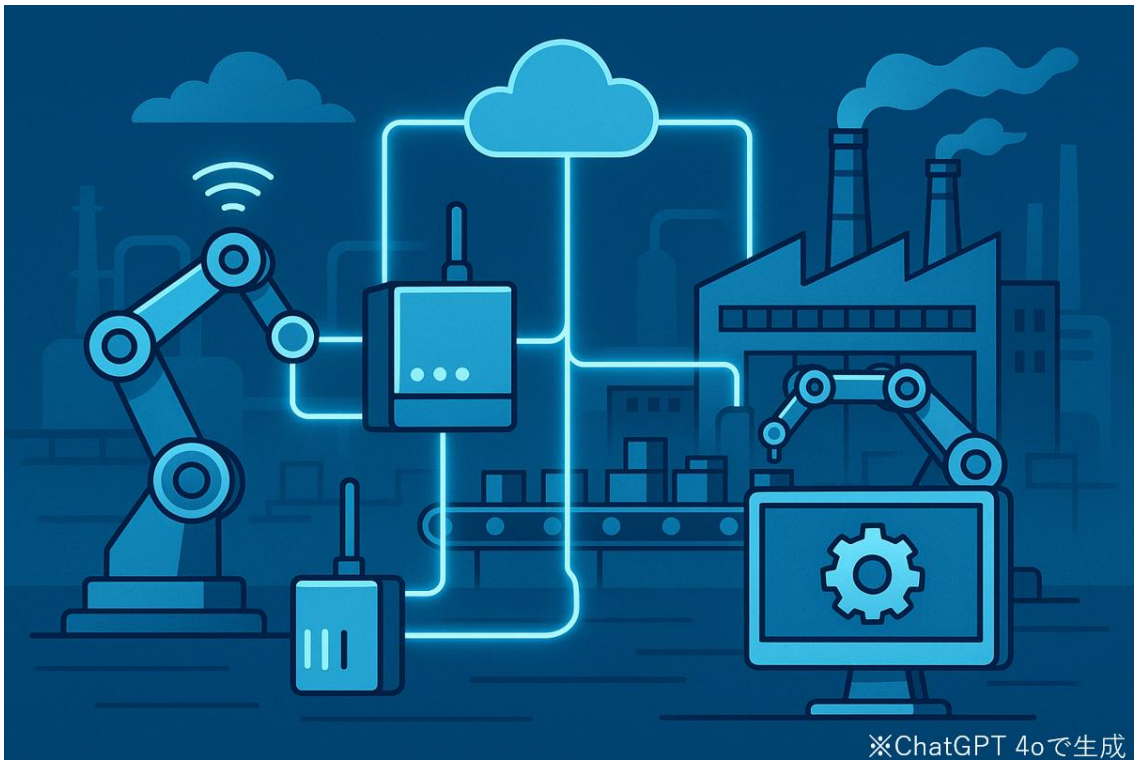
IIoT 機器ライフサイクル管理

構築手引き



2025 年 9 月 独立行政法人 情報処理推進機構

産業サイバーセキュリティセンター

中核人材育成プログラム 8 期生

Intelligent Industrial Optimization Team (IIOT)

改訂履歴

改訂年月日	改訂箇所	改定内容
2025 年 9 月 30 日	–	初版公開

目次

第 1 章　はじめに

本章では、企業が抱える IIoT 機器の課題を述べた上で、それに対する解決策としての本手引きの構成と活用方法について説明する。

1.1 まえがき

工場現場から「この IoT 機器を導入したいのだが、セキュリティ的に大丈夫だろうか？」と相談を受けたとき、セキュリティ担当者はまず何を考えるべきだろうか。一般的に考えられる確認項目として 、デフォルトのパスワードが変更可能かどうか、ファームウェアの更新情報の提供状況、クラウドとの連携有無や、どのような暗号化通信を使っているかといった、基本的な仕様や設定項目を確認することが求められる。

しかし、工場の現場に導入される IoT 機器、いわゆる IIoT（Industrial IoT）機器においては、それらに加えて、機器が接続される制御システムや現場の運用プロセスに与える影響を慎重に評価する必要がある。例えば、PLC や SCADA でも同じように、重要な設備と直接または間接的に接続される場合、誤った設定や管理ミスが制御系全体の挙動に影響を与え、最悪の場合、生産ラインの停止や品質不良、ひいては人的な安全リスクにまで発展する恐れがあるからである。

現場の担当者からは「セキュリティ的に問題がないか確認してほしい」、「そもそも導入までのフローが定まっておらず、毎回時間がかかる」といった悩みも聞かれる。セキュリティ担当者としても、「IIoT 機器に関する明確なガイドラインがなく、どの観点で導入可否を判断すべきかわからない」、「機器が導入された後に、どのように運用されているかの情報が収集できていない」といった声は少なくない。つまり、IIoT 機器の導入は技術面だけでなく、組織的・制度的な整備ができていないことにより、多くの現場で手探りかつ、属人的な対応となっている。

加えて、IIoT 機器のセキュリティリスクは、導入時点で完結するものではない。実際には、導入された機器が適切に設定され、ポリシーに沿って運用されているかを継続的にし、必要に応じてアップデートやパッチの適用、設定変更を行っていく体制が必

要である。さらに導入時にチェックを実施している企業においても、「導入前にセキュリティチェックを実施したから安全である」と認識してしまい、その後の管理や廃棄フェーズにまで目が届いていないのが現実である。

IIoT 機器のセキュリティを真に確保するためには、導入前のリスク評価、導入後の設定確認、機器の廃棄時におけるデータ抹消まで、ライフサイクル全体を視野に入れた管理が不可欠である。これが欠けると、後に想定外のトラブルやインシデントに発展するリスクを抱えることになり、導入の効果が損なわれかねない。

本手引きでは、このような背景を踏まえ、IIoT 機器のセキュリティをどのように考え、どう実施していくべきかを体系的にまとめる。導入の判断基準、関係部門との連携、運用中の管理、そして廃棄時の対応まで、セキュリティ担当者が知っておくべき視点を提示している。

本手引きを通じて、本社セキュリティ部門と現場の関係構築に寄与し、円滑かつセキュアな IIoT 機器ライフサイクル管理の一歩となることを願っている。

1.2 本手引きの想定読者

本手引きは、国内の重要インフラ事業者における本社セキュリティ部門担当者を主な読者として想定している。IIoT 機器に関するセキュリティのライフサイクル管理について解説しており、企業として、IIoT 機器をどのようにライフサイクル全体で管理していくかを検討するための参考資料となることを目的としている。そのため、本手引きは、セキュリティに関する社内ルールの策定や体制整備を担う部署・担当者を対象としている。

さらに、本内容は IIoT 機器導入の申請部門をもっている企業においても同様に活用が可能と考えている。

1.3 本手引きの構成

第 2 章では、IIoT 機器を取り巻くセキュリティの全体像について述べる。現在、IIoT 機器を巡るセキュリティ環境は様々な脅威やリスクにさらされている。それに伴い、日本を含む各国では IIoT 機器を対象としたガイドライン整備や認証制度の運用が進みつつある。本章ではこれらのガイドラインや認証制度について内容を整理する。

第 3 章では、第 1 章の内容を踏まえ、IIoT 機器特有の課題や、本手引きの目的について示す。また、本章では IIoT 機器を用途と利用ケースに応じて分類し、それらがどのような環境で運用されるかを整理する。

第 4 章では、IIoT 機器のセキュリティを確保するためにセキュリティ部門が実施すべき項目をライフサイクル全体にわたり提案する。IIoT 機器は導入から廃棄に至るまで複数のフェーズを経て運用され、それぞれのフェーズで異なるリスクと対策が求められる。本章では、関係部門の役割を明確にしたうえで、各フェーズで必要となるセキュリティ要件を整理する。

第 5 章では、第 2 章から第 4 章までの内容を総括し、IIoT 機器におけるセキュリティ全体像を総論として示す。

1.4 免責事項

- 本手引きは、独立行政法人情報処理推進機構（IPA）および産業サイバーセキュリティセンターの公式な見解を示すものではなく、本プロジェクトとしての考えに基づいて作成したものである。
- 情報提供を目的としており、内容は予告なく変更や更新が行われることがある。
- 本手引きの記載内容について、発行元の了承なしに転載や複製を行うことは認められていない。
- 正確さや完全性、特定の用途への適合性について、本手引きの内容にはいかなる保証も含まれない。明示か黙示かを問わず、商品性や目的適合性に関する保証も一切行っていない。
- 本手引きを利用したことによって生じた不利益や損害について、作成や監修に関わった者は責任を負わないものとする。

第 2 章　IIoT 機器のセキュリティを巡る概況

本章では、IIoT 機器を取り巻くセキュリティリスクの現状と、その制度的・認証的な対応の全体像を明らかにする。

2.1 IIoT 機器を取り巻くセキュリティ環境

本節では、IIoT 機器の特徴や普及状況を踏まえつつ、現場で顕在化しているセキュリティ課題と具体的な被害事例を整理する。

2.1.1 IoT 機器と IIoT 機器

IoT（Internet of Things）は、「モノのインターネット」と訳され、さまざまな機器がインターネットを通じて相互に接続され、データを送受信する仕組みであり、接続する機器を IoT 機器と呼ぶ。身近な例としては、スマートスピーカー、スマート家電、ウェアラブルデバイスなどが挙げられる。これらの機器はセンサやネットワーク機能を備え、利便性や効率性の向上に大きく寄与している。

一方、IIoT（Industrial IoT）は、IoT の技術を産業分野に応用した IoT 機器である。工場やプラント、エネルギーインフラ、交通システムといった社会基盤において、センサ、制御機器、監視装置などがネットワークを介して接続され、リアルタイムに情報を収集・分析・制御することを可能にしている。IIoT 機器には、産業用センサ、RTU（Remote Terminal Unit）、ゲートウェイ、エッジデバイス、クラウド連携デバイスなどが含まれる。

IIoT 機器の大きな特徴は、物理的な制御・監視を担う OT（Operational Technology）領域と、情報処理を担う IT（Information Technology）領域を跨ぐ点にある。これにより、生産性や稼働率の向上、予知保全の実現などの利点が得られる一方で、サイバーセキュリティの観点では新たなリスクを招くことにもなる。

IIoT 機器が運用される制御系ネットワークは本来、物理的に隔離されたクローズドな環境で運用されていたが、近年ではリモート監視やクラウド連携を目的とした外部接続が進んでおり、セキュリティ上の脅威が顕在化しつつある。

2.1.2 IIoT 機器におけるセキュリティリスクと被害事例

制御機器や IIoT 機器がネットワークを通じて相互接続されることで、情報を収集・分析・制御遠隔監視、制御、データ収集といった多くの利便性が実現されている。一方で、インターネットやクラウドとの接続により、従来の制御システムでは想定されていなかったサイバー空間からの攻撃リスクが顕在化している。以下に主なリスクが発生する要因を挙げる。

