サービスロボット・セキュリティガイドライン

第１版

2019 年 5 月

公立大学法人会津大学
TIS 株式会社
ネットワンシステムズ株式会社

目次

１．はじめに　本書の内容と目的

１－１．ロボット・セキュリティの現状と課題

【時代背景】

従来のロボットは、産業用ロボットに代表されるように、特定の環境下で特定の仕事をすることが中心であった。しかし、社会環境の変化や IoT・AI などの技術の進展とともに、ロボットが日常生活空間に入り込み、人間と共生する時代が来つつある。

産業分野だけではなく、介護、清掃、食事支援、災害復旧作業などあらゆる生活の場面で利用され、人とロボットが日常生活の中で共存・共栄することが想定される。人口減少、高齢化社会、災害の多発などがこのような状況を後押ししている。

【ロボット技術の進化】

ロボット技術も近年目覚ましい進化をとげている。従来の特定の環境下で特定の仕事をするロボットから、自律的に環境を認識して、いろいろな仕事をするロボットへと進化してきている。生活空間等、状況が変わりやすい環境下でもロボットが確実性をもって稼働する技術が進展しており、その中には、移動、マニュピュレーション、ユーザーインターフェス、環境認識（センサー)、自律化、知能化、通信技術などが含まれる。

【セキュリティの重要性】

外部との通信から閉ざされていた環境での利用されていたロボットが、ネットワーク・クラウドを介して様々な情報や知識を交換し、複数のロボットが協調動作するクラウド・ロボティクスの考えも進展している。

将来は、通信環境に応じた制御やセキュリティを考慮する必要があることは確実である。ロボットの利用形態の進化とともに、悪意のある外部からの攻撃への対策と保護はますます重要になってくる。

今後のロボットは、次のような新しい特徴をもつ。

- 様々な環境で利用されること
- 人間と共生すること
- 認識情報が多いこと
- ネットワークを介して他のロボットやシステムと協調すること

様々な利用形態の中での脅威やリスクを評価しながら使っていくことが必要であり、そのためのガイドラインは必要である。このような状況の中で、IoT、制御系はガイドラインがあるが、サービス・ロボットに照準を当てたものは現段階では皆無である。

１－２．本書の目的

本書は、ロボットシステムの設計・開発者が実装する機能に対して想定される脅威と対策のてがかりとして活用されることが目的である。悪意のある攻撃者によるセキュリティの侵害が、安全性の阻害につながらないように対策を打つ必要がある。市場に出てからは対策

が難しい面もあるため、設計・開発の段階で考慮することが望ましい。これにより、サービス・ロボットの実用化・普及の促進につながることが大きな狙いである。

また、本書は、ソフトウェア的なサイバー攻撃への対策の視点をとっており、直接的な物理攻撃(電磁波攻撃、装置の破壊・盗難など物理的な攻撃)については、考慮の対象外とした。

２．対象ロボットシステムとその特性

２－１．ロボットの分類

ロボットは、利用用途別、利用される場所や環境、提供機能などによって様々な種類のロボットが存在し、分類の仕方も様々である。図１は利用される環境と提供する機能という視点からロボットの種類を分類したものである。

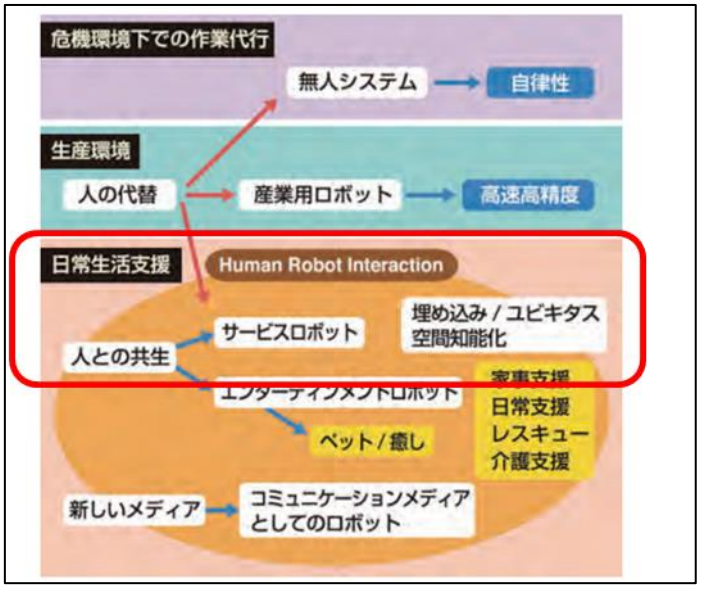


図 1. ロボットの分類（出典：NEDO ロボット白書 ）

本書は、この中で日常生活を支援するサービス・ロボットを対象とする。人の生活の質の改善・向上に寄与するロボットである。

（参考）ISO13482 は、**生活支援ロボット**、**サービス・ロボット**を以下のように定義している。

- **生活支援ロボット**＝医療用を除く、人の生活の質の改善に直接寄与する行為を実施するサービス・ロボット
- **サービス・ロボット**＝産業オートメーション用途を除き、人または機器のために有用なタスクを実行するロボット

２－２．ロボットシステムの基本構成

ロボットシステムは、元来は、認識（センサー）系、制御系、駆動系の３要素をあわせもつものとされてきた。しかし、昨今は、機能の多様化・分散化が進んでおり、様々な形の構成のモデル化が考えられる。本書では、機能を抽象化した論理部位として、認識部、制御部、動作部（サービス部）の３部から構成されるものとして扱う。

図 2 にロボットシステムの基本構成概念、表１にロボットシステムの構成要素を解説する。

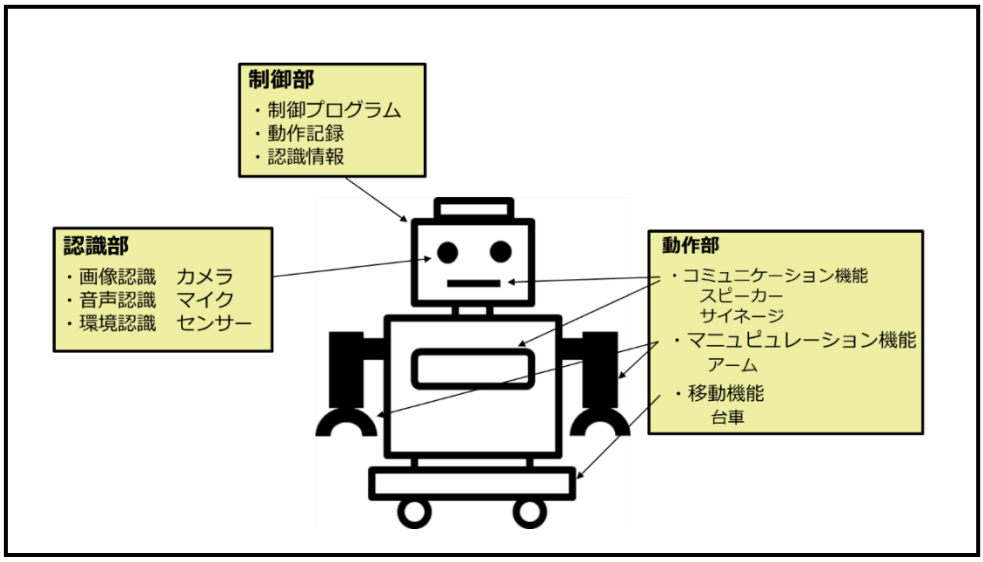


図 2. ロボットシステムの基本構成

表 1. ロボットシステムの構成要素解説

名称	解説	提供機能	構成部品例
制御部	ロボットの動作を制御する部分	制御、管理、通信	
認識部	ロボットが動作するために必要な情報を認識する部分	・画像認識 ・音声認識 ・環境認識 etc	・カメラ,etc. ・マイク,etc. ・各種センサー etc
動作部（サービス部）	ロボットが目的のサービスを提供するために必要な動作を実行する部分	・利用者とのコミュニケーション機能 ・移動機能 ・マニュピュレーション機能 etc	・台車 ・アーム ・スピーカー etc

２－３．ロボットシステムのネットワーク構成

本書で扱うロボットシステムは、利用される敷地や建物内の IP ネットワーク、IoT ネットワークに接続されるのが通常である。ただし、システムの利用用途や構造、環境などによってフィールドネットワークに接続される場合もある。また、5G などの高速インターネットモバイル回線の普及とともにインターネットに直接接続される形態も将来想定される。

ロボットシステムのネットワーク接続構成を図 3 に示す。

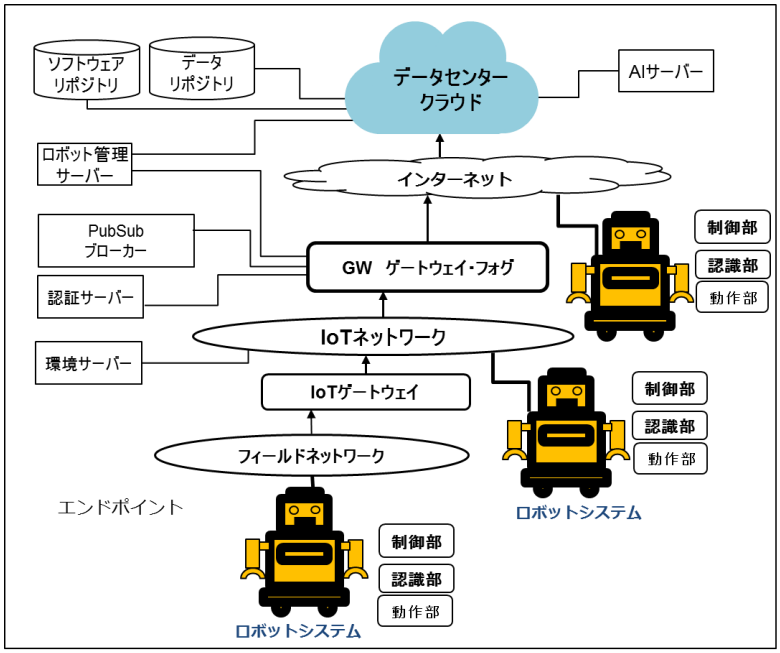


図 3. ロボットシステム　ネットワーク構成図

表 2. ネットワーク構成要素解説

名称	解説
データセンター・クラウド	上位システム（データレポジトリ・AI・統合管理システム）などが設置される
インターネット	インターネットを介して IoT ネットワーク同士が接続される
ゲートウェイ・フォグ	インターネットと IoT ネットワークの境界に位置し、管理システムや中継システムなどが設置される。
IoT ネットワーク	機器同士が IP 通信するネットワーク
IoT ゲートウェイ	フィールドネットワークと IP ネットワークとの境界
フィールドネットワーク	非 IP ネットワーク RS232C,RS485 などのシリアル回線、LoRaWAN、Bluetooth、Zigbee などの無線などが利用される。
エンドポイント	接続される物理機器

