2019 年 4 月 26 日
独立行政法人情報処理推進機構（IPA）

欧州ネットワーク情報セキュリティ機関（ENISA）「スマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティス」

This is a translation undertaken by IPA and therefore is not official translation of ENISA.
The official version is in English and on the ENISA site
http://www.enisa.europa.eu/

本文書は、ENISA の文書 “Good Practices for Security of Internet of Things in the context of Smart Manufacturing” を独立行政法人 情報処理推進機構（IPA）が翻訳したものであり、ENISA による公式の翻訳ではありません。日本語へ翻訳した本文書の著作権は、IPA に帰属します。
本文書は、原文にできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体である IPA は、本翻訳文書に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。原文のありのままの内容を理解する必要のある場合は、ENISA ウェブサイトに掲載されている原文をお読み下さい。

Good Practices for Security of Internet of Things in the context of Smart Manufacturing
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

ENISA について

欧州連合ネットワーク情報セキュリティ機関（European Network and Information Security Agency：ENISA）は、欧州連合（EU）、その加盟国、民間部門およびヨーロッパ市民のためのネットワークおよび情報セキュリティの専門知識を集約している機関である。ENISA はこれらのグループと協力して、情報セキュリティにおけるグッドプラクティスに関するアドバイスや提言を提供している。これは、EU 加盟国が関連する EU 法の実施を支援し、ヨーロッパの重要な情報インフラおよびネットワークのレジリエンスの向上に役立っている。ENISA は、EU 全体のネットワークおよび情報セキュリティの向上に取り組む、国境を越えたコミュニティの発展を支援することによって、EU 加盟国における既存の専門知識の強化を促進している。
ENISA の詳細については、下記ウェブサイトを参照。
www.enisa.europa.eu

連絡先

本文書に関する問い合わせ先：iot-security@enisa.europa.eu
本文書に関するメディアからの問い合わせ先：press@enisa.europa.eu

謝辞

本調査において、以下の個人・企業・各種機関・団体より貴重な意見やフィードバックをいただいた。

Ernie Hayden	443 Consulting
Adrien Becue	Airbus Cybersecurity
Jalal Bouhdada	Applied Risk
Hannes Tschofenig, Reed Hinkel	ARM Ltd.
Denis Justinek	BIOKODA D.O.O.
Alessandro Cosenza	Bticino S.p.A.
Cédric Lévy-Bencheton	Cetome
Jeff Schutt	CISCO
Mirko Ross	Digital Worx GmbH
Gianmarco Baldini	DG JRC
Georges-Henri Leclercq	Engie Laborelec
Brice Copy, Pascal Oser	European Organization for Nuclear Research (CERN)
Jens Mehrfeld	Federal agency for information security (BSI)
Rafal Leszczyna	Gdansk University of Technology
Carlos Valderrama	Geomantis Corporation Limited
Ian Smith	GSM Association (GSMA)
Konstantin	Rogalas Honeywell
Antonio J. Jara	HOP Ubiquitous S.L. (HOPU)
Vangelis Gazis	Huawei Technologies Co., Ltd.
Luca Bizzotto, Mike Edwards, Arndt Kohler, Ivan Reedman Samuel Linares	IBM

Victor Fidalgo Villar	INCIBE (The Spanish National Cybersecurity Institute)
Steve Olshansky, Andrei Robachevsky	Internet Society
Andrey Nikishin, Ekaterina Rudina, Vyacheslav Zolotnikov	Kaspersky Lab
Mahmoud Ghaddar	Legrand
Benedikt Abendroth, Kadri Umay	Microsoft Corporation
Vytautas Butrimas	NATO Energy Security Center of Excellence
Sergi Cuny Lafond	Nestle
Jacques Kruse-Brandao	NXP Semiconductors N.V.
Andrew Tierney, Mark Harrison	PenTestPartners
Stefano Zanero	Politecnico di Milano
Marcin Blasiak, Marcin Tarchalski	Pratt&Whitney
Pirmin Heinzer	MELANI
Jay Thoden van Velzen	SAP
Pierre Kobes, Wolfgang Klasen	SIEMENS AG
Sylvie Wuidart	STMicroelectronics N.V.
Yun Shen	Symantec Corporation
Steffen Zimmermann	Trade Association (VDMA)
Julio Hernández Castro	University of Kent
Antonio Raposo	Volkswagen AG
Filip Chytrý	
EC3/Europol	

目次

ENISA について 2
連絡先 2
謝辞 2
概要 6
１．はじめに 8
1.1 目的 9
1.2 調査の範囲 9
1.3 EU および国際政策の背景 10
1.4 対象読者 12
1.5 方法論 12
1.6 構成 13
2.IIoT：インダストリー4.0 とスマートマニュファクチャリング 14
2.1 定義 14
2.2 セキュリティの課題 19
2.3 参照モデル 21
2.4 資産分類 24
3. 脅威とリスク分析 31
3.1 脅威の分類 31
3.2 インダストリー4.0/スマートマニュファクチャリングのサイバーセキュリティ攻撃シナリオの例 37
4.セキュリティ対策とグッドプラクティス 42
4.1 セキュリティ対策の分類 42
4.2 ポリシー 43
4.2.1 セキュリティ・バイ・デザイン 43
4.2.2 プライバシー・バイ・デザイン 44
4.2.3 資産管理 44
4.2.4 リスクと脅威の管理 45
4.3 組織的対策 45
4.3.1 エンドポイントライフサイクル 45
4.3.2 セキュリティアーキテクチャ 46
4.3.3 インシデント処理 46
4.3.4 脆弱性管理 47
4.3.5 トレーニングと意識向上 47

4.3.6 第三者組織の管理 47
4.4 技術的対策..... 48
4.4.1 信頼性と完全性の管理..... 48
4.4.2 クラウドのセキュリティ 48
4.4.3 事業継続および復旧 49
4.4.4 機械間セキュリティ 49
4.4.5 データ保護 50
4.4.6 ソフトウェア/ファームウェアのアップデート 50
4.4.7 アクセス制御 50
4.4.8 ネットワーク、プロトコル、暗号化 51
4.4.9 モニタリングと監査 52
4.4.10 構成管理 52
用語集 53
付録 A：ENISA「IoT のベースラインセキュリティに関する提言」との関係..... 54
付録 B：セキュリティ対策／グッドプラクティスの詳細なリスト 56
付録 C：調査したセキュリティ標準と参考文献 121
付録 D：指標となるインダストリー4.0 セキュリティインシデントの説明.....130

概要

設計から製造、運用、サプライチェーン、そしてサービスの保守に至る産業オペレーションの全フェーズを自動化するインテリジェントな、相互接続されたサイバーフィジカルシステムを利用するインダストリー4.0 は、急速に現実のものとなりつつある。インダストリー4.0 と IoT に関する脅威は、サイバーフィジカルな性質と固有の自律性により、市民の安全、セキュリティ、およびプライバシーに大きな影響を与え、非常に広範囲となっている。

ENISA は、方法論的なアプローチによって、インダストリー4.0 とスマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティスに関する調査を実施した。この調査は一連の貢献をするものであるが、最も注目に値するのは以下のとおりである。

- 重要なサイバーセキュリティシナリオの共通理解を促進するために、関連する用語（インダストリー 4.0、スマートマニュファクチャリング、IIoT などの用語）を定義。
- 製造プロセスおよびバリューチェーン全体にわたってインダストリー 4.0 の資産を包括的な分類法で分類。
- 関連するリスクと攻撃のシナリオに基づいて、インダストリー 4.0 の詳細な脅威の分類法を紹介。
- 識別された脅威を資産にマッピングし、利害関係者のカスタマイズされた要件に基づくセキュリティ対策の展開を容易にする。
- スマートマニュファクチャリングおよびインダストリー 4.0 における IoT の使用に関連するセキュリティ対策を列挙し、それらを前述の脅威とマッピング。

この調査を実施するにあたり、ENISA は IoT、IIoT（Industrial IoT）、インダストリー 4.0、およびスマートマニュファクチャリングのセキュリティに関する利用可能なドキュメントを確認し、現状を詳細に分析した。また、体系的なアンケートと一連のインタビューを通じて、多くのセキュリティ専門家からの意見を収集した。

また、ライフサイクル（構想段階から生産終了、廃棄まで）を通して、インダストリー 4.0 の機器およびサービスのセキュリティを考慮し、インダストリー 4.0 の要件に固有の課題に細心の注意を払った。したがって、この調査ではセキュリティ対策を 3 つの側面から取り上げている。

- ポリシー
- 組織的対策
- 技術的対策

この調査のもう 1 つの注目すべき要素は、既存のセキュリティイニシアチブ、標準規格、およびスキームへのマッピングである。ENISA は、インダストリー 4.0 および IoT のセキュリティ

に関する 150 を超えるリソースを確認し、それらをこの調査で提案されているセキュリティ対策とマッピングした。このマッピングは、現在 IoT 関連のセキュリティ情報に直面している利害関係者が、共通理解の基礎を持つ助けとなる。

この調査に記載されているガイドラインとセキュリティ対策は、IIoT 機器および生産工程の自動化を高めるソリューションを採用または採用する予定のあるインダストリー4.0 組織がサイバーセキュリティへの取り組みを改善することを目的としている。これらのセキュリティ対策は、IIoT オペレータや製造業者/ベンダーにまたがる幅広い対象者に適用でき、これらの対策や推奨事項をインダストリー4.0 のセキュリティソリューションを検査するためのチェックリストとして利用できる。

この調査の目的は、欧州連合全体でインダストリー4.0 と IIoT のセキュリティに関するコラボレーションを促進し、「セーフティのためのセキュリティ」に焦点を当てて、関連する脅威とリスクについての認識を高めるためのリファレンスポイントとして役立つことである。

1．はじめに

近年、接続性、コラボレーション性、共有性の向上による世界経済の急速な変化によって、データ転送とストレージのコストは大幅かつ急速に減少している。バイモーダル IT 組織がもたらしたこの進展は、スマートコネクテッドワールド、特に製造業の急激な成長を支えている。最近のトレンドには、デジタル化、意思決定の分散化、バリューチェーンの統合などの新しい機能を導入することによって、伝統的な製造業やその他の産業に革命を起こしている「インダストリー4.0」の出現がある。インダストリー4.0 は、サービス・プロビジョニング（サービスの提供）の品質を強化することによって、スマートマニュファクチャリング・インフラを含むインテリジェントなインフラ、接続されたインフラを次々と実現しているサイバーフィジカルシステムに密接に結びついている。

産業界を変革しているモノのインターネット（IoT）を中核とするインダストリー4.0 は、社会、製品の変革、顧客体験、そして労働市場にすでに影響を及ぼしている。そのため、欧州連合のイニシアチブにおいて中心的な役割を果たしており、さまざまな研究、プログラムおよび規制の対象[1]となっている。

第 4 次産業革命、世界中でのコネクテッドデバイス数の急激な増加、それに伴って急増するサイバーセキュリティインシデントによって、特に IoT ソリューションを利用し始めている産業オペレータの間で、サイバーレジリエンスを強化する必要性がさらに重要視されている。インダストリー4.0 とスマートマニュファクチャリングに向けた最近の取り組み[2]は、テクニカルソリューションのセキュリティと、それを信頼する市民の安全に関連する側面により多くの注目が集まっている。新たな脅威によってもたらされる潜在的な影響は、物理的セキュリティの低下から生産の停止時間、製品・機器の損傷、それに伴う経済的損失、および評判の悪化にまで及ぶため、非常に重要である。

インダストリー4.0 とスマートマニュファクチャリングは、特に、製造およびサプライチェーン環境におけるインテリジェンス、自動化、および自律性の導入を加速させる。したがって、EU の産業部門のデジタル化に向けられてきた多大な関心と優先順位付けを前提として、この調査はインダストリー4.0 のコンテキストにおける IoT のセキュリティに焦点を当てている。スマートマニュファクチャリングおよびインダストリー4.0 の進展に関連した脅威に対するベンダーおよびユーザー/消費者の認識は通常限界があるので、このトピックは非常に重要である。同時に、新たな攻撃ベクトルを使用した、安全計装システム(SIS)などの産業用資産に焦点を当てたサイバー攻撃が、最近ますます頻繁に発生している。

---

[1] インダストリー4.0 のコンセプトに関連する EU の取り組みの例：
https://ec.europa.eu/growth/toolsdatabases/dem/monitor/tags/industry-40

[2] EU 内の産業をデジタル化するための取り組みの例：
https://ec.europa.eu/growth/toolsdatabases/dem/monitor/category/national-initiatives

1.1 目的

この調査は、IoT イノベーションの導入によって促進された産業用システムとサービスの進化に関連するセキュリティとプライバシーの課題に取り組むことを目的としている。主な目的は、関連するセキュリティとプライバシーの課題、脅威、リスク、および攻撃のシナリオをマッピングしながら、インダストリー4.0/ スマートマニュファクチャリングにおける IoT のセキュリティ確保のためのグッドプラクティスを集めることであった。

また、欧州連合全体でインダストリー4.0 と IIoT のセキュリティに関するコラボレーションを促進し、「セーフティのためのセキュリティ」に焦点を当て、関連する脅威とリスクについての認識を高めるためのリファレンスポイントを提供することも、調査目的としている。

この調査のもう 1 つの重要な要素は、実施する作業の範囲を設定することでインダストリー4.0 とスマートマニュファクチャリングの概念を定義し、今後の進展の基礎を提供することである。

1.2 調査の範囲

この調査では、産業環境に適用される IoT におけるサイバーセキュリティのためのグッドプラクティスについて概説する。IoT の導入は広範囲に及ぶため、この調査では IIoT（IIoT：Industrial IoT）とスマートマニュファクチャリングに焦点を当てる。これらは、インダストリー4.0 全体[3]の中で最も代表的な要素である。

この調査において ENISA は、IoT、IIoT、インダストリー4.0、スマートマニュファクチャリングおよびその他関連分野のセキュリティに関する利用可能な文書の現状を詳細に分析した。また、体系的なアンケートと一連のインタビューを通じて、多数のセキュリティ専門家からの意見を収集した。既存の作業の徹底的なレビューに基づいて脅威を識別し、インダストリー4.0 とスマートマニュファクチャリングのさまざまな領域をターゲットにした、起こりうる重大な攻撃シナリオを明らかにした。これにより、インダストリー4.0 の IoT におけるセキュリティを確保するためのグッドプラクティスとセキュリティ対策を明らかにすることができた。また、セキュリティの採用におけるギャップと障壁を識別することも可能となった。

この調査では、技術、人、プロセスにおけるセキュリティ上の課題に対処するため、これらの 3 つのグループのセキュリティ対策について説明する。それらの対策には、セキュリティに対するリスクベースの総合的なアプローチが取られた。ENISA は、ライフサイクル全体（構想段階から生産終了まで）を通じて産業環境における IoT 機器とサービスのセキュリティを検討し、特にサプライチェーン全体と第三者組織の管理に注意を払った。

[3] EC, 第 4 次産業革命　: https://ec.europa.eu/digital-single-market/en/fourth-industrial-revolution

1.3 EU および国際政策の背景

世界的に台頭しつつある、接続されるモノのトレンドと、次第に一般的となっている世界中の組織による IoT という概念の採用により、近年の IoT のサイバーセキュリティは、欧州委員会および他の規制機関にとっての関心事となっている。産業およびスマートマニュファクチャリングにおける IoT は、IoT サイバーセキュリティの特定の一部（subset）である。

IoT の可能性とそれに関連するサイバーセキュリティの課題を認識している EU は、アライアンス、専門知識の集約機関の設立、規制文書の作成、パイロットプロジェクトの立ち上げなど、数多くの政策措置を通じて、IoT のセキュリティを確保し、この分野の開発を加速するよう努めてきた。2015 年 3 月、欧州委員会は革新的な欧州の IoT エコシステムを構築することを目的として、IoT イノベーションのための同盟（AIOTI）[4]を始めた。AIOTI は欧州最大の IoT 協会となり、欧州の競争力のある IoT 市場を確立し、新しいビジネスモデルを開発するために、利害関係者と協力するという EU の意向を示した。

2 か月後の 2015 年 5 月、EU はデジタルシングルマーケット（DSM）[5]戦略を採用した。5 つの主要な開発分野の 1 つである IoT に関して、DSM は、ガイドラインの分断や相互運用性の欠如など、セキュア IoT 採用の減速につながる可能性がある一般的な問題に対処することを目指している。2016 年 4 月、DSM のニーズを満たし、今後の方針を周知するために、欧州委員会は IoT に関連するスタッフレポート（staff working repot）を発表した[6]。これは「欧州産業のデジタル化」イニシアチブの一部を構成し、3 つの柱（①繁栄する IoT エコシステム、②人間中心の IoT アプローチ、および③IoT の単一市場）に基づく IoT に対する EU のビジョンを概説している。

IoT と同様に、サイバーセキュリティも標準規格開発の観点において DSM のもう 1 つの優先事項である。それは、IoT におけるサイバーセキュリティと産業システムにおけるサイバーセキュリティにまたがるという広い概念である。IoT サイバーセキュリティに関しては、ENISA は 2017 年に「IoT のベースラインセキュリティに関する提言」[7]という文書を作成し、IoT の概念が生み出されたことで出現したサイバーセキュリティの問題に体系的に示している。[8]
DSM は、典型的な産業イニシアチブの観点から EU の政策を考慮して、ドイツのインダストリー4.0[9]、オランダのスマートインダストリー[10]、フランスのインダストリーデュフューチャー

---

[4] IoT イノベーションのためのアライアンス：
https://ec.europa.eu/digital-single-market/en/alliance-internetthings-innovation-aioti

[5] デジタルシングルマーケット：https://ec.europa.eu/commission/priorities/digital-single-market/

[6] 欧州委員会（2016）「ヨーロッパにおけるモノのインターネットの進歩」：
https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:52016SC0110

[7] ENISA「IoT のベースラインセキュリティに関する提言」：
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

[8] 本文書と「IoT のベースラインセキュリティに関する提言」の関係は付録 A に記載されている。

[9] Plattform Industrie 4.0: https://www.plattform-i40.de/I40/Navigation/EN/Home/home.html

（Industrie du Futur）[11]などのヨーロッパ、各国および地域のイニシアチブの調整を促進することに焦点を当てている。2016 年には、欧州委員会から関連情報が公表された[12]。これらのイニシアチブを通じて、EU はイノベーションを促進し、新しい製品やサービスに備えることを目指している。

IoT と産業のデジタル化は大量のデータの交換、処理、保存に依存しているため、EU の政策措置を議論する際には最近の EU 一般データ保護規則（GDPR）[13]について言及する必要がある。その目的は、プライバシーと個人情報を保護することである。これは、スマートマニュファクチャリング企業、IoT 機器ベンダーおよびオペレータを含むすべての組織に適用される。

EU の方針の展望から国際的な状況に目を移すと、2017 年、米国では IoT のセキュリティ問題に対処するための「IoT サイバーセキュリティ向上法[14]」が提案された。さらに最近、カリフォルニア州知事は、2020 年に発効予定の、米国で最初の IoT サイバーセキュリティ法に署名した。同法は製造業者に、コネクテッドデバイスに合理的なセキュリティ機能を装備することを要求している[15]。この例とは別に、米国国土安全保障省、米国国立標準技術研究所（NIST）、その他の団体も、ガイドライン、フレームワーク、その他の文書の策定を通じて、IoT とスマートマニュファクチャリングに関連するサイバーセキュリティの問題に対処するために取り組んできた。これらのイニシアチブの顕著な例としては、国土安全保障省の出版物「IoT セキュリティの戦略的原則」[16]、または NIST の「サイバーセキュリティフレームワーク 製造業界向けプロファイル」[17]がある。

EU および国際的なイニシアチブを分析することで、IoT のセキュリティに関連するいくつかのポリシーイニシアチブを強調することが可能となる。ただし、インダストリー4.0 および IoT を利用したスマートマニュファクチャリングの概念はまだ策定中であるため、産業環境における IoT セキュリティは依然として規制当局による検討事項と見なされている。

---

[10] Smart Industry: https://www.smartindustry.nl/

[11] Alliance Industrie du Futur: http://www.industrie-dufutur.org/

[12] European Commission (2016) "Digitizing European Industry. Reaping the full benefits of a Digital Single Market": https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0180

[13] European Parliament and Council of European Union (2016) "General Data Protection Regulation": https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[14] United States Congress (2017) "Internet of Things (IoT) Cybersecurity Improvement Act of 2017": https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

[15] California's IoT cybersecurity law: https://www.cnet.com/news/california-governor-signscountrys-first-iot-security-law/

[16] U.S. Department of Homeland Security (2016) "Strategic Principles for Securing the Internet of Things": https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[17] NIST (2017) "Cybersecurity Framework Manufacturing Profile": https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

1.4 対象読者

この調査では、インダストリー4.0 およびスマートマニュファクチャリング組織、すなわち IIoT 機器およびソリューションを採用または採用する予定の組織の IoT サイバーセキュリティへの取り組みを改善するための一連のガイドラインとセキュリティ対策を提供する。これらのセキュリティ対策は、IIoT の通信事業者や製造元/ベンダーをはじめとする幅広い対象者に適用される。想定される対象者のリストには、次のものが含まれる（ただしこれらに限定されない）。

- IIoT の専門家、ソフトウェア開発者、および機器メーカー
- IIoT オペレータとユーザー
- OT（運用・制御技術）および IT セキュリティ専門家およびソリューションアーキテクト
- インダストリー4.0 組織内のセキュリティ担当者（例：最高情報セキュリティ責任者）
- インダストリー4.0 の国際組織およびセキュリティコミュニティのメンバー
- 学術研究開発機関

さらにこの文書は、ポリシー決定レベルでの議論に役立つ可能性もあり、したがって、IIoT セキュリティに関する関連規制の策定にも役立つ可能性がある。

1.5 方法論

この調査の実施にあたって従った方法論（図 1 に示される）は、以下の 5 つのタスクからなる。

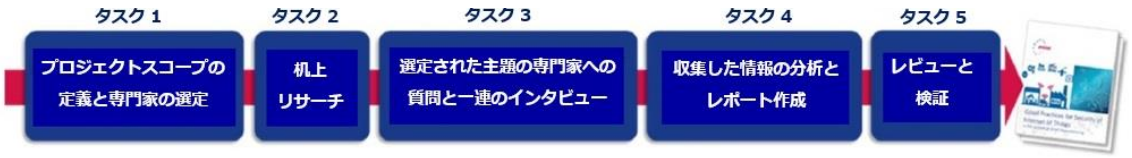

図 1 ：調査で採用された方法論

タスク 1：プロジェクト範囲の定義と専門家の選定

最初のステップは、プロジェクトの範囲を確立することと、レポート作成において考慮される情報や洞察力を持った専門家を選定することであった。ENISA IoTSEC[18]（IoT セキュリティ）および EICS[19]（ENISA インダストリー4.0 サイバーセキュリティ）の非公式専門家グループのメンバー、ならびに選ばれた追加の利害関係者から、専門家が集められた。合計で 42 の異なる機関からの専門家が調査の進展と検証に貢献した。

タスク 2 ：机上リサーチ

このステップでは、プロジェクトに関連する文書を広範囲に調査した。選ばれた情報源は、グッ

[18] IoT Security Experts Group: https://resilience.enisa.europa.eu/iot-security-experts-group-1

[19] EICS Experts Group: https://resilience.enisa.europa.eu/eics-experts-group

ドプラクティスやこのレポートの他の部分を作成するための参考資料として役立った。

タスク 3：選定された専門家への質問と一連のインタビュー

ENISA は、さまざまな IIoT およびインダストリー4.0 セキュリティの側面をカバーする質問表を作成した。質問は専門家グループによって完成された。さらに、これらの専門家との一連のインタビューを通じて、このレポートを作成するための貴重な情報を収集した。

タスク 4：収集した資料の分析とレポート作成

机上リサーチおよび関係者との共同作業から集められたインプットは、ENISA の専門家によって徹底的に分析された。この分析に基づいて、このレポートの最初の草稿が作成された。

タスク 5：レビューと検証

ENISA は再び専門家と連絡を取り、レポートの草稿を彼らと共有し、コメントやフィードバックを得た。利害関係者のフィードバックを考慮し、2018 年 10 月 26 日にニューハンプシャー州ハーグで開催された検証ワークショップで、このレポートの最終版が作成され、専門家によって検証された。

この方法論により、ENISA は関係する利害関係者と積極的に関わることができ、下記を実現した。

- 用語の定義（例：インダストリー4.0、スマートマニュファクチャリング、IIoT など）
- 対応する資産の識別（どのような種類の資産であり、それらが製造プロセスおよびバリューチェーン全体のどこでどのように使用されているか）
- IIoT に対して起こりうる脅威、リスク、および攻撃のシナリオの識別
- 資産と識別された脅威のマッピング
- スマートマニュファクチャリングにおける IoT の使用に関連するセキュリティ対策の一覧化

1.6 構成

この調査は以下のように構成されている。

- 第 1 章：調査の目的、範囲、背景、対象読者、方法論および文書の構成に関する序論的情報。
- 第 2 章：インダストリー4.0 とそのコンポーネントの定義。ここでは、説明した概念と関連するセキュリティ上の課題について概説。
- 第 3 章：脅威の分類とインダストリー4.0 /スマートマニュファクチャリングの攻撃シナリオの例を含む脅威とリスクの分析。
- 第 4 章：脅威、セキュリティドメイン、標準、その他の関連文書にマッピングされたセキュリティ対策とグッドプラクティスの説明。

2. IIoT：インダストリー4.0 とスマートマニュファクチャリング

2.1 定義

このレポートは、比較的新しい用語である IoT、インダストリー4.0、スマートマニュファクチャリング、および IIoT に焦点を当てている。一般的に認められた定義がほとんどない中、これらの用語の定義は数多く存在する。また、出典と文脈によって、用語の説明は大幅に異なる場合がある。したがって、特定の定義を採用し、用語の理解を明確にすることが重要である。この調査において ENISA は、IIoT を産業環境で適用される IoT（ENISA ベースライン IoT セキュリティ勧告で定義されている[20]）として定義している。インダストリー4.0 は、IIoT とスマートマニュファクチャリングを含む、より広い概念である。

ENISA は、インダストリー4.0 を「IoT などの新しいサイバーフィジカル技術を取り入れることで、生産における分散型意思決定を可能にする、デジタル化され統合されたスマートバリューチェーンへのパラダイムシフト」と定義している。

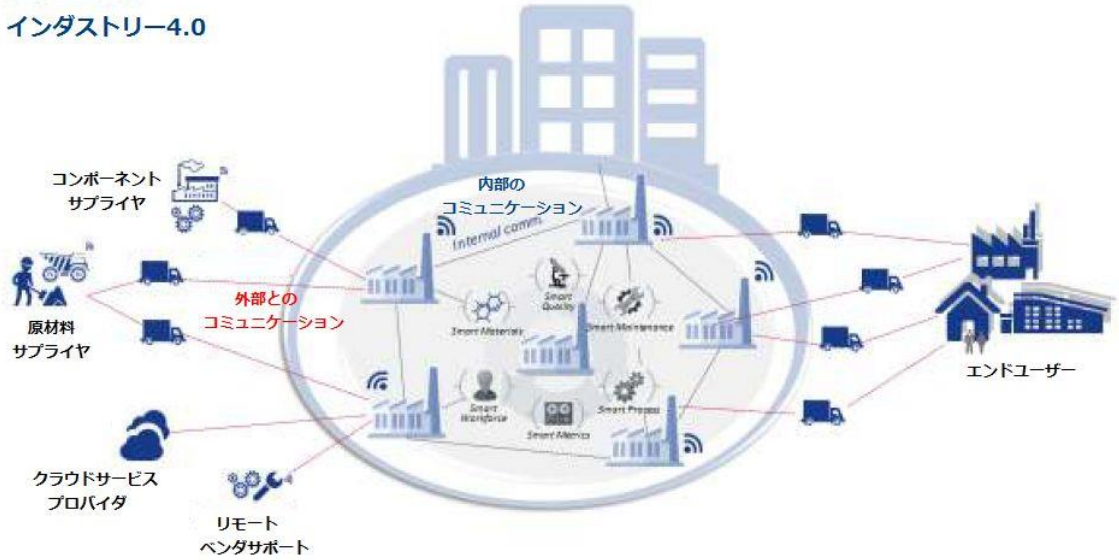

図 2：インダストリー4.0 のコミュニケーションの関係

インダストリー4.0 の設計原則は、第４次産業革命とも呼ばれ、相互運用性、自律性、情報の透明性、技術支援、そして分散した意思決定を含んでいる[21]。伝統的な生産工程の論理を逆転させる最近の技術的進歩は、インダストリー4.0 の概念の形成をもたらし、分散型生産への移行を示している。インダストリー4.0 の出現により、製品は単に機械によって処理されるのではなく、

