface（収集・連携）	ICS-Cloud-GW	暗号化・復号	通信を暗号化、復号する。
			デバイス認証	デバイスが正規のデバイスであるかを認証する。
		連携	API 連携	IT と OT で、Data Lake のデータを API で呼び出す。
			メール送信	生産異常検知、設備異常検知、設備異常予測で閾値越えを認識した際に、アラートメールを送る。
	Applications（処理・可視化）	処理	画像文字認識	メーター画像に書かれた値を読み取る。
			データ変換	読み取った画像文字データをデジタルデータとして保存する。
		データ可視化	WebGUI	ブラウザでダッシュボードを表示する。
	Analytics（分析）	予知保全	学習	予知保全モデルの更新を行う。
			推論	収集した OT、IoT センサーデータや IoT カメラの画像データから、設備の異常を予測する。
			アラート通知	検知した生産異常内容を、外部に通知する。

基盤分類	機能大分類	機能中分類	機能小分類	内容
		最適運転	学習	最適運転モデルの更新を行う。
	Data Lake（保管）	データ保管	生データ	Devices から受信したデータを保管する。
			加工済みデータ	生データから加工されたデータを保管する。
クラウド共通	DevSecOps	開発	—	クラウド内アプリケーションを開発・検証するための機能。
		セキュリティ	—	アカウント管理、アクセス制御、冗長化、検知機能などのセキュリティ機能。
		運用	—	ログ取得・分析、構成管理、障害管理などの運用。
		監査	—	クラウド基盤の設定（例：ストレージへの無制限アクセス）、ガバナンス（例：MFA 適用状況）、コンプライアンスなどが正しくなされているかを確認する。
		ID,権限管理	—	ID とアクセス権限を管理する。
		構成管理	—	リソース情報（ホスト名、OS ver、ソフトウェアのインストール状況など）を管理し、セキュアでないリソースの特定・対応を行う。
		コスト管理	—	クラウドの使用料やその傾向を管理する。
		ログ管理・監視	—	SIEM 含めたログ管理、監視を行う。
		コンテナ管理	—	コンテナを管理する。他環境や Edge レイヤーへのアプリ展開・流用・破棄が容易になり、アプリ開発・活用の生産性が向上する。
		デプロイ管理	—	デプロイの自動化、Blue / Green デプロイメントによるダウンタイム排除、一元管理により管理効率が向上する。
		IaC	—	Infrastructure as Code。クラウドインフラのデプロイを自動化することで操作ミスの防止や、クラウド環境のコピーなどが容易になる（BCP、スケーリングなど）。

6.4 脅威分析の実施

前項で提示した要件を反映したアーキテクチャ（図 6-6）でセキュリティ対策を講じるために、脅威分析を実施する。なお、脅威分析には、大きく「資産ベースによる脅威分析」と「シナリオベースの脅威分析」がある。

「資産ベースによる脅威分析」では、資産一つ一つに対して脅威を分析する。対策の抜け漏れを少なくすることができる一方で、分析された脅威が資産ごとに重複し、対策の優先順位づけが難しいといった側面がある。「シナリオベースによる脅威分析」では、具体的なリスクシナリオ（起きて欲しくない事象）を想定して、脅威を分析することで、各シナリオに対する優先順位を決めやすい。一方で、起きて欲しくない事象や事象の原因を正確に検討するには対象業務知識が不可欠であったり、１つのシナリオだけではセキュリティ対策の抜け漏れを少なくすることは難しかったりする側面がある。

クラウド導入企業の残課題（5.6 節）にも挙げたように、セキュリティ対策をどこまで実施したら分からないといった課題がある。セキュリティ対策予算も限られているため、優先順位をつけて対策をしたいのはどの企業でも言えることである。以上のことから、本指南書ではセキュリティ対策の優先順位をつけやすいよう、「シナリオベースによる脅威分析」を実施することにした。

ICS でのクラウド利用では、クラウド側のいわゆる IT の知識はもちろん、ICS 側の OT への影響を考えられる OT 知識の両方が必要である。本指南書では、シナリオベースによる脅威分析を行った。バックグラウンドや視点の異なる複数のメンバー[47]にてシナリオベースによる脅威分析を行ったため、ある程度網羅性をしつつ適度な粒度のシナリオ想定と脅威分析を行えたと考えている。

[47]多様な業界（放送・鉄鋼・石油・重工業・建設・電気機器・自動車・情報通信）からなるメンバーで構成されており、OT 技術者・IT 技術者それぞれの経験者が揃っている。

6.4.1　　シナリオベースによる脅威分析アプローチ

シナリオベースによる脅威分析のアプローチを実施する上で、CCE（Consequence-driven Cyber-informed Engineering）を参考とした［23］。CCE は、米国アイダホ国立研究所により提唱された分析フレームワークである。このフレームワークは以下の 4 つのステップで構成されている（図 6-8）。

① **ステップ 1 ：対策事象の優先順位付け**
事業継続において起きて欲しくない事象（シナリオ）を列挙し、SQDC[48]+CIA[49]の観点で検討して、起きて欲しくない事象の優先度をつける。

② **ステップ 2 ：事象の原因分析**
原因分析手法（FTA[50]）を用い、起きて欲しくない事象が発生する原因を洗い出す。なお本指南書では ICS へのクラウドサービスを導入したことにより増えた要素にフォーカスを当てて分析を実施する。

③ **ステップ 3 ：原因に関わるサイバー攻撃を分析**
FTA で洗い出された原因を、攻撃者の立場で引き起こすことができる攻撃手法、攻撃経路を検討する。本指南書ではサイバー攻撃経路の分析フレームワーク（後述するサイバーキルチェーン）を用い、攻撃経路を検討する。

④ **ステップ 4 ：セキュリティ対策検討**
検討した攻撃経路一つ一つに対し、セキュリティ対策を検討する。

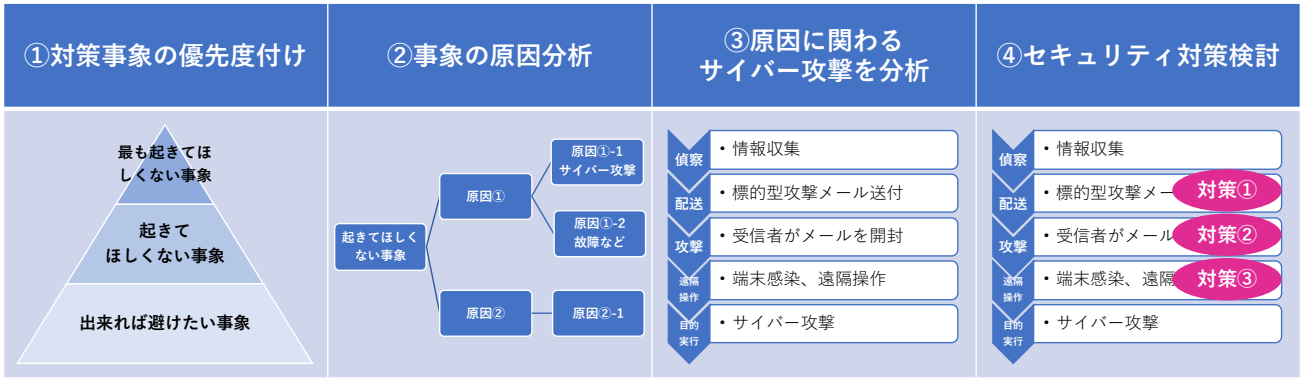


図 6-8 CCE のアプローチ

---

[48] 工場が達成すべき指標である Safety, Quality, Delivery, Cost の頭文字をとった略称。
[49] 情報セキュリティの 3 要素である Confidentiality, Integrity, Availability の頭文字を取った略称。
[50] FTA は、Fault Tree Analysis（故障の木解析）の略称であり、米国 Bell 研究所および Boeing 社により完成された、製造業における製品の故障や事故の発生要因を分析する手法である。製品の故障など原因を分析したい事象を頂点として、考えられる要因を木構造で深掘りしていく。結果と要因を論理回路の AND もしくは OR で繋ぐことで、要因同士の関係を明らかにする。

6.4.2 対策事象の優先度付け【CCE ステップ 1】

ICS をクラウドに接続したことによって発生する「起きて欲しくない事象」として「人命に関わる事故」、「特定の生産業務停止」、「機密情報の漏洩」、「品質の異常」の 4 つを提示する（表 6-3）。

前述の通り、これら 4 つの起きて欲しくない事象を、工場が達成するべき目標である SQDC と、守るべき情報の 3 要素である CIA の計 7 つの観点で評価した[51]。

本章では調査、ヒアリングの結果、ヒアリング先の多くの企業で起きて欲しくない事象として懸念とされていた「特定の生産業務停止」、「機密情報の漏洩」の 2 つを選定し、脅威分析を行った[52]。以後、これら 2 つを引き起こすシナリオをシナリオ 1、シナリオ 2 と呼ぶことにする。

なお、今回「人命に関わる事故」や「品質異常」については各社の固有の状況が大きく影響するため取り上げなかった。本来的には、自社の設備や業務内容に応じた適切な検討の下に当然検討すべきシナリオである。業務内容や発生した時のインパクトをもとに自社の中での優先順位を決め、取り組んでいただきたい。

