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[1]

研究年度　令和４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
共同研究者名　なし

1.　はじめに

Society5.0 の実現に向けてサイバーフィジカルシステム（CPS : Cyber Physical System）の社会への導入が進む一方、CPS を構成する IoT 機器のなかでも現実世界に物理的な変化をもたらすアクチュエータ機能を有する機器（IoT アクチュエータ）に対して、サイバー攻撃の脅威が増大している。IoT 機器を狙った代表的なマルウェアの Mirai[1]は、感染した多数の IoT 機器で巨大なボットネットを構築し、大規模な DDoS 攻撃を引き起こすが、このようなマルウェアは日々進化していることが報告されている[2]。特に、プログラムの未知の脆弱性を悪用するゼロデイ攻撃など、日々進化するサイバー攻撃により発生する IoT アクチュエータに対する不正な制御への備えとして、今後の社会インフラとなる CPS の強靭化は喫緊の課題である。

本研究では、特に、サイバー空間から物理空間へのフィードバックとして物理的な作用を発揮する IoT アクチュエータに求められるセキュリティ要件と、攻撃者が常に傍らに存在するというサイバー空間の変化を踏まえた、現実世界に変化を及ぼす制御に係るセキュリティのフレームワークについて検討し、ゼロトラスト(Zero Trust)と呼ばれるセキュリティの新しい概念を取り入れた IoT アクチュエータにおけるセキュリティ方式を、ゼロトラスト IoT セキュリティフレームワーク(ZeTiots-FW)として提案した。

また、本提案に基づく IoT アクチュエータを導入することで、CPS の強靭化による社会の安全安心の確保、そして Long Term Cyber Security Resilience を備えた Society5.0 の実現につながるものと考える。

2.　IoT アクチュエータにおけるセキュリティ

2.1　IoT アクチュエータの特徴

世界の IoT デバイスの総数は、2023 年に約 340 億台に達すると予想されている。分野別では、これまで増加してきた「通信」に代わって、「医療」「コンシューマー」「産業用途」「自動車・宇宙航空」が高い成長を見せると予想されている[3]。

この IoT デバイスの有する次の特徴は、従来の IT 機器とは異なるサイバーセキュリティやプライバシーのリスクに影響を与えるとされている[4]。

A)　トランスデューサ機能

[1] This dissertation is based on “Proposal of Zero Trust Security Scheme for IoT Actuators” [21], by the same author, which appeared in the 40th Symposium on Cryptography and Information Security, Copyright (C)2023 IEICE.

物理世界と相互作用し、デジタル環境と物理環境の間のエッジとして機能する。すべての IoT デバイスは、2 種類のトランスデューサ機能のうち、少なくとも 1 つを備える。

センシング機能

物理的な世界のデータを測定し提供する能力

例：温度、光センシング、オーディオセンシング、レーダー

アクチュエータ機能

物理的な世界に変化をもたらす能力

例：ヒーターコイル、スピーカ、電子ドアロック、ドローン操作、サーボモーター、ロボットアーム

B)　インタフェース機能

デバイス間インタラクション（デバイスとデバイス、デバイスと人間など）を可能にする機能。

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 機器と人間が直接コミュニケーションをとるための機能

例：タッチパネル、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、LPWA

C)　サポート機能

他の IoT 機能にも対応できること

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

本稿では、A）トランスデューサ機能としてアクチュエータ機能を持つ IoT デバイスを「IoT アクチュエータ」と呼ぶ。IoT アクチュエータは、物理世界に影響を与えることができるため、サイバー攻撃により人命や安全が脅かされたり、機器や設備の破損・破壊、社会インフラなどの重要サービスの停止などの大きな障害が発生したりする可能性がある。Society 5.0 に向けたスマートシティでは、多数の IoT アクチュエータが導入・活用されることとなり、そのセキュリティを確保することが重要である。

2.2　IoT アクチュエータにおける特有のセキュリティの課題

IoT システムは IT と OT の融合であるため[4]、IT に関するサイバーセキュリティの課題は、IoT システムの課題にも包含される。その一例を以下に示す。

- 既知の脆弱性に対する対策の実施
- 脅威分析・リスクアセスメントに基づく対策検討
- 実装時のバグや機能不足の回避・発見

- 通信セキュリティ（FW、IPS/IDS、暗号化など）
- 認証とアクセス制御の実装
- クレデンシャルとトラストアンカの保護と更新
- ロギングと解析

これまで長年取り組まれてきた IT システムのセキュリティに関する研究は、成果が蓄積されており、IoT システムにも活用できるため[4]、後述する「認証・アクセス制御」を除き、本稿では検討対象から除外している。なお、個々の IoT デバイスの制約（計算資源など）により活用が困難な場合は、別途検討する必要がある。一方、本稿では、IoT システムの特徴[4]として挙げられている以下の項目に着目する。

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。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 デバイスは機能や性能には制限がある。
f) 開発者が想定していない IoT システムとの接続の可能性がある