３．セキュリティ検討の流れ

３－１．セキュリティ検討の流れ

サービス・ロボットは、関連している情報やシステムが多岐にわたること、利用される環境が限定されないことから、ソフトウェアの構造やシステム間の通信フローも複雑である。また、サービス・ロボットの開発に利用されている ROS、Open RTM などのロボットミドルウェア・プラットフォームも本格的なセキュリティ対策を考慮し実装されるようになるのは、これからである。したがって、個々のロボットシステムの利用形態の中で脅威やリスクを分析し評価しながら使っていくことが前提となる。システムの設計段階で想定される脅威・リスクを洗い出し分析した上で対策を検討することが非常に重要である。

本書では、以下のような流れと工程でシステムのセキュリティ対策を検討する。

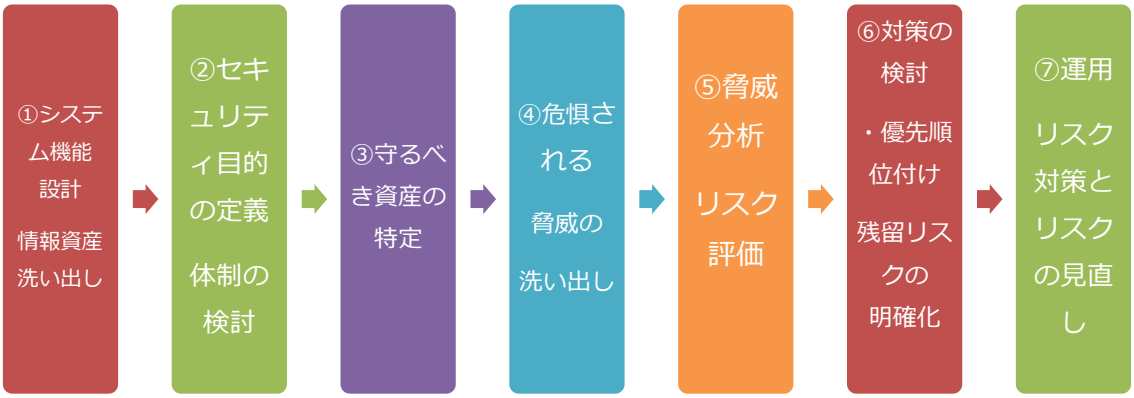


図 4. セキュリティ検討の流れ

表 3. セキュリティ検討の項目解説

項目	説明
システム機能設計・情報資産洗い出し	開発するロボットシステムの機能要件、関連する情報資産を洗い出す
目的の定義・体制の検討	セキュリティ実現の目的を定義する。また、それを実現するための体制を検討する。
守るべき情報資産の特定	守るべき機能、情報を特定する。
危惧される脅威の洗い出し	開発者の視点から危惧される脅威を洗い出しを行う。
脅威分析・リスク評価	システムの構造や利用方法から脅威の潜在的要因や影響を分析する。それによってリスクを評価する。

対策の検討・優先順位付け、残留リスクの明確化	脅威に対する対策を検討し、優先順位付けをして実施する。 また、対策によって残留するリスクも明らかにする
運用　リスク対策とリスクの見直し	リスク対策を実施し、運用する。 定期的にリスクを見直す。必要に応じて追加の対策を行う

３－２．ロボットシステムにおいて保護されるべき資産

セキュリティ上保護されるべき対象の資産には、機能と情報がある。

個々のシステムで守るべき資産と、機能上要求される可用性、完全性、機密性などの条件から、セキュリティの目標を定義する必要がある。

本項では、ロボットシステムで保有する主要な情報資産を洗い出した結果を表.4 に示す。

表 4. ロボットシステムの情報資産

分類	資産名	解説	保有場所・保有形態
動作・制御情報	制御シナリオ情報	ロボットの動作内容や一連の動作の流れを示した情報	ロボットの制御部に保有 通常上位のシステムで開発された内容がダウンロードされる
	状態情報	ロボットの現在位置や姿勢、動作状態を表した情報	ロボットの制御部に保有 上位のシステムからの確認要求に応答する場合と、自ら上位システムに定期的に知らせるパターンがある
	アクチュエーション情報	ロボットの制御指令情報	ロボット制御部から動作部へ伝えられる
	動作記録	ロボットの過去の動作内容を記録した情報	ロボットの制御部に保有 場合によって上位のシステムへアップロードされ蓄積・保管される
認識情報	センサーデータ	センサーが収集するデータ。温度、圧力などから、加速度、位置など様々である	ロボットの認識部で収集され、制御部のメモリ上に展開される。更に上位のシステムへ転送され、制御の最適化や分析に活用される場合もある。この場合、センサーデータは、

			上位システムのストレッジ上に蓄積される
	画像データ	カメラが撮影する画像、動画情報	上位システムのストレッジに転送されることが多い
	音声データ	マイクから収録される音声情報	
	環境データ	ロボットが動作するために必要な周辺情報。たとえば建物の構造や位置などの情報もこの中に含まれる	ロボットが取得するデータ、及び地図データなど事前に準備されたデータを含む。
システム情報	ソフトウェア・ファームウェア	ロボットの機能の実行に必要なプログラム類。ストレッジや上位システムからメモリに展開されるソフトウェアと、チップに書き込まれたファームウェアがある。	ロボットの制御部に保有される。ただし大元は、メーカーなどのダウンロードサイトであることが多い
	ソフトウェアの設定情報	ソフトウェアを目的どおり動作させるための設定情報。	ロボットの制御部に保有される
	設計情報・ロジック情報	ロボットが目的どおり動作するための要求仕様や論理構造に関わる情報	ロボットを管理するシステム内にて保有される
システム管理情報	アカウント情報（ユーザー名、パスワード）	ユーザー、管理者の ID・パスワード情報	
	暗号鍵	暗号化の手順を制御するための情報	
	システムログ	システムが記録する動作履歴	

３－３．その他の留意事項

３－３－１．物理セキュリティ

ロボットシステムは、マシン室などの外部からの物理的な侵入や攻撃に保護された安全な場所に限らずに利用される。産業用ロボットは、人間が立ち入る場所とは隔離されている限定された環境で利用されるのに対して、サービス・ロボットは、不特定な環境で利用される。このため、脅威として物理的な侵入・盗聴などの点も考慮することは非常に重要である。

３－３－２．ユーザーによる誤操作

本書では、ユーザーによるソフトウェア使用時の誤操作は、悪意あるユーザーによる意図した誤操作と事象的には同様のものと扱うこととする。

３－３－３．セキュリティと安全性との関係

セキュリティリスクと物理的な安全性のハザードは、従来は独立事象として扱われてきた。しかし、IoT・サイバーフィジカルシステムにおいては、セキュリティリスクと安全性のハザードは、相互に影響しあうことが指摘されており、国際的には SESAMO（Security And Safety Modelling for Embedded System）プロジェクトでセキュリティと安全性の相互関係のモデル化が検討されている。

システムの設計にあたっては、セキュリティの侵害が、安全性の阻害につながらないことを考慮する必要がある。また、システムの機能安全対策に関しては、IEC61508 をはじめ各産業団体、品質保証より各種ガイドラインが刊行されており、それらを参照されたい。

（“付録Ａ－１．品質保証・安全規格団体による規格“参照）

４．脅威分析とリスク評価

４－１．危惧される脅威事象の洗い出し

ロボットシステムにおいて危惧される脅威事象について表 5 に示す。

表 5. 危惧される脅威事象

分類	内容	項番	脅威事象
なりすまし	ロボットの制御をハッカーに奪われる	1	意図しないノード（ユーザー、ロボット）の接続による動作 （制御ののっとり）
改竄	ロボットを制御するためのデータやプログラムが改竄される	1	内部プログラムののっとり・改竄
		2	外部環境情報（センシング）の改竄
		3	クラウド側でのロボット情報の改竄
		4	通信経路上での改竄
情報漏洩	ロボットが保有するデータの流出（位置情報、顔写真、個人記録、建物情報等）	1	通信経路の流出
		2	ダイアログ（行動履歴）の流出
		3	盗聴
		4	サイドチャネル攻撃
サービス不能攻撃	ロボット動作の非正常化	1	ロボットへのポートスキャン・SYN Flood 攻撃

【脅威事象の解説】

脅威事象１．なりすまし　ロボット制御ののっとり

なりすましとは、偽物が本物のふりをして不正行為をはたらくことである。
サイバーシステムの場合、ユーザーへのなりすまし、IP アドレスのなりすまし、MAC アドレスのなりすましなど方法は様々である。ロボットシステムの場合、偽の管理システムになりすました攻撃者が偽の制御情報を制御部に送りつけて誤動作をさせるなどの手法が危惧される。意図しないノードから接続によって想定外の動作におちいるなどの危険性がある。