- 認証・暗号化機構の不備

組込み OS やリソース制約のある機器では、通信暗号化や認証機能が未実装または初期設定のまま運用されている例が多く見られる。特に、初期パスワードが変更されずに残っているケースは攻撃の糸口となりやすい。

- ソフトウェア更新の困難性

IIoT 機器は工場やプラントに長期にわたり設置され、再起動やアップデートによる停止が生産に影響するため、セキュリティパッチの適用が後回しになりやすい。そのため、既知の脆弱性が長期間放置される傾向がある。

- サプライチェーンに起因するリスク

機器は複数の企業・地域で製造されたハードウェアやソフトウェアで構成されており、設計者が把握していない脆弱性やマルウェアが混入するリスクがある。信頼性の評価やトレーサビリティが求められる。

これらのリスクが現実に被害として顕在化した事例も多数報告されている。例として、2017 年に世界的に猛威を振るった WannaCry ランサムウェアの感染拡大は、IIoT 機器を含む制御システムにも深刻な影響を及ぼした。WannaCry は、Windows の SMBv1 の脆弱性（EternalBlue）を突いて自己拡散するワーム型ランサムウェアである。米セキュリティ企業 Armis の調査では、製造環境に設置されていた Windows ベースの HMI が WannaCry に感染していることが確認された。この HMI からは SMBv1

を利用した異常なトラフィックが観測され、脅威検知システムが感染を検知したが、現場では長期間気付かれないまま稼働を続けていた。これは、企業が運用していた Windows ベースの HMI やエンジニアリング端末に対するセキュリティ管理の不備が要因であり、制御環境で用いられる機器が一般的な IT マルウェアの被害対象になり得ることを示している。[1]

また、2016 年に出現した Mirai マルウェアも、IoT 機器におけるセキュリティの脆弱性が悪用された典型例である。Mirai マルウェアは監視カメラや DVR、ルーター等の IoT 機器に対して、出荷時のままの初期（デフォルト）ユーザ名・パスワードを突く辞書攻撃で感染を拡大し、数十万台規模のボットネットを形成した。このボットネットは大規模な DDoS 攻撃に利用され、Krebs on Security やフランスのホスティング事業者への攻撃をはじめ、DNS サービス事業者 Dyn に対する 2016 年 10 月の攻撃に参加して東部米国で多数の主要サービス（Amazon, Reddit, Netflix 等）の一時的なアクセス障害を引き起こしたと報告されており[2]、Mirai の亜種や派生型は現在も活動を継続しており、規模は増加傾向にある。

こうした攻撃の根本原因は、機器単体の脆弱性のみならず、その脆弱性がライフサイクル全体で放置されていることにある。IIoT 機器は設計、製造、導入、運用、保守、廃棄という長期にわたるプロセスを経るが、その各フェーズでセキュリティを意識した管理が実施されていないと、想定外のタイミングや箇所でこれをアタックベクターとした攻撃が発生する。

こうした背景を受け、日本では情報通信研究機構（NICT）と総務省が連携し、2019

---

[1] Armis - HMI Machine Infected with WannaCry

https://www.armis.com/blog/hmi-machine-infected-with-wannacry/?utm_source=chatgpt.com&__cf_chl_f_tk=mysHih_MSRgt_gtjr_RYnSFi8ACR.QQx9Akg4Er61l0-1756540046-1.0.1.1-M.eTQ4BiGujxzoy1UOq2zo.rPhp3UYO7.LBms8kxSg8

[2] Krebs on Security - Hacked Cameras, DVRs Powered Today's Massive Internet Outage

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/?utm_source=chatgpt.com

年より「NOTICE（National Operation Towards IoT Clean Environment）」[3]プロジェクトを開始している。これは、脆弱な IoT 機器がインターネットに接続されていないかを自動的に調査し、脆弱な機器の所有者に対してインターネットサービスプロバイダ（ISP）を通じた注意喚起を行う取り組みである。

さらに、IoT 機器のセキュリティを製品選定段階で評価できるよう、経済産業省は「JC-STAR[4]」の認証制度運用を 2025 年 3 月より開始しており、IoT 機器のセキュリティ確保を支援する取り組みが国を挙げて促進されている。

IIoT 機器のサイバーセキュリティインシデントは、生産停止や業務影響にとどまらず、人命・環境・インフラに対する物理的被害につながる可能性もある。そのため、他の IT 機器以上に慎重かつ長期的な視点でのセキュリティ管理が求められる。

次章では、先ほど触れた JC-STAR に始まり、IoT・IIoT 機器に関連する主な認証制度やガイドラインを概観し、各国におけるセキュリティ確保の枠組みを紹介する。

---

[3] NOTICE （National Operation Towards IoT Clean Environment）

https://notice.go.jp/

[4] セキュリティ要件適合評価及びラベリング制度(JC-STAR)

https://www.ipa.go.jp/security/jc-star/detail.html

2.2 IIoT 機器のセキュリティ制度・認証制度

本節では、IIoT 機器の安全性を確保するための国内外の制度や認証制度について、その目的、構造、運用状況を概観する。

2.2.1 IIoT 機器におけるセキュリティ制度の必要性と背景

IIoT 機器は、生産現場や社会インフラを支える重要な構成要素であると同時に、IT と OT の境界に位置する特性から、多様なサイバーリスクに晒されている。1.1 節で述べたように、脆弱な構成や長期運用、クラウド接続といった要因が複雑に絡み合い、従来型の IT セキュリティ対策だけでは十分とは言えない状況が続いている。

こうした背景から、機器そのもののセキュリティ品質を客観的に評価し、一定水準以上であることを可視化・保証する枠組みとして、制度化の必要性が高まっている。

特に、製品を導入するユーザが、機器のセキュリティ対応状況を判断できる「物差し」として、セキュリティ認証制度の整備は不可欠である。

日本ではこの流れを受け、1.1.2 項で紹介した経済産業省が中心となって策定した「JC-STAR」の認証制度が 2025 年 3 月より開始している。JC-STAR は、IIoT 機器を含む IoT 機器製品におけるセキュリティ機能の有無や設計思想、脆弱性管理の体制などを第三者機関が評価し、製品の信頼性を担保する仕組みである。これにより、ユーザは導入前の製品選定段階でセキュリティレベルを比較検討できるようになる。

また国際的にも、IoT・IIoT 機器のセキュリティを法制度で規定する動きが加速している。欧州連合（EU）では、Cyber Resilience Act（CRA）[5]を制定し、製品のライフサイクル全体を通じたセキュリティ確保を義務化する新たな枠組みが構築されつつある。

このように、国内外において製品セキュリティを制度的に担保する動きが本格化しており、今後はガイドラインやフレームワークとの連携を含めた、実効性のある運用体制の構築が必要となる。

---

[5] CRA(Cyber Resilience Act)

https://www.cyberresilienceact.eu/the-cyber-resilience-act/

次節では、IoT・IIoT 機器に関連する JC-STAR を含むセキュリティ認証制度や代表的なガイドラインの具体的な内容について整理する。

2.2.2 認証制度

(a) JC-STAR

JC-STAR は、経済産業省が主導し、2024 年に導入された日本の IoT 製品向けセキュリティ認証制度である。機器の導入判断においてセキュリティ水準を「見える化」し、調達者・運用者の判断支援と製品ベンダーの取り組み促進を目的としている。制度では、製品が独立行政法人情報処理推進機構(IPA)によって定められた適合基準を満たしているかを自己適合(☆1・☆2)または第三者認証(☆3)により評価し、「JC-STAR ラベル」を付与できる。ラベルには QR コードがあり、評価結果や更新・脆弱性対応状況などの情報を確認可能である。

運用主体	経済産業省
制度運営	IPA がスキームオーナーとして制度を実施
評価方式	☆1・☆2 は製品ベンダーによる自己適合宣言(評価ガイドに基づいた文書審査等) ☆3 以上は第三者認証(IPA 認定機関による審査・IPA による認証)
対象	IP 通信機能を持ち、データの送受信を行う IoT 製品および付随するサービス。産業用(IIoT)製品も対象に含む
非対象	PC やスマートフォン等の汎用 IT 機器 ただし、セキュリティ対策をユーザが施せない場合は対象となることがある

本制度は、スマート家電から産業用装置までを広くカバーしており、特に政府機関・重要インフラ・地方公共団体の調達要件としての活用が今後進められる。

評価はライフサイクル全体(設計・運用・更新)を含み、国際基準(ETSI EN 303 645、NISTIR 8425、CRA など)との整合性も意識されている。今後は海外制度との相互認証も視野に入れ、国際展開を見据えた制度として位置づけられている。

(b) Cyber Resilience Act

Cyber Resilience Act（CRA） は、欧州連合（EU）が 2024 年 10 月に制定した製品のサイバーセキュリティ確保に関する包括的な法制度であり、正式名称は「Regulation (EU) 2024/2847」である。本制度は、デジタル要素を含むすべての製品に横断的なセキュリティ要件を課す世界初の包括的な法制度であり、EU の内部市場に流通する製品のセキュリティ強化を目的としている。

制定主体	欧州議会および欧州連合理事会
施行日	2024 年 10 月 23 日（Regulation (EU) 2024/2847 として公布）
適用開始	段階的に実施予定（2027 年頃までに完全適用が見込まれる）
対象	・ソフトウェアおよびハードウェア製品 ※ネットワーク接続の有無を問わず ・スマート家電、IoT デバイス、エンタープライズ向け IT 製品、産業用制御機器（IIoT 含む） など
非対象	医療機器、自動車機器、有線のみの製品、既存のEU 法令でサイバー対策が規定されている製品

CRA では、製造者に対して次のような要件が課される

- 製品のライフサイクル全体にわたるセキュリティの確保
- 既知の脆弱性の特定・是正
- セキュリティ更新の提供とその期間の明示
- 脆弱性開示体制の整備（Coordinated Vulnerability Disclosure）
- 適合評価および CE マークの取得

これらはすべて製品の市場投入前に実施されるべき要件として規定されており、違反が確認された場合には制裁金（最大で製品年間売上の 2.5%）が科される可能性がある。

この CRA の根底にあるのは、「セキュリティ・バイ・デザイン」の原則である。製造者が設計フェーズからセキュリティを考慮し、出荷時点で既知の脆弱性がない状態で市場に出すことを法的に義務付けている点が大きな特徴である。さらに、製品のライフサイクル全体にわたるセキュリティ確保や、脆弱性情報の共有体制の整備を義務付けており、セキュリティの継続的な担保とインシデント対応力の強化も求められている。