これらの特徴から、b) IoT デバイスの出荷後に発見された脆弱性が脆弱性対応に影響を与える可能性がある、c) 脆弱性がパッチやアップデートされないまま放置される可能性がある、e) IoT デバイスのリソース制限によりパッチの適用が困難な場合がある、f) IoT デバイスはセキュリティリスクに対して脆弱な場合がある、といった懸念が生じる。更に、パッチやアップデートの提供に関して、経済的な観点から以下の指摘がなされている[5]。

- 現在、デバイスベンダやメーカは、IoT のパッチの継続的なアップグレードを保証する金銭的なインセンティブをほとんど持っていない
- IoT デバイスのメンテナンスは、企業の収益がメンテナンスではなく、デバイスの販売によってもたらされるため、収益を減少させる可能性がある
- 販売者は、販売後の継続的なメンテナンスに法的な責任を持たない（日本の国土交通省は車検制度により自動車の安全性を確保している[6]）
- ベンダは、既存の機器を維持するよりも、継続的な販売によって利益を最大化するために、機器の計画的陳腐化を追求する傾向がある
- IoT デバイスの管理会社・団体の倒産・解散

IoT アクチュエータを含む IoT システムにおいては、これらの条件、特性、指摘に伴うリスクを考慮する必要がある。

3. 関連研究

3.1 現実世界との相互作用に係るセキュリティ

IoT システムは多様であり、使用する IoT 機器やシステム構成が類似していても、IoT システムの目的や用途によって、求められるセキュリティ対策が異なることが指摘されている[7]。IoT 機器は、現実世界のデータを入手するセンサ機能と、現実世界に物理的な変化を及ぼすアクチュエータ機能の、双方についてセキュリティが必要である[4]。センサ機能に関するセキュリティは、計測セキュリティ[8]と呼ばれ、音声入力を受け付けるスマートデバイスに対して超音波で不正なコマンドを入力する攻撃[9]、スピーカから生成されたアナログ信号が他の IoT センサのマイクの不正入力につながる攻撃[10]などの研究がある。そのアプローチとしては、センサへの入力を分析することが一般的であった。すなわち、図 1 において現実世界からサイバー空間に流入（Ingress）する(A)のアナログ信号に関する攻撃への対策の研究となる。

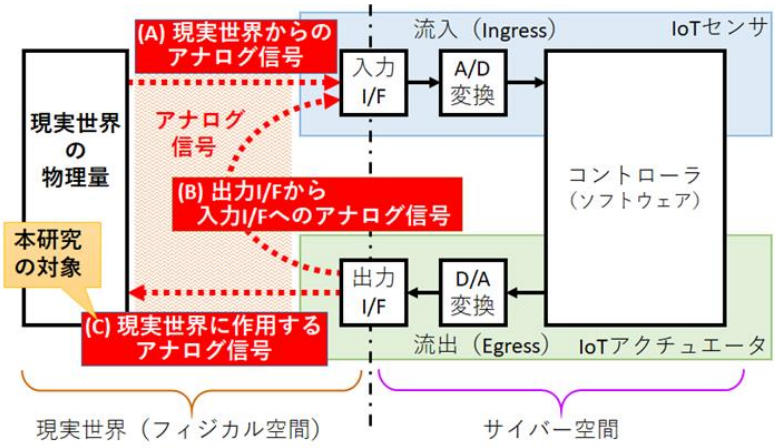

図 1: CPS におけるアナログ信号の分類

一方で、サイバー空間から現実世界に流出（Egress）する(B)のアナログ信号に関する攻撃の研究として、IoT アクチュエータの 1 つとされるスピーカへの脅威に注目した先行研究[11]がある。この先行研究では、センサへのアナログ信号の脅威への対策として、ファイアウォールに似た仕組みで CPS のアナログ信号出力を検知・規制する Cyber-Physical Firewall（CPFW）フレームワークを提案している。CPFW でコントローラのデジタル信号出力への出力アクセスを制御し，デジタル-アナログ変換後の出力インタフェースから安全なデジタル信号出力のみを出力することで、音信号がもたらす脅威への対策として CPFW が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多種多様な脅威が存在することを挙げ、既知の攻撃に対するアクセス制御ポリシーを策定し、事例評価により効果を確認している。一方、スピーカと異なり、モータなど運動によって環境に変化をもたらす場合は今後の課題とし、さらにアクチュエータに起因する二次的な影響については、機械工学的なアプローチが必要だとしている。また、原理的に既知の攻撃のみが対策の対象となる。

このことから、特に「(C) 現実世界に作用するアナログ信号」が引き起こす攻撃への対策という重要な課題が解決されておらず、早急な取り組みが必要な状況にあると考える。そこで本研究では、現実世界に作用するアナログ信号に関する攻撃への対策について検討する。

