SoS-CPS 安全設計ディスカッションペーパー

Ver.1.0.0（初版発行） 2025-03-31

●履歴一覧

Rev.	内容
0	初版発行　2025 年 3 月 31 日

IPA : Information-technology Promotion Agency , Japan

DADC : Digital Architecture Design Center

本ディスカッションペーパーの内容は予告なく改訂されることがあります。

The contents of this publication may be revised without prior notice.

<Trademark>

IPA Better Life with IT

独立行政法人 情報処理推進機構の登録商標です。

Digital Architecture Design Center

独立行政法人 情報処理推進機構 デジタルアーキテクチャデザインセンターの登録商標です。

Printed in Japan

●本書の作成に携わったメンバー（五十音順）

大野嘉子
清水勝人
白石雅裕
菅沼賢治
福山訓行

目次

図目次

表目次

1　はじめに

1.1　本ディスカッションペーパーの位置づけ

第 5 期科学技術基本計画において提唱された Society5.0 において我が国は、CPS（Cyber Physical System)/IoT（Internet of Things）に代表されるシステムを SoS（System of Systems）として使用することで(つまり異なった事業者で構成された CPS のことで SoS-CPS と呼ぶ)、アーキテクチャル・イノベーションによる誰もが快適に質の高い生活を送れるような社会を目指している。

これまでの社会や産業は縦割りに分かれており、それぞれに分割された範囲で実現する価値しか提供できなかった。社会や産業が横割りの構造になり、自律分散した各々のサービスが協調領域であるデジタルインフラに参加し連携しあうことによって、より人々の生活や社会のニーズに合う人間中心の価値提供ができるようになる。

例えば、モビリティとヘルスケアがつながれば、病院の予約に合わせて自動運転車が家まで迎えに来てくれ、移動中の交通流も全体最適がなされ人にも環境にも優しい。等である。このような社会を目指すために、大きく３つの重要なポイントがあると述べられている(注 1)。

①サイバー空間とフィジカル空間の融合、つまり、IT や AI 等の自動処理によって、その間に人が介入することなく閉ループが成立し、人が介在することなくシステムが進化する。それにより、フィジカル空間がサイバー空間を通じて相互につながること。
②社会課題解決と経済発展が両立されること。
③人間中心のアプローチであることを明示的に示している事。
つまり、人間中心に課題を認識し、サイバー空間とフィジカル空間の高度な融合によって解決することが出来れば、社会課題が解決するだけでなく、経済発展にもつながる。

このような CPS を実現していく為には、安全サイドでは守りの視点「リスク回避」、そして開発・革新を実現していくために攻めの視点「リスク許容」、のバランスをとることになる。そうした「攻め」と「守り」の形をどのように作るかということが、技術革新、技術開発競争が起きている時代の設計として重要である。

本ディスカッションペーパーでは、守りの視点から CPS の安全設計の考え方について概説し、人への安全（人命の保護）についてどのように対処すべきかを、現時点（2025 年 3 月）の保守的な設計を基本に説明した。

事業者それぞれに分割された範囲で実現する価値しか提供しないシステムや製品であれば、モノづくりの不具合で事故が発生した場合の作り込みが、調達、開発・設計、製造、検査のいずれの部署に原因があっても対外的には、事業者等のそうした関連部署にモノづくりを要請している事業者のマネジメントの問題となる。その最終的な対応の責任は、そのオペレーションを行う経営陣にあるとされる。一方で、複数の事業者によるシステムが連携し CPS として機能していく SoS では、そのような考えに留まれなくなり、事業者を社会に置き換えた時にどのようにしていくべきなのか考えなければならなくなる。

保守的な設計に固執していくことも、技術進歩に付随するイノベーションを迅速に実現する SoS-CPS にとっては障害になる面がある。SoS では想定外リスクの残留や発現も避けられない。今後の技術進展や慣習

変化などによっても求められ許容される安全の要求が変化していくことも考えられる。このような SoS の安全について、まだ規範的な記載ができる状況にはない。今後 SoS の安全について Society5.0 の実現に向けたディスカッションがなされ、たたき台として資することを期待し本ディスカッションペーパーを作成した。