加えて、CRA は欧州市場における法的統一性を確保し、各国が個別にサイバー要件を課すような規制の断片化（fragmentation）を防ぐことも目指している。これにより、製造者や輸入業者にとっての負担が軽減され、EU 域内での製品の自由な流通が促進されることが期待されている。

(c) Cyber Trust Mark[6]

Cyber Trust Mark は、アメリカの連邦通信委員会（FCC）が 2024 年 3 月に正式に導入した、IoT 製品向けのサイバーセキュリティラベリング制度である。本制度は、消費者が IoT 製品のセキュリティ水準を簡単に判断できるようにすることを目的とした任意制度であり、米国政府のサイバーセキュリティ強化策の一環として位置づけられている。

この制度では、対象となる製品が FCC の定める最低限のセキュリティ基準を満たしていることを確認することで、製品に「Cyber Trust Mark」（サイバー信頼マーク）を表示することができる。マークには QR コードも付与されており、それを読み取ることで消費者は製品のセキュリティ情報（例：更新期間、認証機能、暗号化の有無など）を確認できるようになっている。

[6] Cyber Trust Mark

https://www.fcc.gov/CyberTrustMark

運用主体	米国連邦通信委員会（FCC）
制度運営	FCC が制度設計を行い、実際のラベリング認可や監査などは「Cybersecurity Label Administrators（CLAs）」という民間組織が担う。
評価方式	CLAs が認定する試験機関で製品が試験を受け、適合すれば申請のうえ認可を得てラベルを表示できる。
対象	Wi-Fi や Bluetooth 等を利用する消費者向けワイヤレス IoT 製品
非対象	医療機器、自動車機器、有線のみの製品、既存の連邦法でサイバー対策が規定されている製品

なお、産業用（IIoT）製品は現時点では対象外となっているが、将来的な対象範囲の拡大も検討されている。また、本制度は NIST（米国標準技術研究所）が策定したガイドライン（NISTIR 8259、8425 など）に準拠しており、国際的な相互運用性を視野に入れている。

この制度の最大の狙いは、消費者にとって分かりやすい指標を提供することで、市場全体での「セキュリティ・バイ・デザイン」を促進することにある。加えて、製造業者が製品セキュリティを向上させるインセンティブとなり、サプライチェーン全体のリスク低減にもつながると期待されている。

2.2.3 ガイドライン

(a) 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン[7]

本ガイドラインは、経済産業省が中心となって策定したものであり、製造業における

[7] 工場システムにおける サイバー・フィジカル・セキュリティ対策ガイドライン Ver1.1

https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.1.pdf

工場システム（制御・情報・物理システム）を対象に、サイバー攻撃への対策を「サイバー」、「フィジカル」、「マネジメント」の三つの観点から包括的に整理している。その目的は、経営層から現場までが一体となって工場システム全体のリスクを管理し、現実的かつ持続可能なセキュリティ対策を実装できるよう支援することにある。
このガイドラインは、事業継続性の確保を重視しつつ、工場システム全体の現実的なセキュリティ対策を段階的に導入するための支援策を示したものである。対象とする工場システムは、制御・情報・物理の各システムに加え、サプライチェーンなど外部要素も含む多層的な構造を想定しており、参考情報として「管理」「システム」「フィジカル」の 3 レイヤでの視点から対策例を提示している。なお、これらのレイヤは一律の適用を求めるものではなく、各組織のリスク状況や体制に応じて柔軟に参照することが想定されている。

- レイヤ 1（管理レイヤ）：経営層や本社セキュリティ部門が対象。セキュリティポリシーの策定、リスク評価、責任体制の明確化などが含まれる。
- レイヤ 2（システムレイヤ）：工場全体のシステム設計・構築・運用に関わる層。ゾーニングや認証・認可、ログ管理、資産管理などが中心。
- レイヤ 3（フィジカルレイヤ）：設備・機器の物理的な保護、現場オペレーションの安全確保、侵入検知・妨害対策などが該当する。

加えて、各レイヤに対して、それぞれ「成熟度モデル」が設定されており、段階的にセキュリティレベルを引き上げる指針として活用できる構成になっている。さらに、ISO/IEC 27001 や IEC 62443 などの国際規格とのマッピングも付されており、自社の既存体制との整合性確認にも利用できる。

工場システムにおけるセキュリティ対策は、単に IT 対策にとどまらず、現場作業や物理セキュリティも含めたサイバー・フィジカル・システム（CPS）全体の保護が必要である。本ガイドラインはその実装に向けた実践的な指針であり、特に IIoT 機器の導入・管理において、組織横断的な対応を可能にする手引きとして活用できる。

(b) 電力制御システムセキュリティガイドライン[8]

本ガイドラインは、電力業界におけるサイバーセキュリティ対策の強化を目的として策定された指針であり、旧一般電気事業者や新電力、制御システム提供事業者など、広範な関係者の協力を得て整備されたものである。ガイドラインの発端は、2013年度に経済産業省が実施した委託調査「電力システムのサイバーセキュリティ対策」であり、その提言を踏まえて 2015 年 6 月に日本電気技術規格委員会（JESC）により設置された情報専門部会において、本ガイドラインの検討が本格的に開始された。

本ガイドラインは、電力制御システム等のライフサイクルにおけるサイバーセキュリティ確保を目的としており、計画・設計から運用・保守、廃止に至る各フェーズにおいて、電気事業者が実施すべき要求事項を包括的に示している。

また、単なる技術的対応にとどまらず、組織ガバナンスや教育体制、情報共有といった運用面も重視しており、サイバーとフィジカル両面からの対策を総合的に講じることの重要性を強調している。

(c) スマートメータシステムセキュリティガイドライン[9]

本ガイドラインは、スマートメーターシステムのセキュリティ確保を目的として、一般送配電事業者が講ずべき具体的な対策事項を体系的に整理したものである。制定の背景には、電力の小売全面自由化を受けて本格導入が進んだスマートメーターの普及に伴い、その通信機能や遠隔操作機能を狙ったサイバー攻撃への懸念が高まったことがある。

本ガイドラインは、ISO/IEC 27001 および 27002 の情報セキュリティマネジメント規格をベースとしつつ、米国 NISTIR 7628 や国内ワーキンググループの報告書も参照

---

[8] 電力制御システムセキュリティガイドライン JEAG 1111-2019
発行「一般社団法人 日本電気協会 情報専門部会」　令和元年 10 月 25 日第 2 版

[9] スマートメータシステムセキュリティガイドライン JEAG 1101-2019
発行「一般社団法人 日本電気協会 情報専門部会」　令和元年 10 月 25 日第 2 版

しており、既存の ISMS 体制との整合性を重視した構成となっている。特に、セキュリティ対策を段階的・重層的に実施する「多層防御アプローチ」が採用されており、想定される脅威に対し冗長性と持続性のある防御策を講じる方針を示している。

ガイドライン全体は、システムのライフサイクル（設計・開発・調達・運用・保守・廃止）を網羅しつつ、次のような主要テーマに分類されている。

- 組織体制：経営層の責任明確化、セキュリティ管理組織の設置、教育訓練の実施
- 文書と報告：セキュリティ関連情報の文書化と管理、定期的な報告体制の確立
- システム・通信・機器の管理：暗号や認証、コマンド制御、ファームウェア管理など技術的対策
- 運用と物理対策：アクセス管理、ログ管理、物理施設や端末の保護
- 事故対応と継続性確保：セキュリティ事象の検知・報告・訓練と、サービス継続管理の確保

また、ガイドライン内では、セキュリティ項目に対し「勧告」、「推奨」といった適用レベルが明示されており、重要性に応じた柔軟な運用が可能となっている。

本ガイドラインは、スマートメーターという社会インフラの一端を担うシステムにおけるセキュリティの信頼性を高めることを目的としており、特に委託先を含む関係者全体での共通理解と実行力が求められる。今後の運用においても、情報共有や監査による継続的改善が重視され、セキュリティ事故の予防と迅速な対応を可能とする枠組みづくりが期待されている。

(d) IISF (Industry IoT Security Framework)[10]

[10] Industry IoT Security Framework An Industry IoT Framework Publication Version 2.0-2023-06-12
https://www.iiconsortium.org/wp-content/uploads/sites/2/2023/06/IISF-Version-2.pdf

本フレームワークは、産業用 IoT（IIoT）システムの信頼性・セキュリティを確保するために、広範な業種・関係者が参画して策定された包括的な指針である。エネルギー、製造、医療、輸送、公共分野など、IIoT の導入が進む領域において、制御システムと IT 環境が高度に統合されるなか、物理世界と接続された多様なエンドポイントのセキュリティが重要性を増している。

本フレームワークでは、IIoT システムを従来の IT/OT と異なる存在として捉え、「信頼性（Trustworthiness）」の確保を中核概念に据えており、セキュリティ、安全性、信頼性、レジリエンス、プライバシーの 5 特性をバランスよく備える必要性が強調されている。IT がセキュリティを、OT が可用性を優先する傾向にあるのに対し、IIoT ではそれらを統合した全体最適が求められる。

構成は、全体を通じてビジネス観点、実装観点の双方からセキュリティを体系的に整理している。具体的には、まず「リスク管理」を核としたビジネス観点を提示し、運用ユーザ、システムビルダー、コンポーネントビルダーといった異なる関係者の役割と責任を定義している。また、IoT セキュリティ成熟度モデル（SMM）を導入し、関係者が自組織のセキュリティ能力を自己評価・向上できる仕組みを提供している。

技術的対策においては、「信頼性を実現する機能ブロック」として以下の 6 領域に分類されている。

- エンドポイント保護：ID 管理、セキュアブート、物理・ハードウェアセキュリティの導入
- 通信および接続保護：認証・暗号によるトラフィック保護と情報フロー制御
- セキュリティ監視と分析：全体状態の監視とインシデント検知のサイクル運用
- 構成と管理：セキュリティ制御と信頼性維持のための一元的設定管理
- データ保護：保管中・通信中・使用中の機密性・完全性・可用性の保持
- セキュリティポリシー：ライフサイクル全体を対象とした方針と統制

さらに付録では、各業界における標準や規制、技術と要件の対応、用語集・参考文

献が整理されており、実践的な導入支援も想定されている。

なお、IISF は技術仕様の遵守を強制する文書ではなく、規範的なガイドラインとして位置付けられている。将来の技術進化やセキュリティ脅威の変化にも対応可能な柔軟性を備えつつ、IIoT の安全な普及と信頼性向上に資する実装指針として、国際的にも参照されるフレームワークとなっている。

第 3 章　IIoT 機器の課題と本手引きにおける定義

本章では、IIoT 機器の導入・運用にかかわる主要な課題と、その現状について示す。

3.1 IIoT 機器における課題

前章で述べた通り、各国のガイドラインや認証制度においては、IIoT 機器のライフサイクル全体にわたる運用が重要視されている。しかし、企業現場では実際にその運用が十分に実践されていないのが現状である。IIoT 機器の導入にあたっては、ライフサイクル全体を対象とした包括的な運用体制の構築が急務である。