[20] ENISA (2017) “Baseline Security Recommendations for IoT”: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

[21] Connected Factory Global (2016) “Manufacturing Control System Cybersecurity: Risk Assessment & Mitigation Strategies”: http://www.connectedfactoryglobal.com/resources/cybersecurity-report/

関連する情報と指示を提供する環境と通信する（デジタルツインの概念を参照）。製品と生産ラインはもはや隔離されておらず、ネットワーク全体の不可欠な部分となっている。

明確なコミュニケーション階層を持つハードウェアをベースにしたシステム構造が普及していた業界の伝統的なアプローチとは対照的に、インダストリー4.0 は機能がハードウェアに縛られずにネットワーク全体に分散される柔軟なシステムを取り入れた。これらの新しいシステムでは、組織内の階層レベルを越えた内部コミュニケーションを見ることができる。新しいタイプのやり取りが生まれ（図 2 を参照）、組織外部とのやり取りが大きく変化し、より柔軟になった[22]。

インダストリー4.0 は生産を情報通信技術に結び付け、エンドユーザーデータと機械データを結合して、機械同士の通信を可能にする。その結果、コンポーネントや機械が柔軟で効率的、かつ省資源となる方法で、自律的に生産を管理することが可能となった。その利点には、とりわけ、より高い製品品質、より高い柔軟性、より短い製品発売までの時間、新しいサービス、およびビジネスモデルが含まれる[23]。図に示されているフローは物理的なモノおよびデータ（例えばデジタルツインのやり取り）を参照していることに留意することが重要である。データフローは少なくとも双方向である（例：顧客は生産/製造工程にフィードバックを提供することができる。）

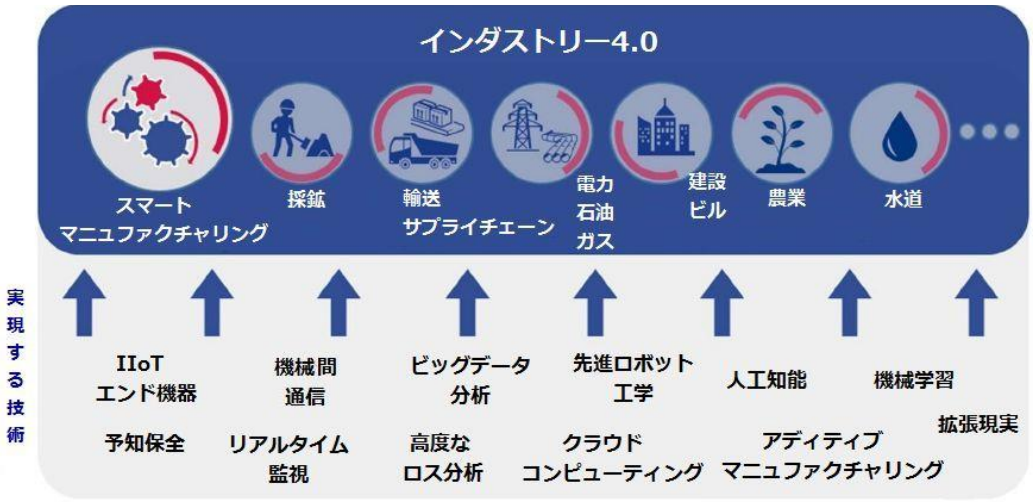

図 3　インダストリー4.0 のスマートマニュファクチャリング

インダストリー4.0 は、さまざまな新機能を導入することで、製造への新しいアプローチ、つまりスマートマニュファクチャリングを可能にする。新技術を使用した製品の製造に焦点を当てたこの特定の概念は、インダストリー4.0 のほんの一部にすぎない。インダストリー4.0 は、さまざまな産業分野を網羅する上位集合（superset）と見なすことができる。図 3 は、スマートマ

[22] Plattform Industrie 4.0 (2016) “Technical Overview: Secure Identities”: https://www.plattformi40.de/I40/Redaktion/EN/Downloads/Publikation/secure-identities.pdf?__blob=publicationFile&v=9

[23] Plattform Industrie 4.0 (2018) “RAMI4.0 – a reference framework for digitalisation”: https://www.plattformi40.de/I40/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.pdf?__blob=publicationFile&v=4

ニュファクチャリングがインダストリー4.0 およびその他の使用されている技術とどのように関連しているかを示している。

ENISA は、スマートマニュファクチャリングを「アディティブマニュファクチャリング、高度な分析、IT / OT 統合など、インダストリー4.0 に沿って出現した情報通信技術に基づいて構築された、次世代の工業生産プロセスおよびシステム」と定義している。この新しい用語は、コネクテッドデバイスとセンサなど、デジタル情報の急速な流れと普及を促進する高度な技術を使用して、コスト、配送、柔軟性、品質などの機能を最大化しようとするシステムを表す[24]。スマートマニュファクチャリングは、初期の製造モデルの機能のいくつかを組み合わせながら、高度な意思決定を含む独自の新機能を導入した。共同サプライチェーンとともに、組織は市場の変化や混乱に迅速に適応することができる。

イノベーションと望ましい拡張機能を実現するために、インダストリー4.0 とスマートマニュファクチャリングは、次のようなさまざまな技術を活用している（図 4 を参照）。

- IIoT エンド機器
  センシング、アクチュエーティング、データの保存、および/または処理などのさまざまな機能を持ち、ネットワークを介してデータを処理・交換する機器。

- 機械間通信（M2M：Machine-to-Machine）
  人を介さずにネットワーク内の機器間の直接通信を促進する技術。

- ビッグデータ分析
  スマートセンサ、機器、ログファイル、ビデオ、およびオーディオによってリアルタイムに生成された膨大な量のさまざまな種類のデータセットを調べるプロセス。

- 先進ロボット工学
  エラーから学び、パフォーマンスを向上させる機能など、スマートな機能を備えた複雑なタスク用に設計された先進の産業用ロボット。

- 人工知能（AI：Artificial Intelligence）
  コンピュータやデジタル機器が通常は人間が行うタスクを実行できるようにするアルゴリズム。

- 機械学習（ML：Machine Learning）
  明示的にプログラムされていなくても、コンピュータが自ら学び、予測能力を向上させるこ

[24] NIST (2016) “Current Standards Landscape for Smart Manufacturing Systems”: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8107.pdf

とを可能にするアルゴリズム。

- 予知保全（Predictive Maintenance）
  可能な限り低い頻度で効果的にメンテナンスを実行するために、障害が発生する可能性がある時期を予測する、機器の状態を監視するソリューション。

- リアルタイム監視
  システムコンポーネントからのセキュリティデータの収集と集約、およびネットワークで発生するイベントの監視と分析を可能にする技術。

- 高度なロス分析（Advanced loss analytics）
  スマートマニュファクチャリング環境で発生する可能性があるさまざまな種類のロスを、それらを排除または軽減することを目的として分析するための方法。

- クラウドサービス
  最小限の管理やサービスプロバイダとのやり取りで、ネットワーク、サーバー、アプリケーションなどの共有リソースセットへのアクセスを可能にするソリューション。

- アディティブマニュファクチャリング（Additive Manufacturing）
  材料を追加することによって様々な幾何学的形状のオブジェクトの作成を可能にする技術。（例：3D 印刷またはラピッドプロトタイピング）

- 拡張現実（Augmented Reality）
  手動組立作業の効率を向上させるためにスマートマニュファクチャリングで使用される技術など、現実世界環境の認識を変更する技術。

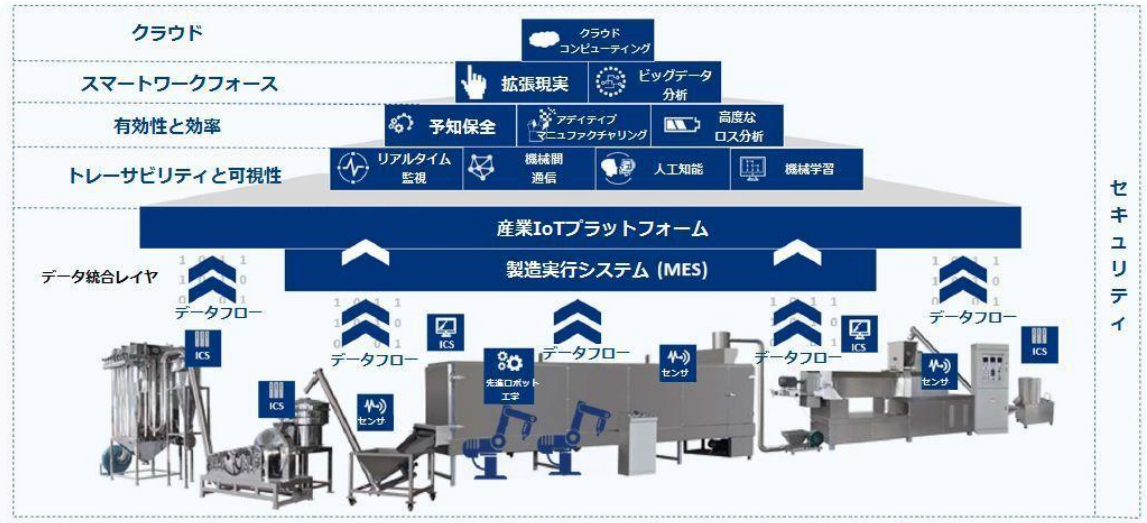

図 4：インダストリー4.0 とスマートマニュファクチャリングの機能

インダストリー4.0 とスマートマニュファクチャリングの概念はかなり複雑である。専門家へのインタビューの回答および関連する出版物の分析に基づいて、ENISA は以下の主要な要素を識別した。

- ICS（産業用制御システム）

  ICS は、SCADA（監視制御およびデータ収集）や DCS（分散制御システム）などの制御システム、PLC（プログラマブルロジックコントローラ）、および HMI（ヒューマンマシンインターフェース）などのその他の制御システム要素と機器で構成されている。システム内の様々な制御コンポーネントは、互いに協働して特定の制御目的を達成する。（例；パイプ内の液体の流れを設定された流速に維持する、圧力または温度を範囲内に維持するなど、事前設定パラメータ内で製品を製造または望む状態を作り出す）。さらに、ICS にはリモート診断およびメンテナンスツールが含まれている場合がある。

- IIoT エンド機器

  IIoT エンド機器には、センシング、アクチュエーティング、情報の保存、処理など、さまざまな機能がある。産業用アプリケーションで長年使用されてきたセンサやアクチュエータなどの従来の機器との違いは、IIoT エンド機器がネットワーク上でデータ交換することである。スマートマニュファクチャリング環境では、大量の新しいタイプのデータを利用できるようにすることで、生産の合理化に貢献する。

- 製造プロセスとビジネスプロセス

  製造プロセスおよびビジネスプロセスは、特定の目標を達成するための活動から成る。特定の目標とは、原材料または部品から最終製品を得ることである。これらのプロセスには、企業の特性によって大きく異なる可能性のある技術的手順や組織的なプロセスが含まれ、これらによって企業全体を正常に運営することができる。

- 人工知能と機械学習

  スマートマニュファクチャリングでは、産業プロセスから膨大な量のデータを収集するため、さまざまな機械学習および AI アルゴリズムが分析に使用される。人工知能は、産業用ロボットの再プログラミングに長い時間を費やすことなく、製造を状況に容易に適応可能にすることで製造を変容し、予知保全を可能にし、そして柔軟性を向上させる。[25]

- 制御システムの通信ネットワークとそのコンポーネント

  制御システムの通信ネットワークとそのコンポーネントには、ネットワーク、ネットワーク機器、および産業用プロトコルが含まれる。ネットワークは、異なるノードがデータリンクを介して、データや情報を交換することを可能にするため、スマートマニュファクチャリン

[25] TOPBOTS (2017) “Future Factories: How AI enables smart manufacturing”: https://medium.com/topbots/future-factories-how-ai-enables-smart-manufacturing-c1405f4ec0e6

グ・エコシステムにおいて重要な役割を果たす。制御システム通信におけるネットワークは、入力および出力をエンド機器へ転送、またはエンド機器から転送するためのシリアルリンクおよびデジタルリンクを含む。ネットワーク機器には、ゲートウェイ、ルーター、スイッチなどがある。産業用通信プロトコルの典型的な例には次のものが含まれる（ただしこれらに限定されない）： HART[26]、Modbus TCP/IP[27]、OPC[28]、および OPC-UA[29]。

2.2 セキュリティの課題

インダストリー4.0 の技術を採用し、製造をスマートにすることによる多くの利点は、重大なセキュリティ課題と密接に関係している。最近の調査で、65%の企業が、OT / ICS のサイバーセキュリティのリスクは、IoT 技術で発生する可能性が高いと関係者が考えていることが明らかになった[30]。スマートマニュファクチャリングとインダストリー4.0 が直面する一般的なセキュリティの課題について、以下に詳しく説明する。

- 脆弱なコンポーネント

  第４次産業革命とともに、新しい“モノのインターネット（IoT）”という領域が、世界中で何百万ものコネクテッドデバイスと共に出現した。そのため、スマートマニュファクチャリングで IoT を保護するには、接続された膨大な数の資産を保護する必要がある。さらに、IoT サイバーセキュリティは独立した概念ではなく、いくつかのセキュリティ分野と相互に関連している。例えば、IT セキュリティ、OT セキュリティ、および物理的なセーフティはこの領域をさらに広げた。閉じたサイバーフィジカルシステムから相互接続されたサイバーフィジカルシステムに移行した結果として、スマートマニュファクチャリング企業は、そのようなシステムの典型的な脆弱性の問題に対処する必要がある。産業環境では、ほとんどのシステムがサイバーセキュリティを念頭に置いて設計されていない[31]ため、ハードウェアの脆弱性がますます一般的になっており、かなりの困難をもたらす可能性がある[32]。

- プロセスの管理

  コネクテッドデバイスが持つ大きな攻撃面（attack surface）に加え、スマートマニュファクチャリングに関連する多数の複雑なプロセスも考慮する必要がある。インダストリー4.0 の企業では、特に機能性と生産効率がサイバーセキュリティよりも優先度が高いと見なされ

[26] HART (Highway Addressable Remote Transducer Protocol): https://www.fieldcommgroup.org/technologies/hart

[27] MODBUS TCP/IP Specification: http://www.modbus.org/specs.php

[28] OPC (Open Platform Communications): https://opcfoundation.org/about/what-is-opc/

[29] OPC Unified Architecture (OPC UA): https://opcfoundation.org/about/opc-technologies/opc-ua/

[30] Kaspersky Lab (2018) “Worried about IoT, but hit by malware: Kaspersky Lab reveals industrial organization pain points”: https://www.kaspersky.com/about/press-releases/2018_ics-cybersecurity

[31] Hongmei He (2017) “Security Challenges on the Way Towards Smart Manufacturing”: https://www.iotsecurityfoundation.org/security-challenges-on-the-way-towards-smart-manufacturing/

[32] Positive Technologies (2018) “ICS SECURITY: 2017 IN REVIEW”: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/ICS-Security-2017-eng.pdf

ているため、サイバーセキュリティを念頭に置いてプロセスを管理することが課題となる。

- 接続性の向上

  製造プロセスはグローバル規模でオブジェクトや環境と相互作用する必要があり、スマートマニュファクチャリングで使用されるシステムは、複数の組織間でコラボレーションを可能にする必要がある。接続性を高めるための最大の課題の 1 つは、セキュリティがセーフティに直接影響を与える可能性があることである。

- IT/OT の融合

  ICS 領域への IT コンポーネントの組み込みが一般的になると、ICS が隔離されるということはなくなった。IT ネットワークに対応した組織との統合は、複雑な環境の管理を簡素化したが、同時に新しいセキュリティリスクをもたらした。 IT / OT 統合の管理は重要な課題である。寄与する要因には、セキュアでないネットワーク接続（内部および外部）、OT 環境に未知のリスクをもたらす既知の脆弱性を持つ技術の利用、および ICS 環境の要件への理解不足が含まれる。全体的なセキュリティは、デジタルツインと物理的な実装をカバーする必要がある。

- サプライチェーンの複雑さ

  製品やソリューションを製造する企業が製品のすべての部分を製造することはほとんど不可能であり、通常は第三者組織のコンポーネントに頼る必要がある。技術的に高度な製品の開発では、非常に複雑なサプライチェーンが形成され、多くの人や組織が関与することになり、管理面で非常に厳しいものとなる。すべてのコンポーネントをそのソースまで追跡できないということは、製品のセキュリティがその製品の最も脆弱な個所に準ずる以上、製品のセキュリティを確保できないということを意味する。

- レガシーな ICS

  最近の調査によると、回答者の 3 分の 1 以上が、レガシーなハードウェアが、IIoT を採用する上で重大な障害となっていると回答している[33]。製造業者はレガシーシステムの上に新しいシステムを構築するが、これは時代遅れの防御対策であるほか、何年もの間悪用されずに済んでいた未知の脆弱性を含んでいる可能性がある。古くなったハードウェアに新しい IoT 機器を追加すると、攻撃者がシステムを侵害する新しい方法を見つける可能性があるという懸念がある[34]。

- セキュアでないプロトコル

  製造コンポーネントは、特定のプロトコルを使用して専用の産業用ネットワークを介して通

[33] World Economic Forum (2015) “Industrial Internet of Things: Unleashing the Potential of Connected Products and Services”: http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

[34] Synopsys (2017) “State of Fuzzing 2017”: https://www.synopsys.com/content/dam/synopsys/sigassets/reports/state-of-fuzzing-2017.pdf

信する。最近のネットワーク環境では、これらのプロトコルは多くの場合、サイバー脅威に対する適切な保護を保証できない。最近の報告によると、最もセキュアでないプロトコル 5 つのうち 4 つが ICS に固有のものである。

- ヒューマンファクタ
  新しい技術を採用することは、工場の従業員とエンジニアが新しいタイプのデータ、ネットワーク、およびシステムを新しい方法で操作しなければならないことを意味する。彼らはデータを収集、処理、分析することに関連するリスクについて意識していないため、攻撃者にとって格好の標的になる可能性がある。2016 年に最もフィッシングメールの標的とされていた業界が製造業であったことを考えると、これはますます懸念事項となってきている[35]。

- 未使用の機能
  産業用機械は、多数の機能やサービスを提供するように設計されているが、その多くは実際のオペレーションに必要ない場合がある。産業環境では、機械またはコンポーネントは、しばしば潜在的な攻撃領域を大幅に拡大する可能性がある未使用の機能にアクセスでき、攻撃者の侵入口になることがある。

- セーフティ面
  物理的世界で動作するアクチュエータの存在によって、セーフティは IoT／スマートマニュファクチャリングに非常に重要なものとなっている。セーフティのためのセキュリティは、最重要課題の 1 つとして浮上している。

- セキュリティの更新
  IoT にセキュリティの更新を適用することは非常に困難である。ユーザーインターフェイスの特殊性によって、従来の更新メカニズムを使用できないためである。更新メカニズムをセキュアにするメカニズムは、特に無線によるアップデートを考えると大変な課題である。OT 環境では特に、ダウンタイム中にスケジュールして実行する必要があるため、更新を適用するのが難しい場合がある。

- セキュアな製品ライフサイクル
  機器のセキュリティは、製品のライフサイクル全体、さらには機器の生産終了やサポート終了までも含めて検討する必要がある。

2.3 参照モデル

多数の要素からなるスマートマニュファクチャリング環境は、かなり複雑に見えることがある。この概念をよりよく説明するために、このプロジェクトの範囲に合わせて調整されたパデューモ

[35] NTT Security (2017) “Global Threat Intelligence Report 2017”: https://www.nttsecurity.com/en-us/gtir-2017

デル（Theodore J. Williams、およびコンピュータ統合生産 [CIM]のための米製造業・パデュー大学コンソーシアムのメンバーによって開発されたパデュー・エンタープライズ参照アーキテクチャー[36]。ISA-95[37]で参照されている。）に基づく参照モデルが提案されている（図 5 を参照）。

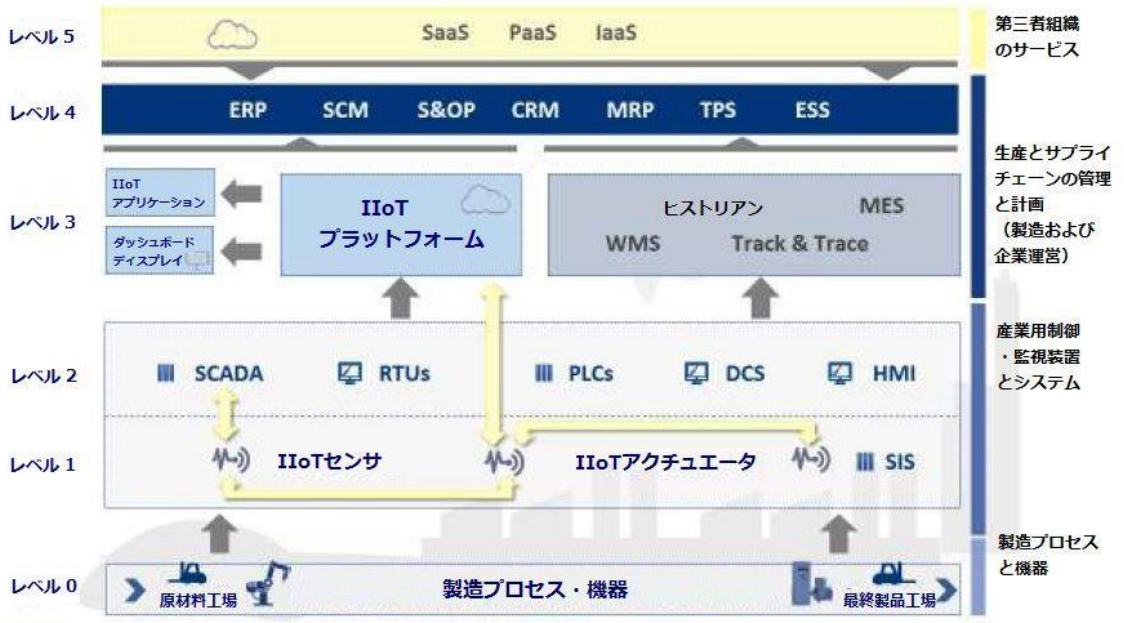

図 5：参照モデル

提示された概念では、スマートマニュファクチャリング環境を 6 つの階層に分けている。これらは順番に配置され、一番下の階層（レベル 0）が製造プロセス、次に機器、システム、サービス（レベル 1－5）となっている。レベル 1 とレベル 2 は OT 層を表している。IIoT 機器はこのモデルのレベル 1 に分類される。レベル 4 は企業の IT 部分に対応し、レベル 3 はシステムを IT と OT の間に分類した中間層である。IIoT プラットフォームの利用は、レベル 3 の一部に含まれる。パデューモデルには表示されていない最上位のレベル 5 は、一般的に外部のサービスが使用されるスマートマニュファクチャリングに固有のものである。

参照モデルの目的は、最も重要な資産（セクション 2.4 を参照）とコンポーネント（セクション 2.1 を参照）の関係の一般的な概要の説明である。灰色の矢印は、モデル内のより大きなグループ間の簡略化された通信経路を表している。さらに、インダストリー4.0 で導入され、IIoT 機器をネットワークに組み込むことで可能になった新しい通信経路（IIoT 機器間の通信および IIoT 機器の IIoT プラットフォームへの直接接続など）が、セキュリティとプライバシーの観点から重要性を強調するために黄色の矢印で追加されている。

[36] The Purdue Enterprise Reference Architecture by T.J. Williams: https://www.sciencedirect.com/science/article/pii/0166361594900175

[37] ISA95: https://www.isa.org/isa95/

以下、参照モデルの各レベルについて簡単に説明する。

レベル 0：製造工程と設備（機械、ロボット）

スマートマシンやロボットによって実行される製造プロセスが行われる、最下層の IIoT 環境。参照モデルの上位レベルにある機器とシステムによって測定および制御される。

レベル 1：IIoT 機器 - センサとアクチュエータ

システムパラメータを測定する IIoT 機器（IIoT センサ）と特定のアクションを実行する IIoT 機器（IIoT アクチュエータ）で構成される。データは IIoT プラットフォーム（レベル 3）と同様に IIoT 機器と制御システム（レベル 2）の間で伝送される。レベル 1 には SIS も含まれる。

レベル 2：産業用制御装置とシステム

IIoT 機器（レベル 1）からの情報に基づいて産業プロセス（レイヤ 0）を制御する機器およびシステム。コントローラー（PLC、RTU）、分散制御システム（DCS）、オペレータパネル（HMI）、および監視制御システム（SCADA）が含まれる。

レベル 3：製造業務システムと IIoT プラットフォーム

OT と IT 環境の間の中間層。製造工程を管理するために使用されるシステム（製造実行システム（MES）、ヒストリアン、倉庫管理システム（WMS）および追跡システムなど）が含まれる。これらのシステムは、OT 環境と IT 環境の両方と通信する。この層を区別することで、通信を制御することが可能になり、OT 層と IT 層の間の直接通信が妨げられる。参照モデルのレベル 3 には、IIoT 機器によって提供される製造および制御プロセスからのデータを分析・管理する IIoT プラットフォームも含まれる。

レベル 4：エンタープライズオペレーションシステム

企業レベルで業務をサポートする IT システム。サプライチェーンと生産管理・計画が含まれる。レベル 2 のシステムとは対照的に、リアルタイムでは動作しない。このレイヤには、以下のシステムが含まれる（この一覧はすべてを網羅しているわけではない）。

ERP（Enterprise Resource Planning：統合基幹業務システム）、SCM（Supply Chain Management：サプライチェーン管理）、S&OP（Sales & Operations Planning：販売・業務計画）、CRM（Customer Relationship Management：顧客関係管理）、MRP（Material Requirements Planning：資材所要量計画）、TPP（Transaction Processing System：トランザクション処理システム）、および ESS（Executive Support System：経営支援システム）。

レベル 5：第三者組織のサービス

前述のように、第三者組織のサービスへの依存はスマートマニュファクチャリングに固有の特性である。このため、インダストリー4.0 とスマートマニュファクチャリングの詳細をよりよく反映するために、第三者組織のサービスを含めるレベルを ISA 95 モデルの上に追加した。これらのサービスは様々な形態がある。例えば、サービスとしてのソフトウェア（SaaS）、サービスと

してのプラットフォーム（PaaS）、およびサービスとしてのインフラ（IaaS）など。

2.4 資産分類

スマートマニュファクチャリングにおける IoT セキュリティの詳細に焦点を当てるには、IoT という広大で複雑な環境の資産の識別と分解から始めることが不可欠である。ここでは、保護が必要な主要な資産グループと資産の概要を説明する。インダストリー4.0 / スマートマニュファクチャリング資産は、図 6 と表 1 に示す主要グループに分類される。表中の各資産グループに割り当てられたレベルは、セクション 2.3 で定義されたレベル、すなわち図 5 に示された参照モデルに対応する。最も低いレベルの分類は示唆的なものであり、網羅的なものではない。たとえば、センサの種類やネットワークプロトコルがすべて記載されているわけではなく、代表的なものだけが記載されている。