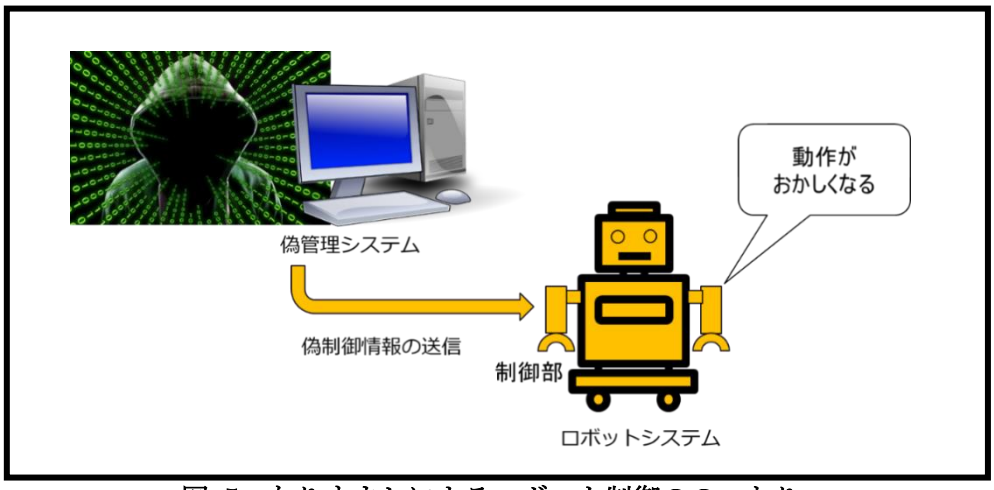


図 5. なりすましによるロボット制御ののっとり

脅威事象２．改竄　ロボットを制御するためのデータやプログラムが改竄

改竄とは、情報が不当に書き換えられる事象である。

ロボットシステムの場合、内部プログラムの書きかえ、制御情報のかきかえ、にとどまらず、改竄された不正な情報が外部から送信され認識誤動作に陥ることや、逆に外部に送信する認識情報や状態情報が改竄されるなど想定される脅威事象はさまざまである。いずれの場合も、ロボットシステムの動作は想定外の状況に陥り影響は多大である。

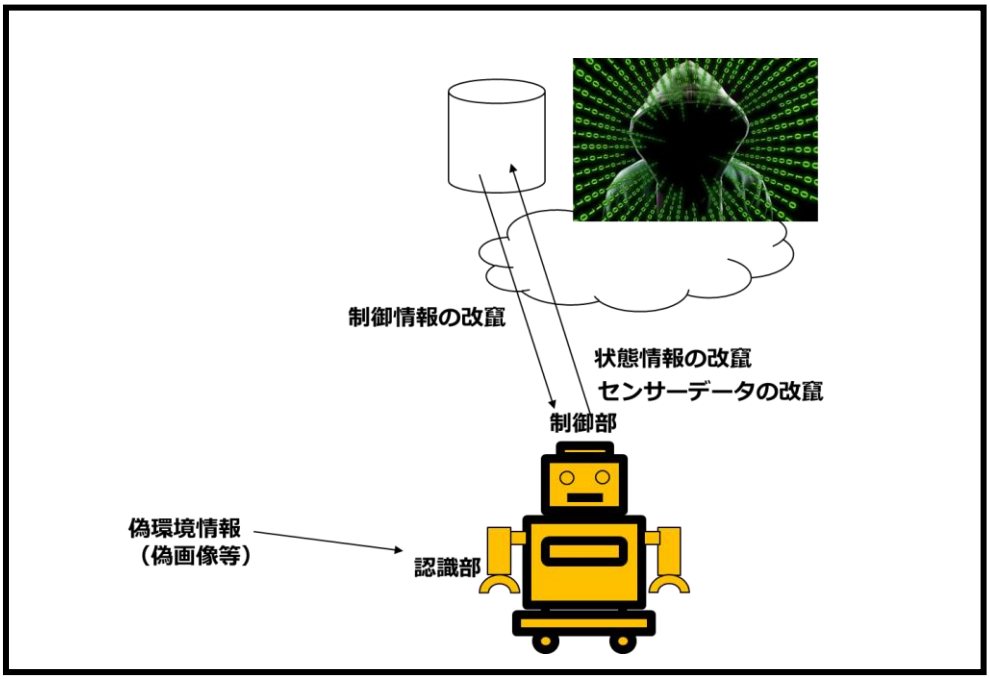


図 6. ロボットを制御するためのデータやプログラムが改竄される

脅威事象３．情報漏洩

情報漏洩とは、内部に留めておくべき情報が何らかの原因により外部に漏れてしまう事象である。サービス・ロボットが動作するためには、位置情報、顔写真、個人記録、建物情報など様々な情報がネットワーク上を行きかうことが想定される。　そのため、これらの情報が通信経路上からあるいは集められたクラウドから情報を搾取されることは、機密性・プライバシー保護という点において非常に大きな脅威となりうる。

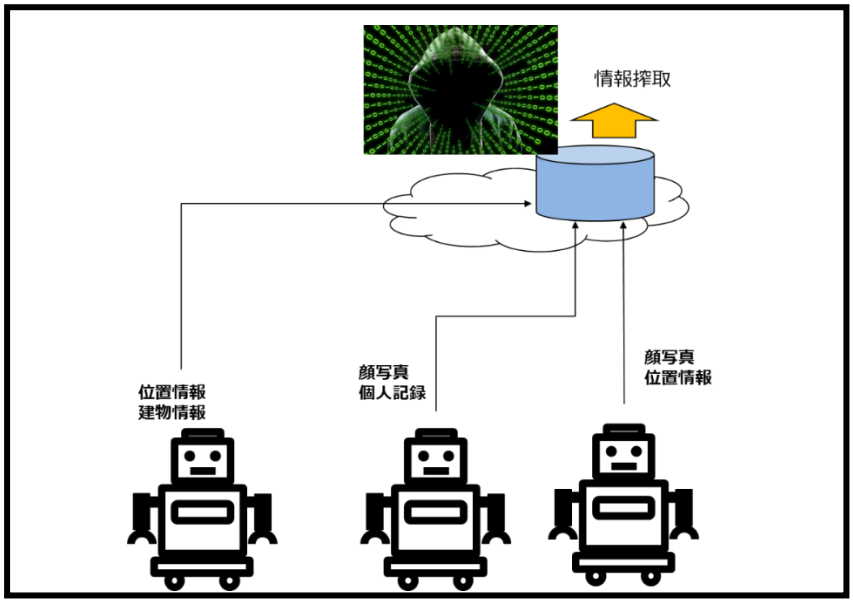


図 7. 情報漏洩

脅威事象４．サービス不能攻撃（DOS 攻撃）

サービス不能攻撃（DOS 攻撃）は、サービスの可用性を侵害することを目的とした攻撃である。ロボットシステムの場合、軽度な緩い攻撃であっても、動作のリアルタイム性が阻害される可能性があり、大きな脅威となりうる。

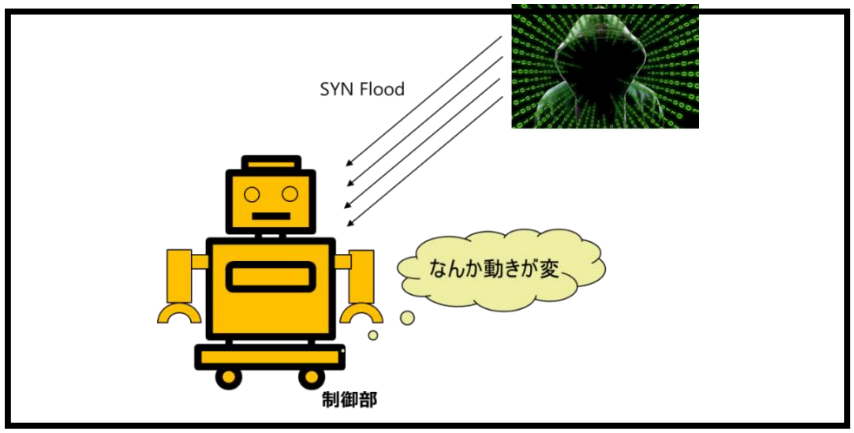


図 8. サービス不能攻撃

４－２．脅威分析・リスク評価手法

セキュリティに関する脅威を分析し、リスクを正しく評価し、対策を導き出すためには、様々の方法がある。

サービス・ロボットは、関連している情報やシステムが多岐にわたること、利用される環境が限定されないことから、ソフトウェアの構造やシステム間の通信フローも複雑である。また、システム全体に関係するステークホルダも多方面にわたることが想定される。このために、運用にはいってから対策を講じることはより困難となる。したがって、システムの設計段階で想定される脅威・リスクを洗い出し分析した上で対策を検討することが必要である。

本書では、下記の手順に従うことを提案する。

- **ユースケースの整理・洗い出し**
- **ミスユースケースの洗い出し**
- **アタックツリー（脅威の相互関連性）の分析**
- **リスク評価**
- **対策の検討・優先順位付け**
- **残留リスクの検討**
- **対策の実施**