3.2　　ゼロトラスト（Zero Trust）

今日の IT システムは、クラウドサービスとの連携や、モバイル環境での端末によるリモートワークなど、複雑なネットワーク環境下で運用されている。このような複雑な環境では、組織の内部と外部の境界を一意に定義することが難しく、従来の境界防御型のセキュリティ対策ではサイバー攻撃を防ぎきることが困難であると考えられている。そこで現在、「ゼロトラスト」という新しい概念が注目されており、それに基づく「ゼロトラスト アーキテクチャ」というサイバーセキュリティ・アーキテクチャが注目されている[12]。

ゼロトラストは、リソースの保護に焦点を当て、信頼は決して暗黙のうちに与えられるものではなく、継続的に評価されなければならないという前提に基づいている。これは、攻撃者が境界の内側に存在し、外側の人と同様に信頼できないことを前提としているためである。

また、リソースはデータに限らず、計算資源や IoT のアクチュエータも含まれることを想定している。そして、完全に排除することが難しい攻撃者によるサイバー攻撃を低減するために、認証、認可、暗黙の信頼区間の縮小に焦点を当てており、可用性の維持と認証メカニズムの時間遅延を最小化することを目的としている。更に、アクセス制御ルールは、リクエストの実行に必要な最小限の権限を強制するため、可能な限り粒度の細かいルールにすることが前提となっている。ゼロトラストアクセスの概念図を図 2 に示す。

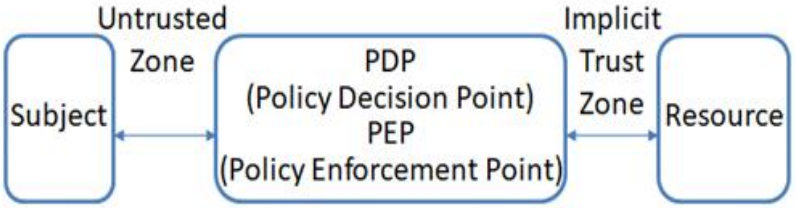

図 2: Zero Trust Access の概念図

主体（Subject）がリソースにアクセスする場合、PDP（ポリシー決定ポイント）と対応する PEP（ポリシー実施ポイント）を経由する。しかし、PDP/PEP を越えて追加のポリシーを適用することはできない。したがって、PDP/PEP とリソースの間の暗黙の信頼領域は可能な限り小さくする必要がある。ゼロトラストの基本的な考え方を以下に示す

1. すべてのデータソースとコンピューティングサービスをリソースとして考慮
2. ネットワークの場所に関係なく、すべての通信を保護
3. リソースへのアクセスは、セッションごとに許可
4. リソースへのアクセスは、クライアント ID、アプリケーションサービス、要求しているアセットの状態、その他の行動属性・環境属性を含むダイナミックポリシーによって決定
5. すべての資産の整合性とセキュリティ動作を監視し、測定
6. すべてのリソースの動的な認証と承認、アクセス許可前の厳格な実施
7. 資産、ネットワークインフラ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に活用

行動属性とは、上記 4.で示したアクセス主体の分析、観測された利用パターンからの逸脱などである。環境属性には、アクセスのタイミングや現在進行中の攻撃の検出などが含まれる。これらの属性は時間や履歴、状況の変化に影響されるため、それらを考慮したアクセスルールであるポリシーを動的に適用することでアクセスを決定する。

図 3 は、ゼロトラストアーキテクチャを構成する論理的な構成要素と、それらの相互作用の基本的な関係を示す概念的な枠組みモデルである[13]。

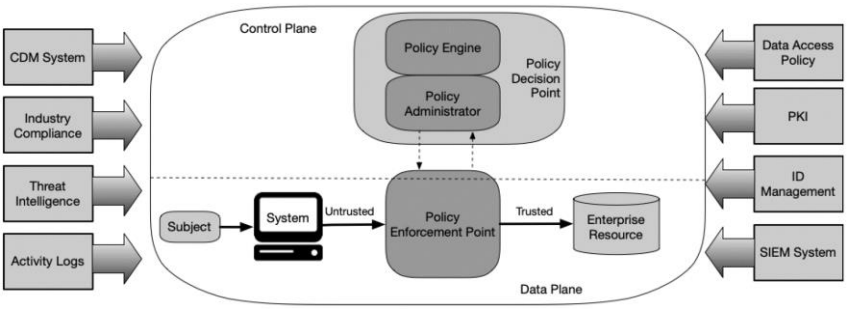

図 3: ゼロトラストの論理的構成要素［13］

PDP は PE（ポリシーエンジン）と PA（ポリシーアドミニストレーター）という 2 つの論理コンポーネントに分解されている。

PE（ポリシーエンジン）

主体（Subject）のリソースへのアクセスを許可するかどうかの最終決定は、Trust Algorithm (TA)によって行われる。外部ソース（CDM システム、脅威インテリジェンスなど）とポリシーを Trust Algorithm のインプットとして使用し、リソースへのアクセスを制御する。

米国では、NIST がデータ要素間の関係性に基づく ABAC（属性ベースのアクセス制御）の規格である NGAC（Next Generation Access Control）［14］の参照実装として、多様なアクセス制御ポリシーに対応することを目的に、ポリシーマシン［13］を開発中である［15］。