本手引きでは、IIoT 機器の導入に際し、以下のような 3 つの課題が存在すると考える。

(a)ドキュメントの不足

IIoT 機器導入時に参照すべき社内のガイドラインや基準が整備されておらず、申請部門における導入判断が困難となっている。

(b)IIoT として利用する IoT 機器の範囲が不明

IIoT 機器としての対象範囲が不明のため、結果としてすべての機器に対して一律にセキュリティチェックを行う必要が生じ、工数過多となっている。

(c)ライフサイクル管理の未整備

IIoT 機器の導入から廃棄に至るまでのライフサイクル全体を通じた管理体制が 構築されておらず、運用・保守および更新計画が属人的かつ場当たり的になっている。

これらの課題について、実際の企業では同様の課題を持っているか調査を行った。調査対象としては、中核人材育成プログラムを修了した 1 期生～7 期生を対象に上記 3 つの課題に対する質問をし、合計 26 社(有効件数 13 社)の回答を収集した。

その結果、「ドキュメント不足」の課題については、調査対象の約 47%もの企業についてドキュメント類の整備がなされていた。一方で「IIoT 機器の定義の不明確さ」の課題については約 31%の企業しか IIoT 機器の定義がされておらず、「ライフサイクル管理の未整備」の課題については約 8%の企業しか整備していないことがわかった。

なお、全体の回答結果は別途 Appendix に掲載している。

3.2 本手引きの目的

本手引きは、「制御システムで使用される IIoT 機器」に対し、その導入から廃棄までを一貫して管理するためのライフサイクル管理の基本的な枠組みを提示することを目的とする。

また、本手引きを通じて、本社のセキュリティ部門と申請部門が連携し、組織内における IIoT 機器のライフサイクル全体にわたる役割と責任を明確化することで、セキュアかつ効率的な管理体制を構築することを目指す。

3.3 IIoT 機器の分類

本手引きでは IIoT 機器を用途と利用ケースで分類する。

(a)IIoT 機器の用途

(b)IIoT 機器の利用ケース

(a)IIoT 機器の用途

IIoT 機器の用途を以下のように 3 つに分類する。

① 制御

現場の生産設備や装置の動作を直接制御する。

リアルタイムでの制御信号のやり取りを行い、製造ラインやプロセス機器の安定稼働を支える役割を担う。

② 予測・分析

機器の稼働状況や生産データをもとに、状態の可視化や異常の兆候把握、エネルギーの最適化などを行う。

生産性向上やトラブル予防、メンテナンスの効率化を目的として導入されることが多い。

③ 蓄積

センサや制御機器から得られたデータを保存・蓄積する。

データを一時的または長期的に保持し、上位システムとの連携や分析処理に備える役割を持つ。

(b) IIoT 機器の利用ケース

IIoT 機器の利用ケースを以下のように 2 つに分類する。

① 本番利用（Production Use）

定義

IIoT 機器が、実際の制御系ネットワーク上に恒常的に配置され、生産設備や装置の動作に関与する形で運用される状態を指す。

特徴

・生産プロセスに直結するため、可用性や安定性が強く求められる

・操作ミスや不具合が発生した場合、品質や安全、操業への影響が大きい

・セキュリティや運用手順に関して、厳格な管理体制が必要となる

② 検証利用（PoC・概念検証利用）

定義

IIoT 機器の性能評価や有用性の検討を目的として、一時的・限定的に実施される検証的な利用を指す。PoC（Proof of Concept：概念実証）などが該当する。

特徴

・実際の生産系には接続されず、独立または仮想的な環境で試験される

・導入判断や運用設計の前段階として活用される

・柔軟性やスピード感が重視される一方で、一定のセキュリティ対策も必要

以上、これらの機器用途と利用ケースの2軸により、後述する3章でリスク評価やチェックシートの適用範囲が定義される。

3.4 IIoT 機器のインフラ構成

本節では、IIoT 機器が運用される環境の主要な特徴とそのインフラ構成について解説する。

3.4.1 IIoT 機器が利用される環境の特徴

IIoT 機器のインフラ構成には以下のように4つの特徴がある。

(a)ハイブリッドな通信環境

多様なプロトコルへの対応：IP ベースのプロトコルに対応している場合が多いため、HTTP や SMB などの IT 系プロトコルと、OPC-UA、Modbus といった OT 系プロトコルの双方を使用する。

IIoT 機器の用途に応じた目的により、24 時間ネットワーク接続されることがある。

(b)長期運用を前提とした設計

更新の困難性： IIoT 機器は、制御システムと同様に長期運用を前提として導入されることが多く、パッチ適用や機能更新が制限される傾向がある。このため、最新のセキュリティ要件への即応が難しく、結果としてセキュリティリスクが長期にわたり残存する可能性がある。

(c)IT と OT の融合と連携

部門間の統合管理：IT 部門による認証・通信管理と、OT 部門による現場運用が協調して管理する必要がある。

(d)サイバーとフィジカル両面からの保護

サイバーフィジカル観点でのリスク対策：IIoT 機器は物理的なプロセス制御に直接影響を与えるため、ネットワーク設計や機器構成は、サイバーとフィジカルの両視点から

保護を講じる必要がある。

3.4.2 インフラ構成

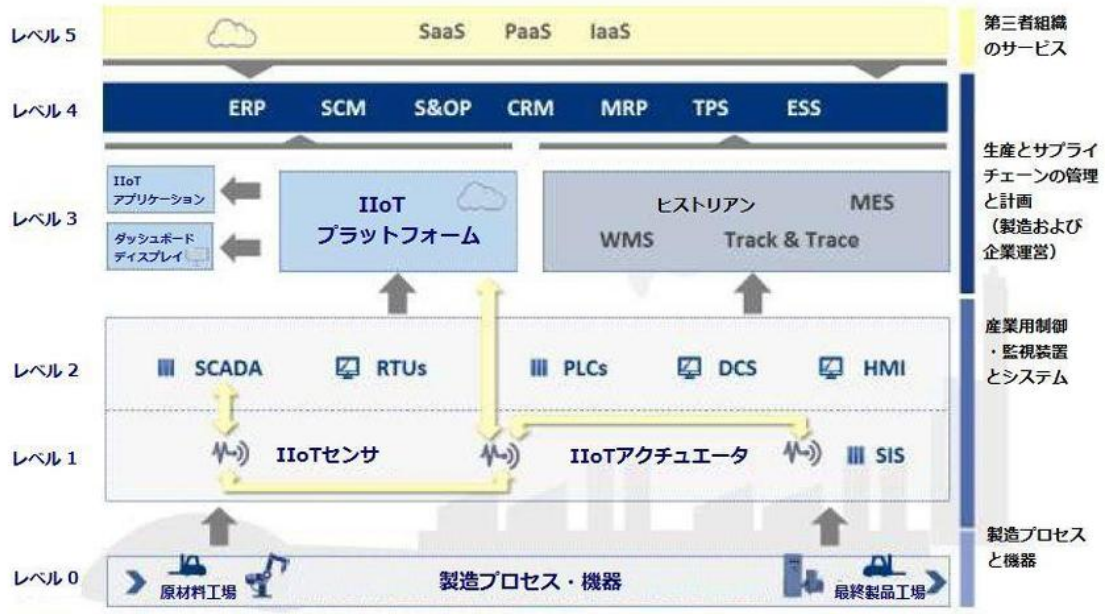
IIoT 機器の導入・運用においては、機器がどのネットワーク層に位置するかを明確にすることが、セキュリティ設計や管理体制の構築において極めて重要である。この整理のための基本的な枠組みとして、PA(プロセスオートメーション)分野では「パデューモデル（Purdue Enterprise Reference Architecture）」を活用する。一方、FA(ファクトリーオートメーション)分野では、ラインごとに制御機器やメーカーが異なることが多く、いわゆるマルチベンダー構成となるケースが一般的であるため、階層モデルによる一律の表現が困難である。そこで本手引きでは FA 系においてよく見られる一般的な構成をもとに整理を行う。

(a)PA 系

パデューモデルとは、産業制御システム（ICS）におけるネットワークおよびシステム構成を、機能・役割・責任の観点から階層的に整理した参照アーキテクチャである。このモデルは、制御機器から企業の情報システムに至るまでを 0～5 のレベルに分類し、それぞれの階層における機器や業務の位置づけを明確化するものである。
特に IIoT 機器の配置や管理方針を検討する上で、影響範囲の可視化とセキュリティ対策の設計基盤として重要な指標となる。
※製造業の業種によってパデューモデルの適用や階層の解釈に違いがあるので、あくまで参考として、自社のシステムに置き換える事が必要である。

レベル		主な機能
レベル 0	物理プロセス層	実際の製造・処理が行われる層
レベル 1	基本制御層	リアルタイム制御
レベル 2	制御装置層	制御ロジックや装置制御
レベル 3	監視制御層	運転管理と遠隔監視
レベル 4	サイト業務層	製造現場の業務システム層
レベル 5	企業 IT 層	経営情報系システムが集約される層

パデューモデルの参考例を示す。



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」[11]より参照

(b)FA 系

本手引きでは、FA 系におけるインフラ構成の整理手法として、経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver.1.1』に示された「想定工場のゾーン」モデルを参考にする。このモデルでは、業務内容や保護対象の性質に応じて工場システム全体を以下のようなゾーンに分割し、ゾーン単位でセキュリティ対策を検討するアプローチを採用している。