表 6-3 起きて欲しくない事象一覧

#	シナリオ	内容（例）	影響 1（SQDC）	影響 2（CIA）
1	人命に関わる事故	サイバー攻撃によって、機器が誤作動を起こしたり、機器が制御不能になったりすることで、人命が危険に晒されている状態	S	A
2	特定の生産業務停止	ランサムウェア、データの改ざん、DDoS、クラウド障害などによって工場の一部生産業務が継続できない状態	QDC	I, A
3	機密情報の漏洩	クラウドに保存されている工場の機密データが漏洩した状態	—	C
4	品質異常	品質に関わるシステムの機能やデータが改ざんされ、品質に影響を及ぼす状態	SQC	I

[51] 工場内では SQDC が重要視されるが、本指南書では守るべき情報の CIA を取り上げている。Integrity（完全性）や Availability（可用性）は工場にも馴染みがあるが、Confidentiality（機密性）もここでは言及している。自社の機密情報漏洩による競争力低下や、他社との取引情報漏洩による社会的信頼低下など、起きて欲しくない事象として加える必要があると考えた。

[52] 選定理由はあくまで我々が調査した範囲の話であり、全てのアーキテクチャが人命につながる事故が発生しないわけではないことを了承いただきたい。もちろん PA（Process Automation）などは爆発、激毒物の漏洩、死傷者の発生などが挙げられる。なおどのシナリオを取っても、ステップ 1～4 に沿って同様に実施することができる。自社のビジネス要件に従って、シナリオを検討していただきたい。

6.4.3　事象の原因分析【CCE ステップ２】

【シナリオ１】特定の生産業務停止

シナリオ１「特定の生産業務停止」に対し、FTA を実施した結果を図 6-9 に示す。

特定の生産業務停止につながる原因として「工場設備の故障」と「生産管理システム機能停止」の２つを深堀した[53]。「工場設備の故障」では最適運転モデルの学習に用いる ICS クラウド基盤の「データレイクの改ざん」を、「生産管理システム機能停止」では「MES 機能停止」を、それぞれの事象を引き起こす原因事象として定めた。

シナリオ１の原因となる事象はこれ以外にも存在するが、上記の通り、ICS にクラウドを導入した際に追加となる事象の一部を取り上げている。実際に FTA を実施する際には起こり得る原因事象について、幅広くかつ深く、検討することが望ましい。

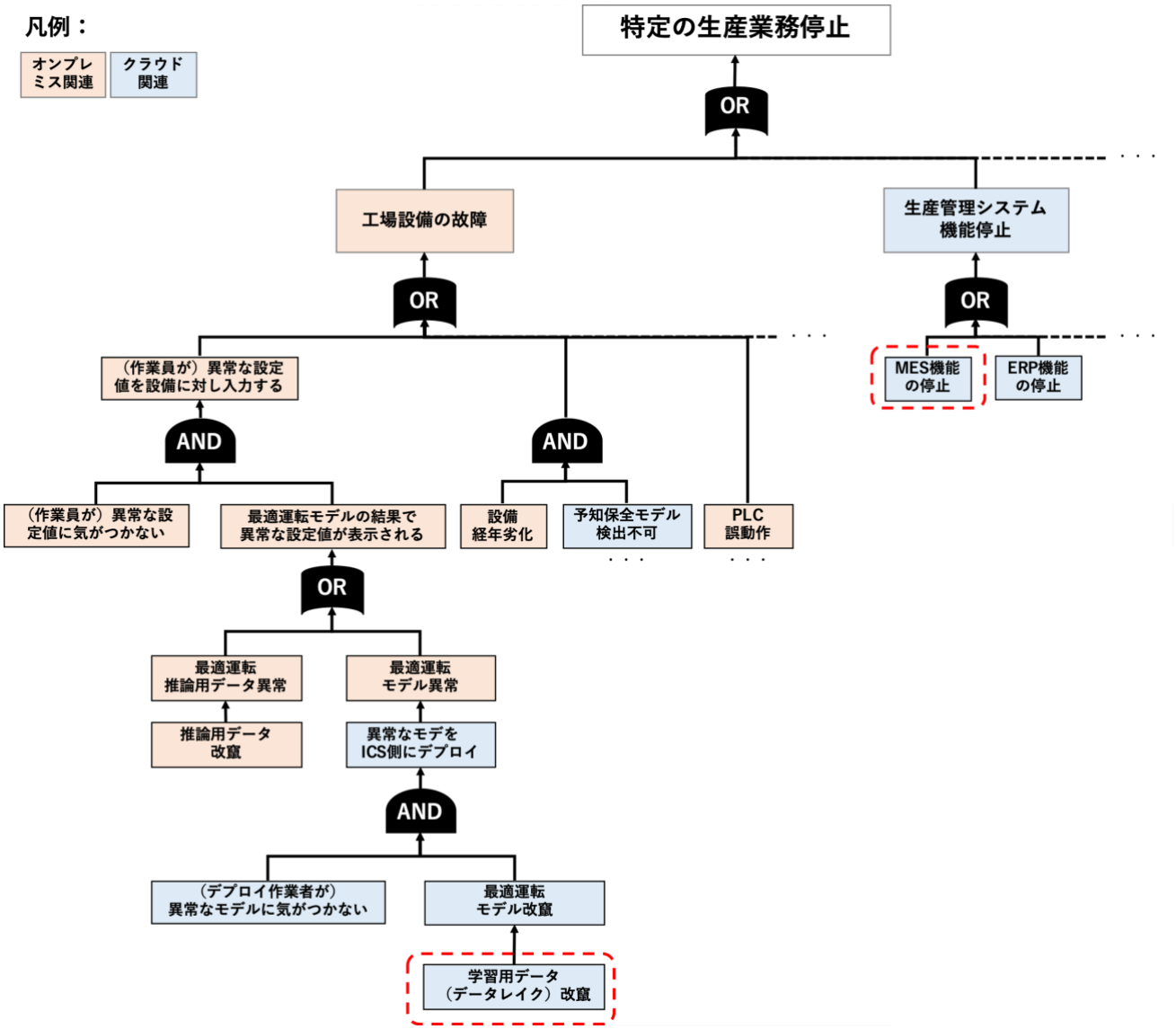


図 6-9 シナリオ１（特定の生産業務停止）の FTA

[53] その他にも、4M（Man・Machine・Material・Method）の観点では「従業員の不足」や「材料の不足」などが挙げられるが、ここではサイバー攻撃に関係がありそうな２つ（Machine・Method）を選定した。

【シナリオ２】機密情報の漏洩

シナリオ 2「機密情報の漏洩」に対し、FTA を実施した結果を図 6-10 に示す。

「機密情報の漏洩」をツリーの頂点として、機器要因と人為的要因の 2 つを深堀した。機器要因は「システムからの情報漏洩」、人為的要因は「従業員による情報持ち出し（内部犯）」と「その他人的ミス（誤操作）」として分析した。このうち ICS にクラウドサービスを導入する際に新たに生じる脅威は「システムからの情報漏洩」である。シナリオ 1 と同様に、「システムからの情報漏洩」を深く分析した。

分析の結果、「IoT 機器からの情報漏洩」、「エッジ機器[54]からの情報漏洩」、「データレイクからの情報漏洩」、「クラウド基盤の端末からの情報漏洩」、「通信経路からの情報漏洩」の 5 つを「機密情報の漏洩」の原因事象として定めた。