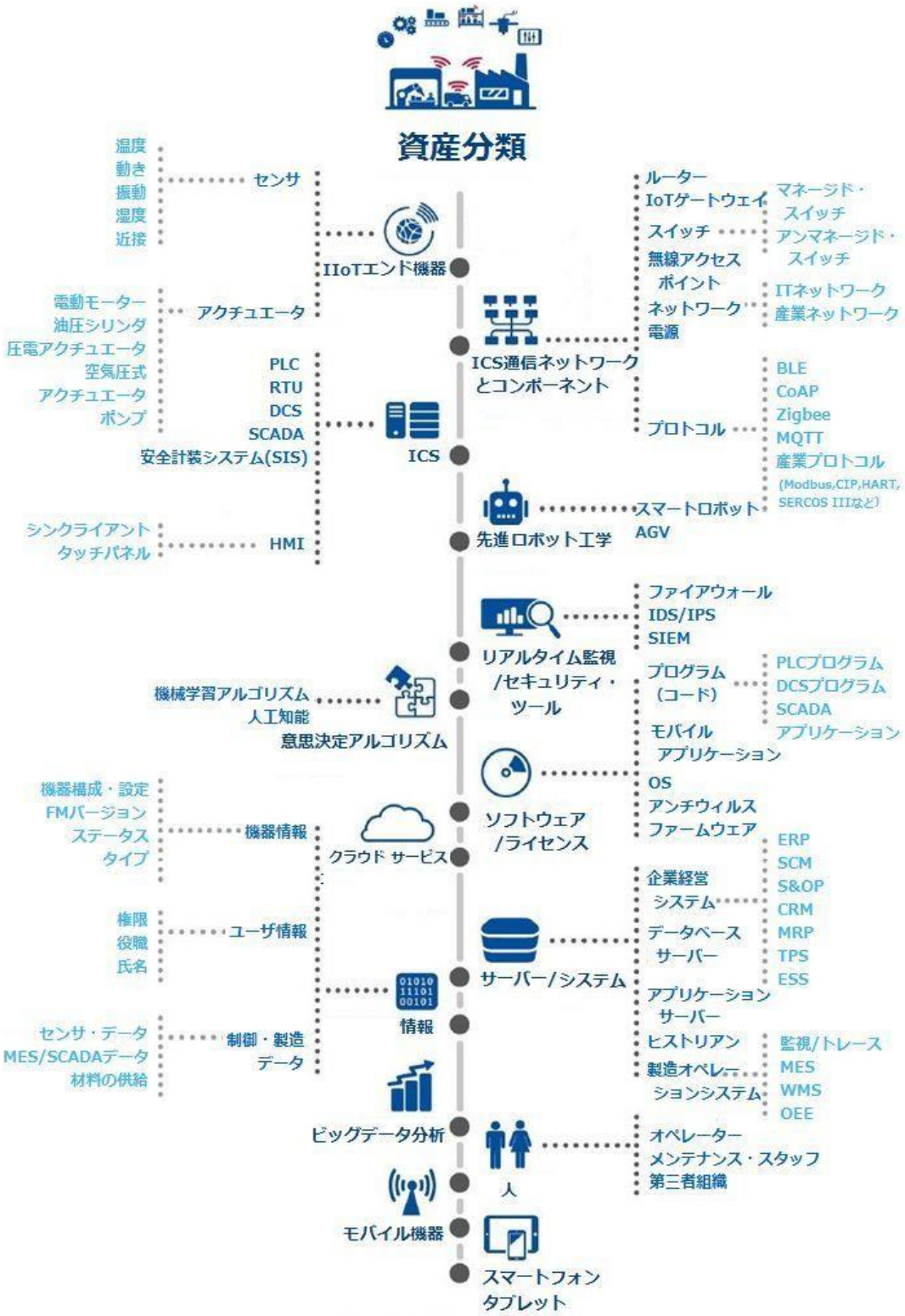

図 6：インダストリー4.0 の資産分類

表 1 資産分類

資産グループ	資産	説明
IIoT エンド機器 **レベル 1**	センサ	その環境内のイベントを検出・測定し、それらが処理される他の電子システムに情報を送信する機器。温度、動き、振動などを測定する、さまざまな目的のセンサがある。
	安全計装システム（SIS）	センサ、ロジックソルバー、および所定の条件に違反した場合にプロセスを安全な状態にすることを目的とする最終操作端（とアクチュエータ）で構成されるシステム。
	アクチュエータ	メカニズムまたはシステムを駆動または制御することによって環境と相互作用する装置。エネルギー（例えば、電気、油圧または空気圧）を運動に変換する。
ICS **レベル 2**	PLC (Programmable Logic Controller)	産業用ネットワーク内で制御を自動化するために使用される専用の産業用コンピュータ。通常、センサとアクチュエータを接続するための入出力モジュールのような追加のプラグインモジュールを備えている。
	RTU (Remote Terminal Unit)	主に、変電所や遠隔地で使用される機器。PLC と同様に、フィールドパラメータを監視し、データをセントラルステーションに送信することが目的である。
	DCS (Distributed Control System)	制御プロセスについての情報、すなわち管理ロジックを単一の中央装置に頼るのではなく、分散する制御システム。
	SCADA (Supervisory Control and Data Acquisition)	産業用資産およびプロセスからのデータ収集、それらの可視化、監視および制御管理に使用されるシステム。このようなワークステーションは通常 Windows OS 上で動作する。
	HMI (Human-Machine Interface)	オペレータが PLC、RTU、その他の電子機器を監視および制御できるコントロールパネルやダッシュボード。
ICS コミュニケーションネットワーク&コンポーネント **レベル 1－3**	ルーター	産業環境内の異なるネットワークと IoT エコシステムの間でデータパケットを転送するネットワーク機器。
	IIoT ゲートウェイ	異なるプロトコルを使用する IoT 環境から別のネットワークと接続するために使用されるネットワーク機器。ゲートウェイは、システムの相互運用性を提供するために、プロトコル変換機能、障害分離機能なども提供する。
	スイッチ	ローカルエリアネットワーク内のパケットをフィルターおよび転送するネットワーク機器。

資産グループ	資産	説明
	無線アクセスポイント	無線機器を有線ネットワークに接続する機器。Wi-Fi、または関連規格を使用している。
	ファイアウォール	所定の規則に基づいてネットワーク間またはホストとネットワーク間のネットワークトラフィックを制御するネットワークセキュリティ装置またはシステム。
	ネットワーク	ネットワークは、データリンクを介して、IoT エコシステムのさまざまなノードが、データと情報を交換することを可能にする。空間的範囲によって異なる種類のネットワークがある。例えば、(W) LAN、(W) PAN、PAN、および (W) WAN。
	プロトコル	2 つ以上の IoT 機器が特定のチャネルを介して通信する方法に関して定義した一連の規則。有線または無線の多くの通信プロトコルがある。
	電源	IoT 機器とその内部コンポーネントに電力を供給する。電源は、外部のものでも有線のものでも、あるいは装置自体に内蔵された電池でもよい。
情報 **全レベル**	運用・生産データ	センサデータ、MES および SCADA データなどの IIoT システム運用および生産データに関する情報が含まれる。
	機器情報	モデル、タイプ、構成、ファームウェアのバージョン、ステータスなどの情報が含まれる。IP アドレス、物理的な場所など。資産一覧表には、すべてのシステム機器に関する機器情報が含まれている。
	ユーザー情報	名前、役割、権限などの情報が含まれる。
意思決定アルゴリズム **レベル 2–5**	人工知能 (AI)、機械学習	これらの用語は、知的生命体が行う典型的なタスクを実行するための機械 (例えばコンピュータ、ロボットなど) の能力を表す。スマートマニュファクチャリングでは、大量のデータが産業プロセスから収集されるため、さまざまな機械学習および AI アルゴリズムを分析に利用できる。
クラウドサービス[38] **レベル 3–5**	最小限の管理とサービスプロバイダとのやり取りで、ネットワーク、サーバー、アプリケーションなどの共有リソースセットへの迅速なユニバーサルネットワークアクセスを可能とするサービス。	

[38] ENISA's study on Cloud Computing, "Towards secure convergence of Cloud and IoT": https://www.enisa.europa.eu/publications/towards-secure-convergence-of-cloud-and-iot

資産グループ	資産	説明
ビッグデータ分析 **レベル 3－5**	スマートマニュファクチャリングにおいて、この用語は、スマートセンサ、機器、ログファイル、ビデオ、およびオーディオによってリアルタイムで生成された膨大な量のさまざまなデータセットを分析するプロセスを表す。このデータは、製造工場、トランザクションアプリケーションなどを含むすべての自動化レベルで作成される。ビッグデータは、隠されたパターン、未知の相関関係、傾向ほか、情報に基づいたより慎重な決定を下すのに有用な情報を明らかにする。	
先進ロボット工学 **レベル 0**	スマートロボット、無人搬送車	エラーから学び、パフォーマンスを向上させる機能など、スマートな機能を使って複雑なタスクを実行するように設計されている高度な産業用ロボット。
リアルタイム監視／セキュリティツール **レベル 3－5**	SIEM (Security Information And Event Management)	さまざまなシステムコンポーネントからセキュリティデータを収集および集約し、それらを単一のインタフェースを介して意味のある情報の形式に変換するために利用されるアプリケーション。
	IDS/IPS 不正侵入探知システム／ 不正侵入防御システム	コンピュータシステムまたはネットワークで発生するイベントの自動監視と、起こり得るインシデントの兆候についての分析を可能にするシステム。 IPS はさらに、検出されたインシデントを阻止するためのアクションを実行する。
ソフトウェア／ライセンス **レベル 2-5**	プログラム（コード）	PLC ロジック、SCADA アプリケーション、HMI アプリケーション、産業用ロボットプログラムなどを含む、特定の目的を達成するために IIoT エコシステム内の機器用に作成されているプログラム。
	OS	コンピュータのハードウェアリソースを管理し、他のコンピュータプログラムを実行するための共通のサービスを提供するシステム。
	モバイルアプリケーション	タブレットやスマートフォンなどのモバイル機器上で実行され、リモート監視やプロセスの制御（例：モバイル SCADA クライアントアプリケーション）、機器のメンテナンス、その他のタスク（例：倉庫の在庫管理）に使用されるプログラム。
	アンチウィルス	コンピュータまたはネットワークを監視するソフトウェア。マルウェアを識別し、機器への感染を防ぎ、感染した機器からマルウェアを駆除する。
	ファームウェア	機器の読み取り専用メモリに格納されているソフトウェアを指し、機器の動作方法に関する指示を提供する。実行中は、動的に書き込んだり変更したりできない。
サーバー／システム	ヒストリアン	産業用機器からデータを収集し、それらを専用のデータベースに保存するソフトウェアシステム。

資産グループ	資産	説明
レベル 3-5	アプリケーションサーバー	アプリケーションをホストするコンピュータ。ユーザーワークステーションのアプリケーションなど。
	データベースサーバー	センサ、エージェント、および管理サーバーによって提供されるイベント情報のリポジトリとして使用されるサーバー。
	企業オペレーションシステム（ERP、CRM など）	組織のさまざまな部署からの情報を統合するシステム。（製造、流通、財務、人事など）また、組織とその顧客およびサプライヤとの間の接続も提供する。
	製造実行システム（MES など）	ネットワークコンピューティングを使用して生産管理とプロセスを自動化し、ビジネスと製造現場のギャップを埋めるシステム。 指示書のダウンロード、製造結果に関する情報のスケジューリングおよびアップロードに使用される。
モバイル機器 **レベル 3**	タブレット、スマートフォン	手で操作することができる携帯機器。モバイルアプリケーションを実行し、オペレータがさまざまなタスクを実行できるようにする。
人 **全レベル**[39]	オペレータ、保守スタッフ、第三者組織	OT システムへの物理的アクセスまたはリモートアクセスを持つすべての個人を指す資産グループ。人は製造環境において不可分の要素であるため、セキュリティの観点から重要な資産を定義する際には考慮する必要がある。OT 環境へのアクセス権を持つすべての人が、マルウェアをシステムに（意図的または意図的でなく）持ち込んだり、フィッシングの標的になったり、システムに損害を与えたり、さまざまな方法でセキュリティを侵害する可能性がある。一方、セキュリティ上の問題が発生した場合、プライバシーと物理的なセーフティが脅かされる可能性があるため、人々は特別な保護を必要とする。

図 7 は、インタビュー中に専門家から得た回答に基づいて、資産分類に記載されている主な資産の重要性を示している。これらのインタビューには、体系的な質問票が含まれ、その質問のうち一つは、重要度に応じて主要な IIoT /スマートマニュファクチャリング資産を詳細に評価するものであった。専門家は、IIoT エコシステムのサイバーセキュリティの観点から最も重要と考えられる資産をいくつでも選択できた。以下に提示された数字は、専門家が与えられた選択肢を選択した割合を示している。

[39] 全レベルとは、2.3 高次モデルで説明されているレイヤの概念に対応している。

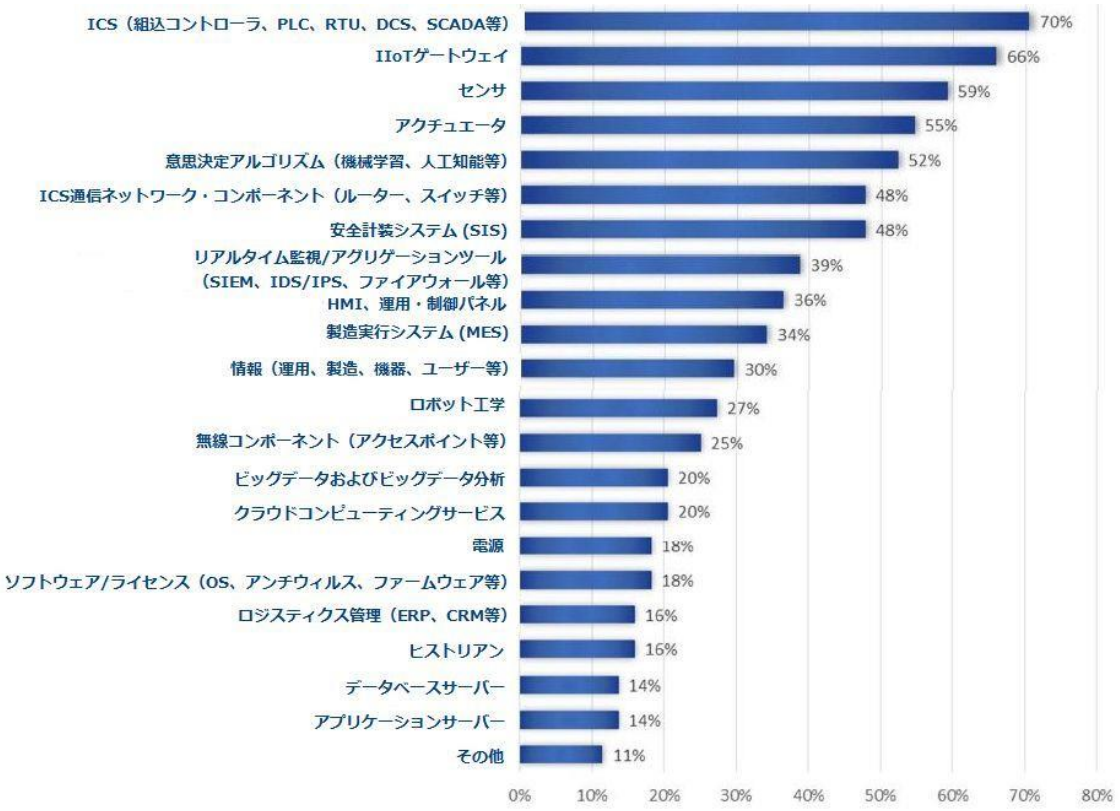

図 7：資産の重要性

この図は、利害関係者が、スマートマニュファクチャリングおよびインダストリー4.0 にとって ICS（PLC、RTU、DCS、および SCADA システムなど）が最も重要な資産であると考えていることを示している。これらのシステムは生産プロセスを制御・監視しており、その機能は生産の適切な実行と安全のために不可欠であるため、この結果は驚くに当たらない。重要性の観点から、ICS の後には IoT 機器、特に IIoT ゲートウェイ、センサおよびアクチュエータが続いている。回答者の半数以上がこれらの資産を選択し、OT 環境への新しいコネクテッドデバイスの導入はセキュリティ上の課題であり、さらなる保護が必要であることを認識している。

他の回答では、ヒューマンファクタ（例えば、オペレータ、メンテナンススタッフ、および第三者組織）が強調されていた。人はフィッシング攻撃の標的になる可能性があるため、重要な資産として識別されているほか、ヒューマンエラーはマルウェアがシステムに侵入することを可能にする。さらに、利害関係者は、資産そのものとは別に、資産管理が非常に重要であることに注目していた。企業は資産を適切に保護するために、所有する機器とソリューション、それらが配置されている場所、およびそれらがどの程度セキュアであるか、つまりどのような種類の保護メカニズム/セキュリティ対策が適用されているかを知っておく必要がある。

3. 脅威とリスク分析

3.1 脅威の分類

インダストリー4.0 環境は、数々の要因によって引き起こされるセキュリティ上の多くの課題に直面しており、さまざまなサイバーセキュリティの脅威に対処するための準備が必要である。IoT 技術に関連する脅威のほかに、インダストリー4.0 およびスマートマニュファクチャリング企業は、OT／IT 環境の一般的な脅威に加えて、さらなる脅威の影響を受ける可能性がある。この脅威の代表例は、最近の NotPetya[40]と呼ばれる大規模なランサムウェア攻撃である。この攻撃を受けた企業の 50%以上が工業企業であった[41]。

ENISA 脅威分類法[42]に従って、ENISA はインダストリー4.0 に焦点を当てた脅威の分類法を開発した。これを図 8 に示し、表 2 で詳しく説明する。

[40] 付録Dの指標となるインシデントのリスト参照

[41] Kaspersky Lab (2017) “More than 50% of organizations attacked by ExPetr (Petya) cryptolocker are industrial companies”: https://ics-cert.kaspersky.com/alerts/2017/06/29/more-than-50-percent-of-organizations-attacked-byexpetr-petya-cryptolocker-are-industrial-companies/

[42] ENISA (2016) “ENISA Threat Taxonomy A tool for structuring threat information”: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threatlandscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

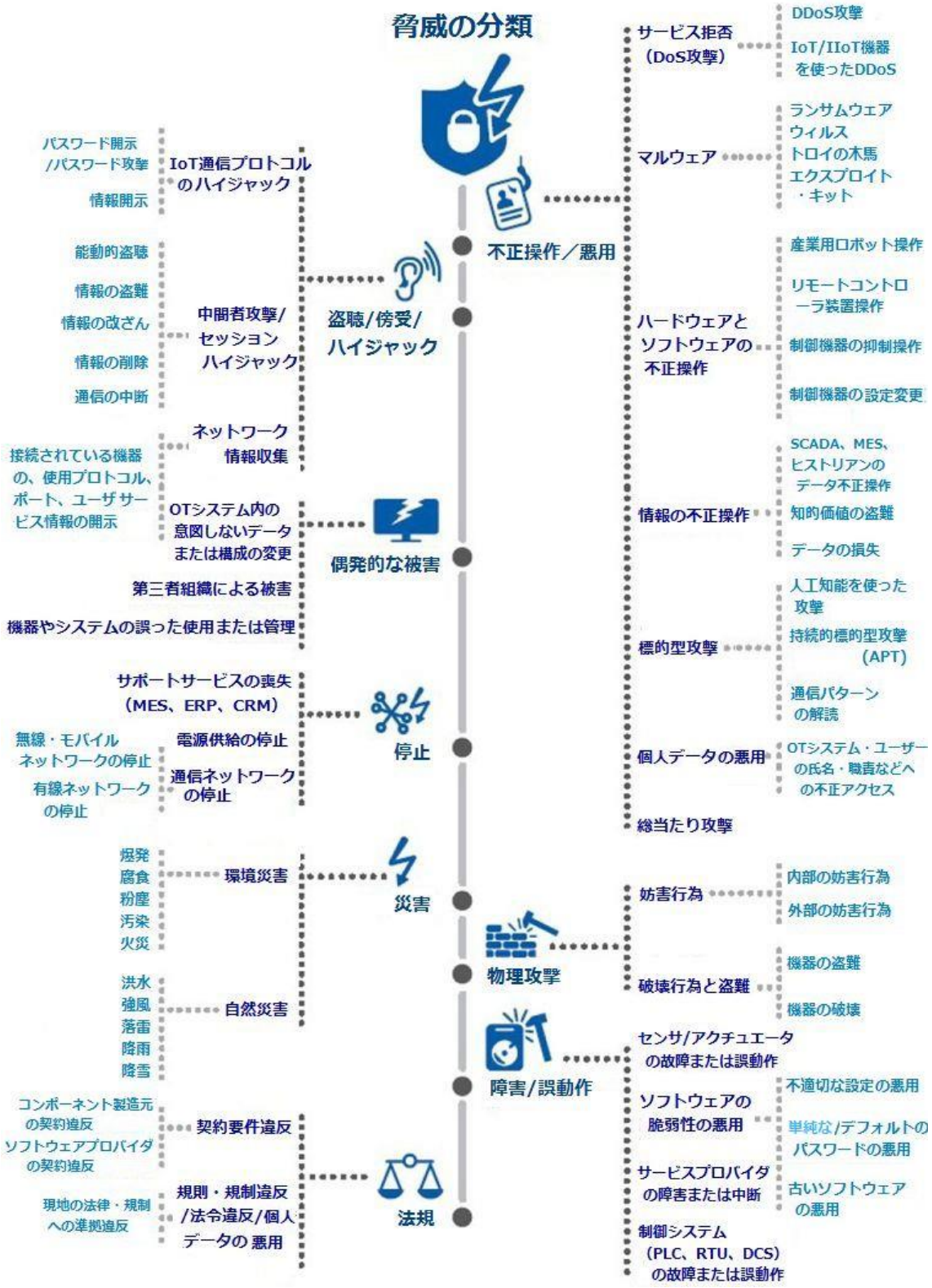

図 8：インダストリー4.0 の脅威の分類

表２：インダストリー4.0 の脅威の分類

カテゴリ	脅威	説明	影響を受ける資産
不正操作／悪用	サービス拒否 (DoS)	DoS 攻撃は双方向となることがある。 IIoT システムをターゲットにし、システムに送信される大量のリクエストによってシステムが使用不能となり生産が中断される。 また、産業環境の多数の IIoT 機器を利用し、他のシステムを攻撃するためのプラットフォームとして多数の IoT ボットネットを作成することがある。	- IIoT エンド機器 - ICS - ICS 通信ネットワークとコンポーネント - 情報 -クラウドサービス - モバイル機器 - サーバーとシステム - ソフトウェア
	マルウェア	IIoT への悪意のあるソフトウェアの侵入は、不正な行為の実行を目的とし、OT システム、運用プロセス、および関連データに損傷を与える可能性がある。 この脅威の一般的な例：ランサムウェア、ウイルス、トロイの木馬、スパイウェア	- IIoT エンド機器 - ICS - サーバーとシステム - リアルタイム監視およびセキュリティツール - 情報 - クラウドサービス - ソフトウェア
	ハードウェアとソフトウェアの不正操作	攻撃者による OT システム内の機器ソフトウェアまたはアプリケーションの不正操作の脅威。IIoT システムにおいて、攻撃者の行為には、産業用ロボットの操作、制御装置の状態を抑制するリモートコントローラ装置の操作、およびその構成の変更が含まれる。	- IIoT エンド機器 - ICS - ICS 通信ネットワークとコンポーネント - ソフトウェア - リアルタイム監視およびセキュリティツール - 高度ロボティクス - 人
	情報の不正操作	攻撃者によるデータの望ましくない、不正な改ざんの脅威。OT システム、または SCADA、MES、ヒストリアン等の生産支援系システムの改ざん、およびプロセスデータの改ざん等が考えられる。想定される被害には、誤った情報に基づく不適切な判断の実施が含まれることがある。	- IIoT エンド機器 - ICS - 情報 - クラウドサービス - ビッグデータ分析 - リアルタイム監視およびセキュリティツール - サーバーとシステム - ソフトウェアとライセンス

カテゴリ	脅威	説明	影響を受ける資産
	標的型攻撃	特定の組織（またはその組織内の特定の人物）を標的としたサイバー攻撃の脅威。この攻撃は、重要な機器への不正侵入やオペレータを欺いてテレメトリデータを改ざんするなど、さまざまな技術的手段を使用してシステムを乗っ取ることによって、組織を害することを目的としている。その他の影響には、評判の低下や企業秘密の窃取などがある。例えば、ターゲットが製造企業である場合、攻撃者は、製法や配合を盗んでそれらを競合他社に販売しようとする可能性がある。攻撃者は人工知能を使用して、選択したグループまたは個々の従業員に合わせて高度にパーソナライズされた攻撃を実行する可能性がある。この攻撃は、攻撃者によって作成された特定の Web サイトに接続する企業、または特定の脆弱性を持つ機器またはソフトウェアを使用している企業への感染を目的とした、より広範囲な攻撃とは異なる。	- IIoT エンド機器 - ICS - 情報
	個人データの悪用	機器やクラウドに保存されている個人情報や機密情報が危険にさらされる恐れがある。攻撃者の目的は、この種のデータに不正にアクセスし、それを不正に使用することである。製造企業では、OT システムユーザーの名前と職務がこれらの情報に該当する。生産データはプライバシーの対象とは見なされないが、個々の従業員のパフォーマンスに紐づけできる場合は問題となることもある。	- IIoT エンド機器 - 情報 - クラウドサービス - 人
	総当たり攻撃	想定される膨大な数の暗号鍵またはパスワードの試行によって、組織のリソース（データ、システム、機器など）へ不正アクセスされる脅威。産業用機器およびシステムに、単純な、またはデフォルトのパスワードの使用を許可しているインダストリー4.0 組織は、このような攻撃に対して特に脆弱な場合がある。	- IIoT エンド機器 - ICS - モバイル機器 - ICS 通信ネットワークとコンポーネント - リアルタイム監視およびセキュリティツール
盗聴/傍受/ハイジャック	中間者攻撃/セッションハイジャック	盗聴の可能性を意識していない関係者間で交換されたメッセージが、攻撃者によって窃取される、能動的盗聴の脅威。攻撃者が交換されたメッセージをただ聞く（例えば、企業の機微な情報や機密情報を盗むために）、または送信された情報を変更または削除することで、通信が阻害されることがある。	- 情報 - ICS 通信ネットワークとそのコンポーネント - IIoT エンド機器 - モバイル機器

