IoT 制御システムにおけるゼロトラストアーキテクチャの研究

研究年度　令和３年度
研究期間　令和３年度～令和４年度
研究代表者名　小林信博

I.　はじめに

近年、社会における IoT システムの活用が進展している。我が国が目指す Society 5.0 は、「サイバー空間とフィジカル空間（現実世界）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会」と定義されており、一例として、フィジカル空間のセンサから IoT を通じて情報が集積（ビッグデータ）され、人工知能（AI）が解析し、高付加価値な情報、提案、機器の制御などを、フィジカル空間にフィードバックすることが示されている。一方で、IoT システムへのサイバー攻撃によりサービス停止や不正操作等の問題が発生すると、我々の生活や経済・社会活動に深刻な影響を及ぼす可能性がある[1][2]。

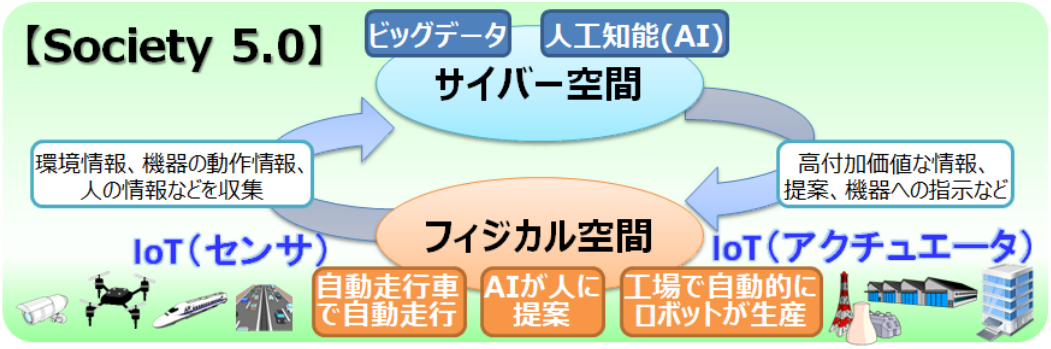

図 1 Society5.0 と IoT システム

本報告書では、特に、サイバー空間からフィジカル空間へのフィードバックとして、物理的な作用を及ぼす IoT アクチュエータにおけるセキュリティについて考察した結果について述べる[3][4][5][6][7]。また、IoT アクチュエータにおける今後のセキュリティ対策の方向性について示す。

II.　IoT アクチュエータについて

全世界の IoT デバイスの総数は、2022 年に約 350 億台に達すると予想されている。分野としては、これまで増加してきた「通信」にかわり、「医療」「産業」「コンシューマ」「自動車・宇宙航空」が高い伸びを示すとされている[8]。この IoT デバイスのもつ以下の機能は、サイバーセキュリティやプライバシーのリスクに従来の IT デバイスとは異なる影響を与える[4]。

・トランスデューサー機能

物理的な世界と相互に作用し、デジタル環境とフィジカル環境の間のエッジとして機能する。全ての IoT デバイスは、２種類のうち少なくとも１つのトランスデューサー機能を有する。

センシング機能

物理世界の測定しデータを提供する能力

例）温度、光学的センシング、オーディオセンシング

アクチュエータ機能

物理世界に変化を生じる能力

例）加熱コイル、電子ドアロック、ドローンの操作、サーボモーター、ロボットアーム

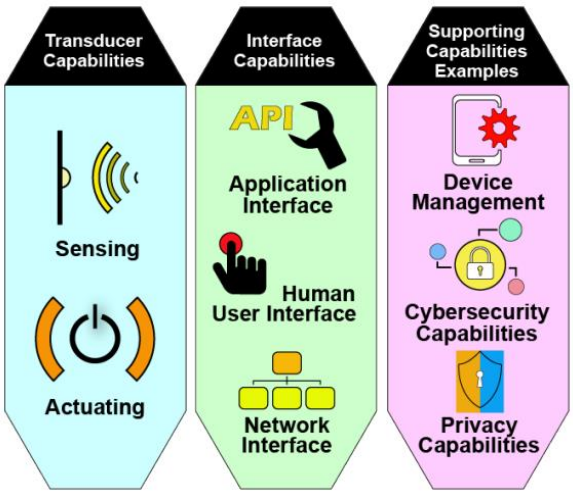

図 2　IoT デバイスの機能概要　（出典: NIST IR 8228）[4]