シナリオ 1 と同様に、この結果が全てではない。実際に FTA を実施する際には起こり得る原因事象について、幅広くかつ深く、検討することが望ましい。

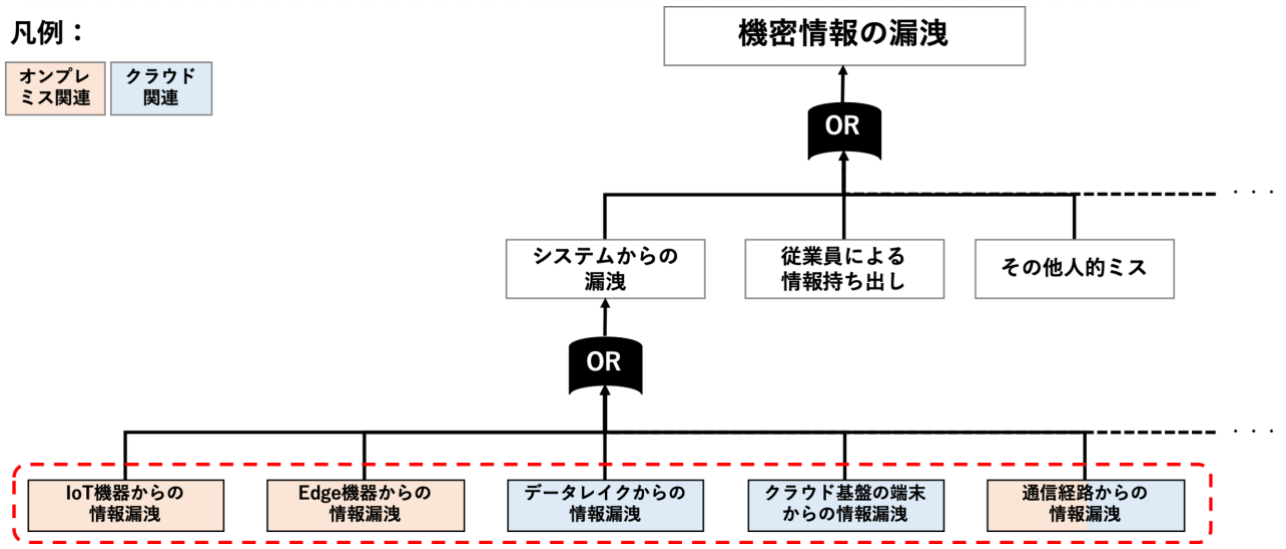


図 6-10 シナリオ 2（機密情報の漏洩）の FTA

[54] 工場の Edge Processing にある機器のことを示す。

6.4.4　　原因に関わるサイバー攻撃を分析【CCE ステップ３】

本項では、前項で FTA 分析を実施した結果を、サイバー攻撃によって引き起こす方法について、フレームワーク（サイバーキルチェーン）を用いて検討する。サイバーキルチェーンは、米国 Lockheed Martin 社により提唱された、サイバー攻撃に関する手法を体系化したフレームワークである [24]。サイバーキルチェーンでは、近年の高度化するサイバー攻撃を、「偵察」、「武器化」、「配送」、「攻撃」、「インストール」、「遠隔操作」、「目的の実行」の複数の攻撃フェーズに分類している（図 6-11）。それぞれのステップで適切なセキュリティ対策を講じることにより攻撃から守ることを目的としているが、サイバーキルチェーンで重要な点は、「サイバー攻撃からシステムを守るためには、どこかのステップでチェーンを切ることで攻撃を防げば良い」といった考え方である。なお本指南書ではサイバーキルチェーンの一部のプロセスは簡略化している。具体的には、「偵察」と「武器化」並びに「攻撃」と「インストール」はそれぞれをまとめて検討している。前者に関しては直接的な被害まだ発生していない外部の活動と捉えてまとめている。また後者は「目的実行」の直接的な活動である「遠隔操作」に至る前までの「攻撃活動フェーズ」と捉えてまとめている。

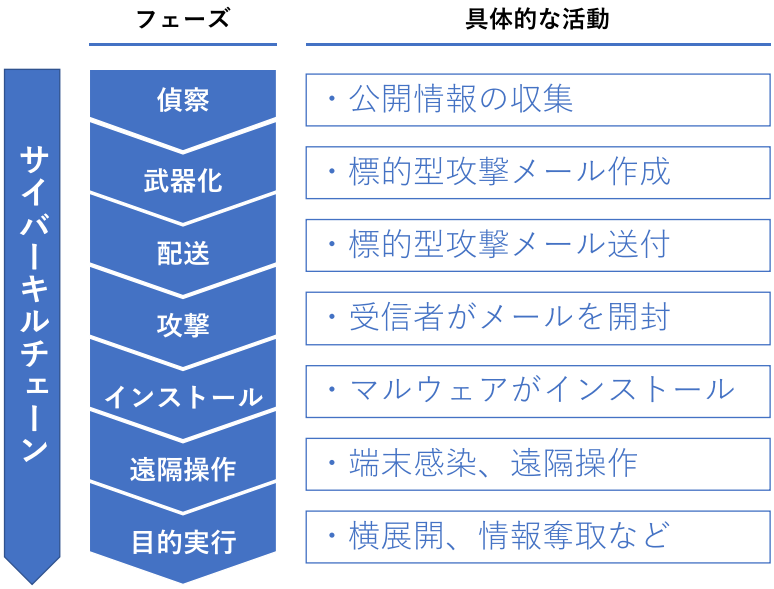


図 6-11 サイバーキルチェーンの概要

【シナリオ１】特定の生産業務停止

まずシナリオ１（特定の生産業務停止）を引き起こす原因の「データレイクの改ざん」と「MES の機能停止」をサイバー攻撃で発生させることができるかを検討した。具体的には、サイバーキルチェーンを用いて攻撃者の視点で脅威分析をそれぞれ実施した（図 6-12、図 6-13）。

なお図の見方として、攻撃として実現させたい事象（データレイクの改ざんや MES の機能停止）を頂点にそれを実現するための攻撃活動をサイバーキルチェーンの攻撃フェーズごとに記載している。それぞれの、詳細は次ページの表 6-4 に示す。なお、図 6-13 に関しては、図 6-12 で使用していない攻撃活動をグレーアウトし、差分を赤字としている。

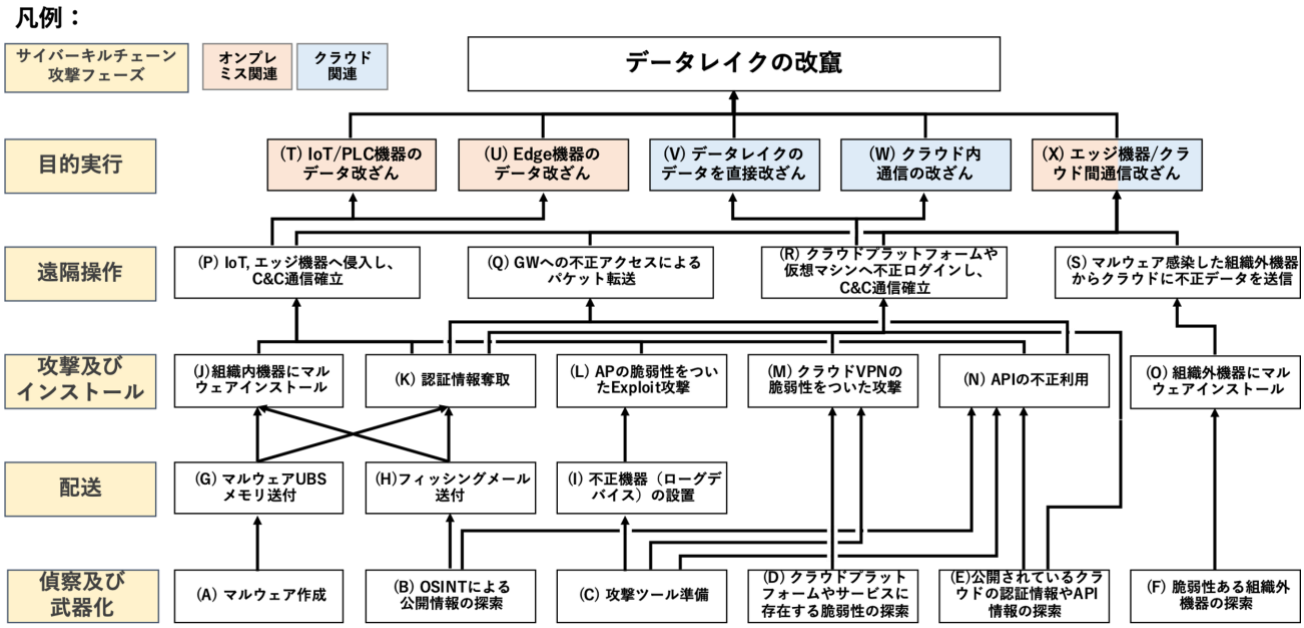


図 6-12 シナリオ１（特定の生産業務停止）：「データレイクの改ざん」のサイバーキルチェーン

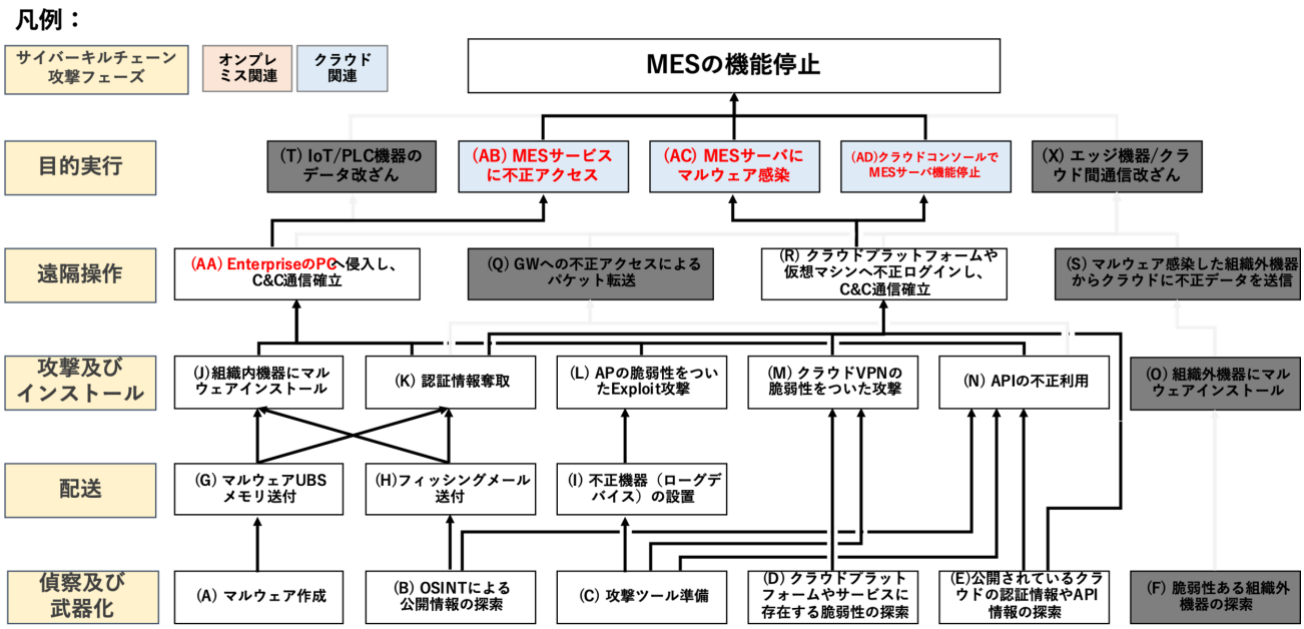


図 6-13 シナリオ１（特定の生産業務停止）：「MES の機能停止」のサイバーキルチェーン

【シナリオ２】機密情報の漏洩

続いて、シナリオ１と同様にシナリオ２（機密情報の漏洩）を引き起こす原因の「システムからの情報漏洩」に対しサイバーキルチェーンを用いて攻撃者の視点で脅威分析をそれぞれ実施した（図 6-14）。なお、図 6-14 に関しても、図 6-13 と同様に図 6-12 で使用していない攻撃活動をグレーアウトし、差分を赤字としている。