カテゴリ	脅威	説明	影響を受ける資産
	IoT 通信プロトコルのハイジャック	2 つのネットワークコンポーネント間の既存の通信セッションを攻撃者が乗っ取ることの脅威。パスワードやその他の機密情報が漏洩する可能性がある。	- 情報 - ICS 通信ネットワークとそのコンポーネント - IIoT エンド機器 - 意思決定アルゴリズム
	ネットワーク情報収集	受動的にネットワークをスキャンしようとしている攻撃者に、内部ネットワーク情報（接続されている機器、使用されているプロトコル、開いているポート、使用されているサービスなど）を公開してしまう脅威。攻撃者はこの知識を使って、不正アクセスのために次に取るべき行動を計画することができる。	- 情報 - IIoT エンド機器 - ICS 通信ネットワークとコンポーネント
物理攻撃	破壊行為と盗難	OT 環境への物理的アクセスを得た妨害者、つまり不十分な物理的セキュリティ対策を回避した外部または内部の者（たとえば、何らかの理由で組織に危害を及ぼしたいと思っている不満を抱いた従業員）による、機器への物理的損傷の原因となる脅威。この脅威には盗難も含まれる。 損傷または盗難にあった装置の交換が必要になると、スペアパーツの納期による計画外のダウンタイムが発生することがある。	- IIoT エンド機器 - ICS - モバイル機器 - ICS 通信ネットワークとコンポーネント - 高度ロボティクス - 人
	妨害行為	OT 環境への物理的アクセスを得た攻撃者、つまり不十分な物理的セキュリティ対策を回避した外部または内部の者（たとえば、何らかの理由で組織に危害を及ぼしたいと思っている不満を抱いた従業員）による、機器の改ざんの脅威。攻撃者が不適切なポート設定を悪用する可能性がある。また、不正なオペレータ操作を実行することもある。	- IIoT エンド機器 - ICS - モバイル機器
偶発的な被害	OT システム内の意図しないデータまたは構成の変更	OT システム内で、十分に訓練されていない従業員による、意図しないデータまたは構成の変更によって、運用プロセスが中断される脅威。悪意はなくても、その結果を意識していない未熟な従業員は、特に必要以上の高い権限が与えられていた場合、システムに不適切な変更を加えることがある。	- IIoT エンド機器 - ICS - ICS 通信ネットワークとコンポーネント - 高度ロボティクス - 情報 - クラウドサービス - ビッグデータ分析 - ソフトウェアとライセンス - サーバーとシステム - 人

カテゴリ	脅威	説明	影響を受ける資産
	機器やシステムの誤った使用または管理	十分に訓練されていない従業員による意図しない IIoT /OT 機器の誤用によって、運用プロセスが中断されたり、機器に物理的な損傷が引き起こされたりする脅威。悪意はなくても、未熟な従業員がうっかりマニュアルやガイドライン通りに機器を使用しないことがあり、それによって機器の操作が中断されたり、物理的に損傷したりすることがある。	- IIoT エンド機器 - ICS - モバイル機器 - ICS 通信ネットワークとコンポーネント - 高度ロボティクス - 情報 - 人
	第三者組織による被害	第三者組織によって引き起こされる OT 資産に損害を与える脅威。インダストリー4.0 では、第三者組織がメンテナンスまたはソフトウェアアップデート目的で OT システムにアクセスすることがある。このアクセスが十分な方法で制御されていないと、第三者組織のセキュリティ侵害がその組織のサービスを受ける企業に影響を与えることがある。	- IIoT エンド機器 - ICS - ICS 通信ネットワークとコンポーネント - 高度ロボティクス - クラウドサービス - 情報
障害/誤動作	センサ/アクチュエータの故障または誤動作	IIoT エンド機器の故障または誤動作の脅威。これは特に、適切なメンテナンスや機器のマニュアルと指示の順守が攻撃の際に保証されていない場合時折起こることがある。	- IIoT エンド機器 - ICS
	制御システム（PLC、RTU、DCS）の故障または誤動作	制御システムの故障または誤動作の脅威。これは特に、適切なメンテナンスや機器のマニュアルと指示の順守が攻撃の際に損なわれた場合時折起こることがある。	- IIoT エンド機器 - ICS - ICS 通信ネットワークとコンポーネント
	ソフトウェアの脆弱性の悪用	攻撃者が IIoT エンド機器のファームウェアまたはソフトウェアの脆弱性を利用する脅威。IIoT エンド機器は、アップデートの欠如、弱い、またはデフォルトのパスワードの使用、および不適切な設定のために、しばしば脆弱である。	- IIoT エンド機器 - 情報 - ソフトウェアとライセンス
	サービスプロバイダの障害または中断	第三者組織のサービスに依存するプロセスが、サービスの障害または機能不全の際に中断する脅威。	- IIoT エンド機器 - ICS - ICS 通信ネットワークとコンポーネント - 情報 - クラウドサービス - ビッグデータ分析
停止	通信ネットワークの停止	ケーブル、無線またはモバイルネットワークに関する問題による通信リンクの利用不能の脅威。	- ICS 通信ネットワークとコンポーネント

カテゴリ	脅威	説明	影響を受ける資産
	電源供給の停止	電源の故障または誤動作の脅威。重要なシステムに非常用電源が存在しない場合、電源が中断されると、製造プロセスが突然停止して深刻な被害が生じることがある。	- IIoT エンド機器 - ICS - ICS 通信ネットワークとコンポーネント - 高度ロボティクス
	サポートサービスの喪失（MES、ERP、CRM）	生産または物流をサポートするシステム、すなわち MES、ERP および CRM の故障または誤動作の脅威。	- サーバーとシステム
法規	規則・規制違反/法令違反/個人データの悪用	個人データの処理に関連する法的問題や金銭上の損失の脅威。（例：IIoT エンド機器の使用に関する現地の法律または規制を遵守しない。）EU 内での事業では、これらの要件は EU 一般データ保護規則（GDPR）によって企業に課されている。	- IIoT エンド機器 - 情報
	契約要件違反	必要なセキュリティ対策を確実に怠った場合に、コンポーネント製造元およびソフトウェアプロバイダとの契約上の要件に違反するという脅威。	- IIoT エンド機器 - クラウドサービス - 情報 - ICS - ソフトウェアとライセンス
災害	自然災害	OT 環境のコンポーネントに物理的損傷を引き起こす可能性がある、洪水、落雷、強風、雨、降雪などの自然災害の脅威。	- IIoT エンド機器 - ICS - ICS 通信ネットワークとコンポーネント - 高度ロボティクス - 人
	環境災害	OT 環境のコンポーネントに物理的損傷を引き起こす可能性がある、事故、および火災、汚染、粉塵、腐食、爆発などの脅威	

3.2 インダストリー4.0/スマートマニュファクチャリングのサイバーセキュリティ攻撃シナリオの例

専門家は、インタビューの中で、これらの脅威に基づく攻撃シナリオを評価し、スマートマニュファクチャリング組織にとって重要な攻撃シナリオを識別した。それぞれの攻撃シナリオに対して、専門家は彼らが認識した重要度レベル（重要ではない、重要度が低い、中程度、高い、致命的）を選択した。表 3「IIoT 攻撃シナリオ」は、専門家の回答を分析し、まとめたものである。

表 3： IIoT 攻撃シナリオ

攻撃シナリオ		重要度
1.	コントローラ（例：DCS、PLC）とアクチュエータ間の接続に対する攻撃。	高
2.	センサに対する攻撃（測定値/状態の変更、それらの再設定、等）	高
3.	アクチュエータに対する攻撃（状態を抑制し、構成を変更する）	高 – 致命的
4.	ネットワーク経由で送信された情報への攻撃	高 – 致命的
5.	IIoT ゲートウェイへの攻撃	高 – 致命的
6.	リモコン装置（例えば操作パネル、スマートフォン）の不正操作	高
7.	安全計装システム（SIS）への攻撃	致命的
8.	マルウェアによる攻撃	高
9.	IoT ボットネットを使った分散型サービス妨害（DDos）攻撃	中 – 高
10.	踏み台攻撃（クラウドに対する攻撃等）	中
11.	ヒューマンエラーによる攻撃およびソーシャルエンジニアリング攻撃	高
12.	人工知能技術を使用した高度にパーソナライズされた攻撃	中 – 高

それぞれの攻撃シナリオについて、脅威の分類法（3.1 脅威の分類）に基づいた潜在的な影響と関連する脅威の詳細な説明を以下に示す。

1. コントローラ（例：DCS、PLC）とアクチュエータ間の接続に対する攻撃。

攻撃者が監視されていない回線を使用して、侵入したシステムからコードを挿入して実行したり、データを（操作して）送信したりする攻撃。

- 影響：不正操作または制御の喪失、バッチ/製品およびインフラの損傷。
- 関連する脅威：内外の妨害行為、ハードウェアとソフトウェアの不正操作、制御装置の設定の不正操作。

2. センサに対する攻撃（測定値/状態の変更、それらの再設定、等）

測定データがエンド機器で操作される攻撃。例えば、攻撃者はセンサに侵入し、測定値の調整など、ファームウェアや設定を変更する。

- 影響：不正操作されたデータに基づいてオペレータが誤った判断をする。不正確な測定に基づいてプロセスを実施する。規制の対象となる測定値が、正しく評価されない。
- 関連する脅威：情報の変更、妨害行為、ハードウェアおよびソフトウェアの不正操作、送信されたセンサデータの不正操作。

3. アクチュエータに対する攻撃（状態を抑制し、構成を変更する）

誤った設定、しきい値、またはデータを使用させるため、アクチュエータの設定/パラメータが不正操作される攻撃。動作設定を妨害することで通常動作に影響を与える。

- 影響：影響を受けるアクチュエータによって異なる。製造工程に影響する可能性がある。
- 関連する脅威：ハードウェアおよびソフトウェアの不正操作、センサ/アクチュエータの故障または誤動作、制御システム（PLC、RTU、DCS）の故障または誤動作。

4. ネットワーク経由で送信された情報への攻撃

ネットワーク層（OSI 参照モデルのレイヤ 2/3/4）でデータを不正操作することを目的とした攻撃。OSI 参照モデルのレイヤ 5/6/7、すなわち制御装置および制御システム（DCS、SCADA）のレベルでは、データ値は正しいように思われる。不正操作は、ネットワーク層のトラフィック監視によって検出できる。

- 影響：不正操作されるデータによって異なる。製造工程に影響を与えたり、損傷を与えたりする可能性がある。（例：炉を、爆発を引き起こす可能性がある温度に操作する。）
- 関連する脅威：APT、中間者攻撃、妨害行為、マルウェア。

5. IIoT ゲートウェイへの攻撃

攻撃者が IIoT ゲートウェイに不正アクセスすると、環境全体に侵入される可能性がある。脆弱なプロトコル、またはデフォルトのパスワードまたはプロトコルが使用されている場合、この攻撃の成功の可能性はかなり高い。この種の攻撃は、さまざまな段階/フェーズで構成されており、通常は見つからないように行われる。この種の攻撃を、機器のライフサイクル全体にわたって考慮に入れる必要がある。

- 影響：攻撃者は、機器、システム、およびネットワーク機器へのアクセスを含む、ネットワークおよびデータへのアクセスを取得する。これは、システム全体とそのコンポーネントを悪用する最初の段階となる。
- 関連する脅威：パスワード攻撃、エクスプロイトキット、個人データの悪用、マルウェア、および DDoS 攻撃。

6. リモコン装置の不正操作（例：操作パネル、スマートフォンなど）

攻撃者は、制御システムから遠く離れた機器（分散環境）に侵入することができる。多くの場合、そのような機器はローカル制御を目的としており、継続的に監視されていない。このような機器の攻撃者による掌握は、ネットワーク全体に侵入されて機器が損傷する可能性があり、状況を把握するのに時間がかかるため、被害が拡大する可能性があり、大きな脅威となる。

- 影響：システムへのアクセス、および制御層へのフルアクセス、エンジニアリングツールおよび変更の取得。IoT 環境に危険な変化を引き起こす可能性がある。
- 関連する脅威：パスワード攻撃、ソフトウェアの脆弱性の悪用、セッションの乗っ取り、情報の漏えい。

7. 安全計装システム（SIS）への攻撃

最も危険な攻撃の 1 つは、環境、人命、企業を大きな経済的損失から防ぐシステムに対する攻撃である。制御システムの乗っ取り、またはシステムの不正操作は、設備の破壊を招く可能性がある。また、危険性が最も低い場合でも、プロセスの計画外の中断を招く可能性がある。そのよ

うな攻撃の例は最近の Triton による攻撃[43]である。

- 影響：SIS への侵入、SIS の不正操作または中断は、多くの人々に影響を及ぼし、環境問題を引き起こし、さらには他のシステムにまで拡大し、それらの運用に影響を与え、停止させることさえある。
- 関連する脅威：マルウェア、破壊行為、リモートコントローラ機器の不正操作、APT。

8. マルウェアによる攻撃

ネットワーク上に広がる悪質なコードによって実行される攻撃。感染機器のデータへのアクセスを可能にする。マルウェアをベースとしているこれらの攻撃は、脆弱な機器をアップデートする、またはパッチを適用することで回避できる。これは、IIoT エコシステム外でも可能である。IIoT に関する問題は、IIoT 機器の中には、アップデートやパッチを適用する機能を備えていないものがあり、アップデート、またはパッチを適用するのが難しいことである。る。

- 影響：IIoT には、マルウェアの標的となる可能性のあるものが多数ある。攻撃者が冬の真只中にスマートサーモスタットを制御して電源が入らないようにしたり、電力グリッドや病院システムを制御して人々の安全を危険にさらす可能性がある。
- 関連する脅威：エクスプロイトキット、マルウェア、DDoS、パスワード攻撃。

9. IoT ボットネットを使った分散型サービス妨害（DDos）攻撃

IIoT 機器そのものをターゲットにするのではなく、代わりにそれらを使用して、その他の機器を攻撃する攻撃。 まず、マルウェアが脆弱な IoT 機器を自動的に検出し感染させ、それらをボットネットに組み込み、DDoS 攻撃を仕掛けるために標的のサーバーを悪意のあるトラフィックであふれさせる。

- 影響：標的となった機器またはサービスは悪意のあるトラフィックであふれ、停止する。
- 関連する脅威：エクスプロイトキット、DDoS、およびマルウェア。

10. 踏み台攻撃（クラウドに対する攻撃等）

匿名の攻撃を仕掛ける一般的な攻撃。匿名の攻撃は、攻撃者自身のコンピュータからではなく、彼らが以前侵入した別のホストから攻撃を開始するので、侵入者によって彼らの正体を隠すためにしばしば使用される。

- 影響：攻撃者が踏み台攻撃を行う場合、ホストの一群に侵入し、攻撃コマンドを中継するための踏み台としてそれらを使用する。
- 関連する脅威：APT、DDoS、マルウェア。

11. ヒューマンエラーベースの攻撃およびソーシャルエンジニアリング攻撃

この種の攻撃は通常、他の種類の攻撃を仕掛ける入口で、目的を達成するための手段であり、シ

[43] FireEye (2017) “Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure”: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attackframework-triton.html

ステムへの不正な特権アクセスを取得するために使用される。これにより、他の悪意のあるコンテンツやバックドアがインストールされたり、機器に物理的にアクセスされたりする可能性がある。ターゲットが単一のシステム/機器であるか、ネットワーク全体または施設全体であるかにかかわらず、攻撃の一部として行われる。技術的な特性がないため、これらの攻撃を検出することは困難である。また、従業員に対する非常に優れた意識向上トレーニングに基づいて、環境内の疑わしい行動を検出する方がはるかに容易である。

- 影響：この攻撃が成功すると、ソーシャルエンジニアリング攻撃によってシステムや施設への侵入口が作成され、場合によっては特権が昇格される。ヒューマンエラーベースの攻撃は、システムを破壊したり、不安定にさせたりする可能性がある。この攻撃は一般的に大規模で高度な攻撃の一部として行われ、単純なる情報窃取目的の攻撃の一端の場合も、高度な APT 攻撃の一端の場合もある。
- 関連する脅威：機器やシステムの誤った使用または管理、OT システム内の意図しないデータの変更または設定、機器の物理的損傷、知的財産の盗難。

12. 人工知能技術を使用した高度にパーソナライズされた攻撃

一致するパターンを特定するための攻撃や、IIoT システムへの直接攻撃。主な脅威は、潜在的に重要でないことが多い情報の使用である。人工知能技術を駆使することによって、攻撃者はインターネットから取得した特定のデータと明示的なデータを組み合わせてセキュリティホールを見つけることができる。

- 影響：これらの攻撃は非常にパーソナライズされたものであり、特定の人々（システム管理者など）を標的とする可能性がある。IIoT エコシステムを経由したコミュニケーションの広がりも標的となる可能性がある。このような攻撃は、最初の攻撃や、その後の攻撃段階でもあり得る。
- 関連する脅威：データの損失、ネットワークの偵察。

4.セキュリティ対策とグッドプラクティス

4.1 セキュリティ対策の分類

スマートマニュファクチャリングにおける IoT のセキュリティ対策の開発は、この調査の焦点の 1 つであった。その背後にある考えは、適用すれば潜在的なサイバー攻撃を防止または適切に対処し、IIoT 環境の全体的なセキュリティとセーフティを確保するのに役立つ、IIoT オペレータ、製造業者およびユーザー向けのガイドラインと提言を提供することであった。この調査の一環として、IoT のセキュリティ対策に関連するすべての側面を識別するために、かなりの努力が費やされた。

まず、広範囲に及ぶ机上リサーチを実施した。関連する情報源（付録 C に記載）の徹底的な分析により、IIoT セキュリティで頻繁に言及されているトピックを特定できた。その後、これらのトピックをまとめてセキュリティ対策分野の最初のリストを作成した。

利害関係者とのインタビューに基づいて最終的な一連の領域が明確化され、調整された結果、インダストリー4.0 の全体像を包括的に示し、保護が必要な領域を示す 20 の領域のリストが出来た。

論理的に領域を整理するために、3 つの主要グループに分類した。

- ポリシー
- 組織的対策
- 技術的対策

これらのグループは上位レベルの区分を提供し、ENISA の「IoT のベースラインセキュリティに関する提言」の調査の分類と一致している。

図 9：グッドプラクティスの概要

4.2 ポリシー

このセキュリティ対策の最初のグループは、特に IIoT ソリューションが関係する場合、適切なレベルのサイバーセキュリティ確保のために組織内で確立する必要があるポリシーと手順について言及している。さらに、プライバシーの問題は、自社のソリューションがプライバシー規制に違反しないようにする必要がある製造元の観点、およびプライバシー関連のリスクに敏感に対処し、ユーザーの個人情報をさらさずに IIoT 機器を使用する方法を知っておく必要がある運用者の観点で取り上げている。

4.2.1 セキュリティ・バイ・デザイン

製品開発の最初から適用されるべきセキュリティ対策。

PS-01：スマートマニュファクチャリング・システム開発ライフサイクル（SDLC）のすべての段階で、機器とインフラの観点から「セキュリティ・バイ・デザイン」のアプローチを採用し、エンドツーエンドのプロセスとしてではなく、サイクルとして IoT サイバーセキュリティを扱う。

PS-02：ネットワークレベルだけでなく、エンドポイントの組み込み機能でサイバーセキュリティに対処する。

PS-03：セキュリティとセーフティ評価の結果、適切であると判断された場合、非常に限られた処理能力しか持たない最も基本的なコネクテッドデバイス（アクチュエータ、コンバータなど）にも識別および認証機能を備え、IAM ソリューションとの互換性を確保する。

PS-04： 機器の設計プロセスのごく初期段階からサイバーセキュリティの専門家を巻き込んでリスクと脅威の分析を行い、どのセキュリティ機能が必要になるか明らかにする。
PS-05： 各設計文書に、産業環境におけるすべての情報および制御システムのセキュリティを扱う章を含める。

4.2.2 プライバシー・バイ・デザイン

プライバシーと個人データの保護に関連するセキュリティ対策。この対策は、製品開発の最初の段階から適用する必要がある。

PS-06： EU 一般データ保護規制（GDPR）[44]などの適用される国内および国際的な規制に基づいてプライバシー関連の問題に対処する。
PS-07： 機微なデータを収集したり不必要に提供したりせずに、設計段階で機器によって処理されるデータの範囲および処理の目的を定義する。
PS-08： データストレージの物理的な場所を確立し、どの組織間でデータを転送するかを定義して、収集された個人データへのアクセスを許可された個人のみに制限する。
PS-09： 機器によって処理されるデータについて、プライバシー影響評価（PIA）を実施する。
PS-10： 個人を識別するために使用できるデータを他の情報から分離し、そのセキュリティを確保する。（例えば、IIoT 環境内で転送される個人データの暗号化を通じて）

4.2.3 資産管理

資産の発見、管理、監視および保守に関するセキュリティ対策。

PS-11： 組織および産業環境に固有の資産を動的に発見、識別、および列挙できる資産管理サポートツールを利用する。
PS-12： 企業が一貫した最新の資産一覧表を持っていることを確認する。
PS-13： レガシーなシステムがある複雑な産業環境では、可能な限りパッシブ監視装置を使用するか、またはアクティブ監視ツールを検討する場合は実装前にテストフェーズを実施する。
PS-14： 製造工場内のコンピュータ化された環境全体に集中管理型資産一覧を使用する。
PS-15： 専用の管理ネットワークを介したインフラとセキュリティ機器のセキュアな管理を検討する。
PS-16： 確立、承認、伝達された変更管理プロセスに従ってのみ、新しい機器をシステムに追加する。
PS-17： 容認されたビジネス要件がない場合は、USB ポートを無効にしてリムーバブルデバイスの使用を避ける。

[44] General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

4.2.4 リスクと脅威の管理

インダストリー4.0 環境に適応したリスクおよび脅威管理のプロセスへの推奨アプローチに関するセキュリティ対策。

PS-18： 新しいパラメータ、脅威、および攻撃のシナリオを考慮した、インダストリー4.0 およびスマートマニュファクチャリングに特化したリスク管理へのアプローチを採用する。

PS-19： 製造環境の重要なインフラについては、企業、セーフティ、および環境面でのリスク管理と完全に一致する、リスク管理確立する。それらのリスク管理領域に対する脅威、脆弱性、および保護対策を評価し、特徴付ける。

PS-20： 企業の個々のニーズとセキュリティ要件に従ってリスクと脅威の管理プロセスを確立する。

PS-21： 少なくとも年 1 回、サイバーセキュリティの側面を含めたリスク分析を実行する。また、変更管理、インシデント処理、脆弱性管理などの他のプロセスと統合する。リスクアセスメントは、セキュリティポリシーとプロセスの有効性の技術的および手続き的テストを網羅する必要がある。

PS-22： さまざまな情報源を使い、信頼できる業界パートナー、ISAC、および CERT と情報を共有し、脅威インテリジェンスプロセスを企業の脅威管理アプローチに組み込むことを検討する。

PS-23： 組織の観点から、選択した脅威を監視し、リスク分析を実行してシステムへの影響を判断する。

PS-24： リスク管理プロセスに関しては、トップダウン／ボトムアップの 2 つの異なるアプローチを同時に採用する。トップダウンで組織全体の観点からのサイバーセキュリティに対処し、ボトムアップ[45]で企業の状況に関するきめ細かい詳細な見解を提供する。

4.3 組織的対策

通常、組織の原則とガバナンスは、企業のセキュリティの観点から重要で不可欠な要素である。以下のセキュリティ対策では、スマートマニュファクチャリングおよび他のインダストリー4.0 企業の運営方法、確立して従うべき組織のルールと責任、およびサイバーセキュリティインシデントを効果的に処理し、脆弱性を管理し、ライフサイクルを通して IIoT ソリューションのセキュリティを確保するための、従業員および第三者業者に対するアプローチについて説明する。

4.3.1 エンドポイントライフサイクル

調達プロセス、サプライチェーン、製品の引き渡し、利用、使用終了など、製品（エンド機器およびインフラを含む）ライフサイクルのさまざまな段階におけるセキュリティに関連するセキュリティ対策。

[45] トップダウンとボトムアップのアプローチについては、付録 B を参照。

OP-01：エンドポイントライフサイクルのあらゆる段階におけるソフトウェアとハードウェアのセキュリティに焦点を当てる。
OP-02：サプライチェーン全体を通してセキュリティについて検討すべき事項を考慮に入れる。
OP-03：調達プロセス全体において、特定の機器/ソリューションに合わせて調整されたセキュリティ対策と要件を定義し、セキュリティ面を考慮する。
OP-04：さまざまな検証活動や製品ライフサイクルの段階で、技術仕様に対するサイバーセキュリティの受け入れテストを実施する。
OP-05：プロジェクト実施プロセスの引継ぎ段階で、すべてのサイバーセキュリティ文書、プロセスおよび手順を適切に整備し引き渡す。

4.3.2 セキュリティアーキテクチャ

アーキテクチャベースのアプローチとセキュリティアーキテクチャの確立に関するセキュリティ対策。

OP-06：コンピュータ化されたエコシステムでセキュリティを確保するために、包括的なアーキテクチャベースのアプローチを採用し、ビジネス要件に基づいてリスクに合わせたセキュリティアーキテクチャを開発する。
OP-07：セキュリティアーキテクチャを定義しながら、組織から物理的な実装の問題まで、関連するすべてのセキュリティの側面を含むようにする。
OP-08：セキュリティアーキテクチャ内で、セキュリティに対する明確な役割と責任を割り当てる。 OT システムとセキュリティプロセスの両方の役割を明確に定義し伝達する。
OP-09：確立されたセキュリティアーキテクチャにコンプライアンス管理を統合し、すべての製品がその中で定義された要件を満たすことを確実にする。

4.3.3 インシデント処理

インダストリー4.0 環境で発生する可能性のあるインシデントの検出と対応に関するセキュリティ対策。

OP-10：企業の事業分野と運用範囲に基づいて、組織にとって重要なサイバーインシデントを定義し、適用可能な基準に従ってそれらを分類する。
OP-11：サイバーセキュリティインシデントをサポートするための OT および IT サイバーセキュリティスペシャリストからなるサイバーセキュリティオペレーションセンター（SOC）の設立を検討し、適切な役割と責任を持つ特定のサポートラインに分割する。
OP-12：影響を受ける資産の識別、脆弱性の識別と分類、エスカレーションと通知から成る、インシデント処理のためのプロセスを確立する。
OP-13：セキュリティに関連した異常なイベントをすべて迅速に検出して調査する。

4.3.4 脆弱性管理

脆弱性管理プロセス、関連する活動、および脆弱性の開示に関するセキュリティ対策。

OP-14：リスク分析の結果を基に、自動および手動ツールの利用を含む、組織内の包括的な脆弱性管理プロセスを定義する。
OP-15：脆弱性を排除しながら、資産とシステムの重要性を考慮して最も重要なものから始める。
OP-16：脆弱性を開示するための包括的で明確なプロセスを確立する。
OP-17：新しい IIoT ソリューションの侵入テストを、管理された環境、または試運転段階の前または最中に、また定期的に、およびシステムの重要な更新後に実施する。
OP-18：OT 部門と IT 部門の緊密なコラボレーションを確立する。システムビジネスのオーナー、意思決定機関、およびその他の利害関係者とのコラボレーションも効果的になるようにする。

4.3.5 トレーニングと意識向上

セキュリティトレーニングおよび IIoT 機器とシステムを扱う従業員の意識向上に関する推奨アプローチに関するセキュリティ対策。

OP-19：セキュリティトレーニングと従業員の意識向上のための総合的なアプローチを採用し、組織のあらゆるレベルの従業員を対象とし、新たなインダストリー4.0 関連の脅威に対処する。
OP-20：新規雇用者全員に、実際に仕事を始める前にサイバーセキュリティトレーニングを実施する。
OP-21：セキュリティトレーニングが継続的、定期的、そして頻繁に更新されるようにする。
OP-22：IIoT 機器とエコシステムを保護するために展開されている技術を説明するために、機器の安全な使用法について IIoT ユーザーにトレーニングを実施する。
OP-23：サプライチェーンを含むレベルで他社とのコミュニケーションを検討し、組織での議論、協力、および情報共有を可能にするために形成された国際的なセキュリティコミュニティに参加してセキュリティ意識を向上させる。

4.3.6 第三者組織の管理

第三者組織の管理および第三者組織のアクセス制御に関連するセキュリティ対策。

OP-24：制御層または生産層への第三者組織は厳密に制御し、必要な時のみ、一時的に、特定の目的のため、かつ最小権限の原則に基づきアクセスを許可する、
OP-25：制御層または生産層のシステムにベンダーからは直接接続しない。選択された必要な機能とネットワークの一部だけにアクセスを許可する。