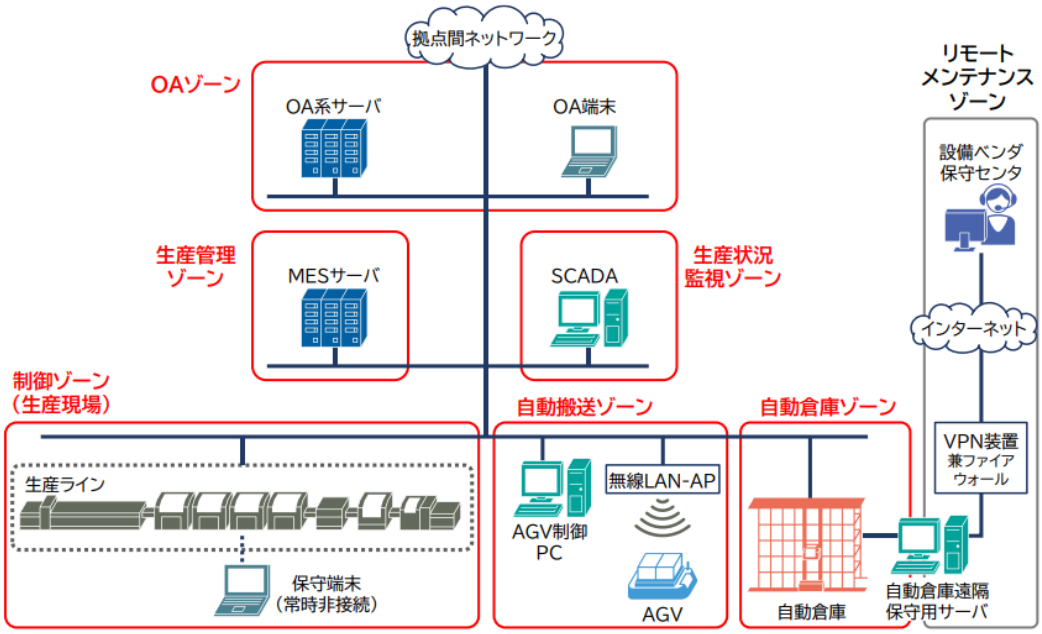
制御ゾーン	製品を生産するための生産ライン。制御装置・機器などで構成されるゾーン
自動搬送ゾーン	部材や完成品の運搬を行う AGV を運用するゾーン

[11] 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

https://www.ipa.go.jp/security/iot/ug65p900000197zo-att/000073490.pdf

自動倉庫ゾーン	部材を保管しつつ、自動で入出庫する装置を運用するゾーン
生産管理ゾーン	生産計画の管理、トレーサビリティデータの管理などを行うサーバ群からなるゾーン
生産状況監視ゾーン	生産状況や設備情報の取得・見える化を行う設備からなるゾーン
OA ゾーン	生産に直接関係ない業務を行うゾーン
リモートメンテナンスゾーン	設備ベンダーの保守センタが、自動倉庫をリモートで監視するためのゾーン

ゾーン分割における参考例を示す。



工場システムにおけるサイバー・フィジル・セキュリティ対策ガイドライン [5] より参照

IIoT 機器を導入・運用する際には、対象機器がネットワーク上のどの層・領域に位置づけられるかを明確にすることが、セキュリティ対策の出発点となる。PA 分野ではパデューモデルを参考に階層構成を整理することで影響範囲の可視化が可能となり、FA 分野ではゾーンモデルを用いて業務や設備の特性に応じた柔軟な分類と対策が図られる。いずれの場合も、インフラ構成を体系的に把握することで、リスクの可視化と実効性あるセキュリティ対策の設計に繋がる。

3.5 本手引きにおける IIoT 機器とは

IIoT 機器の定義には一定の幅があるが、本手引きでは IIoT 機器を「制御システムで使用される IoT 機器」と定義する。

IIoT 機器は一般的な IoT 機器とは異なり、物理的制御や安全性に直結する用途に使用されるため、そのリスクもより深刻となる可能性が高い。したがって、導入時のリスク評価、運用時の体制整備、廃棄時の手順確認など、ライフサイクル全体を通じた対応が求められる。

第 4 章　IIoT 機器のライフサイクル構築

本章では、関係部門の役割整理と連携強化、リスク評価の実施、セキュリティ要件の明確化について解説し、IIoT 機器のライフサイクルの構築の指針を提示する。

4.1 関係部門の連携とその役割

本節では、関係部門間の連携について現状と課題を整理し、各部門の役割について示す。

4.1.1 部門間連携の現状と課題

IIoT 機器の導入から廃棄に至るまで、セキュリティを確保しながら一貫した管理を行うためには、関係部門の協力が不可欠である。

また、関係部門間の連携が不十分で、申請部門もしくは IIoT 導入計画部門のセキュリティに対する意識が低い場合、IIoT 機器の導入においても問題が生じやすい。たとえば、導入時にセキュリティ部門へ相談を行わなかったり、機能要件にセキュリティに関する要件を盛り込まなかったりする。また、そもそもどのようなセキュリティ機能が必要かを把握していないこともある。その結果、セキュアでない IIoT 機器が導入されてしまうリスクが高まる。そのうえで導入後についても管理運用が属人的、かつ断片的になることで IIoT 機器を起因としたサイバーセキュリティインシデント発生のリスクが上昇し、さらにインシデントに対する対応も遅れてしましい事業継続に影響をあたえるという課題がある。

したがって、関係部門間が協力して IIoT 機器のライフサイクルを構築し運用していく環境を構築することが、IIoT 機器のセキュリティを確保することの第一歩であることは、ここで述べておきたい。

各組織の関係部門間の連携について、その現状の課題とあるべき姿を以下にまとめる

(a)現状の課題

- IIoT 機器のライフサイクルについて文書化がされていない。

- 本社セキュリティ部門が IIoT 機器の導入について一方的な審査のみを行いサポートを行えていない。
- 申請部門は規定に記されていない一方的な審査をさけるために本社セキュリティ部門に相談せずに IIoT 機器の導入を行う。
- 本社セキュリティ部門と申請部門が IIoT 機器の管理ができておらずシャドーIT と化している。
- ベンダーは IIoT 機器の導入時にしか関与せず、アップデートや脆弱性情報の提供などのサポートについての取り決めができておらず継続的な支援体制が構築されていない。
- 経営層の多くは IIoT 機器も BCP に影響をあたえるサイバーセキュリティインシデントの発生源としての認識できていない。

(b)あるべき姿

- IIoT 機器のライフサイクルが明確に文書化され、適切に管理されている。
- 本社セキュリティ部門は IIoT 機器の導入において、審査に加えて申請部門への積極的なサポートと連携を行っている。
- 申請部門は IIoT 機器の導入に際し、規定に基づき本社セキュリティ部門と事前に相談・連携を行っている。
- 経営層が BCP との関係を理解し、最終的なリスクオーナーとして関与する。
- 本社セキュリティ部門と申請部門が連携して IIoT 機器の管理を適切に行っており、シャドーIT は発生していない。
- ベンダーと IIoT 機器導入後も継続的なアップデート対応や脆弱性情報の提供などを含むサポート体制について取り決めがなされており、長期的な支援体制が整っている。
- 経営層は IIoT 機器が BCP に影響を与える可能性のあるサイバーセキュリティインシデントの発生源であることを十分に認識している。

比較カテゴリ	現状の課題	あるべき姿
ドキュメント管理	ライフサイクルが文書化されてない。	文書化され、管理されている。
本社と現場の連携	一方的な審査となり、相談が回避されている。	規定に基づく連携と支援がされている。
機器責任	シャドーIT 化されている。	台帳等にて管理されている。
ベンダー関与	導入時のみ関与している。	ライフサイクルを通し関与している。
経営層の認識	BCP への影響の認識がない。	BCPへの影響を理解し対策している。

4.1.2 各部門の役割と責任

IIoT 機器の適切な導入・設定・運用・廃棄に至るまでのライフサイクル管理を実現するためには、IIoT 機器ベンダーを巻き込んだうえで申請部門・本社セキュリティ部門・経営層のそれぞれが明確な役割を担い、連携して対応することが不可欠である。

また、3.2 節において紹介するチェックシートに申請部門責任者が確認した旨を記し、申請部門が IIoT 機器に関する現場のリスクオーナーであることを明確にする。その際、リスク評価を行う本社セキュリティ部門がリスク評価結果を申請部門と共有し、現場責任者が IIoT 機器の導入に伴うリスクを認識する。一方で記載したチェックシートの確認漏れ等により発生したインシデントについては、チェックシートの確認箇所である本社セキュリティ部門が責任を負うことなどの免責についても整理が必要となる。

以下に各部門の役割を示す。

(a) 申請部門の役割

申請部門は、IIoT 機器の導入目的を明確にし、工場の運用についての知見をもとに、本社セキュリティ部門との協議を通じて、適切な機器の選定・構成・設置・運用を

進めることが求められる。導入に際しては、社内の規定や手順に則り、セキュリティ要件の確認・実装にも主体的に取り組むことが重要である。また、導入後も機器の状態や使用状況を継続的に把握し、問題が発生した場合には速やかに報告・対応を行い、IIoT 機器の管理部署として IIoT 機器に関する現場のリスクオーナーである自覚を認識することが求められる。

(b) 本社セキュリティ部門の役割

本社セキュリティ部門は、全社のセキュリティを事業継続の視点でガバナンスを行う立場にあるため、IIoT 機器導入に関する技術的・運用的な審査を実施するだけでなく、申請部門に対して積極的な支援と情報提供を行い、実効性のあるセキュリティ対策の実装を後押しする立場となることが重要である。導入フェーズでは IIoT 機器に必要とされるセキュリティ要件の提案をその理由とともに説明し、運用フェーズでは脆弱性情報の管理方法や運用支援など、ライフサイクル全体を通じたサポートを提供することが求められる。

(c) 経営層の役割

経営層は、IIoT 機器に内在するリスクが企業の BCP と密接に関係することを理解し、全社大の最終的なリスクオーナーとしての立場からガバナンスの強化に関与することが重要である。特に、全社的なセキュリティ方針の策定、継続的な改善のためのリソース確保、関係部門間の連携体制の推進などが求められる。

(d) IIoT 機器ベンダーの役割

IIoT 機器のベンダーは、単なる導入時の委託業者としての役割にとどまらず、ライフサイクル全体を見据えた継続的な支援提供者として機能することが重要である。そのためにはベンダーをコントロールするための取り決めをユーザ側から明示する必要があり、SLAなどの契約文書を通し、導入後のソフトウェア・ファームウェアのアップデート提供、脆弱性情報の迅速な通知、セキュリティパッチの適用手順の提供、長期保

守契約の整備を提供する体制構築をことが求められる。また、ユーザ環境に即した設定やセキュリティ強化策についての技術的助言を行い、単なる取引先にはとどまらず信頼できるパートナーとしての役割を果たすことが求められる。

4.2 ライフサイクル構造とリスク評価手法

本節では、ライフサイクルを構成する 5 つのフェーズについて説明を行い、IIoT 機器のリスク評価手法を提案したうえで、ライフサイクルの全体像を示す。

4.2.1 ライフサイクルにおいて使用するチェックシート

本手引きにおいて提案する IIoT 機器のライフサイクルは「事前相談」、「導入審査(リスク評価、導入チェック)」、「設定チェック」、「運用チェック」、「廃棄チェック」の 5 つのフェーズから構成され、それぞれのフェーズにおいてチェックと評価を行う。

これらのチェックと評価については、以下の表のとおり、各チェックシートを用いて確認する。

なお、各チェックシートについては申請部門が記入し、リスクチェックシートに基づくリスク評価と各チェックシートの確認については本社セキュリティ部門の担当とするが、その内容に専門的内容が含まれるため申請部門での記入の支援を本社セキュリティ部門が行うものとする。