①　ユースケースの整理・洗い出し

通常の利用形態の整理と洗い出しである。本書では、UML 形式によるアクターとユースケースによって整理を行う例を示す。

- **アクター**：機器、システム、人間を示す
- **ユースケース：**　機能、機能間のつながり方を示す
- **ユースケース図例**

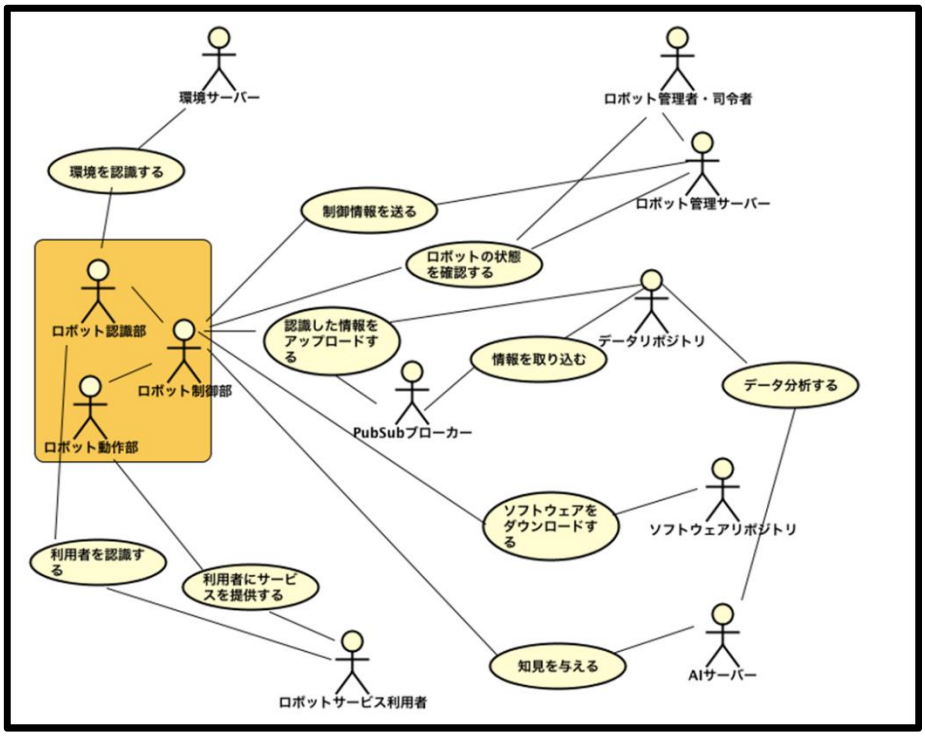


図 9. ロボットシステム　ユースケース図例

②　ミスユースケースの洗い出し

通常の利用形態から考えられる攻撃パターンの洗い出しを行う。

本書では、前節のユースケース図に攻撃者と攻撃パターンを追記する方法を紹介する。

この図をミスユースケース図と呼ぶ。以下詳細である。

- ミスユースケース図

ユースケース図に攻撃者と攻撃パターンを追記したもの

本書では、そこに対策をユースケースとして追記し、その有効性について検証が可能なようにする。これにより残留リスクも評価することが可能である。

下記の例では、攻撃者（ミスアクター）を赤塗りのアクター、攻撃パターン（ミスユースケース）を赤線で示している。また、対策の検討にあたって、対策内容を青字のユースケースで示す。

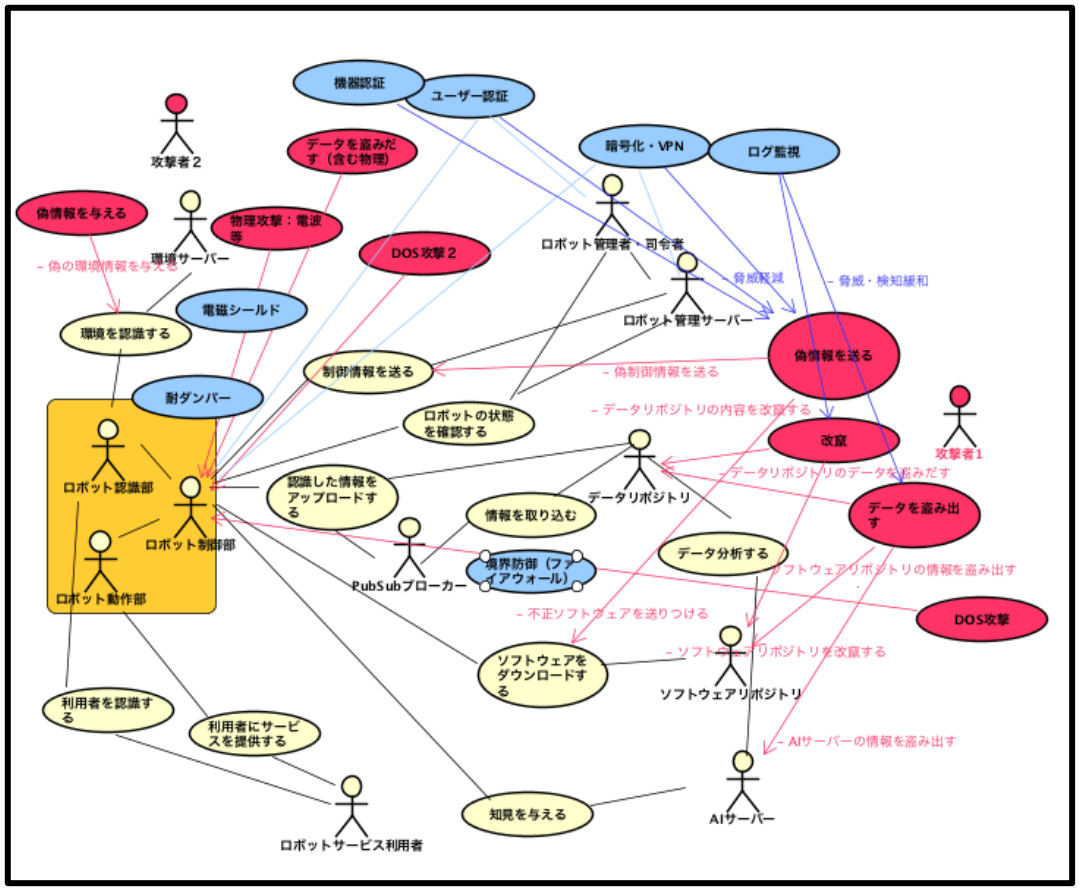


図 10. 対策入りミスユースケース図例

③ アタックツリー

ミスユースケースから洗い出された攻撃・脅威の相互関連性について明らかにするものである。図 7 に例を示す。

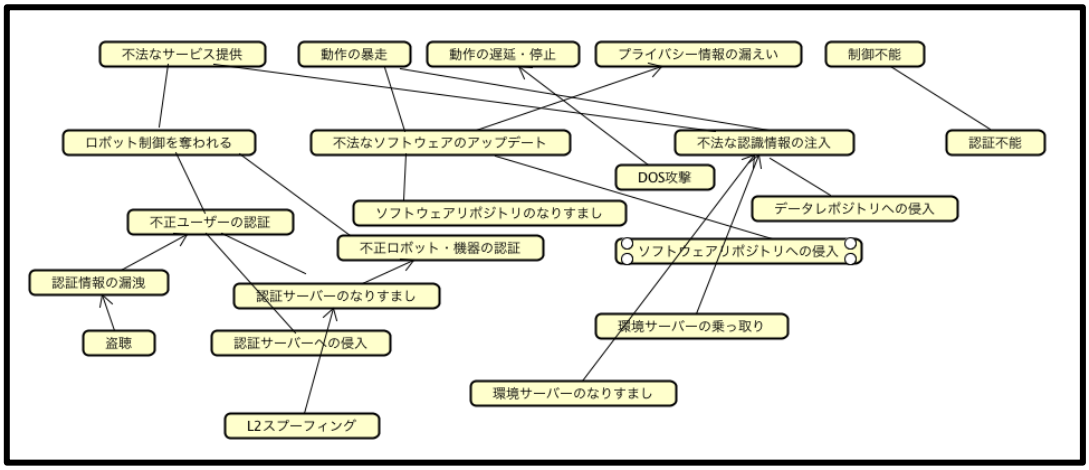


図 11. アタックツリー例

④　リスク評価

本書では下記のポイントでリスク評価を行う。

脅威に対するリスク＝（脅威の影響度）×　（攻撃の可能性）

脅威の影響度：脅威による影響度合いである。
ひとつの脅威が別の脅威をもたらすなど影響が大きいものはリスクが高い。

攻撃の可能性：脅威による影響だけでなく、攻撃の可能性も考慮して指標化する必要がある
攻撃者にとってコストが低く、利益が大きいものが攻撃の対象になりやすい

攻撃の可能性　＝　攻撃によって得られる攻撃者の利益／攻撃のコスト（難易度）

⑤　対策の検討・優先順位付け、⑥残留リスクの検討、⑦対策の実施

脅威分析、リスク評価結果を元に、優先順位を付けて対策を検討すると同時に、対策後も残留リスクについての検討・把握を行うべきである。対策のコストに対して残留リスクがあまりに大きい場合は、再度対策を検討しなおす必要がある。

４－３．脅威分析　具体例

本項では、公立大学法人会津大学において実施した２つのシステム構築事例の脅威分析について紹介する。

具体的例１：WRS2018 スパイダー

➢ システム概要

2018 年 10 月に開催された World Robot Summit（WRS2018）の競技会に参加した会津大学チームの災害対応スパイダーシステムについてとりあげる。

本システムは、遠隔で各種指令を与えることによって、スパイダーロボットが災害対応に必要な各種動作を実施し、災害からの復旧を支援するシステムである。動作内容が特定されない環境で利用されるために、管理システムとロボット制御部の間で頻繁に制御情報、認識情報が交換されるという特徴を持つ。

