

ロボットセキュリティ ガイドライン Version 2.0



ロボットの企画・開発から運用・廃棄にいたるライフサイクルのセキュリティ対策に関するガイドライン

2022 年 6 月
ロボット革命・産業 IoT イニシアティブ協議会
ロボットイノベーション WG
ロボットセキュリティ調査検討委員会

発行者 ロボット革命・産業 IoT イニシアティブ協議会
〒105-0011 東京都港区芝公園 3-5-8
機械振興会館 507 号室 日本機械工業联合会内
TEL 03-3434-6571
E-mail office@jmfri.gr.jp
URL <https://www.jmfri.gr.jp/>

Copyright © 2022 ロボット革命・産業 IoT イニシアティブ協議会 All Rights Reserved.

本文書は、著作権法および国際条約により保護されています。個人または会社（または会社に準ずるもの）内部での使用を目的として、本文書をダウンロード、印刷、または電子的に閲覧することができます。本資料の内容の全部又は一部については、私的使用又は引用等著作権法上認められた行為として、適宜の方法により出所を明示することにより、引用・転載複製を行うことができます。内容の全部又は一部について、ロボット革命・産業 IoT イニシアティブ協議会に無断で改変を行うことはできません。

ロボット革命・産業 IoT イニシアティブ協議会はいかなる目的においても使用可能性を保証するものではなく、本文書の内容を使用したいかなる場合においても責任を負いません。本文書の使用者は、本文書に記載された内容の使用に関連して発生したすべての要求、請求、訴訟、損失、損害（人身事故による損害を含む）、費用、経費（弁護士費用を含む）について、ロボット革命・産業 IoT イニシアティブ協議会に何らの損害も与えないことに同意するものとします。

目次

目次	2
1. はじめに	7
1.1. 背景	7
1.1.1. ロボットを取り巻く環境の変化とセキュリティの重要性	7
1.1.2. ロボットセキュリティの現状	8
1.2. ロボットセキュリティの特徴と課題	10
1.3. 目的	12
1.4. 本ガイドラインにて提示する情報	12
1.5. 対象読者	12
1.6. 委員名簿	14
2. スコープ	15
2.1. 対象としているロボットシステム	15
2.2. 対象となるセキュリティの範囲	16
2.3. セーフティとの関係性	18
2.4. プライバシーとの関係性	19
3. ロボットシステムのライフサイクルとセキュリティ検討	20
3.1. アプローチ	20
3.2. ロボットシステムのライフサイクル構成	21
3.3. ライフサイクルの各フェーズとセキュリティ検討	22

3.4. セキュリティ検討の実施組織～ビジネスケースにおける複数ステークホルダ間の連携について	24
3.4.1. ロボットビジネスに関連するステークホルダ	24
3.4.2. ビジネスケースにおける組織間の連携・承認のワークフロー	29
3.5. リスク評価の考え方	33
4. コンセプトフェーズ	35
4.1. コンセプトフェーズ概要	36
4.1.1. コンセプトフェーズの目的とゴール	36
4.1.2. コンセプトフェーズの実施組織	36
4.1.3. コンセプトフェーズの実施事項	37
4.2. 被害分析の前準備～資産・ユースケースの整理	39
4.2.1. 資産の整理	39
4.2.2. ユースケースの整理	41
4.3. 脅威の想定と被害分析	42
4.3.1. 脅威の想定	42
4.3.2. 被害分析～上位レベルのリスク評価	45
4.4. セキュリティゴールの設定	48
5. 設計フェーズ	50
5.1.1. 設計フェーズの目的とゴール	50
5.1.2. 設計フェーズの実施組織	51
5.1.3. 設計フェーズの実施事項(概要)	51
5.2. ユースケース・資産の詳細整理	53
5.3. 関連脆弱性情報の収集	55
5.4. 攻撃分析(可能性分析)	56
5.4.1. 攻撃分析手法・フレームワークについて	56
5.4.2. 攻撃の起点の明確化と整理(通信フローの整理)	57
5.4.3. 脅威・攻撃の相互関係の分析	59
5.5. 安全性リスク評価(セキュリティ～セーフティの相互影響の評価)	60

5.5.1.	背景	60
5.5.2.	安全性(セーフティ)とセキュリティ.....	62
5.5.3.	安全性(セーフティ)を踏まえたセキュリティリスク評価(セキュリティを踏まえた安全性評価)	62
5.6.	リスク総合評価	65
5.7.	対策基本設計.....	68
5.7.1.	対策の優先順位付け.....	68
5.7.2.	対策の選択.....	69
6.	実装フェーズ	76
6.1.	実装フェーズ概要	76
6.1.1.	目的とゴール	76
6.1.2.	実施組織	77
6.1.3.	実施事項	78
6.2.	対策実装作業・テストの前準備	80
6.2.1.	対策の実装内容と作業分担の確定	80
6.2.2.	実装作業の詳細検討	81
6.2.3.	テスト方法の検討	89
6.2.4.	実装作業・テストの諸準備.....	91
6.2.5.	関係者の教育・訓練の実施.....	92
6.3.	実装作業・テストの実施と結果の整理	92
6.3.1.	テスト結果の収集と整理	92
6.3.2.	総合評価の事前準備	92
6.4.	総合評価(～妥当性評価(セキュリティゴールの達成度合いの評価)と関係組織の承認 (チェックポイント 2)).....	93
7.	運用フェーズ	94
7.1.	運用フェーズ概要	94
7.1.1.	運用フェーズの目的とゴール.....	95
7.1.2.	運用フェーズの実施組織	95
7.1.3.	運用フェーズでの実施事項概要	97
7.2.	運用フェーズの準備(サポートプロセスの確立)	98

7.2.1.	運用担当組織による関連文書(通信フロー図等)のチェック(システム部門のポリシーとの適合性チェック)	99
7.2.2.	運用レベルのリスクアセスメントと対策方針の策定	100
7.2.3.	運用フェーズの実施体制の構築	101
7.2.4.	運用フェーズの実施項目の設計	103
7.2.5.	運用担当組織における教育・訓練の実施	103
7.2.6.	想定外のセキュリティリスクへの対応方針	104
7.3.	運用管理業務の実施	104
7.3.1.	定常業務の実施	104
7.3.2.	非定常(イベントドリブン)業務の実施	105
7.3.3.	再アセスメントの実施	106
8.	廃棄フェーズ	107
8.1.	想定される利害関係者	108
8.2.	廃棄の形態 — 物理的破壊とソフト処理による消去 —	108
8.3.	ロボットが保有・活用する情報のうちセキュリティ上考慮すべきもの	109
8.3.1.	そのロボットの個体自身のシステム内での認証情報	109
8.3.2.	ロボットが個体内にローカルに保有する情報	110
8.3.3.	レンタル・リース品やリユース品を利用する際の注意点	111
	あとがき	112
	APPENDIX A. 関連規格	113
	APPENDIX A-1. 主な関連規格と本書との関係性	113
	APPENDIX A-2. セーフティ・セキュリティ相互関係に関する規格	114
	ISO-TR22100-4	114
	IEC TR63069、IEC63074	115
	APPENDIX B 参考文献	117
	APPENDIX C 対策事例	122
	APPENDIX C-1. 代表的な脅威と対策実施例	122

APPENDIX C-2 時系列でのセキュリティ対策実施事項(例)	126
APPENDIX. D テストツール類	129
APPENDIX E. 各種チェックシート	130
APPENDIX E-1. セキュリティ関連 タスク管理シート	130
APPENDIX E-2. セキュリティゴール定義書	133
APPENDIX E-3. 脅威想定表	134
改訂履歴	135

1. はじめに

本書は、ロボット全般のセキュリティに関するガイドラインである。近年、様々な分野におけるサイバー攻撃が増加し、連日ニュースとして報じられるなど、サイバーセキュリティへの関心が高まっている。ロボット分野においては、従来の産業用ロボットに加えてサービスロボットの市場も広がりつつある一方、セキュリティに関しては、体系的なガイドラインや指針は存在せず、個別のメーカ・サービス事業者に任されているのが現状である。個人情報扱ったり、物理的に動くロボットは、セキュリティの脅威にさらされた際に、IT・IoT 機器とはまた異なるリスクが顕在化する可能性も指摘されている。

本ガイドラインは、既存の IT・IoT、あるいは FA 機器等のセキュリティ標準やガイドラインを援用しつつも、ロボット特有の守るべき資産・情報について見直すとともに、システム構造やサービス運用から想定される脅威や、ロボット特有の安全機能との関係、これらを総合した結果としてのリスクについて明らかにし、ロボットとその開発・運用などに必要な機能・設備を含めたシステム（以下、ロボットシステムと呼ぶ）において、とるべきセキュリティ対策の指針を示すことを目的とする。

ロボットシステムは物理空間とサイバー空間が相互に連携して動作することからセーフティとの相互影響や関係性も考慮する必要がある。このようなロボットシステムの特徴を踏まえたセキュリティの検討のために、RRI（ロボット革命・産業 IoT イニシアティブ協議会）では 2021 年度からロボットセキュリティ調査検討委員会を設置し、多様な業種・職種から構成される委員が集まって様々なユースケースを集め共通のテーマや課題を検討・整理する活動を行ってきた。本ガイドラインはその成果をまとめたものである。

1.1. 背景

1.1.1. ロボットを取り巻く環境の変化とセキュリティの重要性

ロボットを取り巻く環境は急激に変化している。

従来のロボットは、産業用ロボットに代表されるように従来のロボットは工場の生産現場を中心に活躍してきた。特定の環境の元で特定の仕事を速く正確に行うのがロボットの主な仕事であった。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の中で人間と共存しながら様々な環境で様々な仕事をする事が期待されるようになった。いわゆるサービスロボットである。サービスロボットの普及は、新型コロナウイルス感染症の影響もありますます加速しつつある。一方、工場内でも人と作業空間を共有する人協働型ロボットも普及しつつあり、ロボットは工場の柵の中にとどまらず工場内の搬送まで含めてその活動範囲を拡大しつつある。

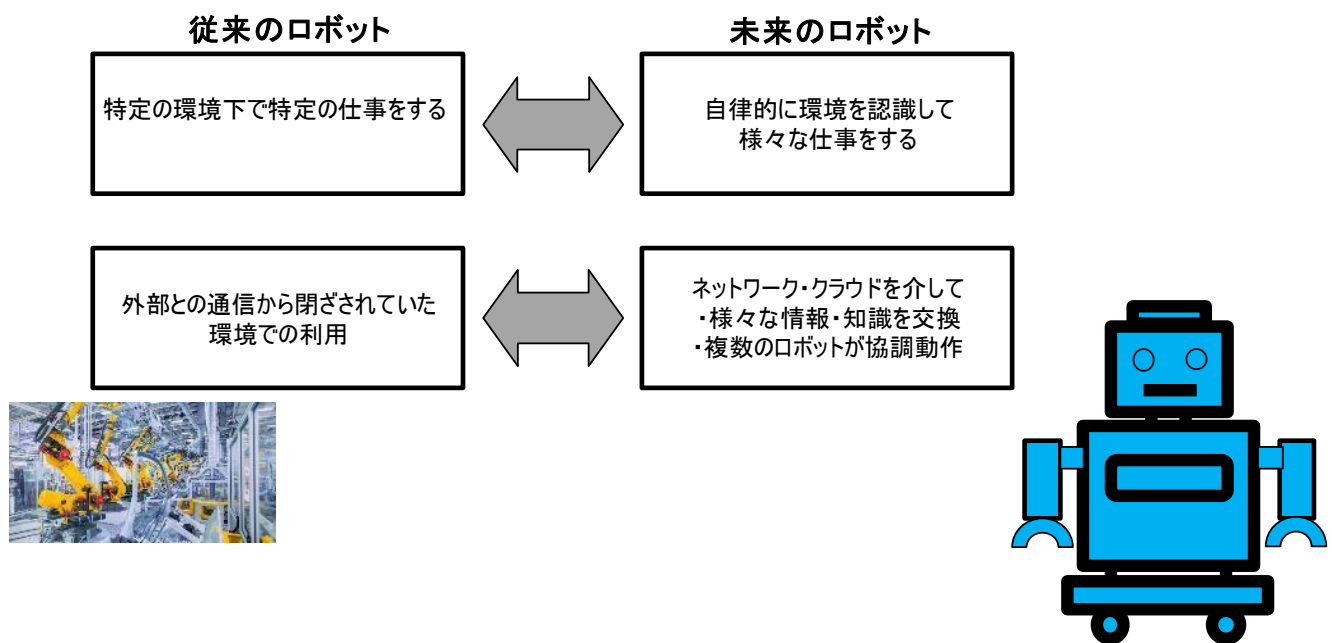


図 1-1 従来のロボットとこれからのロボットの違い

ロボット技術も進化を遂げている。SLAM 等を実装し自律的に環境を認識して移動し様々な仕事をするロボットへと進化している。また、新しい技術を柔軟に取り入れるために、ロボット単体の中にすべての機能を埋め込むのではなく、機能要素を分散しネットワーク経由でそれらが連携して目的の機能を提供するという形態へと進化している。この考え方は、クラウドロボティクスとも呼ばれる。従来は、外部との通信から閉ざされていた環境で動いていたロボットが、ネットワークを介して様々な情報や知識を交換するようになる。

1.1.2. ロボットセキュリティの現状

ロボットの多様化・多目的化、クラウド化の流れが進展すると、危惧されるのがセキュリティへの懸念である。悪意ある攻撃によりネットワーク経由でロボットが攻撃され情報を搾取されたり、機能

を停止されたりするだけにとどまらず、制御にかかわる情報が改竄されると誤った行動を起こさせる可能性もあり、その影響は非常に大きい。

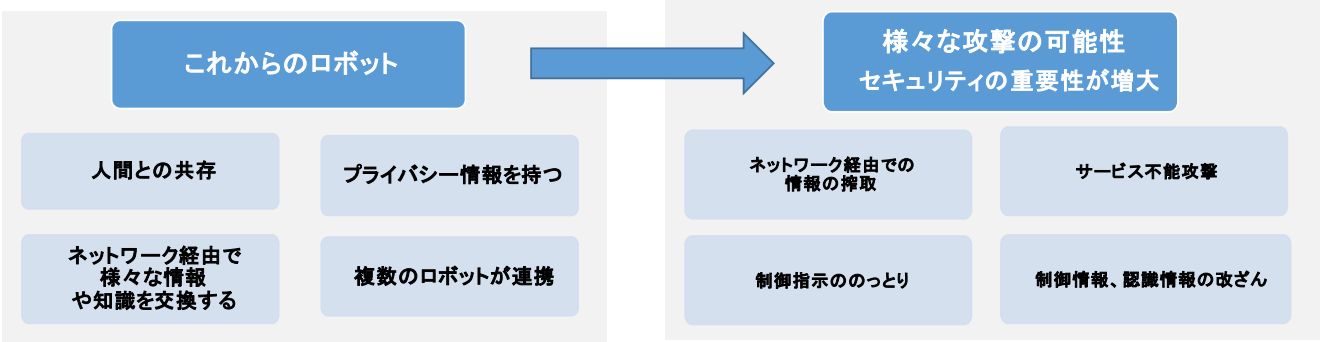


図 1-2 増大するロボットセキュリティの重要性

ロボットのセキュリティを扱った研究やガイドラインは現段階では非常に少なく、国内の事例はわずかしかない。その多くは関連する他の分野、例えばセーフティや IoT などの中で一部が言及されてきたにとどまっており、ロボットの性質やユースケースを踏まえた上で体系的に整理されているとはいえないのが現状である。

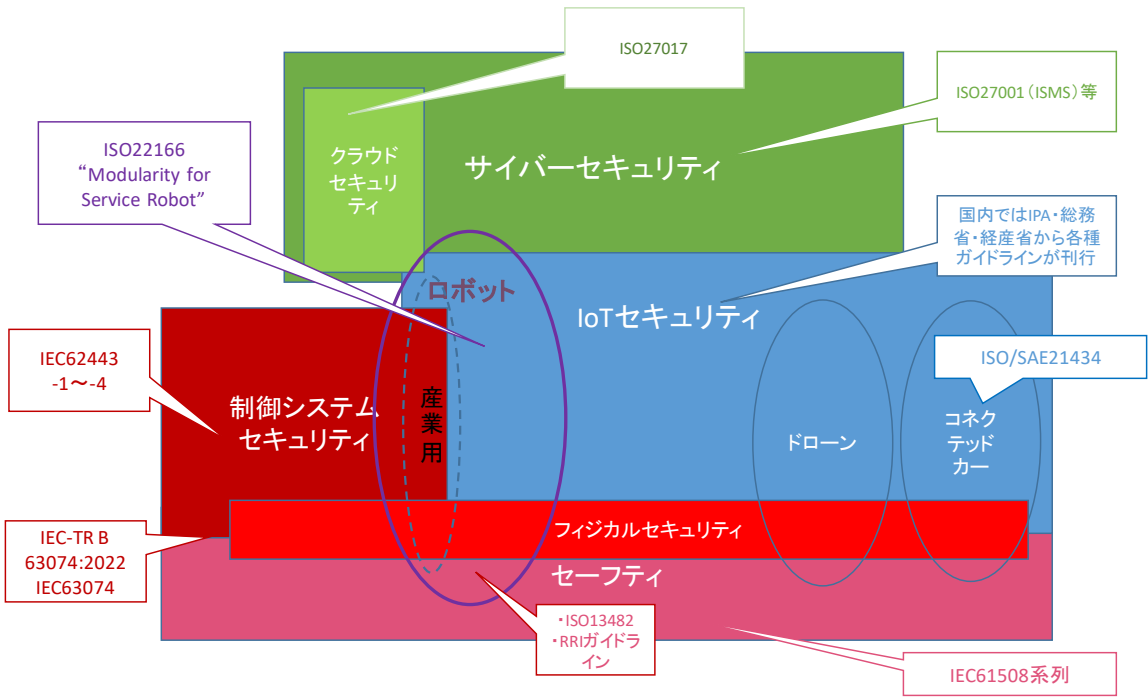


図 1-3 ロボットセキュリティ関連の規格

1.2. ロボットセキュリティの特徴と課題

ロボットのセキュリティには、従来のサイバーセキュリティにはない、あるいはより重視が必要な特徴と課題がいくつか存在する。

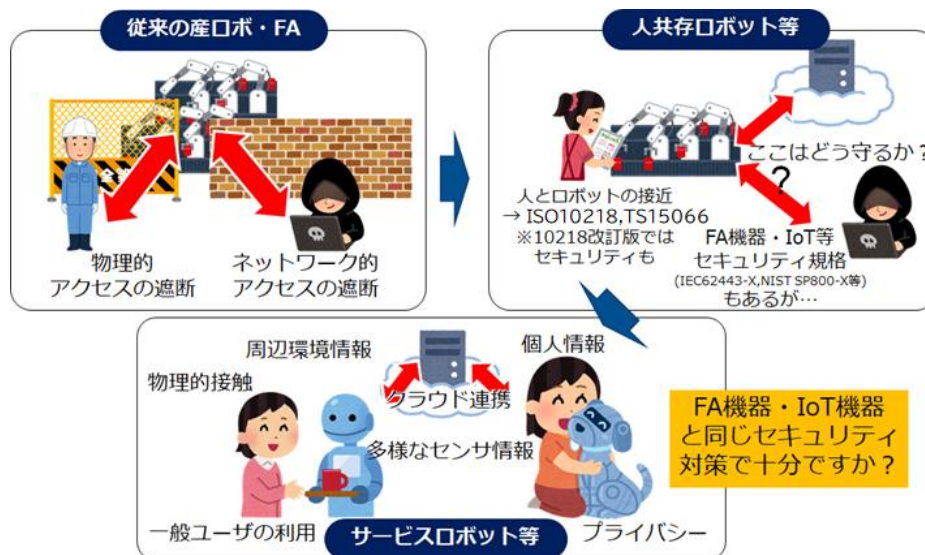


図 1-4 ロボットセキュリティの特徴

① 守るべき資産の多様性

ロボットのセキュリティを考える上での大きな特徴のひとつは、関連する資産が非常に多岐にわたる点である。工場で行われる産業用ロボットに対し、サービスロボットはより多彩な環境で使用されるためにこの特徴は色濃く表れる。例えば情報資産を例にとっても、センサーが認識する環境情報、カメラが認識する画像、ロボットの状態を示す情報、制御に関わる情報など様々でありこの中にはプライバシーに関わる情報も含まれる。

また、情報資産だけにとどまらずロボットが動作する環境に存在する物理資産や扱う対象物なども守るべき対象として考慮に入れる必要がある。セキュリティ対策を検討するにあたっては、それらの資産の洗い出しと整理が重要となる。

② 物理的な脅威とその影響

ロボットは物理空間とサイバー空間が相互に連携して動作することからセーフティとの相互影響や関係性も考慮する必要がある。

③ ユースケースと通信フローの複雑さ

ロボットが目的どおり動作にするには、関連するシステムとの間で様々な情報をやりとりする。

セキュリティを検討するにあたっては、ロボットが動作するのにともなってどのような情報が処理され、どのような情報が伝達されるのかのユースケースと通信フローを洗い出す必要がある。

たとえば管理者が搬送ロボットへ目的地への移動を指示する場合は、管理システムの UI へ目的地が入力された後、その情報は座標変換されて移動メッセージが生成される。移動メッセージは通信ブローカを介してロボットへ伝達され、その内容を受信した搬送ロボットは、経路計画を立てて内部の台車機構に移動方向や速度を指示するなどの一連の挙動が発生する。

④ 脅威事象の多岐にわたる影響範囲や相互影響

ロボットでは、セキュリティの脅威がもたらす事象とその影響範囲が従来のサイバーセキュリティ以上に大きくなる場合が多い。たとえば、“改竄”という脅威について考えてみると、従来のサイバーセキュリティの観点ではそれは“完全性”の阻害にあたる。サーバーコンテンツやメールの内容の書き換えが発生した場合に誤った情報が様々な混乱をもたらす可能性はあるが、人が間にはいるために影響は一定レベルに抑えられる。一方ロボットの場合は、動作ロジックや状態ロジック、認識情報の改竄が行われた場合は、データの“完全性”の阻害だけではなく、ロボットの動作や提供するサービスの誤動作など“可用性”にも影響を与える。

ロボットセキュリティにおいては、網羅的に脅威を洗い出し、それによる影響・リスクを分析して可視化していくことが従来のサイバーセキュリティ以上に重要になる。

⑤ 多数のステークホルダを含むサプライチェーンとセキュリティポリシーの違い

ロボットを利用したシステムやサービスは、多くの場合、複数の組織や事業者による分散開発が基本であり、企画から設計・開発、運用までには、様々なステークホルダが関連してくる。ロボットコンポーネントのハードウェア・ソフトウェアやその部品を提供するメーカ・サプライヤ、管理システム等を開発する IT ベンダ、ソフトウェア開発会社、それらを組み上げるロボットシステムインテグレータ、更には出来上がったシステムをサービスとして利用者に提供するサービス事業者、そのサービスの運用維持を行う運用管理者・メンテナンス事業者などである。

ロボットシステム全体は、上記のような多数のステークホルダを含むサプライチェーンで成り立っており、設計時のセキュリティ要件から運用時のインシデント対応までを、これらの関係者間で調整し実現する必要がある。

1.3. 目的

本書は、ロボットシステムの価値を利用者に安全に届けるためのセキュリティ上の検討の指針となることを目的とする。

1.4. 本ガイドラインにて提示する情報

- ロボットシステムのセキュリティに関する基本的な考え方と検討の流れ(フェーズ・プロセス)
- 各フェーズ・プロセス検討のポイント(脅威分析・リスク評価・対策・テスト・運用項目など)
- ユースケース・ケーススタディ
- 実ビジネススキームにおけるロボットセキュリティ実施のための体制やワークフロー例
- 各種関連情報

1.5. 対象読者

ロボットに関わる以下のステークホルダを対象とする

- ロボットメーカ(ロボットコンポーネント開発者・製造者等)
- ロボット関連部品サプライヤ
- ロボット関連 IT ベンダ(ロボットソフトウェア開発会社等)
- ロボットシステムインテグレータ

- ロボットサービス提供者(事業者)(ロボットサービスプロバイダ)
- ロボット運用管理者
- ロボット関連施設・インフラ提供者

表 1-1. 各章と対象読者の対応表

	ロボット メーカー	ロボット 関連サ プライヤ	ロボット 関連 IT ベンダ	システム インテグ レータ	サービス 提供者	ロボット 運用管 理者	施設・イン フラ提 供者
第1章	◎		◎	◎	◎	○	○
第2章	◎		◎	◎	◎	○	○
第3章	◎		◎	◎	◎	○	○
第4章	○		○	○	◎		
第5章	◎		◎	◎			
第6章	◎	◎	◎	◎		◎	○
第7章	○		○	○	◎	◎	◎
第8章					◎	◎	

＜凡例＞◎:必須、○:推奨

ロボット利用者(サービス受益者)は、直接的な対象読者ではないが、利用者が実施すべきセキュリティ対策などがあればサービス事業者(提供者)側からその内容を提示するという前提にたっている。したがって、利用者側もサービス提供者から促されるセキュリティ対策は必要に応じて実施する場合があることは考慮されたい。また、上記の各種事業における情報セキュリティ対策の実施責任者もロボットシステムのセキュリティを監査する立場が今後要求されることも想定され、本ガイドラインがその参考になれば幸いである。上記の各種事業の経営者もビジネスを発展・継続させる立場からロボットに関わるセキュリティリスクを認識しておくことは非常に重要であり、冒頭の3章の部分は読みいただければ幸いである。

1.6. 委員名簿

委員長	エンハンスザックス(株)	山崎 治郎
副委員長	(学)会津大学	屋代 眞
監修	(国研) 産業技術総合研究所	安藤 慶昭
委員	(学)会津大学	中村 章人
	(学)会津大学	成瀬 継太郎
	(学)会津大学	矢口 勇一
	アズビル(株)	八鍬 宏司
	国際航業(株)	武田 浩志
	(国研)産業技術総合研究所	五十嵐 広希
	(株)JR東日本商事	大野 誠一郎
	セイコーエプソン(株)	長谷川 浩
	セイコーエプソン(株)	中槇 基裕
	(株)セック	建部 貴隆
	(株)セック	中本 啓之
	TIS(株)	松井 暢之
	THK(株)	三好 崇生
	テュフラインランドジャパン(株)	深見 正教
	テュフラインランドジャパン(株)	貝田 章太郎
	(株)東芝	平山 紀之
	(一財)日本品質保証機構	高村 博紀
	ネットワンシステムズ(株)	東根 真司
	ネットワンシステムズ(株)	佐々木 藏徳
	パナソニック(株)	岡本 球夫

(株)日立製作所

吉内 英也

富士ソフト(株)

二宮 恒樹

(株)本田技術研究所

鵜浦 清純

(一社)日本ロボット工業会

三浦 敏道

(学)東北大学

田所 諭

オブザーバー

(国研)新エネルギー・産業技術総合開発機構

赤羽根 亮子

2. スコープ

2.1. 対象としているロボットシステム

ロボットとは、元来は認識系、制御系、動作系の3要素を合わせ持ち、与えられた目的を実行するために動作する装置・機械のことである。

現代のロボットの機能・用途は様々である。従来は、産業用ロボットとサービスロボットに大別されることが多かった。しかし、昨今は、産業用ロボットも工場の製造ラインの柵内だけにとどまらず、工場内の搬送などまで含めてその活動範囲(利用範囲)を拡大しており、サービスロボットとの境界はなくなりつつある。

本ガイドラインでは、このような流れを踏まえ、ロボットシステムを広く捉え、関連する機能をコンテキストとして明確にし、セキュリティに関する要件定義から行うというアプローチをとることとした。

ロボットは、近未来より多くの事業領域に利用されるとともにその使われ方や提供する機能も拡張されることが見込まれる。将来新しい種類のロボットが出てきたときにそれに対応できる柔軟性と拡張性を持っておくことが理想的であり、従来の枠組みの中で固定的に考えると内容の形骸化も早くなることを考慮した。

2.2. 対象となるセキュリティの範囲

ロボットの動作に直接関わる全システムを対象としてセキュリティを検討することとした。この中には、ロボットを管理するシステムやロボットが動作するにあたって参照するシステム、ネットワークも含まれる。また、クラウド上で動作するシステムについても検討の対象とした。図2-1に検討対象となるシステム構成概念図、表2-1に構成する各部位の解説を記載する。

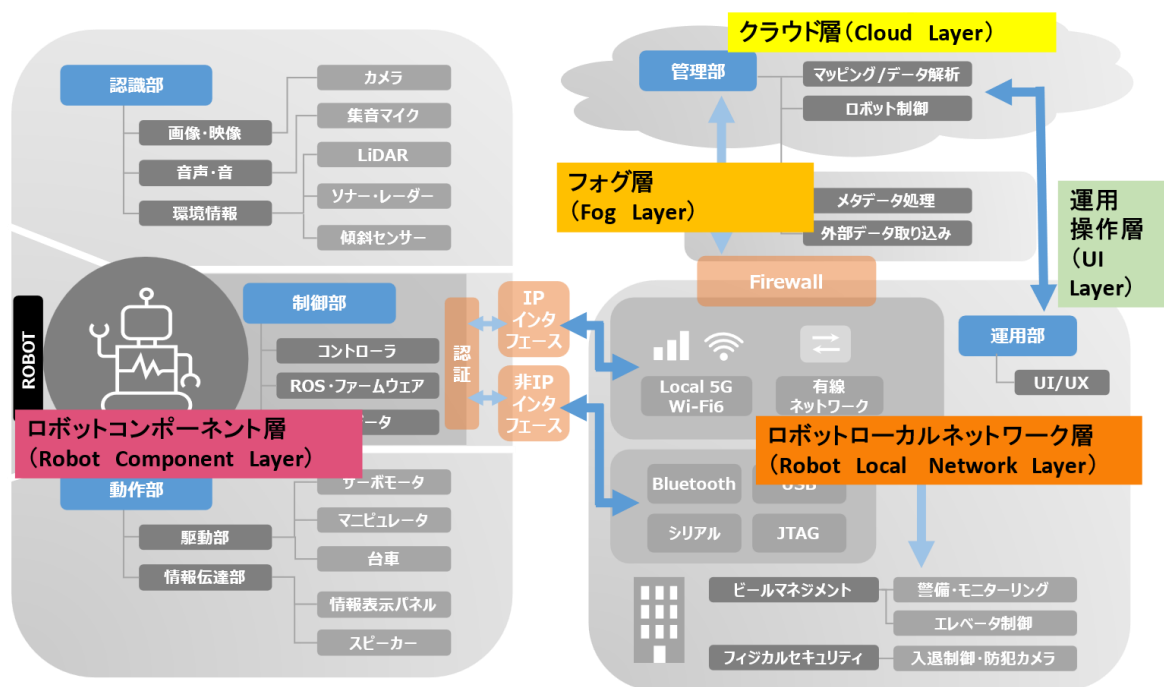


図 2-1 ロボットシステム構成概念図

表 2-1 ロボットシステム構成部位の解説

階層	部位	機能解説	設置システム例
クラウド層 (Cloud Layer)		<ul style="list-style-type: none"> ・ロボットを管理する機能を提供する ・ロボットと外部システムとの中継システムを提供する ・ロボットが実行する仕事を管理する <ul style="list-style-type: none"> - 命令の制御情報への変換 - ロボット状態情報の管理 	<ul style="list-style-type: none"> ・ロボット管理ソフトウェア ・データリポジトリ ・AI 学習・推論システム
フォグ層 (Fog Layer)		<ul style="list-style-type: none"> ・複数のロボット・ローカルネットワークを集約し、クラウド層へ中継する役割を果たす ・ロボットとクラウド層のシステムを仲介するシステムを提供する 	<ul style="list-style-type: none"> ・AI 推論システム ・メッセージ PubSub ブロカー ・踏み台サーバ ・ファイアウォール・DMZ

階層 (続き)	部位	機能解説	設置システム例
ロボットコンポーネント層 (Robot Component Layer)	制御部	<ul style="list-style-type: none"> ・ロボットの動作を制御・管理する機能を提供する ・上位システムとの連携インターフェースを提供する ・通信インターフェースを提供する (IP インターフェース、非 IP インターフェース) ・システム情報を管理する <ul style="list-style-type: none"> -アカウント管理機能 -認証・認可機構 -ログ機能 ・施設連携インターフェースの提供 	<ul style="list-style-type: none"> ・ロボット・コントローラ ・制御 PC
	動作部	<ul style="list-style-type: none"> ・制御部からの指定を受けて動作機構(マニピュレータ、移動台車等)を駆動する (・動作情報を制御部へ伝達する) 	<ul style="list-style-type: none"> ・マニピュレータ ・移動台車 ・スピーカー
	認識部	<ul style="list-style-type: none"> ・ロボットが仕事をするために必要な情報を認識する機能を提供する 	<ul style="list-style-type: none"> ・カメラ、マイク ・環境センサー
運用操作層 (UI/)		<ul style="list-style-type: none"> ・人間がロボットへの仕事を指示するユーザインタフェース(UI)を提供する ・ロボットの状態、仕事の軌跡を視覚化するインターフェースを提供する 	<ul style="list-style-type: none"> ・タブレット ・スマホ ・ペンダント ・スマートスピーカー

ただし、クラウド層においてクラウドサービス事業者側が担保するセキュリティの責任範囲については検討の対象外となる。クラウドサービス事業者が提唱する責任共有モデルに従い責任を分担することが前提となる。(図 2-2 クラウドサービス責任共有モデルイメージ参照)