PA（ポリシーアドミニストレータ）

PA は PE と密接に連携し、アクセスを許可するか拒否するかの判断を PE に委ねる。PA は PE の判断に基づき、PEP にエンティティやリソース間の通信経路を確立またはブロックさせる。

PEP (ポリシーエンフォースメントポイント)

PEP は PA と連携し，PA からポリシーの更新を受信する．そして、受信したポリシーを適用して、主体（Subject）とリソース間の通信経路の確立、遮断、監視を行う。

TA (Trust Algorithm)

PE でアクセス権を決定する際のアルゴリズムを TA と呼ぶ。このアルゴリズムは、以下のように分類される。

A)　アクセスリクエスト
B)　主体(Subject)に関するデータベースとヒストリ
C)　リソースに関するデータベース
D)　リソースポリシの要求事項
E)　スレットインテリジェンスとロギング

また、TA の実装方法は、その特徴により大きく 2 つに分類される。

1.　基準ベース（2 値）／スコアベース（重み付け）
2.　単一（個別要求）／文脈的（履歴を考慮）

文脈的でスコアベースの TA は、動的できめ細かいアクセス制御を実現すると考えられている。

3.3　TEE（Trusted Execution Environment）

IoT アクチュエータにおいて、マルウェア等の攻撃による影響を受けずにセキュリティに係るクリティカルな処理を実行する観点から、IoT アクチュエータなどの IoT 機器に採用されている半導体チップの一種である SoC（System on Chip）のハードウェアセキュリティ機能である TEE（Trusted Execution Environment）［14］に着目した。

TEE は、アプリや OS から独立した隔離された実行環境であり、隔離された実行環境内の Secure World は、アプリや OS が実行される Normal World の影響を受けずに処理を行うことが可能である。従って、ゼロトラストにおける PEP に係る処理を、Secure World 内に配置することで、マルウェアなどの攻撃から保護することができる。TEE を提供するハードウェアの例として、Arm TrustZone [15]、RISC-V Keystone [16]、Intel SGX [17][18] 等がある。

4.　ゼロトラスト IoT セキュリティフレームワーク

IoT アクチュエータのセキュリティ対策としては、CPFW の考えに基づき、コントローラと出力インタフェース間の信号伝送の過程で、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であると考えられる。一方、個々の脅威に特化したポリシー策定を行う場合は、ポリシー数の増加や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信号の種類によって、アナログ信号から抽出できる情報（ATTRIBUTE）と脅威信号の関係が異なると考えられており、この関係を明確にする必要がある。そして、出力インタフェースへのアクセス制御で脅威信号を規制できたとしても、二次的な影響でより深刻な事態になることが懸念されるため、IoT システムのサービス継続性の観点からも上位のポリシーとの整合性を確保する必要がある。

4.1　　想定する IoT システムの概略

IoT システムにおいて、IoT アクチュエータは、クラウド上の IoT サービスと連携することで、さまざまな付加価値を提供する。この場合、IoT アクチュエータ上で動作するアプリケーションは、IoT サービスからの要求に応じて、物理空間内のアクチュエータを制御する。なお、IoT アクチュエータは、もう一つのトランスデューサ機能であるセンシング機能を有していてもよい。IoT アクチュエータと IoT システムの概略を、以下に示す。

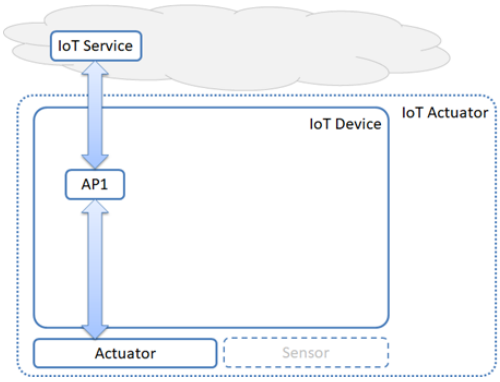

図 4: IoT アクチュエータを含む IoT システム

物理空間におけるアクチュエータの代表的なものに、モータがある。モータとは、電力を用いて物理的な回転運動を発生させる装置である。この回転運動は、河川防災システムや水田用水供給システムのポンプを駆動したり、ドローンのプロペラや自動配送ロボットの車輪を回転させたりするために利用される。図 5 は、本論文で想定しているモータ付き IoT アクチュエータのデバイス構成例である[19]。図 5 のように、IoT デバイスがコントローラに相当する。また、モータドライバとモータで構成されるモータユニットがアクチュエータに相当する。