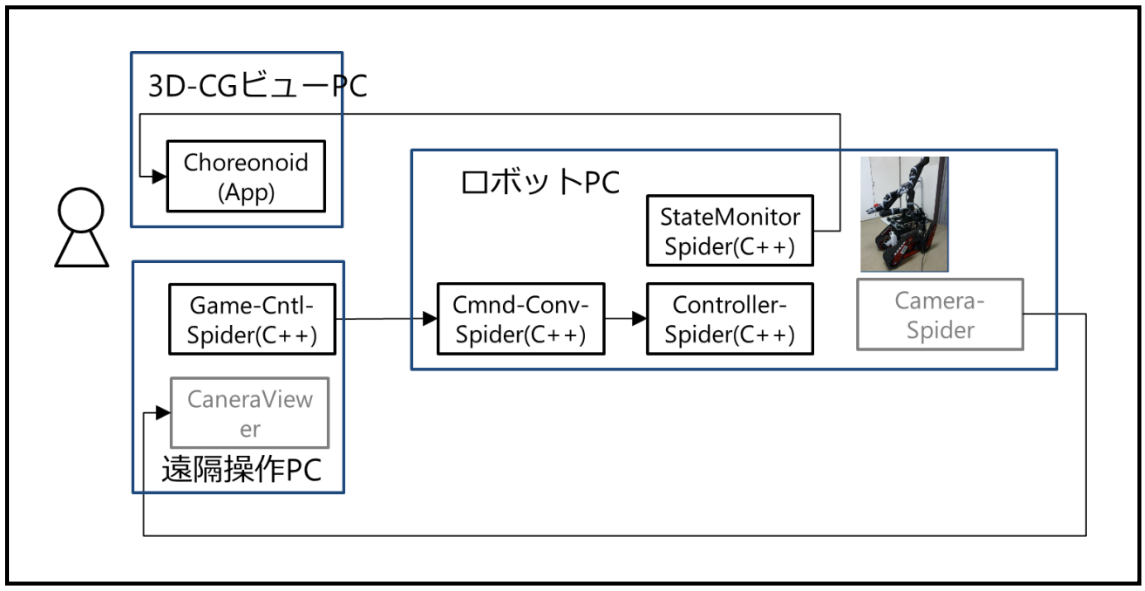


図 12. WRS2018 スパイダー　システムブロック図

➢ ユースケース概要

・ロボット認識部（カメラ）が撮影する映像は、操作者が操作する PC（操作 PC）へ転送され、カメラビューアによって操作者へ伝えられる

・ロボット制御部は、状態情報を操作 PC 内の 3D・CG ビューアへ転送する。

・操作 PC よりゲームパッドを通して、指令情報がロボット制御部へ送られる。

これらの通信は、OpenRTM のノード間通信（TCP）として行われる。

OpenRTM のノードとして各ノード（ロボット制御部、操作 PC）は、OpenRTM の DNS へのノード登録を行う。

➢ ミスユースケース

ミスユースケースから浮き上がった脅威は、以下の点である。

- 偽操作 PC、偽ゲームパッドによる偽コマンドの送信
- 偽ロボットノードによる偽状態の送信
- コマンドの盗聴
- ノード情報の盗聴
- RTM DNS への侵入・レコードの搾取

図 13 は、ユースケース・ミスユースケースと対策を図式化したものである。

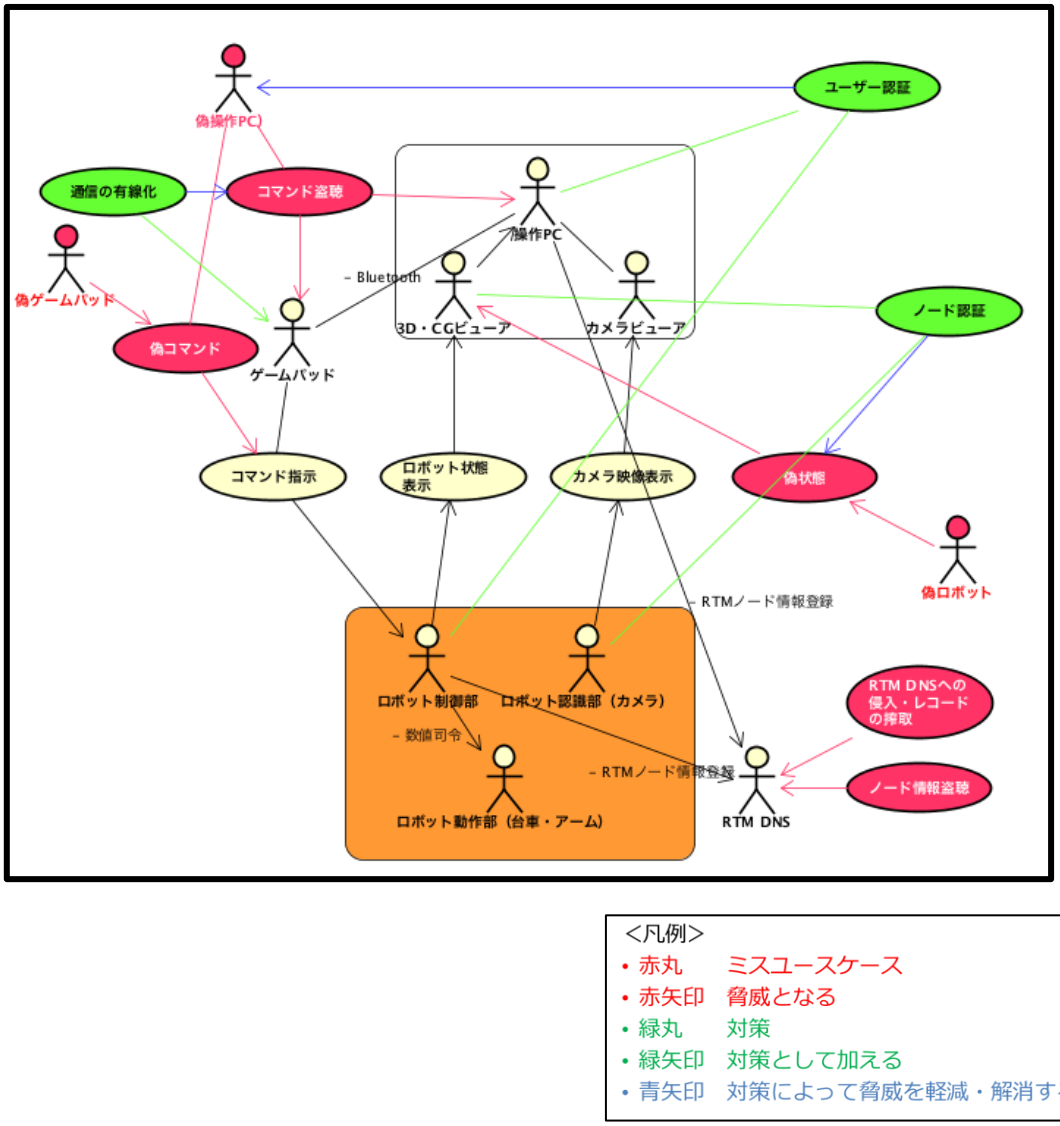


図 13. ミスユースケース図　WRS2018 スパイダーシステム

➢　アタックツリー

図 14 に WRS2018 スパイダーシステムにおけるアタックツリーを示す。

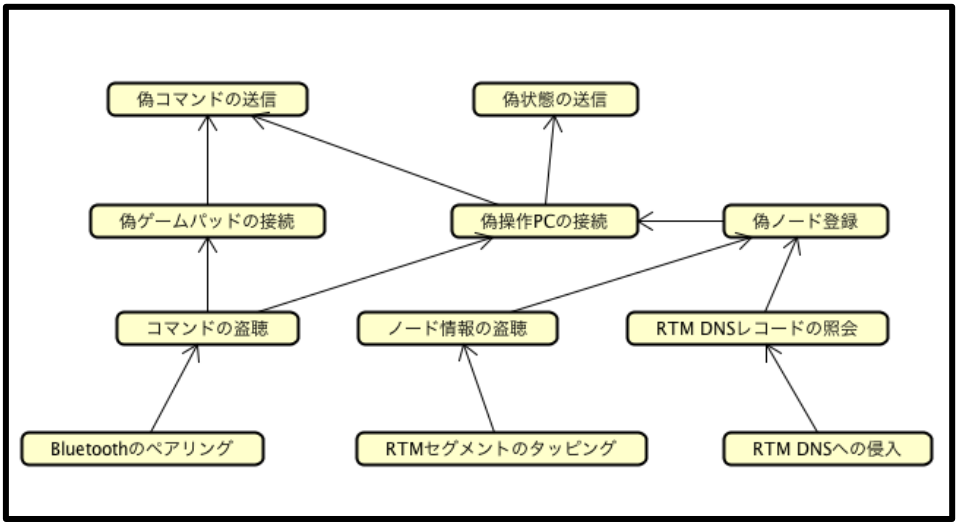


図 14. アタックツリー　WRS2018 スパイダーシステム

➢　リスク評価、対策と優先順位

表. に WRS2018 スパイダーシステムにおけるリスク評価・対策と優先順位についてまとめて示す。

表 6. 具体例１. WRS2018 スパイダーシステム　リスク評価結果

ミスユースケース	リスク評価	対策案	優先順位
コマンドの盗聴(操作 PC～ゲームパッド間（Bluetooth))	**大** （影響：大 可能性：大）	操作 PC～ゲームパッド間の有線化	**高**
ノード情報の盗聴（RTM DNS～ノード間通信のタッピング）	**中** （影響　大 可能性　中）	セグメント分離	**中**
RTM DNS への侵入、DNS レコードの搾取	**中** （影響　大 可能性　小）	RTM DNS の堅牢化 セグメント分離 アクセス制限	**中**
偽操作 PC、偽ゲームパッドによる偽コマンドの送信	**大** （影響　大 可能性　中）	ユーザー認証・機器認証	**高**
偽ロボットノードによる偽状態情報の送信	**中** （影響　中 可能性　中）	ノード認証・機器認証	**中**

具体例２：LICTiA 受付・誘導ロボットの例

➢　システム概要

公立大学会津大学の復興支援センター施設（LICTiA）内において、来客を受付、目的の場所へ誘導するロボットの実証実験を行った。このシステムの目的は、複数のロボットが連携して来客を安全に目的の場所へ誘導することである。