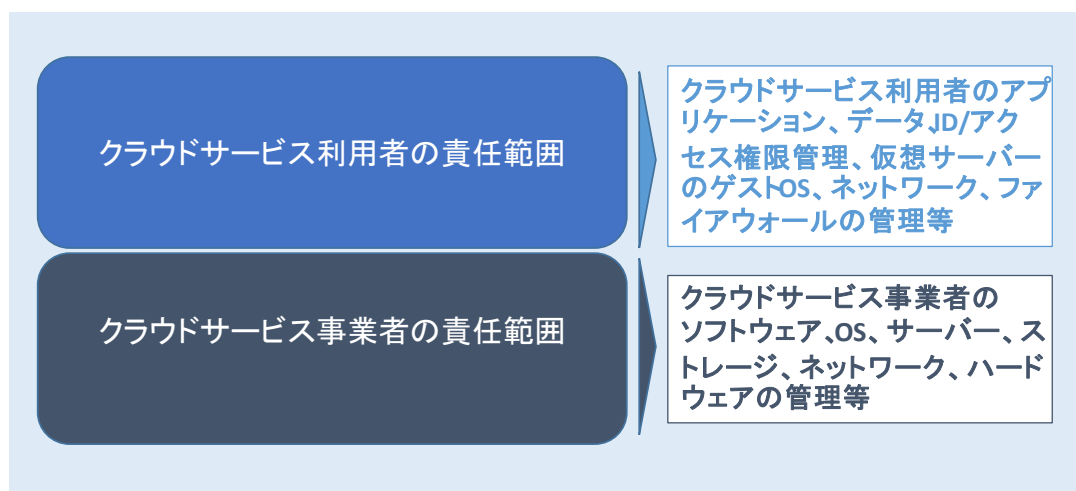


図 2-2 クラウドサービス責任共有モデルイメージ

ロボットは、サイバー空間と物理空間が相互に連携して動作することから、従来のサイバーセキュリティのようにサイバー空間内だけでなく、物理的な要因・影響も含めて考えることとした。

表 2-2 物理空間とサイバー空間の相互影響

トリガー(要因)	影響	例
サイバー攻撃	サイバー空間	<ul style="list-style-type: none"> ➤ ロボットへネットワーク経由で侵入し情報を盗み出す ➤ ネットワーク越しにロボットへサービス不能攻撃をしかける
サイバー攻撃	物理空間	ロボットに偽制御情報を送り付け、ロボットの動作や経路を狂わせる
物理攻撃	サイバー空間	<ul style="list-style-type: none"> ➤ 物理的にロボットを元の場所から動かし、自己位置推定情報を狂わす ➤ ロボットの物理インターフェースに攻撃用 PC をつなぎサイバー攻撃
物理攻撃	物理空間	<ul style="list-style-type: none"> ➤ ロボット本体を持ちだしディスクを盗難する、破壊する

2.3. セーフティとの関係性

サービスロボットは日常生活で人間との共生すること、物理空間とサイバー空間が相互に連携して動作することからセーフティとの相互影響や関係性も考慮する必要がある。

セキュリティ、セーフティともに日本語に翻訳すると“安全”である。

- セキュリティ 悪意のある攻撃からの保護（可用性、完全性、機密性の維持）
- セーフティ 誤動作、事故、悪環境からの保護（許容可能なレベルに維持）

セキュリティとセーフティは似ているが、その向かうベクトルが異なる。セキュリティは、環境からシステムへの影響を無害にすることを目指しているのに対して、セーフティは、システムが環境に対して与える影響を無害にすることを目指している。（図 2-3 参照）

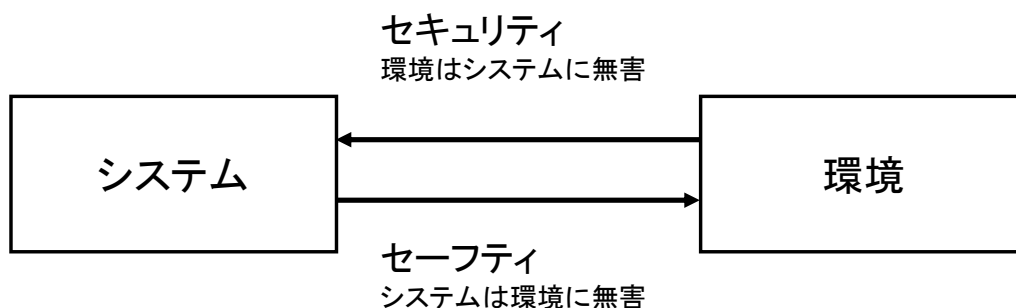


図 2-3 セキュリティとセーフティの関係性

従来は、セキュリティのリスクとセーフティのハザードは独立した別々の要件として考えられてきた。しかし、ロボットも含む IoT システムではセキュリティとセーフティが相互に影響しあう可能性が出てきた。特にサービスロボットシステムにおいては、サイバー攻撃が物理的な危害を引き起こす可能性もある。逆に、セーフティを確保するための物理的な所作や機構が逆にサイバーシステムのリスクを引き起こす可能性もある。本ガイドラインでは、それらの相互関係を踏まえセキュリティ側で考慮すべき点、セーフティ側で考慮すべき点とその相互影響を整理してモデル化することとした。

詳細は、第 5 章をご参照されたい。

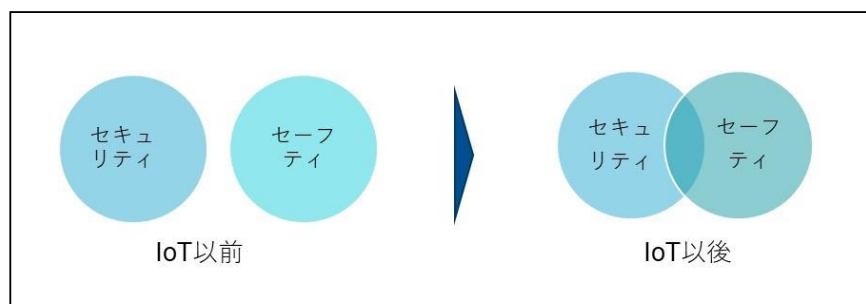


図 2-4 セキュリティとセーフティの関係性の変化

2.4. プライバシーとの関係性

ロボットシステムは、個人情報、プライバシーにかかわる情報を保持・交換するケースも想定される。本ガイドラインではプライバシー対策については直接扱わない。セキュリティリスクがプライバシーを侵害する可能性がある場合は、その影響を考慮に入れる。

3. ロボットシステムのライフサイクルとセキュリティ検討

本章では、ロボットのシステム開発～運用に至るセキュリティ検討の流れとその位置づけについて解説する。

3.1. アプローチ

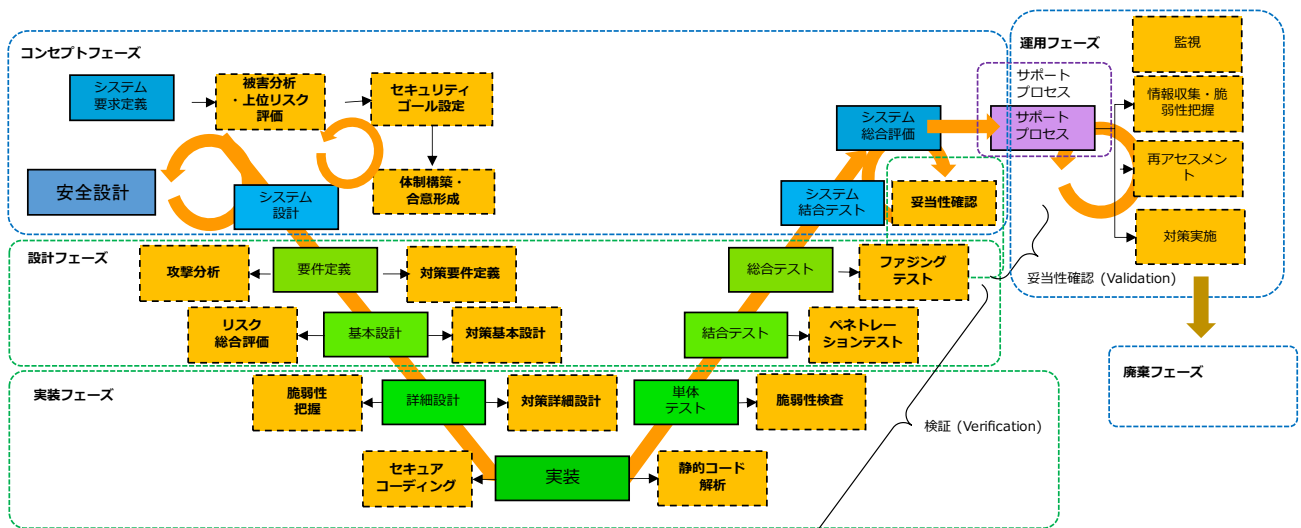
セキュリティの検討には様々なアプローチがある。代表的なものとしては、一定の基準を参照して対策を検討するベースラインアプローチや、設計段階でシステム毎のリスク評価をおこなった上で対策を検討するセキュリティバイデザインのアプローチなどである。

本ガイドラインでは、主としてセキュリティバイデザインアプローチをとることとした。同じ機能を持つロボットでも、使用される環境と用途によって生まれるセキュリティリスクが違ふこと、セキュリティ要素への優先順位が異なることも考慮する必要があるからである。ただし、それはシステムの企画・検討段階からセキュリティを考慮して設計を行うというアプローチであり、運用後は何もしないというアプローチではない。セキュリティは、攻撃手法の進化や関連するシステムの更新などの環境変化によって時間の経過とともにリスクや対策の要件が変化するために、全ライフサイクルに及ぶ検討を繰り返し行う必要がある。運用段階に入っても定期的な対策内容の見直しやリスクの再評価も必要である。その意味では、セキュリティバイデザインアプローチをとりながらも、システム全体のライフサイクルの中でセキュリティに関わる実施内容を整理して記載することとした。また、ベースラインアプローチによって、セキュリティレベルを一定以上に保つという考えも重要であり、対策の事例を第5章、及び末尾の APPENDIX C に Hint&Tips 的につけることとした。

また、ロボットシステムは、ソフトウェア、ハードウェア、クラウドサービスなど多岐にわたるサブシステムから構成され、関連するステークホルダも多岐にわたる分散開発が基本である。そのために、セキュリティの検討においても、節目節目で関係する組織でその内容を合意しながら次の工程へ進むことがセキュリティレベルを維持する意味では非常に重要になる。セキュリティ検討の流れにおいては、それら複数組織をまたがる連携や合意形成についても考慮した。

3.2. ロボットシステムのライフサイクル構成

本ガイドラインでは、セキュリティ検討をロボットシステムのライフサイクルの中に組み込むことを考慮に入れ、安全性の検討の流れとも整合を取ることにした。このような考え方にのっとり、RRI の他のガイドラインでも採用しているロボットシステムの開発から実用までの V 字モデルと3フェーズアプローチをベースとして、それに運用、廃棄のフェーズを加えた5フェーズの構成の中でセキュリティを扱うこととした。(図 3-1 参照)。ロボットは内部に利用者のプライバシーにかかわる情報を保持する場合も多く、廃棄にあたってはそれを消去するなどの対策も必要となるからである。



引用：ESPR (Embedded System development Process Reference) 2.0
システム開発プロセス（実線）にセキュリティ関連項目（破線）を追記

図 3-1 ロボットシステムのライフサイクルとセキュリティ検討項目

引用：ESPR (Embedded System development Process Reference) 2.0

システム開発プロセス（実線）にセキュリティ関連項目（破線）を追記

ロボットシステムのライフサイクルを構成する各フェーズの位置づけを以下に解説する。

➤ コンセプトフェーズ

ロボットを利用した製品・システム・サービスの機能や利用形態を検討し、その効果や事業性を実証するフェーズ

➤ 設計フェーズ

商品化を前提にロボットを利用した製品・システム・サービスの詳細を設計するフェーズ

➤ 実装フェーズ

設計した製品・システム・サービスを開発・実装・テストし、商品として完成させるフェーズ

➤ 運用フェーズ

商品化した製品・システム・サービスをリリースし、運用するフェーズ

➤ 廃棄フェーズ

製品・システム・サービスに関わるリソースを廃棄または返却するなどして利用を停止するフェーズ

3.3. ライフサイクルの各フェーズとセキュリティ検討

ロボットシステムのセキュリティは、ライフサイクル全体で考える必要がある。前項で示したライフサイクルの各フェーズにおいて、セキュリティ検討の目的とゴールがあり、関係するステークホルダー間でその内容を相互確認しながら次のフェーズへと進む必要がある。各フェーズのセキュリティ検討における目的とゴールは以下のように設定することを推奨する。(表 3-1)

表 3-1. ロボットシステムのライフサイクルとセキュリティ検討の関係

フェーズ	目的	ゴール	実施事項
<p>コンセプトフェーズ</p> <p>(説明) ロボットを利用した製品・システム・サービスの機能や利用形態を検討し、その効果や事業性を実証するフェーズ</p>	<ul style="list-style-type: none"> ・セキュリティゴールを設定し、関係者で合意形成すること 	<ol style="list-style-type: none"> 1. セキュリティゴールの策定 2. セキュリティ実施体制の構築 	<p>被害分析</p> <p>上位レベルのリスク評価</p>
<p>設計フェーズ</p> <p>(説明) 商品化を前提にロボットを利用した製品・システム・サービスの詳細を設計するフェーズ</p>	<ul style="list-style-type: none"> ・セキュリティリスク評価 ・セキュリティ対策の要件定義 	<p>セキュリティ対策の優先順位付けと要件の確定</p>	<p>攻撃分析</p> <p>安全性影響評価</p> <p>リスク総合評価</p> <p>対策要件定義</p>
<p>実装フェーズ</p> <p>(説明) 設計した製品・システム・サービスを開発・実装・テストし、商品として完成させるフェーズ</p>	<ul style="list-style-type: none"> ・セキュリティ実装作業とテスト ・総合評価 	<p>セキュリティ実装結果の評価と承認</p>	<p>実装作業・テスト</p> <p>結合テスト</p> <p>総合テスト</p> <p>総合評価</p>
<p>運用フェーズ</p> <p>(説明) 商品化した製品・システム・サービスをリリースし、運用するフェーズ</p>	<ul style="list-style-type: none"> ・セキュリティゴールの維持管理 	<ul style="list-style-type: none"> ・運用設計・サポートプロセスの構築 ・運用体制の構築 ・運用業務の実施 	<p>関連文書のチェック</p> <p>運用レベルのリスク評価</p> <p>運用体制の構築</p> <p>教育・訓練</p>
<p>廃棄フェーズ</p> <p>(説明) 製品・システム・サービスに関わるリソースを廃棄または返却するなどして利用を停止するフェーズ</p>	<p>廃棄時、あるいは再利用時に情報が削除された状態で機能を停止・再開できること</p>	<p>安全に機能を停止し、情報を削除すること</p>	<p>情報の削除作業</p> <p>機能の停止作業</p>

3.4. セキュリティ検討の実施組織～ビジネスケースにおける複数ステークホルダ間の連携について

ロボットシステムのコンセプトを企画・実証し、関連する製品やサービスの設計・開発をへて、運用・実用にのせる実際のビジネスケースを考えた場合、多岐にわたるステークホルダが絡み、その中で目標とするセキュリティレベルを維持するには、その節目・節目において関連する組織・ステークホルダが方針や実施内容・結果について合意、承認をする必要がある。

本項では、前項で述べたセキュリティ検討の流れと各フェーズでの位置づけを踏まえ、関係する組織がどう連携し、どう相互確認を行うべきかについて事例を踏まえて考察する

3.4.1. ロボットビジネスに関連するステークホルダ

第2章で述べたようにロボットは多岐にわたる用途で使われており、その用途やビジネスの形態に応じて関係する組織や機関は異なる場合があり、本ガイドラインで示すのはあくまでも一例である。しかし大部分のケースにおいては必要な役割は共通しており、役割分担が異なるだけのことが多い。

例えば、典型的な事例における機能要求・非機能要求をいくつか挙げてみる。

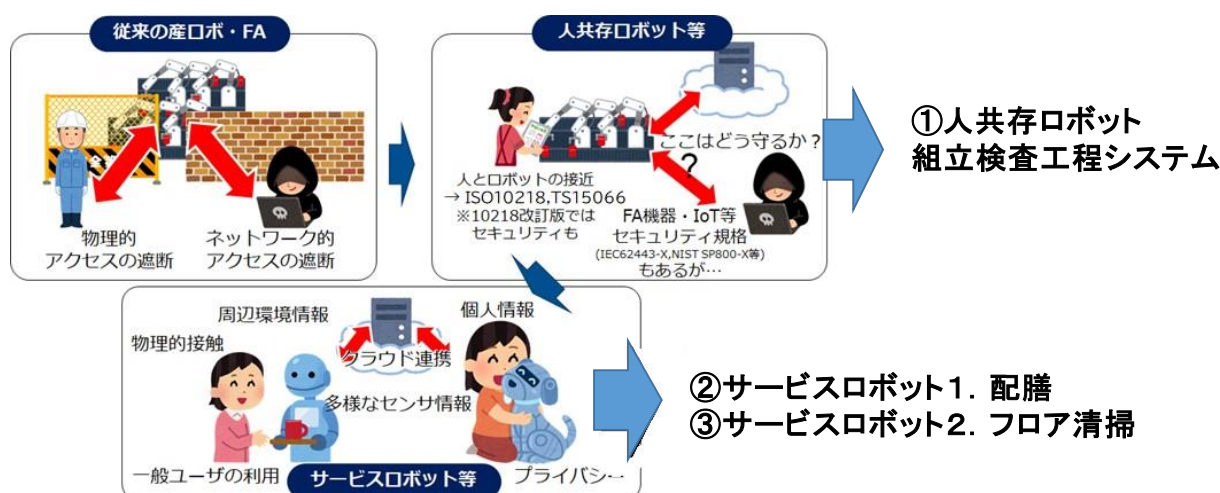


図 3-2 広がるロボットの利用形態

事例①: 図 3-2 「人共存ロボット」

○想定機能: 製造工場において、産業用ロボット(マニピュレータ)を用いた組立・検査工程システム

- ・ 対象物の情報(形状等)を持ち、それに基づいて対象物をハンドリングし、画像で検査する。
- ・ 検査用データはクラウドに上げて分析し、検査機能を継続的に改善する。

○上位要求:

- ・ 効率的な生産をしたい
- ・ 製造状況のリモートモニタリングや、データ収集による工程改善を行いたい
- ・ 安全でセキュアな運用をしたい
 - ・ 製造対象に関するデータは機密情報なので、漏洩はさせない
 - ・ 外部からの攻撃でシステムが止まったり、誤動作したりはさせない
- ・ 現実的な投資額の中で実現したい
 - ・ 立上コスト、運用コスト

事例②: 図 3-2 「サービスロボット1: 配膳」

○想定機能: レストランで、料理の注文を取って配膳・下膳するロボット

- ・ 来店したお客様とコミュニケーションを取る
- ・ 適切なテーブルに料理を運ぶ
- ・ 基本はロボットに任されているが、場合によってはリモートから人間の管理者が介入して、お客様と対話したりロボットを遠隔操作したりする

○上位要求

- ・ お客様に不快な思いをさせずに配膳・下膳したい
- ・ 安全で衛生的に時間をかけすぎずに料理を運びたい
- ・ セキュアな運用をしたい
 - ・ お客様のプライバシーにかかわる画像を漏洩させない
 - ・ 外部からの攻撃でロボットが止まったり誤動作したりはさせない
- ・ 現実的な投資額の中で実現したい
 - ・ 立上コスト、運用コスト

事例③: 図 3-2「サービスロボット2:フロア清掃」

○想定機能: 一般者が行き来する大規模施設で、床面を走査して清掃するロボット

- ・ 清掃状況をリモートでモニタリングしたり記録したりできる
- ・ 障害物の位置が動的に変化しても対応できる
- ・ 基本はロボットに任されているが、場合によってはリモートから人間の管理者が介入してロボットを遠隔操作できる

○上位要求:

- ・ フロア全体を定期的に清掃する
未清掃の場所を残さない
- ・ その場にいる一般者に迷惑をかけない
人にぶつからない、危害を加えない
一般者の移動を妨害しない
- ・ セキュアな運用をしたい
お客様のプライバシーにかかわる画像を漏洩させない
外部からの攻撃でロボットが止まったり、誤動作したりはさせない
- ・ 現実的な投資額の中で実現したい
立上コスト、運用コスト

このようなビジネスを実現するときに、様々な組織やステークホルダが関係してくる。代表的な組織・ステークホルダとそのビジネス上の役割を表 3-2 に挙げる。実際のビジネスケースにあてはめた場合には、同じ事業体の中にこれら複数の職種が含まれる場合もあれば、それぞれが別の事業体として連携する場合もあり、その内容はさまざまである。

表 3-2 ロボットビジネスのステークホルダと位置づけ・役割

ステークホルダ名称	ビジネス上の位置づけ・立場
サービス受益者	ロボットシステムが提供する利便性の恩恵を受ける立場の人。あるいはロボットシステム稼働時にその場にいる人。例えば、工場のライン担当者やレストランのお客様、清掃ロボットが稼働する大規模施設にいる人など
インフラ提供者	ロボットサービスが提供される施設などのオーナー・管理者。レストランのオーナー、工場のラインマネージャ、ビルの施設管理者など
サービス提供者 ※JIS Y1001 では、サービスプロバイダ	<ul style="list-style-type: none"> ・ロボットを活用したシステム・サービスをビジネスとして提供する ・何をしたいか？セキュリティをどこまで考慮し、どこまでコストをかけるか？判断する
システムインテグレータ	<ul style="list-style-type: none"> ・サービス提供者の実現するシステムを構築する ・必要な部品や部材をメーカから調達する ・システム構築コストや運用コストとのバランスを考慮して安全やセキュリティの機能を定める
ロボットメーカ	サービスを提供するときに必要となる「部品」「部材」を供給する。
IT ベンダ ※含むクラウドサービス事業者	ネットワークやストレージ等の基盤システムや運用サービスを提供する
サプライヤ	メーカや IT ベンダに対して更に「部品」を提供する
ロボットシステム 運用管理者・メンテナンス事業者	サービス提供者の要求に基づいて、構築されたシステムを運用する運用時のセキュリティ、メンテナンス等を担当する

ロボットビジネスにおいてセキュリティを考える場合は、直接関わるステークホルダ・組織の他に、情報システム・情報セキュリティ組織、危機管理組織が必要に応じて技術支援をしたり、内容を監査することも想定しなければならない。（図 3-3） また、実際のビジネスケースでの組織の機能とステークホルダの対応例を表 3-3 に示す。

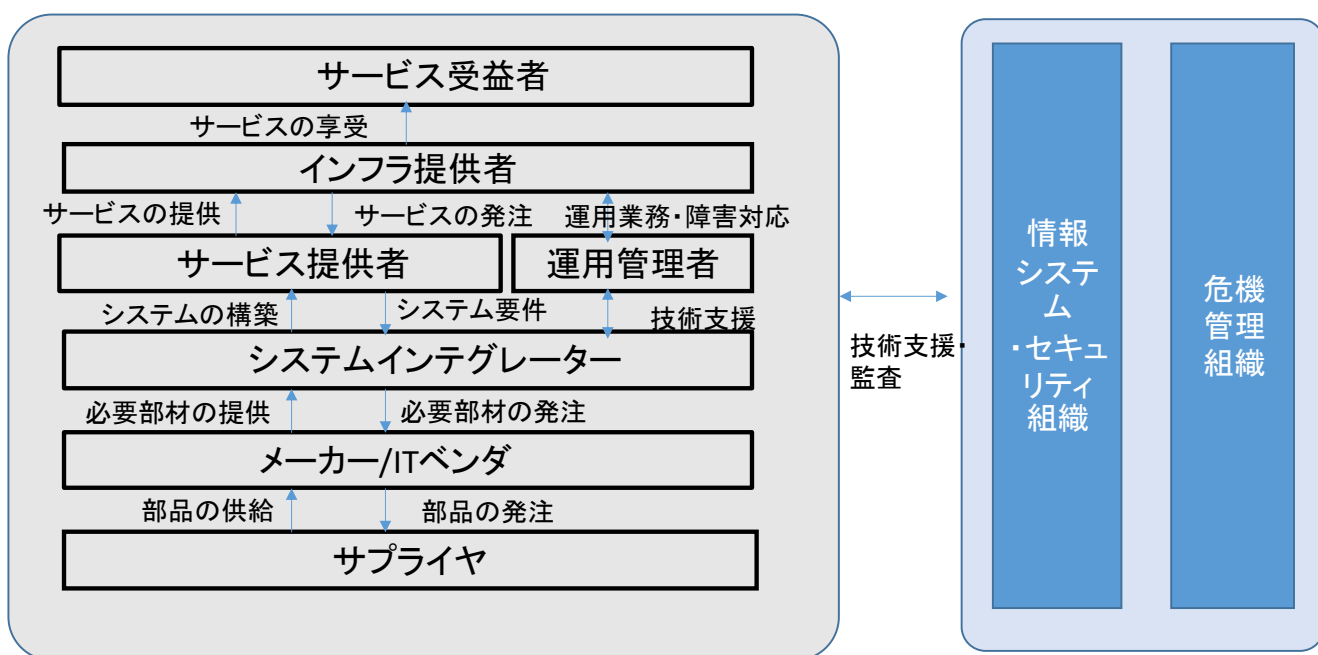


図 3-3 ロボットセキュリティに関連するステークホルダ・組織の連携体制図(例)

表 3-3 ロボットに関連するステークホルダとセキュリティ検討における機能分担(例)

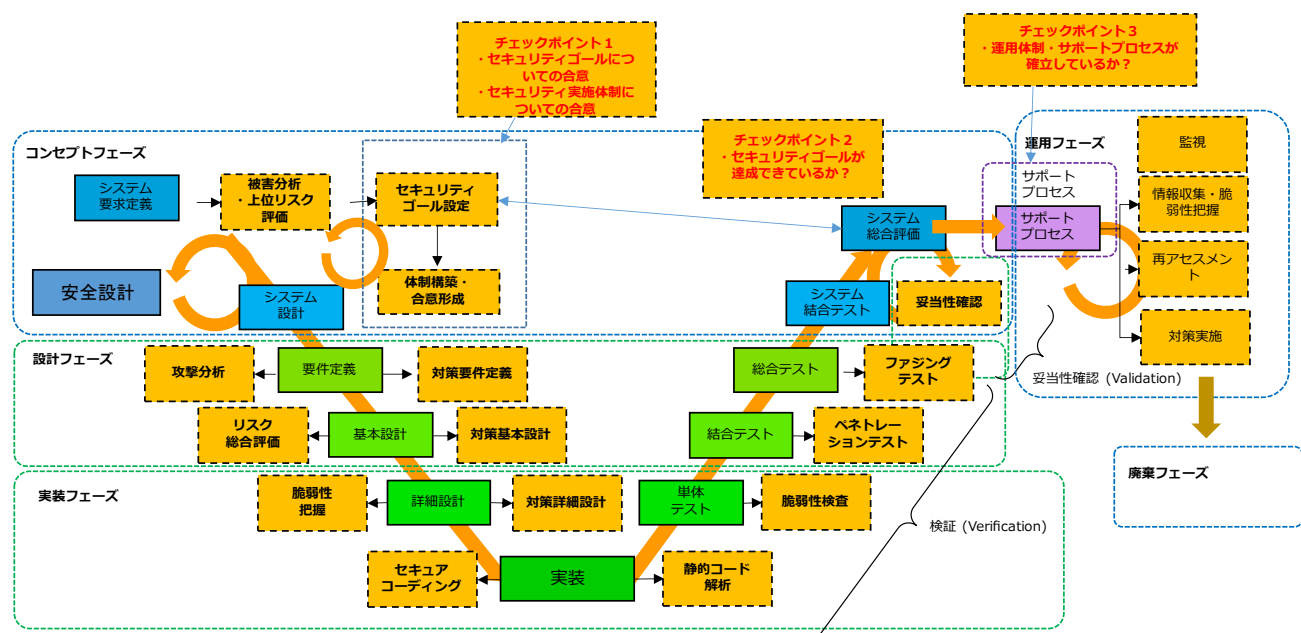
フェーズ	担当組織	解説	ビジネスケースにおける担当ステークホルダ(例)
コンセプト	企画担当組織	ロボットを利用した製品・サービスを考案・企画する組織	サービス提供者・システムインテグレータ
設計・実装	設計開発担当組織	ロボットを利用した製品・サービスを商品化・事業化するための設計開発を実施する組織	システムインテグレータ、メーカー、ITベンダ、サプライヤ
運用	運用担当組織	商品化・事業化された製品・サービスを運用管理する組織	運用管理者・メンテナンス事業者・システムインテグレータ

3.4.2. ビジネスケースにおける組織間の連携・承認のワークフロー

本節では、前項で記載したステークホルダ・組織が実際のビジネスケースにおいて目標とするセキュリティのレベルを達成するために、どう相互に連携し、相互確認を行うかについて論述する。

ロボットシステムの規模によっては、上記の 8 つの立場のうち、同一組織が複数の役割を兼ねることも多いと思われるが、いずれにせよロボットシステムがセキュアに運用されるためには、上記のような様々な立場の組織が適切に連携し、セキュリティに関する様々な観点での検討が抜け漏れなく実施され、合意されていなければならない。

本委員会では、これら様々な立場で実際のロボットビジネスに関わる委員や関係者による議論や検討を重ねた結果として、手戻りがなくセキュリティリスクを極小化するために、以下の 3 つのチェックポイントを設けることを提案する。



引用：ESPR (Embedded System development Process Reference) 2.0
システム開発プロセス（実線）にセキュリティ関連項目（破線）を追記

図 3-4 ライフサイクルにおけるセキュリティ検討のチェックポイント

チェックポイント1:コンセプト案確定時

チェックポイント2:システム構築終了時(システム納品時)

チェックポイント3:運用開始前確認時

以下、各チェックポイントの狙いと、主たるプレーヤーに期待される役割の概要を述べる。

○ チェックポイント1:コンセプト案確定時

まず、コンセプト案を確定する段階では、システムを実現する主体者であるシステムインテグレータ(企画組織)が主体となり、セキュリティゴールを検討し、それを実現するための体制や実施内容も含めて関連するプレーヤー(ステークホルダ)と合意した上で、設計・実装のフェーズへと進むべきである。セキュリティゴールとは、「どのようなリスクをどこまで受容するか?」、「どのようなリスクは絶対に回避するのか?」の基本方針・目指すレベル感である。たとえば、目標とするセキュリティのレベルをあまりに高く完全にすると製品やサービスを目標とする価格で提供できなくなるなどの事業的なトレードオフも存在する。逆にセキュリティのレベルを下げることをあまりに受容すると、情報漏洩などによる社会的な信頼低下や製品・サービスの信頼性低下などによる事業的な影響となっはねかえってくるリスクが生じる。

システムインテグレータは、使用する機器やサービスなどメーカやITベンダ、サプライヤからの情報を集約し、サービス提供者が要求するセキュリティゴールの実現のためにかかるコストや実現性を示すことで、最終的なセキュリティの基本方針をこの段階で定めるべきである。また、この時点で運用時の実現可能性や負荷・コストについても考慮し、合意しておくことが望ましい。

設計・実装フェーズで重要な脆弱性や欠陥に気づいた場合、余分な手戻りが発生し、納期やコストにも大きく影響してくるばかりでなく、致命的な問題を抱えたまま製品やサービスをリリースしてしまう危険も生じる。チェックポイント1へ向けて必要な検討事項やステークホルダとの合意・承認については、“第4章 コンセプトフェーズ”で事例も含めて詳説する。

○ チェックポイント2:システム構築終了時(システム納品時)

設計・実装フェーズの最終段階では、コンセプトフェーズで定めたセキュリティゴールをどの程度達成できているかを評価し、製品・サービスをリリースして良いかについて関連ステークホルダ、特に

サービス提供者やシステム運用者、IT ベンダやインフラ提供者の最終的な承認を得たうえで運用フェーズへと進む必要がある。ここはシステムを実現する主体者であるシステムインテグレータ(企画組織)がシステムを納品する際に実施すべきチェックであり、発注者であるサービス提供者はチェックポイント1で合意されたセキュリティゴールがどのように実現されているのかをこのチェックで確認していただきたい。チェックポイント2へ向けての必要なチェックシートやワークフローの例については、第5章、第6章の中で詳述する。

○ チェックポイント3:運用開始前確認時

運用フェーズを開始するにあたっては、定常的な運用だけでなく、新たな脆弱性が発見された場合の関係者への通知や、セキュリティインシデントが発生した場合の対応の責任分界点や連絡体制について、あらかじめ関係組織と合意をとっておく必要がある。このチェックの主体はシステム運用者となる。問題が重大化した場合はロボットに関連する部門ばかりでなく、CSIRT や経営層にも必要に応じてエスカレーションすることも考慮に入れておくべきである。また、その対応に関しても、ソフトウェア、ハードウェアのベンダやメンテナンス事業者と作業範囲や責任分界点をあらかじめ明確にしておくことが重要になる。チェックポイント3へ向けての合意事項や承認のワークフロー例などについては、“第7章 運用フェーズ”で詳説する。

関係するそれぞれの実施主体に求められる役割とインプット・アウトプットについて述べる。第2章で述べたようにロボットは多岐にわたる用途で使われており、その用途やビジネスの形態に応じて関係する組織や機関は異なる場合があり、本ガイドランで示すのはあくまでも一例である。しかし大部分のケースにおいては必要な役割は共通しており、役割分担が異なるだけのことが多い。

表 3-4 ライフサイクルの各フェーズにおけるインプット・アウトプット・実施事項

インプット	セキュリティ実施事項	実施組織 主体 (副)(支援・監査))	アウトプット
事業・製品企画書 概要設計書 機能定義書(注1) 想定製品仕様書	コンセプトフェーズ ・被害分析 ・上位レベルのリスク評価 ・セキュリティゴールの設定 ・セキュリティ実施体制の構築 (・安全分析(注2))	企画組織 (開発設計担当組織) (情報システム ・セキュリティ組織)	セキュリティゴール定義書(Appendix E-2 参照) セキュリティ実施体制表 【チェックポイント1】 ＜副産物＞ ・ユースケース図・ミスマスケース図 ・通信フロー概要 ・資産管理表(概要)
セキュリティゴール定義書 セキュリティ実施体制表 安全関連文書(注2)	設計フェーズ ・ユースケース・資産詳細整理 ・関連脆弱性情報収集 ・攻撃分析 ・安全性への影響評価 ・リスク総合評価 ・対策方針策定・対策要件定義	設計・開発担当組織 (企画担当組織、運用担当組織)	脅威想定表(リスク評価結果・対策要件入り) (Appendix E-3 参照) ＜副産物＞ 資産管理表(詳細入り) 対策入りミスマスケース図 アタックツリー図 通信フロー図 最新の脆弱性情報
セキュリティゴール定義書 脅威想定表(リスク評価結果・対策要件入り) ＜副次資料＞ 対策入りミスマスケース図 アタックツリー図 通信フロー図 最新の脆弱性情報	実装フェーズ ・前準備(脆弱性情報、ツール、ソースコードレビュー等) ・対策実装内容と分担の確定 ・実装作業とテストの実施(単体、結合、総合) ・総合評価	設計・開発担当組織(運用担当組織、企画担当組織)(情報システム・セキュリティ組織)	脅威想定表(リスク評価結果・対策要件・対策結果・テスト結果・残留リスク入り) ・実装作業テスト計画書・報告書 ・最新の脆弱性情報 ・通信フロー図 ・資産管理表(詳細入り) セキュリティゴール定義書(妥当性評価追記) (Appendix E-2 参照) 【チェックポイント2】