・インタフェース機能

デバイス間の相互作用（デバイス to デバイス、デバイス to 人間など）を可能にする。

アプリケーションインタフェース

アプリケーションプログラミングインタフェース等

ヒューマンユーザインタフェース

IoT デバイスと人間が直接コミュニケーションをとるための機能

例）タッチスクリーン、マイク、カメラ、スピーカ

ネットワークインタフェース

IoT デバイスが通信ネットワークを利用する能力

例）イーサネット、Wi-Fi、LTE、ZigBee 等

・サポート機能

他の IoT 機能をサポートする機能

例）デバイス管理、サイバーセキュリティ機能、プライバシー機能

本報告書では、トランスデューサー機能としてアクチュエータ機能を有する IoT デバイスを、IoT アクチュエータと呼ぶこととする。IoT アクチュエータは、物理世界に影響をあたえることができることから、人間の安全や生命を脅かしたり、機器や設備を損傷・破壊したり、社会インフラのような重要サービスの停止など大きな混乱を生じる恐れがある。Society 5.0 に向けたスマートシティにおいても、多数の IoT アクチュエータが配置され、活用されることとなり、そのセキュリティ確保は重要であると考えられる。

また、従来の IT システムと IoT システムにおけるサイバー攻撃の影響とその対策の違いの一例として、IT システムにおいては一般的に有効と考えられているネットワークの通信遮断が、IoT システムにおいては、事故や災害等の悪影響を及ぼす可能性があることを下図に示す。

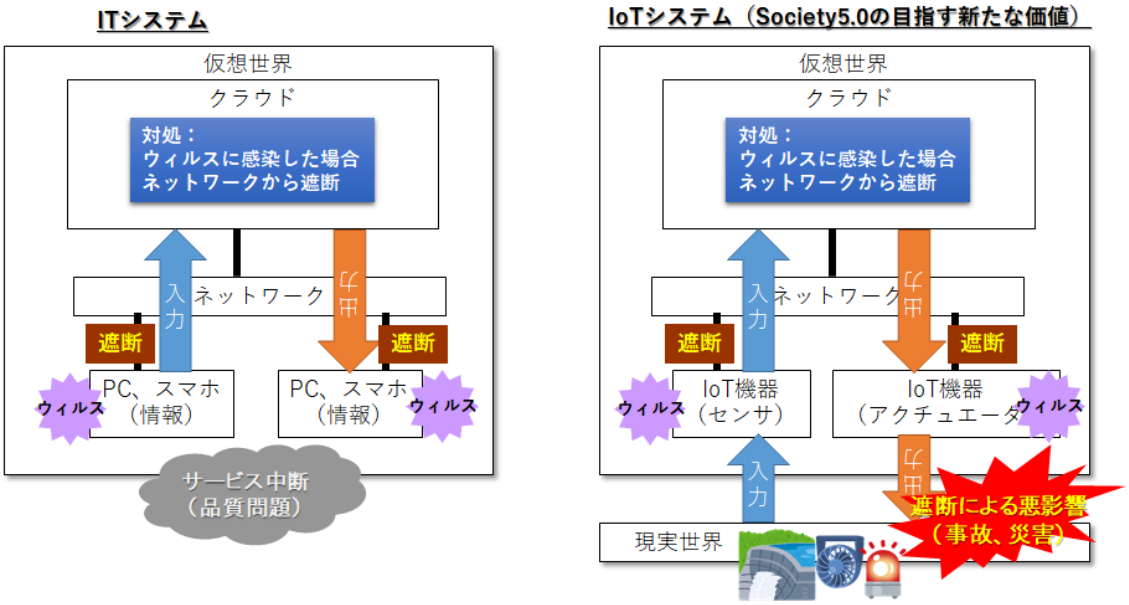

図 3　IT システムと IoT システムにおけるサイバー攻撃の影響の違い

III. 検討のスコープについて

IoT システムは、IT と OT の融合したシステム[4]であることから、IT に関するサイバーセキュリティの課題は、IoT システムにおける課題に包含される。