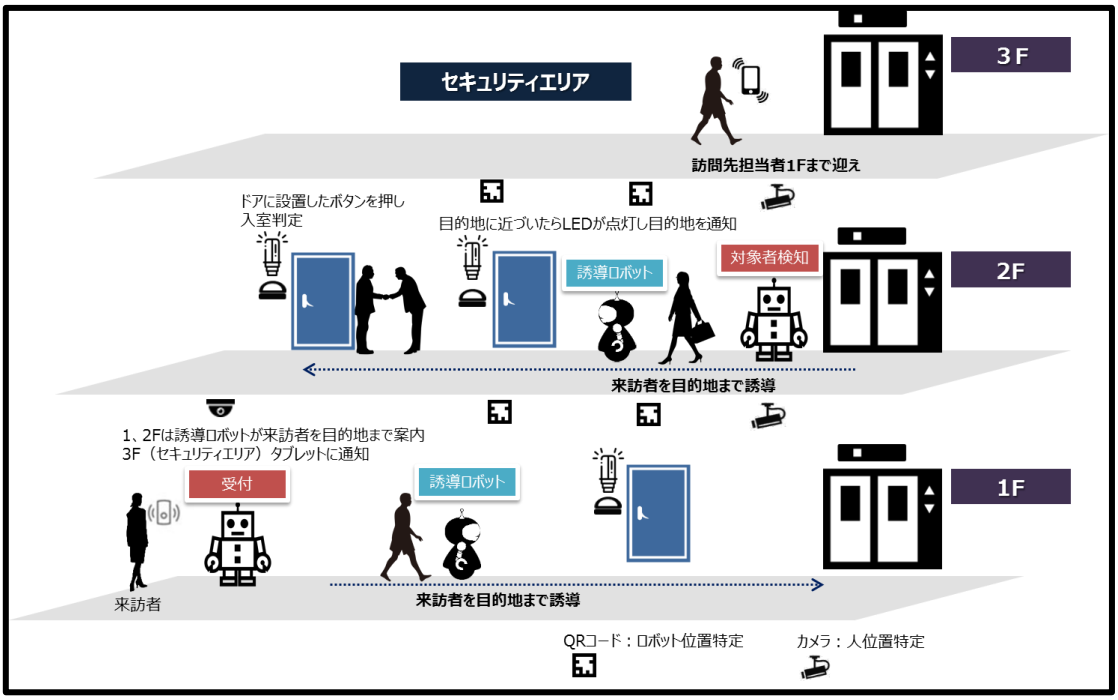


図 15. 具体例２．ロボット利用イメージ図

➢　ユースケース

・来客は、１F 受付ロボットに目的地を伝える。

・受付ロボットは、許可を得た上で来客の顔写真を撮影する。

・受付ロボットのコンパニオン PC は、撮影した写真をクラウド上にあるストレージへ転送する。通信プロトコルは HTTPS である。

・クラウドストレージは、写真のメタ情報を FIWARE へ送信する。

・受付ロボットのコンパニオン PC は、来客の目的地情報を FIWARE へ送信する。転送方式は、MQTT であり、正確には、MQTT のブローカーを介して FIWARE へ送信される。

・FIWARE 上で目的地情報は、座標変換される。

・座標変換された目的地情報は、FIWARE より MQTT ブローカー経由で１F、または２F 誘導ロボットへ転送される。

・１F、または２F 誘導ロボットは、受信した目的地情報にしたがって、来客を目的地へ誘

導する。
１F 誘導ロボット、２F 誘導ロボット、１F 天井カメラ、２F 天井カメラは、ROS ノードとして ROS ブローカーにノード登録を行っている。

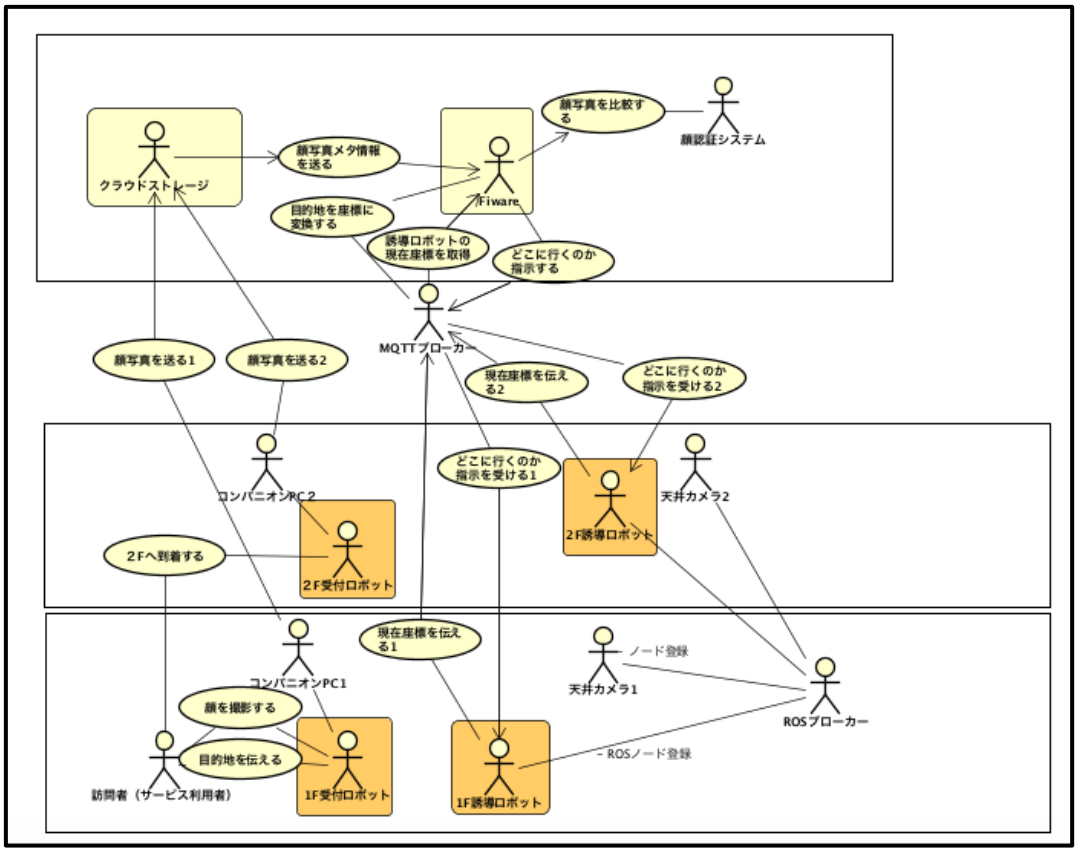


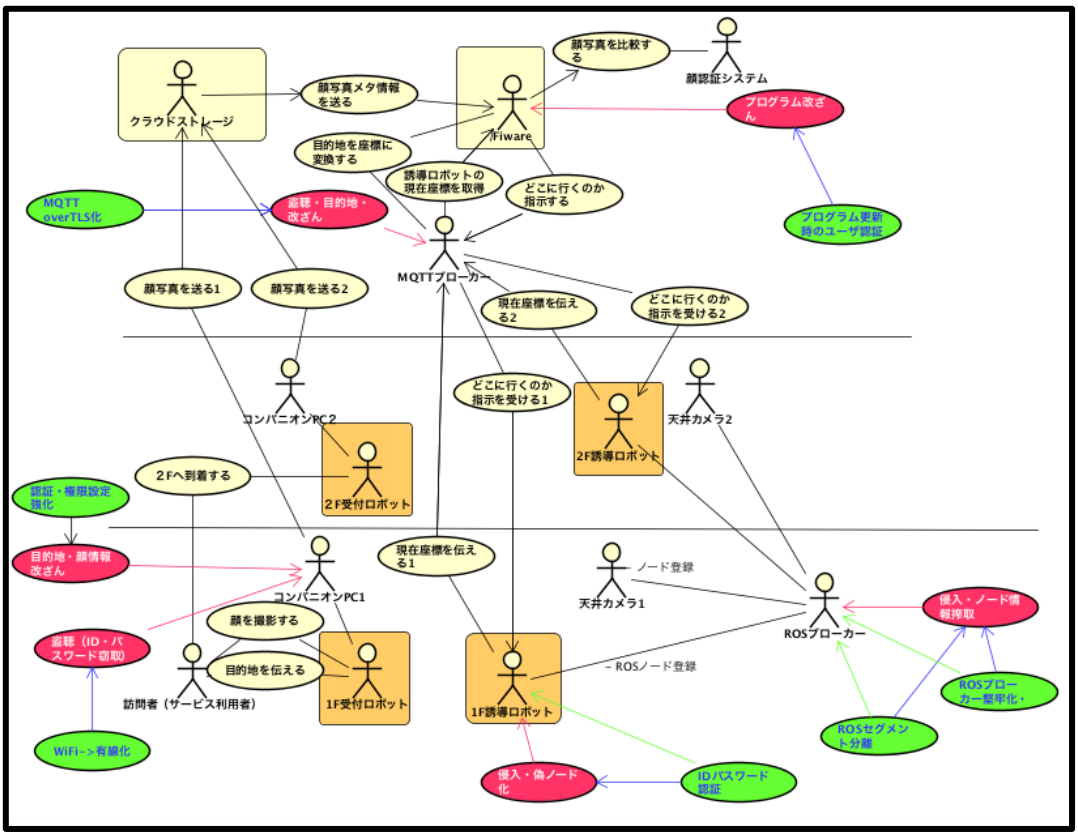
図 16. LICTiA 受付・誘導ロボット　ユースケース

➢　ミスユースケース

ミスユースケースから浮き上がった脅威は、以下の点である。

- MQTT の盗聴・目的地等の改竄
- コンパニオン PC への侵入
- Wifi への接続、写真、目的地の盗聴
- 誘導ロボットへの侵入
- ROS ブローカーへの侵入
- 偽 ROS ノード登録
- クラウドストレージの写真情報の搾取
- FIWARE　プログラムの改竄