フェーズ	ツール
事前相談	―
導入審査(リスク評価)	リスクチェックシート(PA/FA)
導入審査(導入チェック)	スペックチェックシート 自社運用チェックシート ベンダーサポートチェックシート
設定チェック	設定チェックシート
運用チェック	運用チェックシート
廃棄チェック	廃棄チェックシート

役割	担当
リスクチェックシート、各チェックシートの記入	申請部門

リスク評価、チェックシート確認、記入の支援、 リスク評価結果の申請部門への共有	本社セキュリティ部門

4.2.2 IIoT 機器のリスク評価手法

IIoT 機器の導入に伴うリスクを評価することでインシデント発生時の迅速な対応に備える。また、チェックシートの記載内容を評価するうえで事業へのリスク度合いで施策を評価する必要がある。本手引きにて提案するライフサイクルにおけるリスク評価では、リスクチェックシートを使用する。リスクチェックシートを使用したリスク評価の方法は一般的なリスク計算式で実施するのではなく、事業への影響度を基軸とした下記の考え方を用いる。そこには用途及び利用ケースの 2 つの軸から構成されるマトリックス（以下、2 軸マトリックス）が記載されている。用途と利用ケースの組み合わせで IIoT 機器を起因とするサイバーセキュリティインシデントの事業影響度（リスクレベル）が決定される。

用途(制御/予測・分析/蓄積)×利用ケース(本番利用/検証利用) = 事業影響度(高/中/低)

	制御	予測・分析	蓄積
本番利用	例：高	例：高	例：中
検証利用	例：低	例：低	例：低

用途と利用ケースの組み合わせによって決定した事業影響度の評価により、影響度が高い物は BCP 策定計画等が必要となるため導入審査におけるチェックの項目数が調整される。

事業影響度については、リスクの高い順から「高」、「中」、「低」の三段階の評価とし、対象企業の業種やネットワーク構成に応じてその「高」・「中」・「低」を、本手引きを活用する各企業にて決定する。事業影響度の評価基準については以下のように定め

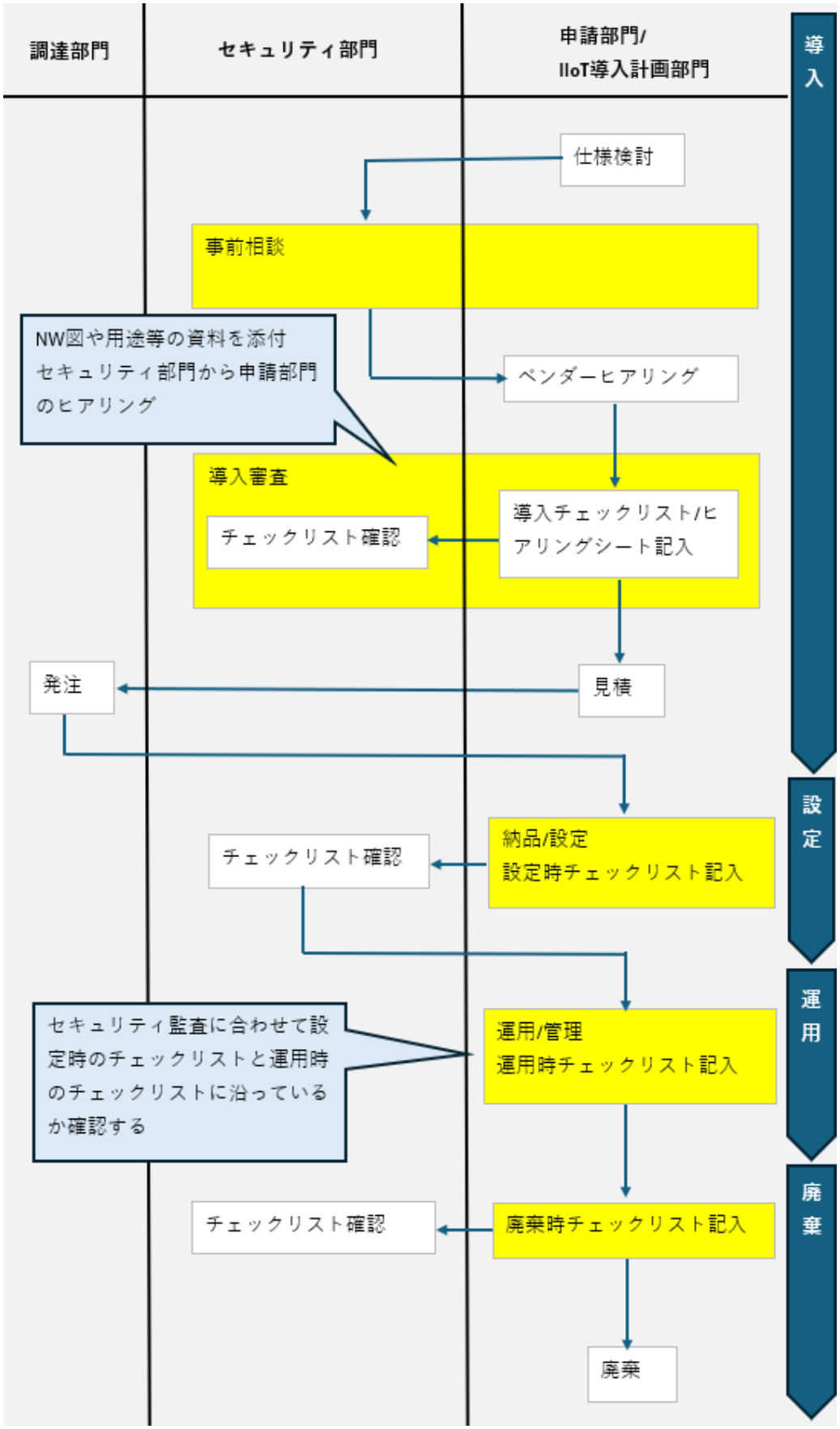
る。

事業影響度	評価基準
高	事業継続が困難になるインシデント ・影響範囲が製造ライン全体や企業の中核業務に及ぶもの。 ・人命へ影響が生じるもの。 ・設備の長期停止、製品出荷停止、重大な品質事故、顧客への供給遅延などが生じるもの。 ・企業ブランドや社会的信頼の失墜、法的・契約上の損失にもつながるもの。 ・復旧に時間、コスト、専門的対応を要し、BCP（事業継続計画）の発動が必要となるもの。
中	業務継続が困難なインシデント ・特定部門や業務の継続が困難となるもの。 ・主に現場業務や業務部門単位で支障が生じるもの。 ・品質判断ミス、工程遅延、分析データの信頼性低下などによる業務の停滞が想定されるもの。 ・全社的な業務停止には至らないが、誤判断や作業効率の低下により間接的に生産性や納期へ影響を及ぼす可能性があるもの。 ・適切な対応とリカバリー処理により業務復旧は可能であるが、一定の業務負荷や運用リスクが残るもの。
低	回復可能なインシデント ・一時的な障害であり、復旧可能なもの。 ・個別設備や特定機能（ログ記録、データ保存など）に限定された影響が発生するもの。 ・現場の運用には軽微な影響しか及ぼさず、業務の代替手段や再起動対応で復旧可能なもの。 ・後処理の手間や一時的な監視負荷が発生する程度で、重大な事

	業・業務リスクには発展しにくいもの。

これまで説明したリスク評価において、2 軸マトリックスにおける「用途」については第 2 章の記述に従い分類を行う。「利用ケース」については、本番利用をプラントの運転時（試運転を含む）に制御におけるネットワークにて使用するものと定義し、検証利用とは PoC(Proof of Concept)などにおいてプラントのネットワークから完全に物理的に切り離された環境における使用と定義する。

検証利用においても本手引きのライフサイクルの対象とした理由としては、PoC での利用においてもセキュリティを考慮した設計とすることで、本番利用へのセキュリティ要件を備えた円滑な移行を促すためである。


調達部門
セキュリティ部門
申請部門/
IIoT導入計画部門
導入
仕様検討
事前相談
NW図や用途等の資料を添付
セキュリティ部門から申請部門
のヒアリング
ベンダーヒアリング
導入審査
チェックリスト確認
導入チェックリスト/ヒ
アリングシート記入
発注
見積
設定
チェックリスト確認
納品/設定
設定時チェックリスト記入
運用
セキュリティ監査に合わせて設
定時のチェックリストと運用時
のチェックリストに沿っている
か確認する
運用/管理
運用時チェックリスト記入
廃棄
チェックリスト確認
廃棄時チェックリスト記入
廃棄

4.2.3 IIoT 機器のライフサイクル構造

(a)事前相談

リスク評価と導入審査を行うあたり必要な手続きの流れや手続きにあたって記入すべき各チェックシートについて本社セキュリティ部門から現場へ説明及び、導入審査までに必要な書類に記入を行えるよう支援を行う。

(b)導入審査

①リスク評価

導入を検討している IIoT 機器について、その IIoT 機器を使用することによるリスク、つまり IIoT 機器を起因とするサイバーセキュリティインシデントが事業にあたえる影響度(事業影響度)を特定する。リスク評価にあたってはヒアリングシートを利用し、本手引きを活用する各企業の業種(FA/PA)に応じた IIoT 機器の用途を制御/予測分析/蓄積に分類したうえで、利用ケースにより事業影響度のランク付け行ったものを現場が本社セキュリティ部門へ提出をする。

②導入チェック

リスク評価とあわせて導入を検討している IIoT 機器が具備すべきセキュリティ機能のチェックを行う。セキュリティ機能についてはベンダーが開示できないものも存在するため、その場合はベンダーへの自己宣言してもらうことを要件とする。なお、セキュリティを導入審査にて満足できない場合は設置までにセキュリティ機能を備えることを条件に合格を出す。また、IIoT 機器を管理していくにあたって、現場が備えている運用体制が構築されているかのチェックも行う。IIoT 機器に導入後の運用を見据えて、IoT 機器ベンダーのサポート体制に関するチェックを行う。

なお、JC-STAR1 の☆1 認定を取得している IIoT 機器を導入する場合は当該チェックを一部免除できるものとする。

(c)設定チェック

設定ミスをなくすことを目的として、入チェックにより確認した IIoT 機器のセキュリテ

ィ機能が、IIoT 機器の設定時にそのセキュリティ機能が反映されているかのチェックを行う。本チェックについては申請部門が行うものとし、その結果を本社セキュリティ部門に提出する。

(d)運用チェック

やりっぱなしの防止を目的として、運用を開始した IIoT 機器について導入チェックシートにより確認した運用体制の継続的に維持されているかをチェックする。チェックのタイミングとしては任意のタイミングとし本手引きにおいては特段指定しないが、セキュリティ監査などの定期的な監査とあわせて実施することを推奨する。