(続き)

インプット	セキュリティ実施事項	実施組織 主体 (副)(支援・監査))	アウトプット
【チェックポイント3】 セキュリティゴール定義書 脅威想定表(リスク評価結果・対策要件・対策結果・テスト結果・残留リスク入り)(Appendix E-3 参照) 資産管理表 通信フロー図 最新の脆弱性情報	運用フェーズ ・運用実施体制の構築 ・運用実施項目の検討・手順書化 ・教育訓練の実施 ・残留リスクへの対策方針策定 ・運用業務の実施 (脆弱性情報把握、パッチ適用・監視、インシデント対応、リスク再評価)	運用担当組織 (開発担当組織、設計担当組織) (情報システム・セキュリティ組織、危機管理組織)	運用体制図 インシデント対応フロー 脆弱性対応フロー 緊急連絡網 各種業務手順書 教育訓練マニュアル 脅威想定表(リスク評価結果・対策要件・対策結果・テスト結果・残留リスク入り) 最新版 資産管理表 脆弱性管理文書
脅威想定表(リスク評価結果・対策要件・対策結果・テスト結果・残留リスク入り) 最新版 (Appendix E-3 参照) 資産管理表 最新の脆弱性情報	廃棄フェーズ ・機能無効化 ・関連情報削除	運用担当組織	廃棄記録(チェックリスト) 資産管理表(廃棄内容の反映)

注1. 機能設計が別組織で実施される場合は、その担当部門からのインプットとなる。

注2. 安全設計とセキュリティ検討とが別組織で実施される場合は、設計フェーズにおいて安全管理文書を担当部門から入手する。

3.5. リスク評価の考え方

セキュリティの検討が、通常のシステム開発とは異なる点として、要件≒脅威と考えると、その要件自体は目に見えるステークホルダではなく、目に見えない攻撃者という第3者が持っている点である。したがって、ステークホルダは、要件の仮説をたてて対策を設計・実装することが必要になり、このことはロボットにおいても同様である。本ガイドランでは、リスク評価を行うための脅威分析を2段階で実施することを提唱する。

コンセプトフェーズにおける被害分析・上位レベルのリスク評価では、まだ対象となるシステムの詳細設計が完了していない段階であり、網羅的な分析は難しい。採用する予定の製品やサービス

の仕様や、提供しようとしている機能から起こっては困る被害を類推し、それ防ぐためのコストなどの事業条件から目標、方針を立てる。本ガイドラインは、それを“セキュリティゴール”と呼んでいる。

設計フェーズでは、設計したシステムの詳細の内容から、攻撃による被害の可能性分析(攻撃分析)を実施し、安全性への影響も含めてリスクを総合評価し、対策の要件を確定するというアプローチである。

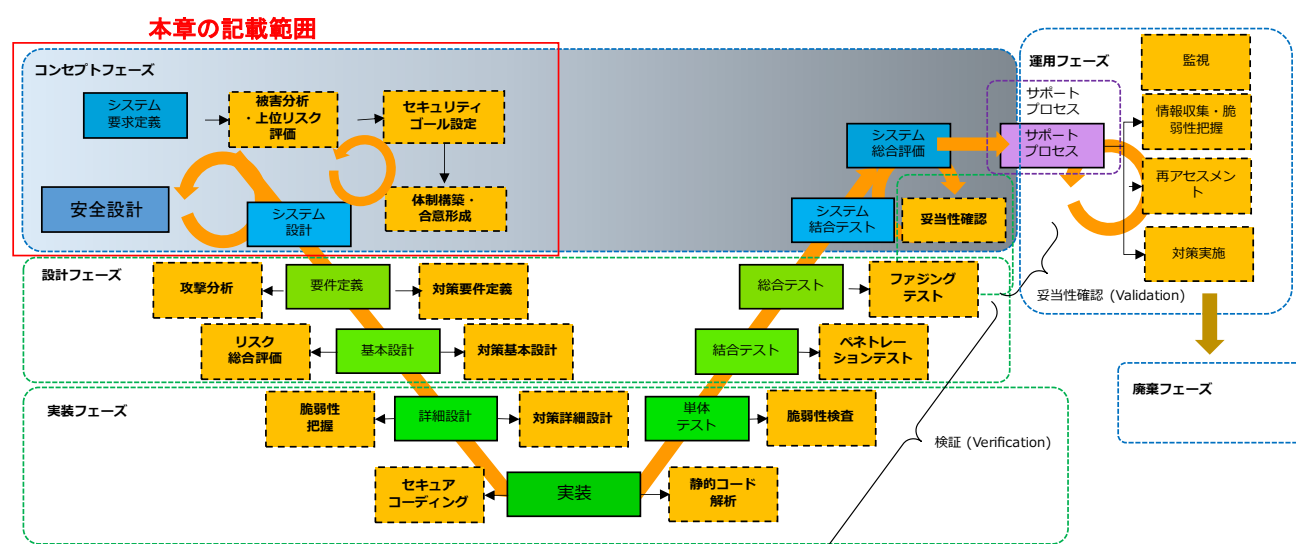
これにより、コンセプトフェーズ、設計フェーズで段階的に脅威分析を実施し、その結果を元にセーフティも含めたリスク評価を実施する方針としている。分析手法については一意には規定はせず、対象とするシステムの内容や時間・リソースなどの兼ね合いを考慮して最適化するという考え方をとり、実施例を参考として引用することとした。



図 3-5 リスク評価の考え方

4. コンセプトフェーズ

本章ではロボットシステムのライフサイクルのコンセプトフェーズにおけるセキュリティ検討項目について述べる。コンセプトフェーズはロボットシステムが実現するサービス・機能に関する要件を整理する段階であり、ロボットシステムのあるべき姿を検討する。このフェーズはロボットのハードウェアや各種のサーバなどの具体的なシステム構成が固まる前の段階であり、開発者が意図した機能をシステムが実現するために必要な機器やソフトウェアの構成を検討しながら、セキュリティに関する要件を並行して進めていくことになる。コンセプトフェーズにおけるセキュリティ要件は、システムとして何を保護すべきかというセキュリティゴールと、システムに対して外部から攻撃をされた場合に、どのような被害が発生するかを分析することが重要である。コンセプトフェーズでのセキュリティ要件検討結果に基づき、続く設計フェーズにおいて被害を最小限に食い止めるための対策の検討や、対策の効果を検証していくことになる。なお、システム実装後にコンセプトフェーズで設定したセキュリティゴールの達成度合いを関係者でレビューし、総合評価することもコンセプトフェーズの延長にあたるが、その内容については、第6章に記載する。



引用：ESPR (Embedded System development Process Reference) 2.0
システム開発プロセス（実線）にセキュリティ関連項目（破線）を追記

図 4-1 コンセプトフェーズの位置づけとセキュリティ検討項目

4.1. コンセプトフェーズ概要

4.1.1. コンセプトフェーズの目的とゴール

コンセプトフェーズにおけるセキュリティ検討の目的は、システムの利用目的や条件を踏まえてセキュリティのゴールを設定することである。

同じ機能を提供するロボットシステムであっても、使用される業務や環境、条件によって、セキュリティの可用性、完全性、機密性の要件は異なる。荷物の搬送機能を提供するシステムであっても、病院内で利用される場合、企業内で利用される場合と公共施設で利用される場合とでは要求される内容は異なる。コンセプトフェーズでは、対象のシステムの機能、ユースケース、資産を整理し、危惧される被害を分析して、保護すべき機能、資産の要素の視点からセキュリティのゴールを設定する。これによって、設計・実装フェーズにおいて被害を最小限に食い止めるための対策の検討や、対策の効果を検証していくことが可能になる。

作成されたセキュリティゴールの素案は関連する組織によって議論され、全社的なセキュリティポリシーとの整合性やビジネス的な事業性を判断しつつ、関連組織の合意が得られるまで修正・更新が繰り返される。最終的な承認を経たのち、開発するシステムが満たすべきセキュリティゴールとして関係者に認知される。以降の項で、セキュリティゴールの策定に関わる組織と、セキュリティゴールの策定プロセスについて説明する。

4.1.2. コンセプトフェーズの実施組織

コンセプトフェーズにおけるセキュリティ検討の実施組織は、企画担当組織(部門)が主体となる。ただし、企画の実現性も含めた検討も必要になるために、設計担当組織、開発担当組織とも連携し支援してもらう体制を構築するのが理想である。また、組織内の情報セキュリティ部門との連携も場合によっては必要になり、特にセキュリティゴールについては関連組織の合意形成が重要になる。

4.1.3. コンセプトフェーズの実施事項

コンセプトフェーズでの実施事項は、ユースケース・関連資産の整理、脅威による影響分析、セキュリティゴール(方針・目標)の設定である。コンセプトフェーズを開始するにあたり、事前準備として表3に示すインプットが必要である。検討対象となるロボットシステムの機能や用途、関係する資産についての情報は場合によっては担当する組織から事前入手が必要である。

コンセプトフェーズの作業によって得られるアウトプットはセキュリティゴールの定義書と、実施体制表である。セキュリティゴール定義書には、セキュリティゴールが対象とするシステムを構成する有形の物理資産、または無形の情報資産、システムの機能を説明するユースケース、潜在的な脅威とそれによってもたらされる被害分析、それぞれの脅威の評価と対応策が含まれる。セキュリティゴール体制表には、セキュリティゴールの策定に関わった各関連部門の合意を経て認可された、セキュリティゴール定義書に記載された内容の推進に関係する各関連部門の役割と業務内容が定義されている。

表 4-1 コンセプトフェーズの実施事項・インプット・アウトプット

インプット	セキュリティ実施事項	実施組織 主体(副)	アウトプット
・概要設計書 ・機能定義書 (注1)	<u>コンセプトフェーズ</u> ・機能理解 ・想定製品仕様調査 ・ユースケース整理 ・関連資産整理 ・被害分析・上位リスク評価 ミスユースケース等 ・セキュリティゴール策定 ・セキュリティ実施体制構築 ・安全分析(注2)	・主体:企画部門 ・副主体:開発部門、セキュリティ部門	・セキュリティゴール定義書(Appendix E-2 参照) ・セキュリティゴール実施体制表

注1. 機能設計が別組織で実施される場合は、その担当部門からのインプットとなる。

注2. 安全設計とセキュリティ検討とが別組織で実施される場合は、設計フェーズにおいて安全管理文書を担当部門から入手する。

またセキュリティゴールの内容については、実際に製品やサービスを設計・開発するときに関連するサプライヤ・ベンダとも合意をとる必要がある。ゴールを設定するにあたっての具体的な検討内容については次項で詳説するが、サプライヤやベンダから元となる製品を仕入れてサービスやシステムを構築する場合には、以下の点も考慮に入れる必要がある。

□ 使用を想定している製品の仕様の調査

-機能

-構成(ソフト、ハード、OSS 有無、扱うデータの種類)

-使用環境(物理環境、通信ネットワーク)

□ ユースケース図、通信フロー図概要、資産整理表への落とし込み

□ 利用する事業領域での法的な制約の確認(セキュリティ事故が法令に違反する可能性がないかの検討)

□ 想定顧客・事業領域に対して防がなければならない被害・影響の特定

-被害分析 安全性影響、プライバシー影響、事業影響

□ 上位レベルのリスク評価：

システムの詳細が確定してはいない段階ではあるが、事業的な視点でのリスクを評価する。

上記のようなポイントを踏まえて、関係組織と合意形成し、製品やサービスの設計・開発へとすすむためのチェックポイントを踏まえたセキュリティゴール策定のワークフローの例を図 4-2 に示す。

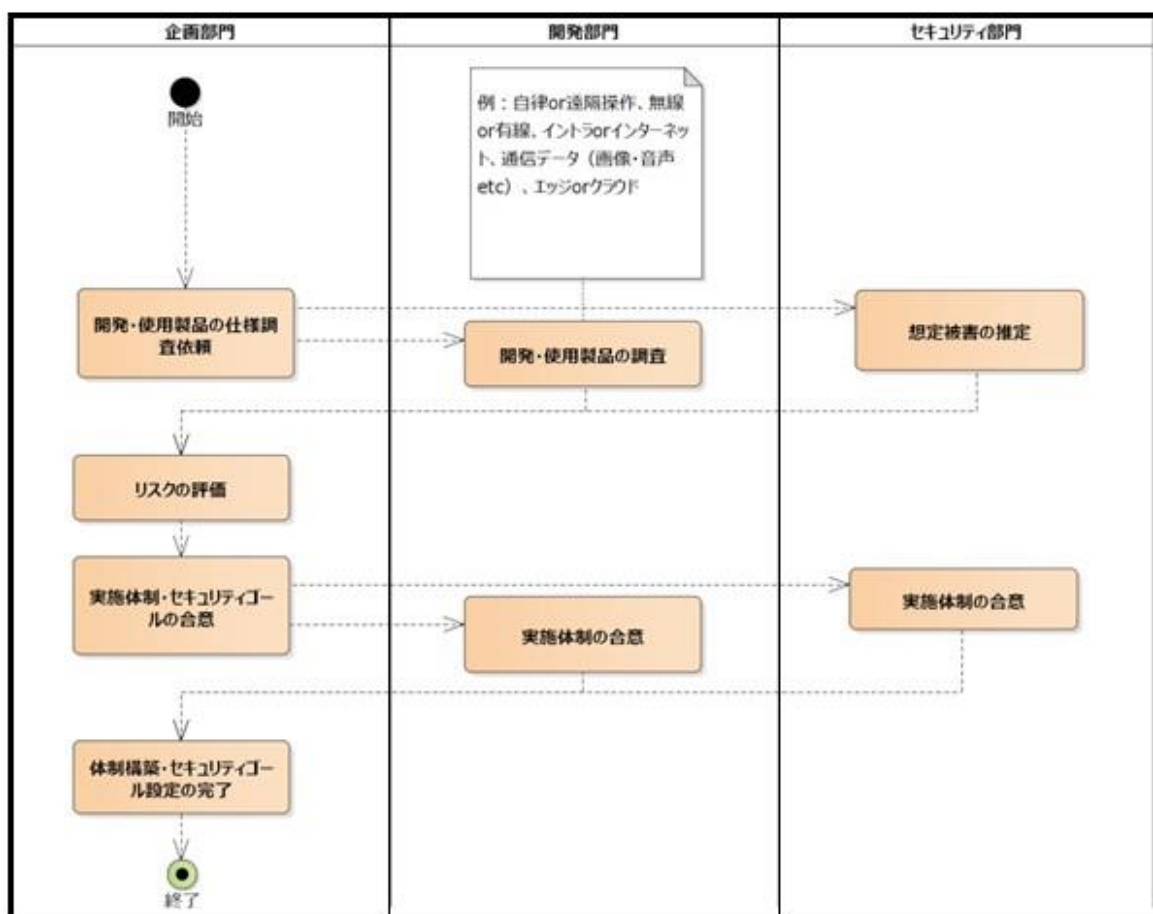


図 4-2 コンセプトフェーズにおける関連組織間のワークフロー例

4.2. 被害分析の前準備～資産・ユースケースの整理

ロボットシステムのセキュリティゴールを検討するにあたって、対象のシステムが提供する機能とそれを実現するための資産、ユースケースを整理する必要がある。

4.2.1. 資産の整理

資産はロボット自体を構成する制御装置、駆動装置などのハードウェアのみならず、ロボットシステムが取り扱う各種の情報からなる情報資産がある。表 4-2 は、保護対象資産を洗い出した例である。

表 4-2 資産整理(例)

資産分類	中項目	小項目	概要
物理資産	ロボット本体	ロボット機体	ロボットが内包する各種構成機器を支えるフレーム・筐体等
		ロボット制御 PC	ロボットの各種動作を制御するコンピュータ
		マニピュレータ	ロボットの各種操作を実現する機構
		移動機構	ロボットの移動機能を実現する機構
		カメラ	画像認識, 地図生成などに用いるカメラ
		マイク	音声認識に必要な音声入力機能を実現するデバイス
		スピーカ	ロボットの発話機能を実現するデバイス
		センサー類	ロボットが外界の情報を取得するために利用する種々のデバイス
	管理サーバ	CPU	ロボットシステムにおいて各種機能を実現するサーバの CPU
		内部記憶装置	サーバのプログラム類を格納するメモリ等
		外部記憶装置	サーバのプログラムやデータを格納するハードディスク, SSD 等
情報資産	ロボット制御 PC	カメラ画像	カメラから取得した画像
		音声データ	マイクから取得した音声データ
		自己位置推定センサ情報	自己位置推定のためのセンサデータ
		アプリケーション設定ファイル	各種アプリケーション用の設定ファイル
		アプリケーションログ	各種アプリケーションの動作ログ
		OS アカウント	OS ログイン用のアカウント
		アプリケーションアカウント	アプリケーション用のアカウント
		ファイアウォール設定情報	管理サーバのファイアウォール設定値
		サーバ IP	管理サーバの IP アドレス
		ロボット ID	ロボットを一意に特定する管理用識別子
	管理サーバ	ロボット基本情報	ロボットの機器構成などに関する基本的な情報
		ロボット状態情報	ロボットの動作状態に関する情報, 機体の状態や実行中のタスクなど
		カメラ画像	ロボットから送信された画像
		音声データ	ロボットから送信された音声データ
		アプリケーションデータ	各種アプリケーションが管理するデータ
		アプリケーションログ	各種アプリケーションの動作ログ
		OS アカウント	OS ログイン用のアカウント
		アプリケーションアカウント	アプリケーション用のアカウント
		顧客情報	ロボットシステムを利用する顧客の情報
		画像処理結果	ロボットから送信された画像を処理した結果データ
		音声認識結果	ロボットから送信された音声を処理した結果データ

4.2.2. ユースケースの整理

対象のシステムが提供する機能とそれを実現するためのユースケースもこのフェーズで可能であれば整理しておくことが望ましい。

表 4-3 は、スーパーの品出しロボットを例にしたユースケースの例である。
また、ユースケースを UML 形式のユースケース図として表すと、次項以降の脅威分析を実施する上で有効である。(図 4-3)

表 4-3 ユースケースの整理(例)

	分類	項番	アクター	ユースケース	通信内容
1	初期状態	-1	ロボット制御PC	カメラ画像、センサー(LiDR)情報を定期的に管理サーバへ送信する	ロボット制御PC→管理サーバ
2	基本操作	-1	店員、利用者タブレット	店員がロボットを呼び出す ①タブレットからの各ロボットの状態・位置を確認する ②対象のロボットを呼び出す	①位置・状態確認 利用者タブレット→管理サーバ ②呼び出し操作 ➢ ロボットタブレット→管理サーバ ➢ 管理サーバ→対象ロボット制御 PC
		-2	店員、ロボットタブレット	台車(陳列商品)を目的の通路へ移動させる	➢ ロボットタブレット→管理サーバ ➢ 管理サーバ→対象ロボット制御 PC 上記通信により、対象のロボットへ目標位置、経路情報が伝達される

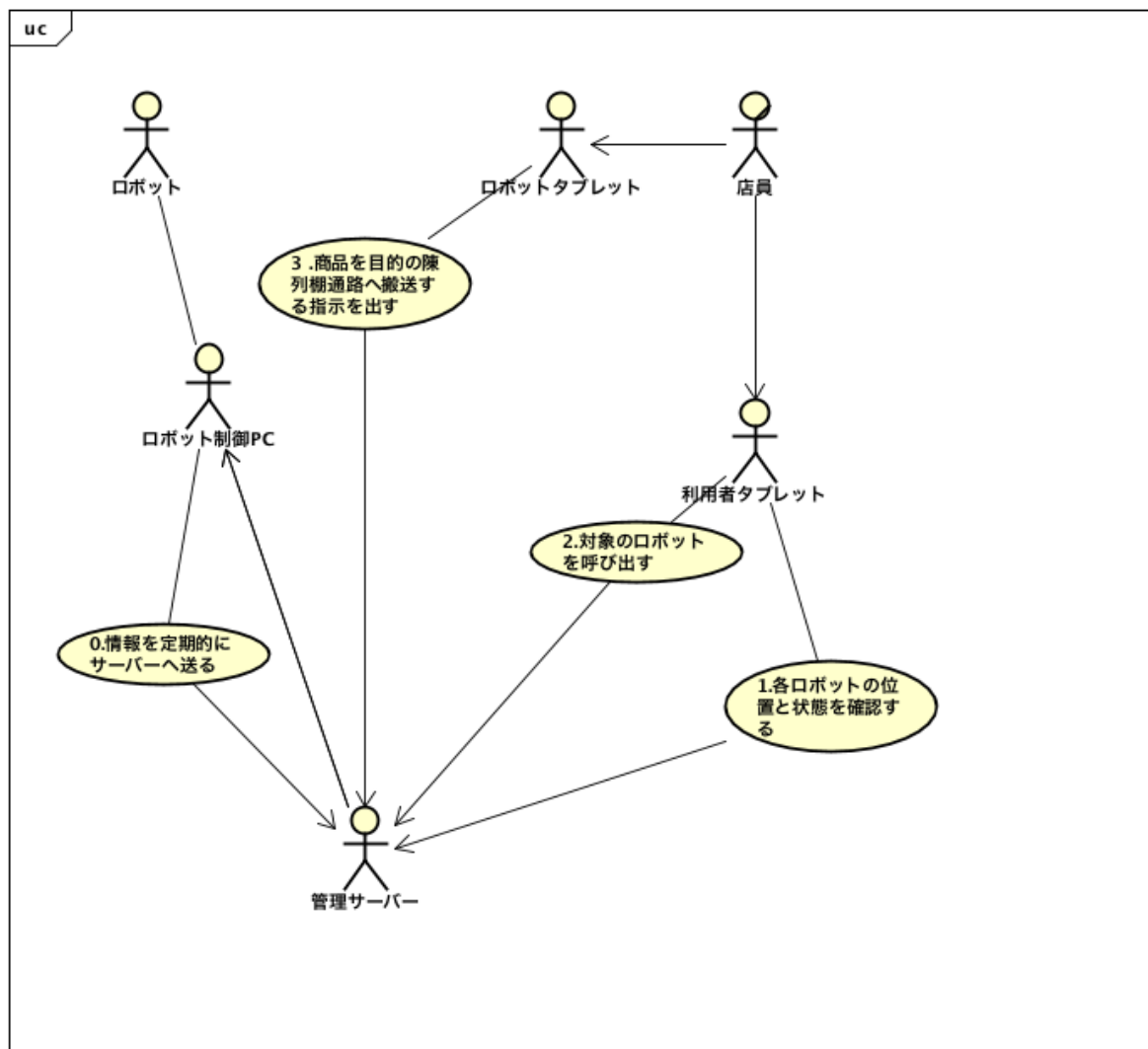


図 4-3 品出しロボット ユースケース図

4.3. 脅威の想定と被害分析

4.3.1. 脅威の想定

前項で洗い出し・整理を行った資産・ユースケースについて、危惧される脅威を想定しその影響を分析することが必要であるが、ガイドワードにより脅威を連想しやすくなる手法がいくつか提唱されている。本ガイドランでは、マイクロソフト社の脅威モデルの中で提唱されている STRIDE をベースにロボットの特徴を踏まえて(P)物理攻撃、最新のマルウェアへの脅威(M)を加えて整理する手法を提案する。各ガイドワードの内容については表 4-3 に示す。

表 4-4 脅威想定ガイドワード

	キーワード	解説
S	なりすまし	管理プラットフォームになりすまされ、ロボットに不正な命令が送信される
		各種センサーになりすまされ、偽のセンサー情報が送りこまれる
T	改竄	ロボットの制御プログラムが書き換えられ、ロボットが暴走させられる
		記録されているロボットのテレメトリや周辺画像が書き換えられ、事故発生時の証拠が消される
R	否認	ロボットに送信された命令を送ったのは自分ではないと否定され、ロボットが暴走した責任者がわからなくなる
		ロボットに記録された事故映像に対し、事後に書き換えられていると否定する
I	情報漏洩	ロボットの制御ユニットへログインできるアカウント情報が漏洩し、制御ユニットに不正アクセスされる
		管理プラットフォームを操作できるアカウント情報が漏洩し、ロボットに不正な命令が送信される
D	サービス拒否	管理プラットフォームがパケット過多でハングアップし、ロボットからのテレメトリが喪失する
		ロボットの制御ユニットがパケット過多でハングアップし、ロボットが暴走する
E	権限の昇格	ロボットの制御ユニットの特権が奪取され、制御ユニットに不正なプログラムが混入される
		管理プラットフォームの特権が奪取され、ロボットに不正な命令が送信される
P	物理的な攻撃	盗難、盗聴、物理的な破壊など物理手段による攻撃
M	マルウェア	不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコード

上記のガイドワードを元に、前項で例示したスーパーの品出しロボットの脅威を洗い出した例を表 4-5 に表示する。

表 4-5 想定脅威(例)

項番	分類	枝番	内容
1	なりすまし	-1	サーバになりすましてロボットへ偽の目標位置情報を送りつける
		-2	ロボットになりすまして、サーバへ偽の画像、位置情報を送りつける
		-3	ユーザになりすましてサーバへ侵入
		-4	ユーザになりすましてロボットへ侵入
2	改竄	-1	マップが改竄される
		-2	駐機情報が改竄される
		-3	ロボットの状態が改竄される
		-4	タスク情報が改竄される
		-5	カメラ画像が改竄される
3	情報漏洩	-1	カメラ画像が漏洩する
		-2	ロボットの状態・タスク情報が漏洩する
4	DOS 攻撃	-1	ロボット PC へ DOS 攻撃をかける
		-2	サーバへ DOS 攻撃をかける
5	権限昇格	-1	サーバへ侵入し、権限昇格する
		-2	ロボット PC へ侵入し、権限昇格する
6	物理攻撃	-1	タブレットを盗み出し、サーバに侵入し、不正操作を行う
		-2	ロボット、ロボット PC を盗み、細工する

また、洗い出した脅威を図 4-4 のようにユースケース図にミスユースケースとして書き出すと想定脅威をより視覚化することができる。ガイドワードとミスユースケース図を複合的に使用することによってシステムのアーキテクチャが定まる前の段階でも脅威を想定しやすくなる。

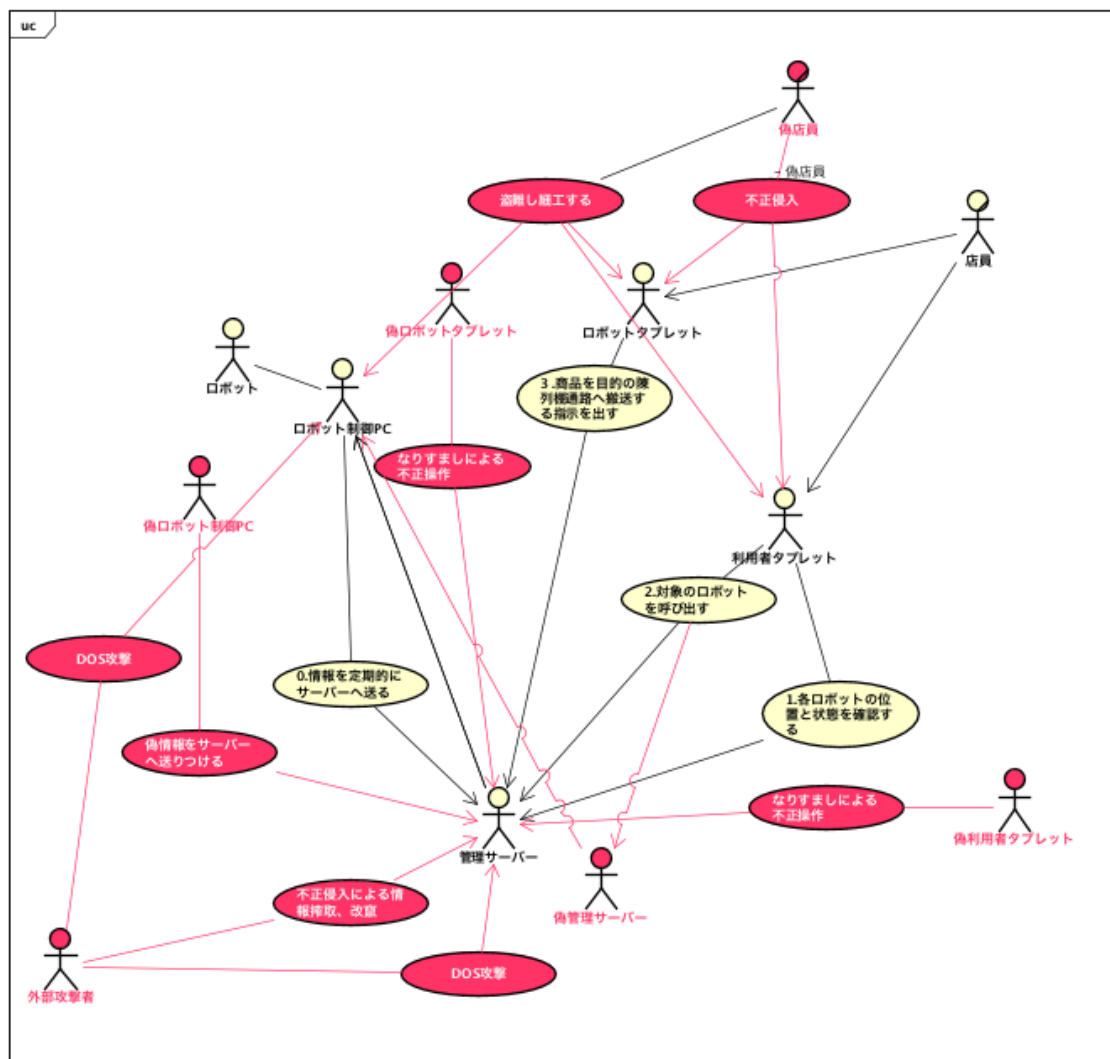


図 4-4 品出しロボット ミスユースケース図

4.3.2. 被害分析～上位レベルのリスク評価

セキュリティゴールを設定するには、機能、資産、ユースケースから想定される脅威についての影響を分析する必要がある。影響は、金銭面などへの事業的な影響も含めて定量化することが理想的であるが、本ガイドラインでは金銭面に換算する前段階での影響分析の例を紹介する。分析方法、フレームワークもプロジェクトの内容や規模、体制によって考慮するのが現実的である。ひとつの方法としては、想定脅威が関連する資産へ要求される機密性、完全性、可用性をスコアしその合算から影響を定量化する手法である。表 4-6 は搬送ロボットにおいて影響分析を実施した例である。

表 4-6 被害分析(例) 資産ベース

想定脅威	脅威に晒される情報資産		脅威に晒される物理資産		優先度	影響度
	資産	価値	資産	価値		
ロボットを不正に操作される	root アカウント	15	ロボット本体	10	A	1092
	実行アカウント	15	ロボット制御 PC	10		
	NTPd 等の常駐デーモン	9	Pixhawk	10		
	OS 設定	12	通信用 SIM	10		
	OS ログ	10	360 度カメラ	10		
	ROS ライブラリ	10	各種センサー	10		
	自律移動 ROS プログラム (cartographer)	10	荷物室本体	10		
	自作 ROS プログラム	10	制御用の Raspoberry Pi	10		
	Azure ServiceBus 接続 ID とパスワード	13	配達物	40		
	自律移動する目的地と経路	13	ロボットから荷物を受け取る人	50		
	センサーから得た生データ	9	ロボットの周辺を移動する人	50		
	推定した自己位置と姿勢	11	建造物等の私有財産	30		
	ロボット周辺の 360 度画像	13	ガードレール等の公有財産	30		
	Watermark を焼き込んだ 360 度画像	13				
	Watermark を焼き込んだ 360 度画像のハッシュ値	14				
	360 度画像のハッシュ値を計算する Salt	13				
	Azure BLOB Storage の接続キー	13				
ロボット制御 PC の管理者になりすまされ、ロボットの制御が乗っ取られる	ロボットが推定した自己位置と姿勢の履歴	13				
	360 度画像のハッシュ値の記録	13				
	Watermark を焼き込んだ 360 度画像の履歴	13				
	ロボットが推定した自己位置と姿勢の FIWARE 上の最新データ	12				

また、コンセプトフェーズの段階では厳密な構成が固まっておらず、詳細の指標化が難しい場合や分析にかけられるリソースが限られる場合も多い。その場合は、想定脅威から類推される影響を書き出し影響範囲を類推するなどの手法も可能である。表 4-7 は、スーパーの品出しロボットの想定脅威と影響を書き出した例である。