図 11 は、ユースケース・ミスユースケースと対策を図式化したものである。



<凡例>
- 赤丸　ミスユースケース
- 赤矢印　脅威となる
- 緑丸　対策
- 緑矢印　対策として加える
- 青矢印　対策によって脅威を軽減・解消する

➢　アタックツリー

図 12 に LICTiA 受付・誘導ロボットシステムにおけるアタックツリーを示す。

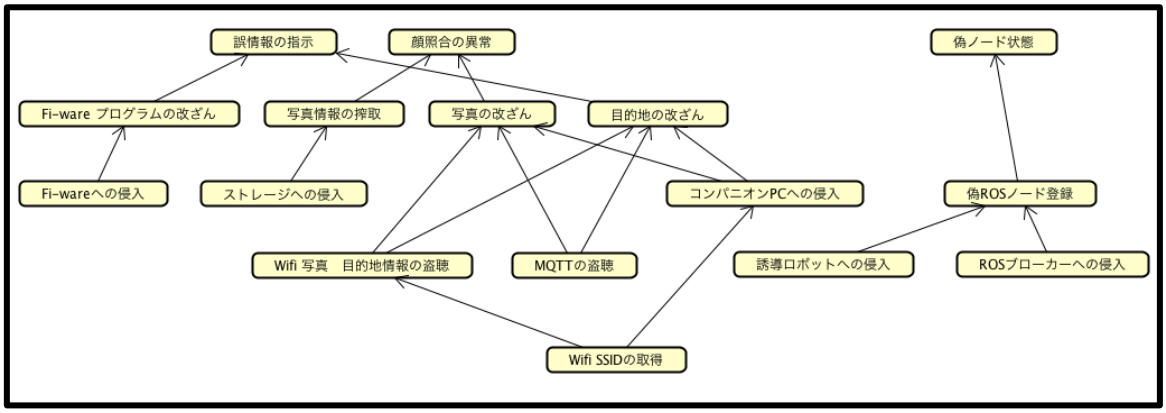


図 17. アタックツリー　LICTiA 受付・誘導ロボット

➢　リスク評価、対策と優先順位

表. に LICTiA 受付・誘導ロボットシステムにおけるリスク評価・対策と優先順位についてまとめて示す。

表 7. 具体例 2. LICTiA 受付・誘導ロボットのリスク評価結果

ミスユースケース	リスク評価	対策案	優先順位
MQTT の盗聴・目的地等の改竄	大（影響：大 可能性：高）	MQTT Over TLS の実装	高
コンパニオン PC への侵入	大（影響：大 可能性：高）	コンパニオン PC の認証強化、権限設定強化	高
写真、目的地情報の盗聴・改竄	中（影響：中 可能性：高）	受付ロボット～コンパニオン PC 間の有線化	高
		コンパニオン PC　耐タンパ	
誘導ロボットへの侵入	中（影響: 中　可能性　：中）	誘導ロボット堅牢化	高
ROS ブローカーへの侵入	中（影響　大　可能性　中）	ROS ブローカーの堅牢化　ROS のセグメント分離	中
偽 ROS ノード登録	中（影響　中　可能性　中）	ROS のセグメント分離	中
クラウドストレージの写真情報の搾取	中（影響　大　可能性　小）	クラウドストレージでの認証、クラウドストレージ内のデータストラインピング	中
FIWARE プログラムの改竄	中（影響　大　可能性　小）	プログラム更新時のユーザ認証・認可	中

５．対策のガイドライン

前章でとりあげた脅威分析の事例にみられるように、なりすまし、改竄、情報漏洩、サービス不能攻撃といった脅威は、脅威同士も相互に密接に関係している。個々のケースにおいて脅威分析を行った上で対策を検討する必要がある。本章では、主要な脅威の特徴と対策のポイントについて解説する。

５－１．主な脅威事象の特徴と対策の方向性

洗い出された脅威事象についての対策の方向性を表 8 に示し、その特徴について解説する。

表 8. 脅威事象と対策の方向性

分類	内容	脅威事象	対策の方向性
なりすまし	ロボットの制御をハッカーに奪われる	意図しないノードの接続による制御ののっとり	ユーザー認証・認可
			機器認証
			ログ監視の強化
			動作環境しきい値の設定
改竄	ロボットを制御するためのデータやプログラムが改竄される	内部プログラムののっとり・改竄	権限設定強化
			ログ監視強化
			コンテンツ暗号化
			ソフトウェア認証
		外部環境（センサーデータ）の改竄	メッセージ認証・デジタル署名
		ロボット情報をクラウド側で改竄	データストア・ストライピング
		通信路における改竄	メッセージ認証・デジタル署名
情報漏洩	ロボットが保有するデータの流出（位置情報、顔写真、個人記録、建物情報等）	通信経路の流出（ネットワーク構成情報等）	ユーザー認証・認可 コンテンツ暗号化
		ダイアログ（行動履	ユーザー認証・認可

		歴）の流出	コンテンツ暗号化
		通信内容の盗聴	通信の暗号化
			セグメント分離
		サイドチャネル攻撃	耐タンパ
		内部プログラムの漏洩	ユーザー認証・認可 権限設定強化
サービス不能攻撃	ロボット動作の非正常化	ロボットへのポートスキャン・SYNFlood	余分なポートの閉塞化
			アクセス制限
			セグメント分離

【解説】

なりすまし

“なりすまし”は、一般概念としては、“にせもの“が本物のふりをする行為全般を指す。従来のサイバーシステムでは、ユーザースプーフィング、IP スプーフィング、L2 スプーフィングなどの攻撃例がある。

サービス・ロボットの場合にあてはめると、”管理者のふりをする“、”ノードのふりをする“などが攻撃パターンとして考えられる。

対策技術のキーは、認証・認可である。ユーザーレベルの認証と、機器・装置レベルの認証の両方が必要である。なりすましによってシステム内に侵入された場合に、その影響範囲を極小化するためには、システム内の権限管理も重要である。また、なりすましは、検知が難しいという特徴を持ち合わせる。通常時の行動パターンの違いを検知するために行動記録の監視と閾値の管理も非常に重要である。

改竄

“改竄”は、一般概念としては、“情報が不当に書き換えられること”全般を指す。従来のサイバーセキュリティでは、完全性の阻害にあたり、例としては、サーバーコンテンツの改竄、メールの内容改竄などの例が挙げられる。

サービス・ロボットにあてはめると、ロボットの内部プログラムやロジックの改竄、状態情報の改竄、センサーなどによる認識情報の改竄などが考えられる。これらのいずれの場合も、データの完全性の阻害にとどまらず、ロボットの動作やサービスに誤動作を引き起こすなど、可用性にも影響を与える可能性がある。

対策技術のキーは、ハッシュ関数を用いたメッセージ認証、デジタル署名の技術である。また、“なりすまし”によるシステム内への侵入から改竄が発生する可能性も多く、システム内の権限管理も非常に重要である。

情報漏洩

“情報漏洩”は、一般概念としては“内部”の情報が“外部”へ流出すること全般を指す。従来のサイバーセキュリティでは、機密性の阻害に相当し、盗聴やタッピング、不正侵入などによって機密情報を攻撃者が搾取するパターンが考えられる

サービス・ロボットにあてはめると、制御ロジックの漏洩、システム情報の漏洩、センサーなどによる認識情報の漏洩などが考えられる。サービス・ロボットが認識する情報には、利用者の個人記録、写真、建物情報などが含まれ、これらの情報が漏洩すると、個人情報の流出やプライバシーの侵害につながる恐れがある。

対策技術のキーは、暗号化技術、認証・認可技術である。暗号化は、コンテンツ暗号化、通信の暗号化などを必要に応じて施す必要がある。暗号鍵の管理もあわせて非常に重要である。

サービス不能攻撃

“サービス不能攻撃”は、サービスの可用性を侵害することを目的とした攻撃全般を指す。従来のサイバーセキュリティでは、サーバーへの接続要求を連続的に行うなどによりサーバーに高負荷を与え、サービスを実質的に停止させるなどの攻撃例が挙げられる。

サービス・ロボットにおいても同様の攻撃が起こりうるが、軽度の攻撃であってもロボットの動作のリアルタイム性に影響をあたえ、それによる誤動作が安全性や可用性を阻害することも想定する必要がある。

対策技術のキーは、システムへのアクセス制御である。実際にロボットが動作するセグメントを分離し、境界でパケットフィルタリングなどを行う設計も検討する必要がある。
また、ロボットのアーキテクチャ設計として、CPU の高負荷が動作部の物理的な動作に影響を与えにくいように考慮することも重要である。

５－２．対策技術の活用ガイドライン

前項において検討対象となった対策技術と対象脅威・場所・残留リスクの対応内容をガイドラインとして表 9 に示す。

表 9. 対策内容、対象脅威、残留リスク・課題　一覧

分類	対策名	対象脅威	対象場所	残留リスク・課題
認証・認可	ユーザー認証・認可	不正侵入・なりすまし・改竄	ロボットシステム、管理システム、周辺システム	ID・パスワードの複雑化、多要素認証

	機器認証	なりすましによる制御ののっとり	ロボットシステムと外部	機器の識別方法
	メッセージ認証	センサーデータ等認識情報の改ざん検知	ロボットシステムと情報転送先	暗号鍵・証明書の管理
	ソフトウェア認証	プログラムの改竄検知	ソフトウェアリポジトリ	暗号鍵・証明書の管理
暗号化	通信暗号化	盗聴・改竄	ロボットシステムと外部との通信	暗号鍵・証明書の管理
	コンテンツ暗号化	改竄、情報漏洩	管理サーバー、ソフトウェア・データリポジトリ	暗号鍵・証明書の管理
	データストア・ストライピング	改竄、情報漏洩	データストレージ	暗号鍵の管理
境界防御		サービス不能攻撃	ロボットシステムと外部との境界	境界 GW におけるアクセス制限
セグメント分割		サービス不能攻撃、不正侵入、盗聴	ロボットノードセグメントとそれ以外のセグメントを分割	・外部との GW におけるアクセス制限 ・拠点外にもロボットノードが存在する場合の対策
無線通信方式の有線方式化		盗聴、不正侵入、なりすまし	ロボットシステム内の無線部分、ロボットシステムと周辺システム間の無線部分	無線設定の無効化、有線接続部分の管理
権限管理	権限設定強化	なりすまし　改竄	ロボットシステム制御部、ロボット管理システム	設定情報の管理 管理者情報の暗号化

監視	ログ監視強化	なりすまし・改ざん検知	ロボットシステム、ロボット管理システム	検知方法・精度、検知後の対策フロー、 見逃しのリスク
	動作環境閾値設定	なりすまし検知	ロボットシステム、ロボット管理システム	閾値の指標、値の精度、見逃しのリスク
アーキテクチャ設計	制御部の高 CPU 処理による動作部への影響を最小化する構造設計	サービス不能攻撃	ロボットシステム制御部	機能安全性への考慮
物理対策	耐タンパ	盗聴、不正侵入	ロボットシステム制御部	
	電磁波シールド	盗聴、サービス不能攻撃	ロボットシステム制御部	