1.2 用語説明と注釈

本ディスカッションペーパーで使用する用語についての説明を表 1.2.1 に示す。

また、本文中に記載の注釈について表 1.2.2 に示す。

表 1.2.1 用語説明一覧

用語	説明
エッジ機器	CPS または SoS-CPS におけるフィジカル空間と直接インタフェースする自律的な制御を行う最小単位の装置で、サイバー空間と通信機能で接続される。 例えば、OT 制御装置、自律ロボット、自動運転車、ドローン等。
計算機	CPS または SoS-CPS におけるサイバー空間を構築するクラウドやサーバーのことで、フィジカル空間のエッジ機器と通信機能で接続される。
通信機能	CPS または SoS-CPS におけるサイバー空間（計算機）とフィジカル空間（エッジ機器）とを接続する機能。 例えば公衆回線、企業内の専用回線等。
サイバーシステム	CPS または SoS-CPS におけるサイバー空間を構築するシステムのことであり、計算機や通信機能等。本ディスカッションペーパーではフィジカル空間に位置するエッジ機器は含まないものとする。
構成システム	CPS または SoS-CPS を構成するシステムのこと。 CPS を構成する要素で、エッジ機器、センサー、変換器、計算機（サーバーやクラウド）、通信機能等があげられる。各構成システムは同じ事業者で運営される。 SoS を構成する要素で、各構成システムはそれぞれ事業者が異なる前提で、CPS と同じ要素であるが、CPS そのものも構成システムとして扱う。
SoS	System of Systems 個々の構成システムがそのままでは達成できないサービスを提供するために，相互的に作用するシステムの集合体。その構成システムは管理運用の独立性といった特徴を持つ。 例えば、事業者が異なる構成システム(K)で作られたシステムのこと （K1＋K2＋・・・＝SoS）
CPS	Cyber-Physical System サイバー空間とフィジカル空間が接続されたシステム。 サイバー空間側には計算機(クラウド等)や通信機能(公衆回線等)があり、フィジカル空間にはエッジ機器がある。直接人命に関わるエッジを含むため、セーフティとして考慮が必要。 断りがない限り、単独事業者による CPS を示す。 複数事業者で構成した CPS は、SoS-CPS に含む。但し、あえて区別するために SoS 構成の CPS と表現する場合もある。
SoS-CPS	① 事業者が異なる CPS が複数繋がったもの （CPS1＋CPS2＋・・・＝SoS-CPS） ② 事業者が異なる構成システム(K)で CPS が作られたもの （K1＋K2＋・・・＝SoS-CPS） ③ 事業者が異なる CPS と事業者が異なる構成システム(K)が繋がったもの （CPS1＋K1＋K2＋・・・＝SoS-CPS） ④ 事業者が異なる CPS や構成システム(K)と SoS-CPS が繋がったもの （CPS1＋K1＋K2＋SoS-CPS1＋・・・＝SoS-CPS）
安全度水準	機能安全規格(IEC 61508 や ISO26262)における安全設計における水準のこと。 IEC 61508 は、SIL 1～4 までの 4 段階。1 は最も緩く、4 が最も厳しい設計が必要。 ISO 26262 は、ASIL A～D までの 4 段階。A は最も緩く、D が最も厳しい設計が必要。
パフォーマンスレベル	機械安全規格(ISO 13849-1)における制御システムの安全関連部の能力を規定する区分レベルのこと。PL a～e までの 5 段階。a は最も緩く、e が最も厳しい設計が必要。
インフラ基盤	CPS または SoS-CPS において、構成システム間でデジタル接続でき、制御ループに人か介在しないデジタル完結できるエッジ機器を含まないインフラシステム部分であり、エッジ機器の動作/運用を補佐するシステム。

フィジカルシステム	CPS または SoS-CPS において、フィジカル空間と直接インタフェースするエッジ機器、センサー、変換器等の構成システム。
安全通信	構成システム間で受け渡しする情報や指示に対して、人命に関わる情報や指示についても安全を担保した伝送ができる通信のこと。一般的な実現方法は、通信機能として安全を担保するのではなく、通信機能の両端に接続される構成モジュール上に安全レイヤを設けることで安全を担保する。
安全レイヤ	安全通信を実現するための通信プロトコル。IEC 61508 機能安全規格でその手法が定められている。通信機能の両端に接続される構成システム上に実装される。
ブラックチャネル	通信機能を情報や指示を単に伝達するだけの“土管”として扱った表現。通信機能は情報や指示に対して処理を施してはならない前提。IEC 61508 機能安全規格で使われる表現。
DEOS	IEC 62853 で標準化されている Open Systems Dependability (OSD)。Dependability（総合信頼 性）は、「要求された時にその要求通りに遂行するための能力」。OSD ではこれに「総 合品質」盛り込まれている。

表 1.2.2　注釈一覧

記号	参照元	注釈の説明
（注１）	・1.1 項	出典：デジタル時代の社会・産業構造をデザインする新たなアプローチ （白坂成功氏：2024-JSAE 自動車技術）
（注２）	・1.6.2 項	出典：自動運転車に関するアジャイル型の制度設計 （羽深宏樹氏：2024-JSAE 自動車技術）
（注３）	・3.1.2 項 1)	処理機能とフェイルセーフ機能について： 一般的にセンサーの機能不全（故障等）を検出するために、処理機能と独立したフェイルセーフ機能を設置するのは難しいと考えられる。独立させた結果別途センサーが必要であり、その処理機能まで含めて安全設計する必要になるため、最初から処理機能とそれと組み合わせたフェイルセーフ機能の両方を安全設計した方が経済的である。その理由からセンサーは処理機能とフェイルセーフ機能の両方を安全設計することになると考えられる。またセンサー（例えばカメラ）の安全状態は、映像等の情報提供を停止することである。情報を停止すれば、少なくとも誤った情報をエッジ機器に提供することは避けられ、その結果エッジ機器は誤った情報により人に危害を与える動作をしないで済む。
（注４）	・3.1.2 項 2)	保護機能の独立性について： 制御が正しく行えない際に、保護機能は自律的な制御機能とは独立した入力情報によって制御が正しくないことを検知し、決められた時間内に自律的な制御出力に割り込んでエッジ機器を安全状態に遷移させる必要がある。
（注５）	・3.1.2 項 2)	自立的な制御機能の安全設計について： 人命への危害を防ぐためのエッジ機器の安全状態が“動作停止”という比較的単純な状態であり、独立した保護機能だけで安全状態に遷移できるのであれば、自律的な制御機能に対して安全設計を施す必要はない。安全設計された保護機能が自律的な制御機能の出力に割り込んで動作を停止させればよい。しかし例えばエッジ機器が自動運転車の場合、動作を停止することが安全とは言い切れない特性をもつ場合、その状況に応じてブレーキ制御以外にステアリング制御やアクセル制御を正しく連動させて、安全状態に遷移させる必要がある。またそれらの機能が故障した場合は別の機能によって安全を担保する必要がある。つまりそれらの自律的な制御機能を確実に作動させるとともに、それらの故障を確実に検出して別の機能に引き継がなければならない。独立した保護機能（例えば独立補助ブレーキ機能等）だけでは、本来の安全状態に遷移させることが難しいため、自律的な制御機能に対しても安全設計が必要となる。
（注６）	・3.1.8 項内の表 3.1.3 No.1	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（第一版）について：