表 4-7 被害分析(例) ミスユースケースベース

項番	分類	枝番	内容	脅威による影響
1	なりすまし	-1	サーバになりすましてロボットへ偽の目標位置情報を送りつける	商品が目的の列に届かない ロボットが周辺環境の邪魔をする
		-2	ロボットになりすまして、サーバへ偽の画像、位置情報を送りつける	指示する内容が実態に合わなくなる 自己位置推定不能となり自律移動不可となる
		-3	ユーザになりすましてサーバへ侵入	各種情報の搾取・偽制御情報の送信
		-4	ユーザになりすましてロボットへ侵入	各種情報の搾取・偽制御情報の送信
2	改竄	-1	マップが改竄される	自己位置推定不能となり自律移動不可となる
		-2	駐車情報が改竄される	ロボットを呼び出せなくなる
		-3	ロボットの状態が改竄される	ロボットへ正常な動作指示が出せなくなる
		-4	タスク情報が改竄される	ロボットが目的位置まで正しい経路で移動できなくなる
		-5	カメラ画像が改竄される	ロボットへ正常な動作指示が出せなくなる
3	情報漏洩	-1	カメラ画像が漏洩する	来客者の顔などの個人情報が漏洩しプライバシーが侵害される
		-2	ロボットの状態・タスク情報が漏洩する	刻々と変化する値なので、漏洩自体の影響は少ない
4	DOS 攻撃	-1	ロボット PC へ DOS 攻撃をかける	正常な通信が不能になり、命令を受けられなくなる、あるいは遅延する
		-2	サーバへ DOS 攻撃をかける	ロボットの状態を認識できなくなる・指示を出せなくなる
5	権限昇格	-1	サーバへ侵入し権限昇格する	多種多様
		-2	ロボット PC へ侵入し権限昇格する	多種多様
6	物理攻撃	-1	タブレットを盗み出し、サーバに侵入し不正操作を行う	ロボットへの不正移動指令、停止などが可能になってしまう
		-2	ロボット、ロボット PC を盗難し、細工する	多種多様

4.4. セキュリティゴールの設定

前項までに整理した機能、資産、ユースケース、想定脅威、影響分析結果を元に、セキュリティゴールを設定する。「何を何から守るか?」「抽出した資産をどこまでどう守るか?」とともに機密性、完全性、可用性、更には安全性などの要素への考慮も必要である。ゴールの記載方法は、定式化されたものは存在しないが、大きな方針と、セキュリティ上の目標となる要件が優先順位とともに明示されていることが望ましい。末尾の APPENDIX E-2 に、セキュリティゴール定義書のサンプルを添付する。また、事例として、スーパーの品出しロボット、及び搬送ロボットの事例におけるセキュリティゴールの記載例を以下表 4-8、表 4-9 に示す。

表 4-8 セキュリティゴールの設定例1

目標
商品やフロア環境を壊さないことが最優先とする。 そのためにはロボットの機能が停止してもよい
基本方針
1. ロボットの自己位置推定のための情報の完全性を保つ （攻撃により自己位置を喪失あるいは誤認識しないようにする） 2. ロボットの制御情報が書き換えられ、誤動作することを防ぐ 3. ロボットが撮影する画像データが流出しないようにする （セキュリティ要素の優先順位） 完全性＞機密性＞可用性

表 4-9 セキュリティゴールの設定例2

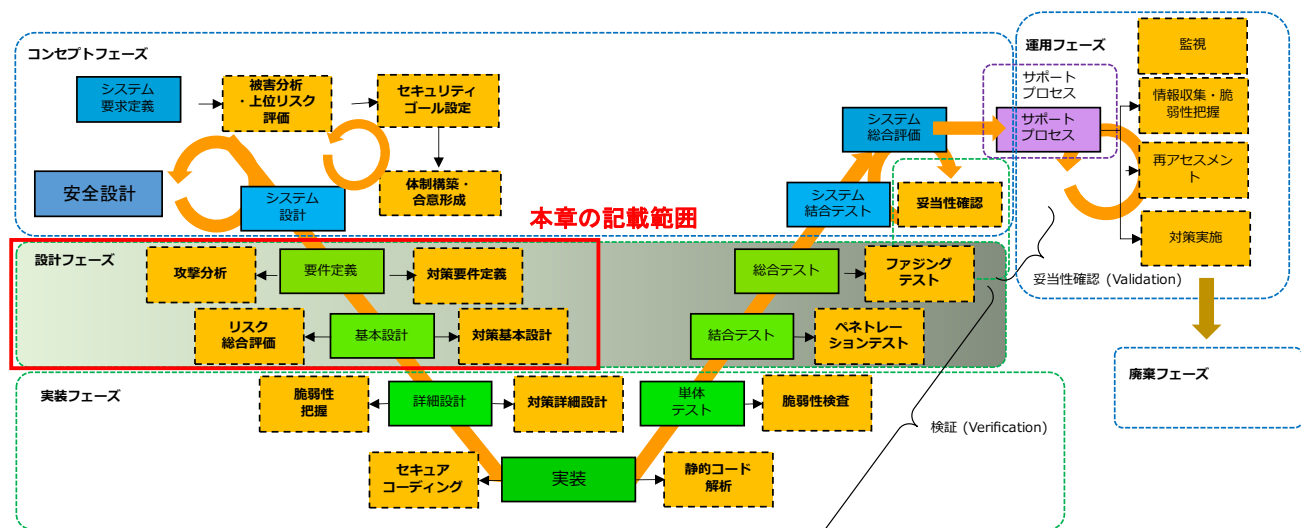
優先度	セキュリティ目標
A	周囲の人や財産への損害を防ぐ
A	配送物の盗難や損壊を防ぐ
A	ロボットの暴走を防ぐ
B	配達先の住所や電磁ロックのキー情報といった、個人に関する情報の流出を防ぐ
B	ロボット周辺の 360 度画像には人が撮影されている可能性があるため、その流出を防ぐ
B	ロボット周辺の 360 度画像の真正性を保証するため、その改竄を防ぐ
C	ロボット自体の盗難、損壊を防ぐ
C	ロボット自体のプログラム、及びロボット管理プラットフォームのプログラムの改竄を防ぐ
C	ロボットが自己位置を誤った位置として推定することを防ぐ
C	ロボットが誤った目的座標へ移動することを防ぐ

5. 設計フェーズ

本章では 4 章のコンセプトフェーズでの検討結果を受け、ロボットシステムのライフサイクルの設計フェーズにおけるセキュリティ検討項目について述べる。

5.1.1. 設計フェーズの目的とゴール

設計フェーズのゴールは、コンセプトフェーズで検討した守るべきセキュリティゴールと攻撃を受けてしまった場合の想定される被害分析の結果を踏まえ、ロボットシステム全体としてのセキュリティとセーフティを脅かす具体的な攻撃手段を可能な限り洗い出すこと、ロボットシステムに発生しうるリスクを定量的に評価して対策の優先順位を付けることである。また、ロボットシステム全体としての具体的なハードウェア・ソフトウェア及びネットワークアーキテクチャの設計にセキュリティ脅威への対策を踏まえたロボットシステムのあるべき姿を反映させることである。第4章で設定したゴールを達成するためのポリシーの細則がここで決まり、ポリシーの細則を関係者と共有する、必要な教育・訓練を実施することも重要な実施事項である。なお、システム実装作業後に設計内容が正しく反映されているかのテストの計画や結果のレビューも設計フェーズの延長と考えるべきであるが、その内容の詳細については、第6章にて記載する。



引用：ESPR (Embedded System development Process Reference) 2.0
システム開発プロセス（実線）にセキュリティ関連項目（破線）を追記

図 5-1 設計フェーズの位置づけとセキュリティ検討項目

5.1.2. 設計フェーズの実施組織

設計フェーズの実施組織は、設計・開発を担当する組織（部門）が主体となるが、企画担当組織もその内容のレビューなどで支援していくことが望ましい。

設計フェーズの最終段階である対策の要件定義のプロセスにおいては、対策の実現性の検討も含めて運用組織が支援していくことが望ましい。これにより設計フェーズに続く実装フェーズ・運用フェーズへの移行や内容の引継ぎが円滑になるはずである。

設計フェーズにおける関連組織がどう連携するかについて例として図示する。

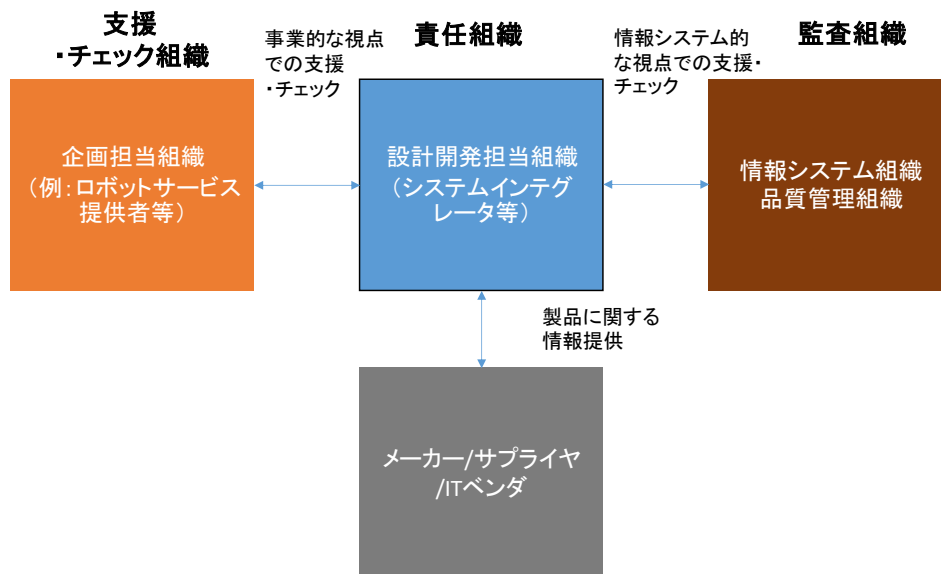


図 5-2 設計フェーズの実施体制図(例)

5.1.3. 設計フェーズの実施事項(概要)

設計フェーズでの実施事項は、攻撃分析、リスク評価、その結果を受けての対策方針の検討（要件定義）となるが、本ガイドランでは、特にリスク評価の中の安全性（セーフティ）への影響についてのポイントが非常に重要であるためひとつの項目として記載することとした。冒頭にも解説したとおり、ロボットでは、セキュリティとセーフティが相互に影響・関連するからである。

設計フェーズにおける実施事項の流れは以下の通りである。

- システム基本設計
- セキュリティ対策要件定義
 - ◇ 脅威分析準備
 - ◇ ユースケースの詳細整理
 - ◇ 通信フローの詳細整理
 - ◇ 資産の詳細整理
- 脅威分析(第2段目)の実施
 - ◇ 攻撃分析(ミスユースケース分析、資産のスコア化・脆弱性情報収集、アタックツリー)
 - ◇ 影響分析(詳細) 安全性への相互影響分析
- リスク総合評価
 - ◇ 可能性×影響×ポリシーで評価
- 対策の基本設計
 - ◇ 対策の優先順位付け(リスク総合評価を元に)
 - ◇ 対策手段の選択

設計フェーズを開始するにあたり、事前準備として表 5-1 に示すインプットが必要である。このうち、資産管理表、ユースケース図、ミスユースケース図、脅威想定表、セキュリティ方針記載書は、

4章のコンセプトフェーズで作成されたものを引き継ぐ形になるが、安全関連文書は、安全分析・設計を担当した組織(部門)から情報提供が必要である。

表 5-1 設計フェーズの実施事項・インプット・アウトプット

インプット	セキュリティ実施事項	実施組織 主体(副)	アウトプット
セキュリティゴール定義書 セキュリティ実施体制表 安全関連文書(注)	設計フェーズ ・ユースケース・資産詳細整理 ・関連脆弱性情報収集 ・攻撃分析 ・安全性への影響評価 ・リスク総合評価 ・対策方針策定・対策要件定義	設計・開発担当組織 (企画担当組織、運用担当組織)	脅威想定表(リスク評価結果・対策要件入り) (Appendix E-3 参照) ＜副産物＞ 資産管理表(詳細入り) 対策入りミスユースケース図 アタックツリー図 通信フロー図 最新の脆弱性情報

注. 安全設計とセキュリティ検討とが別組織で実施される場合は、設計フェーズにおいて安全管理文書を担当部門から入手する。

5.2. ユースケース・資産の詳細整理

コンセプトフェーズでは、ユースケース、資産の整理もそのロボットシステムで要求される機能を提供することにフォーカスしていた。設計フェーズでは、**実装・テスト**時に必要になるユースケースや資産、**運用・実用**段階で要求されるユースケースや資産についても改めて洗い出し整理する必要がある。たとえば、構築時だけに必要な通信(アプリケーションやミドルウェアの最新版のダウンロード、SSHによる設定追加など)を運用時に閉塞することを忘れたり、運用段階で必要になる通信(監視、ログ収集)から攻撃の起点が生まれる可能性もあるからである。また、資産を構成するミドルウェアや OS などの情報も資産管理表には付け加えておくべきである。これによって、それらに内在する既知の脆弱性を洗い出すことが必要になるからである。

表 5-2 詳細整理した資産管理表の例

装置	資産	詳細 (型式・OS 等)	可 用 性	機 密 性	完 全 性	価 値
ロボット制御 PC	root アカウント	Ubuntu 16.04	5	5	5	15
	実行アカウント	Ubuntu 16.04	5	5	5	15
	NTPd 等の常駐デーモン	Ubuntu 16.04	3	1	5	9
	改竄検知ツール	Ubuntu 16.04	5	5	5	15
	OS 設定	Ubuntu 16.04	4	3	5	12
	OS ログ	Ubuntu 16.04	1	4	5	10
	ROS ライブラリ	ROS Kinetic Kame プログラム	4	1	5	10
	自律移動 ROS プログラム (cartographer)	ROS Kinetic Kame プログラム	4	1	5	10
	Azure ServiceBus 接続 ID と パスワード	フラットファイル	3	5	5	13
	自律移動する目的地と経路	ROS Kinetic Kame メッセージ ※一時的	4	4	5	13
	センサーから得た生データ	ROS Kinetic Kame メッセージ ※一時的	2	3	4	9
	推定した自己位置と姿勢	ROS Kinetic Kame メッセージ ※一時的	3	4	4	11
	ロボット周辺の 360 度画像	ROS Kinetic Kame メッセージ ※一時的	4	5	4	13
	Wartermark を焼き込んだ 360 度画像	オンメモリのバイナリファイ ル ※一時的	4	5	4	13
	Wartermark を焼き込んだ 360 度画像のハッシュ値	オンメモリのバイナリ ※一時 的	4	5	5	14
	360 度画像のハッシュ値を計 算する Salt	フラットファイル	3	5	5	13
	Azure BLOB Storage の接続 キー	フラットファイル	3	5	5	13

5.3. 関連脆弱性情報の収集

ロボットシステムに採用する可能性のあるハードウェア・ソフトウェア・ネットワークアーキテクチャなどを列挙し、それぞれ CVE や CWE を参照に攻撃されうる脆弱性にはどのようなものがあるか、性能やコストのトレードオフを考えた場合に実施できるセキュリティ対策はどの程度のものかの概略を事前に把握しておくに進めやすい。

ただし新たな攻撃手段が日々発見され続けるセキュリティ界限においては、この攻撃分析も一度実施すれば終わりというものではない。攻撃手段に関する情報を日々収集し、自らのロボットシステムに対して今まで想定していなかった攻撃が成立しないか、定期的に見直す必要があることを心に留めておくの良いだろう。

表 5-3 脆弱性情報参照サイト

情報提供組織	情報提供サイト
JPCERT/CC (一般社団法人 JPCERT コーディネーションセンター)	脆弱性対策情報 https://www.jpcert.or.jp/vh/top.html
IPA/ISEC (独立行政法人情報処理推 進機構 セキュリティセンター)	脆弱性対策情報 https://www.ipa.go.jp/security/vuln/documents/index.html
JNSA (特定非営利活動法人日本ネ ットワークセキュリティ協会)	脆弱性ポータルサイト https://jvn.jp/ 脆弱性対策情報データベース https://jvndb.jvn.jp/index.html
NISC (内閣サイバーセキュリティセン ター)	脆弱性関連情報 https://www.nisc.go.jp/

5.4. 攻撃分析（可能性分析）

攻撃分析は、ユースケース、資産再整理、脆弱性情報の収集等の前準備を受けて、ロボットシステム全体としてどのような攻撃に晒される可能性があるかを可能な限り洗い出すことである。目的は、被害分析の結果と合わせて脅威に対するリスク評価を行い、そこから対策の優先順位や方向性を導き出すことである。下記は、攻撃の可能性を分析する場合に参照する関係式である。

攻撃の可能性＝攻撃の価値（攻撃者にとっての価値）／攻撃の難易度（コスト）

攻撃の難易度（コスト）＝攻撃の複雑さ × α（攻撃手法の成熟度など）

ATA（アタックツリー分析）などを利用

DFD（データフロー図）などを利用

ミスユースケース図などを利用

内在する既知の脆弱性（CVE）も考慮

5.4.1. 攻撃分析手法・フレームワークについて

攻撃の可能性を分析するには、ユースケースと攻撃パターンの分析、脅威の相互関係の分析などを複合的なフレームワークを用いて脅威とそれによる影響・リスクを可視化していくことが非常に重要になる。攻撃可能性の定量化には定まった方式は無いが、例えば攻撃可能性の多寡を相対的に見積もり、ロボットシステム内で一意な値を割り当てる方法や、攻撃を実行するために必要なコストを金額換算して定量化する方法などが用いられる。

本ガイドラインでは、コンセプトフェーズで例示したミスユースケース分析、資産整理の結果を元に、攻撃の起点を明確化するための通信フローの整理、脅威・攻撃の相互関係を明らかにするためのアタックツリー分析を複合的に用いることを推奨する。

5.4.2. 攻撃の起点の明確化と整理（通信フローの整理）

攻撃の可能性をはかるには、その攻撃の起点になりうる場所がネットワーク・システムのどこに存在するかを洗い出し整理することが重要になる。その際、ロボットシステムのハードウェア・ソフトウェアの特性やネットワーク構成など、具体的な設計仕様を念頭に置かねば、具体的な攻撃手段を見出すことができない。そのために、第4章で洗い出し整理したユースケースについて、「通信レベルでどういうやりとりが行われるか？」（プロトコル、やりとりされるデータの内容）について洗い出し整理することが必要になる。

攻撃手段を洗い出す上では、ロボットやその管理プラットフォーム等ロボットシステム全体の物理的な配置とデータの流れを図示化し、攻撃されやすそうな箇所にとどのような脅威が潜んでいるかを一つ一つチェックしていく手法がわかりやすい。

まずはロボットシステム全体をモデル化し、ロボットシステムを構成する物理的なコンポーネントの配置と、それらの間のデータの流れを図示化する。各コンポーネント間の物理的な境界面を通過するデータの流れる場合、その境界面との交差点が、脅威が潜むポイントになる。例えば管理プラットフォームと常時接続し、ロボットへの命令やロボットのテレメトリを送受信するロボットシステムの場合、その送受信するデータが攻撃対象になる。「ロボットが受信したその命令は、本当に信頼できる管理プラットフォームから送られたものなのか？」あるいは「管理プラットフォームが受信したそのテレメトリは、本当にロボットの実際の状態を反映しているのか？」が問われなければならない。

このモデル化は、多層的に検討しなければならない場合がある。例えば公道を走行する自律移動ロボットを想定した場合、悪意ある第三者が走行中のロボットを鹵獲し、ロボットに搭載されたセンサーと制御ユニットの間にデバイスを割り込ませて信号を改竄することも不可能ではない。あるいは制御ユニット自体をロボットから取り外し、ストレージを取り出して機密情報を盗難することも不可能ではない。このような攻撃手法も想定する場合、センサーと制御ユニット間の物理的な境界面、あるいは制御ユニット内部の境界面も脅威が潜むポイントになり得ることに注意が必要である。

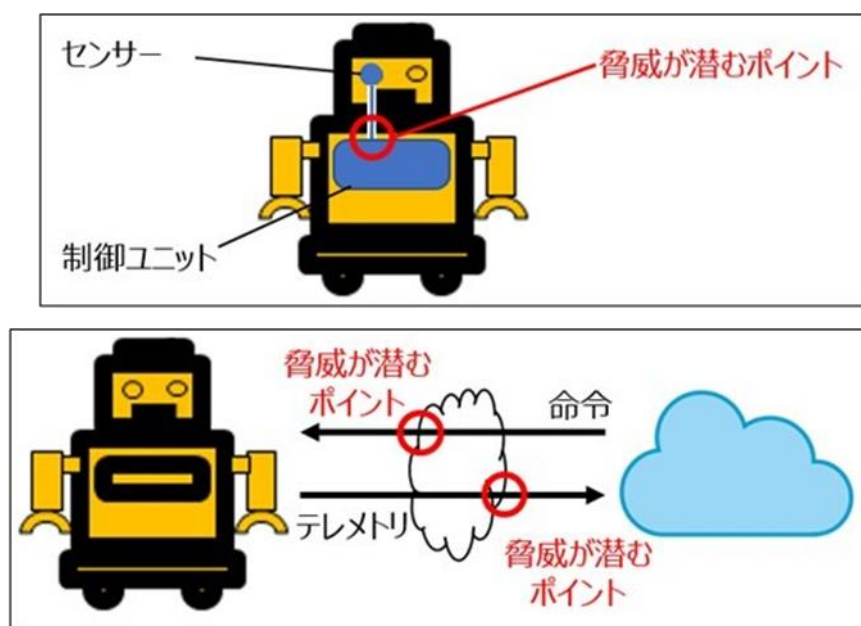


図 5-3 脅威が潜むポイント

なお図 5-3 のようなポンチ絵で脅威が潜むポイントを図示しても良いが、DFD(Data Flow Diagram)を用いて脅威を洗い出す手法も Microsoft から提案されている(図 5-4)。詳細は参考文献を参照のこと。

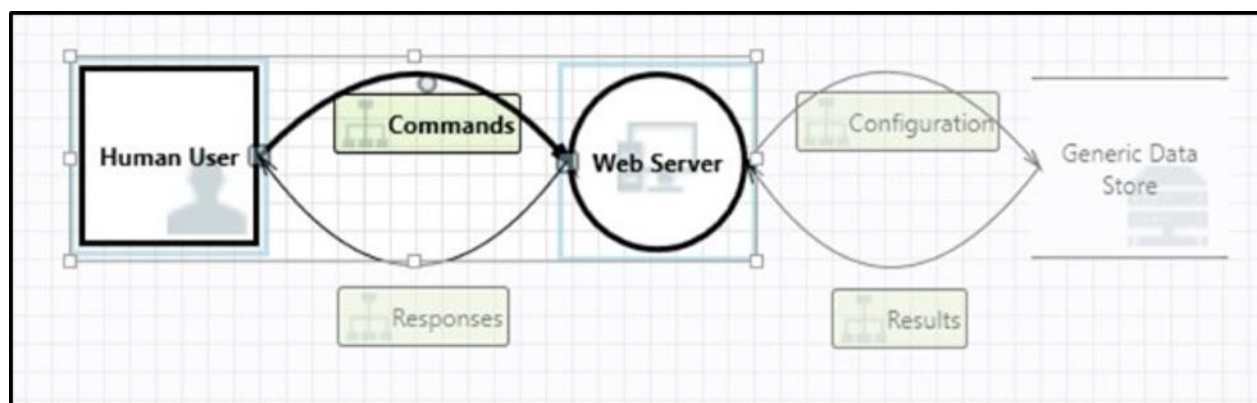


図 5-4 DFD(出典:マイクロソフト脅威モデル)

図 5-5 は前章でユースケースを例示したスーパーにおける品出しロボットの通信フローを模式図化したものである

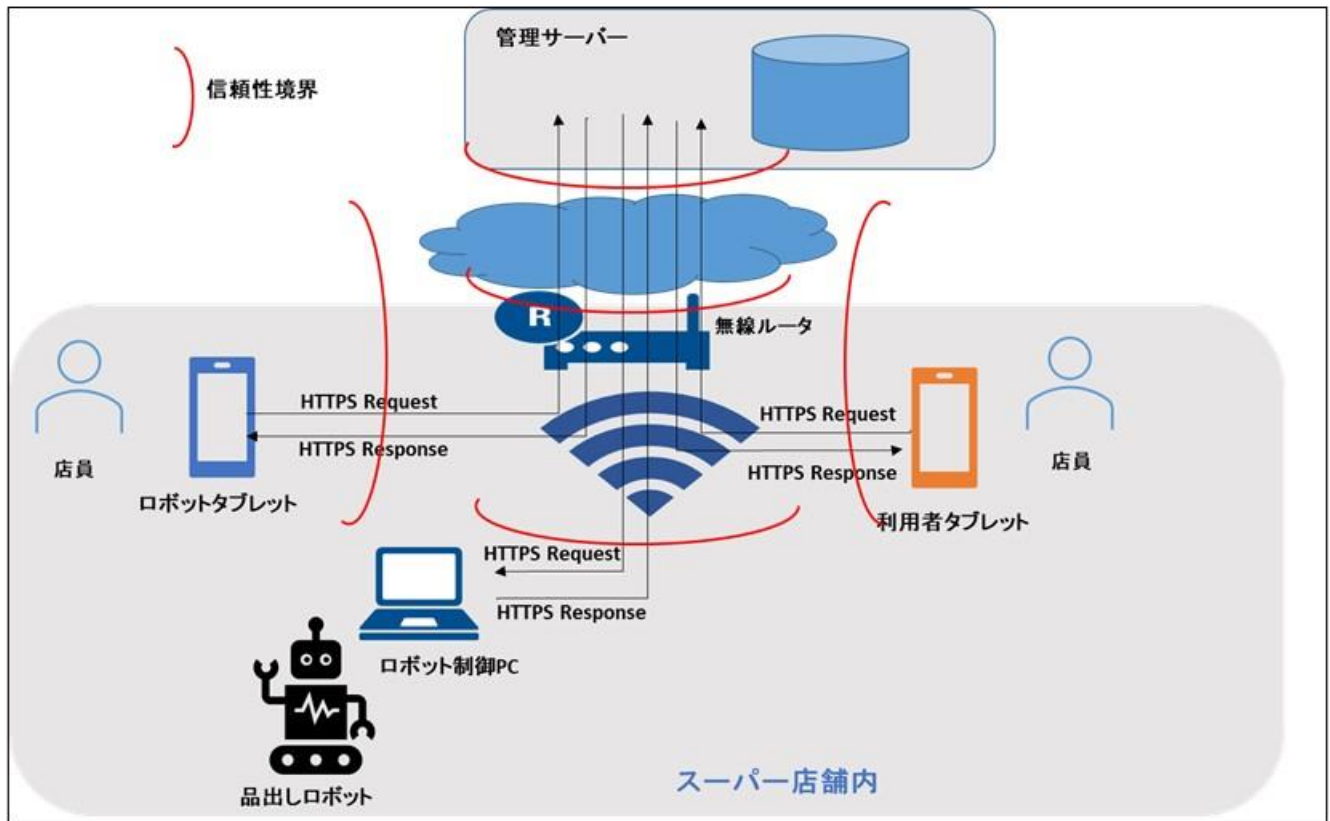


図 5-5 品出しロボット 通信フロー(例)

5.4.3. 脅威・攻撃の相互関係の分析

ロボットにおいては、ひとつの脅威が他の脅威にも影響を及ぼす場合がある。たとえば、なりすましによる不正なシステムの侵入により制御情報の改竄が発生し、その誤った制御情報を受信したロボットが誤動作を起こし、周囲の環境や人間などに危害が加えられるなどである。

アタックツリーは安全分析における分析手法 (Fault Tree Analysis) をセキュリティの分野に応用したものである。ロボットシステムへの攻撃やその発生条件を、より抽象度の高い手段からより詳細で具体的な手段に木構造で分解する。そして具体的で実行可能な末端ノード(葉)の攻撃手段に対して、攻撃はどの程度実行しやすいか(金銭・時間・専門知識・専用ツールの必要性等の総合的なコスト)を見積もる。アタックツリーを利用することで攻撃が実現する条件や攻撃される経路を可視化することができ、攻撃の可能性の検討を見通し良く実施することができる。

図 5-6 は、スーパーの品出しロボットにおける脅威の相互関係をアタックツリー図に落とし込んだものである。

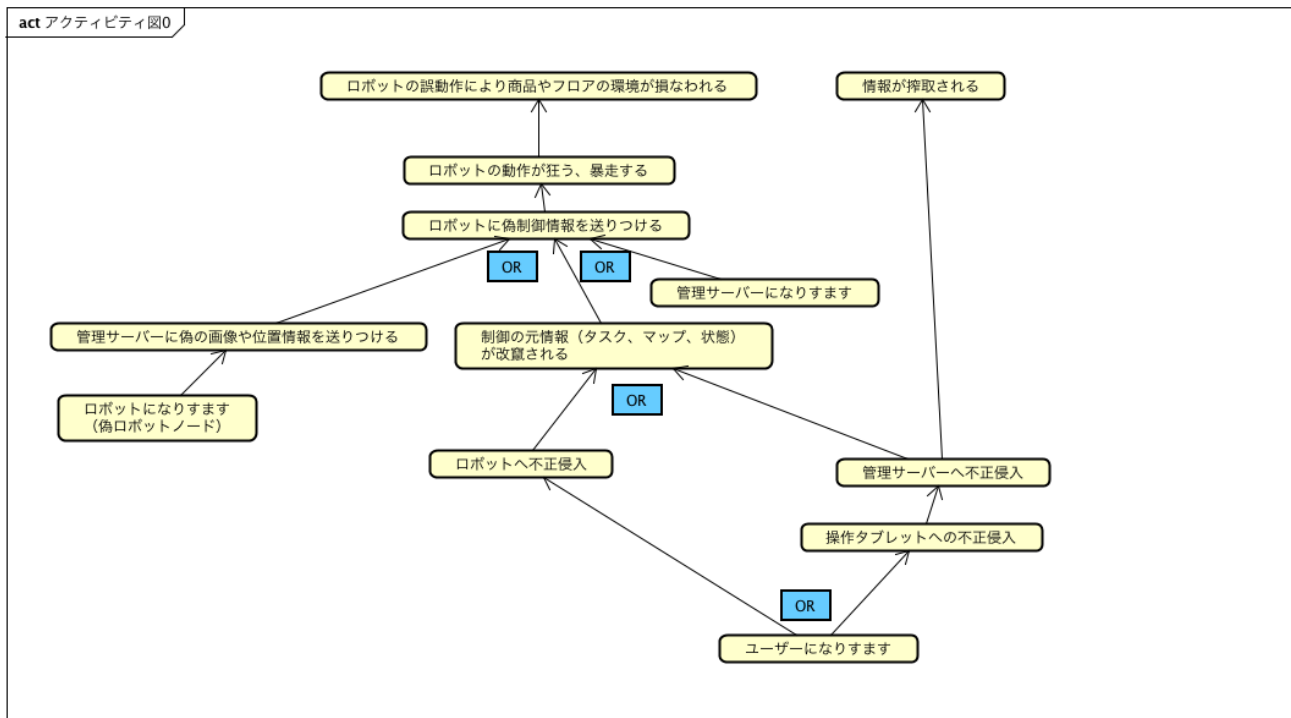


図 5-6 品出しロボット アタックツリー

5.5. 安全性リスク評価 (セキュリティ~セーフティの相互影響の評価)

5.5.1. 背景

ロボットは様々な機能を実現するために、それに応じた動力(エネルギー源)を有する。また、動作も機能実現のためにある程度の速度を有しており安全上のリスクが存在する。従来のロボットは産業用であれば固定され、周囲に柵を施すことにより、いわゆる隔離と停止の原則により安全を担保していた。

しかし、産業用ロボットにおいても人と作業空間を共有する人協働型ロボットやいわゆるサービスロボットといわれる人と接することでサービスを提供するロボットの出現など、ロボットが利活用される場面が増えれば増えるほど、隔離と停止の原則だけで安全を確保することが難しくなっている。

そのため、ロボットを利活用する場合には、どのような環境においてどのように使われるかについてユースケースを明確にしたうえでリスクアセスメントを実施することが要求されるようになっている。

そのなかで制御による安全の確保として機能安全が重要かつ自然なものとして考えられている。リスクアセスメントを実施するにあたっては ISO12100 などの国際規格に準拠することが要求され、リスクアセスメントの妥当性やその結果導出された安全メカニズムについて機能安全規格である ISO13849-1 や IEC62061 への準拠が求められる。

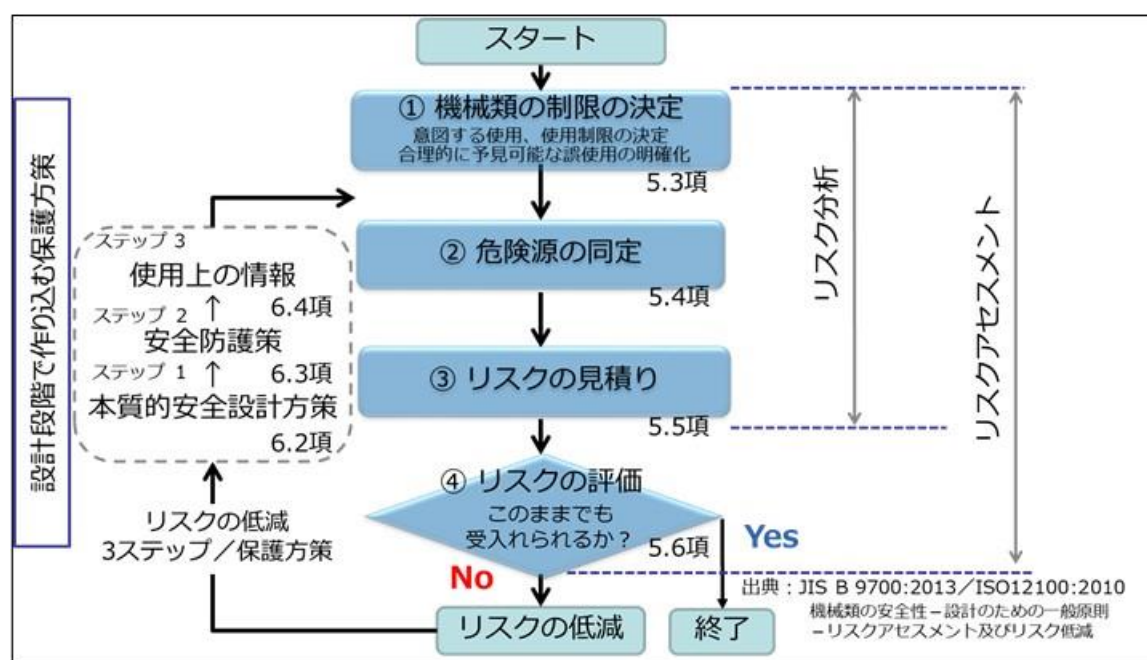


図 5-7 安全性リスクアセスメントの流れ

機能安全 (IEC61508) は 2000 年初頭より高い安全性が要求される化学プラントなど、ひとたび問題が発生し大事故につながると多くの人命の損失に繋がるような設備の制御にかかる安全の確保として登場したが、現在では自動車 (ISO26262) など多くの分野において安全に関する基本的な考え方となっている。