OP-26：自社のプロセスのセキュリティと自社製品向けのコミットメントに関する情報をサプライヤに要求し、ベンダーとサービスプロバイダのための専用のセキュリティ要件を開発する。
OP-27：適切な合意書および契約書の中で、セキュリティを含む、第三者組織とのパートナーシップのすべての側面を明確に定義する。

4.4 技術的対策

ポリシーや組織的な対策の実装とは別に、IIoT ソリューションの適切な技術的機能とそれらが展開されている環境を通じてセキュリティに対処する必要がある。下記の技術的セキュリティ対策は、インダストリー4.0 およびスマートマニュファクチャリング企業がセキュリティレベルを向上させることを可能にするパズルの最後のピースである。このセクションでは、どのような技術的セキュリティ対策を機器に実装する必要があるか、および対応するソリューションとそれらの実装方法について概説する。また、スマートマニュファクチャリング企業がインフラのレジリエンスと製造プロセスの継続性を確保するための推奨方法についても説明する。

4.4.1 信頼性と完全性の管理

データと機器の完全性と信頼性を保証するのに役立つセキュリティ対策。

TM-01：実行を開始する前にソフトウェアの完全性を検証し、それが信頼できるソースから来ていること（ベンダーによって署名されたものであること）、そしてセキュアな方法で入手されていることを確認する。
TM-02：適切な方法を利用して OT ネットワーク内のすべての IIoT 機器を認証する。（例：デジタル証明書/ PKI）
TM-03：IIoT 機器間のデータ交換チャネルをホワイトリストの形式で定義し、可能な限り安全なチャネルのみを選択する。
TM-04：アプリケーションホワイトリストを実装し、少なくとも年 1 回、システムに変更があった場合にはリストを見直す。
TM-05：実装する機器の処理能力に合わせて調整された適切な暗号化メカニズムとキーストレージを利用して、生産データの完全性を確保する。
TM-06：保管中および転送中の生産データを監視して、潜在的な許可されていないデータ変更を識別する。

4.4.2 クラウドのセキュリティ

クラウドサービスのさまざまなセキュリティの側面に関するセキュリティ対策。

TM-07：クラウドの種類の選択に関する決定は、クラウドセキュリティプロバイダの国や接続拠点（points of presence）に適用される法律や規制や存在感も考慮し、ビジネスと

プライバシーへの影響評価に基づく。

TM-08：可能であれば、クラウドセキュリティプロバイダとの合意にセキュリティと可用性の側面を含める。

TM-09：クラウドベースのアプリケーションと集中型システムでは、単一障害点を避ける。

TM-10：パブリッククラウドの利用を検討している場合は、重要なシステムとアプリケーションをプライベートまたは少なくともハイブリッド展開モデル内に配置し、実装前にリスク分析を行う。

TM-11：クラウド攻撃に関連するリスクを軽減するために、ゼロ知識セキュリティアプローチを採用し、クラウド内および転送中のすべてのデータを保護する。

4.4.3 事業継続および復旧

セキュリティインシデント発生時にレジリエンスと業務の継続性を確保するための企業の計画の策定、テストおよびレビューに関するセキュリティ対策。

TM-12：事業継続計画（BCP）と災害復旧計画（DRP）を作成することにより、インダストリー4.0 システムのレジリエンスの確保に焦点を当てる。計画を定期的にテストし、テストおよび実際のセキュリティインシデントから学んだ教訓を踏まえてそれらを更新する。

TM-13：重要なビジネスプロセスおよび技術プロセスを定義し、それらがビジネスの継続性にどの程度影響を与えるかを判断する。

TM-14：脅威とリスクの評価を実施し、評価の結果に合わせて通常の（明確に定義された）運用状態に戻す方法に関する手順書を作成する。

TM-15：リスク分析の前に緊急時対応計画を検討する。緊急時対応計画を定義し、管理された演習を実行してそれらをテストする。計画を定期的に見直し、適切に更新する。

TM-16：事業継続および回復計画において、第三者組織に関する側面を含める。

TM-17：目標復旧時間（RTO）、目標復旧時点（RPO）、最大許容停止時間（MTO）、最小事業継続目標（MBCO）など、企業の事業継続に関する重要なパラメータを定義する。

4.4.4 機械間セキュリティ

機械間通信セキュリティにおけるキーストレージ、暗号化、入力検証、および保護に関するセキュリティ対策。

TM-18：インフラ機器内のサーバーHSM に（公開鍵以外の）サービス層で使用する長期鍵を保管する。

TM-19：相互認証、完全性、および機密性を提供するために、通信機器間で実績のある安全な暗号化アルゴリズムでセキュリティアソシエーションを確立する。

TM-20：メッセージの全部または一部が、以前のメッセージの不正な再送信であるかどうかを

検出する機能を含む通信プロトコルを使用する。
TM-21：クロスサイトスクリプティングおよびコマンドインジェクションから保護するために、ポジティブ/ホワイトリスト型の入力検証を使用する。

4.4.5 データ保護

組織のさまざまなレベルにおける守秘データの保護およびデータへのアクセスの管理に関するセキュリティ対策。

TM-22：保管中、転送中、使用中のデータ（揮発性メモリと不揮発性メモリの両方）を保護する。
TM-23：リスク分析に基づいて OT システムに関連するデータを分類し、その重要性を評価し、適切なレベルのセキュリティを保証するために必要なセキュリティ対策を定義する。
TM-24：最小権限の原則と“知る必要のある人にだけ知らせる”という原則を念頭に置いて、特定のカテゴリのデータへのアクセスを第三者組織に許可し、このアクセスを文書化する。
TM-25：機密性の高いデータについては、認証されたユーザーのみが情報を読み取ることができるように、暗号化と鍵管理を実装する。データ損失防止ソリューションを使用する
TM-26：社内で処理された直接的または間接的な個人データを匿名化して保護する。 職務ベースのアクセス制御と暗号化により、関連するすべての法的要件を考慮する。

4.4.6 ソフトウェア/ファームウェアのアップデート

パッチの検証、テスト、および実行に関するセキュリティ対策

TM-27：エンドポイントのソフトウェア/ファームウェアの信頼性と完全性を検証し、アップデートを厳重に管理する。
TM-28：アップデートの作成元を検証し、リスク分析に基づいている場合にのみ自動更新手順を実行する。
TM-29：IIoT 機器用のパッチの展開は、悪影響がないことを証明した後にのみ実行し、パッチを本番環境に実装する前にテスト環境でテストする。
TM-30：パッチがテストされ、機器に悪影響を及ぼさないことを保証し証明することができる場合、または該当する条項に従って第三者組織がアップデート責任を負う場合にのみ、第三者組織にパッチの適用を許可する。TM-31：更新できない制御システムの場合は、代替措置を適用する。

4.4.7 アクセス制御

リモートアクセス、認証、特権、アカウント、および物理アクセスの制御に関するセキュリティ

対策。

TM-32：リモートアクセスを通常のアクセスと分離する、すなわちリモート通信を制御するための一連の規則を策定する。
TM-33：IIoT 機器およびシステムの最低限の認証セキュリティを確保し、承認によってシステムの特定のセグメントへのアクセスのみが許可されるようにする。
TM-34：IIoT ソリューションに多要素認証機能を実装/使用する。
TM-35：試運転中/初回使用時にデフォルトのパスワードとユーザー名を変更する。強力なパスワードを使用し、定義された期間の後に新しいパスワードの設定を要求する。
TM-36：最小権限の原則を適用し、複数のユーザーがいる環境では、役割が適切に分離され、適切な人によって承認されるようにする。
TM-37：可能な限り、すべてのユーザーに対して個別のアカウントを作成する。
TM-38：IIoT 機器でアカウントロックアウト機能を実装/使用する。
TM-39：多数の機器を含む大規模で多様なネットワークの場合は、特権アクセス管理（PAM）ソリューションを採用する。
TM-40：アクセス制御の範囲内で、建物、区域、部屋およびキャビネットへの物理的アクセスの側面を考慮する。

4.4.8 ネットワーク、プロトコル、暗号化

セキュリティ対策は、適切なプロトコルの実装、暗号化、およびネットワークセグメンテーションを通じて、通信のセキュリティを確保するのに役立つ。

TM-41：IIoT ソリューションに関連する通信チャネルを保護し、重要なデータの場合、技術的に可能な場合には通信を暗号化する。
TM-42：非武装地帯（DMZ）の確立およびゾーン間のトラフィック制御を含む（例えば、パデューモデルによる）事前定義されたゾーニングモデルに基づいて産業プラントネットワークをセグメント化する。
TM-43：少数機器から成る複数のセグメントを構築し、その中で互いとのみ通信し、セグメント間のネットワークトラフィックを制御するマイクロセグメンテーションアプローチに従う。
TM-44：可能であれば、安全計装用ネットワークをビジネスおよび制御ネットワークから分離する。
TM-45：IIoT ソリューションでは、標準規格および技術上の推奨事項に基づいて、既知のセキュリティ機能を備えた実績のあるプロトコルを実装する。セキュアであることが証明されているプロトコルを使用するか、過去のセキュリティ問題（TLS 1.3 など）に対処し、既知の脆弱性（Telnet、SNMP v1、v2 など）を回避するソリューションを選択する。
TM-46：同じシステム内のさまざまな機器に異なるプロトコルを実装するときに、セキュリテ

ィ機能とプロトコル間の相互運用性を保証する。

TM-47：可能であれば、特定の環境内に実装されるプロトコルの数を制限し、未使用のデフォルトネットワークサービスを無効する。

TM-48：鍵交換と鍵管理のためのセキュアな環境を確保し、複数の機器間で暗号鍵を共有することを避ける。

TM-49：転送中および保管中のデータおよび情報（制御メッセージを含む）の機密性、信頼性および/または完全性を保護するための暗号の適切かつ効果的な使用を確保する。標準規格および強力な暗号化アルゴリズムと強力な鍵を適切に選択し、安全でないプロトコルを無効にする。実装の堅牢性を確認する。

4.4.9 モニタリングと監査

ネットワークトラフィックと可用性の監視、ログ収集とレビューに関するセキュリティ対策。

TM-50：IT および OT 環境にパッシブ監視ソリューションを実装して、産業用ネットワークトラフィックのベースラインを作成し、異常とその基準の順守を監視する。

TM-51：セキュリティログを収集し、専用のツールを使用してリアルタイムでそれらを分析する。（例：セキュリティオペレーションセンター（SOC）内の SIEM クラスソリューション）

TM-52：ネットワークログ、アクセス制御権限、および資産の設定の定期的なレビューを実施する。

TM-53：技術的に可能な場合は、IIoT 機器の可用性をリアルタイムで監視する。

4.4.10 構成管理

セキュリティ構成、構成の変更管理、機器の強化、およびバックアップ検証に関するセキュリティ対策。

TM-54：さまざまな種類の資産に合わせたベースラインセキュリティ構成を確立する。

TM-55：構成管理を可能にするメカニズムと支援ツールを導入する。

TM-56：リスク分析に基づいて組織が策定した変更管理ポリシーに従って、構成の変更を実施し文書化する。

TM-57：影響分析のための専用手順を開発し、システムへの変更を実施する前にそれを実行する。

TM-58：IIoT ソリューションを堅牢化し、これを変更管理ポリシーに含める。

TM-59：さまざまな種類の資産に合わせた、定期テストの条項を含む包括的なバックアップ計画を作成して適用する。

用語集

APT	Advanced Persistent Threat	持続的標的型攻撃
BCP	Business Continuity Plan	事業継続計画
BLE	Bluetooth Low Energy	Bluetooth LE
CRM	Customer Relationship Management	顧客関係管理
CERT	Computer Emergency Readiness Team	コンピュータ緊急対応チーム
(D)DoS	(Distributed) Denial of Service	(分散型) サービス妨害攻撃
DCS	Distributed Control System	分散制御システム
DRP	Disaster Recovery Plan	災害復旧計画
ERP	Enterprise Resource Planning	企業資源計画
ESS	Executive Support System	経営戦略支援システム
HMI	Human Machine Interface	ヒューマンマシンインタフェース
ICS	Industrial Control System	産業用制御システム
IDS	Intrusion Detection System	侵入検知システム
IP	Internet Protocol	インターネットプロトコル
IPS	Intrusion Prevention System	侵入防止システム
ISAC	Information Sharing and Analysis Centre	情報共有分析センター
M2M	Machine to Machine	機械間
MES	Manufacturing Execution System	製造実行システム
ML	Machine Learning	機械学習
MQTT	Message Queuing Telemetry Transport	メッセージ・キューイング・テレメトリー・トランスポート
PLC	Programmable Logic Controller	プログラマブルロジックコントローラ
QC	Quality Control	品質管理
RTU	Remote Terminal Unit	遠隔端末装置
SCADA	Supervisory Control and Data Acquisition	監視制御データ収集システム
SIEM	Security Information and Event Management	セキュリティ情報イベント管理
SIS	Safety Instrumented System	安全計装システム
SOC	Security Operation Centre	セキュリティオペレーションセンター
TCP	Transmission Control Protocol	伝送制御プロトコル
WMS	Warehouse Management System	倉庫管理システム

付録 A：ENISA「IoT のベースラインセキュリティに関する提言」との関係

「IoT のベースラインセキュリティに関する提言」は、重要な情報インフラにおける IoT セキュリティのガイドラインの策定を目的とした、ENISA による以前の調査である。これは、IIoT およびインダストリー4.0 の特定の分野におけるサイバーセキュリティの側面の詳細調査に焦点を当てているこの調査の基礎、およびリファレンスポイントとなっている。

この調査は「IoT のベースラインセキュリティに関する提言」を元にしており、採用された定義と IoT との関連は、ENISA の一般的なアプローチと合致している。以下、IIoT と IoT の関係について説明する。 ENISA は、モノのインターネット（IoT）を、**「意思決定を可能にする、相互接続された物理的な及び潜在的に仮想的なセンサやアクチュエータから成るサイバーフィジカルエコシステム」**と定義している。情報が IoT の中心にあり、センシング、意思決定、実行という連続的なサイクルを生み出している。

ビジネス機能の基準に基づいて、図 10 に示すように、モノのインターネットは次のように分類される。
コンシューマー向け IoT - 個々の顧客に付加価値を与えるスマートコネクテッド製品プラットフォームを含む。
IIoT - 資産のパフォーマンス、製品の品質、およびトレーサビリティ（追跡可能性）とアカウンタビリティ（説明責任）を向上させる機器の接続性に対応する。

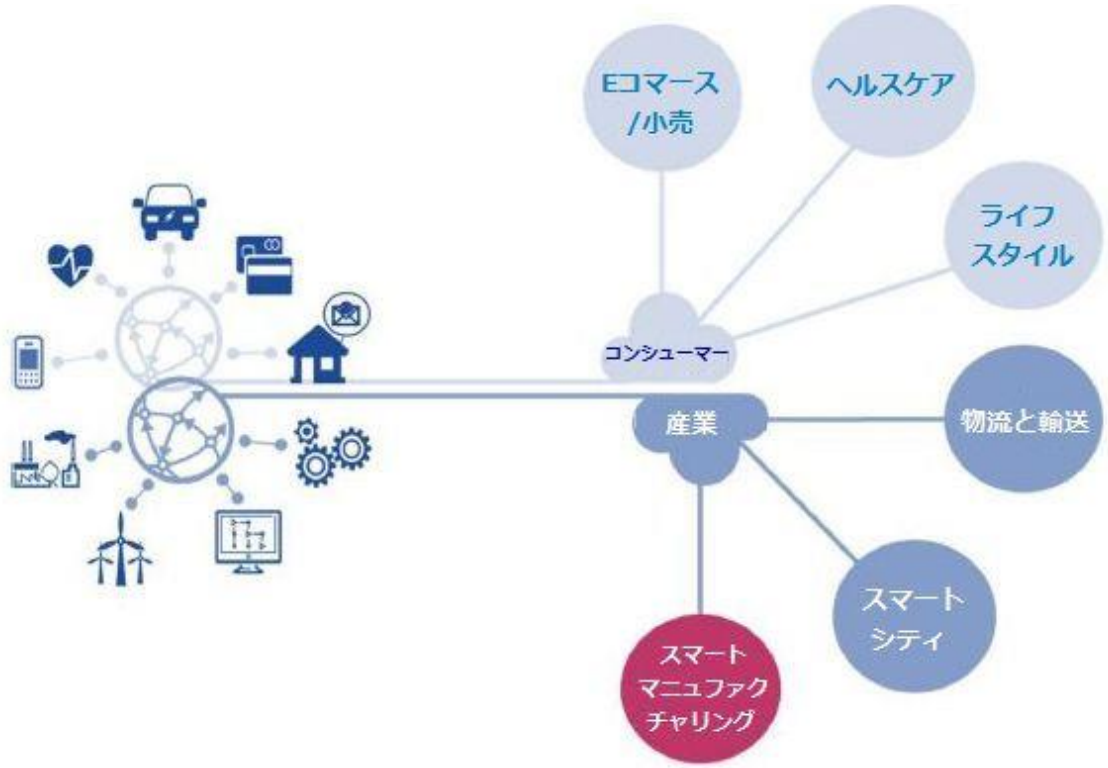

図 10：コンシューマー向け・IIoT 機器

産業用モノのインターネット（IIoT）の概念は、デジタル化する産業界に焦点を当てた IoT に関連付けられている。一般的に IoT はさまざまな消費者向け製品を含む広い概念だが、IIoT は特に OT 環境で使用される。技術的に類似した特徴を持つ IoT システムは、通常、セーフティよりもユーザビリティに重点を置いている。一方、IIoT システムは OT 環境に固有のセキュリティ要件を満たす必要があり、その結果、表 4 に示すように、ビジネス上の推進要因と特性の点[46]で違いがある。

表 4：IoT と IIoT の間の選択された側面に関する指標の違い

選択された特性	IoT	IIoT
フォーカス	個人データと資産の保護	プロセスの中断防止、セーフティ
優先度	機密性、完全性、可用性	可用性、完全性、機密性
機器障害の影響	致命的な影響なし	プロセスの中断、生産への影響、潜在的な物理的脅威
脅威への対応	電源を切って修復が可能	メンテナンス時
アップグレードとパッチ管理	運用時間中に可能。延期する理由はなし。	ダウンタイム中にスケジュールを設定して実行する必要があるため、アップグレードはかなりの時間延期される可能性あり。
機器のライフサイクル	比較的頻繁に機器をアップグレード	長い（15 年以上[47]）
設置状況	通常	過酷な環境（温度、振動など）

[46] Industrial Internet Consortium (2016) “Industrial Internet of Things Volume G4: Security Framework”: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

[47] CISCO (2017) “Cybersecurity for Industry 4.0”: https://i40.hkpc.org/CyberSec/pdf/Day%201_1110-1150_Mr.%20Garrick%20Ng%20(new).pdf

付録 B：セキュリティ対策／グッドプラクティスの詳細なリスト

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
セキュリティ・バイ・デザイン	**PS-01：**IoT のサイバーセキュリティは、エンドツーエンドのプロセスとしてではなく、サイクルとして扱う。最初からソリューション開発のあらゆる活動におけるサイバーセキュリティの側面を考慮に入れる。 インフラの観点からだけでなく、機器の観点からもセキュリティ・バイ・デザインアプローチによるセキュリティを採用する。 「セキュリティ・バイ・デザイン」の概念の中で PS-01 は、スマートマニュファクチャリング・システム開発ライフサイクル（Secure SDLC）の各ステップ、すなわち分析、設計、実装、テスト、運用および保守における継続的なセキュリティ改善サイクルに関連している。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・Huawei - IoT Security White Paper 2017 ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future ・VDC - Industry 4.0: Secure by design
セキュリティ・バイ・デザイン	**PS-02:**コンピュータの計算能力のような制約を考慮した上で可能ならば、ネットワークレベルだけでなく、エンドポイントの組み込み機能でサイバーセキュリティに対処する。 設計段階から、フェイルセーフとフェイルセキュアのメカニズムを導入することにより、自動化システムにサイバーセキュリティを組み込む。	・不正操作/悪用 ・障害/誤動作	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・Huawei - IoT Security White Paper 2017 ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・Symantec - An Internet of Things Reference Architecture ・VDC - Industry 4.0: Secure by design

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
セキュリティ・バイ・デザイン	**PS-03 :** セキュリティとセーフティの評価の結果、適切であると判断された場合、非常に限られた処理能力しか持たない最も基本的なコネクテッドデバイス（例：アクチュエータ、コンバータ）にも識別および認証機能を備え、IAM（アイデンティティ/アクセス管理）クラスソリューションとの互換性を確保する。 これは特に、許可されていない再較正や再設定に対する保護に適用される。 例えば、測定装置の設定において、 a）装置構成および較正エンジニアリングツールにアクセスするための最小権限の原則 b）エンジニアリングツールにアクセスするエンジニアの認可と認証 c）L0 / L1 機器に対する堅固な物理的セキュリティ d）脆弱な無線プロトコルの無効化 e）テスト/デバッグ機能の無効化	・不正操作/悪用 ・物理攻撃 ・偶発的な被害	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・Huawei - IoT Security White Paper 2017 ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
セキュリティ・バイ・デザイン	**PS-04:**機器の設計プロセスのごく初期段階からサイバーセキュリティの専門家を巻き込んでリスクと脅威の分析を行い、どのセキュリティ機能が必要となるか明らかにする。 分析には、機器が遭遇する可能性のある、各々の事情に合わせた使用事例を含める必要がある。さまざまな攻撃シナリオに対するレジリエンスを考慮するために、IIoT システムおよび攻撃ツリーの脅威モデリングを開発することを推奨する。サイバーセキュリティの専門家は、現在の脅威とリスクの展望に関する経験と知識に基づいて、制御システムが直面している脅威とリスクに関する洞察を与えるためのプロセスに関与する必要がある。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ETSI (European Telecommunications Standards Institute) - ETSI GR QSC 004 V1.1.1 (2017-03) Quantum Safe Cryptography; Quantum-Safe threat assessment ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISA - ANSI/ISA-95 Part 1: Models and Terminology ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
セキュリティ・バイ・デザイン	**PS-05 :** 各設計文書には、産業環境におけるすべての情報と制御システムのセキュリティを扱う章を含める。機能仕様および/または技術仕様には、少なくとも下記のような、使用されるセキュリティ対策に関する情報が含まれている必要がある。 a）システムアーキテクチャ b）アクセス制御 c）インタフェースと通信セキュリティ d）ポリシーの執行 e）モバイルのセキュリティ f）クラウドのセキュリティ g）バックアップ/災害復旧	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・European Parliament and Council of the European Union - General Data Protection Regulation (GDPR) (EU) 2016/679 ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEEE - Internet of Things (IoT) Security Best Practices ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
プライバシー・バイ・デザイン	**PS-06：**EU 一般データ保護規制（GDPR）など、適用される国内および国際的な規制に基づいてプライバシー関連の問題に対処する。 組織内のコンプライアンス機能は、すべての新システムが規制上の要件に準拠していることを確認する必要がある。これには、入札/調達プロセスにおいて技術仕様書に要件を記載することが含まれる。 組織はまた、プライバシー保護の説明責任の側面を考慮に入れ、組織が関連する行動および有効性を実証できる対策を実施するべきである。	・法規	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・IoT Security Foundation - Security Challenges on the Way Towards Smart Manufacturing ・ISA - ANSI/ISA-95 Part 1: Models and Terminology ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・OWASP (Open Web Application Security Project) - IoT Security Guidance ・VDC - Industry 4.0: Secure by design
プライバシー・バイ・デザイン	**PS-07：**設計段階で、機器によって処理されるデータの範囲および処理の目的を定義する。 最小限の個人データのみが機器によって収集されるようにする。機微なデータの収集は避ける。 IIoT システムのユーザーは、必要がなければ個人情報や機微な情報を提供しない。	・不正操作/悪用 ・法規	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・ETSI (European Telecommunications Standards Institute) - ETSI TR 103 375 SmartM2M; IoT Standards landscape and future evolutions ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISA - ANSI/ISA-95 Part 1: Models and Terminology ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・OWASP (Open Web Application Security Project) - IoT Security Guidance