各サイバーキルチェーンを用いた脅威分析の結果（図 6-12、図 6-13、図 6-14）を見てわかるように、4.2 節のクラウドインシデントで示した「設定ミス」は非常に危険であることがわかる。例えば設定ミスによって認証情報を公開してしまった場合、「偵察及び武器化」である「(E) 公開されているクラウドの認証情報や API 情報の探索」から「配送」と「攻撃及びインストール」をスキップし「遠隔操作」を実施されてしまい、目的実行まで行いやすくなることが分かる。

また、各サイバーキルチェーンを見て分かるように、想定される攻撃経路はシナリオ 1 とシナリオ２で多くは重複する。シナリオ１は「特定の生産業務停止」、シナリオ２は「機密情報の漏洩」だが、目的が異なるだけで攻撃対象の機器やシステムが同じであれば、攻撃者が目標の機器やシステムに至る経路もある程度パターン化されるためである。

もちろん、ここで挙げている攻撃経路は全てではなく、実際に各企業で実施する場合はさまざまな観点で検討することが望ましい。

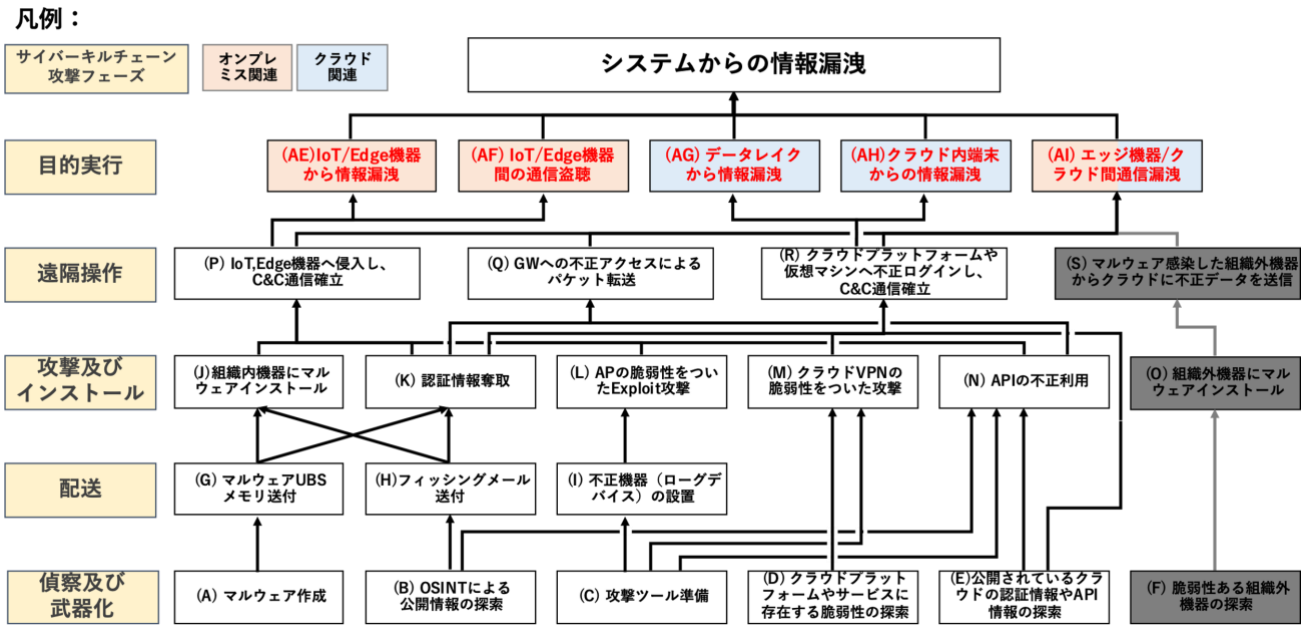


図 6-14 シナリオ２（機密情報の漏洩）：「システムからの情報漏洩」のサイバーキルチェーン

表 6-4 攻撃フェーズと攻撃活動の内容

#	攻撃活動名	攻撃活動の説明
偵察/武器化フェーズ		標的企業が有するシステム構成の把握や、サイバー攻撃に使用するツールを準備する。
A	マルウェア作成	サイバー攻撃に利用するマルウェアを準備する。
B	OSINT による公開情報の探索	標的企業の公開サイトや SNS からサイバー攻撃に活用できそうな情報を収集する。専用の情報収集サービスを使えば、工場からインターネットにつながっている IoT 機器なども見つけることもできる。また、標的企業が利用しているクラウドの API を見つけることができれば、クラウドに対して脆弱性のスキャンをかけることも可能である。
C	攻撃ツール準備	サイバー攻撃に使用するツールを準備する。
D	クラウドプラットフォームやサービスに存在する脆弱性の探索	作業ミスによるクラウドサービスの設定ミスや、クラウドプラットフォーム自体が有する脆弱性を探索する。
E	公開されているクラウドの認証情報や API 情報の探索	設定ミスなどにより誤ってインターネットへ公開されている認証情報、API 情報を探索する。
F	脆弱性のある組織外機器を探索	アーキテクチャ内の工場やクラウド基盤に接続する可能性があり、かつ脆弱性を持つ外部機器を探索する。
配送フェーズ		攻撃に使用するツールの送付や、標的企業の機器やネットワークにアクセスする。標的企業のシステムへアクセスする方法は、インターネットを経由する、あるいは物理的に侵入して LAN に接続する方法の 2 種類が考えられる。
G	マルウェア USB メモリ送付	工場宛にマルウェアを仕込んだ USB メモリを送り、受領者が社内 PC に挿入することを狙う。
H	フィッシングメール送付	従業員のメールアドレス宛てにフィッシングメールを送ることで、マルウェアに感染させる
I	不正機器（ローグデバイス）の設置	工場に物理的に接近し、工場内に接続するための不正機器（ローグデバイス）を設置する。

#	攻撃活動名	攻撃活動の説明
攻撃/インストールフェーズ		マルウェアや攻撃に使用するツールを実行し、標的デバイスに侵入する。
J	組織内機器にマルウェアインストール	フィッシングメールやマルウェアを仕込んだ USB メモリにより従業員端末をマルウェアに感染させる。
K	認証情報奪取	フィッシングメールや USB メモリにより感染したマルウェアにより、認証情報を収集する。
L	AP の脆弱性をついた Exploit 攻撃	無線 AP の脆弱性をつき、AP に接続し、工場ネットワークに侵入する。
M	クラウド VPN の脆弱性をついた攻撃	工場とクラウドの間は VPN で繋いでいる。VPN が脆弱性を持っている場合、攻撃者は脆弱性を突き、ネットワークに侵入する。
N	API の不正利用	クラウドインタフェースの API の脆弱性をつき、機密情報などを取得やデータ改ざんを行う。
O	組織外機器にマルウェアインストール	制御システムの保守事業者が持ち込んだ機器にマルウェアを感染させる。
遠隔操作フェーズ		攻撃対象企業の機器やシステムへのログインおよび不正操作を実施する。
P	IoT,機器、エッジ機器へ侵入し、C&C 通信の確立	工場のネットワークに侵入した攻撃者は、収集した認証情報を用い、IoT 機器、エッジ機器へのログインを試みる。ログインが成功した場合、マルウェアを IoT,機器、エッジ機器へインストールし、攻撃者サーバに情報を送る C&C 通信を開始する。
AA	Enterprise の PC へ侵入し、C&C 通信の確立	工場のネットワークに侵入した攻撃者は、収集した認証情報を用い、Enterprise の PC へのログインを試みる。ログインが成功した場合、マルウェアを Enterprise の PC へインストールし、攻撃者サーバに情報を送る C&C 通信を開始する。
Q	GW への不正アクセスによるパケット転送	VPN の脆弱性を突き、ネットワークへの侵入が成功した場合、通信パケットを攻撃者のサーバに転送することで、工場-クラウド間の通信を盗聴する。
R	クラウドプラットフォームや仮想マシンへ不正ログインし、C&C 通信確立	ICS クラウド基盤のネットワークに侵入した攻撃者は、収集した認証情報や攻撃者が作成した不正ユーザーでクラウドインスタンスへのログインを試みる。ログインが成功した場合、マルウェアをクラウド上の仮想マシンにインストールし、攻撃者サーバに情報を送る C&C 通信を開始する。
S	マルウェア感染した組織外機器からクラウドに不正データを送信	クラウド上の仮想マシンにマルウェア感染した組織外機器から不正なデータを送り込む。