一例を以下に示す。

- 既知の脆弱性についての対策導入
- 脅威分析やリスク評価に基づく対策検討
- 実装時のバグの混入や機能不足の回避・検出
- 通信のセキュリティ（FW、IPS・IDS、暗号化等）
- 認証、アクセス制御の導入
- クレデンシャルやトラストアンカの保護、更新
- ログの取得や分析

これまで長年に渡りと取り組まれてきた IT システムのセキュリティ確保に関する研究は、その成果が蓄積されており、IoT システムにおいても活用が可能と考えることから、本報告書における検討からは除外する[4]。なお、個別の IoT デバイスの制約（計算機リソース等）により活用が困難な場合においては、別途検討を行う必要がある。

一方、本報告書においては、IoT システムの特徴として挙げられている以下の項目を中心に検討を行う。

a) 脅威の範囲や影響の度合いは非常に広く、大きくなる。
b) IoT システムの需要、特に運用・保守においては、10 年以上となる。
c) IoT デバイスを監視管理することは非常に困難な場合がある。
また、管理されていない IoT デバイスが存在する可能性がある。
d) IoT デバイス同士がお互いの環境を十分に認識することが困難な場合がある
e) IoT デバイスの機能や性能には制限がある
f) 開発者が想定していなかった IoT システムの接続の可能性がある

これらの条件や特性に付随するリスクを、IoT システムは検討する必要がある。

Ⅳ. IoT アクチュエータにおけるセキュリティ対策の方向性

IoT システムは多種多様であり、使用する IoT デバイスやシステム構成が類似している場合でも、IoT システムの目的や用途によって、必要なセキュリティ対策がことなることが指摘されている。

また、先行研究として、IoT アクチュエータの１つと考えらえるスピーカへの脅威に関する取り組みが挙げられる。この研究では、センサを対象としたアナログ信号の脅威に関する対策として、CPS のアナログ信号の出力を、ファイアウォールと同様の仕組みで検知・規制するフレームワーク「Cyber-Physical Firewall (CPFW)」が提案されている[9]。