		このガイドによって、ロボットサービスの安全マネジメントシステム　[JIS Y 1001]（ロボット運用時の安全の規格化）が制定された。ロボット本体に対する安全規格：産業用⇒ISO 10218/JIS B 8433、サービス用⇒ISO 13482/JIS B 8445
（注 7）	・2.2.2 項 2) ・3.2.3 項	RoAD to the L4： 『自動運転レベル 4 等先進モビリティサービス研究開発・社会実装プロジェクト』のこと。
（注 8）	・2.2.2 項 2) ・3.2.3 項	CooL4： Cooperative Level 4 Automated Mobility Service in mixed traffic environment：混在空間における協調型自動運転レベル 4 モビリティサービスのこと
（注 9）	・2.2 項内の 図 2.2.1	Voter： システムの信頼性を向上させる目的でシステムを多重化した際に、どのシステムが正しい結果を出力しているか判断する機能。例えば、システムが 2 重系の場合は、2 つのシステムの出力が一致した場合（または一致せずともある範囲に入った場合）のみその出力を正しいと判断する。システムが 3 重系の場合は、3 つのシステムの出力を多数決し、2 つ以上一致した出力を正しいと判断する。一致せずとも出力が範囲を持つ場合は、3 つの出力の中間値を正しいと判断する（これは 2 つのシステムが同時に故障しないと考えられるからである）。
（注 10）	・5.1 項	GOVERNANCE INNOVATION Ver.2 報告書　経済産業省
（注 11）	・5.1 項	「システムオブシステムズの現状と課題（ソフトウェア・シンポジウム 2019）」　ソフトウェア技術者協会

1.3 想定読者

本ディスカッションペーパーの想定読者は、CPS（単独事業者）または SoS-CPS（異なった事業者で構成された CPS）における下記の者である。具体的には図 1.3.1 の通りである。

① 構成システム設計者
② CPS 設計者
③ SoS-CPS 設計者

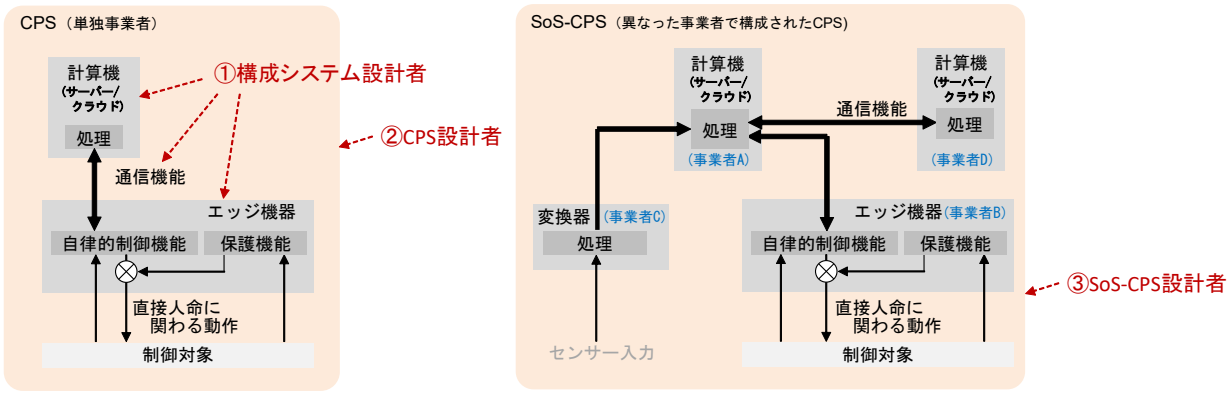


図 1.3.1 本ディスカッションペーパーの想定読者

① 構成システム設計者とは、CPS を構成する要素であるエッジ機器、計算機、通信機能、変換器、等の構成システムの企画、開発、運営方法、品質管理等構成システムの設計に従事する者である。
② CPS 設計者とは、CPS の企画、構成システムの準備・接続、運営方法、品質管理等 CPS の設計に従事する者である。
③ SoS-CPS 設計者とは、SoS-CPS の企画、構成システムの準備・接続、運営方法、品質管理等 SoS-CPS の設計に従事する者である。

1.4 関連図書

（１） JIS Z8051 Guide 51 (2014)

（２） IEC 61508:2010

Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1 through Part 7

（３） ISO 13849-1:2015

Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design

（４） ISO 26262:2018

Road vehicles – Functional safety — Part 1 through Part 9

（５） IEC 62443-4-1:2018

Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

（６） IEC 62443-4-2:2019

Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

（７） IEC White Paper Safety in the future

Advanced robotics, artificial intelligence, the Internet of Things are transforming how humans and electrotechnical systems interconnect. With the introduction of new technologies, it is critically important to ensure that human safety remains at the centre of the human-machine relationship.