#	攻撃活動名	攻撃活動の説明
目的実行フェーズ		攻撃者は、シナリオの「データレイクのデータを改ざん」、「MES 機能の停止」、「情報漏洩」を実現する。
T	IoT/PLC 機器のデータ改ざん	不正ログインした IoT 機器または PLC 機器に保存されたデータレイクに送る設備データを改ざんする。その結果、改ざんされたデータがデータレイクに保存される。
U	エッジ機器のデータ改ざん	不正ログインしたエッジ機器に保存された設備のマスターデータを改ざんする。その結果、データレイクに改ざんされたマスターデータがデータレイクに保存される。
V	データレイクのデータを直接改ざん	ICS クラウド基盤ネトワークを利用してデータレイクにログインし、不正ログインしたクラウドプラットフォームや仮想マシンからデータレイクに保存された設備データを直接改ざんする。
W	クラウド内通信の改ざん	不正ログインしたクラウドプラットフォームやクラウドサービス内の通信を盗聴し、通信データを改ざんする。その結果、データレイクに保存される設備データが改ざんされる。
X	エッジ機器/クラウド間通信改ざん	不正ログインした機器やサービスを利用してエッジ機器とクラウド間の通信を盗聴し、データレイクに送られる通信データを改ざんする。その結果、データレイクに保存される設備データが改ざんされる。
AB	MES サービスに不正アクセス	不正ログインした Enterprise の PC から不正アクセスを実施する。その後、生産業務に関わる内容を改ざんや停止することで MES 機能を停止させる。
AC	MES サーバにマルウェア感染	不正ログインしたクラウドプラットフォームやクラウドサービスにて MES サーバにマルウェア感染させ、不正ログインした対象の機能を停止させる。
AD	クラウドコンソールで MES サーバ機能停止	不正ログインしたクラウドプラットフォームやクラウドサービスを起点に、クラウドコンソールなどから MES サーバ機能を直接停止させる。
AE	IoT / エッジ機器からの情報漏洩	不正ログインした IoT 機器、エッジ機器に保存されている情報を窃取する。
AF	IoT / エッジ機器間の通信盗聴	不正ログインした IoT 機器、エッジ機器などに流れる通信を窃取（盗聴）する。
AG	データレイクからの情報漏洩	ICS クラウド基盤ネットワークを利用してデータレイクにログインし、不正ログインしたクラウドプラットフォームや仮想マシンからデータレイクに保存されたデータを窃取する。
AH	クラウド内端末からの情報漏洩	不正ログインしたクラウドプラットフォームやクラウドサービスにてクラウド内端末に不正ログインし、保存されたデータを窃取する。
AI	エッジ機器/クラウド間通信漏洩	不正ログインした機器やサービスを利用してエッジ機器とクラウド間の通信情報を窃取（盗聴）する。

6.5 セキュリティ対策検討【CCE ステップ 4 】

CCE の最後にあたるステップ 4 セキュリティ対策では、シナリオ 1（特定の生産業務の停止)、シナリオ 2（機密情報の漏洩）を引き起こさないようにするためのセキュリティ対策を検討していく。

6.5.1 セキュリティ対策

今回利用したフレームワーク（サイバーキルチェーン）を用いたセキュリティ対策の考え方は、部分的な攻撃被害を前提にした対策を講じること、攻撃経路を切る対策を講じること、この 2 点である。

前者に関しては、外部からの攻撃を防ぐ防御策のみではなく、ネットワークなどが侵害されて部分的な被害が発生する場合も考慮して対策を講じることである。後者に関しては、ネットワークに侵入されたとしても、「遠隔操作」や「目的実行」に至るまでの間で攻撃を防ぐことができれば被害（目的実行）を防ぐことができるということである。このことは、セキュリティ対策の優先順位を決める上で参考になると考えられる。

本項では、シナリオ 1、シナリオ 2 に関するセキュリティ対策の一覧を表 6-5 に示し、対策内容の詳細を表 6-6 に示す。なお、セキュリティ対策はシナリオ 1、シナリオ 2 で重複が多く、共通のものとして扱う。

表 6-6 には、各セキュリティ対策について 2 つの観点を記載している。1 つ目は NIST CSF[55]でどのコアに該当するか、2 つ目は人的対策、運用対策、技術的対策（いわゆる PPT[56]）のどれに該当するかを示している。なお、人的観点のセキュリティ対策（例 社員のセキュリティ教育、セキュリティ人材育成、各工場とセキュリティ部門の連携体制整備、CSIRT・CISO の設置など）は、個々の攻撃ではなく、組織全体に関わってくるため、表 6-6 には記載していない。

---

[55] NIST CSF は、NIST：National Institute of Standards and Technology（米国標準技術研究所）が発行した重要インフラのサイバーセキュリティ対策を改善するためのリスクベース型のフレームワークである。（CSF：Cyber Security Framework の略）

NIST CSF はサイバーセキュリティ対策が「特定」「防御」「検知」「対応」「復旧」の 5 つの機能に大別され、それぞれの機能に実施すべきセキュリティ対応が記載されているサブカテゴリーが紐付いている。

[56] PPT とは、People, Process, Technology の頭文字を取った言葉であり、セキュリティ対策を検討する上で必要な観点である。3 つの観点で対策を網羅的に行うことで組織全体として脅威に対するサイバーレジリエンス、つまり攻撃を受けてもすぐに立ち直ることができる柔軟な適応力が高まる。

表 6-5 シナリオ１、シナリオ２のセキュリティ対策

攻撃活動	攻撃内容	セキュリティ対策（No）
偵察&武器化		
A	マルウェア作成	―（攻撃者側で完結する活動のため対策は存在しない）
B	OSINT による公開情報の探索	不要な情報公開の見直し(15)
C	攻撃ツール準備	―（攻撃者側で完結する活動のため対策は存在しない）
D	クラウドプラットフォームやサービスに存在する脆弱性の探索	セキュリティ監査(13)
E	公開されているクラウドの認証情報や API 情報の探索	脆弱性管理(1) セキュリティ監査(13)
F	脆弱性ある組織外機器の探索	サプライチェーンセキュリティ(14)
配送		
G	マルウェア USB メモリ送付	USB セキュリティ強化(9)
H	フィッシングメール送付	メールフィルタリング(8)
I	不正機器（ローグデバイス）の設置	入構者管理 不正接続防止(10) セキュリティ監査(13)
攻撃&インストール		
J	組織内機器にマルウェアインストール	セキュリティ監視・分析（機器）(12)
K	認証情報奪取	セキュリティ監視・分析（NW）(11) セキュリティ監視・分析（機器）(12) データ暗号化(7)
L	AP の脆弱性をついた Exploit 攻撃	脆弱性管理(1) 脆弱性診断(2) セキュリティ監視・分析（NW）(11)

M	クラウド VPN の脆弱性をついた攻撃	脆弱性管理(1) 脆弱性診断(2)
N	API の不正利用	脆弱性管理(1) 脆弱性診断(2) 認証機能適応(3)
O	組織外機器にマルウェアインストール	サプライチェーンセキュリティ強化(15)
遠隔操作		
P	IoT, エッジ機器へ侵入し、C&C 通信確立	認証機能適応(3) セキュリティ監視・分析（機器）(12) 不正通信遮断(6)
Q	GW への不正アクセスによるパケットデータ転送	認証機能適応(3) 認証機能強化(4) セキュリティ監視・分析（NW）(11) 不正通信遮断(6)
R	クラウドプラットフォームや仮想マシンへ不正ログインし、C&C 通信確立	サーバレス、マネージドサービス利用（14） 認証機能適応(3) 認証機能強化(4) 認証情報管理(5) セキュリティ監視・分析（機器）(12) 不正通信遮断(6)
S	マルウェア感染した組織外機器からクラウドに不正データを送信	認証機能適応(3) セキュリティ監視・分析（NW）(11) 不正通信遮断(6)

表 6-6 セキュリティ対策の詳細

No.	対策	対策例	NIST CSF	対策区分（PPT）	
				運用的対策	技術的対策
1.	脆弱性管理	自社資産の脆弱性情報の収集、適切なパッチ適用、OS アップデート	特定	X	—
2.	脆弱性診断	クラウドプラットフォーム、アプリケーションなどの脆弱性診断	特定	X	—
3.	認証機能適応	ID/PW、端末情報、証明書による認証を適応	防御	—	X
4.	認証機能強化	多要素認証の導入	防御	—	X
5.	認証情報管理	適切な権限設定、アクセスログの取得・管理	特定	X	X
6.	不正通信遮断	FW、IPS、WAF などを用いた C＆C 通信、脆弱性をつく Exploit 通信の遮断	防御	—	X
7.	データ暗号化	通信するデータやストレージに保存されているファイルの暗号化	防御	—	X
8.	メールフィルタリング	ばらまき型や標的型メールのフィルタリング	防御	—	X
9.	USB セキュリティ強化	社内 USB 使用ポリシー策定、持ち込み USB 機器のチェックなど	防御	X	X
10.	不正接続防止	ホワイトリストスイッチなど、不正デバイスの機器への接続を防止	防御	—	X
11.	セキュリティ監視・分析（NW）	IDS などの NW トラフィックログ監視・分析	防御 検知	X	X
12.	セキュリティ監視・分析（機器）	アンチウイルス、EPP/EDR などのセキュリティソフト、syslog などのログ監視・分析	防御 検知	X	X
13.	セキュリティ監査	定期的な資産管理、CSPM などを利用したクラウドプラットフォームの設定ミス防止	特定 防御	X	—
14.	サーバレス・マネージドサービス利用	サーバレス、マネージドサービスの利用による、責任共有モデルに則ったセキュリティ管理対象の削減	防御	X	—
15.	サプライチェーンセキュリティ強化	契約書へのセキュリティ要件記載などによるサプライチェーンセキュリティの強化	防御	X	—
16.	不要な情報公開の見直し	インターネットに公開する予定のない機器がインターネット上で公開されていないか検索システムなどを用いて確認を行う	特定	X	—

以上、表 6-6 にサイバーキルチェーンの攻撃を断つためのセキュリティ対策を記載した。しかし、記載した内容以外にも、シナリオ 1 及びシナリオ 2 で実施できる対策がある点をご留意いただきたい。