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
プライバシー・バイ・デザイン	**PS-08:**組織によって保存されたデータの物理的な場所を確立し、どの組織間でデータを転送するかを定義する。収集した個人データへのアクセスは、許可された個人にのみ制限する。定期的にアクセス権を見直し、従業員の転職/退職後できるだけ早くアクセス権を削除する。	・不正操作/悪用 ・物理攻撃 ・法規	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ENISA - Baseline Security Recommendations for IoT ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
プライバシー・バイ・デザイン	**PS-09：**機器によって処理されるデータについて、GDPR 要件に沿って - プライバシー影響分析（PIA）を実施する。これはリスク管理プロセスに統合することができる。	・不正操作/悪用 ・法規	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ETSI (European Telecommunications Standards Institute) - ETSI TR 103 375 SmartM2M; IoT Standards landscape and future evolutions ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・Huawei - IoT Security White Paper 2017 ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines
プライバシー・バイ・デザイン	**PS-10:**個人を識別するために使用できるデータを他の情報から分離し、そのセキュリティを確保する（情報の保存と取得、通信サービス、暗号化など）。 IIoT 環境内で転送される個人データはすべてトラフィック内で暗号化する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・法規	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
資産管理	**PS-11：**資産管理をサポートするツールを利用する（例えば自動資産可視化ツール）。 資産管理システムは堅固で堅牢であるべきである。 組織や産業環境に固有の資産（独自のプロトコルを使用しているものも含む）を動的に発見、識別、および列挙できる資産管理ツールを選択する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・障害/誤動作	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques – Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns ・SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
資産管理	**PS-12：**企業が一貫した最新の資産一覧表を持っていることを確認する。この一覧表には、IP アドレス、物理的な場所、ホスト、現在のファームウェア/ OS のバージョン、使用されている通信プロトコルなどを含める。資産一覧表には、特定の資産に関連して収集された既知の脆弱性情報も含める必要がある。 最新の資産一覧表を維持していく責任を明確に定義し、システムの所有者/管理者に伝える。	・盗聴/傍受/ハイジャック ・物理攻撃 ・障害/誤動作	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
資産管理	**PS-13:** レガシーなシステム資産がある複雑な産業環境では、アクティブ監視ソリューションの代わりにパッシブ監視装置を使用する。パッシブ監視装置はシステムの動作を妨げないので、可能な限りパッシブ監視装置を使用することを推奨する。アクティブ監視装置を利用すると、OT 環境に悪影響を及ぼし、製造工程を中断させる可能性がある。 アクティブ監視ツールの実装を検討する場合は、実験/テスト環境でテストフェーズを設け、システムに悪影響を及ぼすかどうか、つまりネットワーク負荷が大幅に増加しないかどうかを確認する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
資産管理	**PS-14:** 製造工場内のコンピュータ化された環境全体に集中管理型資産一覧を使用する。システム変更を実装した一覧を更新する。 実装後および変更ごとに最新バージョンのソフトウェアを保管する。 定期的なレビュー（例：年 1 回）も推奨する。 構成管理と変更検出を可能にするセキュリティツールを使用することを推奨する。	・不正操作/悪用 ・物理攻撃 ・偶発的な被害	・BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
資産管理	**PS-15：**資産のセキュアな管理を検討する。 IoT 機器の管理にセキュア/暗号化方式を利用する。（HTTPS、SSH など）。また関連する鍵管理にもセキュア/暗号化方式を利用する。 インフラおよびセキュリティ機器の管理は、専用の管理ネットワークを介して行う必要がある。	・不正操作/悪用	・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
資産管理	**PS-16 :** 確立・承認・伝達された変更管理プロセスに従ってのみ、新しい機器をシステムに追加する。所定の承認を受けない限り、いかなる変更も許可しない。承認された変更は文書化し、関連文書を更新する。 緊急の変更は、変更管理委員会のリーダーおよびシステムオーナーからの口頭での承認に基づいて実行できる。ただし、緊急事態の収束後は、変更とリスク分析を文書化するための通常の手順を適用する必要がある。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害	・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
資産管理	**PS-17 :** 容認されたビジネス要件がない場合は、リムーバブルデバイスの使用を避け、USB ポートを無効にする（または技術的に USB ポートでのリムーバブルメディアの使用を制限する）。リムーバルデバイスを環境に接続する必要がある場合は、少なくとも最新の定義を含むマルウェア検出ソフトウェアを使用してリムーバブルデバイスをスキャンする。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・Huawei - IoT Security White Paper 2017 ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NIST.SP 1500-202 - Framework for Cyber-Physical Systems: Volume 2, Working Group Reports ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
リスクおよび脅威の特定と評価	**PS-18：**インダストリー4.0 とスマートマニュファクチャリングに特化したリスク管理へのアプローチを採用する。リスク管理へのアプローチは定性的または定量的であること。 評価フェーズでは、新しいパラメータ、脅威、および攻撃のシナリオを検討し、サイバーフィジカルシナリオ、サイバーフィジカル環境およびセーフティの間の相互依存性をすべて網羅する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Homeland Security - Strategic Principles for Securing the Internet of Things ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
リスクおよび脅威の特定と評価	**PS-19：**製造環境における重要なインフラについては、企業・セーフティ・環境面でのリスク管理と完全に整合したリスク管理を確立する。 それらのリスク管理分野に対する脅威、脆弱性、および保護対策を評価し、特徴付ける。 それに基づいて、OT および重要インフラの場合は、具体的な影響に基づくリスク管理アプローチを確立する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-4-1:2013 Secure product development lifecycle requirements ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
リスクおよび脅威の特定と評価	**PS-20:**企業の個々のニーズとセキュリティ要件に従って、リスクと脅威の管理プロセスを確立する。そのプロセスには、重要なセキュリティ資産を識別するためのセキュリティリスク評価と、セキュリティリスクと軽減策を識別するための脅威のモデリングを含める。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
リスクおよび脅威の特定と評価	**PS-21：**少なくとも年 1 回、サイバーセキュリティの側面を含むリスク分析を実行する。また、リスク分析を確実に実行するために、変更管理、インシデント処理、脆弱性管理などの他のプロセスと統合する。 - 新しいシステムを導入する場合、または既存のシステムに大幅な変更を加える場合 - 重大なセキュリティ問題が発生した場合 - 重大な脆弱性が検出された場合 - システムオーナーの要求または特別な状況の場合 リスク評価は、セキュリティポリシーとプロセスの有効性の技術的および手順的テストを網羅する必要がある。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
リスクおよび脅威の特定と評価	**PS-22:** 企業の事業分野に関連する潜在的な攻撃の種類と原因、および新たな脆弱性について知るために、脅威インテリジェンスプロセスを脅威管理アプローチに組み込むことを検討する。 ベンダーの通知、専門機関、他社の Web サイト、オープンソースなど、脅威情報の様々な情報源を使用する。 脅威インテリジェンスプログラムの詳細は、個々の企業のニーズに合わせて調整する必要があり、特に大企業の場合は、サイバーセキュリティニュースをフォローするなどの基本的な方法から、特別なツールや前述の情報源を利用する高度な方法までさまざまである。 プログラムの実施前に、受け取ったデータをどのように取り扱うか、責任者を誰にするか、そしてこのプログラムに関して企業の目標をどのようにするかを事前に計画する。 信頼できる業界パートナー、ISAC（情報共有分析センター）および CERT（情報システム緊急対応チーム）との情報共有を取り入れる。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators ・Huawei - IoT Security White Paper 2017 ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・International Telecommunications Union - Security capabilities supporting safety of the Internet of things ・NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
リスクおよび脅威の特定と評価	**PS-23 :** 組織の観点から、選択した脅威を監視し、リスク分析を実行してシステムへの影響を判断する。 脅威インテリジェンスプロセスを通じて検出された脅威をコントロールする。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices ・VDC - Industry 4.0: Secure by design
リスクおよび脅威の特定と評価	**PS-24 :** リスク管理プロセスに関して、同時に 2 つの異なるアプローチを採用する： - 組織のビジネスニーズを考慮しながら、組織のセキュリティ問題に対処する方法について明確に定義された戦略を使用した総合的なアプローチに従うトップダウン・アプローチ。 これは、統一されたポリシー、手順、および実践を通じて、組織全体の観点からサイバーセキュリティに対処するのに役立つ。 - 人と資産の観点から、企業の状況のきめ細かく詳細な見解を提供するボトムアップ・アプローチ。 これにより、部門、人事、特定のプロセスなどの違いを区別し、組織全体のプログラムを組織のより小さな部署に固有の特定のニーズに適応させることができる。 これら 2 つのアプローチを組み合わせて、組織全体およびその特定の下位部門の側面に合わせたセキュリティ計画を確立する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
製品ライフサイクルを通じたサポート	**OP-01：**エンドポイントライフサイクルのあらゆる段階におけるソフトウェアとハードウェアのセキュリティに焦点を当てる。発注段階で、個々のコンポーネントのセキュリティ機能レベルを含む、定義済みのセキュリティ要件をベンダーに提供する。IIoT 機器の場合、使用する前にローカルで試運転を実行する。 使用段階では、保守手順のセキュリティを確保する。 機器のライフサイクルの使用終了段階では、機器から重要なデータを削除し、管理された方法で機器を実稼働から撤去する。	・障害/誤動作 ・法規	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・International Telecommunications Union - Security capabilities supporting safety of the Internet of things ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NIST SP 800-61r2: Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
製品ライフサイクルを通じたサポート	**OP-02：**サプライチェーン全体を通してセキュリティについて検討すべき事項を考慮に入れる。 サプライチェーン全体において、ソフトウェア、ハードウェア、およびそのコンポーネントを監視し、不正な変更を検出して防止する。（ソフトウェアへのマルウェア挿入など） 固有の機器 ID を作成し、それを機器のライフサイクル全体にわたって維持する。 信頼の基点、デジタル署名、および組み込んだ識別子に基づいて完全性が検証できる。 製造された機器の完全性が評価され、検証されることを確認する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Security Foundation - Security Challenges on the Way Towards Smart Manufacturing ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - Best practices in cyber supply chain risk management. Smart Manufacturing The Future of Manufacturing and Value Chain Competitiveness ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations ・OWASP (Open Web Application Security Project) - IoT Security Guidance

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
製品ライフサイクルを通じたサポート	**OP-03：**調達プロセス全体において、特定の機器/ソリューションに合わせて調整されたセキュリティ対策と要件を定義し、セキュリティ面を考慮する。 セキュリティの専門家は、リビジョン時に参加するものとする。 IIoT の調達プロセスでは、IIoT の技術要件仕様書を作成する。この文書では、推奨される技術と、製品サポートおよびセキュリティサポートライフサイクルの側面を含む最小限のサイバーセキュリティ要件を定義する。	・障害/誤動作 ・サービス停止 ・災害	・Elsevier - Avoiding the internet of insecure industrial things ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Security Foundation - Security Challenges on the Way Towards Smart Manufacturing ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - Best practices in cyber supply chain risk management. Smart Manufacturing The Future of Manufacturing and Value Chain Competitiveness ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
製品ライフサイクルを通じたサポート	**OP-04：**さまざまな検証活動や製品ライフサイクルの段階において技術仕様のサイバーセキュリティ受け入れテスト（例：FAT、SAT、本番前の侵入テスト）を実施する。	・障害/誤動作 ・サービス停止 ・災害	・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・NIST - Cybersecurity for Smart Manufacturing ・NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
製品ライフサイクルを通じたサポート	**OP-05：**プロジェクト実施プロセスの引継ぎ段階で、すべてのサイバーセキュリティ文書、プロセスおよび手順を適切に整備し引き渡す。 ドキュメントには、システムアカウントとサービスアカウントのリスト、セキュリティログ、対応計画、すべてのソフトウェアとファームウェアのバージョンの確認、最新のネットワーク図、システムアーキテクチャ、リスク登録一覧、およびセキュリティ制限を含める。 プロセスには、保守ルーチン、ウイルス対策の適用状況と保証、パッチ適用プロセスとアカウントの管理および認証プロセスを含める。 手順には、ファイアウォールの基本設定、管理と監視、変更管理、およびフォールオーバーテストを含める。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・障害/誤動作 ・法規	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・MIT - Security Analysis of Zigbee ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Smart Factory Innovation Forum - Managing security, safety and privacy in Smart Factories ・VDMA - Industrie 4.0 Security Guidelines Recommendations for actions ・World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
セキュリティアーキテクチャ	**OP-06：**コンピュータ化されたエコシステムでセキュリティを確保するために、包括的なアーキテクチャベースのアプローチを採用し、ビジネス要件に基づいてリスクに合わせたセキュリティアーキテクチャを開発する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規	・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・Homeland Security - Strategic Principles for Securing the Internet of Things ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISA - ANSI/ISA-95 Part 1: Models and Terminology ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・VDC - Industry 4.0: Secure by design

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
セキュリティアーキテクチャ	**OP-07：**セキュリティアーキテクチャを定義しながら、組織から物理的な実装の問題まで、関連するすべてのセキュリティの側面を含むようにする。 セキュリティアーキテクチャは、次のドメインで構成されている必要がある（ただし、これらに限定されない）。 - セキュリティポリシーと設計原則 - セキュリティガバナンスと運用モデル（組織） - セキュリティネットワーク設計図（ゾーニングモデル） - セキュリティ技術要件 - セキュリティサービスの設計 - セキュリティ手順	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Homeland Security - Strategic Principles for Securing the Internet of Things ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISA - ANSI/ISA-95 Part 1: Models and Terminology ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・VDC - Industry 4.0: Secure by design
セキュリティアーキテクチャ	**OP-08：**セキュリティアーキテクチャ内で、IT 部門、エンジニアリング/オートメーション部門、および運用部門の間で、セキュリティに関する明確な役割と責任を割り当て、配分する。 OT システムとセキュリティプロセスの両方の役割を明確に定義し伝達する。 明確な権限と明確な意思決定プロセスを備えた統治機関を設置する。	・不正操作/悪用 ・偶発的な被害 ・障害/誤動作	・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISA - ANSI/ISA-95 Part 1: Models and Terminology ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・SANS Institute - Building the New Network Security Architecture for the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
セキュリティアーキテクチャ	**OP-09：**確立されたセキュリティアーキテクチャにコンプライアンス管理を統合し、すべての製品がその中で定義された要件を満たすことを確実にする。	・偶発的な被害 ・障害/誤動作 ・法規 ・災害	・Homeland Security - Strategic Principles for Securing the Internet of Things ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISA - ANSI/ISA-95 Part 1: Models and Terminology ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・SANS Institute - Building the New Network Security Architecture for the Future
インシデント管理	**OP-10：**企業の事業分野と範囲に基づいて、組織にとって重要なサイバーインシデントを定義する。 これらのインシデントは、一般的な攻撃ベクトル (リムーバブルメディア、電子メール、web サイトなど) の使用状況、またはその影響 (組織の事業、データなど) に応じてグループ化するなど、適用される標準規格に基づいて分類する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
インシデント管理	**OP-11：**サイバーセキュリティインシデントをサポートするための明確な役割、責任、IT、OT およびサイバーセキュリティの専門家から成る、OT サイバーセキュリティオペレーションセンター（SOC）の創設を検討する。 SOC 要員は適切な役割と責任を持つ特定のサポートラインに分割する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ENISA - Baseline Security Recommendations for IoT ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future
インシデント管理	**OP-12：**影響を受ける資産の識別、脆弱性の識別と分類、エスカレーションと通知からなるインシデント処理のためのプロセスを確立する。少なくとも年 1 回、および大きな変更があった場合はできるだけ早くプロセスの見直しを行う（例えば 組織階層の変更、契約の変更など）。 セキュリティインシデントの分析と解決から学んだ教訓を生かしてプロセスを更新する。 少なくとも年 1 回プロセスをテストし、起こりうる様々なインシデントを検討する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
インシデント管理	**OP-13：**セキュリティに関連した異常なイベントをすべて迅速に検出して調査する。 IT/OT 環境へのアクセス権を持つ従業員、請負業者、および外部企業に、セキュリティ上の弱点および異常が認められる、または疑いがある場合に通知および報告することを義務付ける。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
脆弱性管理	**OP-14：**リスク分析の結果を基に、自動および手動ツール（例えば、パッシブ脆弱性スキャナー）の利用を含む、組織内の包括的な脆弱性管理プロセスを定義する。 アクティブスキャナーを実装する場合は、テスト段階の前に、システム所有者による承認が必要。 OT 環境でアクティブなスキャナーを使用すると、特にレガシー機器を使用している場合、システムに悪影響を及ぼし、製造プロセスを中断させる可能性があることに留意する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作	・Huawei - IoT Security White Paper 2017 ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
脆弱性管理	**OP-15：**セキュリティのギャップの排除は、資産とシステムの重要性を考慮して最も重要な脆弱性から始める。 資産一覧表に資産およびシステムの重要性に関連するデータが含まれている場合、このプロセスは資産一覧表によってサポートされる。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・障害/誤動作 ・サービス停止	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・Homeland Security - Strategic Principles for Securing the Internet of Things ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation ・SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
脆弱性管理	**OP-18：**OT 部門と IT 部門の間で緊密なコラボレーションを確立する。 IT セキュリティの責任を負う個人が、プラントエンジニアの認知と協力なしに、脆弱性管理を含むサイバーセキュリティポリシーを OT システムに実装することを許可しない。 IT 部門と OT 部門が、システム運用と脅威についての知識を共有するようにする。 ※訳注：原文では本項目の対策番号は OP-16 となっていますが、記載されている対策は本文（4.3.4）では OP-18 のため、OP-18 としています。	・障害/誤動作	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ENISA - Baseline Security Recommendations for IoT ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・Homeland Security - Strategic Principles for Securing the Internet of Things ・IEEE - Internet of Things (IoT) Security Best Practices ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
脆弱性管理	**OP-16：**脆弱性を開示するための包括的で明確なプロセスを確立する。 製造元である場合は、脆弱性が識別された場合は、専用の電子メールまたはポータルを通じて機器にパッチを適用する方法についてユーザーに通知する。 企業内での脆弱性の開示を促進するには、バグバウンティプログラムを立ち上げる（実装されたインフラまたは最終製品に重大なセキュリティの脆弱性を特定した人々に報酬を与える）。 ※訳注：原文では本項目の対策番号は OP-17 となっていますが、記載されている対策は本文（4.3.4）では OP-16 のため、OP-16 としています。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・障害/誤動作	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEEE - Internet of Things (IoT) Security Best Practices ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation ・SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
脆弱性管理	**OP-17：**制御された環境（例えば、実験室、試験環境）において、または試運転段階の前・途中（例えば、FAT または SAT 段階の間）に新しい IIoT ソリューションの侵入テストを実施する。 さらに、侵入テストを定期的に実施する（例：2～3 年に 1 回、およびシステム所有者の承認を得てシステムの重要なアップデートをした後）。 ※訳注：原文では本項目の対策番号は OP-18 となっていますが、記載されている対策は本文（4.3.4）では OP-17 のため、OP-17 としています。	・偶発的な被害	・ECSO (European Cyber Security Organisation) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector ・Cloud Security Alliance - Future Proofing the connected world ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Shaun Bligh-Wall - Industry 4.0: Security imperatives for IoT — converging networks, increasing risks. ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor ・VDMA - Industrie 4.0 Security Guidelines Recommendations for actions

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
セキュリティ教育と意識向上	**OP-19：**セキュリティトレーニングと従業員の意識向上のための総合的なアプローチを採用する。そのアプローチは、組織のあらゆるレベルの従業員を対象とし、インダストリー4.0 の新機能によって製造環境にもたらされる新たな脅威をカバーし、従業員の役割と責任、参加者の知識レベルの違いに合わせたものであること。 さらに、従業員の職務・職責が変わった際には必ず追加のトレーニングを受けるようにする。	・不正操作/悪用 ・偶発的な被害	・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
セキュリティ教育と意識向上	**OP-20：**新規雇用者全員に、実際に仕事を始める前にサイバーセキュリティトレーニングを実施する。 システムにアクセスするための認可を受ける前に、IIoT ソリューションのすべてのユーザーに基本的なセキュリティ意識とトレーニングを提供する。	・不正操作/悪用 ・偶発的な被害	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IoT Security Foundation - Security Challenges on the Way Towards Smart Manufacturing ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
セキュリティ教育と意識向上	**OP-21：**セキュリティトレーニングが継続的かつ定期的に行われるようにする。 新たな重要な脅威が公開された後にトレーニングプログラムを更新し、現在のインシデント処理および復旧活動から学んだ教訓に従ってそれらを調整する。	・不正操作/悪用 ・偶発的な被害	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
セキュリティ教育と意識向上	**OP-22：**IIoT ユーザーに、機器のセキュアな使用法を訓練する。 トレーニングセッション中に、IIoT 機器とエコシステムを保護するために展開されている技術とエコシステムについて IIoT ユーザーに説明する。	・不正操作/悪用 ・偶発的な被害	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation ・OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation ・World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
セキュリティ教育と意識向上	**OP-23：**セキュリティ意識向上のために、サプライチェーンを含むレベルで他の企業とのコミュニケーションを検討する - 製造業者、コンポーネントプロバイダ、ソフトウェアプロバイダ、サービスプロバイダおよび顧客とのコミュニケーションが推奨される。 また、組織間での議論、協力、および情報共有を可能にするために形成された信頼に基づいて、国際的なセキュリティコミュニティへの参加を検討する。 Plattform Industrie 4.0 、 Industrial Internet Consortium、Cloud Security Alliance などのコミュニティがある。	・障害/誤動作	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・ECSO (European Cyber Security Organization) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) ・OWASP (Open Web Application Security Project) - IoT Security Guidance

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
第三者組織管理	**OP-24：**第三者組織による制御層または生産層へのアクセスを厳密に管理する。(例：ベンダーが RJ45 ジャックに物理的に差し込むことでアクセスできる、またはタイマーシステムからアクセスできる、など。) さらに、専用のレジストリアカウント、多要素認証、および暗号化を利用する。 必要な時のみ、特定の目的のため、一時的に、かつ最小権限の原則に従い、制御層又は生産層へのアクセスを第三者組織に許可する。 セッションを記録および管理し、待機セッションは許可しない。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・ECSO (European Cyber Security Organization) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・NIST - Framework for Cyber-Physical Systems: Volume 1, Overview ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
第三者組織管理	**OP-25：**制御層または生産層のシステムにベンダーからは直接接続しない。 ネットワークセグメンテーション、VLAN の設定、実装されているファイアウォール、ネットワークトラフィックのフィルタリングにより、リモートアクセスのセキュリティをサポートする。 選択された必要な機能およびネットワークの一部へのアクセスのみを許可する (最小権限の原則に基づく必要がある)。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・偶発的な被害 ・障害/誤動作	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ECSO (European Cyber Security Organization) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector ・ENISA - Baseline Security Recommendations for IoT ・Homeland Security - Strategic Principles for Securing the Internet of Things ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・IoT Security Foundation - Security Challenges on the Way Towards Smart Manufacturing ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation ・SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
第三者組織管理	**OP-26：**サプライヤに、彼らのプロセスのセキュリティと提供する製品向けのコミットメントに関する情報の提供を促す。（例：納入品目に対するセキュリティへの取り組みについてサプライヤにアンケートを作成し、その結果を考慮してパートナーを選択する） ベンダーとサービスプロバイダ向けのセキュリティ要件を作成する。IIoT ソリューションプロバイダを選択する前に、システムのライフサイクルを通して定期的にベンダーとサービスプロバイダの監査を実施する必要がある。	・偶発的な被害 ・障害/誤動作	・Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ECSO (European Cyber Security Organization) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEEE - IEEE Std 802.1X-2010 - Port-Based Network Access Control ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
第三者組織管理	**OP-27：**適切な合意書および契約書の範囲内で、セキュリティを含む、第三者組織とのパートナーシップが関連するすべての側面を明確に定義する（例：SLA-サービスレベル合意書、NDA-秘密保持契約）。 協業を開始する前に、これらの契約書に署名する。	・偶発的な被害 ・障害/誤動作 ・法規	・ENISA - Baseline Security Recommendations for IoT ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・VDC - Industry 4.0: Secure by design

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
信頼性／完全性管理	**TM-01：**ソフトウェアを実行する前に、ソフトウェアの完全性を確認する。 信頼の基点とセキュアブートメカニズムを確認する。 ソフトウェアが（ベンダーによって署名された）信頼できるソースのもので、セキュアな方法で入手されていること（例えば暗号化された接続を介してダウンロードされたこと）を確認する。 ソフトウェアが正規のものであることを確認するために、ソフトウェアの署名および/またはチェックサムの管理を実施する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃	・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・International Telecommunications Union - Security capabilities supporting safety of the Internet of things ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・VDC - Industry 4.0: Secure by design

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
信頼性／完全性管理	**TM-02：**適切な方法（例えば、デジタル証明書／ PKI）を利用して、OT ネットワーク内のすべての IIoT 機器を認証する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns
信頼性／完全性管理	**TM-03：**IIoT 機器間のデータ交換チャネルを定義し、システム所有者がそれらを確実に受け入れるようにする。できるだけ安全なチャンネルのみを選択し、ホワイトリストを実装する。 モバイル機器で機微なデータを送信するときは、SMS、MMS、通知などの安全でないチャネルを使用しない。	・盗聴/傍受/ハイジャック	・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・OWASP (Open Web Application Security Project) - Mobile Top 10 2016 ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
信頼性／完全性管理	**TM-04：**アプリケーションホワイトリスト（産業用制御環境での実行が許可されているアプリケーションのリスト）、および他のすべてのアプリケーションの実行を妨げるメカニズムを実装する。 そのリストはベンダーによって提供されるか、またはベンダーとの協議で定義されたものであり、少なくとも毎年、そしてシステム変更を実施する際には見直されるものとする。 ホワイトリストでは、不要なアプリケーションや既知の脆弱性を持つアプリケーションは、攻撃者が使用する可能性があるシステムへのバックドアが含まれているため、すべて回避する必要がある。	・偶発的な被害 ・障害/誤動作 ・サービス停止	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・Symantec - An Internet of Things Reference Architecture
信頼性／完全性管理	**TM-05：**実装する機器の処理能力に合わせて調整された適切な暗号化メカニズムとキーストレージを利用して、生産データの完全性を確保する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
信頼性／完全性管理	**TM-06：**保管中および転送中の生産データを監視して、潜在的な許可されていないデータ変更を識別する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・Cloud Security Alliance - Future Proofing the connected world ・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・SANS Institute - Building the New Network Security Architecture for the Future
クラウドのセキュリティ	**TM-07：**クラウドの種類の選択に関する判断は、クラウドサービスプロバイダの国や接続拠点（point of presence）に適用される法律や規制、および拠点を考慮した上で、ビジネスおよびプライバシーへの影響評価、つまり定量的リスク評価に基づいて行う。 重要度を評価するためのリスクベースのアプローチは、非常に重要である。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・偶発的な被害 ・障害/誤動作 ・法規	・Cloud Security Alliance - Future Proofing the connected world ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・SANS Institute - Building the New Network Security Architecture for the Future
クラウドのセキュリティ	**TM-08：**クラウドセキュリティプロバイダとの合意にセキュリティと可用性の側面を含める。 クラウドセキュリティの側面に対する責任は明確に定義し、特定の当事者または個人に割り当てる。 サービスの可用性は測定可能なものとし、特定のパラメータを通して定義されるものとする。	・盗聴/傍受/ハイジャック ・サービス停止 ・法規	・Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management ・Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・Online Trust Alliance - IoT trust framework 2.5
クラウドのセキュリティ	**TM-09：**クラウドベースのアプリケーションと集中型システムでは、単一障害点を避ける。	・障害/誤動作 ・サービス停止	・ECSO (European Cyber Security Organization) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・NIST - NIST SP 800-146 Cloud Computing Synopsis and Recommendations ・Online Trust Alliance - IoT trust framework 2.5 ・SANS Institute - Building the New Network Security Architecture for the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
クラウドのセキュリティ	**TM-10：**重要なシステムとアプリケーションをプライベートまたは少なくともハイブリッドモデル内に配置する。パブリッククラウドの利用を検討している場合は、この決定の前にリスク分析を行う。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・障害/誤動作	・Cloud Security Alliance - Future Proofing the connected world ・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・Online Trust Alliance - IoT trust framework 2.5
クラウドのセキュリティ	**TM-11：**クラウド攻撃に関連するリスクを軽減するために、ゼロ知識証明のセキュリティアプローチを採用する。 つまり、サービスプロバイダは暗号化キーにアクセスせずにデータを保存および管理する。 クラウド内のすべてのデータと転送中のデータを保護する。すべてのデータを暗号化するのが理想的である。アプリケーションとインタフェースも保護する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ビジネスの継続と復旧	**TM-12：**事業継続計画（BCP）と災害復旧計画（DRP）を作成することにより、インダストリー4.0 システムのレジリエンスの確保に焦点を当てる。 セキュリティ上の問題が発生した場合でも、システム運用の継続性を確保する。 それらの計画の定期的なテストを実行し、テストと実際のセキュリティインシデントから学んだ教訓を踏まえてそれらを更新する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management ・Homeland Security - Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ビジネスの継続と復旧	**TM-13：**重要なビジネスおよび技術プロセスを定義し、それらがビジネスの継続性にどの程度影響を与えるかを判断する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・ETSI (European Telecommunications Standards Institute) - ETSI GR QSC 004 V1.1.1 (2017-03) Quantum Safe Cryptography; Quantum-Safe threat assessment ・Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
ビジネスの継続と復旧	**TM-14：**通常の（明確に定義された）運用状態に戻す方法に関する手順書を作成する。 これらの手順を確立する前に、脅威とリスクの評価を実行し、評価の結果に合わせて手順を調整する。 手順の中で、特定の必要な行動に対する役割と責任を定義する。 インシデント対応計画のコピーを、関与するインシデント対応担当者に配布する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ビジネスの継続と復旧	**TM-15：**リスク分析の前に緊急時対応計画を検討する。緊急時対応計画を定義し、管理された演習を実施してそれらをテストする。計画を定期的（少なくとも年 1 回や大きな変更がある場合）に見直し、適切に更新する。緊急時対応計画を作成する際には、企業の通常の業務を妨害する可能性のある、サイバーインシデントによって生じる大規模災害と小規模な事案の両方を考慮する。対応策の各段階に責任者を定義し、報告プロセスを確立する。対応計画はシンプルなものとし、適切なトレーニングを通じて従業員の意識向上を確実にする必要があることに留意する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・The Cavalry - Hippocratic Oath for Connected Medical Devices
ビジネスの継続と復旧	**TM-16：**事業継続および復旧計画に、第三者組織に関する側面を含める。適切な第三者組織の管理とその関与の管理は、企業の事業継続性を確保するために不可欠である。	・偶発的な被害 ・障害/誤動作	・Center for Internet Security (CIS) - Critical Security Controls ・Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ビジネスの継続と復旧	**TM-17：**目標復旧時間（RTO）、目標復旧時点（RPO）、最大許容停止時間（MTO）、最小事業継続目標（MBCO）など、企業の事業継続に関する重要なパラメータを定義する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・Infineon - Hardware-based solutions secure machine identities in smart factories ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report
機械間セキュリティ	**TM-18：**（公開鍵以外の）サービス層が使用する長期鍵を、インフラ機器内のハードウェア・セキュリティ・モジュール（HSM）に保管する。M2M 長期サービス鍵を保管する HSM は、物理的および／または論理的手段を使用して、M2M 機器または M2M ゲートウェイに紐づけられていなければならない。 HSM は、システム管理者などの認可された M2M システムオペレータであっても、保存されている（公開鍵以外の）秘密鍵の値を明らかにしてはいけない。	・盗聴/傍受/ハイジャック	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・Huawei - IoT Security White Paper 2017 ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations ・oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report ・Symantec - An Internet of Things Reference Architecture