（８） IEC 61131-3:2013（JIS B 3501）

Programmable controllers - Part 3: Programming languages

1.5 本ディスカッションペーパーの目的と対象範囲

1.5.1 目的

Society5.0 が実現される将来、様々なイノベーションを創出しながら、様々な社会課題の解決し、豊かな社会を目指していくために、これまでの人間の活動の大半をロボットや AI を活用したサービスが装備されたデジタル社会が実現することを想定することが重要と考える。そうした社会は、あらゆる情報を活用して、行動や活動の最適化を図るために、あらゆるモノやヒトが容易に繋がり、連携できるシステム化された社会となる。そして、その形態は、従来の OT システム、IT システムという切り分けられたシステム同士を（人の）業務で連携させていた形態から、アルゴリズムが判断して連携させていく、OT と IT が融合した CPS システム（従来のモノを含めたシステム化されたコトの単位）で実現される。その場合には、各所に AI がヒトの代替えとして導入しながら、多様なサービスを連携させて実現する形態＝責任者の異なるシステムが連携する形態、つまりは SoS として実現されることになる。

これらの背景を踏まえ、本ディスカッションペーパーは、以下の２つを目的にして作成した。

1 つ目は、CPS または SoS-CPS によりイノベーションがメリットをもたらすことができるように、CPS または SoS-CPS における社会が受容できる安全の確保について、技術的対処から考察することである。

2 つ目は、システムの十分な安全性を確保（1 つ目の目的達成）したうえで、システムのライフサイクル全体を通じて継続的に安全性が社会に受容されるレベルに達している事を示し続けること（ガバナンス）によって、CPS または SoS-CPS の社会への導入が可能になることを提案することである。

本ディスカッションペーパーは、CPS あるいは SoS-CPS に対する社会システムのアーキテクチャを設計する際に、その安全性を実装する設計指針としてまとめたものである。CPS（単独事業者）の安全設計に対しては、基本的に各事業者で実施されている既存の安全性実現方法（社内品質管理、社内安全管理、PL 法遵守、製品安全規格への適合、機能安全規格への適合）の実施を推奨すると説明している。また、サイバーシステム（クラウドやサーバー等の計算機、通信機能）に対する安全設計は、現時点では難しいことも説明している。SoS-CPS の安全設計に対しては、単独事業者による CPS の安全設計を前提として、さらに事業者が複数存在する構成になることで考慮しなければならない事柄を説明している。

SoS では全てのリスクを想定できない中で、SoS-CPS を継続的に安全に運用できるようにするためには、SoS-CPS 全体やその構成システムをガバナンスの対象にする必要があり、そのガバナンス設計の考え方も説明する。

1.5.2 対象範囲

本ディスカッションペーパーの対象範囲とするシステム構成は、図 1.5.1 に示す通り、次の２つの構成である。

① CPS

② SoS-CPS

いずれも CPS 形態のシステムであるが、それは CPS が直接人命に関わるエッジ機器を含んだシステムであり、今後はサイバーシステムとエッジ機器の協調運転が必須となるため、本ディスカッションペーパーでその安全設計について検討するためである。従って、CPS 形態を伴わない IT システムやその SoS 構成については、対象外としている。