なお表 6-6 ではサイバーキルチェーンを断つための対策を記載したため NIST CSF 列を見ると特定・防御・検知は存在するが、対応・復旧に関しては挙げられていない。しかし、攻撃を受けることを前提での対策を検討することが重要である。従って、攻撃を受けた後を想定し、表 6-6 に掲載されていない検知・対応・復旧の対策例を以下に示す。

- **ログ監視・分析体制の確立（NIST CSF：検知・対応）**

  市場には様々なセキュリティ製品があり、セキュリティ対策に役に立つことは間違いないが、ただ製品を導入することで安心してはならない。むしろ、導入した製品が出力するデータを元に、インシデントレスポンスをはじめとしたアクションを実行できる運用体制が重要である。ログ監視においても、様々なセキュリティ製品のログを SIEM にためるだけでなく、分析した結果を受けてアクションできる体制があって初めて有効に機能する。

- **連絡体制の確立（NIST CSF：対応）**

  通常業務中にサイバー攻撃が疑われる事象に遭遇したとき、セキュリティインシデントが発生した、あるいは発生した恐れがあるときに、状況の深刻度毎に連絡する体制、フローを決めておく。予め決めておくことで、未然にインシデントを防ぎ、インシデント被害の拡大を抑えることができる。

- **被害発生時対応（縮退運転、生産中止、被害報告など）の事前検討（NIST CSF：対応）**

  攻撃被害発生後、時間が経つごとに被害は拡大していく可能性がある。従って、実際に被害が発生した場合を想定し、縮退運転、生産中止、被害報告などの基準、対応手順を経営判断の拠り所としてあらかじめ決めておくことが重要である。

- **バックアップ（NIST CSF：復旧）**

  万が一サイバー攻撃によりデータレイクのデータが改ざんされたり、クラウド内端末にマルウェアを感染されたりした場合でも、事前にバックアップをとっておくことで、攻撃を受ける前の状態に戻すことができる。

上記は全て運用的対策（Process）に関わる部分である。つまりセキュリティを確保するためには、技術的対策（Technology）だけでなく、技術的対策（Technology）を生かすための運用的対策（Process）も同時に考える必要があることを強調しておきたい。

6.5.2　セキュリティ対策の優先度について

前項では、分析して明らかになった脅威に対するセキュリティ対策を記載したが、実際に対策を実施する場合、リソースは有限であるため、優先順位をつけて実施することになる。実施効果、実施コストや実施による既存システムへの影響度合いなどが優先順位をつける際の判断軸として考えられる。例えば、効果についての一つの考え方としては「サイバーキルチェーンの序盤の攻撃フェーズである配送や攻撃、インストールで攻撃を止めることができるセキュリティ対策は、その後の攻撃を防ぐことができるという意味で効果が高い」と言える。しかし、これらの判断軸に対する重みづけ、つまりどの判断軸を重要視するかは、最終的には企業の規模や企業が抱える課題による。従って本指南書では画一的なセキュリティ対策の優先順位づけは行わない。自社のセキュリティ戦略など、総合的に判断した上で優先順位を決めることが重要である。

6.6 アーキテクチャ、脅威分析、セキュリティ対策による気づき

本節では、本指南書の著者らが実際に第 6 章で述べた設計や分析などを行った結果得られた気づきを紹介する。著者ら各人の気付きを列挙しているため、必ずしも整理され、一貫しているものではないかもしれないが、"リアル"な感想や雰囲気を感じ取っていただき、参考にしていただければ幸いである。

・ **セキュアアーキテクチャ設計**

アーキテクチャの粒度は概念レベル、機能レベル、詳細レベルの 3 種類を考えた。本指南書で示したアーキテクチャは機能レベルに該当し、経営層に説明でき、かつ各コンポーネントの具体的な機能もある程度記載しているものである。

アーキテクチャは、一枚に収めることで構成の全体が一目で把握できる。エンジニアなどと会話する際にも有用なツールである。

攻撃者の攻撃経路を考える際は、機能レベルのアーキテクチャに加え、データフローまで記載することで攻撃経路を決めることができる。今回の脅威分析においても、例えば「最適運転推論」のデータフローなら、学習フェーズと推論フェーズをアーキテクチャ上で流れを図示することで分析を実施した。

・ **脅威分析**

本指南書で記載した CCE の前に、各オンプレミスの機器やクラウドの機能ごとに脅威と脆弱性とセキュリティ対策を洗い出す資産ベースの脅威分析を行った。取り掛かりやすい反面以下のようなデメリットがあり、効率的な分析が困難であった。

- 膨大な機器・機能に対し一つずつ脅威や対策を検討する負担が大きい。
- 検討で洗い出した脅威や脆弱性が重複した。
- 攻撃経路が判別しづらく、対策の優先順位づけが難しい。
- アーキテクチャとして機器と機器が繋がったことによって発生する脆弱性に対応できない。
- アーキテクチャを機能単位で作成しているため、資産と脅威の捉え方が難しい。

サイバーキルチェーンを用いて、2 つのシナリオを検討した。攻撃シナリオは直感的に網羅されていないように見えるが、サイバーキルチェーンにおける「目的実行」をする対象の機器や機能が同じであれば、そこに至る経路はある程度パターン化される。またサイバーキルチェーンの攻撃経路を切れば良いという考えは、セキュリティ対策の優先順位を決める上でも有用であると考えられる。

ICS とクラウドを両方で脅威分析する上で、OT 及び IT の双方の知見が必要であることが判明した。起きて欲しくない事象の中には現場の製造機器など物理的に影響する OT 知識、それを引き起こすサイバー攻撃に伴う IT 知識が必要である。双方の知識を持った人材はそこまで多くはなく、**実業務としては OT 担当者、IT 担当者双方を巻き込んで脅威分析を実施することが望ましい。**

・ **セキュリティ対策**

セキュリティは技術的対策（Technology）だけでは不十分である。技術的対策（Technology）を扱う人（People）や最大限に生かすための運用的対策（Process）が活かされることで初めてセキュリティが機能する。セキュリティ対策を検討する場合は、PPT 全てがかみ合い無理のないセキュリティ対策となっているか常々意識する必要がある。

第7章　　おわりに

7.1 まとめ

本指南書では、まず第 2 章で、データ利活用とセキュリティ対応の両立が必要である背景を説明し、データ利活用促進のための ICS へのクラウドサービス活用の有効性を説明した。

第 3 章では、国内および海外の ICS へのクラウドサービス導入事例を調査し、様々な業種でクラウドサービスを活用されており、それぞれメリットを享受できていることが判明した。実際にどのような利用方法があり、どのようなメリットがあるのかを認識し、自社に導入する際に参考にされたい。

第 4 章では、ICS へクラウドサービス導入にあたり、関連する技術要素である OT システムおよびクラウドサービスによるインシデント事例を紹介し、どのようなリスクがあるのかを提示した。クラウドサービスを活用することでデータ利活用が促進し、メリットがある一方で、脅威・リスクにさらされることを今一度理解いただきたい。そして、セキュリティ対策を実施する上で、どのような脅威・リスクがあるのか認識する上で参考にされたい。

第 5 章では、ICS へのクラウドサービスを導入した先進企業へのヒアリング結果をまとめた。実際に ICS へクラウドサービスを導入するにあたり、多くの組織で企画、導入、運用のフェーズごとに課題が発生していることが判明した。ここで挙げている内容は実例ベースであり、自社で取り組む際に同様の課題が発生する可能性がある。それらの課題に対しどのように対応したら良いか、自社で取り組む際に参考になれば幸いである。

第 6 章では、ICS のデータ利活用を実施するためにクラウドサービスを導入する際のアーキテクチャ設計、脅威分析、セキュリティ対策の一連のプロセス並びに対策例を提示した。本プロセスを実施した上で特に重要なことは、脅威分析において様々なバッククラウドを持つ人材と一緒に行うことが必要であるということである。具体的には、工場への影響を検討するための生産設備を熟知している OT 技術者、クラウドサービスやセキュリティ上の脅威を分析できる IT 技術者（セキュリティ担当者)、それぞれの人材が必要である。またセキュリティ対策自体も技術的なことだけではなく、組織体制や運用体制について工場側の協力が不可欠である。従って、ICS にクラウドサービスを導入する際の脅威分析やセキュリティ対策を実施する上では、IT 技術者（セキュリティ担当者）だけではなく、OT 技術者などの人材と一緒に協力して行うことが望ましい。

なおセキュリティ対策を講じたとしても、実際に被害が発生してしまう残存リスクは存在する。そのため、被害が発生したときの対応方法についてもあらかじめ検討しておくことが望ましい。

上記のように、本指南書では取り組み事例の調査、ヒアリング、設計・脅威分析・セキュリティ対策検討を多様な業界からなる OT 技術者、IT 技術者といった様々なバックグラウンドを持ったメンバーで実施した。ICS にクラウドサービスを導入する際に必要な観点を一つにまとめているものであり、導入時に参考になれば幸いである。

7.2 本指南書の課題と制約

第 3 章に示したように、国内は ICS 環境にあるデータの利活用が多く見られたが、制御システム機能（MES/ SCADA/HMI / PLC など）へのクラウド活用はまだ多く見られなかった。これらを実現することでより柔軟な制御システムを実現できると考えられるが、より強固なセキュリティ対応が必要であると考えられる。今後、クラウド MES、クラウド SCADA、クラウド PLC などが普及してくる可能性があり、本指南書では取り上げられなかったが、今後の研究の課題である。