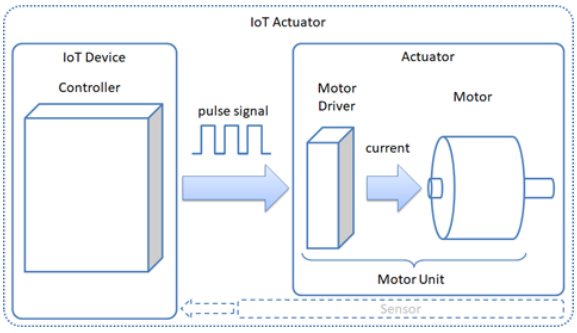

図 5: IoT アクチュエータの構成例

4.2　　現実世界の物理量変化を考慮した出力のアクセス制御方式

IoT アクチュエータを攻撃するマルウェアは、IoT デバイス上で動作するアプリケーション（ソフトウェア）に感染し、アクチュエータに対してサイバー攻撃を仕掛けることが想定される。しかし、2.2 節で指摘したように、脆弱なプログラムを早急にアップデートすることは不可能である。更に、プログラムの更新やパッチの提供が遅れたり、提供されなかったりするケースもある。さらに、近年では、パッチや回避策が公開される前にソフトウェアの脆弱性が発見され、悪用されるゼロデイ攻撃も深刻な問

題となっている。

そこで、マルウェアに感染したアプリケーションが不正なアクチュエータを制御することを防ぐため、ゼロトラストの考え方に基づき、CPFW に相当する機能を検討する。まず、ゼロトラストアーキテクチャにおける PDP と PEP は、PDP をクラウド側に、PEP を IoT アクチュエータ側に配置する。この PEP が CPFW として機能することで、不正な制御を防止する。また、PDP は IoT サービスと連携することで、対象アプリケーションの行動属性や環境属性を取得することができる。これにより、PEP は PDP と連携し、動的なポリシーに基づく機器アクセス制御を行うことができる。IoT アクチュエータにおけるゼロトラストの適用の概略を以下に示す。

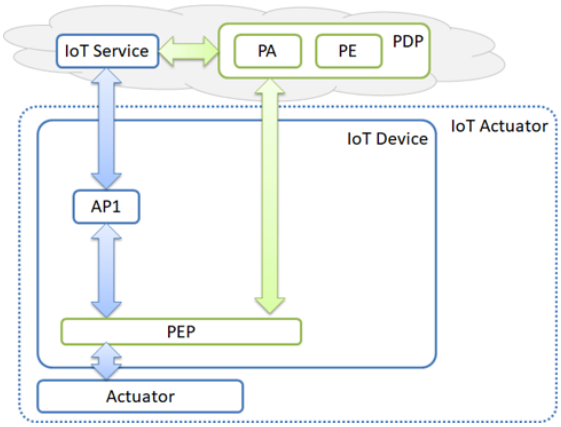

図 6: IoT アクチュエータへのゼロトラストの適用

しかし、IoT アクチュエータに追加された PEP がマルウェアの新たな攻撃対象になることが懸念される。PDP がクラウド側のセキュリティ対策で守られていても、PEP による適切なアクセス制御が行われていなければ、アクチュエータへの攻撃や物理空間への被害が発生する可能性があると考えられる。

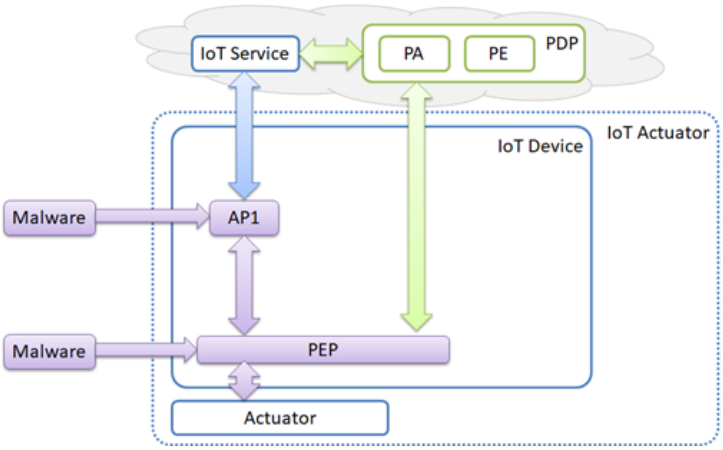

図 7: PEP に対するサイバー攻撃の例

そこで、IoT アクチュエータなどの IoT 機器に採用されている半導体チップの一種である SoC（System on Chip）のハードウェアセキュリティ機能である TEE（Trusted Execution Environment）に着目し