(e)廃棄チェック

寿命や更新等により、廃棄を行う IIoT 機器について、データ抹消等の適切な廃棄を行えるようチェックする。廃棄については原則として社内にて規定されている情報資産の廃棄規定に従うものとするが、当該規定が整備されていない会社については廃棄チェックシートにより安全な廃棄がなされるかをチェックする。

4.3 各フェーズ別のセキュリティチェック要件

本節では、各フェーズにおいて実施するセキュリティチェックの要件について説明する。

4.3.1 各チェックシートの要件

本手引きのライフサイクル各フェーズで使用するチェックシートは、JC-STAR、電力制御システムセキュリティガイドライン、スマートメータシステムセキュリティガイドラインをベースにし、一部廃棄チェックシートは媒体のデータ抹消に関するガイドライン(以下、NIST SP 800-88 Rev.1 Guidelines for Media Sanitization[12])をベースに作成している。以下にリスクチェックシートを除く各チェックシートで要求しているセキュリティチェック要件について説明する。

(a)スペックチェックシート

①セキュリティ機能

・セキュア通信機能の確認

IIoT 機器や重要情報資産へのアクセスは、認証に基づくアクセス制御により正当な機器・ユーザに限定されていることを要件する。アクセス認証にはパスワード、多要素認証、証明書等が用いることと規定し、さらに、通信経路上の情報は CRYPTREC 準拠の暗号により盗聴防止が施され、初期設定で保護機能が有効化されていることを求めている。

・情報保護機能の確認

IIoT 機器が取得する重要情報資産は、CRYPTREC 準拠の暗号化や電子署名により機密性・完全性が確保されていることを要件とする。ユーザにより自身のデータ(個

[12] NIST SP800-88 Rev.1 Guidelines for Media Sanitization

https://www.ipa.go.jp/security/crypto/gmcbt80000005u4j-att/SP800-88rev1.pdf

人情報・設定値・認証情報など）を削除でき、その手順を参照できること。さらに、データ削除後も製品のアップデート状態（セキュリティ修正等）が維持されていることを求めている。

・攻撃防御機能の確認

IIoT 機器は、あらかじめ定められたプログラムおよび正規のコマンドのみが実行される設計とし、不正な処理や権限の濫用を防止していることを要件とする。さらに、ネットワーク経由のユーザ認証には、多要素認証や試行制限により総当たり攻撃への対策が講じられていることが求められる。

②管理機能

・機器管理機能の確認

IIoT 機器は、ユーザが製品の型番を確認できる手段を備えていることを要件とする。さらに、パスワードや認証トークンなどの認証値については、ユーザが任意に変更可能であり、その手順がマニュアル等で明示されていることを求めている。

・パスワード管理機能の確認

IIoT 機器は、パスワードなどの認証値は変更可能なうえで、安全な初期設定や初回変更の強制が実装されている

・アップデート/脆弱性機能の確認

IIoT 機器の、更新ソフトウェアはその適用前にハッシュ照合やデジタル署名により完全性が確認され、不正なソフトウェアのインストールを防止する仕組みを備えていることを要件とする。さらに完全性が確認できないときはインストールが中止される。加えて、使用されるアルゴリズムは CRYPTREC 推奨の安全な方式であることを求めている。

(b)自社運用チェックシート

①全社運用体制の構築の確認

全社的にセキュリティマネジメント体制が確立され、BCP やインシデント対応・報告・記録の手順が整備されていることを要件とする。さらに、関係者に対しては、定期的なセキュリティ教育と、サイバーセキュリティインシデント対応に備えた訓練（連絡訓練・机上演習等）が計画的に実施されていることを求めている。

②現場運用体制の構築の確認

IIoT 機器の安全な運用のため、セキュリティ管理責任者や関係者の役割を明確化し、事故対応ができる情報収集体制を整備することを要件とする。さらに情報資産をリスト化したうえで脆弱性情報は継続的に収集し、評価と対応手順を策定することを求めている。

(c)ベンダーサポートチェックシート

IIoT 製品の外部サポート委託先に対して、明確なセキュリティ役割と遵守事項を取り決めていることを要件とする。この取り決めにおいては安全な利用手順やサポート期間が明示されていること、ユーザにアップデートの内容・必要性・リスクが通知および、脆弱性の報告連絡先・対応方針・管理体制が開示されていることを求めている。

(d)設定チェックシート

スペックチェックシートにて確認した内容について、IIoT 機器の設置時に適切に反映されていることを求めている。

(e)運用チェックシート

自社運用チェックシートにて確認した内容について、全社運用体制と現場運用体制が維持されていることを求めている。

(f)廃棄チェックシート

本手引きは、各企業において情報資産の廃棄に関する規定が整備されていない場合に活用することを想定している。IIoT 機器を廃棄する際は、対象機器の情報（型番、シリアル番号、設置場所など）を特定・記録し、機器内に保存されている情報の種類を把握したうえで、機密性評価に基づき「高・中・低」に分類する。その分類結果に応じて、「消去（Clear）」、「除去（Purge）」、「破壊（Destroy）」のいずれかの方法を選択し、メーカーが推奨するツールを用いて適切にデータを抹消する。なお、リムーバブルストレージやセンサなどの消耗品も対象とし、抹消後には復旧不可能であることを検証・確認することを要件とする。さらに、社内方針に従い法令を遵守したうえで廃棄または移管を行い、外部委託する場合は信頼性のある業者を選定することを求める。

第 5 章　IIoT 機器のライフサイクル構築総論

IIoT 機器のセキュリティを確保するためには、単一フェーズでの対応にとどまらず、導入から廃棄に至るまで、ライフサイクル全体を通じた継続的な管理が不可欠である。また、その実現には、適切な判断基準の設定、日常的な運用管理、そして部門間の協力体制といった多面的な取り組みが求められる。本章では、こうした観点を踏まえ、IIoT 機器のセキュリティを企業として実現していくうえでの3つの基本方針を提示する。

(a)企業としてのリスク認識と導入可否判断

IIoT 機器の導入にあたっては、まず当該機器が事業に与える影響度、すなわちリスクを適切に評価することが、導入可否判断の前提となる。本手引きでは、リスク評価の枠組みとして「用途（制御／予測・分析／蓄積）」と「利用ケース（本番／検証）」の二軸による定量的な可視化手法を提案している。これにより、IIoT 機器が業務に及ぼす影響を客観的に把握し、自社として受容可能なリスク水準を明確にすることが可能となる。

特に、業務プロセスやシステム構成が多様化する現在においては、機器の用途や利用状況に応じた判断基準を設け、それを共通化・可視化することが求められる。こうした定量的アプローチは、属人的な判断を排除し、再現性のある判断プロセスの確立を可能にする。これにより、個別現場の裁量に依存した場当たり的な導入を防ぎ、全社的に整合の取れた導入判断が可能となる。IIoT 機器の安全かつ効果的な活用には、このような統一的で透明性のある判断プロセスが不可欠である。

(b)ライフサイクル全体を通じた継続的なセキュリティ管理の実現

IIoT 機器のセキュリティ管理は、導入前の審査にとどまらず、導入後の設定、日常的な運用、さらには廃棄・撤去に至るまで、ライフサイクル全体を通じて継続的に実施

されるべきものである。特に IIoT 機器は、現場に長期間設置されることが多く、機器更新のサイクルも一般的な IT 機器より長いため、時間の経過とともに新たなリスクや脆弱性が顕在化する可能性が高い。

各フェーズにおいて求められる対応は異なり、例えば設定フェーズでは初期パスワードの変更、運用中には脆弱性情報の収集・適用、廃棄フェーズには記録媒体の安全なデータ消去などの対策が必要になる。こうした多様な対応事項に漏れなく取り組むためには、各フェーズに応じたチェックシートや手順書を整備し、それを継続的に活用・見直していく体制が求められる。

このように、IIoT 機器のライフサイクル全体を俯瞰しながら、フェーズごとの適切な管理を実践することにより、セキュリティリスクの早期発見と継続的な低減が可能となる。結果として、業務の中断や情報漏えいといった重大なインシデントの予防にもつながり、IIoT 活用における持続可能なセキュリティ確保を実現できる。

(c)部門をまたいだ協力体制の構築

IIoT 機器のセキュリティ対策は、本社セキュリティ部門のみの責任で完結するものではない。申請部門、調達部門、経営層、さらには機器ベンダーを含む多様な関係者が、それぞれの立場や専門性に応じた役割を果たし、連携して対応する体制の構築が不可欠である。

例えば、本社セキュリティ部門はリスク評価やガバナンスの観点から全体方針をリードし、標準化を推進する役割を担う。一方で、申請部門はチェックシートに基づいた日常的な確認や、実際の機器の状態把握・管理を行い、調達部門は契約段階においてセキュリティ要件の明確化と反映を行う必要がある。さらに、経営層は IIoT 機器のセキュリティを事業継続計画（BCP）や全社的リスクマネジメントと結び付ける視点が求められ、ベンダーには、導入後も継続的に脆弱性対応や運用支援を提供する責任がある。

本書ではチェックシートや評価マトリクスといったツールを“共通言語”として活用す

ることで、部門をまたいだ協力体制を実効性あるものとして機能させることができる。

本手引きは、主に国内の製造業やインフラ企業における IIoT 機器の安全な導入・運用を支援することを目的として作成されたが、その枠にとどまらず、今後さらに幅広い展開が期待される。

まず社内展開としては、本手引きを標準作業手順書（SOP）として制度化し、セキュリティ教育、内部監査、日常運用の基準として活用することが可能である。チェックシートや評価マトリクスを定常的なツールとして用いることで、個人依存の判断を排し、組織的・再現的な運用体制の構築につながる。

次に他社展開の可能性として、業界団体や取引先企業との間で本手引きを共有し、サプライチェーン全体でのセキュリティレベルの底上げを図ることが考えられる。共通の評価テンプレートとして活用することで、企業間の協働や相互確認プロセスの効率化にも寄与する。

このように、本手引きは単なる社内ガイドラインにとどまらず、「導入判断」、「運用体制」、「教育・ガバナンス強化」といった観点から、IIoT 機器の安全な利活用における中核的な指針として機能し得るものである。

あとがき

国立大学法人 名古屋工業大学 名誉教授 越島一郎

経済産業省は「スーパー事業者認定制度」の中で、「IoT、ビッグデータの活用等の高度な保安の取組を行っている事業所認定し、能力に応じて規制を合理化」するとしている。新設されたスーパー認定事業所では、連続運転期間が 8 年に伸び、検査方法も事業所が自由に設定した方法が許されている。さらに、2023 年 12 月 21 日に施行された「高圧ガス保安法等の一部を改正する法律の施行に伴う関係政令の整備に関する政令」（同時にガス事業法並びに電気事業法）は、「テクノロジーを活用しつつ、自立的に高度な保安を確保できる事業所について、安全確保を前提にその保安確保能力に応じて保安規制に係る手続・検査を合理化する制度 」であり、スマート保安の推進を後押ししている。これらの施策は、製造現場が直面している運転コスト削減（競争力強化）と人材不足への対応として重要であり、これまで手薄であった「工場メンテナンス」をスマート化（スマート保安）することで、このインセンティブを手にする好機である。本「IIoT 機器ライフサイクル管理構築手引き」は、IIoT によるスマート保安推進を行う上で検討すべきセキュリティ対応を包括的に示しており、実務家にとって好適な参考図書となると考える。