第 6 章でも述べたが、ICS へのクラウドサービス導入では、ICS 側やクラウド側両方の脅威分析が必要であり、本指南書のアプローチを取ることが必要である。一方で、この章で述べたアーキテクチャ並びに脅威分析・セキュリティ対策が絶対の正解ではなく、全てではない。実際のビジネス要件によってアーキテクチャ設計、脅威分析、セキュリティ対策の検討を実施する必要がある。

7.3 本指南書の活用に関して

全体を通して、①本指南書を読む前と比べて、「データ利活用」と「セキュリティ向上」の両立が重要であること。②そして ICS のデータ利活用を行う上でクラウドサービスを活用することが有効であること。これら 2 つを認識することで実際に導入へ前向きになっていただきたい。そして、実際に導入を決めた際に、本指南書の導入時の課題や乗り越え方が参考とされ、「データ利活用」と「セキュリティ向上」の両立の実現に際し、助けになれば幸いである。

謝辞

本指南書の作成にあたり、JFE エンジニアリング株式会社、アクセンチュア株式会社、旭化成株式会社、アズビル株式会社、ダイキン工業株式会社、株式会社牧野フライス製作所の企業をはじめ、先進的な取り組みをされた多くの企業にご協力いただきましたことを、心より感謝申し上げます。

諸般の事情により、全ての方のお名前をここに挙げることはできませんが、お世話になりました皆様にこの場を借りて心より御礼申し上げます。

また産業サイバーセキュリティセンター中核人材育成プログラムの講師であられる、門林雄基先生、小林和真先生、佐々木弘志先生、橋本芳宏先生、満永拓邦先生、青山友美先生、並びに情報処理推進機構 中山顕様には、プロジェクト活動においてご指導・ご助言とともに、各検証機材のご支援を賜り続けてきました。改めて御礼申し上げます。

そして、本指南書の作成や本プロジェクトをともに実施した、メンバーの皆様にも感謝を伝えたいと思います。

プロジェクトメンバー

本指南書は、独立行政法人 情報処理推進機構 産業サイバーセキュリティセンター中核人材育成プログラムにおける卒業プロジェクト「セキュアな ICS クラウド導入指南書」の成果物として作成されました。

（総勢１６名）

＜プロジェクトメンバー＞

（◎リーダー、○サブリーダー、●チームリーダー）

◎　田原　淳平
○　黒木　隆一
○　鈴木　真徳
○　中山　健太
●　古澤　大樹
●　篠原　隆
●　中村　誠
赤木　駿一
荒木　一匡
奥村　友紀
木村　太祐
駒居　智之
林　拓雅
宮下　靖子
山口　義治
行　良治

引用文献

[1] 内閣府経済社会総合研究所国民経済計算部, “2019 年度（令和元年度）国民経済計算年次推計（2015 年（平成 27 年）基準改定値）（フロー編）,” 2020.

[2] 経済産業省、厚生労働省、文部科学省, “2021 年版ものづくり白書,” 2021.

[3] フォースタートアップス株式会社, “【STARTUP DB 独自調査】2022 年世界時価総額ランキング。世界経済における日本のプレゼンスは？,” 26 1 2022. [オンライン]. Available: https://prtimes.jp/main/html/rd/p/000000153.000032589.html. [アクセス日: 28 8 2022].

[4] 独立行政法人情報処理推進機構 社会基盤センター, “DX 実践手引書　IT システム構築編 暫定第 2.0 版,” 2022.

[5] 経済産業省、厚生労働省、文部科学省, “2020 年版ものづくり白書,” 2020.

[6] 経済産業省 中部経済産業局, “スマートファクトリーロードマップ,” 2017.

[7] 三菱総合研究所, “令和 2 年度スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査,” 2021.

[8] NIST, “The NIST Definition of Cloud Computing,” 2011.

[9] 独立行政法人 情報処理推進機構, “NIST によるクラウドコンピューティングの定義,” 2011.

[10] 内閣官房内閣サイバーセキュリティセンター 重要インフラグループ, “クラウドを利用したシステム運用に関するガイダンス,” 2022.

[11] 各府省情報化統括責任者（ＣＩＯ）連絡会議決定, “政府情報システムにおけるクラウド サービスの利用に係る基本方針,” 2021.

[12] デジタル庁, “「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」の改定について,” 2022.

[13] 総務省, “令和 2 年版情報通信白書,” 2020.

[14] 経済産業省, “デジタル産業に関する現状と課題,” 2021.

[15] 総務省, “令和 3 年版情報通信白書,” 2021.

[16] 経済産業省, “データの越境移転に関する研究会 報告書,” 2021.

[17] X-Force, “X-Force 脅威インテリジェンス・インデックス 2022,” 2022.

[18] IDC Japan, “2021 年 国内 IoT/OT セキュリティユーザー調査,” 2021.

[19] 経済産業省、厚生労働省、文部科学省, “2018 年版ものづくり白書,” 2018.

[20] T. W. a. K. Jonakin, “Executive Conversations: Accelerating COVID-19 vaccine development with Marcello Damiani, Chief Digital and Operational Excellence Officer at Moderna,” 1 3 2021. [オンライン]. Available: https://aws.amazon.com/jp/blogs/industries/executive-conversations-accelerating-covid-19-vaccine-development-with-marcello-damiani-chief-digital-and-operational-excellence-officer-at-moderna/. [アクセス日: 4 6 2022].

[21] JPCERT コーディネーションセンター, “制御システム・ セキュリティの 現在と展望 〜 この 1 年間を振り返って 〜,” 2022.

[22] トレンドマイクロ株式会社, “産業制御システムのサイバーセキュリティ実態調査,” 11 7 2022. [オンライン]. Available: https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220711-01.html. [アクセス日: 19 7 2022].

[23] Mission Support Center National & Homeland Security Directorate Idaho National Laboratory , “Consequence-driven Cyber-informed Engineering (CCE),” 2016.

[24] Lockheed Martin, “ THE CYBER KILL CHAIN, ” [オンライン]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [アクセス日: 23 7 2022].

[25] Cloud Security Alliance, “クラウドの重大セキュリティ脅威 11 の悪質な脅威,” 2019.

[26] 内閣府, “第 5 期科学技術基本計画,” 2016.

付属資料

付録 A：用語集

用語	意味・解説
API	Application Programming Interface：アプリケーション・プログラミング・インターフェース ソフトウェアやアプリケーションの一部を異なるソフトウェア、アプリケーション、サービスに提供・連携できるインターフェースのこと
BCP	Business Continuity Plan：事業継続計画 災害、システム障害、テロなど危機的状況下に置かれた場合でも、重要な業務が継続できる方策を用意し、事業を継続できるようにしておくための計画のこと。
CIA	情報セキュリティの 3 要素である Confidentiality（機密性）, Integrity（完全性）, Availability（可用性）の頭文字を取った略称。 3 要素の優先度は、情報セキュリティでは C > I > A だが、制御セキュリティでは A > I > C の順に重要となる場合もある。
CSIRT	Computer Security Incident Response Team：シーサート コンピュータセキュリティインシデントに関する報告を受け取り、調査し、社内外との情報連携など、対応活動を行う組織体の名称。その他にも、製品(Product)に特化した PSIRT、工場(Factory)に特化した FSIRT など、様々な分類が存在する。
CVE	Common Vulnerabilities and Exposures：共通脆弱性識別子 個別製品中の脆弱性を対象として採番される識別子のこと。 米国政府の支援を受けた MITRE 社が採番されている。
DataOps	DataOperations の略称。 組織全体のデータ管理者とデータ消費者の間のデータフローのコミュニケーション、統合、自動化を改善することに焦点を当てた共同データ管理プラクティスのことを指す。
DevSecOps	Development、Security、Operations の冒頭部分を繋げた略称。 DevOps に Security を加えた手法。DevOps とは開発担当（Development）と運用担当（Operations）が連携・協力し、フレキシブルかつスピーディーに開発するソフトウェアの開発手法。この DevOps にセキュリティを融合し、セキュリティを確保しつつ開発スピードを損なわないようにするスタイルのこと。
FTA	Fault Tree Analysis：故障の木解析 望ましくない事象に対しその要因を探る、トップダウン型の解析手法のこと。
HMI	Human Machine Interface：ヒューマンマシンインターフェース 人間と機械が情報をやり取りする手段やそのための装置･ソフトウェアの総称であるが、本指南書では特に機器の操作端末を指す。
IaaS	Infrastructure as a Service：サービスとしてのインフラ サーバやストレージなどのインフラをサービス提供するクラウドサービス形態の一