た。Secure World による PEP 保護の模式図を以下に示す。

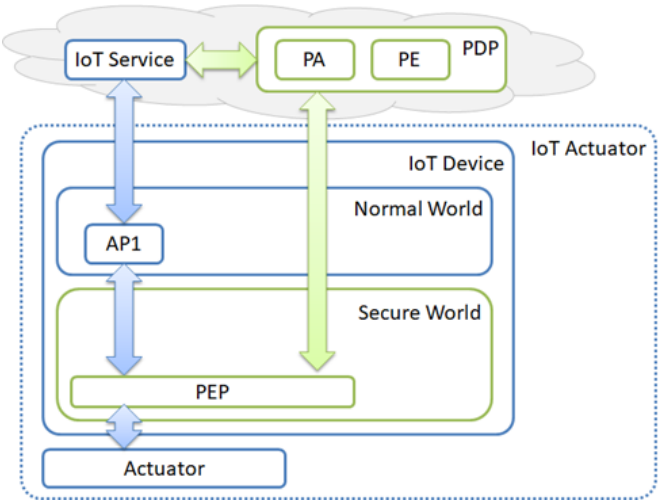

図 8: TEE による PEP の保護

この構成により、PEP がマルウェアに感染したアプリケーションによるアクチュエータの不正な制御を防止することが可能となる。また、PEP 自身がマルウェアに感染することを防ぐことも可能である。ただし、マルウェアに感染したアプリが PEP と PDP の連携を妨害するサービス拒否攻撃（DoS 攻撃）を受ける危険性がある。また、正常なアプリがアクチュエータを適切に制御できないため、IoT アクチュエータが本来果たすべきサービスを提供できなくなるリスクもある。

図 9 は、IoT アクチュエータに対する DoS 攻撃の一例を示している。IoT アクチュエータは、物体の動きの可否が重要なアプリケーションでの利用が想定されるため、このような DoS 攻撃への対策が必要である。

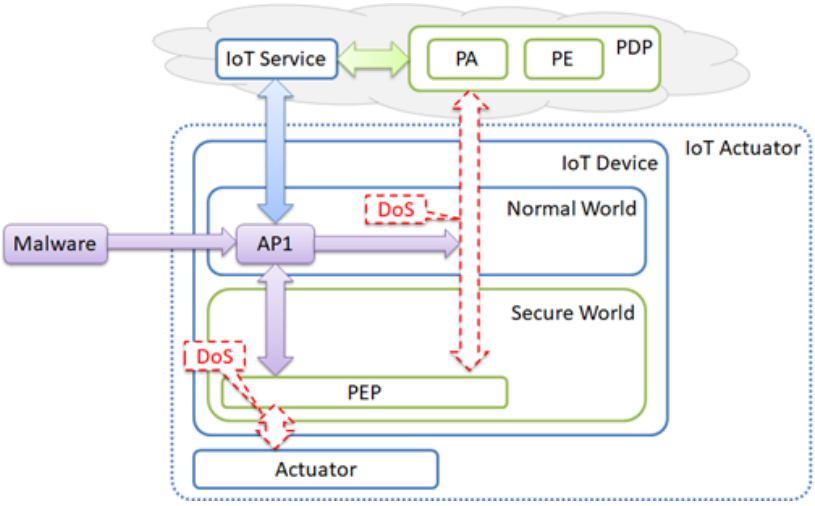

図 9: DoS を引き起こすサイバー攻撃の例

そこで、クラウド側の PDP と IoT アクチュエータ内の PEP が連携できない事態に備え、PDP のサブセットである Self PDP を IoT アクチュエータに導入することとする。しかし、Self PDP の PEP へ

の入力は IoT アクチュエータ内に限定されるため、TA による処理は限定される。一方、PEP と Self PDP の連携に必要な通信リソースが不要になり、リアルタイム性・可用性の向上が期待できる。また、通常のアプリケーションがアクチュエータを正常に制御できないことによる IoT アクチュエータの二次被害を軽減するため、Failsafe 機能を持つアプリケーションを IoT アクチュエータに導入する。例えば、モータの回転数を徐々に下げるなど、アクチュエータが動作中に安全に停止するように制御する機能を提供する。また、Failsafe 機能の応用として、IoT デバイスの EOL（End of Life）を実現することも可能である。Failsafe 機能による EOL の管理は、管理されていない IoT 機器が DDoS 攻撃ボットなどに悪用されることを防ぐというメリットがあり、これは前章の IoT システムの特徴 b）と c）に関連する。また、マルウェア攻撃への対策として、PEP と同様に Self PDP と Failsafe AP を Secure World に配置する必要がある。

最終的に、Zero Trust アーキテクチャを IoT アクチュエータに適用した構成要素間の関係を「Zero Trust IoT セキュリティフレームワーク」として図 10 に示す。