(株)日立製作所　制御セキュリティ設計部 セキュリティエバンジェリスト /
国立大学法人 名古屋工業大学 客員教授　中野利彦

製造現場において制御システムのセキュリティを確保ことは、事業継続のために不可欠なことは間違いない。一方でより一層の生産合理化や生産ラインの柔軟性確保のために IoT 機器を活用した DX が進展していきている。
これら両者を両立させることが不可欠であるが、セキュリティを統括する部門と製造現場を統括している部門間の知識は異なることが多く、双方が相手の状況を正確に認識していることは少ない。

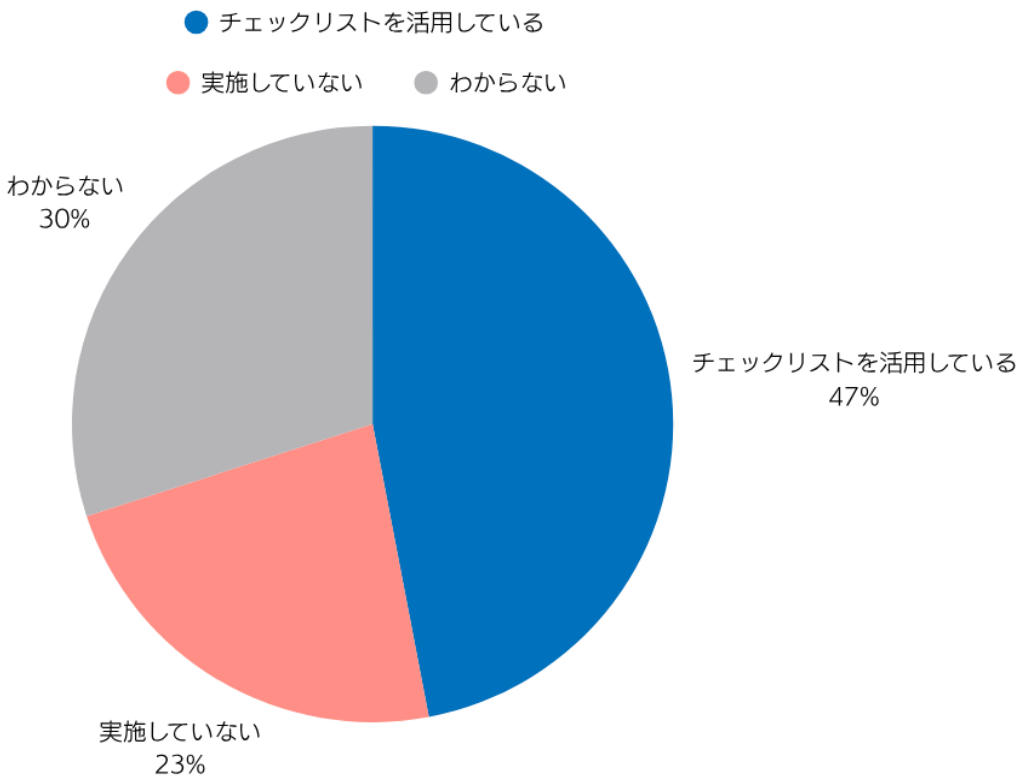
本卒業プロジェクトで作成したチェック手順およびチェックシートは、この異なる知識を持つ両組織の懸け橋となるものとして有効に活用できると考える。
ぜひ本成果を活用いただき、製造現場においてIoTを活用した制御システムのDX推進が、本成果物を活用することによりセキュリティインシデントの発生を予防するとともに事業へのインパクトをおさえることができれば幸いである。

Appendix

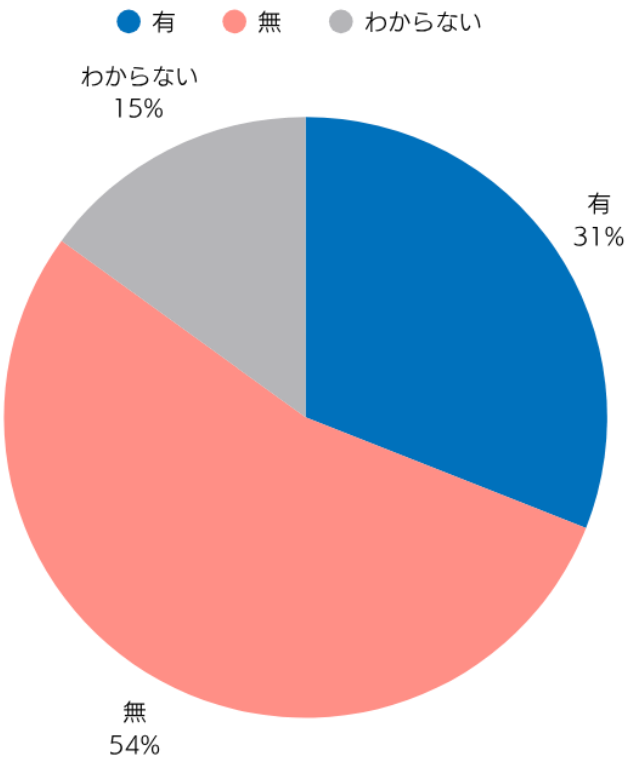
中核人材育成プログラム修了生の所属企業を対象に IIoT 機器実態調査のアンケートを実施した。

総回答数は 24 社あり、IIoT 機器を実際に利用している回答を有効回答としているため、有効回答数 13 社で結果を示した。

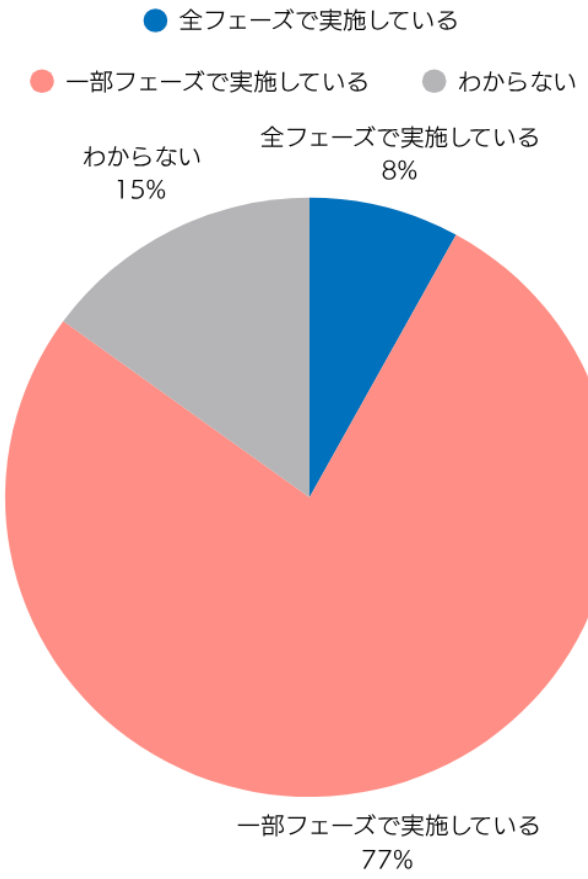
1.セキュリティチェックはどのように実施していますか？



2.社内規定上 IIoT 機器の定義はありますか？



3.IIoT 機器のライフサイクル(導入～廃棄)管理を実施していますか？



謝辞

本プロジェクトのアンケートにご協力いただきました叶会所属企業様、特に現地ヒアリングにご協力いただいた大阪ガス株式会社の辰巳様に深く感謝申し上げます。

また、本プロジェクトにご尽力いただいた産業サイバーセキュリティセンター中核人材育成プログラムの講師であられる越島先生、橋本先生、門林先生には、多方面にわたるご支援とご助言を賜りました。

そして、内容の検討に際し、多大なご意見と丁寧なレビューをお寄せいただいた株式会社日立製作所のセキュリティエバンジェリストであられる中野先生に、心より御礼申し上げます。

最後に、本プロジェクトを共に実施した下記メンバーの皆様にも感謝の意を表します。

＜Intelligent Industrial Optimization Team (IIOT) メンバー＞

【リーダー】

佐藤 蘭丸

【サブリーダー】

佐々木 太地

【メンバー】

安達 輝　伊藤 直　太田 智也

参考文献

1: Armis – HMI Machine Infected with WannaCry

https://www.armis.com/blog/hmi-machine-infected-with-wannacry/?utm_source=chatgpt.com&__cf_chl_f_tk=mysHih_MSRgt_gtjr_RYnSFi8ACR.QQx9Akg4Er61l0-1756540046-1.0.1.1-M.eTQ4BiGujxzoy1UOq2zo.rPhp3UYO7.LBms8kxSg8

2: Krebs on Security – Hacked Cameras, DVRs Powered Today's Massive Internet Outage

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/?utm_source=chatgpt.com

3: NOTICE（National Operation Towards IoT Clean Environment）

https://notice.go.jp/

4: セキュリティ要件適合評価及びラベリング制度(JC-STAR)

https://www.ipa.go.jp/security/jc-star/detail.html

5: CRA(Cyber Resilience Act)

https://www.cyberresilienceact.eu/the-cyber-resilience-act/

6: Cyber Trust Mark

https://www.fcc.gov/CyberTrustMark

7: 工場システムにおける サイバー・フィジカル・セキュリティ対策ガイドライン Ver1.1

https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.1.pdf

8: 電力制御システムセキュリティガイドライン JEAG 1111-2019

発行「一般社団法人 日本電気協会 情報専門部会」 令和元年 10 月 25 日第2版

9: スマートメータシステムセキュリティガイドライン JEAG 1101-2019

発行「一般社団法人 日本電気協会 情報専門部会」 令和元年 10 月 25 日第2版

10: Industry IoT Security Framework (IISF) An Industry IoT Framework Publication Version 2.0-2023-06-12

https://www.iiconsortium.org/wp-content/uploads/sites/2/2023/06/IISF-Version-2.pdf

11: 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

https://www.ipa.go.jp/security/iot/ug65p900000197zo-att/000073490.pdf:

12: NIST SP800-88 Rev.1 Guidelines for Media Sanitization

https://www.ipa.go.jp/security/crypto/gmcbt80000005u4j-att/SP800-88rev1.pdf