用語	意味・解説
	つ。
IaC	Infrastructure as Code の略称。 コードを使用してインフラストラクチャの管理と展開を行う。インフラストラクチャ仕様を含む設定ファイルが作成され、設定の編集と配信が容易となる。また、毎回同じ環境をプロビジョニングできるようになる。
MEC	Multi-access Edge Computing：マルチアクセスエッジコンピューティング ユーザー端末の近くにサーバ（エッジ）を分散配置し、データ分析などの処理を端末に近いエッジサーバで実施することで、低遅延を実現させる手法の一つ。
MFA	Multi-Factor Authentication：多要素認証 本人確認のための複数の要素をユーザーに要求する認証方式のこと。
NIST	National Institute of Standards and Technology：米国立標準技術研究所 米国商務省配下の科学技術分野における計測と標準に関わる研究所。サイバーセキュリティ関連文書を数多く発行しており、日本国内においても経済産業省を始めとした各組織が参照している。
OSINT	Open Source Intelligence：オープンソースインテリジェンス インターネットなどで一般に公開されている情報を収集・分析する諜報活動の一種。
OT	Operational Technology：制御・運用技術 ハードウェアやソフトウェアを使用し、工場、プラント、ビルなどの産業機器を制御・運用する手法や技術のこと。
PaaS	Platform as a Service：サービスとしてのプラットフォーム アプリケーションやシステム開発環境や実行するための基盤（プラットフォーム）をサービスとして提供するクラウドサービス形態の一つ。
PLC	Programmable Logic Controller の略称。 製造現場などの機器や設備などの制御に使われる機器（コントローラ）のこと。
Purdue	本指南書では、Purdue Enterprise Reference Architecture を指す。 システムを機能階層ごとに論理的に区分し、セキュリティを確保すべき IT/OT ネットワークゾーンのマップを提示できるようにするモデルのこと。
SaaS	Software as a Service：サービスとしてのソフトウェア 従来パッケージとして提供されていたアプリケーションをサービス提供するクラウドサービス形態の一つ。
SIEM	Security Information and Event Management IT（OT）機器のログを一元的に収集・管理・解析し、ネットワークの監視やサイバー攻撃やマルウェア感染などのインシデントにつながる脅威を検知する仕組み。
SQDC	工場が達成するべき目標である Safety（安全）, Quality（品質）, Delivery（納期）, Cost（コスト）の頭文字を取った略称。 このうち品質・納期・コストの 3 要素を改善することで顧客満足度が高まるが、工場

用語	意味・解説
	においては生産環境が安全であることが前提にある。
WAF	Web Application Firewall：Web アプリケーション用 Firewall Web アプリケーションの脆弱性を悪用した攻撃から Web サイトを保護するセキュリティ対策の一つ。
アジャイル開発	仕様や設計の変更が当然であるという前提のもと、初めから厳密な仕様は決めず、短い開発期間単位を採用することで、変更に対する柔軟性を高めようとする開発手法の一つ。
エッジコンピューティング	利用者側の端末そのものや、端末の近くのサーバでデータ処理・分析を行うコンピューティングの概念。ユーザーや端末の近くでデータ処理することで、クラウドなどでデータ処理する方法に比べ通信負荷や遅延を解消する。
オンプレミス	システムの稼働やインフラの構築に必要となるサーバやネットワーク機器、ソフトウェアなどを自社で保有し運用するシステムの利用形態。
コミュニティクラウド	同一業界・業種などの特定コミュニティに属する利用者を特に対象として提供されるクラウドの利用形態の一つ。
サーバレス	自社でのサーバ構築・管理などを必要とせず、サーバレス提供会社の基盤を用いプログラムを実行できる仕組み。
ハイブリッドクラウド	自社内のプライベートクラウドと社外のパブリッククラウドを組み合わせたクラウド利用形態のことを指す。利用データの種類やデータ量によってプライベートクラウド、パブリッククラウドなどのクラウドサービスの特徴に応じて運用する。
パブリッククラウド	広く一般のユーザーや企業など、不特定多数の利用者に対してクラウドコンピューティング環境を提供しているクラウド利用形態のことを指す。
プライベートクラウド	企業・組織が自社内でクラウド環境を構築し、社内やグループ会社といった閉じた関係者に提供するクラウド利用形態のことを指す。
マネージドサービス	運用管理、保守障害対応などに関してクラウド事業者にアウトソーシングすることができるサービスのことを指す。
ローグデバイス	ネットワークに接続されたデバイスの中で、正規に管理されている機器を除いたデバイスを指す（ローグ：rogue＝はぐれ者という意味）

付録 B：脅威分析の参考情報

6.4 節の脅威分析をする上で参考となる情報やフレームワークをここに記載する。

・ STRIDE

STRIDE は、米国マイクロソフト社により提唱された脅威分析の手法である。Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information Disclosure（情報漏洩）、Denial of Service（サービス拒否）、Elevation of Privilege（権限昇格）の頭文字を取ったものであり、それぞれの脅威を検討することで網羅性の高い分析が可能であるとされている。

・ CSA によるクラウドにおける脅威ランキング

CSA（Cloud Security Alliance）は、クラウドコンピューティングのセキュリティを実現するために、ベストプラクティスを広め推奨する活動を国際的に展開している非営利法人である。CSA により「クラウドの重大セキュリティ脅威 11 の悪質な脅威［25]」などが発表されている。

・ CIS Benchmarks

CIS Benchmarks は、CIS（Center for Internet Security）が発行した、情報システムを安全に構築・維持管理するためのベストプラクティスをまとめたガイドラインである。OS・ミドルウェア・ネットワーク機器などが対象となっており、140 種類以上のベンチマークが発行されている。

項目それぞれにレベルが設定されており、レベルを達成するために必要な対策が詳細に記載されている点が大きな特徴である。

・ MITRE ATT&CK

MITRE ATT&CK は、Adversarial Tactics, Techniques, and Common Knowledge（敵対的な戦術とテクニック、共通知識）の略称であり、米国のサイバーセキュリティに関する活動を行っている非営利団体 MITRE 社による、サイバー攻撃に関する手法を体系化したフレームワークである。また、CVE をもとに、脆弱性を悪用した実際の攻撃を戦術と技術または手法の観点で分類したナレッジベースでもある。

付録 C：システム構築を通じて得られた気づき

本指南書で紹介したアーキテクチャを参考に、著者らで実際に ICS とクラウドを接続した環境を概念検証（PoC）的な観点で構築した。時間・費用面の制約から構成を省略した部分も多々あり、企業で使用できる水準には至っていないが、実際に”手を動かしてみる”ことで得られた気づきがあったため以下に記載する。

なおここではクラウドのメリットも述べている。これは、大きくは2.3.3 項で述べた内容が具体化されているものである。一方、留意点や苦労した点も述べている。これらは、クラウドのデメリットではなく、上手に活用する上でのポイントである。これらを企画・導入時や PoC の参考情報として利用していただければ幸いである。

＜メリット＞

- クラウドではコンソール画面から数分でサーバ（仮想マシン）を準備できる。ハードウェアの管理の手間が削減される。
- さらにサーバレスを使うことで、OS のバージョン管理やパッチ適用などの手間が削減される。
- すぐにサーバを準備できることは、BCP の向上にも繋がる。
- クラウドには十分なサービスの数があり、オンプレミス環境で実現したいことの殆どはクラウドで実現可能であると考えられる。
- サービスの中には、セキュリティに関するサービスも多数あり、特に集約されたマネージドサービスも存在している。これらを活用することでセキュリティ対策自身の管理・運用も容易になる。
- クラウドサービスに関する情報（クラウド事業者からの公式情報、ユーザーの情報）は充実している。留意点で挙げたリスクなどに対しても十分対処できる。
- クラウドでは単一のプラットフォームでシステム実装からセキュリティ対策まで完結できるため学習コストや運用管理面で有利である。
- 今回使用したサービスではデフォルト設定がセキュリティ上安全寄りになっているものもあり、セキュリティ観点で安全性が高い。

＜留意点＞

- クラウド事業者に起因するサービス停止が発生した。ユーザー側でのリスク低減策（機器・経路冗長化、マルチクラウド採用、人による業務継続など）の検討が必要。
- クラウドを利用することでクラウドの機能に由来する新たなセキュリティリスクは発生する（アカウント管理、ICS/クラウド間の通信傍受など）。
- クラウドの使い方によっては長期的に見るとオンプレミス環境での実装よりもコストが上回る可能性も否定できない（期間中に検証できず）。
- クラウドサービスの規約の改定やサービスのアップデート（変更）が業務継続のリスクになる可能性がある。
- クラウドに接続するオンプレミス環境の機器（VPN）などは、従来同様、セキュリティを確保する必要がある。

- クラウド側の仕様に合わせたオンプレミス環境側の機器の設定が必要など、オンプレミス側を設定するにも多少はクラウド側の知識が必要となる。
- クラウド側に制御システムを置く場合、オンプレミス環境側の設備（コントローラなど）との通信断が工場稼働に影響しないよう、短時間の通信断に対応出来る構成にするなどの設計時の考慮が必要となる。
- オンプレミス環境からクラウドへの移行方法は一つではない。業務要件とシステムアーキテクチャに応じて直接移行や多段階移行、並行移行などの手段が取れる。
- オンプレミス環境からクラウドへの移行に伴い、NW セグメントが変わり、セグメントをまたいだデータ取得方式（いわゆる、プッシュ/プル）が変わることによるアプリ改修が必要となる。
- クラウドの仕様に合わせたアプリ改修（例えば、サーバレスサービスでは使用できないライブラリの変更）などが必要である。

＜苦労した点＞

- クラウドのコンソール画面がいつの間にか更新されており、既存の情報やマニュアルと対応関係がなくなってしまっていることがあった。
- サービスによっては、インスタンス（仮想マシン）に独自のポリシーを適用しなければ通信ができないことがある。オンプレミス環境におけるサブネットの概念と異なる点があり初めは戸惑う。
- クラウドから出力されるログは、大量かつ出力内容、出力先が多岐にわたる。クラウドに専門知識をもった人材による対応が必要となる。
- クラウド固有の仕様や初期設定に起因するエラーに遭遇した。それらを把握していないと円滑な環境構築が困難である。

セキュアな ICS クラウド導入指南書

～ データ利活用促進とセキュリティ向上の両立へ ～

初版発行　2022 年 9 月

独立行政法人　情報処理推進機構
産業サイバーセキュリティセンター
中核人材育成プログラム　第 5 期受講生
ICS Cloud プロジェクト