5.5.2. 安全性(セーフティ)とセキュリティ

近年、IoTといわれるネットワークを介して様々なデバイスが接続され連携されている状況が加速している。ロボットにおいてもこの状況は同様である。ネットワークを介して接続されるということは、ネットワークを通じて他の機器とコミュニケーションがとれるということであり、単体のロボットでは実現が難しかったロボットや他の機器との連携による複雑なサービスの提供など、我々の生活をより充実したものとする可能性が広がる。一方で、つながることによるセキュリティ上の問題が発生する可能性も潜在的に有することとなる。つまり、ネットワークを介してロボットに不正にアクセスし、その正しい制御を不能とさせ、起こってはいけない挙動をロボットに対して実行することによる危険性が生じる可能性がある。このことから、ロボットにおけるセキュリティは重要な課題であり、今後は連携が進み、より高度なサービスを複数のロボットや他の機器との連携により実現するであろう近い将来に先んじてロボットにおけるセキュリティ対策を考えていく必要がある。

前述したように、従来の産業用ロボットは固定され、機械的な連携は他の機器とは存在して生産ラインなどの一部として稼働してきたが、今後は機械的な連携に留まらず、データの上での連携などいわゆる製造業におけるデジタルトランスフォーメーション(DX)への対応からもセキュリティ対策が注目されるようになっている。

5.5.3. 安全性(セーフティ)を踏まえたセキュリティリスク評価(セキュリティを踏まえた安全性評価)

セーフティとセキュリティの相互影響を分析・評価する手法は、セーフティを検討してからセキュリティとの相互影響を検討する、セーフティとセキュリティを並行して検討するなどいくつかの手法がロボットに限らず提唱されている。詳細については、Appendix A-2を参照されたい。

本ガイドラインでは、安全分析による安全設計が終了していることを前提にセキュリティとの相互影響を分析・評価する手法を推奨する。事前準備として、安全設計内容を入手し担当組織にその経緯を確認する。その上で、次の3つの視点での検討を行う必要がある。

- ・1. 安全機能への攻撃によるセキュリティリスクとその対策

- ・2. セキュリティリスクの受容がセーフティを損なわないか？
- ・3. セキュリティリスクへの対策によってセーフティが損なわれないか？

その検討の流れをまとめたものを図 5-8 に示す。

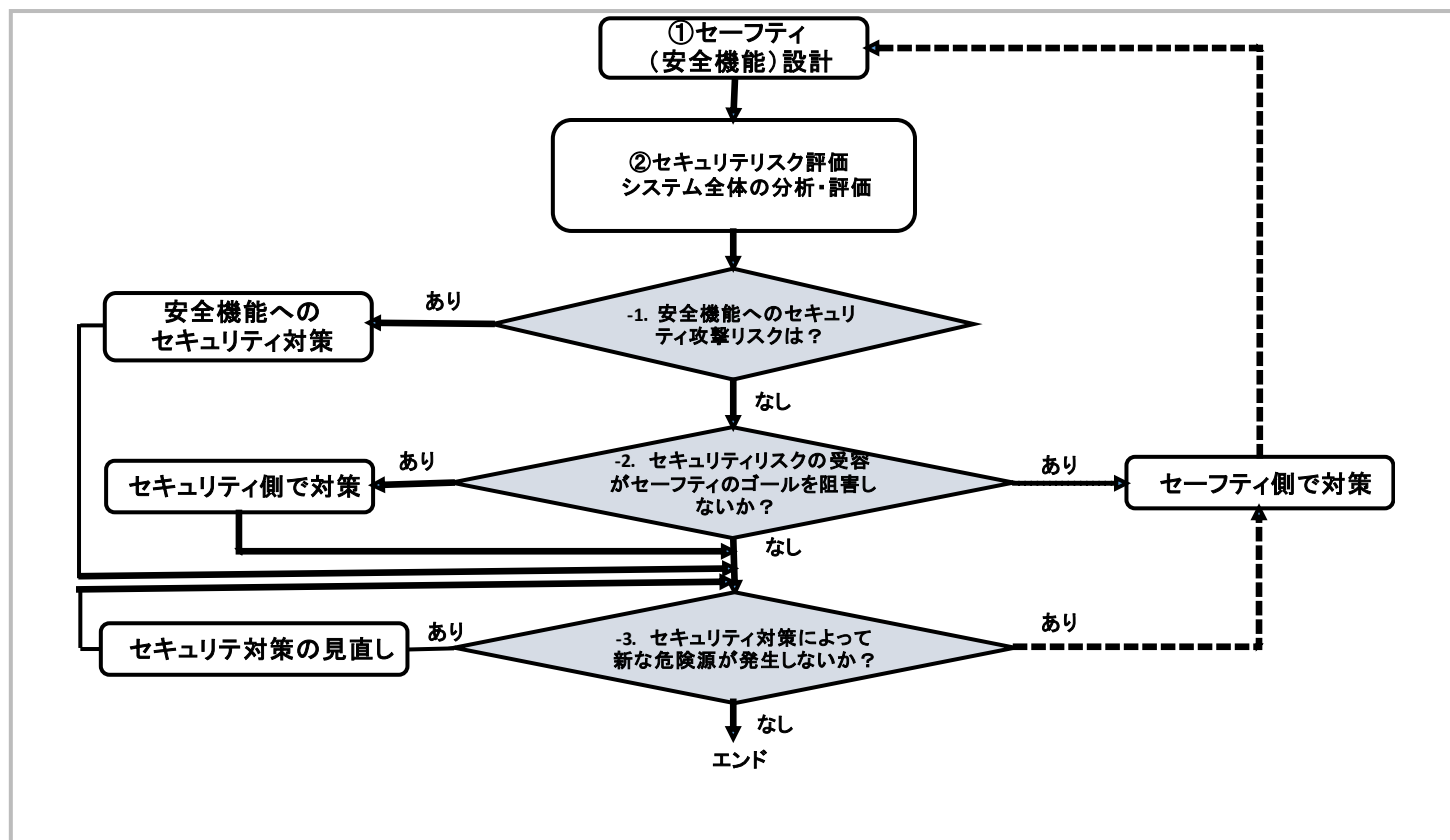


図 5-8 安全設計とセキュリティ検討の流れ

それぞれの実施項目の内容と関連する規格を整理したものを表 5-4 に示す。

表 5-4 安全設計とセキュリティ検討のポイント整理

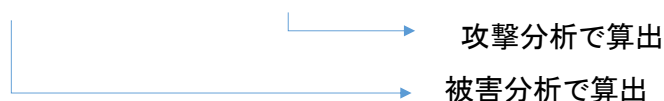
	検討ポイント	内容・目的	関連規格	検討の流れ	例
1	Security for Safety(安全機能に対するセキュリティ)	・安全機能に対するセキュリティ(攻撃)リスク評価と対策の検討	IEC63074、D0326、等 ※セキュリティ対策が新たな危険源を生み出さないことが前提	①安全機能の設計 ②安全機能へのセキュリティリスク評価 ③安全機能へのセキュリティ対策	衝突検知機構を構成する資産への攻撃
2	Safety with Security RISK	・セキュリティのリスクを受容した上でもセーフティは維持されるかの検討	IEC63069	①安全機能の設計 ②システム全体のセキュリティリスク評価 ③セキュリティリスクを受容した場合のセーフティへの影響検証 ④影響あれば、セキュリティ or セーフティのいずれかで対策	DDOS 攻撃により把持している製品を把持できなくなり、製品が落下する
3	Security Countermeasure and Safety	・セキュリティ対策をしても安全性を阻害しないか？	IEC63069	①安全機能の設計 ②システム全体のリスク評価と対策 ③セキュリティ対策によるセーフティへの影響 ④影響あれば、対応を検討	盗難防止用の外箱を付けたら、非常停止ができなくなってしまった。

5.6. リスク総合評価

ロボットのセキュリティにおいても従来のサイバーセキュリティと同様にすべての脅威に対策を施しリスクをゼロにすることは不可能である。しかし、網羅的に脅威を洗い出し、そのリスクを可視化することにより優先順位をつけて対策を打つことができる。

セキュリティリスクの大小は、(攻撃による影響) × (攻撃の可能性) によって表される。

$$\bullet \text{ リスク} = (\text{攻撃による影響}) \times (\text{攻撃の可能性})$$



これまでに取り上げた個々の脅威について攻撃の可能性と被害の大きさ、特に安全性への影響の有無なども含めて定量的に評価する形が望ましい。プロジェクト毎に指標となるスコアを準備して分析する場合、プロジェクトで扱うシステムの規模や複雑さ、分析にかけられるコストや体制なども考慮して最適な方法を選ぶことになる。

ただし、厳密な定量評価をするにはその前提となる要素の検討に多くの時間と労力が必要であり、現実的には難しい場合は、コンセプトフェーズで策定したセキュリティゴール・方針からリスクの大中小などの目安をつけて優先順位を確定する場合もある。

本ガイドラインでは、スコア化して優先順位を決定する例(表 5-5)と、相対的な高中低レベルの評価をつける例(表 5-6)とを参考例として例示する。(注)

(注)従来のサイバーセキュリティでは、リスクを CVSS(Common Vulnerability Scoring System)という指標で表現する手法なども活用されているが、ロボットシステムにおいては、物理的な環境要素、安全性(セーフティ)への影響度合などの変動要素も考慮する必要があるため、CVSS のリスク計算式はそのままではあてはまらない部分が多い。国際的には、ロボットシステムの特性を踏まえたセキュリティリスクの指標化手段として、RVSS(Robot Vulnerability Scoring System)を提唱する動きもあるが、現時点では、手法的に成熟しているとはいえず、本ガイドラインでは、案件、

プロジェクト毎にリスクの指標は最適化するというアプローチで事例を示すというアプローチをとっている。

表 5-5 リスク総合評価(例) 1

項番	枝番	脅威事象	リスク評価		
			影響度	攻撃可能性	評価値
1	-1	ロボット制御 PC の管理者になりすまされ、ロボットの制御が乗っ取られる	1092	50%	546
	-2	ロボット管理プラットフォームになりすまされ、ロボットの制御が乗っ取られる	714	50%	357
	-3	Pixhawk に偽のロボット制御 PC が接続され、ロボットの制御が乗っ取られる	664	50%	332
2	-1	各種センサーやカメラになりすまされ、偽のセンサー情報や周辺画像が送られる	506	10%	51
3	-1	荷物室の制御 RaspberryPi の管理者になりすまされ、配達物を持ち去られる	210	90%	189
	-2	配達物の受取人になりすまされ、配達物を持ち去られる	210	90%	189
4	-1	Azure の管理者になりすまされ、ロボット管理プラットフォームが乗っ取られる	1158	50%	579
5	-1	ロボットになりすまされ、誤ったロボットの状態を送り付けられる	75	60%	45
	-2	ロボットになりすまされ、誤った周辺画像を送り付けられる	38	60%	23
6	-1	ロボット制御 PC の ROS プログラムやデバイスドライバが改竄される	1000	40%	400
	-2	Pixhaws の ArduPilot プログラムやデバイスドライバが改竄される	642	30%	193

表 5-6 リスク総合評価(例)2

項番	分類	枝番	内容	脅威による被害	被害評価	可能性	可能性評価	リスク値
1	なりすまし	-1	ユーザになりすまして利用者タブレットへ侵入	・複数ロボットの位置状態情報の閲覧 ・複数ロボットの不正な呼び出し	高	ID/パスを破れれば比較的容易	高	超高
		2	ユーザになりすましてロボットタブレットへ侵入	・複数ロボットの不正な移動・動作	高	ID/パスを破れれば比較的容易	高	超高
		-3	タブレットになりすまして管理サーバと通信	・複数ロボットの状態確認・不正な操作	高	サーバ・タブレット間の認証情報が盗み出せば可能	中	高
		-4	管理サーバになりすましてロボット制御PCと通信	・複数ロボットの不正制御	高	同じ内容のサーバを構築することは困難	低	低
		-5	ロボット制御PCになりすまして管理サーバと通信	・不正な情報(状態・画像)の送信	中	同じ内容の制御PCを構築することは今年	低	低
		-6	ユーザになりすまして管理サーバへ侵入	・各種情報の搾取 ・不正な制御	高	ID/パスを破れれば比較的容易	高	高
		-7	ユーザになりすまして制御PCへ侵入	・制御不能 ・不正制御・情報破壊・搾取	高	ID/パスを破れれば比較的容易	高	高
2	改竄	-1	マップが改竄される	自己位置推定不能となり自律移動不可となる	高	直接的には困難。間接的にはセンサー、カメラ等のいたずらで可能	低	低
		-2	駐機情報が改竄される	ロボットを呼び出せなくなる	低		低	低
		-3	ロボットの状態が改竄される		低	リアルタイムに変わる情報なので改竄は困難	低	低
		-4	タスク情報が改竄される	ロボットが目的位置まで正しい経路で移動できなくなる	中	リアルタイムに変わる情報なので改竄は困難	低	低
		-5	カメラ画像・センサー情報が改竄される	位置情報・衝突検知に影響	中	物理的にいたずらすれば比較的容易	中	中

5.7. 対策基本設計

5.7.1. 対策の優先順位付け

リスク総合評価の結果を受けて具体的な対策の内容を検討する。どこまでを対策し、どこまでを容認するかをプロジェクト毎に検討する必要がある。リスクが高いもの、特にセーフティへの影響が考えられる脅威の対策は最優先となる。対策を検討するにあたって考慮しなければならない点として以下があげられる

- ・リスク評価結果を元にした対策要否の判断、優先順位付け
- ・対策の有効性と実装のためのコスト(実装後のテスト、運用も含めて考慮が必要)
- ・対策の実装が生み出す副作用や新たなリスク
- ・対策による残留リスク

以下の例(表 5-8)では、セーフティへの影響する可能性がある脅威を最優先として対策を検討している。リスクが低いものに関しては、そのリスクを容認することによって、「コンセプトフェーズで設定したセキュリティゴールが損なわれないか？」をベースに対策の要否を判断することになる。

表 5-7 対策要件定義(例)

分類	枝番	内容	脅威による被害	被害度	可能性	リスク値	対策の方向性
なりすまし	-1	ユーザになりすまして利用者タブレットへ侵入	・複数ロボットの位置状態情報の閲覧 ・複数ロボットの不正な呼び出し	高	高	超高	0. 無線 LAN (Wifi) の認証強化 1. タブレットの認証・認可の強化 ・ID/パスだけではなく、顔認証、指紋認証などを加える ・管理者と閲覧のみの権限で ID を分ける
	2	ユーザになりすましてロボットタブレットへ侵入	・複数ロボットの不正な移動・動作	高	高	超高	
	-3	タブレットになりすまして管理サーバと通信	・複数ロボットの状態確認・不正な操作	高	中	高	2. タブレット～管理サーバ間の認証・暗号化

分類	枝番	内容	脅威による被害	被害度	可能性	リスク値	対策の方向性
なりすまし (続き)	-4	ユーザになりすまして管理サーバへ侵入	・各種情報の搾取 ・不正な制御	高	高	高	3. 管理サーバへのユーザ認証・認可の強化
	-5	ユーザになりすまして制御 PC へ侵入	・制御不能 ・不正制御、・情報破壊・搾取	高	高	高	4. 制御 PC への認証・認可の強化
DOS 攻撃	-1	サーバへ DOS 攻撃をかける	ロボットへ命令を出せなくなる可能性	中	低	中	境界でのアクセス制御 (サーバ→制御 PC の通信のみ許可)
	-2	ロボット制御 PC へ DOS 攻撃をかける	ロボットへ命令を出せなくなる可能性	中	低	中	
情報漏洩・搾取	-1	カメラ画像が漏洩する	来客者の顔などの個人情報の漏洩やプライバシーの侵害	高	低	中	・管理サーバ側のアクセス制限 ・管理サーバにおける暗号化・ハッシュ値の保存
	-2	ロボットの状態・タスク情報が漏洩する	リアルタイムに変化する情報なので影響は小さい	低	低	低	
物理攻撃	-1	タブレットを盗み出し、サーバと通信し不正操作を行う	ロボットへの不正操作・制御	高	高	超高	1. タブレットの認証・認可の強化(緩和) 2. タブレット～管理サーバ間の認証・暗号化 5. ロボットタブレットは、鎖などで持ち運びできなくする
	-2	ロボット制御 PC を盗難し、細工する	ロボット制御の機能不全	高	中	高	6. 盗難防止用センサーをつける 7. 制御用 PC は鎖などでロボットへつなぐ

5.7.2. 対策の選択

前節で検討した想定脅威に対する対策の優先順位にもとづいて、適切な対策方法を選択する必要がある。ただし、技術的な面では有効であるが、コストや対応する人員などの関係から実装が難しい、実装できても運用・維持する体制がないなどの事情も考えられる。その場合は、前節の対策

の優先順位だけに立ち戻り、対策は見合わせ残留リスクは受容することなども考慮する必要がある。

代表的な攻撃手法とその影響、対策のキーポイントについて表 5-8に示す。

表 5-8 代表的な攻撃手法と対策のキーポイント

攻撃手法の分類	特徴と影響範囲	対策技術	キーポイント
不正侵入	侵入によって機密性、可用性、完全性に加えて安全性へも影響の可能性もある	認証・認可、権限管理 アクセス制御、アクセスログの監視 不要インターフェースの閉塞	多要素認証 ID・パスワードの複雑化 接続制限
なりすまし(ユーザ)	ロボットの場合、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。	認証・認可(ユーザレベル) 権限管理 行動記録の監視 しきい値の管理	設定情報の管理
なりすまし(デバイス)		認証(機器レベル)	機器の識別方法
改竄	制御に関わる情報が改竄されると、データの完全性の阻害にとどまらず、ロボット自体の動作やサービスへ影響を与える可能性がある	ハッシュ関数を用いたメッセージ認証、デジタル署名 システム権限管理 ストレージの暗号化・ハッシュ値の保存 セキュアブート・セキュアアップデート	暗号鍵、証明書の管理
情報漏洩	ロボットが扱う製品など営業上の機密情報、写真などの個人プライバシーに関わる情報の性質・漏洩による影響を考慮する必要がある	認証・認可 暗号化 セキュアコーディング	暗号鍵、証明書の管理
DOS 攻撃	攻撃による負荷増大がロボットのリアルタイムな動作へ影響する可能性	アクセス制御、境界制御	影響を受けにくい内部構造のデザイン
マルウェア	システム上の各部位で混入の可能性があり、影響範囲が特定しづらい	マルウェア対策ソフト、脆弱性検査の定期的な実施、最新パッチ適用等のアップデート	
物理攻撃	盗難、物理侵入、盗聴など、影響は多岐に及ぶ可能性あり	・物理インターフェースの無効化・閉塞 ・セキュリティワイア、ICカードによるロックなどの盗難対策 ・入退室管理	監視、検知、不要情報の削除

【代表的脅威と対策選択のポイントの解説】

➤ 不正侵入

不正侵入とは、許可されていない外部のユーザがシステム内に侵入し、不正な操作をすること全般を指す。従来のサイバーシステムでは、ネットワーク上の境界点やインターフェースが侵入のポイントになりうるが、ロボットシステムの場合は、ロボットコンポーネントが不特定多数の人と接する場所に設置される場合も多く、物理的なインターフェースからの侵入への対策も考慮する必要がある。

対策のキーとしては、システム内の各部位での認証・認可である。システム上の重要なポイントでは、ユーザ ID/パスワードだけでなく、生体認証などの組み合わせた多要素認証を導入することも検討すべきである。また、不正侵入に成功されたとしても、重要な情報や操作にはアクセスできないようにするアカウントの権限管理も重要なポイントになる。また、各システムでのアクセスログの記録と管理も重要なポイントとなる。

物理的な侵入対策としては、使用しないインターフェース、たとえば USB ポート、Bluetooth などはあらかじめ無効化するなどの対策も有効である。

システムやその間のネットワークの各地点において、通信相手、通信ポートも制限し、不要なポートは閉塞しておくことも重要である。

➤ 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表す。従来のサイバーシステムでは、ユーザスプーフィング、IP スプーフィング、L2 スプーフィングなどの攻撃がある。ロボットシステムの場合にあてはめると、“管理者のふりする”、“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。ロボットシステムの構成要素、例えばロボット制御 PC、クラウド上の管理システムへのユーザやノードになりすましての侵入、ユーザやノードになりすましての不正なコマンドの送信などがこれにあたる。

対策技術のキーは、認証・認可である。ユーザレベルの認証と認可・権限管理が構成要素の

各システムで要求され、重要な要素には、多要素認証も必要である。また、タブレットなどのUIの操作には、生体認証、顔認証などを導入することも効果がある。また、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権限管理も重要である。

なりすましは、検知が難しいという特徴も持ち合わせている。通常時のロボットの行動パターンと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”全般を表す。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、Web サーバ上のコンテンツの改竄、メールの内容の改竄などがこれにあたる。

ロボットシステムの場合は、ロボットが収集するセンサー情報の改竄、ロボットが動作するロジックや制御情報、状態情報の改竄などが考えられる。その影響は、データとしての完全性の阻害だけにとどまらず、ロボットの動作や提供するサービスの可用性、更には安全性へ影響する可能性もある。

対策は、システム全体、及びシステムを構成する各部位で考慮する必要がある。

ハッシュ関数を用いたメッセージ認証、デジタル署名、システム権限管理、ストレージの暗号化・ハッシュ値の保存、セキュアブート・セキュアアップデートなど起動時の改竄チェックの仕組み、セキュアアップデートなどである。

ハッシュ関数とは、任意のデータから別の値を得るための操作であり、逆にその算出された値からデータに戻すことはできない不可逆的な値を作り出すものである。ハッシュ関数によって作り出されたハッシュ値を管理することによって、元のデータが改竄されたかをチェックする仕組み構築が可能となる。

この仕組みを用いてデータの完全性とその作成者の真偽性を保証するものがデジタル署名であり、通信経路においての送信元との真偽性と送信されたメッセージの完全性を保証するものがメッセージ認証となる。この仕組みにおいては、勿論ハッシュ値自体も暗号化される。ブロックチェーン技術やデジタル作品の著作権を保証する非代替性トークンなどもこの仕組みの延長上にあると考えてよい。

ロボットシステムにおいてこの仕組みの適用を考えた場合、まず最初に考える必要があるのはデータの集まる場所における対策である。改竄されたくないデータは、ハッシュ値とともに管理する仕組みを構築することが望ましい。たとえば、クラウド層のデータストレージにおいては、データと同時に暗号化されたハッシュ値も同時に保存して管理することなどである。サーバの改竄検知ソフトウェアもこの仕組みを利用したものであり、場合によってはその導入も検討する必要がある。

ロボットコンポーネント層の制御部(ロボットコントローラ、制御PC)においても、ファームウェアの改竄など対策として、起動時にハッシュ値を照合して真偽性をチェックする仕組み、すなわちセキュアブートの導入することが理想的である。サプライチェーンにおける改竄や異物混入などの対策にもなりうる。この仕組みをファームウェア、ソフトウェアの更新にも拡張したものがセキュアアップデートであり、メッセージ認証の仕組みを用いて、更新時の要求元、送信元が正しいか、コンテンツが改竄されていないかを検証しながらアップデートを実施することができる。

この仕組みを導入した場合にキーになるのは、ハッシュ値の暗号鍵やそれを検証するための検証鍵の管理であり、信頼の起点(Root of Trust)とも呼ばれる。(以下、RoTと呼ぶ) RoTの保管に関しても、OSレベルでの制御、ハイパーバイザレベルでの分離、ハードウェアの分離などの実装によってセキュリティのレベルの差があり、コストや手間との兼ね合いでどの内容を選択する必要がある。

➤ 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”へ流出することをいい、機密性の侵害に当る。従来のサイバーセキュリティでは、盗聴やタッピング、不正侵入などによって機密情報を搾取するパターンや、データベースへのコマンドによって、内部情報を引き出す攻撃などが存在する。代表的な例が、SQL インジェクション攻撃である。ロボットシステムの場合も、同様の攻撃の脅威は存在し、その対策技術のキーは、システム全体に及ぶ。

ロボットコンポーネント側では、漏洩の影響が大きい個人やプライバシーに関する情報は内部には蓄えず、上位システムへ転送する対処を考慮する必要がある。

上位システム側では、蓄積されたデータベース側での諸対策が必要になる。システムへの不

正侵入対策としての認証・認可、データ自体の暗号化・難読化、ハッシュ値の保存と監視による改竄への対策である。また、コンポーネント～上位システム間の通信も暗号化する必要がある。

データを扱うプログラムにおいてはセキュアコーディングを実施し、コマンドインジェクなどの攻撃へのリスクを極小化することも重要である。

➤ DOS 攻撃

DOS 攻撃は、Denial of Service の略で、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し、サービス不能攻撃とも呼ばれる。従来のサイバーセキュリティでは、サーバの接続要求を連続的に行うなどしてサーバに高負荷を与え、サービスを実質的に中止させる SYN Flood 攻撃などが代表的なものである。

ロボットシステムにおいても同様の攻撃の可能性があるが、その影響範囲は、従来のサイバーシステムの場合よりも大きくなる可能性がある。例えば、ロボットコントローラーへの軽度の DOS 攻撃であってもロボットの把持機能に影響を与え、把持しているものが落下してしまうなどことも起こりうる。DOS 攻撃による影響が、可用性ばかりでなく安全性を阻害するなどの影響も考慮しなければならない。

対策技術のキーは、システム上の各境界でのアクセス制御である。実際には、ロボットコンポーネントが動作するセグメントを外部と分離し、その境界で特定の送信元から特定のポート・送信先への通信のみを許可するなどの制御である。

また、逆に攻撃された場合の影響を緩和する対策も検討する必要がある。例えば、DOS 攻撃によりロボットコントローラーの CPU が高負荷となった場合にも物理的な動作に影響を受けにくいようなアーキテクチャを設計することなどである。

➤ マルウェア対策

マルウェアは、不正かつ有害な動作を引き起こす意図で作成された悪意あるソフトウェアやコード全般を指す。ウィルス、ワーム、ボット、最近ではランサムウェアなども代表的な例である。ロボットシステムにおいても、その構成要素を分解するとサイバーシステムであり、常にマルウェア混入のリスクにさらされていることは、従来のサイバーシステムと同様である。

対策技術のキーは、ウィルス対策ソフト、最新脆弱性やマルウェアへの対策を含んだパッチの適用などを運用することである。また、ネットワークの境界点において、不正な通信パターンやログなどを監視する機構も有効である。また、マルウェア感染の疑いがもたれる場合は、その部位は、即ネットワークから隔離し、動作も停止する必要がある。

➤ 物理攻撃

ロボットシステムは、従来の産業用ロボットを除けば、物理的な隔離された安全な場所に設置されているとは限らず、物理的なインターフェースやコンポーネントに対する対策も検討の必要がある。

- ◇ 物理的な設置場所への対策： 入退室管理、監視カメラなど

- ◇ 物理プラットフォームへの対策： 耐タンパ性の向上

- ◇ 物理インターフェースへの対策

 - :使用しないインターフェース(USB、Bluetooth、JTAG 等)の無効化

- ◇ 物理盗難対策:セキュリティワイヤ、カードロック、警報システム、GPS による動線追跡など

6. 実装フェーズ

本章では第5章の設計フェーズでの検討結果を受け、ロボットシステムのライフサイクルの実装フェーズにおけるセキュリティの実施項目について述べる。なお、設計フェーズの内容を検証する総合テスト、コンセプトフェーズで設定した内容の総合評価についても、本章に記載する。

6.1. 実装フェーズ概要

6.1.1. 目的とゴール

実装フェーズの目的は、ロボットシステムを目的どおり動作させるための実装作業・テストの実施である。実装フェーズでは、第5章の“設計フェーズ”で検討したセキュリティ対策を実装し、その有効性をテストする。また、実装フェーズの終了時は、第4章の「コンセプトフェーズで設定したセキュリティゴールがどの程度達成されたか？」第5章の「設計フェーズで評価したリスクがどの程度軽減されたか？残留リスクは何か？」についても評価する。

実装フェーズのゴールは、セキュリティ上必要な対策とテストを実施し、ロボットシステムをあるべき姿で安全に運用開始できるようにすることである。ただし、実装フェーズだけですべての脅威・リスクに対応できるわけでない。運用でカバーする多重防御も必要であり、運用にはいるにあたって何が残留リスクかを明らかにすることも重要なゴールである。

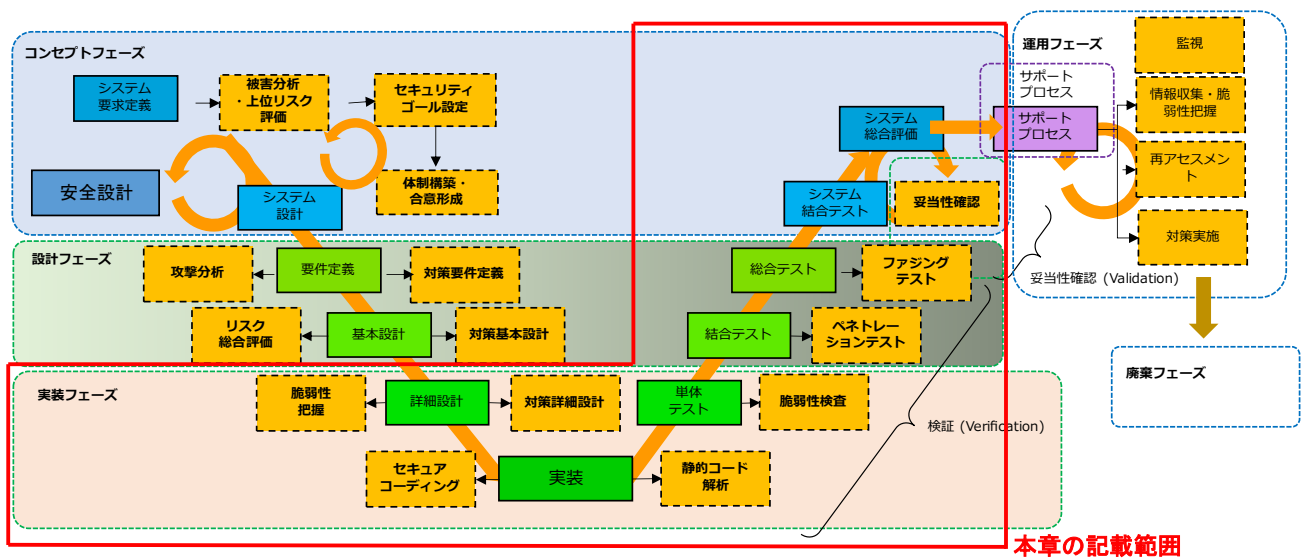


図 6-1 実装フェーズの位置づけとセキュリティ検討項目

6.1.2. 実施組織

実装フェーズの実施主体となる組織は、システムインテグレータなどの設計開発担当組織である。ただし、セキュリティ対策の実装作業は、システムの各構成部位単位で作業することになり、担当するメーカーや IT ベンダ、サプライヤとの共同作業となる。

対策の実装にあたっての作業分担、責任分担、および関係者への教育、訓練もこのフェーズで実施する。また、定義した対策の要件をポリシーとして細則化する、ガイドライン化することなども、大きな案件、プロジェクトにおいては作成することが望ましい。

また、サプライヤ・ベンダ側での実装内容やテスト結果も精査できるようなチェックポイントを設け、そのエビデンスも入手しておくべきであり、主担当の設計開発組織の責任者がこれを承認する必要がある。

実装フェーズの最終段階では、コンセプトフェーズで定義したセキュリティゴールと実態の整合性を最終チェックする必要がある。設計開発担当組織が実施した実装作業・テスト結果を企画組織が評価する。また、実装した製品やサービスが情報システム部門、品質管理部門の規定にも適合しているかの承認手続きも必要になるケースが出てくる。また、運用組織もその結果を承認すべきである。

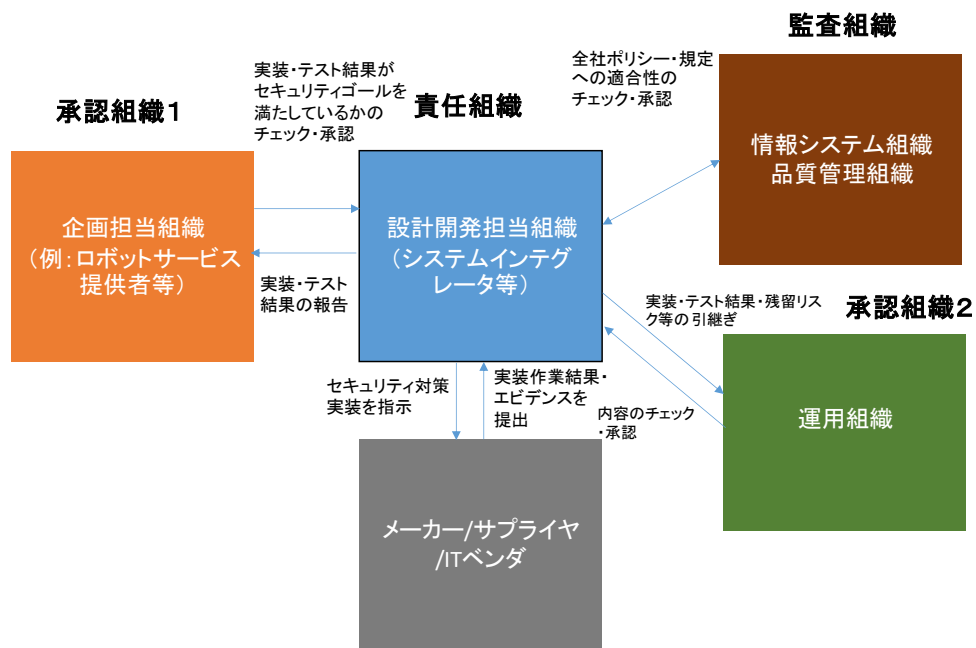


図 6-2 実装フェーズ 実施体制図(例)