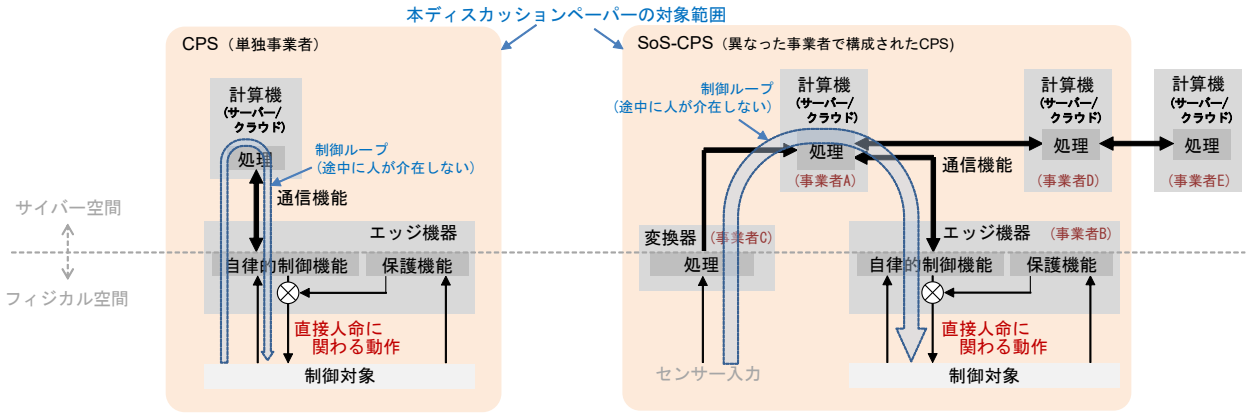


図 1.5.1　本ディスカッションペーパーの対象範囲

SoS-CPS においては、制御ループに直接関わる構成システム（事業者 A の計算機、事業者 B のエッジ機器、事業者 C の変換器）と、そこに直接接続される構成システム（事業者 D の計算機）が SoS-CPS に含まれるものとして対象範囲にしている。

なお、制御ループの途中には人が介在しないことを前提としている。人が介在したループは、途中に人の判断が入るため、システムの安全を担保することができないためである。ただし、人が介在した場合でも、システム的に安全が担保され続けている場合はその限りではない。例えば、自動運転車が発進不能な状態に陥った場合に、図 1.5.2 に示す通り、人が介在して運転を代行した場合でも、自動運転車の安全機能（ここでは保護機能）を解除しない状態（有効）で継続運転できれば、これは本ディスカッションペーパーの安全設計の対象となる。しかし安全機能（保護機能）を解除した状態は対象外となるため、このような運用は本ディスカッションペーパーでは推奨しない。

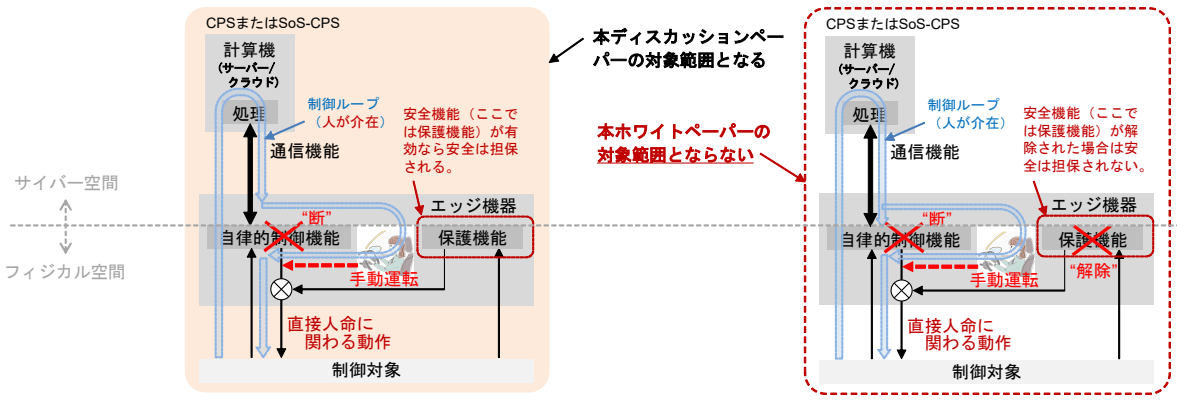


図 1.5.2　制御ループに人が介在した場合の安全担保について

1.5.3　安全の定義

本ディスカッションペーパーにおける安全の定義　：　人命への許容できないリスクがない状態
（財産と環境は除外して検討した）

安全規格の最上位に位置するガイド 51（ISO/IEC GUIDE 51、日本では JIS Z 8051）では、安全とは、人・財産・環境に対し許容できないリスクがない状態としている。本ディスカッションペーパーにおいては、安全の定義として「人命への許容できないリスクがない状態」とした。人命の保護は対象であるが、財産（設備含む）に対する保護は含めていない。また環境への被害（放射能、有害ガス等）の多くは直接人命に関わる場合が多いので、人命の保護に含める（例えば原子力発電の制御システム、石油・ガス・化学系プラント制御システム）。

本ディスカッションペーパーにおいて財産を含めない理由は、それを保護する（守る）手段が人命を保護する（守る）手段と大きく異なる（セキュリティやトラスト等が大きく関与する）ため、これを含めると本ディスカッションペーパーの内容が複雑に入り組み、理解しにくくなってしまうことを懸念している。そこで分かり易さを優先し、人命を保護する設計に特化し、人命を保護するしくみの考え方について浮彫にするため、この本ディスカッションペーパーは財産を対象外とする。

1.6 本ディスカッションペーパーの構成

1.6.1 目次構成の考え方

本ディスカッションペーパーの対象範囲は、1.5 項に示した通り、CPS および SoS-CPS の 2 つである。この 2 つに対する安全設計について理解しやすいように、CPS の中で人に最も近い位置で動作するエッジ機器、次にサイバーシステム、そして SoS-CPS までを順番に段階的に安全設計の考え方を膨らませながら説明する。図 1.6.1 に示す章構成としている。なお、CPS、SoS-CPS の定義については 1.7 項を参照のこと。

まず CPS の安全設計について説明する。その中をエッジ機器の安全設計→サイバーシステムの安全設計と段階的に説明する。CPS の安全設計について理解できたところで、さらに CPS が SoS 構成をとる際に、付け加えてどのような安全設計を考慮しなければならないのかについて、SoS-CPS の安全設計で説明する。