５－３．具体例における対策と残留リスク・課題

第４章でとりあげた具体例のシステム（WRS2018 スパイダーシステム、LICTiA 受付・誘導ロボットシステム）における対策、残留リスク・課題を参考例として表 10、表 11 に示す。

表 10．具体例１．WRS2018 スパイダーシステムにおける対策、残留リスク・課題例

脅威	リスク評価	対策	優先順位	残留リスク・課題
コマンドの盗聴（操作 PC～ゲームパッド間（Bluetooth））	大	操作 PC～ゲームパッド間の**有線化**	高	Bluetooth 設定の無効化
偽操作 PC、偽ゲームパッドによる偽コマンドの送信	大	機器認証、ノード認証	高	認証情報の管理
ノード情報の盗聴 （RTM DNS～ノード間通信のタッピング）	中	セグメント分割	中	・分割されたセグメントとのゲートウェイの管理（アクセス制限等） ・分割されたセグメントへのタ

				ッピング
RTM DNS への侵入、DNS レコードの搾取	中	RTM DNS の堅牢化	中	管理者権限情報の暗号化など
偽ロボットノードによる偽状態情報の送信	中	機器認証、ノード認証	中	認証情報の管理

表 11. 具体例２．LICTiA 受付・誘導ロボットの対策・残留リスクと課題例

脅威	リスク評価	対策	優先順位	残留リスク・課題
MQTT の盗聴・目的地情報の改竄	大	MQTT Over TLS の実装	高	証明書、秘密鍵の管理
コンパニオン PC への侵入	大	コンパニオン PC の認証強化、権限設定強化	高	認証情報の管理、管理者領域の暗号化
受付ロボット～コンパニオン PC 間の盗聴、写真、目的地情報の・改竄	中	受付ロボット～コンパニオン PC 間の有線 LAN 化	高	有線 LAN へのタッピング
		耐タンパ	中	
誘導ロボットへの侵入	中	誘導ロボット堅牢化	高	管理者情報の管理
ROS ブローカーへの侵入	中	ROS ブローカーの堅牢化	中	管理者情報の管理
	中	ROS のセグメント分離	中	分離されたセグメントとのゲートウェイの管理（アクセス制限等） 分離されたセグメントへのタッピング
偽 ROS ノード登録	中	ROS のセグメント分離	中	
クラウドストレージの写真情報の搾取	中	クラウドストレージでの認証、クラウドストレージ内のデータストラインピング	中	認証情報、暗号鍵の管理
FIWARE プログラムの改竄	中	プログラム更新時のユーザー認証・認可	中	認証情報の管理

６．対策後に検討が必要な課題

対策後は、その有効性を検証・評価を実施するためのセキュリティ・テストが必要である。セキュリティ・テストの方法は、様々な手法があり、システムと対策の内容も対応方法は異なる。本書では、その具体的な内容は取り上げないが、システムの内容とセキュリティの目的・目標に応じたテストの方法を別途検討する必要がある。

対策後のシステムの運用もセキュリティを維持する上では非常に重要なポイントである。本書は設計・開発段階における内容に主眼を置いているために具体的な内容については記載していないが、付録に示す関連するガイドラインなどを参照にして検討することを推奨する。

付録 A. 関連ガイドライン

近年多くの情報セキュリティ推進団体から IoT に関するセキュリティガイドラインが刊行されている。一方、品質保証・安全性推進団体からは、機能安全（Safety)の視点で IoT・ロボットに関する安全規格・認証制度が提案されている。以下にその内容を示す。

付録 A−1. 情報セキュリティ推進団体より刊行されているガイドライン

名称	組織	発刊日	内容と特徴	URL
“つながる世界の開発指針”	IPA（独立行政法人情報処理推進機構）	2017年6月第2版	IoT システムの開発者がセキュリティを考慮する上で検討すべき内容を17の指針として提示	https://www.ipa.go.jp/sec/reports/20170630.html
“IoT 開発におけるセキュリティ設計の手引き”	IPA（独立行政法人情報処理推進機構）	2018年4月最新版	IoT 開発におけるセキュリティ設計を進める上で、具体的な参考となることが目的	https://www.ipa.go.jp/files/000052459.pdf
IoT セキュリティガイドライン Ver1.0	IoT 推進コンソーシアム、総務省、経済産業省	2016年7月版	IoT の関係者がセキュリティ確保上取り組むべき基本的な項目と関係者間相互の認識の共有を促すための材料提供的な位置づけ。	http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf
「つながる世界」を破綻させないためのセキュアな IoT 製品開発 13 のステップ	CSA（クラウドセキュリティアライアンス）ジャパン	2017年6月版	セキュアな開発手法、プロセス、開発環境、インテグレーション環境などに関して示唆が豊富	https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/future-proofing-the-connected-world_J_20170520.pdf

付録 A－2.　関連事業推進団体によるセキュリティガイドライン

名称	組織	発刊日	内容と特徴	URL
自動車の情報セキュリティへの取組ガイド “「つながる」自動車に情報セキュリティを“	IPA（独立行政法人 情報処理推進機構）	2017年3月	コネクテッドカーに照準をあてたセキュリティガイドライン。検討すべき内容、流れを 記載	https://www.ipa.go.jp/security/iot/emb_car2.html
ドローンセキュリティガイド	一般社団法人セキュアドローン協議会	2018年3月	ドローンに照準をあてたセキュリティガイドライン。運用体制などについても記載。	https://www.secure-drone.org/wp-content/uploads/drone_security_guide_201803.pdf

付録 A=3.　品質保証・安全規格推進団体による規格

名称	組織	発刊日	内容と特徴	URL
ISO13482 “パーソナルケアロボットの安全”	ISO(International Organization of Standards, 国際標準化団体)	2014 年 2 月	日本主導で作られた安全規格 JQA（一般社団法人 日本品質保証機構）が認証サービスを開始している リスクアセスメントとそのレベルに基づく低減策などを記載している	https://www.jqa.jp /service_list/fs /service/13482/
IEC61508 “機能安全”	IEC(International Electrotechnical Commission, 国際電気標準化会議)	2000 年 Ver1.0 2010 年 Ver2.0	リスクを許容可能なレベルに低減する「機能安全」という考え方に基づいている 機能安全の確保に必要な要求事項を定めた機能安全規格を記載	http://www.iec.ch /functionalsafety /standards /page1.htm
生活支援ロボット及びロボットシステムの安全性確保に関するガイドライン	RRI（ロボット革命イニシアティブ）	記載なし	危険源・リスク分析・リスク評価、残留リスクを工程に分けて整理している 「移動サービス型ロボット」、「搭乗型ロボット」、「装着型身体アシストロボット」を対象に、製造者、実証実験実施者、販売者等、システム管理者等の責務について記載	https://www.jmfrri.gr.jp /content/files/Open/2016 /SWG2GL.pdf

付録 B. 参考文献

[1] 独立行政法人情報処理推進機構, “つながる世界の開発指針　～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント　第 2 版“,2017. https://www.ipa.go.jp/sec/reports/20170630.htm

[2] 独立行政法人情報処理推進機構,“IoT 開発におけるセキュリティ設計の手引き”, 2018. https://www.ipa.go.jp/files/000052459.pdf

[3] IoT 推進コンソーシアム,総務省,経済産業省,” IoT セキュリティガイドライン Ver1.0”, 2016. http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf

[4] クラウドセキュリティアライアンスジャパン,”「つながる世界」を破綻させないためのセキュアな IoT 製品開発の 13 のステップ“,2017. https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/future-proofing-the connectedworld_J_20170520.pdf

[5] 独立行政法人情報処理推進機構,“自動車の情報セキュリティへの取組ガイド　第 2 版”, 2017. https://www.ipa.go.jp/security/iot/emb_car2.html

[6] 一般社団法人セキュアドローン協議会, “ドローンセキュリティガイド “, 2018. https://www.secure-drone.org/wp-content/uploads/drone_security_guide_201803.pdf

[7] International Electrotechnical Commission, “IEC61850 Ver2.0”, 2010. http://www.iec.ch/functionalsafety/standards/page1.htm

[8] International Organization of Standards, “ISO13482”,2014. https://www.jqa.jp/service_list/fs/service/13482/

[9] ロボット革命イニシアティブ, “生活支援ロボット及びロボットシステムの安全性確保に関するガイドライン “, 2016. https://www.jmfrri.gr.jp/content/files/Open/2016/SWG2GL.pdf

[10] 独立行政法人情報処理推進機構,” 制御システムのセキュリティリスク分析ガイド第 2 版”,2017. https://www.ipa.go.jp/files/000069436.pdf

[11] 大久保隆夫　情報セキュリティ大学院大学　” 脅威分析法　組み込みの安全とセキュリティを保証するために”,2015. https://www.ipa.go.jp/files/000046476.pdf

[12] 国立研究開発法人新エネルギー・産業技術開発機構　” NEDO ロボット白書 2014”, 2014.　https://www.nedo.go.jp/content/100563895.pdf

[13] 独立行政法人情報処理推進機構, “つながる世界のセーフティ＆セキュリティ設計入門 “,2016. https://www.ipa.go.jp/files/000055007.pdf

[14] 田口研治　“セーフティとセキュリティの統合に関する課題と方法論 “,2017 http://www.jssm.net/wp/wpcontent/uploads/2014/04/IT%E3%83%AA%E3%82%B9%E3%82%AF%E5%AD%A6%E7%A0%94%E7%A9%B6%E4%BC%9A_%E7%99%BA%E8%A1%A8%E8%B3%87%E6%96%99_2017-0802-%E5%85%AC%E9%96%8B%E7%94%A8.pdf

問い合わせ先

公立大学法人会津大学

企画連携課

〒965-8580　福島県会津若松市一箕町鶴賀

TEL：0242-37-2511

E-mail：cl-innov@u-aizu.ac.jp

URL: http://www.u-aizu.ac.jp

本ガイドラインは、以下の URL からダウンロード可能です。

URL：　https://rtc-fukushima.jp/technical/3170/