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
機械間セキュリティ	**TM-19：**相互認証、完全性、および機密性を提供するために、通信機器間で実績のある安全な暗号化アルゴリズムでセキュリティアソシエーションを確立する。	・盗聴/傍受/ハイジャック	・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations ・oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report
機械間セキュリティ	**TM-20：**メッセージの全部または一部が、以前のメッセージの不正な再送信であるかどうかを検出する機能を含む通信プロトコルを使用する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・ENISA - Baseline Security Recommendations for IoT ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
機械間セキュリティ	**TM-21：**クロスサイトスクリプティングおよびコマンドインジェクションから保護するために、ポジティブ/ホワイトリスト型の入力検証を使用する。つまり、エンコードされた入力値をすべてデコードしてから、入力値を受け入れる前にそのデータの長さ、文字、フォーマットを検証する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・障害/誤動作	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ENISA - Baseline Security Recommendations for IoT ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・OWASP (Open Web Application Security Project) - IoT Security Guidance

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
データ保護	**TM-22：**（揮発性メモリおよび不揮発性メモリに）使用中・転送中のデータを保護する。 保管中のデータの保護は、職務ベースのアクセス制御と認証の要件によって実現できる。重要なデータの場合は、暗号化アルゴリズムの実装が推奨される。 アクセス制御リストなどの適切なセキュリティ対策を講じずに、機微なデータを SD カードに保存しないように特に注意する。 転送中のデータに関しては、システムコンポーネント間のトラフィックが確実に暗号化されるようにすることを推奨する。（例：SSL / VPN トンネルまたは TSL の利用）。 使用中のデータの保護には、アクセス制御と認証メカニズムを実装する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IOActive, Embedi - SCADA And Mobile Security In The Internet Of Things Era ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
データ保護	**TM-23:** リスク分析に基づいて OT システムに関連するデータを分類する。製造、機器、ユーザー情報を考慮に入れる。 定義されたカテゴリには、例えば、生産計画データ、顧客データ、研究開発データ、資産管理データ、欠陥および品質データ、生産ラインデータなどが含まれる。 各カテゴリについて、データの重要性を評価し、適切なレベルのセキュリティを確保するために必要なセキュリティ対策を定義する。 例えば、製法は製造企業にとって極めて重要であると考えられているため、暗号化など最先端の方法で保護されなければならない。	・不正操作/悪用	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
データ保護	**TM-24 :** 最小権限の原則と“知る必要のある人にだけ知らせる”という原則を念頭に置いて、特定のカテゴリのデータへのアクセスを第三者組織に許可し、このアクセスを文書化する。すなわち、第三者組織は必要なデータのみにアクセスし、最小限の権限しか持たないようにする（例：変更されてはいけないデータへの読み取り専用アクセス）。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・偶発的な被害	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
データ保護	**TM-25：**機密性の高いデータの場合は、許可されたユーザーだけが情報を読み取れるように暗号化と鍵管理を実装する。さらに、データ損失防止ソリューションを使用する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・偶発的な被害	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・OWASP (Open Web Application Security Project) - IoT Security Guidance
データ保護	**TM-26：**関連するすべての法的要件を考慮して、企業のシステム内で処理される直接的／間接的な個人データ（システム運用者の名前およびそのパフォーマンスに関する情報など）を匿名化するか、適切に保護する（例：職務ベースのアクセス制御と暗号化による保護）。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・Homeland Security - Strategic Principles for Securing the Internet of Things ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・OWASP (Open Web Application Security Project) - IoT Security Guidance ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor ・The Cavalry - Hippocratic Oath for Connected Medical Devices

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ソフトウェア／ファームウェアアップデート	**TM-27：**エンドポイントのソフトウェア/ファームウェアの信頼性と完全性を検証し、アップデートを厳重に管理する。 コードのアップデートに署名し（ロードされる前にコードを認証できるようにするため）、信頼性を維持することが推奨される。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・障害/誤動作	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・Homeland Security - Strategic Principles for Securing the Internet of Things ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor The Cavalry - Hippocratic Oath for Connected Medical Devices
ソフトウェア／ファームウェアアップデート	**TM-28：**リスク分析に基づいている場合、および自動アップデートを許可できる機器が特定されている場合にのみ、自動アップデート手順を実行する。 また、アップデートの作成元を確認する。	・不正操作/悪用 ・物理攻撃	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・Homeland Security - Strategic Principles for Securing the Internet of Things ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security The Cavalry - Hippocratic Oath for Connected Medical Devices
ソフトウェア／ファームウェアアップデート	**TM-29：**IIoT 機器用のパッチの展開は、悪影響がないことを証明した後にのみ実行する。本番環境に実装する前に、テスト環境でパッチをテストする。それが不可能な場合は、システムの 1 つのセグメントにのみパッチを適用することから始める。選択したセグメントにパッチが悪影響を及ぼした場合でも、他のゾーンが正常に動作し続けるようにする。	・障害/誤動作	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - Framework for Improving Critical Infrastructure Cybersecurity V1.1 NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ソフトウェア／ファームウェアアップデート	**TM-30：**パッチがテストされ、機器に悪影響を及ぼさないことを保証し証明することができる場合、または該当する条項に従って第三者組織がアップデートの責任を負う場合にのみ、第三者組織にパッチの適用を許可する。 さらに、パッチ適用プロセスに関連して実行されたアクションを報告し、それらについて事前に通知することを第三者組織に要求する。 アップデート手順は文書化され、組織内で周知され、管理されること。	・偶発的な被害 ・障害/誤動作	・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・IoT Security Foundation - Establishing Principles for IoT Security ・NIST - Framework for Improving Critical Infrastructure Cybersecurity V1.1 ・The Cavalry - Hippocratic Oath for Connected Medical Devices
ソフトウェア／ファームウェアアップデート	**TM-31：**アップデート不可能な制御システム（例えばレガシーなシステム）については、ネットワークセグメンテーション、マイクロセグメンテーション、システム移転または追加のリアルタイム監視ツールなどの代替措置を適用する。 リスク分析を実行して、既存のシステムのセキュリティを向上させることが可能で十分かどうか、あるいはシステムの入替が必要かどうかを判断する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・NIST - Framework for Improving Critical Infrastructure Cybersecurity V1.1 ・NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
アクセス制御	**TM-32：**リモートアクセスを通常のアクセスと分離する、すなわちリモート通信を制御するための一連の規則を策定する。 必要なシステムだけにリモートアクセスを制限し、それを監視する。 ユーザーの完全なトレーサビリティと説明責任を確保する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・偶発的な被害 ・障害/誤動作	・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・International Telecommunications Union - Security capabilities supporting safety of the Internet of things ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・OWASP (Open Web Application Security Project) - IoT Security Guidance ・VDMA - Smart Manufacturing General security and privacy principles to ensure a Trusted IoT environment

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
アクセス制御	**TM-33：**IIoT 機器およびシステムに対して最低限の認証セキュリティを確保する。 セグメント化されたネットワーク/システムでは、認可によって特定のセグメントへのアクセスのみが許可され、システムの他の部分へのアクセスは許可されないことを確認する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・偶発的な被害	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・OWASP (Open Web Application Security Project) - IoT Security Guidance ・VDC - Industry 4.0: Secure by design

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
アクセス制御	**TM-34：**IIoT ソリューションのベンダーは、多要素認証機能（Apple Touch ID、セキュリティトークンなど）を実装する。 そのようなソリューションのユーザーは、多要素システム認証を利用する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・ENISA - Baseline Security Recommendations for IoT ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation ・OWASP (Open Web Application Security Project) - IoT Security Guidance

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
アクセス制御	**TM-35：**試運転中/初回使用時にデフォルトのパスワードとユーザー名を変更する。パスワードの複雑さに関する企業のパスワードポリシーに沿った強力なパスワードを使用し、定義された期間経過後に新しいパスワードの設定を要求する。 機器メーカーとクラウドサービスプロバイダは、これらのオプションをユーザーに提供する。 産業用制御システムのパスワードは、必要なときにすぐにアクセスできるよう、複雑すぎないようにする。複雑なパスワードを使用する場合、組織はパスワード変更の頻度が高すぎないことを確認する。 セキュアなパスワード回復メカニズムが実施されていることを確認する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ENISA - Baseline Security Recommendations for IoT ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・OWASP (Open Web Application Security Project) - IoT Security Guidance ・SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
アクセス制御	**TM-36：**ユーザー権限を設定するときに最小権限の原則を適用する。複数のユーザーがいる環境では、役割が適切な人によって適切に分離・承認されていることを確認する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害	・ENISA - Baseline Security Recommendations for IoT ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・OWASP (Open Web Application Security Project) - IoT Security Guidance ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
アクセス制御	**TM-37：**IIoT 機器およびシステムへのアクセスに共有アカウントを使用しない。特定の人に対して実行されたアクションを追跡できるようにするため、可能な限りすべてのユーザーに対して個別のアカウントを作成する。 共有アカウントを使用している場合は、定期的に（たとえば 90 日ごとに）パスワードを変更し、共有アカウントグループ内で人事異動が発生した場合（たとえば従業員が退職するとき）にパスワードを変更する。 また、追加の代替制御（職務分掌、産業用 IDS などのリアルタイム監視ツール）の導入を検討する。	・物理攻撃 ・偶発的な被害	・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・VDMA - Industrie 4.0 Security Guidelines

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
アクセス制御	**TM-38：**ログイン試行の失敗回数が設定されたパラメータの値を超えると実行されるアカウントロックアウト機能を、機器に実装するか、もしくは使用する。クラウドおよびモバイルインターフェースにも適用する。許可された試行回数やロックアウトの時間などの詳細を指定するためのポリシーを作成する。	・不正操作/悪用	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・OWASP (Open Web Application Security Project) - IoT Security Guidance
アクセス制御	**TM-39：**多数の機器を含む大規模で多様なネットワークの場合、特権 ID アクセス管理（PAM：Privileged Access Manager）ソリューションを採用して、昇格した特権（管理者特権）を所定の方法に従い管理する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
アクセス制御	**TM-40：**アクセス制御の範囲内には、建物、区域、部屋、およびキャビネットの場所への物理的なアクセス（たとえば、壁、フェンス、電気錠/機械錠、およびケーシングによる）が含まれる。 定期的に（特に重要な場所への）アクセス権を見直し、物理的アクセスを必要最小限に制限し、企業内での役割に基づいてそれを分離する。 従業員の退職や社内での職務の変更のあとに、物理的なアクセスに対する迅速な変更/削除が行われるようにする（たとえば、物理的なアクセスシステムを人事システムに連動させる）。 物理的なセキュリティをサポートするための追跡および警報システムの導入を検討する。	・物理攻撃	・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ネットワーク／プロトコル／暗号化	**TM-41：**IIoT ソリューションに関連した通信チャネルのセキュリティを確保する。重要なデータ（構成管理データ、個人データ、制御目的のデータなど）がある場合は、可能であればセーフティ、可用性、およびパフォーマンスに影響を与えないよう通信を暗号化する。	・盗聴/傍受/ハイジャック	・BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・International Telecommunications Union - Security capabilities supporting safety of the Internet of things ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation ・OWASP (Open Web Application Security Project) - IoT Security Guidance

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ネットワーク／プロトコル／暗号化	**TM-42：**あらかじめ定義されたゾーニングモデルに基づいて（例えば、パデューモデルのオフィス層、製造層および制御層）産業プラントネットワークをセグメント化する。 オフィス層と制御層間の直接トラフィックが禁止されていることを確認する。これらのネットワークは、常にゼロトラストルール（信頼せずに必ず確認する）により非武装地帯（DMZ）を介して互いに通信する必要がある。各ゾーン間のトラフィックは常にファイアウォールによって制御される。 非武装地帯（DMZ）に、製造および管理ネットワーク（DC、DNS、NTP、バックアップサーバー、AV サーバー、ジャンプサーバーなど）にサービスを提供する、またはオフィス層のためにデータを取得する共有インフラサービスを設置する。 制御層の重要なシステムに専用のネットワークインフラ（物理的に分離）を確保する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・ENISA - Baseline Security Recommendations for IoT ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-1-1:2009 Terminology, concepts and models ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・SANS Institute - Building the New Network Security Architecture for the Future ・SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ネットワーク／プロトコル／暗号化	**TM-43：** 少数機器から成る複数のセグメント（例えば IT または OT ネットワーク）を構築し、その中で互いとにのみ通信し、セグメント間のネットワークトラフィックを制御するマイクロセグメンテーションアプローチに従う。 ファイアウォールを使用して異なるセグメント間のトラフィックを制御する。 ネットワークをセグメント化するときは、最小限の権限と“知る必要のある人にだけ知らせる”という原則を使用する。これは、必要なシステム間の、必要なポート上での、必要なプロトコルを使用した通信のみが許可され、残りは無効にされるべきであることを意味する。感染した際、隔離されたマイクロセグメントは他のネットワークに広がることを防いでくれる。 ネットワーク内のマイクロセグメンテーションは、次の方法で実現できる。 - 各マイクロセグメントに VLAN を使用 - 物理ネットワークの物理的な分離 - ネットワーク層フィルタリング、状態ベースのフィルタリング、ポートおよびプロトコルレベルのフィルタリング、アプリケーションフィルタリングなど、さまざまな層でのネットワークトラフィックのフィルタリング。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・IEC - IEC 62443-1-1:2009 Terminology, concepts and models ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・SANS Institute - Building the New Network Security Architecture for the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ネットワーク／プロトコル／暗号化	**TM-44：**安全計装用ネットワークをビジネスおよび制御ネットワークから分離する。業務上の理由でこれが不可能な場合は、ネットワークトラフィックフィルタリングソリューションが導入されていることを確認する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・Homeland Security - Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies ・IEC - IEC 62443-1-1:2009 Terminology, concepts and models ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・International Telecommunications Union - Security capabilities supporting safety of the Internet of things ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
ネットワーク／プロトコル／暗号化	**TM-45：**IIoT ソリューションでは、標準規格と技術的な推奨事項に基づいて、既知のセキュリティ機能を備えた（最近導入されたプロトコルではなく）実績のあるプロトコルを実装する。 安全であることが証明されているプロトコルまたは過去のセキュリティ問題に対処しているプロトコル（TLS 1.3 など）を使用し、既知の脆弱性を持つプロトコル（Telnet、SNMP v1、v2 など）を回避するソリューションを選択する。		

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ネットワーク／プロトコル／暗号化	**TM-46：**同じシステム内のさまざまな機器に異なるプロトコルを実装するときに、セキュリティ機能とプロトコル間の相互運用性を保証する。 これを実現するための方法例の 1 つは、プロトコルの変換を提供する専用ゲートウェイを使用することである。ゲートウェイは通信を通す際に、安全でないプロトコルを最新の安全なプロトコルに変換することができるため、攻撃対象領域を減らすことができる。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・障害/誤動作 ・サービス停止	・BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations ・Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ENISA - Baseline Security Recommendations for IoT ・GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・OWASP (Open Web Application Security Project) - IoT Security Guidance
ネットワーク／プロトコル／暗号化	**TM-47：**可能であれば、システムの管理性を確保するために、特定の環境内に実装されるプロトコルの数を制限する。 また、未使用のデフォルトネットワークサービスをすべて無効にする。	・障害/誤動作 ・サービス停止	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ENISA - Baseline Security Recommendations for IoT ・GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ネットワーク／プロトコル／暗号化	**TM-48：**暗号鍵を複数の装置で共有することを避け、鍵交換と鍵管理のためのセキュアな環境を確保する。	・盗聴/傍受/ハイジャック ・物理攻撃 ・サービス停止	・BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
ネットワーク／プロトコル／暗号化	**TM-49：**転送中および保管中のデータおよび情報（制御メッセージを含む）の機密性、信頼性および/または完全性を保護するための暗号の適切かつ効果的な使用を確保する。 標準規格、強力な暗号化アルゴリズム、強力な暗号鍵を適切に選択し、安全でないプロトコルを無効にする。実装の堅牢性を検証する。	・盗聴/傍受/ハイジャック	・BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations ・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems ・GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators ・Huawei - IoT Security White Paper 2017 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・OWASP (Open Web Application Security Project) - IoT Security Guidance

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
ネットワーク／プロトコル／暗号化	**TM-50：** IT および OT 環境にパッシブ監視ソリューションを実装して、産業用ネットワークトラフィックのベースラインを作成し、異常とその基準の順守を監視する。 関連する内部トラフィックをキャプチャするために、アクセスレイヤに監視ソリューションを配置する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック	・AT&T Cybersecurity Insights - Exploring IoT Security Volume 2 ・BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations ・Cloud Security Alliance - Future Proofing the connected world ・EC Alliance for Internet of Things Innovation (AIOTI) - AIOTI Digitisation of Industry Policy Recommendations ・EuroSMART (the voice of the Smart Security Industry) - Internet Of Trust Security And Privacy In The Connected World ・Federal Office for Information Security (BSI) - Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073 ・GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・Infineon - Hardware Security for Smart Grid End Point Devices ・International Telecommunications Union - Unleashing the potential of the Internet of Things ・Internet Engineering Task Force (IETF) - Best Current Practices for Securing Internet of Things (IoT) Devices ・Internet Engineering Task Force (IETF) - IETF RFC 7452 Architectural Considerations in Smart Object Networking ・Internet Research Task force (IRTF) - State-of-the-Art and Challenges for the Internet of Things Security ・IOT-A (Internet of Things Architecture) ・ISACA - Performing a Security Risk Assessment ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements #A10. Cryptography ・ISO - ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity 7.4.3 ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
			・NIST - Framework for Improving Critical Infrastructure Cybersecurity V1.1 ・NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations - SC-13 Cryptographic Protection ・oneM2M - Standards for M2M and the Internet of Things ・OWASP (Open Web Application Security Project) - Guide to Cryptography ・Software Assurance Forum for Excellence in Code (SAFECode) - NPO - Call it the Internet of Connected Things: The IoT Security Conundrum ・Symantec - Internet Security Threat Report (ISTR) Volume 22 ・Trusted Computing Group (TCG) - Guidance for Securing IoT Using TCG Technology Reference Document
監視／監査	**TM-51：**セキュリティログ（変更ログ、障害ログ、パフォーマンスログ）を収集してイベントの分析を可能にする。可能な範囲で、イベントログには、ユーザーID、システムアクティビティ、日付、時刻、および重要なイベントの詳細（ログオンおよびログオフの時刻など）、特権の使用などを含める必要がある。 専用のツール（例えば、セキュリティオペレーションセンター（SOC）内の SIEM ソリューションなど）を使用して、ログがリアルタイムでフィルタリング、関連付け、および分析されるようにする。技術的に不可能な場合は、定期的にログを手動で確認する。 リスク分析に基づいて必要なアクションを取る。 また、ログが一般に受け入れられているインタフェースを介してアクセス可能であり、定義された期間保管されていることを確認する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・Federal Office for Information Security (BSI) - BSI-Standards 100-1 - Information Security Management Systems (ISMS) ・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・LNS - Putting Industrial Cyber Security at the top of the CEO agenda ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor ・Symantec - An Internet of Things Reference Architecture ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
監視／監査	**TM-52：**少なくとも年 1 回、およびシステムの大きな変更があった場合に、アクセス権と資産構成の定期的な見直しを行う。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ENISA - Baseline Security Recommendations for IoT ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・OWASP (Open Web Application Security Project) - IoT Security Guidance ・SANS Institute - An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor ・VDC - Industry 4.0: Secure by design
監視／監査	**TM-53：**技術的に可能な場合、IIoT 機器の可用性をリアルタイムで監視する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作	・ENISA - Baseline Security Recommendations for IoT ・Huawei - IoT Security White Paper 2017 ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・OWASP (Open Web Application Security Project) - IoT Security Guidance

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
監視／監査	**TM-54：**さまざまな種類の資産に合わせたベースラインセキュリティ構成を確立する。ベースラインには、特に、システムコンポーネントに関する情報（例：インストールされる必須ソフトウェアのバージョン番号、オペレーティングシステムに関するパッチ情報、アプリケーションのホワイトリスト、必須ポート、プロトコル、機能、および設定パラメータ）、ネットワークトポロジ、システムアーキテクチャにおける論理的配置などを含める。 さらに、組織の情報システムは時間の経過とともに変化するため、ベースラインの見直しおよび新しいベースラインを作成するための手順を確立する。	・不正操作/悪用 ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・災害	・ETSI (European Telecommunications Standards Institute) - ETSI GR QSC 004 V1.1.1 (2017-03) Quantum Safe Cryptography; Quantum-Safe threat assessment ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) ・Smart Card Alliance - Embedded HW Security for IoT Applications
構成管理	**TM-55：**構成管理を可能にするメカニズムと支援ツールを導入する。このメカニズムは、変更の追跡と変更前のシステムの状態の再現が可能であること。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作 ・サービス停止 ・法規 ・災害	・Huawei - IoT Security White Paper 2017 ・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
構成管理	**TM-56：**リスク分析に基づいて組織が策定した変更管理ポリシーに従って、構成の変更を実施し文書化する。変更管理ポリシーには責任（すなわち、システム所有者、承認者など）およびセキュリティ面を含める。資産の所有者である事業主はそれを承認する。	・不正操作/悪用 ・盗聴/傍受/ハイジャック ・物理攻撃 ・偶発的な被害 ・障害/誤動作	・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISA - ANSI/ISA-95 Part 1: Models and Terminology ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
構成管理	**TM-57：**影響分析のための専用の手順を開発する。システムの変更を実施する前に、検討した変更の重要性を判断するための分析を実行する。 運用に影響を与える可能性がある構成変更をテストし、それらの前にリスク分析を行う。	・偶発的な被害	・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
構成管理	**TM-58：**IIoT ソリューションを堅牢化し、これを変更管理ポリシーに含める。未使用のネットワークポート、プロトコル、および機器の不要な機能がすべて無効になっていること、およびテスト/デバッグ機能がロックされていることを確認する。堅牢化には、運用システム、ソフトウェア、ファームウェア、およびアプリケーションを含める必要がある。 さらに、少なくとも年 1 回、およびシステムに大きな変更があった場合には、定期的に重要なものを選んでサンプリングチェックを実行する。	・偶発的な被害	・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・ISA - ANSI/ISA-95 Part 1: Models and Terminology ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security
構成管理	**TM-59：**定期的なテストの規定を含む、さまざまな種類の資産に合わせた、包括的なバックアップ計画を作成して適用する。システムのアップデートやその他の重要な変更の前にバックアップを実行する。 一部の資産については、資産の種類に応じた頻度でバックアップを定期的に作成する必要がある。 バックアップを作成するときは、それが正しく機能するかどうかを確認する（バックアップのテストを実行する）。その確認には、ハッシュを確認するか、専用のアプリケーションを使用する。	・盗聴/傍受/ハイジャック ・物理攻撃 ・障害/誤動作	・Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things ・ENISA - Baseline Security Recommendations for IoT ・IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework ・IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use ・IoT Alliance Australia - Internet of Things Security Guidelines v1.2 ・IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks ・OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation ・OWASP (Open Web Application Security Project) - IoT Security Guidance ・Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor ・Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

要件	セキュリティ対策／グッドプラクティス	脅威とリスクの分類	参照
構成管理	**TM-01：**ソフトウェアを実行する前に、ソフトウェアの完全性を確認する。 信頼のルートとセキュアブートメカニズムを確認する。ソフトウェアが信頼できるソース（ベンダーによって署名された）であることと、それがセキュアな方法で入手されていることを確認する。（例えば、暗号化された接続でダウンロードされた。）ソフトウェアが正規のものであることを確認するために、ソフトウェアの署名および/またはチェックサムの管理を実施する。	・障害/誤動作 ・サービス停止 ・災害	・IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program ・IEC - IEC 62443-3-3:2013 System security requirements and security levels ・ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements ・ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls ・NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations ・NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security ・NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

付録 C：調査したセキュリティ標準と参考文献

著者	タイトル	参照
1. EU イニシアチブ		
EC Alliance for Internet of Things Innovation (AIOTI)	AIOTI Digitisation of Industry Policy Recommendations	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Digitisation-of-Ind-policydoc-Nov-2016.pdf
ECSO (European Cyber Security Organization)	INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector	http://www.ecs-org.eu/documents/uploads/industry-40-and-ics-sector-report-032018.pdf
ENISA	Baseline Security Recommendations for IoT	https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
European Parliament and Council of the European Union	The General Data Protection Regulation (GDPR) (EU) 2016/679	https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG
IOT-A (Internet of Things Architecture)	IOT-A (Internet of Things Architecture)	http://cordis.europa.eu/project/rcn/95713_en.html http://www.meet-iot.eu/iot-a-deliverables.html
2. 米国政府のイニシアチブ		
Homeland Security	Strategic Principles for Securing the Internet of Things	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
Homeland Security	Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies	https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICSCERT_Defense_in_Depth_2016_S508C.pdf
NIST	NISTIR 8183: Cybersecurity Framework Manufacturing Profile	https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf
NIST	Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks	https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf
NIST	NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

著者	タイトル	参照
NIST	NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
NIST	NIST.SP 1500-202 - Framework for Cyber-Physical Systems: Volume 2, Working Group Reports	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-202.pdf
NIST	NIST SP 800 30r1 - Guide for Conducting Risk Assessments	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
NIST	Best practices in cyber supply chain risk management. Smart Manufacturing The Future of Manufacturing and Value Chain Competitiveness	https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-SmartManu-Cyber-SCRM-Case-Study.pdf
NIST	NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
NIST	Cybersecurity for Smart Manufacturing	https://www.nist.gov/sites/default/files/documents/2016/12/05/cybersecurity_for_smart_manufacturing.pdf
NIST	Framework for Cyber-Physical Systems: Volume 1, Overview	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf
NIST	Framework for Improving Critical Infrastructure Cybersecurity V1.1	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
NIST	NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models	https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.300-1.pdf
NIST	NIST SP 800-146 Cloud Computing Synopsis and Recommendations	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

著者	タイトル	参照
NIST	NIST SP 800-61r2: Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology	https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
NIST	NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)	https://csrc.nist.gov/publications/detail/nistir/8200/draft
3. 国際組織／団体		
Auto ISAC (Automotive Information Sharing and Analysis Center)	Automotive Cybersecurity Best Practices – Executive Summary	http://www.sovereignplc.co.uk/sites/default/files/Auto%20ISAC%20Cyber%20Security%20Best%20Practices%20Executive%20Summary.pdf
BITAG (Broadband Internet Technical Advisory Group)	Internet of Things (IoT) Security and Privacy Recommendations	https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Center for Internet Security (CIS)	Critical Security Controls	https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf
Cloud Security Alliance	Security Guidance for Early Adopters of the Internet of Things	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance	Identity and Access Management for the Internet of Things - Summary Guidance	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identityand-access-management-for-the-iot.pdf
Cloud Security Alliance	Future Proofing the connected world	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/futureproofing-the-connected-world.pdf
ETSI （European Telecommunications Standards Institute)	ETSI GR QSC 004 V1.1.1 (2017-03) Quantum Safe Cryptography; Quantum-Safe threat assessment	http://www.etsi.org/deliver/etsi_gr/QSC/001_099/004/01.01.01_60/gr_QSC004v010101p.pdf
ETSI （European Telecommunications Standards Institute)	ETSI TR 103 375 SmartM2M; IoT Standards landscape and future evolutions	http://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf

著者	タイトル	参照
ETSI (European Telecommunications Standards Institute)	ETSI TR 118 518 V2.0.0 (2016-09) oneM2M; Industrial Domain Enablement	https://www.etsi.org/deliver/etsi_tr/118500_118599/118518/02.00.00_60/tr_118518v020000p.pdf
EuroSMART (the voice of the Smart Security Industry)	Internet Of Trust Security And Privacy In The Connected World	http://www.eurosmart.com/news-publications/99-policy-papers/245-eurosmartinternet-of-trust-security-and-privacy-in-the-connected-world.html
Federal Office for Information Security (BSI)	BSI-Standards 100-4 - Business Continuity Management	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1
Federal Office for Information Security (BSI)	BSI-Standards 100-1 - Information Security Management Systems (ISMS)	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1
Federal Office for Information Security (BSI)	Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073	https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf
GSMA	GSMA CLP.11 IoT Security Guidelines Overview Document	https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.11-v1.1.pdf
GSMA	GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems	https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.12-v1.0.pdf
GSMA	GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems	https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.13-v1.0.pdf
GSMA	GSMA CLP.14 IoT Security Guidelines for Network Operators	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.14-v2.0.pdf
IEC	IEC 62443-1-1:2009 Terminology, concepts and models	https://webstore.iec.ch/publication/7029
IEC	IEC 62443-2-1:2010 Establishing an industrial automation and control system security program	https://webstore.iec.ch/publication/7030

著者	タイトル	参照
IEC	IEC 62443-3-3:2013 System security requirements and security levels	https://webstore.iec.ch/publication/7033
IEC	IEC 62443-4-1:2013 Secure product development lifecycle requirements	https://webstore.iec.ch/publication/33615
IEEE	Internet of Things (IoT) Security Best Practices	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf
IEEE	IEEE Std 802.1X-2010 - Port-Based Network Access Control	http://moodle.eece.cu.edu.eg/pluginfile.php/1799/mod_folder/content/1/802.1X-2010.pdf?forcedownload=1
IIC (Industrial Internet Consortium)	IIC Endpoint Security Best Practices	https://www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf
IIC (Industrial Internet Consortium)	Accompanying the Industrial Internet of Things Volume G1: Reference architecture	https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf
IIC (Industrial Internet Consortium)	Industrial Internet of Things Volume G4: Security Framework	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf
IIC (Industrial Internet Consortium)	IoT Security Maturity Model: Description and Intended Use	https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf
International Telecommunications Union	Security capabilities supporting safety of the Internet of things	https://www.itu.int/rec/T-REC-Y.4806/en
International Telecommunications Union	Unleashing the potential of the Internet of Things	https://www.itu.int/en/publications/Documents/tsb/2016-InternetOfThings/index.html
Internet Engineering Task Force (IETF)	Best Current Practices for Securing Internet of Things (IoT) Devices	https://www.ietf.org/proceedings/56/
Internet Engineering Task Force (IETF)	IETF RFC 7452 Architectural Considerations in Smart Object Networking	https://tools.ietf.org/html/rfc7452
Internet Research Task force (IRTF)	State-of-the-Art and Challenges for the Internet of Things Security	https://tools.ietf.org/pdf/draft-irtf-t2trg-iot-seccons-04.pdf

著者	タイトル	参照
IoT Alliance Australia	Internet of Things Security Guidelines v1.2	http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf
IoT Security Foundation	Connected Consumer Products. Best Practice Guidelines	https://iotsecurityfoundation.org/wp-content/uploads/2016/12/Connected-Consumer-Products.pdf
IoT Security Foundation	Security Challenges on the Way Towards Smart Manufacturing	https://www.iotsecurityfoundation.org/security-challenges-on-the-way-towards-smartmanufacturing/
IoT Security Foundation	Establishing Principles for IoT Security	https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf
ISA	ANSI/ISA-95 Part 1: Models and Terminology	https://www.isa.org/store/ansi/isa-950001-2010-iec-62264-1-mod-enterprise-controlsystem-integration-part-1-models-and-terminology/116636
oneM2M - Standards for M2M and the Internet of Things	TR 0008 Security V2.0.0 - Security. Technical Report	http://www.onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2_0_0.pdf
Online Trust Alliance	IoT trust framework 2.5	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
OWASP (Open Web Application Security Project)	Guide to Cryptography	https://www.owasp.org/index.php/Guide_to_Cryptography
OWASP (Open Web Application Security Project)	IoT Security Guidance	https://www.owasp.org/index.php/IoT_Security_Guidance
OWASP (Open Web Application Security Project)	Mobile Top 10 2016	https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
SANS Institute	An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity	https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICSCybersecurity.pdf
SANS Institute	Building the New Network Security Architecture for the Future	https://www.sans.org/reading-room/whitepapers/cloud/building-network-securityarchitecture-future-38255
SANS Institute	The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns	https://www.sans.org/reading-room/whitepapers/analyst/2018-industrial-iot-securitysurvey-shaping-iiot-security-concerns-38505

著者	タイトル	参照
SANS Institute	Vulnerability Management: Tools, Challenges and Best Practices	https://www.sans.org/reading-room/whitepapers/threats/vulnerability-managementtools-challenges-practices-1267
Smart Card Alliance	Embedded HW Security for IoT Applications	https://www.securetechalliance.org/downloads/Embedded-HW-Security-for-IoT-WPFINAL-December-2016.pdf
Software Assurance Forum for Excellence in Code (SAFECode) - NPO	Call it the Internet of Connected Things: The IoT Security Conundrum	http://www.safecode.org/call-it-the-internet-of-connected-things-the-iot-securityconundrum/
Trusted Computing Group (TCG)	Guidance for Securing IoT Using TCG Technology Reference Document	https://trustedcomputinggroup.org/guidance-securing-iot-using-tcg-technologyreference-document/
World Economic Forum	Industrial Internet of Things: Unleashing the Potential of Connected Products and Services	http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf
4. その他		
AT&T Cybersecurity Insights	Exploring IoT Security Volume 2	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
Elsevier	Avoiding the internet of insecure industrial things	https://www.sciencedirect.com/science/article/pii/S0267364917303217
Huawei	IoT Security White Paper 2017	https://www.huawei.com/minisite/iot/img/hw_iot_secutity_white_paper_2017_en_v2.pdf
Infineon	Hardware-based solutions secure machine identities in smart factories	https://www.infineon.com/dgdl/Infineon-IoT+Security+in+Smart+Factories-ART-v01_00-EN.pdf?fileId=5546d46254e133b40154e22c8a7d0251
Infineon	Hardware Security for Smart Grid End Point Devices	https://www.nrel.gov/esif/assets/pdfs/hardware_security_smart_grid.pdf
ISACA	Performing a Security Risk Assessment	https://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-securityrisk-assessment1.aspx
ISO	ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements	https://www.iso.org/standard/54534.html

著者	タイトル	参照
ISO	ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls	https://www.iso.org/standard/54533.html
ISO	ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity	https://www.iso.org/standard/44374.html
LNS	Putting Industrial Cyber Security at the top of the CEO agenda	https://www.honeywellprocess.com/en-US/online_campaigns/lns-cyberreport/Pages/Honeywell-LNSStudy_PuttingIndustrialCyberSecurityattheTopCEOAgenda.pdf
MIT	Security Analysis of Zigbee	https://courses.csail.mit.edu/6.857/2017/project/17.pdf
OpenAI and others	The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation	https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf
Shaun Bligh-Wall	Industry 4.0: Security imperatives for IoT — converging networks, increasing risks.	https://www.henrystewartpublications.com/sites/default/files/Bligh-Wall.pdf
Siemens	Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor	https://www.industry.usa.siemens.com/automation/us/en/formsdocs/Documents/2016%20MIA-%2023%20Industrial%20Security%20Applying%20IoT%20Security%20Controls%20on%20the%20Industrial%20Plant%20Floor.pdf
Smart Factory Innovation Forum	Managing security, safety and privacy in Smart Factories	https://www.pinsentmasons.com/dokument/it-security-in-smart-factories-white-paperapril-2015.pdf
Symantec	An Internet of Things Reference Architecture	https://www.symantec.com/content/en/us/enterprise/white_papers/iot-securityreference-architecture-wp-en.pdf
Symantec	Internet Security Threat Report (ISTR) Volume 22	https://www.symantec.com/security-center/threat-report https://resource.elq.symantec.com/LP=3980?cid=70138000001BjppAAC&mc=202671&ot=wp&tt=sw&inid=symc_threat-report_regular_to_leadgen_form_LP-3980_ISTR22-reportmain

著者	タイトル	参照
Symantec	Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future	https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf
The Cavalry	Hippocratic Oath for Connected Medical Devices	https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf
VDC	Industry 4.0: Secure by design	https://cdn2.hubspot.net/hubfs/582328/whitepapers/VDC%20-%20Industry%204.0%20Secure%20by%20Design%20-%20for%20GrammaTech.pdf?t=1519834251604
VDMA	Industrie 4.0 Security Guidelines Recommendations for actions	http://www.vdmashop.de/refs/Leitf_I40_Security_En_LR_neu.pdf
VDMA	Smart Manufacturing General security and privacy principles to ensure a Trusted IoT environment	http://ec.europa.eu/information_society/newsroom/image/document/2017-11/smart_manufacturing_to_ensure_a_trusted_iot_environment_by_vdma_0B8285E7-9C90-7E5C-04DA25B61A5C3FA5_43660.pdf
IOActive, Embedi	SCADA And Mobile Security In The Internet Of Things Era	https://ioactive.com/pdfs/SCADA-and-Mobile-Security-in-the-IoT-Era-Embedi-FINALab%20(1).pdf

付録 D：指標となるインダストリー4.0 セキュリティインシデントの説明

セキュリティインシデント	日付	説明
安全計装システム（SIS）に対する Triton マルウェア攻撃	2017 年 11 月	安全計装システム（SIS）の目的は、重要なプロセスが計画された以外の方法で実行された際に即座に介入することである。例えば、タンク内の圧力が所定のレベルを超えると、SIS は爆発を防ぐために圧力を下げるバルブを作動させる。このフェイルセーフメカニズムが阻害されると、特に産業プラントでは、深刻な物理的被害が生じる可能性がある。そのような SIS システムの 1 つが 2017 年に Triton によって攻撃された。Triton は、制御系を標的としたマルウェアで、深刻な被害を与えるように設計されていた。これは SIS に対する最初のサイバー攻撃であった。攻撃者はワークステーションへのリモートアクセスを得た後、SIS をマルウェアに感染させた。ゼロ・デイの脆弱性（まだ対策が講じられていないセキュリティ上の脆弱性）を利用して、Triton は SIS に自分自身をインストールし、攻撃者に完全な制御を与えることができた。しかし攻撃者は侵入後、攻撃に失敗し、SIS が司るセーフティシャットダウンを引き起こした。これにより従業員が介入し、マルウェアを検出し、インフラを破壊し生産を停止させる可能性がある重大な被害を引き起こす前に攻撃を停止させた。[48] [49]

[48] CyberArk (2018) “Anatomy of the Triton malware attack”: https://www.cyberark.com/threat-researchblog/anatomy-triton-malware-attack/

[49] Sentryo (2018) “Analysis of Triton industrial malware”: https://www.sentryo.net/analysis-triton-malware/

セキュリティインシデント	日付	説明
NotPetya - 損害を与えるために作成されたランサムウェア	2017 年 6 月	WannaCry からわずか 6 週間後、新たな世界規模のサイバー攻撃が発生した。攻撃者はもともとウクライナの中央銀行、政府および公共事業体（例えば送電網）を狙っていたが、その被害は人々の日常生活にまで及んだ。被害はさらに広がり、NotPetya（ExPetr、Petya とも呼ばれる）は世界中で 20 万台以上のコンピュータに感染し、Rosneft、Merck、Maersk などの多くの産業企業に影響を及ぼした。最初の感染を達成するために SMB プロトコルのエクスプロイトを使用し、次にこのエクスプロイトの影響を受けない（パッチを適用された）機器も含め、認証情報を窃取してネットワーク上の他の機器を制御しようとした。これは NotPetya を特に危険なものにした。脆弱な機器がたった 1 つでもあるとネットワーク全体が危険にさらされる可能性があるためである。感染後まもなく、NotPetya はコンピュータ上のファイルを暗号化し始めた。しかも復号が不可能な方法で暗号化した。これは、暗号化されたすべてのファイルが失われることを意味する。つまり、ウイルスはワイパーのように機能し、システムから重要なデータを削除した。これでは攻撃者は身代金を集めることができないので、NotPetya が本当にランサムウェアなのか、それともランサムウェアに偽装されたサイバー武器であるのかという疑いを引き起こした。[50] [51] [52] [53] [54]

[50] Kaspersky Lab (2017) “More than 50% of organizations attacked by ExPetr (Petya) cryptolocker are industrial companies”: https://ics-cert.kaspersky.com/alerts/2017/06/29/more-than-50-percent-of-organizations-attacked-byexpetr-petya-cryptolocker-are-industrial-companies/

[51] The New York Times (2017) “Cyberattack Hits Ukraine Then Spreads Internationally”:https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

[52] CNet (2018) “US: Russia's NotPetya the most destructive cyberattack ever”: https://www.cnet.com/news/uksaid-russia-is-behind-destructive-2017-cyberattack-in-ukraine/

[53] TechRepublic (2017) “NotPetya ransomware outbreak cost Merck more than $300M per quarter”: https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/

[54] The Register (2018) “IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz”: https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/

セキュリティインシデント	日付	説明
WannaCry ランサムウェアによる世界規模のサイバー攻撃	2017 年 5 月	この世界規模のサイバー攻撃は、150 カ国で 23 万台を超えるコンピュータに感染し、製造業者、銀行、および政府に影響を及ぼした。ルノーやホンダなどの企業は生産を中止せざるを得ず、フェデックスの顧客は配達の遅れを経験し、そして英国の国民健康サービスは何千もの予約を取り消さなければならなかった。これらはこのランサムウェアの確認された犠牲者のほんの一部に過ぎず、さらに多くの組織が感染したことを認めていない。WannaCry は、Microsoft Windows システムの 2 つの高度なセキュリティ上の弱点を悪用し、SMB プロトコルを介して拡散することができ、ユーザーが操作することなく自分自身を脆弱な機器にインストールする（悪意のある電子メール添付ファイルを開くなど）。侵入すると、他のターゲットを探すためにネットワークをスキャンし、それらすべてに感染し、そのプロセスを繰り返し、さらに感染をシステム内に広げた。幸いなことに、この攻撃はキルスイッチの発見によって減少した。キルスイッチはウイルスの大きな欠陥で、研究者がその拡散機能を「オフにする」ことを可能にし、資産所有者に彼らの装置に対策を施し、新たな感染の波に備えるための時間を与えた。これらの機器を保護するには、数ヶ月前にマイクロソフトがリリースしたセキュリティ更新プログラムをインストールするだけで済んだはずであった。
Industroyer - ウクライナの送電網で 2 度目のサイバー攻撃	2016 年 12 月 17 日	ウクライナの送電網への 2 度目のサイバー攻撃は、最初の攻撃からほぼ 1 年後に起こった。前回の攻撃と多くの類似点があったが、使われた攻撃方法が異なった。今回、攻撃者は特に送電網を攻撃するために設計された新しいマルウェア Industroyer を使用した。そのマルウェアは広く使用されている通信プロトコルを標的とし、攻撃者に ICS へのバックドアを提供した。攻撃者は再びサーキットブレーカーを開いて電力供給を停止し、重要なファイルを消去してシステムを応答しなくするなど、さらなる手段で回復を遅らせた。その結果、ウクライナの首都キエフの 5 分の 1 は、1 時間停電した。攻撃者はマルウェアの潜在能力を最大限に利用していないため、この攻撃は大規模なテストであったと疑われている。Industroyer は、水やガスなどの他の重要なインフラをターゲットにするよう変更することができるので、ICS にとって大きな脅威である。[55] [56]

[55] WeLiveSecurity (2017) “Industroyer: Biggest threat to industrial control systems since Stuxnet”: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[56] MIT Technology Review (2016) “Ukraine’s Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks”: https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-forinfrastructure-attacks/

セキュリティインシデント	日付	説明
BrickerBot - 恒久的なサービス拒否のボットネット	2016 年 11 月 – 2017 年 12 月	ICS-CERT が Mirai に似た新しいボット攻撃について注意喚起を発した。作成者によって BrickerBot と名付けられたボットは、telnet への総当たり攻撃を使用して機器へのアクセスを取得し、それを恒久的なサービス拒否状態にして所有者にその機器を再インストールまたは完全に入替せざるをえなくさせる。作成者によると、BrickerBot は約 1 年で 1000 万台を超える機器を使用不能とした。[57] [58]
Mirai - IoT ボットネット攻撃	2016 年 10 月 21 日	Mirai に感染した IoT 機器で作られたボットネットは、これまでに実行された中で最大の分散型サービス拒否（DDoS）攻撃の 1 つとされる。最も顕著な攻撃は Dyn と呼ばれる DNS サービスプロバイダだった。Dyn への世界中の最大 10 万の感染した機器からの攻撃によって、攻撃者は Twitter、Netflix、Spotify などのいくつかの人気のサービスを同時に妨害または切断することさえできた。マルウェアが非常に多くの機器を感染させた方法は、最も一般的なパスワードや、ベンダーが用意したパスワードを利用してそれらにアクセスすることだった。攻撃者はそれらのパスワードを「採用」したため、機器にはほとんど手を加えず、マルウェアの影響は受けていないように見えた。機器を自由に使えるようになった攻撃者は Dyn のように、選択した標的に大量のリクエストを送り付けるように命令し、帯域幅の制限を超えさせ、標的を破壊することができた。おそらく Mirai について最も厄介なのは、そのソースコードが公に利用可能であり、誰にでもボットネットを構築する方法を提供していることである。毎月、新しく改良された「Mirai」の亜種が発見されている。オリジナルの Mirai は特に IIoT 機器をターゲットにしていなかったが、IIoT バージョンはいつでも登場する可能性がある。[59] [60]

[57] ICS-CERT (2017) “Alert (ICS-ALERT-17-102-01A) BrickerBot Permanent Denial-of-Service Attack”: https://icscert.us-cert.gov/alerts/ICS-ALERT-17-102-01A

[58] BleepingComputer (2017) “BrickerBot Author Retires Claiming to Have Bricked over 10 Million IoT Devices”: https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/

[59] Sentryo (2016) “The ‘mirai’ iot botnet, a publically available turn-key threat”:https://www.sentryo.net/themirai-iot-botnet-a-publically-available-turn-key-threat-2/

[60] Xage Security (2016) “Mirai and IIoT Security”: https://xage.com/press/mirai-and-iiot-security/

セキュリティインシデント	日付	説明
ウクライナの送電網へのサイバー攻撃	2015 年 12 月 23 日	ウクライナの送電網へのサイバー攻撃は、綿密に計画され、慎重に準備され、完璧に実行された。攻撃者の目標は、電力供給を妨害することだけでなく、可能な限り回復を遅らせることでもあった。他の多くの攻撃と同様に、この攻撃はマルウェアが埋め込まれた悪意のある Microsoft Office ファイルを含むフィッシングメールで始まった。BlackEnergy と呼ばれるこのマルウェアは、攻撃者がき k のある認証情報を窃取し、ネットワーク情報収集を実行して、感染したシステムに関するすべての情報を見つけることを可能にした。その後 6 か月も経った後、攻撃者はリモートから SCADA システムの制御を奪い、複数のサーキットブレーカーを開き、その結果約 23 万人の人々が停電の影響を受けた。同時に、攻撃者は効果を長引かせるために多くのステップを踏んだ。 1 つ目は、感染したすべてのコンピュータのハードドライブが消去された。2 つ目は、無停電電源装置（UPS）がハッキングされ、サービスが停止した。 3 つ目は、悪意のあるファームウェアをゲートウェイ機器にアップロードすることで「橋を破壊」し、リモートからの復旧を不可能にした。これらのサイドアタックは回復を遅らせることに成功し、最大 6 時間停電した。この攻撃および防御の無力さは、多くの製造業者にとって警鐘となった。[61]
Kemuri Water Company の浄水場でのサイバー攻撃	2015 年	Kemuri Water Company（KWC）は、2015 年に浄水場のセキュリティ侵害を経験した水道会社の仮名である。古くなった OS の使用や、すべてのデータを単一の「古い」サーバー（1988 年の IBM AS / 400）に格納するなどのセキュリティ上の欠陥によって、攻撃者はオンライン決済システムの脆弱性を悪用して、KWC のすべての顧客のデータとその ICS にアクセスすることができた。次に、PLC を操作して化学物質の使用量を改ざんし、水道水の水質に影響を与えた。幸いなことに、攻撃者の主な目的は顧客の機密データを入手することであり、浄水プロセスを妨げることではなかったと考えられるため、この変更は危害を与えることはなかった。彼らの目的が異なっていたとしたら、公衆に深刻な脅威をもたらしただろう。[62]
ドイツ製鉄所への攻撃	2014 年	この攻撃は、他の多くのインシデントと同様に、従業員が開いたフィッシングメールから始まった。攻撃者は企業ネットワークに侵入すると、未だ不明の手法を使用してプラントネットワークに移動し、複数の ICS のコンポーネント（PLC、HMI、および警報システムを含む）の制御を掌握した。そして、個々のシステムを操作してそれらに障害を起こさせると、高炉のセーフティシャットダウンを妨害し、システムに深刻な物理的損傷をもたらした。[63]

[61] SANS ICS (2016) “Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case”: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[62] Sentryo (2017) “The Sentryo Files: Industries Vs. Cyberattacks Episode 5: A Water Treatment Plant Under Attack”: https://www.sentryo.net/sentryo-files-attack-water-treatment-plant/

[63] SANS ICS (2014) “German Steel Mill Cyber Attack”: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

セキュリティインシデント	日付	説明
Havex / Dragonfly - SCADA、PLC、DCS システムを標的とするリモートアクセス型のトロイの木馬	2014 年	2014 年に、Dragonfly と呼ばれるグループによって作成された新しいマルウェアに、欧米の多くの発電施設が感染したと報告された。ICS を標的とするマルウェアは、攻撃者が感染したコンピュータからファイルをアップロード、ダウンロード、実行することを可能にする 2 つのリモートアクセス型トロイの木馬（RAT）で構成されていた。その主な目的は、感染したシステムに関するデータと情報を収集することであったが、バックドアアクセスを持続的に行うことで、より悪意のあるものになる可能性がある。さらに興味深いのは、このマルウェアがどのように感染したかである。フィッシングメールや水飲み場攻撃に加えて、一部の ICS ベンダーのソフトウェアダウンロードをハッキングし、それらに RAT を植え付けたことから、やや慎重なターゲットにまで感染した。[64]
Shamoon virus - サウジアラビアの石油会社（Saudi Aramco）へのサイバー攻撃	2012 年 8 月 15 日	この攻撃は、Saudi Aramco 社の IT チームの従業員が、悪意のあるフィッシングメールを開封して攻撃者の侵入口を提供することから始まった。攻撃者は侵入した後、Shamoon と呼ばれるウイルスをインストールした。 それはすぐに Saudi Aramco 社の IT ネットワーク全体に広がり、少なくとも 35,000 台のコンピュータが感染した。 その後ウイルスは、慎重に選ばれた日付（サウジアラビアの祝日）に、感染したコンピュータ上のすべてのデータを削除し、燃えているアメリカ国旗の画像に置き換えた。そして、コンピュータのマスターブートレコードを上書きして使用不能にした。この攻撃は IT ネットワークのみに影響を及ぼし、ICS には影響はなかったが、ガソリンのトラックへの積載など、他のビジネスプロセスに大きな影響を与えた。[65]
Duqu- 進化した Stuxnet	2011 年	シマンテックによると、Duqu は「Stuxnet とほぼ同じだが、目的がまったく異なる」。Duqu は Stuxnet と同様、Microsoft Windows をターゲットとし、Microsoft Word を使用してカーネルモードでコードを実行する。 一旦機械が感染すると、Duqu の目的はそれを破壊することではなく、将来の攻撃に役立つ情報を集めることである。マカフィーによると、キーストロークとシステム情報の記録以外に、Duqu は将来使うウイルスを正規のものに見せるために使用される可能性があるデジタル証明書を盗む。分析の結果、ICS に関連するコードはなかったが、Duqu によって収集された情報は、将来的に IIoT への攻撃を可能にする恐れがある。[66]

[64] Belden (2014) “How Dragonfly Hackers and RAT Malware Threaten ICS Security”: https://www.belden.com/blog/industrial-security/how-dragonfly-hackers-and-rat-malware-threaten-ics-security

[65] CNNMoney (2015) “The inside story of the biggest hack in history”:https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html

[66] Symantec (2011) “W32.Duqu The precursor to the next Stuxnet”:
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

セキュリティインシデント	日付	説明
アメリカの浄水施設の SCADA システムへのサイバー攻撃により、ポンプの 1 台が破壊される	2011 年 11 月 8 日	この攻撃は、水道業者の SCADA ソフトウェアベンダがハッキングされ、顧客のシステムのユーザー名とパスワードのリストが盗まれることから始まった。サポートのため顧客のシステムへのアクセスを許可されているベンダーは、これらのリストを管理していることがある。攻撃者はこれらの認証情報を入手し、ポンプの制御システムにアクセスし、その破壊につながるコマンドを実行することができた。[67]
スマートメーターへの攻撃	2010 年	2010 年には、PREPA（プエルトリコ電力公社）が、スマートメーターの脆弱性を悪用する電力窃盗犯によって年間 4 億ドルの被害を被ったことが報告された。この攻撃は、光ファイバープローブ、無料で入手可能なソフトウェア、およびメーターへの物理的なアクセスのみで実行できる。その単純さのために、多くのスマートメーターの記録は改ざんされ、莫大な損失をもたらした。[68]
イランのナタンズ核施設への Stuxnet ワーム攻撃	2010 年	2010 年に、イランのナタンズ核施設の従業員は、奇妙な数のウラン濃縮遠心分離機が壊れているのに気づいた。調査の結果、プログラマブルロジックコントローラ（PLC）を標的とした Stuxnet ワームにコンピュータシステムが感染していたことが判明した。Stuxnet ワームは USB 経由でシステムに侵入したと考えられており、Microsoft Windows と Siemens Step7 の脆弱性を悪用して PLC にアクセスし、コードを改ざんし、想定外のコマンドを PLC に送信し、全て正常に見せかけるフィードバックを返した。この事件では、遠心分離機が、オペレータへの警告なしに、壊れるほどの速さで回転させられた。正式な報告は発表されていないが、Stuxnet はイランの遠心分離機のほぼ 5 分の 1 を台無しにしたと推定されている。[69]
Zotob ワームによる複数のダイムラークライスラー自動車製造工場の生産停止	2005 年 8 月 16 日	自動車メーカーのダイムラークライスラーは、2005 年に Zotob ワームによるサイバー攻撃を被った。Zotob ワームは、オンラインで広がり、Windows のプラグアンドプレイサービスの脆弱性を悪用するウイルスである。OT ネットワークと IT ネットワークがファイアウォールで分離されているにもかかわらず、Windows 2000 サーバーへパッチを適用していなかったため、ワームは複数の工場に広がり、1 時間以上にわたって 13 の工場が操業停止した。その結果、計 1,400 万ドルの大きな金銭的損失が生じた。[70]

[67] Computerworld (2011) “Apparent cyberattack destroys pump at Ill. water utility”: https://www.computerworld.com/article/2497351/cybercrime-hacking/apparent-cyberattack-destroys-pump-at-ill--water-utility.html

[68] KrebsOnSecurity (2012) “FBI: Smart Meter Hacks Likely to Spread”: https://krebsonsecurity.com/2012/04/fbismart-meter-hacks-likely-to-spread/

[69] Michael Holloway (2015) “Stuxnet Worm Attack on Iranian Nuclear Facilities”: http://large.stanford.edu/courses/2015/ph241/holloway1/

[70] Sentryo (2017) “The Sentryo Files: Industries Vs. Cyberattacks Episode 9: Cyberattack On A Car Manufacturing Plant”: https://www.sentryo.net/the-sentryo-files-daimlerchrysler-cyberattack/