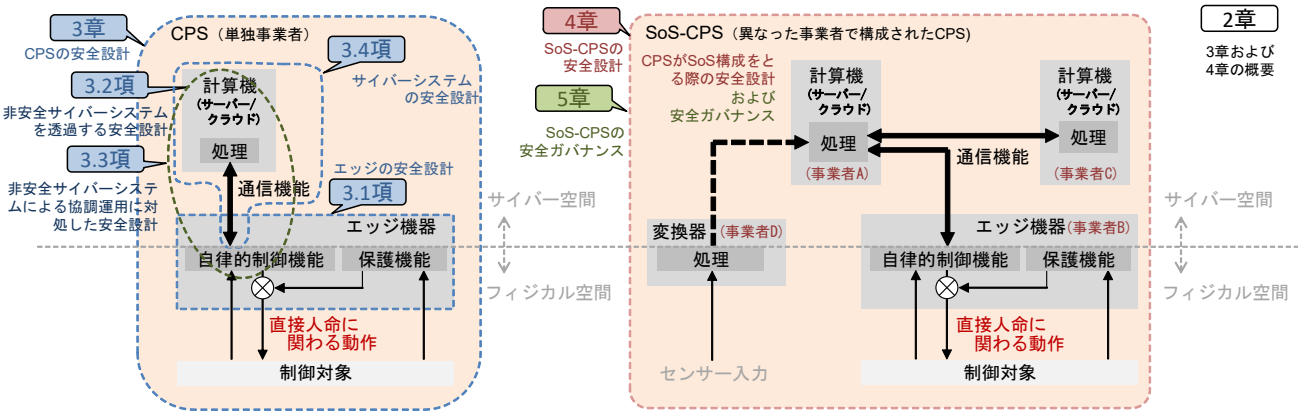


図 1.6.1 本ディスカッションペーパーの目次構成

2 章では、3 章および 4 章の検討の概要として、CPS および SoS-CPS のための安全性を実現する考え方を概説する。

3 章では直接人命に関わる可能性のある CPS の安全設計の考え方について説明する。

- 3.1 項：人に最も近い位置で動作し、直接人命に関わる処理を行うエッジ機器の安全設計の考え方を説明。
- 3.2 項：安全設計されていないサイバーシステムを透過させて運用する際の安全設計の考え方を説明。
- 3.3 項：安全設計されていないサイバーシステムと安全設計されたエッジ機器を協調運転する際の安全設計の考え方を説明。
- 3.4 項：サイバーシステムの出力に誤りをなくし、エッジ機器との連携を確実にするための、サイバーシステムの安全設計の考え方を説明。

4 章では、人命に関わる用途へ適用する SoS-CPS の安全設計の考え方について検討する。

5 章では、SoS-CPS におけるガバナンス設計を説明する。

1.6.2 内容について

CPS または SoS-CPS の安全性検討のために、自動運転車での制度設計への提言(注 2)を参考にし、下記 7 つの観点で具体化を検討した。

① 人命への影響がある CPS を構成する個々のシステム（構成システム）を十分な安全性にする。

② 人命への影響がある SoS-CPS のリスクシナリオをマルチステークホルダーにより合意と更新する。
③ 上記 SoS-CPS の運用中はリスクマネジメントとアカウンタビリティを確保する。
④ 想定外を含む顕在化したリスクについて原因究明し、将来の改善を目的とする事故調査制度を確立する。
⑤ 法制度および責任制度を通じたインセンティブ設計を適用する。
⑥ 被害者救済制度を整備する。
⑦ 専門的なデータ分析等により最終的な責任分担の決定をする。

① は CPS や構成システムを管理する事業者（構成システム設計者、CPS 設計者）がエッジ機器等フィジカルシステムに対して従来から実施しているいわゆる製品やシステムの安全設計であり、これを計算機や通信機能等のサイバーシステムまで広げて 3 章で検討する。
② ～⑦は複数事業者で構成された SoS-CPS ならではの新たな制度設計が必要となり、ガバナンスを用いた安全設計として 4 章および 5 章で検討する。

1.7 CPS、SoS-CPS、インフラ基盤の定義

本ディスカッションペーパーで扱う CPS、SoS-CPS、インフラ基盤の定義を解説する。1.3 項の用語説明と併せて参照のこと。

1.7.1 CPSの定義

本ディスカッションペーパーで扱う CPS は、フィジカル空間のエッジ機器とサイバー空間の計算機が、通信機能で接続されたサイバーフィジカルシステムの基本構成をとり、エッジ機器、計算機、通信機能、の運用者が単独事業者で構成されるシステムのこと。また基本構成に個別のセンサー等の構成システムが付け加わった場合も CPS として扱う。図 1.7.1 に示す。