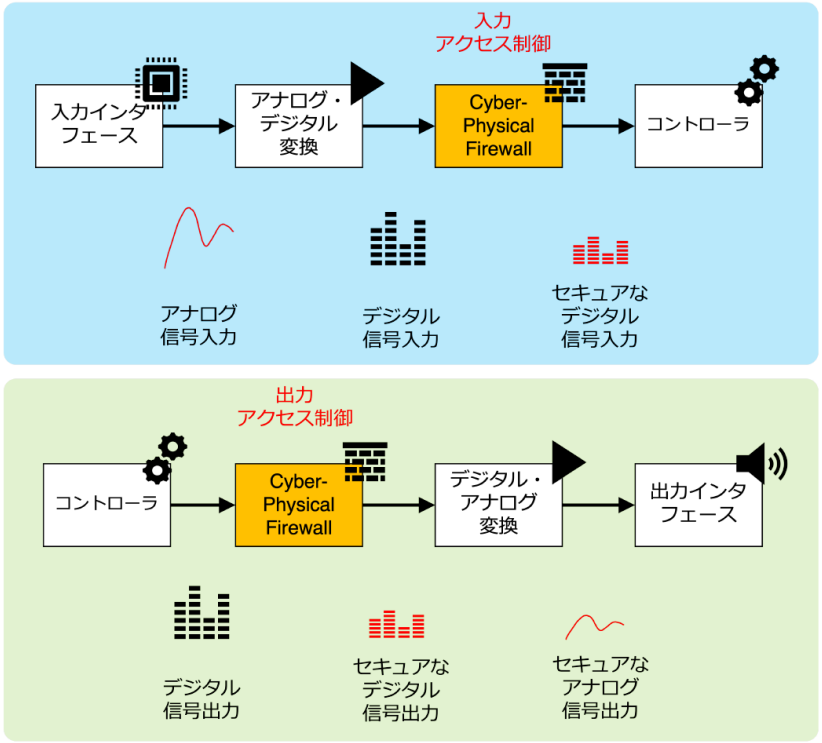

図 4　アナログ信号（音声）に対する攻撃対策例（CPFW）[9]

コントローラのデジタル信号出力を、CPFW により出力アクセス制御し、セキュアなデジタル信号出力のみを、デジタル・アナログ変換のうえ、出力インタフェースから出力することで、音信号による脅威への対策として有効であることが示されている。また、音信号については、アナログ信号の中でも提示されている脅威の種類の多さを挙げており、ケーススタディ評価として既知の攻撃に対するアクセス制御のポリシーを策定している。

一方で、スピーカと異なる、モータなど運動による環境への変化を生じる場合については、今後の課題とされており、さらにアクチュエータから生じる二次的な影響は、機械工学的なアプローチが求められるとしている。

以上を参考に、IoT アクチュエータにおけるセキュリティ対策は、コントローラと出力インタフェースの間における信号の伝達途中において、ポリシーに基づくアクセス制御機構を導入することが有効と考えられる。ポリシーの策定が、個別の脅威に特化したものとなる場合には、ポリシーの増加とリアルタイム性の確保を考慮する必要がある。

また、音信号以外のアクチュエータの信号の種類により、アナログ信号から抽出可能

な情報（attribute）と脅威信号との関係は異なると考えられることから、この関係性を明らかにする必要がある。

更に、出力インタフェースのアクセス制御により、脅威信号を規制出来た場合であっても、二次的な影響がより深刻な事態につながることも懸念されることから、IoT システムのサービス継続の観点でハイレベルなポリシーとの整合性を確保することも必要と考えられる。

これは、指定されたリソースへの最小限のアクセス権限を提供するというゼロトラストの中核的な考え方にも通じるものであり、ポリシー決定ポイント（Policy Dicision Point）とポリシー実施ポイント（Policy Enforcement Point）をクラウド側と連携可能な形で IoT アクチュエータの内部において実現することにより、現実世界に物理的な変化を生じる制御を動的に検証可能とするものである。