6.1.3. 実施事項

実装フェーズでの実施事項は、設計フェーズで定義した脅威への対策要件に合わせて具体的な実装とテストを実施することである。実装フェーズを開始するにあたり、事前準備として表 6-1 に示すインプットが必要であるが、脆弱性情報に関しては最新の情報を再入手しておく必要がある。

表 6-1 実施事項・インプット・アウトプット

インプット	セキュリティ実施事項	実施組織 主体(副)	アウトプット
セキュリティゴール定義書 脅威脅威想定表(リスク評価結果・対策要件入り) <副次資料> 対策入りミスユースケース図 アタックツリー図 通信フロー図 最新の脆弱性情報	実装フェーズ ・前準備(脆弱性情報、ツール、ソースコードレビュー等) ・対策実装内容と分担の確定 ・実装作業とテストの実施(単体、結合、総合) ・総合評価	設計・開発担当組織、(運用担当組織、企画担当組織)(情報システム・セキュリティ組織)	脅威想定表(リスク評価結果・対策要件・対策結果・テスト結果・残留リスク入り)(AppendixE-3参照) ・実装作業テスト計画書・報告書 ・最新の脆弱性情報 ・通信フロー図 ・資産管理表(詳細入り) セキュリティゴール定義書(妥当性評価追記) 【チェックポイント2】

実装フェーズの準備からその結果の承認までには以下のようなステップが必要である。

1. 対策の実装内容と作業分担の確定

◇ 要件を実装レベルに落とし込む

- ・実装レベルの作業分担と責任範囲を明確にする
- ・関係者の合意を得る

2. 実装作業の詳細(作業手順とテスト方法)の確定

◇ 対策の実装作業の詳細手順、およびテスト方法、その結果を示すエビデンスを検討し、確定する

3. 関係者の教育・訓練の実施

4. 対策の実装作業・テストの実施

5. 実装作業結果・エビデンスの収集・整理

6. 総合評価、および総合テストの実施

7. セキュリティゴールの達成度合いの評価と関係組織の承認(チェックポイント 2)

6.2. 対策実装作業・テストの前準備

6.2.1. 対策の実装内容と作業分担の確定

第5章“設計フェーズ”で定義した想定脅威と対策要件は、実装フェーズでは、ロボットシステムを構成する各部位で実装作業することが前提になる。例えば、不正侵入・なりすましへのシステムの各構成部位への対策例について図 6-3 に示す。

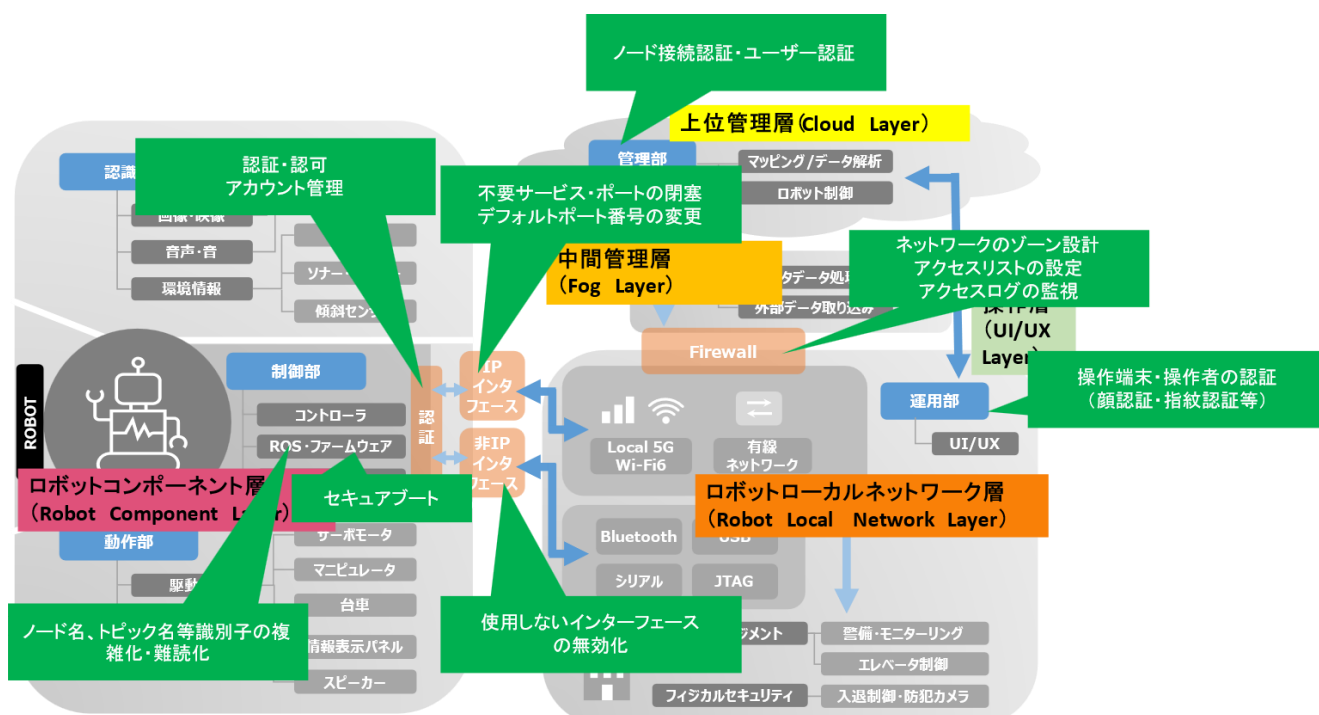


図 6-3 不正侵入・なりすましへの対策実装(例)

したがって、複数の作業員、組織が関わるのが通常であり、その実装内容とそれに対するテストは、実施前、実施後で設計開発組織の責任者がチェックを行う必要がある。また、実装作業・テスト結果を示すエビデンスを作業員は記録し、それを責任者がチェックし承認するプロセスも必要になる。

実装レベルでの作業内容とその分担を確定した後は、その内容について責任者と作業員の間で合意する必要がある。作業員が詳細の内容を検討・確定し、それを責任者が承認する場合、責任

者が作業内容の詳細を確定し、作業者に指示する場合は、案件によって様々であるが、作業にはいる前に合意形成できていることが重要である。

6.2.2. 実装作業の詳細検討

本節では、ロボットシステムを構成する各部位における実装作業の詳細を検討するにあたってのセキュリティ対策のポイントについて技術的側面から解説する。

代表的な脅威に対する対策のポイントは、前章“設計フェーズ”の“対策の選択”の表 5-8 を参照されたいが、実装レベルで共通的に必要になる対策を以下に列挙するので留意されたい。

➤ 共通的な対策例

◇ 認証・認可機構の実装

ID・パスワードの複雑化・
2 要素認証

◇ トピック等識別子のデフォルト値からの変更

◇ マルウェア・ウィルス対策

◇ セキュアプログラミング

プログラム中に機密情報をバーコードせず、公開可能なプログラムをデプロイ

◇ 不要ポート(論理、物理)の閉塞、無効化

◇ 不要サービスの停止

◇ OS、ソフトウェアの脆弱性情報の定期収集、パッチ適用

◇ ファームウェア更新

システム上の各部位での想定脅威への対策の実装例について、下記の表に示し、その内容の詳細を解説する。

表 6-2 想定脅威と対策の実装例

想定脅威／ 構成部位	ロボットコンポーネント層		フォグ層	クラウド層層	運用操作層 (UI)	通信ネットワー ク
	制御部	動作部／ 認識部				
不正侵入	アカウント管理 認証・認可 不要サービス・ ポートの閉塞 通信の暗号化 アクセスログの 監視	盗難対策 使用しないイン ターフェースの 無効化(USB、 JTAG、 Bluetooth)	FWによるア クセス制御 認証 侵入検知	ユーザ認証・認 可 ノード接続認 証・認可 通信の暗号化	端末・操作 者の認証 (顔・指紋認 証など)	ネットワークの ゾーン設計 通信回線の選 択(オープン or クローズ) ローカル通信の 選択(無線、有 線)
なりすまし	ノード名・トピッ ク名等の識別 子の複雑化				端末・操作 者の認証 (顔・指紋認 証など)	アクセスリスト の設定
改竄	セキュアブート データバックア ップ 重要情報のハ ッシュ値保存・ デジタル署名 ディスク暗号化 改竄検知機構 の導入	センサーの多 重化 耐タンパ性の 向上	データバック アップ AIトレーニング データの真 偽性の認証 (メッセージ認 証・デジタル 署名など)	データバックア ップ 重要情報のハ ッシュ値保存・ デジタル署名 ディスク暗号化 改竄検知機構 の導入		アクセスログの 監視 通信の暗号化
情報漏洩	セキュアブート セキュアコーデ ィング			盗難、盗聴によ る機内データ漏 洩 ロボット内の個 人情報(画像 等)の扱い ストレージの暗 号化・ハッシュ 値の保存	盗難、盗聴 による機内 データ漏洩 通信暗号化 キーの漏洩 防止	

想定脅威／構成部位	ロボットコンポーネント層		フォグ層	クラウド層	運用操作層（UI）	通信ネットワーク
	制御部	動作部／認識部				
DOS 攻撃	不要サービス・ポートの閉塞 CPU 負荷・メモリ圧迫の影響を最小限に留める設計	制御部の高負荷による影響を受けない設計		不要サービス・ポートの閉塞 CPU 負荷・メモリ圧迫の影響を最小限に留める設計		不要ポート・通信の遮断 アクセスログの監視
マルウェア対策	ウィルス対策ソフト 定期的な脆弱性検査 パッチ適用 ファームウェア更新			ウィルス対策ソフト 定期的な脆弱性検査 パッチ適用		
物理攻撃	CPU/ディスクのロック	盗難対策 導線監視		入退室管理	操作端末認証 操作者認証（顔・指紋認証）	

【解説】

制御部（ロボットコントローラー、ロボット制御 PC）

制御部は、PCなどのプラットフォームのCPU/メモリ/ディスク、ファームウェア、OS、ミドルウェア、アプリケーションプログラム、データベースなどから構成される。これら、個々の構成要素の脆弱性情報は実装時に収集し、必要なパッチがあれば適用するが、同時に攻撃されても耐えうる内部設計も非常に重要である。高い機密性、完全性が要求される情報と一般の情報の分離しアクセス権を管理する、個人、プライバシー情報などはディスク上には保持しない、などである。また、ロボットが設置される環境によっては、物理的な侵入口に対する対策も非常に重要になる。

以下にポイントを挙げる。

- ファームウェアへの対策:セキュアブート、セキュアアップデート
- OS への対策:アカウント管理の強化、重要情報へのアクセス権の制御・暗号化、不要サービス・ポートの閉塞、最新パッチの適用
- ミドルウェアへの対策:脆弱性対応、トピック等の識別子等の難読化
- API、APP への対策:セキュアプログラミング
- データベースへの対策:インジェクション攻撃対策、機密性の高い情報は暗号化、もしくは難読化
- ネットワークインターフェースへの対策:アクセスリストの設定
- 物理プラットフォームへの対策:耐タンパ性向上対策
- 物理インターフェースへの対策:不要ポートの無効化
- 物理的な設置場所への対策:入退室管理など
- 各種盗難対策

動作部

- 物理的な盗難防止:セキュリティ・ワイヤ、GPS 等による導線監視など
- 扱う対象物の監視:IC カードによる荷物室のロック(搬送ロボットの場合)など

認識部

- センサーの多重化による信頼性向上

フォグ層(Fog Layer)

フォグ層(Fog Layer)は、クラウド層とロボットの各コンポーネント(制御部、動作部、認識部)とを中継する層であり、通常、外部ネットワークとの境界の役割を果たすファイアウォールが設置され

る。また、ファイアウォールの配下の DMZ に、中継サーバ、踏み台サーバなどが設置される。ロボットコンポーネントとの間でリアルタイム性が高い応答性が要求されるアプリケーションサーバ、例えば、AI の推論サーバなどもこの層に設置されるべきである。逆に、クラウド層との間が完全な閉域の通信ネットワークであったり、システムの規模がローカルエリア内にとどまる場合は、この層は必ずしも必要ではない。その構成は、システムの規模や諸条件によって最適化されるべきである。

この層そのものが、セキュリティ的な境界を与えるという目的をもっており、外部との境界の管理や監視、記録などの役目を果たす。

以下にセキュリティ対策の実装のポイントを挙げる。

- 境界 FW での対策: 通信ポート・送信元・送信先を制限、アクセスログの管理、監視
- DMZ、踏み台サーバ、中継サーバ等の対策

クラウド層 (Cloud Layer)

クラウド層は、ロボットの管理システム、ロボットが収集するデータのリポジトリ、管理者のユーザインターフェース、外部システムとの連携のインターフェース、更には昨今では、AI モデルの学習と推論システムが含まれる。それらの対策も非常に重要である。

- ロボット管理システムへの対策: 認証認可、アカウント管理
- データリポジトリへの対策: データの暗号化、ハッシュ値の保存、読み書きの権限管理、コマンドインジェクションへの対策
- AI への対策: トレーニングデータ改竄への対策、AI モデルの機密性対策

運用操作層 (UI)

運用操作層は、ロボットを制御・管理するためのユーザインターフェースを提供するために、管理者のなりすまし、不正な操作端末の接続には十分な対策を打つ必要がある。

- 操作者の認証: ID/パスワードと生体認証 (顔認証、指紋認証) との組み合わせ

通信ネットワーク

➤ ネットワーク構成・設計での対策

相互に連携するロボットコンポーネント(制御部、認識部、動作部)が接続されるロボット・ローカルネットワークと外部のネットワークの境界には、ファイアウォールを設置し、必要とされる通信の種類と相手のみ許可するアクセスリストを設定し、アクセスログを取得可能とすることが望ましい。また、クラウド層からの直接の遠隔接続は攻撃の起点となる侵入口となりうるために、境界に設置したファイアウォールに DMZ を設け、踏み台サーバ経由での接続をとる形態が理想的である。(フォグ層(Fog Layer)の設置) また、相互に連携するロボットコンポーネントが遠隔に存在する場合は、VPN による通信をとることが望ましい。

上記の対策が困難な場合は、クラウド層との間を完全な閉域ネットワークで接続するなどの形態にすべきである。

➤ 無線 LAN への対策

WEP2/WEP3 の暗号化、認証とともに、ロボットコンポーネントが接続されるセグメントと一般の機器が接続されるセグメントは、同じチャンネルには接続せず、専用の SSID を準備する構成を推奨する。また、可能であれば SSID も一般には公布しないステルスモードに設定することが理想的である。

これらの点は、通信のセキュリティ対策になるとともに、ロボットに関連する外部との通信のパフォーマンスという点でも非常に有利であり、可用性の向上にもつながる。

➤ ネットワーク機器への対策

無線アクセスポイント、無線ルーター、ブロードバンドルーター・スイッチ、ファイアウォールなどのネットワーク機器は、ID/パスワードの管理を厳重に行い、管理者特権パスワードなどの設定情報は暗号化しておく必要がある。また、特定のアドレスからのみのアクセス許可を設定し、接続する場合は、DMZなどに設置した踏み台サーバ経由にするなどの対策も有効である。

➤ 通信の種類と対策

ロボットコンポーネントとクラウド層など外部との通信は、実際にはカメラやセンサーなどから非同期に情報を送信する性質の通信(トピック通信とも呼ばれる)、クラウド層から制御情報をロボットコンポーネントへ送信する通信(アクション通信)、ロボットコンポーネントの状態を遠隔で確認するための通信(サービス通信とも呼ばれる)などが存在し、要求される帯域、リアルタイム性、欠損による影響などが異なる。このため、必要に応じてこれらの通信の種類によってインターフェースを分ける、セグメントを分けるなどの対策も、可用性やパフォーマンスという点では有効である。

データ全般

➤ 動作に直接関わるデータへの対策

ロボットの制御に関わるデータ(制御情報、状態情報、制御プログラム、制御ロジック)などは、ロボットの動作に直接関係してくるデータである。また、センサーやカメラの映像データもその情報から次のアクションが決まり、制御に直接影響してくる場合がある。これらの内容のデータは、その完全性の維持が非常に重要であり、例えばサーバや通信経路でこれらのデータが改竄されるとロボットが誤動作したり、それによって非常停止してしまう可能性がある。これらのデータは、その通信経路において、メッセージ認証により通信元とデータの真偽性の確認を行うことが理想的であるが、TLS などによる暗号化と通信相手の認証の仕組みは必須となる。また、サーバに保管されるこれらのデータは、書き込み時点のハッシュ値を保存し、改竄が発生していないかを検証できるようにしておくことが望ましい。

➤ 個人情報・プライバシー関連情報への対策

ロボットシステム、特にサービスロボットでは、個人の顔、声など個人を特定するデータやプライバシーに関わるデータを扱うこともしばしばである。これらのデータは、ロボットコンポーネントからクラウド層のサーバへ転送され管理されるのが通常である。この場合、ロボットコンポーネント側のディスクやメモリ上からは、これらの情報は削除する運用を行うことが望ましい。また、上位のサーバ上のストレージに集められたデータが攻撃者に搾取されると情報漏洩となり社会的なインパクトも非常に大きい。したがって、サーバ上では、データへのアクセス制限を厳重に行い、ディスク上のデータの暗号化、ハッシュ値の保存を行う必要がある。また、サーバへのアクセスログの監視とともに、改竄検知の仕組みを導入することも考慮に値する。

勿論、個人情報、プライバシー情報を含むこれらのデータは、そのロボットがサービスを提供す

る事業者や組織のプライバシーポリシーに従い適切な処置を講ずるのが基本であり、その方針の中で最も適切な対処を講ずるべきである。

➤ 営業機密情報への対策

ロボットが提供するサービスのロジックや昨今ではロボット動作を支援する AI モデルも非常に重要な知財であり営業機密情報である。また、ロボットの特徴として、扱う対象物、たとえば工業製品、清掃する建物、運搬する荷物や食品などがあり、これらはロボットのサービスを利用する顧客の重要な機密情報である場合が多い。これらの情報の扱いについては、前項の個人情報、プライバシー情報とともに、その扱いの方針をあらかじめ決めて適切な対策を実施する必要がある。

➤ システム情報への対策

ロボットの制御部(ロボットコントローラー、制御PC)や、クラウド層のクラウドサーバで管理されるシステム情報(設定情報、アカウント情報)、暗号鍵などは、一般ユーザからは読み書きできないよう権限管理を施すことが重要である。

➤ ログ・証跡記録への対策

ロボットシステムの各部位の各種ログや操作証跡記録は、インシデントが発生した場合などに非常に重要な手がかりとなりうる。攻撃者によっては、これらの記録を削除して証跡を残さないなど手口は高度化してはおり、その意味でもログ関係はバックアップを定期的を取得しておくべきである。

➤ データのバックアップポリシー

ロボットシステムに関連する情報は、設定情報、動作プログラムなどをはじめ直接動作に影響する情報や高い機密性を要求される情報、インシデント発生時に有効な手がかりとなる情報などセキュリティ側面からも重要なデータが含まれており、そういう種類のデータに対してどういうバックアップをどの頻度で取得するかをポリシーとして策定し、運用することが重要である。勿論、そのポリシーを定期的に見直す必要もある。

6.2.3. テスト方法の検討

セキュリティテストについては、以下のような段階を経て実施することを推奨する。また、テストの実施者＝実装作業で良い場合と、できれば分けた方がよい場合があり、予算や体制なども考慮して実施体制の詳細は決定する必要がある。

[1] 個々の実装作業が正常に実施されたかの確認（作業レベルの確認）

前項で検討したセキュリティ対策の実装作業が正常に実施されたかを確認する。

実装作業とともに確認作業を手順書化しておくことが望ましい。また、作業が正常に実施されたことを示す操作記録、確認結果の出力記録などのエビデンスもあらかじめ決めておくことも重要である。これにより後工程において想定通りの結果が確認されなかった場合などに遡って原因を追究することが可能になる。実施体制としては、実装作業＝テスト者で問題ない。

[2] 個々の実装作業によって想定リスクが解消されているか？のテスト

実装作業が正常に実施された結果、想定していたリスクが解消しているか？のテストを実施する。テストの良否判定基準は、目的のリスクが緩和・解消されているかどうか？である。個別の部位だけのテスト（単体テスト）だけでは完全な判定ができず、システム全体でのテストも必要になる場合があり、そのテストによってどこまでの有効性が検証されたか？は事前に把握しておく必要がある。

もしテストの結果が期待どおりでない場合は、対策の実装方法について見直しをすべきである。参考のために搬送ロボットへの対策とテスト内容の事例を表6－3に示す。

表 6-3 搬送ロボットへの対策とテスト内容例

	想定脅威分類	テスト内容
1	ロボット制御 PC への攻撃	ロボット制御 PC へ、WiFi や Bluetooth で物理接続しようとしてもできないこと
2		ロボット制御 PC へ、root 及び ROS 起動ユーザになりすましてコンソール経由で不正にログインしようとしてもログインできないこと
3		ロボット制御 PC へ、root 及び ROS 起動ユーザになりすまして SSH 経由で不正にログインしようとしてもログインできないこと
4		ロボット制御 PC の SSD を取り外し、他の PC に取り付けて情報の盗聴や改竄をしようとしても、機密情報が暗号化されているため盗聴や改竄ができないこと
5		ロボット制御 PC に不正にログインされたとしても、重要なファイルを改竄すると検知されること
6		ロボット制御 PC に不正にログインされ、管理プラットフォームと通信するプログラムが改竄されたとしても、管理プラットフォームが不正なデータを受け取らないこと
7		ロボット管理プラットフォームになりすまし、ロボット制御 PC へ偽の命令を送信しようとしても、ロボット制御 PC が受け付けられないこと
8		ロボット制御 PC の空きポートをスキャンし SYN Flood をかけようとしてもポートが空いていないためにロボット制御 PC の CPU やメモリが消費されないこと
9		ロボット制御 PC の Well Known ポートに SYN Flood をかけようとしても、ポートが空いていないためにロボット制御 PC の CPU やメモリが消費されないこと
10		OS や各種ライブラリ、ROS に含まれる既知の脆弱性に対して攻撃をかけようとしても、攻撃が成功しないこと
11	荷物室への攻撃	荷物室の制御 Raspberry Pi へ、Wifi や Bluetooth で接続しようとしても、できないこと
12		荷物室の制御 Raspberry Pi へ、Root 及び制御プログラム実行ユーザになりすましてコンソール経由で不正にログインしようとしても、ログインできないこと
13		荷物室の制御 Raspberry Pi へ、Root 及び制御プログラム実行ユーザになりすまして SSH 経由で不正ログインしようとしてもログインできないこと
14		荷物室の制御 Raspberry Pi の MicroSD カード等を取り外し、他の PC へ取り付けて情報の盗聴や改竄をしようとしても、機密情報は暗号化されているために盗聴や改竄はできないこと
15		荷物室の制御 Raspberry Pi の空きポートをスキャンし SYN Flood をかけようとしても、ポートが空いていないため荷物室の制御 Raspberry Pi 内の CPU やメモリが消費されないこと
16		荷物室の制御 Raspberry Pi の Well Known ポートをスキャンし SYN Flood をかけようとしても、ポートが空いていないため荷物室の制御 RaspberryPi 内の CPU やメモリが消費されないこと

2. システム全体の検証 ～結合テスト

実装作業によって「想定リスクが解消されているか?」、すなわち「設計フェーズで定義した要件が満たされているか?」の検証である。必要に応じて、ペネトレーションテストなどのテストツールを使用することを検討するとよい。ペネトレーションテストは、システムの脆弱性を検証するテスト手法のひとつで「想定するシナリオに基づいて外部からシステムに侵入できるか?」を試みるテストである。(テストツール類の例については、APPENDIX Dを参照されたい)

この段階のテストは、実装作業とは別の人員をアサインするのが理想的であるが、内部にリソースがない場合は、外部への委託なども検討の余地はある。

3. 総合テスト(「潜在的な脆弱性がどの程度残存しているかどうか?」のテスト)

設計フェーズで定義した要件以外にも、「残留リスクが潜在的な脆弱性がどのくらい残存しているか?」をツール類で検証するなどしておくことも重要である。「想定外のデータの入力があってもセキュリティ要件が行われぬか?」を最終チェックする意味では、ファジングツールによるテストも効果的である。そのほか、脆弱性スキャンツールなどを使用した動的な検査も有効になる。

このテストによって、予期せぬ致命的になりうる脆弱性や残留リスクが発見された場合は、設計フェーズにおける対策の要件定義も見直す必要が生じる場合もある。

6.2.4. 実装作業・テストの諸準備

最新の脆弱性情報の収集

最新パッチ、アップデートの入手

テスト環境・テストツールの準備

脆弱性検査ツール、静的コード解析ツール等

(テストツール類については、APPENDIX D 参照)

6.2.5. 関係者の教育・訓練の実施

実装作業にはいる前に、実装作業担当者の教育・訓練を実施する。内容としては、上位要求であるセキュリティゴール、想定脅威と対策要件の共有、担当する作業内容（実装作業手順、テスト手順）に必要な技術訓練などである。

- セキュリティゴールの共有
- 想定脅威・リスクと対策要件の理解
- 対策実装内容・作業内容の理解
- 作業上必要な技術の習得（ツールの使い方等）

6.3. 実装作業・テストの実施と結果の整理

6.3.1. テスト結果の収集と整理

各担当における実装・テスト作業が実施された後に、設計開発責任者は、各担当者から作業結果エビデンスを集め、内容を確認し、整理する。また、内容に不備がある場合は、作業担当者に実装作業やテストの再実施やエビデンスの再収集を求める。また、テスト結果によっては、作業のやりなおし、あるいは、設計フェーズにおける要件定義のやりなおしも検討することも検討する。

6.3.2. 総合評価の事前準備

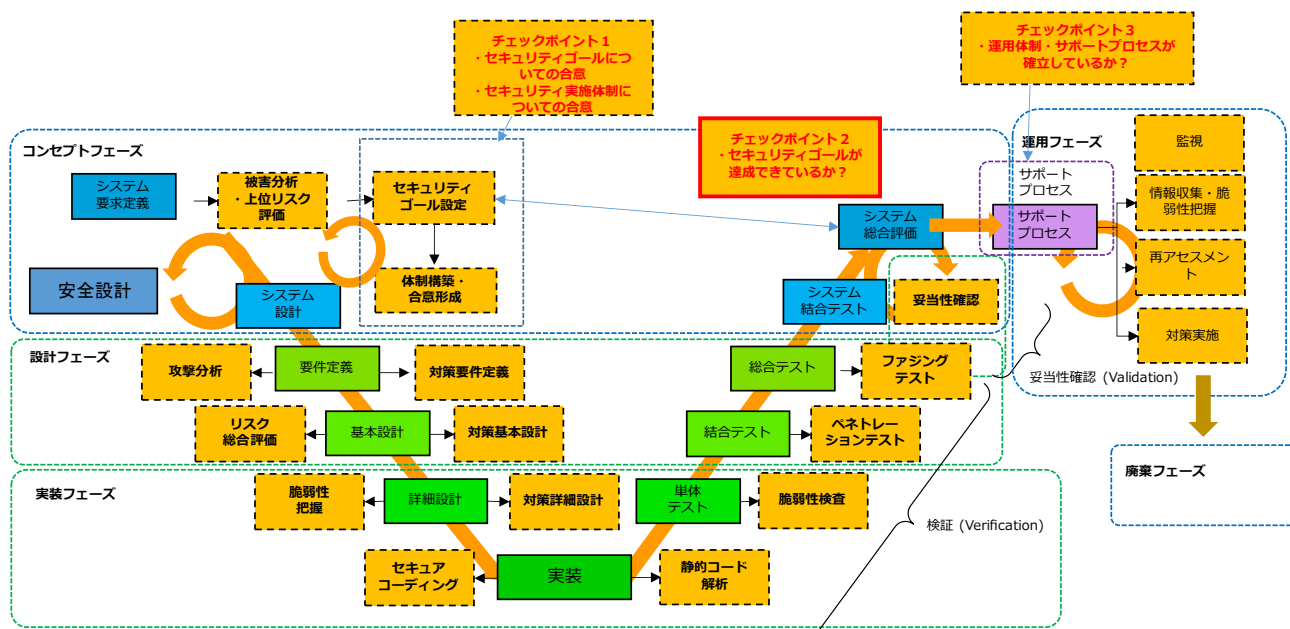
前節で収集・整理した実装作業とテスト結果を踏まえて、設計開発組織の責任者は、設計フェーズで定義した対策要件を満たしていることの採取確認と同時残留リスクについての明確にしておくことが望ましい。APPENDIX E-3 にテストの実施まで含めた想定脅威に対する対策要件と実施のチェックシートを示す。

6.4. 総合評価

(～妥当性評価(セキュリティゴールの達成度合いの評価)と関係組織の承認(チェックポイント2))

設計開発組織の責任者からの結果の報告を受けて、企画組織はその結果が「コンセプトフェーズで設定したセキュリティゴールを満たしているかどうか?」という視点での上位レベルの妥当性評価を行う。実装結果が、セキュリティゴールを満たしていないと判断される場合は、設計フェーズの対策の要件定義からやり直す場合もある。また、場合によっては、セキュリティゴールの設定に立ち戻る場合もある。

企画組織とともに、実際にロボットを利用したサービスの運用を実施する運用組織や組織上横断的に関連する品質管理組織、情報セキュリティ組織などの関連組織でもその結果は承認・合意されるべきである。また、運用組織とは、実装フェーズまでの内容の共有と運用でカバーする要件と、残留リスクについて合意しておくことが重要である。

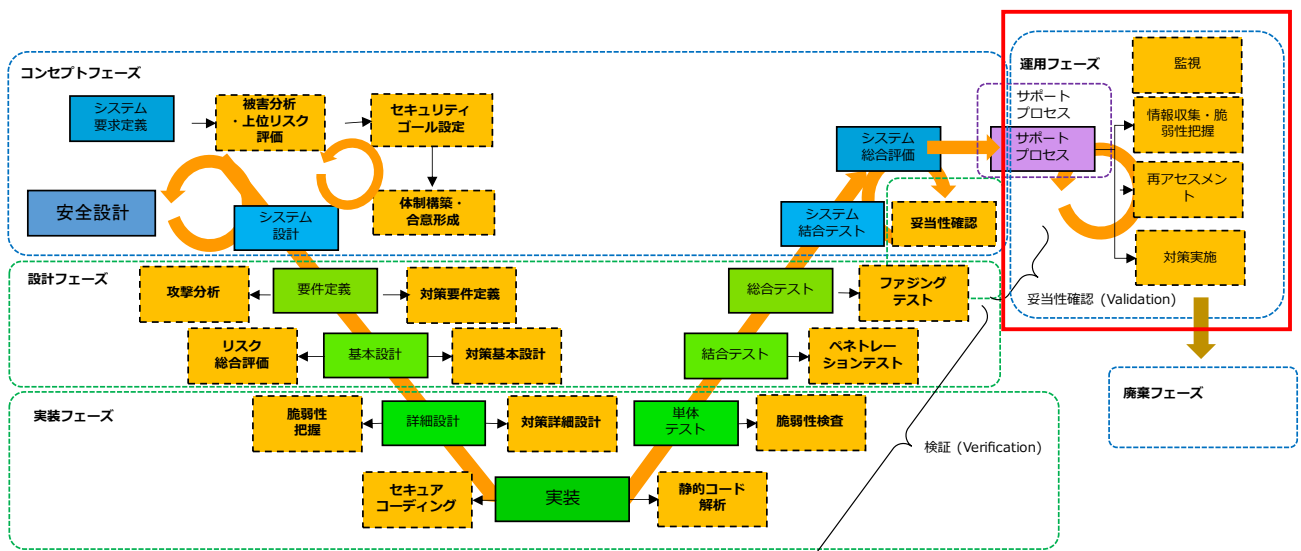


引用: ESPR (Embedded System development Process Reference) 2.0
システム開発プロセス(実線)にセキュリティ関連項目(破線)を追記

図 6-4 実装フェーズ終了時のチェックポイント

7. 運用フェーズ

運用フェーズでは、ライフサイクルのこれまでのフェーズで検討した内容に基づき構築されたシステムに対してセキュリティに対する要求が確実に実装され、機能していることを継続的に監視し、定期的な対策内容の見直しやリスクの再評価を実施する。公表されている脆弱性などについての情報を定期的に収集し、常にロボットを最新の状態に更新したうえで運用中のセキュリティ対策を実施することが重要である。



引用：ESPR (Embedded System development Process Reference) 2.0
システム開発プロセス（実線）にセキュリティ関連項目（破線）を追記

図 7-1 ライフサイクルにおける運用フェーズの位置づけとセキュリティ検討項目

7.1. 運用フェーズ概要

本節では、前章までのライフサイクルのフェーズを経て実装されたロボットシステムのセキュリティについて、その維持のために運用フェーズの中で、関係するそれぞれの実施主体に求められる役割と責任区分及びインプット、アウトプットについて述べる。

7.1.1. 運用フェーズの目的とゴール

運用フェーズにおけるセキュリティリスクとして、個人情報漏洩や機密データ流出のほか、外部からの攻撃によりロボットが制御不能になるなど運用フェーズにおけるセキュリティインシデントの発生、ロボットを利活用する運用担当組織においても、深刻な事態を招く恐れがあることは言うまでもない。サービス分野におけるロボット導入については、導入後における運用担当組織のセキュリティレベル維持への関与が求められることとなり、システム提供側と利用者側が相互の役割と責任区分を明確にし、運用を行っていくことが望ましい。運用フェーズにおけるセキュリティトラブルを回避することを目的にシステム開発プロセスで構築されたセキュリティ内容について目標としている状態に維持することがゴールである。

7.1.2. 運用フェーズの実施組織

運用担当組織が実施主体となるが、実装作業上の瑕疵や不明点、インシデントへの対応も含めて設計開発担当組織と連携しサポートプロセスを構築しておく必要がある。なお、実際は運用担当組織内も設計開発担当組織も組織内における担当部署が細分化されていることが一般的であり、関係する部門それぞれの役割、連絡体制を明確にしておく必要がある。