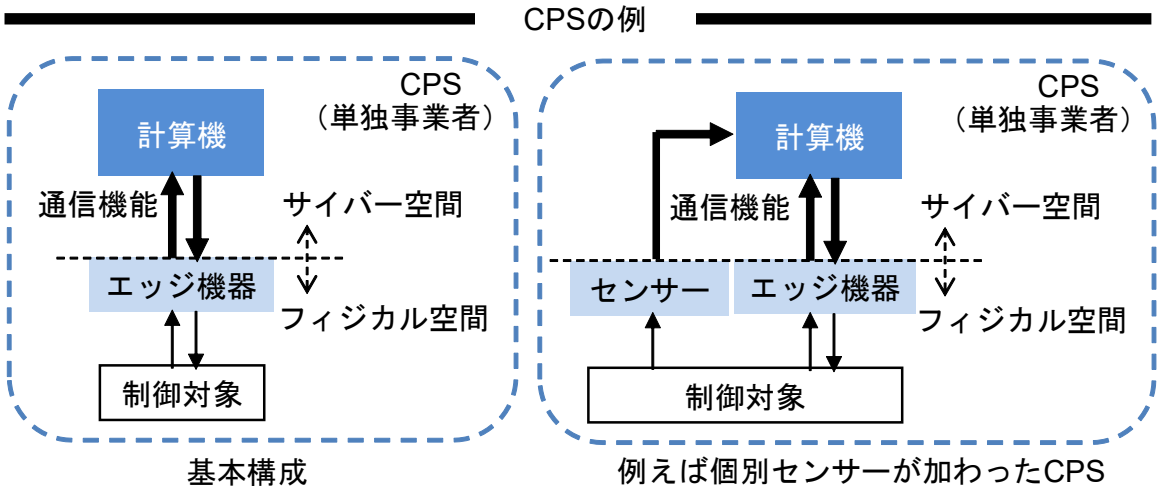


図 1.7.1 CPS の定義

1.7.2 SoS-CPSの定義

一般的に SoS とは、異なった事業者が運用する構成システム（エッジ機器、計算機、通信機能、センサー、CPS 等）が複数接続されたシステムのことであるが、SoS 構成の CPS（異なった事業者で構成された CPS）のことを本ディスカッションペーパーでは SoS-CPS と表現する。本ディスカッションペーパーが安全設計として対象としている SoS は、この CPS 形態のシステムのみである。図 1.7.2 の示す構成例 1 と構成例 2 が SoS-CPS の基本構成である。制御ループに直接関わる構成システムのみで構成される形態である。構成例 3 は、制御ループに直接関わる構成システムに、制御ループに直接関わらない構成システム（IT システム）が接続された場合であり、制御ループに直接関わる構成システムに影響が及ぶ可能性があることから、本ディスカッションペーパーではこのシステムについても SoS-CPS として扱う。また図 1.7.3 に示すように、制御ループに直接関わらない構成システム(A)に、さらに制御ループに直接関わらない構成システム(B)が繋がった場合は、本ディスカッションペーパーでは構成システム(B)について SoS-CPS の範囲に含めない。