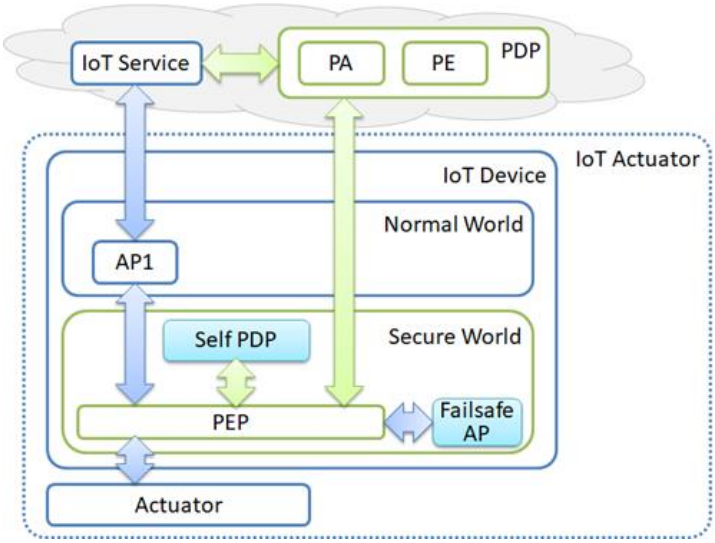

図 10: ゼロトラスト IoT セキュリティフレームワーク

5. 実装方法の検討と予備実験

5.1 PEP の保護と出力ポートのアクセス制御

Arm®のプロセッサが提供する TEE 機能は、TrustZone®と呼ばれており、主にスマートフォン等で利用される Cortex®-A と、マイクロコントローラ等で利用される Cortex®-M などのラインナップがある。今回は IoT アクチュエータでの活用を念頭に、Arm® Cortex®-M を搭載した開発用ボードを対象として実装方法の検討を行った。今回対象とした IoT アクチュエータ実験用ボード[20]の主な仕様を表 1 示す。

表 1　IoT アクチュエータ実験用ボードの仕様

項目	スペック
ボード名称	STMicroelectronics 社製 STM32L562E-DK
SoC（MCU）	STM32L562QEI6QE (Arm® Coretex®-M33) core with TrustZone®
Flash memory	512 Kbytes
SRAM	256 Kbytes
無線通信 I/F	Bluetooth® V4.1 Low Energy
外部通信線および電源	USB-Micro-B STLINK-V3E

まず、PEP の保護について述べる。TrustZone®では、メモリ空間が Secure World と Normal World として区別される。また、プロセッサの状態も Secure / Non-secure として区別され、Non-secure な状態では、Secure World のメモリ空間にアクセスすることはできない。従って、PEP 等のセキュリティに係るクリティカルな処理を、Secure World 側に配置することで、マルウェア等の攻撃から保護することが可能である。

更に、IoT アクチュエータにおいて外部出力の際に利用する出力ポートのアクセス制御について述べる。CPFW 機能で利用する出力ポートは、PEP 以外からの利用を制限する必要があるが、メモリと同様にポートを含むペリフェラルについても Secure World 側に割り当てた場合に、Non-secure な状態で利用することを制限することが可能である。

また、Secure World に割り当てるメモリやポート等のハードウェア資産は、実験用ボードの設定変更ツールにより指定できることが確認できた。この設定は、起動時に固定的に設定され、起動後の変更手段は提供されていない。

従って、TrustZone®に対応した Coretex®-M を搭載する本実験用ボードにより、本稿にて提案するゼロトラスト IoT セキュリティフレームワーク(ZeTiots-FW)を実装可能であることが仕様上で確認できた。

5.2　予備実験

IoT アクチュエータにおけるゼロトラスト IoT セキュリティフレームワーク(ZeTiots-FW)の実装に向けた予備実験として、IoT システムを模擬した簡易的な実験用 IoT 排水システムを準備した。実験用 IoT 排水システムの全体像を図 11 に示す。

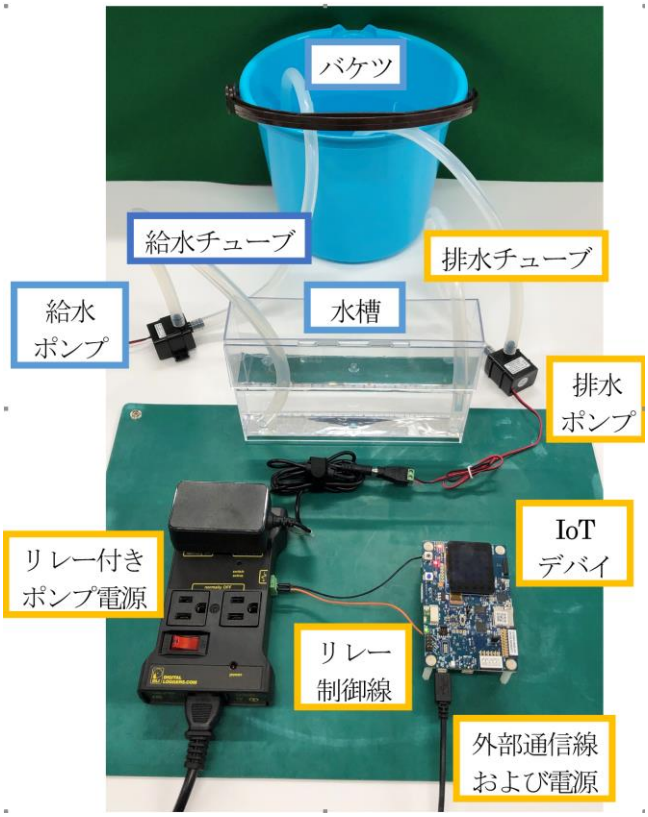

図 11: 実験用 IoT 排水システム

本システムでは、外部から水の流れ込む水槽と、水槽の水を排水ポンプによりバケツへ排出する排水ポンプを設置し、排水ポンプの稼働／停止に必要となる電源を、IoT デバイスから ON/OFF 制御することが可能となっている。