表 7-1 運用フェーズにおける実施組織一覧

運用担当組織関係部署	セキュリティインシデント発生時の役割
施設管理者 (施設オーナー)	①ロボット管理者からの報告により、施設利用者および施設設備等への影響、被害を確認し、必要な措置を講ずる。
ロボット運用管理者	①ロボット利用者からの報告により、施設利用者および施設設備等への影響、被害を確認する。 ②設計開発担当組織に連絡。発生事象を伝え、一次的に必要な措置を確認し、ロボット利用者に講ずる措置について具体的な指示を行う。 ③関係者(施設管理者、運用担当組織内システム管理部門および危機管理部門等)に発生事象概要を報告する。 ・発生インシデント内容 ・発生日時・場所 ・施設利用者および施設設備等への影響、被害(想定されるものも含む)

運用担当組織関係部署	セキュリティインシデント発生時の役割
ロボット運用管理者 (続き)	<ul style="list-style-type: none"> ・一次的に講じている措置 ・設計開発担当組織の対応状況 ・今後の対応 等 <p>④その他、関係者間で予め決めていたセキュリティインシデント発生時において講ずるべき措置を講ずる。</p>
ロボット利用者	<p>① ロボット管理者に発生事象概要を報告する。</p> <ul style="list-style-type: none"> ・発生インシデント内容 ・発生日時・場所 ・施設利用者および施設設備等への影響、被害(想定されるものも含む) ・一次的に講じている措置 等 <p>②ロボット管理者に指示された措置を講ずる。</p> <p>③施設利用者および施設設備等に影響、被害がある場合は、一次的な対応を行う。</p>
システム管理部門	<p>①ロボット管理者からの報告を受け、設計開発担当組織と連携し発生インシデントの内容確認、分析を行う。</p> <p>②危機管理部門に発生インシデントの状況分析、同事象に起因する運用担当組織内システム等への影響範囲、運用担当組織外への影響等を報告する。</p>
危機管理部門	<p>①ロボット管理者およびシステム管理部門からの報告を受け、施設利用者、施設管理者、運用担当組織への影響、被害を確認、分析を行い、必要な措置を関係者に指示する。</p> <ul style="list-style-type: none"> ・関係者への対応 ・広報対応 ・被害及び影響拡大の有無の報告 ・今後の対策 等

また、設計開発組織は、実際には下記のような担当部門に細分化されていることを考慮する必要がある。表7-2にその例を示す。

表 7-2 運用フェーズにおける設計開発組織の構成(例)

設計開発担当組織関係部署	セキュリティインシデント発生時の役割
営業担当	<p>①運用担当組織ロボット管理者からの連絡を受け、システム管理担当部署に報告。</p> <p>②運用担当組織ロボット管理者に、発生したセキュリティインシデントに関して、必要な確認事項を伝え、報告を求める。</p>
設計開発担当者	①(遠隔監視可能な場合は)、遠隔により、セキュリティインシデントの状況確認、被害拡大措置、原因の特定等を行う。
危機管理部門	<p>①営業部門、設計開発担当者からの報告を受け、必要な措置を関係者に指示する。</p> <ul style="list-style-type: none"> ・関係者への対応 ・広報対応 ・被害及び影響拡大の有無の報告 ・今後の対策 <p style="text-align: right;">等</p>

7.1.3. 運用フェーズでの実施事項概要

運用フェーズでの実施事項は、セキュリティゴールで設定した目標の維持のために必要な事項であり、脆弱性情報把握やパッチ適用、監視、実装フェーズでは受容した残留セキュリティリスクのトレースなどの作業がそれにあたる。また、環境の変化や攻撃手法の進化に合わせてリスクの再評価も必要になるが、インシデント対応も含めた PDCA サイクルの回し方、周期を、運用フェーズを開始するにあたり明確にしておく必要がある。

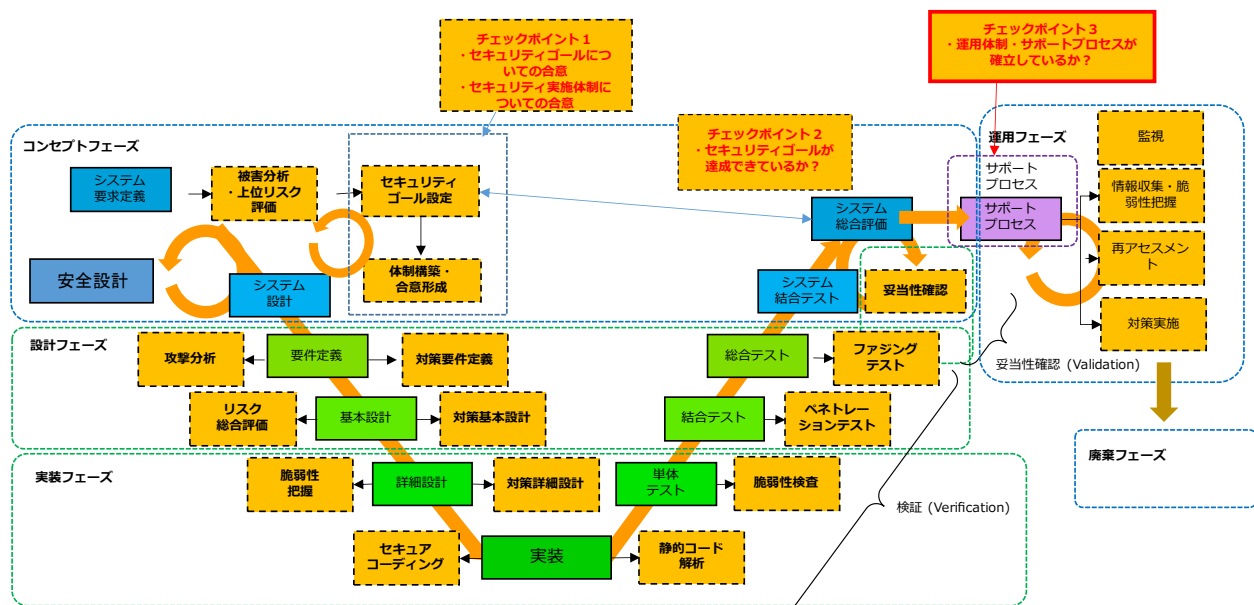
また、事前準備として表 7-3 に示すインプットが必要であるが、その内容は十分に設計開発担当組織から引き継いでおく必要がある。また、実装フェーズの作業やテストだけのために加えた変更 (SSH のポートを開けるなど) は、運用フェーズに入る前に最終形となっていることをチェックする必要がある。

表 7-3 実施事項・インプット・アウトプット

インプット	フェーズ・実施事項	実施組織 主体(副)	アウトプット
【チェックポイント3】 セキュリティゴール定義書 (Appendix E-2 参照) 脅威想定表 (リスク評価結果・対策要件・対策結果・テスト結果・残留リスク入り) (Appendix E-2 参照) 資産管理表 通信フロー図 最新の脆弱性情報	運用フェーズ ・運用実施体制の構築 ・運用実施項目の検討・手順書化 ・教育訓練の実施 ・残留リスクへの対策方針策定 ・運用業務の実施 (脆弱性情報把握・パッチ適用・監視・インシデント対応) ・リスク再評価	運用担当組織 (開発担当組織、設計担当組織) (情報システム・セキュリティ組織、危機管理組織)	運用体制図 インシデント対応フロー 脆弱性対応フロー 緊急連絡網 各種業務手順書 教育訓練マニュアル 脅威想定表 (リスク評価結果・対策要件・対策結果・テスト結果・残留リスク入り) 最新版 資産管理表 脆弱性管理文書

7.2. 運用フェーズの準備 (サポートプロセスの確立)

運用業務を実施するにあたって、体制の確立や業務内容について関連組織間で合意形成が必要である。(図 7-2 中のチェックポイント3)。本項では、その内容について解説する。



引用：ESPR (Embedded System development Process Reference) 2.0
 システム開発プロセス（実線）にセキュリティ関連項目（破線）を追記

図 7-2 運用フェーズ開始時のチェックポイント

7.2.1. 運用担当組織による関連文書(通信フロー図等)のチェック(システム部門のポリシーとの適合性チェック)

ロボット運用管理者は、運用担当組織のシステム管理部門と開発担当組織からのインプットである通信フロー図等をチェックし、運用担当組織内のセキュリティポリシーに適合しているかどうかを確認する必要がある。(チェックポイント3)

運用担当組織が定める主なセキュリティポリシーとしては次のような項目が挙げられる。

- ・データの暗号化
- ・ファイアウォール設定
- ・ローカルサーバ設置個所入退室管理
- ・パスワード管理
- ・疑似攻撃試験内容と結果
- ・セキュリティインシデント発生時対応訓練計画
- ・ウィルス感染対策ソフト
- ・OS 等の修正プログラム対応計画
- ・ログの取得と保管方法

セキュリティポリシーについては、「ロボットとロボット管理サーバ間の無線通信について、インターネット回線を経由するのか」や「ロボットが個人情報や機密情報を送受信するのか」「ロボットを無線通信により遠隔制御するのか」といった条件により組み合わせが異なることもありうる。「個人情報は一切取り扱わない」といったセキュリティポリシーが厳格化するとサービス分野におけるロボットの利活用の妨げとなるケースも想定されるので、運用担当組織においては、システム管理部門を中心に予め組織としての判断基準を定め、定期的な見直しを行うなどの取組みを行うことが望ましい。

7.2.2. 運用レベルのリスクアセスメントと対策方針の策定

ロボット運用担当者組織において、セキュリティインシデントが発生したことにより起きうるリスクについて予め洗い出しを行い、想定されるリスクへの対応について具体的に定めておくことが望ましい。

運用開始後のリスクを想定するためには、ロボットやロボットと繋がるサーバにどのようなデータが送受信され、蓄積されるのかどうかを運用担当組織と設計開発担当組織で共有、確認しておく必要がある。具体的な確認事項としては次のようなものが挙げられる。

➤ ログの管理

情報漏洩防止の観点から、ログの管理について予め決めておく必要がある。例えば、以下の点の考慮が必要である。

- ◇ ロボット本体にログ情報を残さず、センターで処理する
- ◇ 情報の種類によってロボット本体側の情報を消す、消さないをあらかじめ決めておく
- ◇ アプリケーション側に情報を残さない、
- ◇ 電源シャットダウンでメモリ消去する

特に顧客に貸与したデバイス(管理端末・ロボット)内に情報を残すときに注意が必要である。

➤ ロボットの個人情報取得や機密データ保有の有無

ロボットの機能として、個人を特定できるデータ、例えば顔画像データや音声データを取得し保有するかどうかはセキュリティ対策において重要な前提条件である。ロボットの取得情報が設計開発担当組織内のサーバに蓄積されていないかなど、運用フェーズに入る前に確認する必要がある。

➤ 遠隔からのロボットの制御の有無

ロボットを遠隔で監視、制御できる場合は、攻撃により制御機能を喪失する可能性がある。サービス分野で利活用するロボットは、幅広い年齢層の人と空間を共有することから、遠隔からのロボットの監視、制御の有無と攻撃された場合の対策について、運用フェーズに入る前に確認する必要がある。

7.2.3. 運用フェーズの実施体制の構築

運用フェーズの実施体制の構築にあたっては、次のようなポイントに留意する必要があり、その内容について関係組織、関係者間で合意をしておく必要がある。

- 定常的な運用項目と分担の確定
- インシデント対応フロー

設計開発フェーズにおいて、どれだけセキュリティ対策を講じていても、ロボットの運用フェーズにおいてセキュリティインシデントが発生する可能性はある。セキュリティインシデントが発生することを前提に、発生した場合の対応について予め関係者間で定めておくことが望ましい。

◇ セキュリティインシデントが発生した場合(の流れ)

◇ 対応の責任分界点・連絡体制

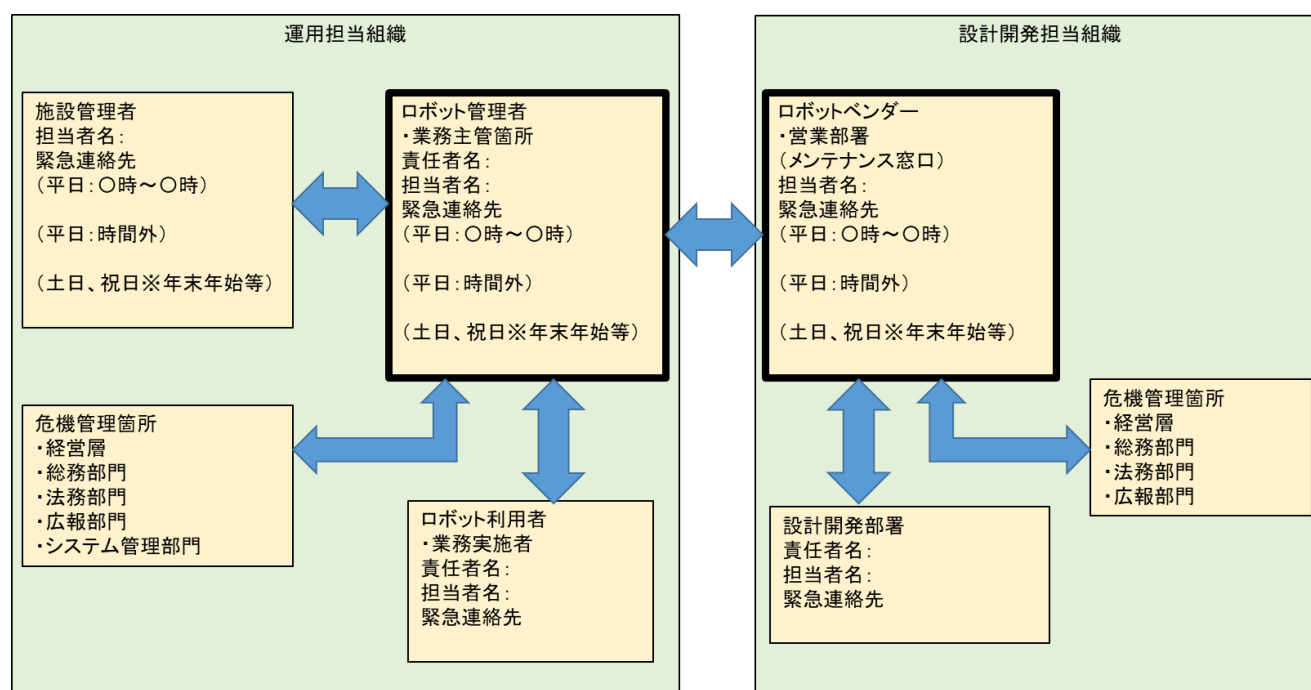
ソフトウェア、ハードウェアのベンダやメンテナンス事業者と作業範囲や責任分界点をあらかじめ明確にしておく

- 緊急連絡体制図(例)

セキュリティインシデント発生時の緊急連絡体制の構築については、発生事象による被害拡大を防止するためにも重要である。サービス分野においては、ロボットが利活用されるシーンがビジネスウィーク(平日)に限られることは少なく、利活用シーンによっては設計開発担当組織が長期休暇期間に該当する際にセキュリティインシデント発生することも想定した緊急連絡体制を予め定めておくことが望ましい。

- また、設計開発担当組織においては、セキュリティインシデント発生時に運用担当組織からの状況報告を踏まえた迅速かつ適切な対応指示を行うためにも、特に平日営業時間外の営業窓口と設計開発部署との緊急連絡体制を予め定めておくことが望ましい。
- 個人情報や機密情報等の漏洩は、時間の経過とともに被害が大きくなることから、関係者間の迅速な連携、一次的対応措置の実施が求められることとなる。担当者変更時の緊急連絡体制更新を確実に行うとともに、各々の担当組織内のみならず運用担当組織、開発担当組織間においても、運用フェーズにおいての定期的な疑似攻撃を想定した緊急連絡体制の確認及び訓練等を実施することが望ましい。

表 7-4 緊急連絡体制表(例)



➤ 脆弱性対応フロー

システムを構成するコンポーネント、例えばファームウェアやソフトウェアに新たな脆弱性が発見された場合も関係者への連絡や対応作業分担をあらかじめ確定するべきである。

◇ 新たな脆弱性が発見・あるいは報告された場合の流れ

関係者への通知(顧客への通知、ベンダへの通知、情報セキュリティ部門への通知)

◇ 対応の作業分担・責任範囲

7.2.4. 運用フェーズの実施項目の設計

運用フェーズにおける業務上の定常的な実施項目などは、手順化しておくことが望ましい。

7.2.5. 運用担当組織における教育・訓練の実施

ロボットの運用フェーズにおいて、実際にロボットを使用する関係者は、ロボットや通信の仕組み、セキュリティに詳しい者ばかりではない。運用担当組織においては、定期的な教育訓練を行うことが望ましい。また、ロボットを使用する関係者だけではなく、経営層においても潜在的なセキュリティリスクや重要インシデント発生時の対応方針についてあらかじめ情報を共有しておく必要がある。

7.9.1. ロボットが保有する情報の漏洩リスクに関する教育

ロボットが保有する個人情報、機密データについて漏洩するリスクについてロボットを使用する関係者に理解させる必要がある。ロボットに限らず、過去の情報漏洩インシデント事例などを通して、ロボットを使用する関係者の故意ではない行動が結果的に情報漏洩インシデントとなるリスクについて教育を行い、ロボットのセキュリティ維持の必要性について意識を高めておくことが望ましい。

7.9.2. インシデント発生時の対応訓練

ロボットがセキュリティインシデントや攻撃などにより、情報漏洩が発生した場合やロボットの制御が不能になった場合などに、全ての関係者が具体的にどのような行動を取らなければならないかを予め整理し、万が一にセキュリティインシデントが発生してしまった場合に備える訓練を日頃から実施しておくことが望ましい。頻度については、ロボットの機能が大幅に変更となった場合や新たにロボットが保有する情報が追加された場合、他組織においてセキュリティインシデントが発生して被害が出た時など、セキュリティに関するロボットを取巻く状況が変化した場合に応じて、適宜実施することが望ましい。

7.2.6. 想定外のセキュリティリスクへの対応方針

設計開発担当組織と運営担当組織において、リスクアセスメントを行い、双方の責任区分、役割を定めたとしても、想定外のセキュリティリスクは残る。それについては、損害保険への加入などで対策を講じることが選択肢として挙げられる。また、インシデントによる被害への賠償として、運用フェーズ実施前に予め保険会社等に相談し、保険の適用範囲、保険料の負担などについて、関係者間で取り決めておくことが望ましい。

7.3. 運用管理業務の実施

7.3.1. 定常業務の実施

脆弱性把握

ロボット運用管理者は運用中のロボットについて脆弱性を把握するとともに関連する情報を収集し、インシデントが疑われるときは必要に応じたサポートプロセスを適用する。運用開始後に顕在化する脆弱性もある。

ソフトウェア・設定情報のバックアップ

監視

定期的に監視すべき項目として、例えば以下が挙げられる。異常を検知した場合に運用管理者が速やかに通報を受け取れるようにすることが望ましい。

- ロボットの測定データ(テレメトリ): 電圧、電流、温度、外力、位置姿勢、速度、カメラ画像など
- ロボットの通信ログ: プロトコル、サービス、通信先 IP アドレス、ポート番号など
- ロボットの動作ログ: 走行軌跡、コマンド実行履歴、成功・失敗履歴、メッセージ履歴など
- ロボットの操作ログ: アクセス、認証成功・失敗記録、ファイルアップロード・ダウンロード、管理者権限(特権)での作業記録、他ロボット・サーバとの相互認証、運用オペレーション記録

これらのデータは情報漏洩防止の観点から、ロボット本体にログを残さない(または情報の種類で消す、消さないをあらかじめ決めておく)、アプリに情報を残さない、電源シャットダウンでメモリ消去する、センターで処理するなどの考慮が必要である。特に顧客に貸与したデバイス(管理端末・ロボット)内に情報を残すときに注意が必要である

監視システムによる監視

システムの規模や内容によって、設計開発組織が専用の監視システムを提供することも考慮する。

7.3.2. 非定常(イベントドリブン)業務の実施

定期または非定期に実施する項目として、例えば以下が挙げられる。

- ロボットOSやインストール済みアプリへのセキュリティパッチ適用と最新バージョンへのアップデート
- 脆弱性、アカウント管理、アクセスコントロール、不要なサービス設定等の検査、パスワードポリシーの見直し
- ロボット内のソフトウェアとシステムの設定情報ファイルのバックアップ、バックアップ媒体の保管、バックアップから復元できることの検査
- セキュリティインシデントの予防保守、点検、新たな脅威の洗い出し

運用中はこれらの項目を漏れなく実施するための手順書の作成、作業記録の管理、教育、複数の責任者によるチェック体制の整備が必要である。

対策・パッチ適用

その他、運用フェーズにおけるセキュリティ対策技術について列挙する。想定される脅威と実現コスト、難易度、残留リスクを考慮し適切な対策を組み合わせで適用することが重要である。

- 不正アクセス対策: 多要素認証(例: パスワードとバイオメトリクスとの組み合わせ)、権限管理(例: 認証・認可プロトコル)、ゼロトラスト、アカウントの紐づけ、境界防御

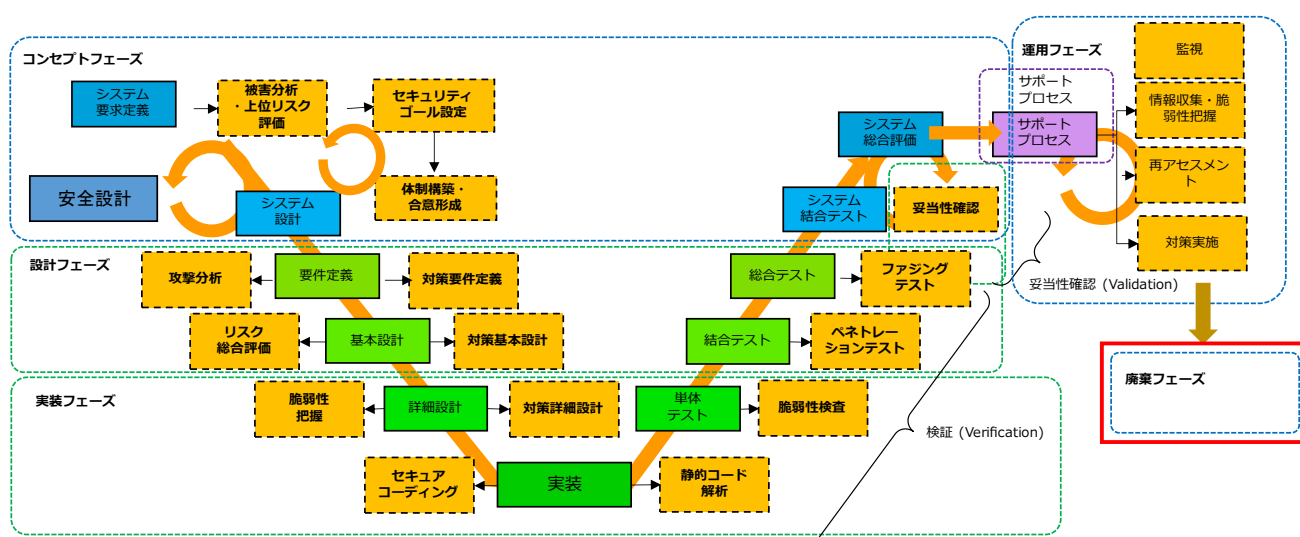
- 情報漏洩対策:通信の暗号化(脆弱性の判明した暗号化方法は使用しない)、専用線、電話回線利用による音声や映像伝送、難読化、平文コードの禁止、ファイル名ランダム化、遠隔デバイスロック
- 改竄対策(システム、ファイル、テレメトリ):検知ツール導入(例:Rkhunter、chkrootkit、WebArgos)、ログローテート、システムバックアップ or システムの自動構築手法の導入(Docker, chef, etc.)、ハッシュ値保存、ストレージのアクセスログ記録、電子署名による送信元ロボットの識別
- 物理的対策:CPU/ディスクのロック、防犯ロック・特殊ネジの使用、Kidnap 対策(警報、位置情報通知、リモートディスク消去)、人感センサ・アラーム設置、フールプルーフ、自然災害・経年劣化への備え、過昇温防止、外気温モニタリング、監視カメラ
- 不正機器接続対策:検知ツール(不審なデバイス追加・削除時に通知、停止)、経路異常検知、物理ポートを塞ぐ、ネットワーク機器・配線の隠蔽
- 脆弱性対策:ペネトレーションテスト・ファジングテスト用ツール
- 稼働率対策(インシデントからの迅速な復旧):バックアップ、多重化

7.3.3. 再アセスメントの実施

運用中にセキュリティインシデントが発生した場合や、ロボットシステム構成の変更があった場合などには対処完了後に再度リスクアセスメントを実施する。それによって、導出された受容できない、あるいは対策を講じなければならないと判断される事項の洗い出しと、その対策の見直し(場合によっては対策手順の見直しも含む)を実施する。その際にはシステムの改善・変更によって「新たな脅威・リスクが生まれていないか」、「残留リスクが増大していないか」の観点で構築後のセキュリティ残留リスクトレースを実施し残存セキュリティリスクを運用上で対策することで低減する。また実施状況を定期的にレビューすることが望ましい。

8. 廃棄フェーズ

本章ではロボットを廃棄する際にセキュリティ上課題となる可能性のある事項を挙げ、必要となる対策・実施事項に関して述べる。なお、ここでは広く2.1節で述べたロボットシステム全般を対象としているが、廃棄対象はロボットの動作に直接関わる全システムを廃棄する想定ではなく、システム内のある1台のロボットを、何らかの理由によりシステムから除外し、廃棄する場合を想定している。



引用：ESPR (Embedded System development Process Reference) 2.0
システム開発プロセス（実線）にセキュリティ関連項目（破線）を追記

図 8-1 ライフサイクルにおける廃棄フェーズの位置づけ

また、ここでは「廃棄」はより広く「使用を中止する」ととらえ、例えばレンタル・リース品の返却時や、ロボットを下取りに出すようなケースも合わせて考察する。

現在用いられている多くのロボットは PC やタブレット端末等と同様に情報機器であり、ストレージデバイス（ディスクやメモ리카ード等）を備えるものも多い。廃棄の際にそれらのストレージデバイスのみが再利用されるといったケースも考慮されなければならない。さらに、移動ロボットなどがゲートやエレベータ等を通る際、ID チップやバーコードのような物理的な手段でロボット自身が認証を受けているケースもある。以下、それぞれの観点で課題と対応策について紹介する。

8.1. 想定される利害関係者

ロボットを廃棄する際、主たる利害関係者は当該ロボットの所有者である。それ以外の関係者としては、当該ロボットを商品化し製造・販売を行ったロボットメーカ、また使用を中止したロボットを第2のユーザ(新所有者)が新たに所有して活用する場合、新所有者においても何らかのセキュリティ上の問題が発生する可能性がある。

8.2. 廃棄の形態 — 物理的破壊とソフト処理による消去 —

ロボットを廃棄する際、下取りやレンタル期間の終了の場合を除き、セキュリティ上好ましい処理はストレージデバイス(ディスク)を物理的に破壊することである。しかし、ロボットの所有者がストレージデバイスを取り外して破壊することは多くの場合簡単ではないと思われる。

PCの場合は 一般社団法人電子情報技術産業協会(JEITA)の「PCの廃棄・譲渡時におけるHDD上のデータ消去に関する推奨方法」として、

ケース1:PCとディスクが稼働する場合

ケース2:PC本体は稼働しないが、ディスクは稼働する場合

ケース3:ディスクが稼働しない場合

について考察されており、ディスクが稼働しないならば物理的破壊、稼働するならば専用ソフトもしくは専用装置にてデータ消去することが推奨されている。

参考:「データ消去技術 ガイドブック」 データ適正消去実行証明協議会 消去技術認証基準委員会

<https://adec-cert.jp/guidebook/pdf/DATAWIPEGUIDEBOOK.pdf>

セキュリティ上考慮すべき情報を内部に保持するロボット製品の場合、ロボットメーカーは廃棄の際のセキュリティ上の作業手順をマニュアル等で開示することが望ましい。また所有者は廃棄の際に安全にストレージデバイスを消去・破壊する手段があることを事前に確認することが望ましい。

物理的破壊ではなくソフト処理でストレージデバイス上のデータを消去する場合、「本当に消去されていること」「データの復元手段がないこと」が望ましい。ただし、より安全な消去にはよりコストがかかるため、どのレベルの処理を行うべきなのか、適切な判断が求められる。（詳しくは「データ消去技術 ガイドブック」を参照されたい）

特にレンタル・リース品の返却の際や下取りに出すような場合、消去処理そのものを他者に委託する場合も想定される。そういった場合には、万一の情報漏洩事故等の発生の際の責任や補償などを契約等で担保しておくことも大切である。

8.3. ロボットが保有・活用する情報のうちセキュリティ上考慮すべきもの

本節では、上記の物理的破壊やデータ消去が適切に行われず、情報がロボット内に残ってしまった場合にどのようなリスクがあるか？とその場合の対策を考察する。

8.3.1. そのロボットの個体自身のシステム内での認証情報

廃棄されるロボットは何らかの通信路でネットワーク的にシステムに接続していたであろう。ロボットを廃棄する場合、ネットワーク側でそのロボットの登録情報を削除もしくは更新し、廃棄後に何者かがそのロボットになりすましてシステムにアクセスした場合、異常を検知できることが望ましい。

また、ID チップや ID カード、バーコードのような物理メディアで移動ロボットのゲート通過などを管理するシステムの場合、ロボットを廃棄した際には全体システム側で適切に権限の更新を行うとともに、廃棄の際には確実にそれらの物理媒体を適切に処分する必要がある。

8.3.2. ロボットが個体内にローカルに保有する情報

○ 個人情報

特にサービス系のロボットの場合、顧客の個人情報に基づいて顧客を識別して適切に対応したり、情報を提供したりする場合がある。このような個人情報・顧客情報は一般にロボット個体内ではなくシステム側にマスタデータを持つことが多いが、一時的にロボット個体内に保持する場合もある。そういった情報が廃棄後に取り出せてしまうと、個人情報の漏洩につながる可能性がある。そのためロボットが個体内ローカルに保有する個人情報については、完全に削除・廃棄すること、また、物理的破壊、ソフト処理等、どのような手法で情報を削除・廃棄したか？について記録を残す必要がある。

○ 組織や資産に関する情報

移動ロボットにおけるフロアマップの情報なども、場合によっては機密情報となることがある。

また、産業用ロボットにおいて、ハンドリングする対象物の情報などを個体内(ロボットコントローラ内)に保持することもある。これらの情報は、営業上極めて機密性が高い情報である場合もあり、流出すると営業上大きな損害となることがあり、その扱いについてはあらかじめ顧客と扱いの方針を定め、その方針にしたがって廃棄も行う必要がある。

また、何らかの有償のソフトウェアなどのライセンス情報がそのロボット個体に紐づいて設定されている場合もある。その場合はそのソフトウェア資産の紐づけを適切に変更する。

○ ロボットのミッションや業務遂行上必要となる情報

ロボットが実際に動作するために必要な設定や動作プログラムなどがある。これらはロボットを導入して使用している所有者(ユーザ)が作成、設定したものもあれば、ロボットメーカーがあらかじめ準備してロボットに搭載している場合もある。これらの情報も、機密情報に該当する場合がある。

ユーザが作成したプログラム等は確実に消去することが望ましい。一方、レンタル・リースや下取りのような再利用を想定した場合、消去すべきでない情報もある。その場合は暗号化等の手段が選択されることが多い。

また、多くの製品において「工場出荷時に戻す」機能が準備されているが、この機能がある場合、確実に実行するようにする。

8.3.3. レンタル・リース品やリユース品を利用する際の注意点

○ 導入時

素性のわからない製品は用いない、というのが大前提である。「トロイの木馬」「バックドア機能」などが設けられているリスクを考慮する。使用しないポートは塞ぐ等の対策、通信路を監視・モニタして異常を検知する仕組みの導入等を検討する。ただしこれらはコストとの兼ね合いになるため、適切なレベルの対応をとる。

○ 返却・下取りの時

通常は物理的に破壊するという手段が取れないため(ストレージを新品と置き換えるという手段が取れる場合もある)、確実に消去し、初期状態に戻すことが基本である。

あとがき

本ガイドラインを作成するにあたって特に意識したことは、ロボットは成長分野であるということである。

コロナ禍の影響も加わり、サービスロボットは急速に実証から実用のステージへと進みつつあり、運搬、配膳、清掃、受付、警備、消毒などはじめと多岐にわたる分野へ活動の場を拡大している。一方工場内では、人と作業空間を共有する人協働型ロボットも普及し、ロボットは工場の柵の中にとどまらず工場内の搬送などまで含めてその活動範囲を拡大しつつある。

このようなロボットの事業としての成長の可能性を阻害せず、事業の成長と継続に必要なアイテムとして本書はロボットセキュリティを捉えている。

本版(Ver2.0)に先立ち、RRI-WG3(ロボットイノベーションワーキンググループ)関係者に向けて内部リリースした前版(Ver1.0)では、ロボットセキュリティに関する技術的な検討の流れやポイントの解説に中心を置いた。しかし、実際にその作業を実行するには、組織間の合意形成や責任分担などのマネージメント的な視点も非常に重要な課題であり、本版では、そのマネージメントに関連する内容を大幅に拡充した。

ロボットをめぐる技術もビジネスも今後更に進化・成長を続けるとともに、新しい業種や職種、さらにはビジネスモデルが現れる可能性も秘めている。したがって、本書の中で例として取り上げているステークホルダの組織の枠組みは、それを固定的な枠とは捉える必要はなく、自社や自組織の環境や立場に読み替えて柔軟に考えていただきたい。

ロボットの導入や実用に関してセキュリティ面の不安を抱えている事業者、さらには、これからロボットのビジネスに新たに取り組もうとしている事業者の方々にも本書が参考になれば幸いである。

また、本ガイドラインの中で提示した技術的内容やフレームワークもまだ完全に成熟しきったものとは言えない部分もある。読者の皆様の現場で本書を活用いただきながら、内容を更に磨きあげていきたいと考えている。忌憚なきご意見やコメントをいただければ幸甚である。