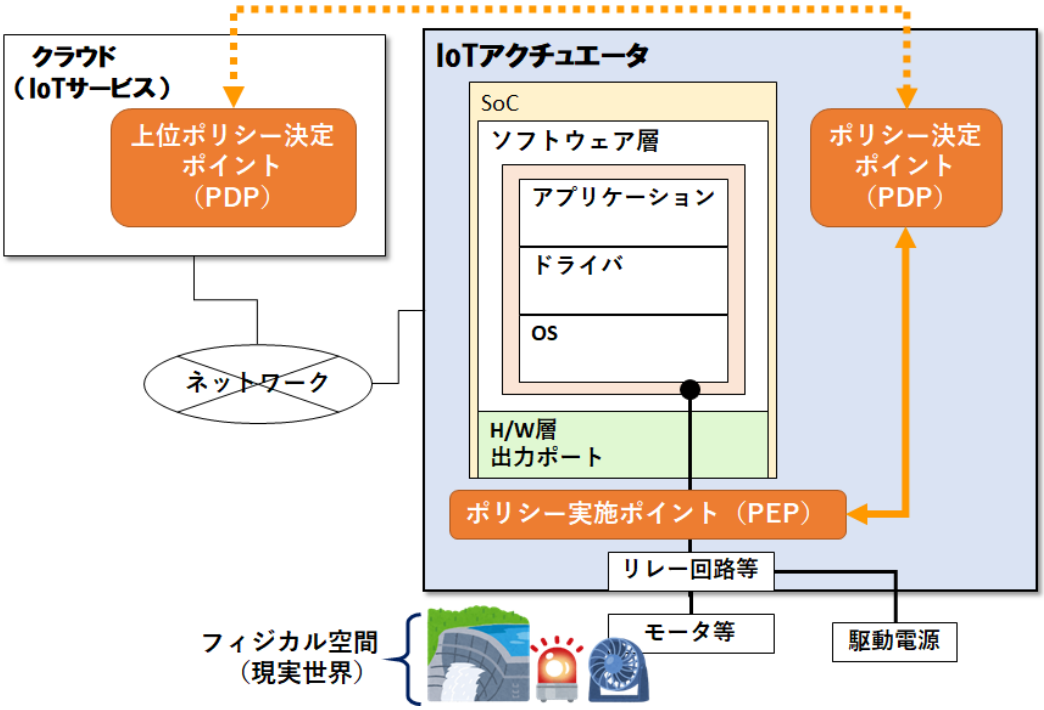

図 5　IoT アクチュエータにおけるゼロトラストの概念

V.　IoT アクチュエータにおけるセキュリティ対策の基本コンセプト

前章で述べた方向性に沿って、IoT アクチュエータにおけるセキュリティ対策の基本コンセプについて検討を行った。Society5.0 における IoT システムの信頼確保に向け

て、現実世界に物理的な変化を生じる IoT アクチュエータが、「ゼロデイ攻撃」と呼ばれるプログラムの未知の脆弱性を狙う新たなサイバー攻撃を受けても、現実世界に悪影響を及ぼさないように無効化するセキュア出力制御技術を実現し、IoT アクチュエータの信頼を向上することを目指す。

この目標達成のため、引き続き以下の研究に取り組む。まず、IoT アクチュエータのプログラムへのゼロデイ攻撃を、ハードウェア的に無効化する①セキュア出力制御技術の研究を行う。また、IoT アクチュエータに最適なセキュリティポリシを定義のうえ、ハードウェアを常にこの対策規則通りに制御する②制御ポリシ判断モジュールの研究を行う。更に、③仮想化環境におけるサイバー攻撃耐性評価実験と、シミュレーション環境あるいは実 IoT システムにおける動作実証実験により有効性を確認する。