今回は、Secure World 側の PEP による CPFW 機能による排水ポンプの出力制御と、Non-secure 状態での排水ポンプの出力制御に利用している出力ポートへのアクセス制限について、確認を行った。IoT デバイスで動作している Secure World 側の PEP に相当するサンプルプログラム１から、排水ポンプの電源が ON/OFF 制御できることと、マルウェアに感染した不正なアプリに相当するサンプルプログラム２から排水ポンプの出力制御に利用している出力ポートへのアクセスが無効となることを確認できた。

6. おわりに

本研究では、特に、サイバー空間から物理空間へのフィードバックとして物理的な作用を発揮する IoT アクチュエータに求められるセキュリティ要件と、攻撃者が常に傍らに存在するというサイバー空間の変化を踏まえた、現実世界に変化を及ぼす制御に係るセキュリティのフレームワークについて検討し、ゼロトラスト(Zero Trust)と呼ばれるセキュリティの新しい概念を取り入れた IoT アクチュエータにおけるセキュリティ方式を「Zero Trust IoT セキュリティフレームワーク（ZeTios-FW）」として提案した。また、実装方法の検討と予備実験により、提案方式の実装可能性を確認した。

参考文献

[1] Antonakakis, M. et al.: Understanding the mirai botnet: Proc. 26th USENIX Conference on Security Symposium, pp.1093–1110 (2017)
[2] Vignau, B., Khoury, R., Hall´e, S.: 10 Years of IoT Malware: A Feature-Based Taxonomy, 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp.458–465 (2019)
[3] 令和 3 年版情報通信白書，pp.43, 総務省，令和 3 年 7 月 30 日，https://www.soumu.go.jp/johotsusintokei/ whitepaper/ja/r03/pdf/01honpen.pdf,
[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] George Corser, Glenn A. Fink, Mohammed Aledhari, Jared Bielby, Rajesh Nighot, Sukanya Mandal, Nagender Aneja, Chris Hrivnak, Lucian Cristache, Internet of Things (IOT) Security Best Practices: whitepaper, IEEE, 2017,
https://standards.ieee.org/wp-content/uploads/import/documents/other/whitepaper-internet-of-things-2017-dh-v1.pdf
[6] 【別紙１】自動車の特定改造等の許可制度について（概要），国土交通省自動車局, 令和２年８月５日, https://www.mlit.go.jp/report/press/content/001358067.pdf
[7] IoT セキュリティガイドライン ver1.0, 総務省、経済産業省、IoT 推進コンソーシアム, 2016 年 7 月, https://www.soumu.go.jp/main_content/000428393.pdf
[8] 松本 勉,「計測セキュリティ」の研究課題, 信学技報, vol. 116, no. 35, ISEC2016-8, pp. 35-35, 2016 年 5 月
[9] Guoming Zhang et al., DolphinAttack: Inaudible Voice Commands. In the 24th ACM SIGSAC Conference on Computer and Communications Security, CCS. 103–117. (2017)
[10] Wenbo Ding et al., On the Safety of IoT Device Physical Interaction Control. In The 25th ACM SIGSAC Conference on Computer and Communications Security, CCS. 832–846. (2018)
[11] 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
[12] 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
[13] 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

[14] 須崎有康, 塚本明, 小島一元, 中嶋健太, Hoang Trong Thuc, 師尾彬, “TEE 比較”、Symposium on Cryptography and Information Security (SCIS) 2020 (2020).
[15] S. Pinto and N. Santos, “Demystifying Arm TrustZone: A Comprehensive Survey,” ACM Computing Surveys (CSUR), vol. 51, no. 6, 2019
[16] D. Lee, D. Kohlbrenner, S. Shinde, D. Song and K. Asanovi´c: “Keystone: A framework for architecting tees”, arXiv (2019).
[17] V. Costan, I. Lebedev, and S. Devadas, “Secure Processors Part I: Background, Taxonomy for Secure Enclaves and Intel SGX architecture,” Foundations and Trends in Electronic Design Automation, vol. 11, no. 1-2, pp. 1-248, 2017.
[18] V. Costan, I. Lebedev, and S. Devadas, “Secure Processors Part II: Intel SGX Security Analysis and MIT Sanctum Architecture,” Foundations and Trends in Electronic Design Automation, vol. 11, no. 3, pp. 249-361, 2017.
[19] ステッピングモータの概要と特徴，オリエンタルモーター株式会社，https://www.orientalmotor.co.jp/products/stepping/overview_1/.
[20] STM32 / STM8 Discovery 開発ボード：STM32L562E-DK, STMicroelectronics 社，https://www.stmcu.jp/design/hwdevelop/discovery/72186/
[21] Nobuhiro Kobayashi, “Proposal of Zero Trust Security Scheme for IoT Actuators,” the 40th Symposium on Cryptography and Information Security, 2D3-3, 2023.