APPENDIX A. 関連規格

APPENDIX A-1. 主な関連規格と本書との関係性

ロボットに関連するところでは、IoTに関連する規格、セーフティに関連する規格、産業用制御システムのセキュリティに関する規格、ガイドラインなどが各種団体から発刊されている。また、サイバーセキュリティ・クラウドセキュリティに関しては、ISO27001、ISO/IEC 27017などの規格が存在する。下表は、主な関連規格に関して本書との違いや特徴についてまとめたものである。

表 A1-1 関連規格と本書との関係性

分類	関連規格	内容・特徴	本書の立場
IoT関連ガイドライン	IPA “つながる世界の開発指針”	あらゆるIoTシステムを対象にしている。開発から運用までのライフサイクル全体を考慮している	・ロボットシステムにフォーカスしている ・エンドデバイスだけでなくシステム全体のつながりを考慮する点は継承している ・企画～廃棄まで含めたライフサイクル全体を考慮している
セーフティ・安全規格	ISO12100 IEC61508 ISO13482	機械、電気に関わる安全規格。誤動作、事故、悪環境からの保護を指向している。悪意ある攻撃からの保護という視点ではない。	安全規格に従う前提で、安全機能へのセキュリティ侵害、セキュリティ対策によるセーフティの影響などの相互影響について言及している
制御系セキュリティ	IEC62443-1~4	・工場内の制御システムに関して、全般、ポリシーと手順、システム、コンポーネントから構成される ・セキュリティ要素は、可用性>完全性>機密性という優先順位を前提としている。 ・ロボットは制御システムの1コンポーネントとして扱われている ・対象としているロボットは限定的であり基本は人から隔離された制限区域で動作し専門教育を受けた運用者がいることを前提としている。移動ロボットや人との協働ロボットまでは想定されていない ・技術的な防御策はネットワークのゾーニングによる境界防御を中心にしている。	・制御システム以外のロボットも扱う ・セキュリティ要素の優先順位は、ユースケースによって異なることを前提としている。 ・境界防御は対策の1手段としている
情報システム・クラウド関連規格	ISO27001 ISO/IEC 27017	ICT機器、ICTシステムを対象にしている。IoTなど情報通信以外の機能を持つ機器、動力を持つ機器のことは想定されていない	ICTシステムに関する考え方は継承。情報資産だけでなく物理資産や環境も含めてロボットシステムのセキュリティを考慮する立場をとっている。

APPENDIX A-2. セーフティ・セキュリティ相互関係に関する規格

セーフティとセキュリティの相互影響を分析・評価する手法は、セーフティを検討してからセキュリティとの相互影響を検討する、セーフティとセキュリティを並行して検討するなどいくつかの手法がロボットに限らず提唱されている。第5章の説明でもあげたが、セキュリティ対策についても自動車における取組みがロボットにおいても参考になるため、これらの状況を鑑みて、安全性とセキュリティの確保(特に security for safety)についてセーフティとセキュリティとの相互関係に関する規格を紹介する。

ISO-TR22100-4

一般的な枠組みとして、ISO TR22100-4 において提唱されている事項について説明する。

セキュリティを考える前に、リスク評価を ISO12100 に基づいて実施する。導出された安全対策(3ステップによる)に対して、セキュリティ脅威を分析する(潜在的な脆弱性の分析)。つまり、まず、安全性について従来通りリスクアセスメントを実施して、安全上必要と導出された安全対策に対して、セキュリティを考えるとどのような問題があるのかについて分析をすることを要求している。セキュリティ上の対策を施さないと、それを攻撃起点として安全対策が機能しなくなり、安全を脅かす、リスクにさらされるため、そうならないためのセキュリティ対策を脅威分析により、コンポーネントレベル、機器レベル、システムレベル、運用レベルなど複合的に軽減するための対策を実施する。セキュリティ対策の原則としては、設計によりセキュリティリスクを排除する: Security by Design を採用して、脅威分析により明らかとなった脆弱性に対して対策を施すことでセキュリティリスクを低減する。その上で、残存セキュリティリスクに対しては運用上で対策することで低減することによりトータルにセキュリティ対策を施す。つまり、様々なレベルに応じたセキュリティ対策を考える必要がある。これを多重防護という。また、セキュリティ脅威に対する脆弱性はシステムが外部とどのように接続しているかに依存するため、外部との接続に重点をおいた分析が必須となる。分析では攻撃者の視点からシステムへの侵入を考えると良い。また、ロボット内部における通信・データの流れとセキュリティ上重要な箇所についても各レイヤにおけるセキュリティ分析を行い、必要な対策を施す必要がある。

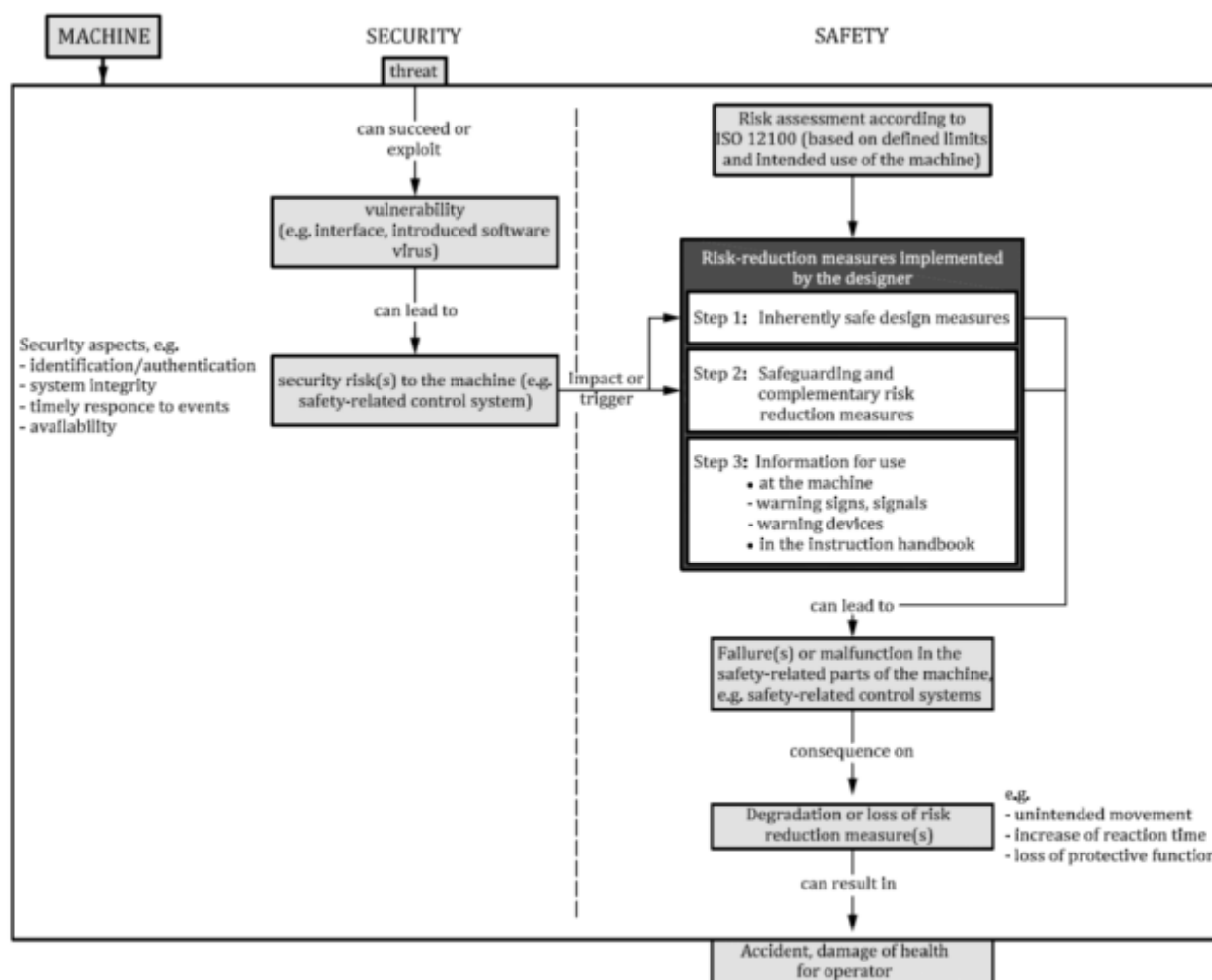


図 A2-1 機械安全と IT セキュリティとの関係
(ISO-TR22100-4 よりの引用)

IEC TR63069、IEC63074

まず安全対策を考え、その上で安全対策のセキュリティ分析を実施し、セキュリティ対策により、結果的に安全性を確保する手法については IEC63074 にも踏襲されている。一方で IEC TR63069 においては安全性とセキュリティを並行して分析して対策を講じるためのプロセスを考えており、こちらは IEC61508 と IEC62443 の融合を念頭ににしたプロセスといえる。このような、安全性とセキュリティの融合に関する研究は航空分野や自動車などで先んじて 2000 年代初頭より研究されており、日本では IPA から 2013 年に発行された「IC カードを用いた社会情報基盤システムに

おける、安全性とセキュリティの同時認証に関する実証実験」に関する実施報告書が ISO/IEC 15408 (Common Criteria) と IEC61508 の融合について論じた最初の報告書であると思われる。

ロボットに対しても、安全性のためのセキュリティとしては、ISO TR22100-4 で提唱されているように、先ずはリスクアセスメントを実施して安全対策を決定して、それぞれのステップで導出・決定した安全対策のセキュリティ上の脆弱性を診断し、対策をすることでセキュリティ侵害による安全対策の機能不全を防ぐ方法は有効であると考ええる。一方で、あらかじめロボットに対して、どのような外部への接続が想定されているのか、ロボット内のネットワークなどデータの流れがどうなっているのかについて十分な分析がなされているのであれば、始めにセキュリティ対策を考えたいうえで、その制約下で安全対策を考えることも必要であると思われる。いずれの方法にしても、抜け漏れなどがないように十分な分析と分析結果を受けた対策の十分性が要求される。

APPENDIX B 参考文献

第1章

- [1] 日本規格協会, ”JIS Q 13335-1:2006 (JSO/IEC 13335-1:2004), 情報技術 – セキュリティ技術 – 情報通信技術セキュリティマネジメント – 第 1 部:情報通信 技術セキュリティマネジメントの概念及びモデル”, <https://kikakurui.com/q/Q27000-2014-01.html>
- [2] 日本工業規格: JIS B 0134:2015 (ISO 8373:2012) ロボット及びロボティックデバイス—用語 Robots and robotic devices-Vocabulary, 2015, <https://kikakurui.com/b0/B0134-2015-01.html>
- [3] 日本工業規格: JIS B 0186:2020 (ISO 19649:2017) 移動ロボット—用語 Mobile Robot – Vocabulary, <http://www.kikakurui.com/b0/B0186-2020-01.html>
- [4] 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: “サービスロボット・セキュリティガイドライン第 1 版”, 2019, <https://rtc-fukushima.jp/technical/3170/>
- [5] 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>
- [6] 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>
- [7] 日本工業規格 “JIS Q 27001:2014 (ISO/IEC 27001:2013) 情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項” <https://kikakurui.com/q/Q27001-2014-01.html>
- [8] International Organization of Standards, “ISO/SAE 21434 Road Vehicles -Cybersecurity engineering”, 2021

- [9] International Electrotechnical Commission, “IEC61508 Ver2.0”, 2010. (機能安全)
<http://www.iec.ch/functionalsafety/standards/page1.htm>
- [10] International Organization of Standards, “ISO13482”, 2014.
https://www.jqa.jp/service_list/fs/service/13482/
- [11] ロボット革命・産業 IoT イニシアティブ協議会, “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.jmfri.gr.jp/content/files/Open/2016/SWG2GL.pdf>

第2章

- [12] Amazon Web Service, “AWS 責任共有モデル”
<https://aws.amazon.com/jp/compliance/shared-responsibility-model/>
- [13] ロボット革命・産業 IoT イニシアティブ協議会, “自律型生活支援ロボットの 安全開発ガイド Ver1.0”, 2020, <https://www.jmfri.gr.jp/followup/1453.html>
- [14] ロボット革命・産業 IoT イニシアティブ協議会, “オープンソースを活用したロボット開発のためのライセンス・特許ガイドライン”, 2019, <https://www.jmfri.gr.jp/followup/1455tml>
- [15] ロボット革命・産業 IoT イニシアティブ協議会, “ロボットシステム開発における OSS 利用の品質保証ガイドライン”, 2020, <https://www.jmfri.gr.jp/followup/1459tml>

第3章

- [16] 独立行政法人 情報処理推進機構 “組み込みソフトウェア向け開発プロセスガイド”, 2007,
<https://www.ipa.go.jp/files/000005126.pdf>
- [17] 独立行政法人 情報処理推進機構, “OSS ライセンス遵守活動のソフトウェアライフサイクルプロセスへの組み込み”, <https://www.ipa.go.jp/files/000029079.pdf>
- [18] 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>

[19]日本規格協会,"JIS Y 1001:2019 -サービスロボットを活用したロボットサービス の安全マネジメントシステムに関する要求事項",2019

第4章

[20]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>

第5章

[21]Microsoft Docs,"Threat Modeling Tool の概要[1]" ,

<https://docs.microsoft.com/ja-jp/learn/modules/tm-introduction-to-threat-modeling/>

[22]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>

[23]International Organization of Standards, ISO12100 (機械安全)

http://www.jmf.or.jp/japanese/standard/pdf/N_3.pdf

[24]独立行政法人情報処理推進機構, “制御システムの安全とセキュリティの両立”

<https://www.ipa.go.jp/files/000062794.pdf>

[25]独立行政法人情報処理推進機構, “共通脆弱性評価システム CVSS v3 概説”,2015

<https://www.ipa.go.jp/security/vuln/CVSSv3.html>

[26]V´ictor Mayoral Vilches,Endika Gil-Uriarte,Irati Zamalloa Ugarte,Gorka Olalde Mendia,Rodrigo Izquierdo Piso´n,Alejandro Hern´andez Cordero Alias Robotics S.L.,Lucas Apa and Ce´sar CerrudoIOActive Inc., “TOWARDS AN OPEN STANDARD FOR ASSESSING THE SEVERITY OF ROBOT SECURITY VULNERABILITIES, THE ROBOT VULNERA- BILITY SCORING SYSTEM (RVSS).”,2021

<https://arxiv.org/pdf/1807.10357.pdf>

[27]JVN iPedia,“脆弱性対策情報データベース”,2022,

<https://jvndb.jvn.jp/index.html>

[28]International Organization of Standards, “ISO15408 CommonCriteria”

[29]International Organization of Standards ISO-TR22100-4 Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects,(発行年)

<https://www.iso.org/standard/73335.html>

[30]International Electrotechnical Commission, “IEC-TR63069:2019 Industrial-process measurement, control and automation - Framework for functional safety and security”,2019

<https://webstore.iec.ch/publication/31421>

[31]International Electrotechnical Commission, “IEC63074:2021 Safety of machinery - Security aspects related to functional safety of safety-related control systems”,2021

<https://webstore.iec.ch/publication/31572>

第6章

[32]JPCERT,“制御システムセキュリティ自己評価ツール(J-CLICS)”,2017

<https://www.jpCERT.or.jp/ics/jclics.html>

[33]荻野 司、伊藤公祐、小野寺 正著、一般社団法人 重要生活連携機器セキュリティ協議会編、株式会社インプレス発行, ”押さえておくべき IoT セキュリティ”,2018

[34]AINow 誌, “危険にさらされる AI -増大する AI セキュリティ の重要性”, 2020

<https://ainow.ai/2020/07/22/226210/>

[35]独立行政法人情報処理推進機構,“つながる世界の品質確保に向けた手引き”～IoT 開発・運用における妥当性確認・検証の重要ポイント”,2018,

<https://www.ipa.go.jp/files/000064877.pdf>

[36]一般社団法人 重要生活機器連携セキュリティ協議会, “IoT セキュリティ評価検証ガイドライン _rev1.0”,2017

[37]IoT 技術コラム,サイバートラスト社, “Root of Trust とは？その定義と用途”,2021,
<https://www.cybertrust.co.jp/blog/iot/techinfo/root-of-trust.html>

[38]National Institute of Standards and Technology, "NIST SP 800-171 Rev2",2020,

第7章

[39]経済産業省 商務情報政策局, “サイバー・フィジカル・セキュリティ対策フレームワーク”,2019,
<https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf>

[40]総務省, “スマートシティセキュリティガイドライン 第 2.0 版”,2021,
https://www.soumu.go.jp/main_content/000746734.pdf

[41]International Organization of Standards,International Electrotechnical Commission, “ISO/IEC 30147 Edition 1.0 ~ Internet of things (IoT) – Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes”,2021

[42]National Institute of Standards and Technology, "NIST SP 800-61 Rev2 -Computer Security Incident Handling Guide",2012,<http://dx.doi.org/10.6028/NIST.SP.800-61r2>

[43]経済産業省,独立行政法人 情報処理推進機構, “サイバーセキュリティ経営ガイドライン Ver 2.0”,2017,
<https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf>

第8章

[44]データ適正消去実行証明協議会 消去技術認証基準委員会, “データ消去技術 ガイドブック 第 2.3 版”,2020
<https://adec-cert.jp/guidebook/pdf/DATAWIPEGUIDEBOOK.pdf>

APPENDIX C 対策事例

APPENDIX C-1. 代表的な脅威と対策実施例

表 C1-1. 全般的な対策事例

脅威の種類	対策技術・手法	実施するフェーズ
全般	パッチ適用	実装・運用
	ファームウェア更新	運用
	セキュアプログラミング	実装
	プログラム中に機密情報をハードコードせず、公開可能なプログラムしかデプロイしない	設計・実装
	OS、ソフトウェアの脆弱性情報の定期収集	実装・運用

表 C1-2. 代表的な脅威への対策事例

脅威の種類	対策技術		実施するフェーズ
分類	手法	詳細	
不正侵入	ノードレベルの対策	不要なサービス停止、不要なポートを閉じる	実装
		デフォルトポートの変更 ・ROS master、RTM ネームサービス等のデフォルトポートが決まっているサービスのポート番号の変更 ・Web サービス(80, 443, 8080 等)、MQTT(1883, 8883) など決まっているポート番号を避ける	実装
		SSH のログイン制限 ・公開鍵のみ使用、ポート番号変更、 ・ホワイトリスト以外から通信遮断、 ・ログイン時通知(メール, Slack, etc..)	実装
	通信ネットワークの対策	ホワイトリスト型ファイアウォール、アクセスログの記録 対象ノードの固定 IP 化、FW 設定による不要なポートとの通信拒否設定	実装・運用
		通信・無線暗号化(脆弱性の判明した暗号化方法は使用しない)	設計・実装
		専用線、closed ネットワークの利用	設計・実装
		Web サービス系の WAF による制限	実装・運用
		リモートログインは踏み台サーバを経由する	実装・運用
		ネットワークのゾーニング(ロボットネットワークとその他のネットワークの分割統治、境界防御)	設計・実装

脅威の種類	対策技術		実施するフェーズ
	手法	詳細	
不正侵入 (続き)	認証	ID/パスワードの複雑化	設計・実装
		公開鍵認証	実装
		多要素認証	実装
	侵入検知	ウィルス対策ソフト、rootkit 対策ソフトの設置	実装
		IDS/IPS (Intrusion Detection/Prevention Systems, swatch/snort 等)の設定	実装・運用
		決まったノードしか許可せず、unknown ノードを検出し通知するシステムの導入	実装・運用
		音声や映像伝送を通常の電話回線を利用する	運用
情報漏洩	盗難、盗聴による機内データ漏えい	通信の暗号化、平文コードの禁止、ファイル名ランダム化などの運用ルール策定	実装・運用
	ロボット内の個人情報(画像等)の扱い	ロボット内のメモリ上でのみ扱いデータは上位システムへ転送して保存	実装・運用
	通信暗号化	インターネットを経由する AMQP や HTTP による通信は、TLS による暗号化を行う	設計・実装
	キーの漏洩防止	電磁ロックに接続されている Raspberry Pi の SD カードに暗号化ボリュームを作成し、開錠キーのリストは暗号化ボリュームに配置することで、SD カードを取り出されて電磁ロック開錠キーが漏洩することを防ぐ	設計・実装
誤操作	意図的な、または人為ミスによる誤動作(急発進など)	入力値、指令値の閾値設定によるリアルタイム監視	運用
	複数人、複数端末による処理競合	限られた人のみが操作できる仕組み(端末認証&個人認証)	設計・実装
	障害、クラッシュや非常停止から復旧時の危険性(二次被害)	自動復旧、または電源 OFF で手動操作できる機構	設計・実装

脅威の種類	対策技術		実施するフェーズ
	手法	詳細	
改竄	システム改竄検知	Rkhunter, chkrootkit 等 rootkit 検知ツールの導入	実装
		ログ保存、ログローテート上の工夫、定期的回収・監査	運用
		システムバックアップ or システムの自動構築手法の導入 (Docker, chef, etc.)	実装・運用
	ファイル改竄検知	ファイルシステムの改竄検知ツールの導入	実装・運用
	テレメトリ改竄検知	テレメトリや周辺画像のハッシュ値の保存 ・データベースにはロボット管理プラットフォーム専用のアカウントを作成し、そのアカウントには Insert 権限しか付与しないことで、たとえロボット管理プラットフォームのプログラムにバグがあったり改竄されてしまったりしても、記録の改竄を防ぐ	実装・運用
		テレメトリや周辺画像のハッシュ値を保存するデータベースの監査ログを記録することで、不正な操作を検知できるようにする	実装・運用
		周辺画像を保存するストレージのアクセスログを記録することで、不正な操作を検知できるようにする	運用
		個々のロボットに個別の秘密鍵をインストールし、全てのテレメトリにその秘密鍵で電子署名を行いそのハッシュ値もテレメトリと同時に記録しておくことで、テレメトリの送信者が当該ロボットであることを保証する	実装・運用
物理対策	CPU/ディスク対策	CPU/ディスクのロック(物理的、施錠など)	実装
		CPU/ディスク周辺のトルクスネジ、特殊ネジの使用	実装
		ディスクの暗号化・難読化	実装
		重要情報・動作時取得情報の RAM ディスク配置	設計・実装
		Kidnap 対策(警報、位置情報通知、リモートディスク消去)	設計・実装
	物理侵入対策	荷物室に電磁ラッチを取り付け、登録済みの NFC カードを持つ人のみ荷物室を開けられるようにする	実装
	不正機器接続	不正機器接続防止(不審なデバイス追加・削除時に通知、停止等)	実装・運用
	盗難防止・経路異常検知	ロボットは常に一定周期で自己位置をロボット管理プラットフォームに通知し、運行経路から著しく離れた位置情報が報告されてきた場合には、ロボットが鹵獲されたと見なして緊急処置を行う	実装・運用
		持ち上げたり、域外に出たりするときにアラーム、センサー側で検知できる仕組みの実装	実装・運用

脅威の種類	対策技術		実施する フェーズ
分類	手法	詳細	
物理対策 (続き)	CPU/ディスク対策	CPU/ディスクのロック(物理的、施錠など)	実装
		CPU/ディスク周辺のトルクスネジ、特殊ネジの使用	実装
		ディスクの暗号化・難読化	実装
		重要情報・動作時取得情報の RAM ディスク配置	設計・実装
		Kidnap 対策(警報、位置情報通知、リモートディスク消去)	設計・実装
	物理侵入対策	荷物室に電磁ラッチを取り付け、登録済みの NFC カードを持つ人のみ荷物室を開けられるようにする	実装
	不正機器接続	不正機器接続防止(不審なデバイス追加・削除時に通知、停止等)	実装・運用
	盗難防止 ・経路異常 検知	ロボットは常に一定周期で自己位置をロボット管理プラットフォームに通知し、運行経路から著しく離れた位置情報が報告されてきた場合には、ロボットが鹵獲されたと見なして緊急処置を行う	実装・運用
		持ち上げたり、域外に出たりするときにアラーム、センサー側で検知できる仕組みの実装	実装・運用

APPENDIX C-2 時系列でのセキュリティ対策実施事項(例)

	コンセプト	設計	実装	運用	廃棄
全般	セキュリティ ゴール・ポリ シーの策定	脅威分析・リス ク評価	・セキュアプログ ラミング	・パッチ適用 ・ファームウェ ア更新 ・脆弱性情報 の定期収集	
不正侵入		・アカウント設 計 ・ネットワーク のゾーニング の設計 ・通信回線の 選択 ・認証・認可機 構の設計	・アカウント管理 実装 ・不要サービス・ ポートの停止 ・デフォルトポ ート番号の変更 ・認証・認可機構 の導入 ・ネットワークの ゾーニング ・アクセス制限 ・専用線の利用 ・踏み台サーバ の設置 ・IDS/IPS の設置 ・ノードレベルの アクセス制限・認 証・認可	・アカウント管 理 ・アクセスログ の記録・監視 ・IDS/IPS によ る監視	アカウント削除
なりすまし		・認証・認可機 構の設計	・認証・認可機構 の導入 ・ID/パスワードの 複雑化 ・公開鍵認証 ・多要素認証	・アクセスログ の記録・監視 ・公開鍵の管 理	—

続き

	コンセプト	設計	実装	運用	廃棄
改竄		<ul style="list-style-type: none"> ・データのバックアップ設計 ・セキュアブート導入の検討 ・改竄検知機構の検討 ・メッセージ認証、デジタル署名の検討 	<ul style="list-style-type: none"> ・データのバックアップ機構の実装 ・セキュアブートの実装 ・ストレージの暗号化・ハッシュ値の保存 ・ログの暗号化 ・改竄検知機構の導入 ・メッセージ認証・デジタル署名の検討 	<ul style="list-style-type: none"> ・ストレージの暗号化・ハッシュ値の保存 ・ログの暗号化 ・改竄検知機構の運用 ・デジタル署名の運用 	
情報漏洩		<ul style="list-style-type: none"> ・通信の暗号化方式の検討 暗号鍵の管理 キーの漏洩防止 ・ノード・ファイル・トピック等の識別子の命名ルールの検討 	<ul style="list-style-type: none"> ・通信の暗号化 ・音声、画像は通常の電話回線経由とする ・セキュアコーディング ・類推しやすい識別子のデフォルト値からの変更 	<ul style="list-style-type: none"> ・ファイル名のランダム化 ・平文コードの禁止 	アカウント情報 製品情報 等削除

続き

	コンセプト	設計	実装	運用	廃棄
物理攻撃		<ul style="list-style-type: none"> ・物理脅威（盗難対策等）への対処方法の検討 	<ul style="list-style-type: none"> ・CPU・ディスクのロック ・トルクスネジ、特殊ネジの使用 ・ディスクの暗号化・難読化 		
誤操作		<ul style="list-style-type: none"> ・操作端末・操作者の認証方法の検討 ・入力値、指令値のしきい値設計 ・障害・クラッシュ・非常停止から復旧時の危険性への対処方法の検討 	<ul style="list-style-type: none"> ・操作端末・操作者の認証機構（顔・指紋認証など）の導入 ・入力値、指令値のしきい値設定 ・自動復旧、または電源OFFで手動操作できる機構の導入 	<ul style="list-style-type: none"> ・操作端末・操作者の認証機構の運用 ・入力値、指令値のしきい値の監視 ・クリティカルな操作はオフラインで実行 	

APPENDIX. D テストツール類

大分類	小分類	目的	ツール例	入手方法
基本ツール	ポートスキャン	・通信ポートの開閉のチェック	・netstat, sockstat ・nmap、zenmap	Linux の OS の中に Bundle
	パケットキャプチャ	・通信内容の漏洩チェック ・暗号化対策等のチェック	Fiddler (HTTPS 通 decrypt&analysis) Wireshark	https://www.telerik.com/download/fiddler https://www.wireshark.org/download.html
	ID・パスワード脆弱性 チェック	ID・パスワードの強度の チェック	IPA パスワードチ ェック	https://www.ipa.go.jp/chocotto/pw.html
	静的コード解析	・コーディング規約への準拠 のチェック ・コードに内在する脆弱性の チェック	Coverity	https://www.synopsys.com/ja-jp/software-integrity/security-testing/static-analysis-sast.html
脆弱性検査	OS、ミドルウェアの脆弱性の チェック	脆弱性スキャナ	OpenVAS	https://sectools.org/tool/opensasl/
			Vuls	https://github.com/future-architect/vuls
			Nessus	https://jp.tenable.com/products/nessus
		Web 脆弱性スキャナ	Nikto	https://github.com/sullo/nikto
ペネトレーション テストツール	シナリオに基づいた 外部から対象システムへの侵入テスト	SYN Flood 攻撃等の生成	hping3	Linux の OS の中に Bundle
		エクスプロイトライブラリによる ネットワーク、機器ののっとり	Metasploit	https://github.com/rapid7/metasploit-framework
		Wifi のパスワードクラック	aircrack-ng	http://www.aircrack-ng.org/
		パスワード解析ツール	Medusa(Medusa Parallel Network Login Auditor)	http://foofus.net/goons/jmk/medusa/medusa.html
		ペネトレーションテスト Linux 向けディストリビューション	Kali Linux	https://www.kali.org
		SQL インジェクション	sqlmap	https://sqlmap.org
		ペネトレーションテスト自動化 ツール	MUSHIKAGO	https://powderkegtech.com/ja/
ファジングテ ストツール	不正データ、予期しないデータ を対象のシステムへ与え意図的 に例外処理を発生させ、潜在的な バグや脆弱性を検出するテスト	定義ファイルに基づくファジ ングに自動実行	Radamsa	https://gitlab.com/akihe/radamsa
		正規表現ファジングデータでの DoS 攻撃ファジング	SDL Regex Fuzzer	https://www.microsoft.com/en-us/search/explore?q=SDL+Regex+Fuzzer

APPENDIX E. 各種チェックシート

APPENDIX E-1. セキュリティ関連 タスク管理シート

フェーズ	タスク	アウトプット	副産物	実施	承認
コンセプト	□被害分析	□脅威想定表	・想定製品仕様書 ・ユースケース図・ミスユースケース図 ・通信フロー図概要・資産管理表（概要）		
	□上位レベルのリスク評価				
	□セキュリティゴール設定	□セキュリティゴール定義書			
	□セキュリティ実施体制の構築	□セキュリティ実施体制図			
設計	□システム基本設計と脅威分析の準備	□脅威想定表（更新版） ・攻撃分析結果、リスク総合評価結果、対策要件を追記	・ユースケース・ミスユースケース図 ・資産詳細管理表 ・アタックツリー図 ・通信フロー図		
	□攻撃分析				
	□安全性影響評価				
	□リスク総合評価				
	□対策要件定義				

フェーズ	タスク	アウトプット	副産物	実施	承認
実装	□対策の実装内容と作業分担の確定	□実装作業・テスト計画書	実装テスト作業手順書 実装テスト作業記録 教育訓練教材		
	□実装作業の詳細の確定	□実装作業・テスト結果報告書 □セキュリティゴール定義書(更新版)			
	□関係者の教育・訓練の実施	・妥当性評価結果を記載 □脅威想定表(更新版)			
	□対策の実装作業・テストの実施	・対策実装結果、残留リスクを記載			
	□実装作業結果・エビデンスの収集と整理				
	□総合評価と総合テストの実施				
	□セキュリティゴールの達成度合いの評価と関係組織の承認				

フェーズ	タスク	アウトプット	副産物	実施	承認
運用	□運用担当組織による関連文書のチェック	□運用体制図			
	□運用実施体制の構築	□インシデント対応フロー			
	□運用レベルのリスクアセスメントと対策方針の策定	□脆弱性対応フロー			
	□運用実施項目の設計	□緊急連絡体制表			
	□運用担当組織における教育・訓練の実施	□各種業務手順書			
	□残留リスクへの対策方針策定	□脅威想定表(更新版)			
	□運用業務の実施	□防災訓練マニュアル			
	□再アセスメント				
廃棄	□情報削除	□情報削除記録			
	□機能停止	□機能停止・廃棄記録			

APPENDIX E-2. セキュリティゴール定義書

セキュリティ目標	

目標を実現するための基本方針	

合意・承認欄(設定時)		
企画組織	設計開発組織	監査組織

実装レベルの妥当性評価	

合意・承認欄(実装完了時)		
企画組織	設計開発組織	監査組織

- セキュリティ目標： 目指す目標を記載
- 目標を実現するための基本方針： 目標を達成するための基本方針を記載
- 実装フェーズを終了した段階での評価：セキュリティ対策の実装状態がセキュリティゴールに対して妥当かどうかを評価し、その結果を記載する
- 関連組織(合意・承認用)：関連組織のチェック欄

APPENDIX E-3. 脅威想定表

項番	①脅威分類	②想定脅威事象	③脅威による想定被害	④被害評価	⑤攻撃可能性	⑥可能性評価	⑦リスク値	⑧対策要件	⑨対策実施	⑩残留リスク

記載事項

①**脅威分類**: 脅威の分類を記載。不正侵入・なりすまし・改竄・情報漏洩・DOS 攻撃・マルウェア・物理攻撃など

②**想定脅威事象**: 攻撃によって想定される事象を記載

③**想定被害**: 想定される被害を記載。機密性、完全性、可用性の侵害など

④**被害評価**: 脅威事象による被害の大きさを記載。大中小など。各案件、プロジェクトの中で評価

⑤**攻撃可能性**: 想定した脅威は攻撃によって発生する可能性を記載

⑥**可能性評価**: 攻撃の可能性の大きさを記載

⑦**リスク値**: リスクの総合評価値を記載。基本は④被害評価×⑤可能性評価であるが、そこにポリシー的な係数を入れるなど各プロジェクトで指標は定める

⑧**対策要件**: 優先順位付けし、対策技術を選択した結果を記載

⑨**対策実施**: 対策を実施したか？どうかを記載

⑩**残留リスク**: 対策実装後の残留リスクを記載

改訂履歴

版数	改訂箇所	改訂内容	改訂日
Ver1.0	—	WG3 内部公開	2021.6.18
Ver2.0	全般	セキュリティマネジメントに関する視点を各章に追加	2022.6.8
	APPENDIX C	対策事例を追加	
	APPENDIX D	テストツール類を追加	
	APPENDIX E	チェックシート類を追加	



ロボット革命・産業IoTイニシアティブ協議会
Robot Revolution & Industrial IoT Initiative