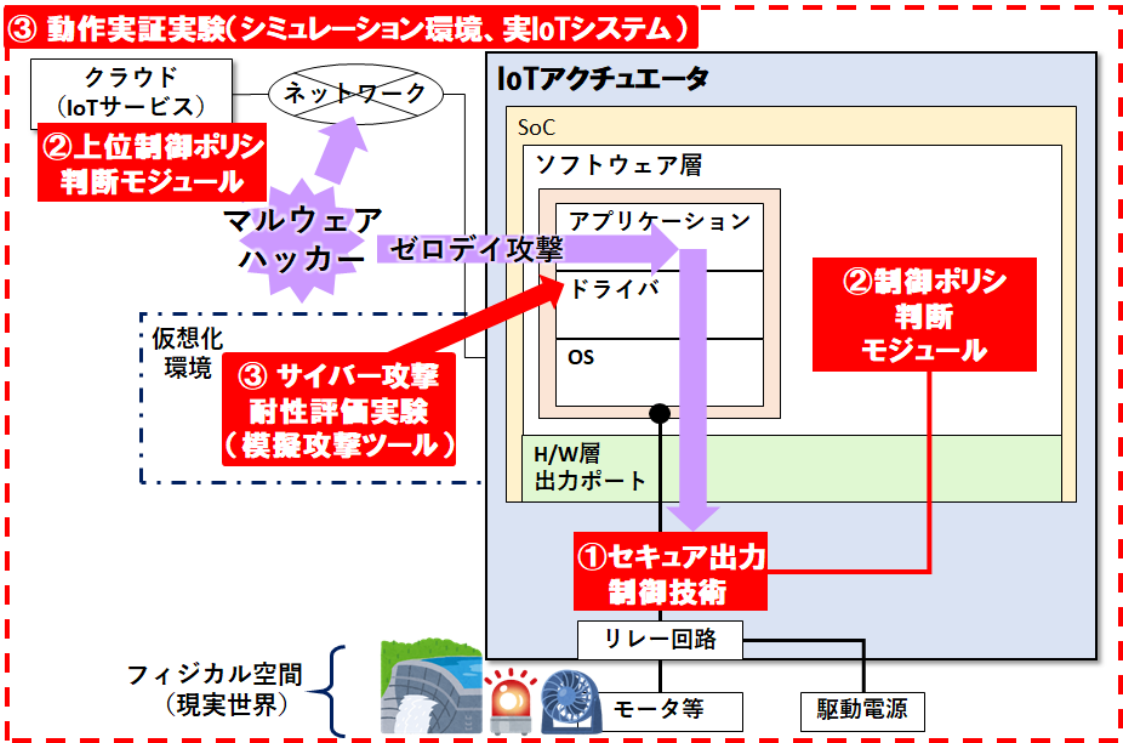

図 6　IoT アクチュエータにおけるセキュリティ対策の研究項目

VI. おわりに

本報告書では、特に、サイバー空間からフィジカル空間へのフィードバックとして、物理的な作用を及ぼす IoT アクチュエータにおけるセキュリティについて考察した結

果について述べた。また、IoT アクチュエータにおける今後のセキュリティ対策の方向性について示した。今後は、対策の詳細な方式検討に取り組むとともに、その有効性について検証を行う予定である。

参考文献

[1]「次期サイバーセキュリティ戦略（案)」, 内閣 サイバーセキュリティ戦略本部, 令和3年9月27日, https://www.nisc.go.jp/conference/cs/dai31/pdf/31shiryou01.pdf

[2] 石倉禅, 山本英朗, 仁佐瀬剛美, 間形文彦, “IoT システムのセキュリティ設計に関する考察”, 2018 年暗号と情報セキュリティシンポジウム (SCIS 2018), 4E2-1, 2018 年 1 月

[3] RON ROSS, MICHAEL McEVILLEY, JANETCARRIER OREN「NIST Special Publication 800-160 Systems Security Engineering」, NIST National Institute of Standards and Technology U.S. Department of Commerce, November, 2016, https://doi.org/10.6028/NIST.SP.800-160v1

[4] Katie Boeckl, Michael Fagan, William Fisher, Naomi Lefkovitz, Katerina N. Megas, Ellen Nadeau, Danna Gabel O’Rourke, Ben Piccarreta, Karen Scarfone,「NISTIR 8228 Considerations for Managing Internet of Things(IoT) Cybersecurity and Privacy Risks」, NIST National Institute of Standards and Technology U.S. Department of Commerce , June, 2019, https://doi.org/10.6028/NIST.IR.8228

[5] Michael Fagan, Katerina N.Megas, Karen Scarfone, Matthew Smith,「NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers」, NIST National Institute of Standards and Technology U.S. Department of Commerce, May, 2020, https://doi.org/10.6028/NIST.IR.8259

[6] Michael Fagan, Katerina N.Megas, Karen Scarfone, Matthew Smith,「NISTIR 8259A IoT Device Manufacturers Cybersecurity Capability Core Baseline」, NIST National Institute of Standards and Technology U.S. Department of Commerce, May, 2020, https://doi.org/10.6028/NIST.IR.8259A

[7] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly,「NIST Special Publication 800-207 Zero Trust Architecture」, NIST National Institute of Standards and Technology U.S. Department of Commerce , August, 2020, https://doi.org/10.6028/NIST.SP.800-207

[8] 「情報通信白書令和 2 年版」, 総務省, 令和 2 年 8 月 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/index.html
[9] 飯島 涼 , 竹久 達也 , 森 達哉, “アナログ信号による脅威を検知・規制するセキュリティフレームワークの提案と検証”, コンピュータセキュリティシンポジウム 2021 論文集, pp. 79 - 86, 2021 年 10 月 19 日