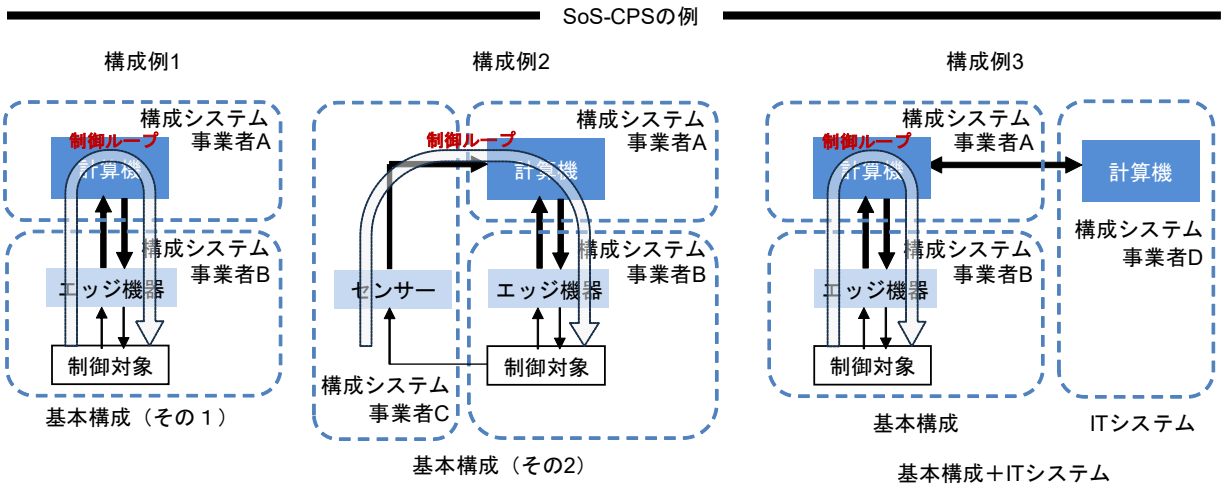


図 1.7.2　SoS-CPS の定義

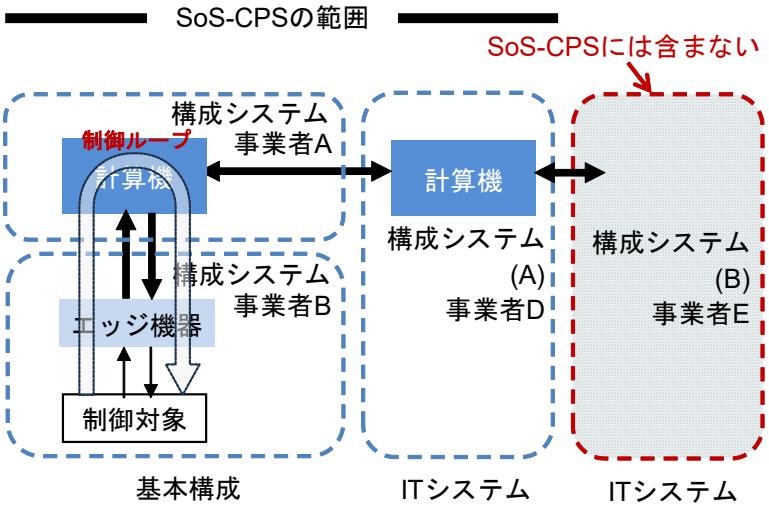


図 1.7.3　SoS-CPS の範囲

1.7.3　CPS形態ではないSoSについて

図 1.7.4 に示す構成例 1 のように、事業者 E が運用する計算機と事業者 F が運用する計算機が接続しているシステム（フィジカル空間に位置するエッジ機器が存在しないシステム、つまり CPS 形態ではない SoS）は、IT の分野における一般的な SoS であるが、OT の分野であるエッジ機器がないゆえに人命に直接関わらないシステムであるため、本ディスカッションペーパーでは対象外としている。本書で扱う SoS は、構成例 2 や構成例 3 のように IT の分野と OT の分野が融合（IT＋OT）した CPS 形態の SoS（SoS-CPS）である。

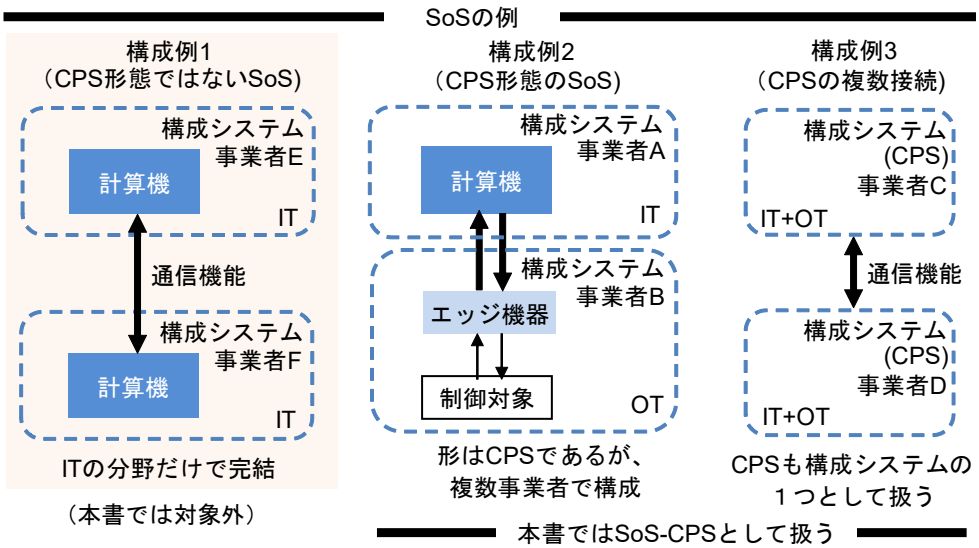


図 1.7.4　CPS 形態でない SoS について

1.7.4　インフラ基盤の定義

インフラ基盤という言葉を敢えて使う理由は、一般的なインフラという言葉が示す範囲と同じでは無いため、混乱を招かないようにする目的である。

一般的にインフラとは、電気、ガス、上下水道、通信（インターネット網、公衆回線、クラウド、等）、交通（飛行機、船舶、鉄道、バス、タクシー、等）、道路（市道、県道、国道、高速道路、等）、公共機関（役所、図書館、等）等のことであり、利用者である人に対する前提である。

しかし本ディスカッションペーパーが対象にしている CPS や SoS-CPS におけるインフラは、自律的に動作するエッジ機器に対するインフラであり、具体的には通信機能（公衆回線等）や計算機（クラウド等）を示す。エッジ機器とデジタル的に接続できるかつデジタル完結できるインフラが条件である。

インフラ基盤の定義　：　デジタル接続できデジタル完結できるもので、エッジ機器の動作/運用を補佐するシステム

本ディスカッションペーパーが対象としている CPS または SoS-CPS においては、エッジ機器はインフラシステムに含まない。CPS または SoS-CPS におけるエッジ機器は、自律的に動作/運用できる前提としているため、インフラシステムは CPS または SoS-CPS におけるエッジ機器の動作/運用を補佐する役目であると定義する。つまりインフラ基盤とは、デジタル完結した CPS または SoS-CPS におけるエッジ機器動作/運用を補佐するシステムである。

SoS-CPS におけるインフラ基盤の例を、図 1.7.5 に示す。自動運転車の自律運転をインフラ基盤と協調し補佐することで、エッジ機器単体で走行するよりもより安全（事故が発生しにくい）で効率的（例えば渋滞が発生しにくい）な走行を実現する SoS-CPS の例である。

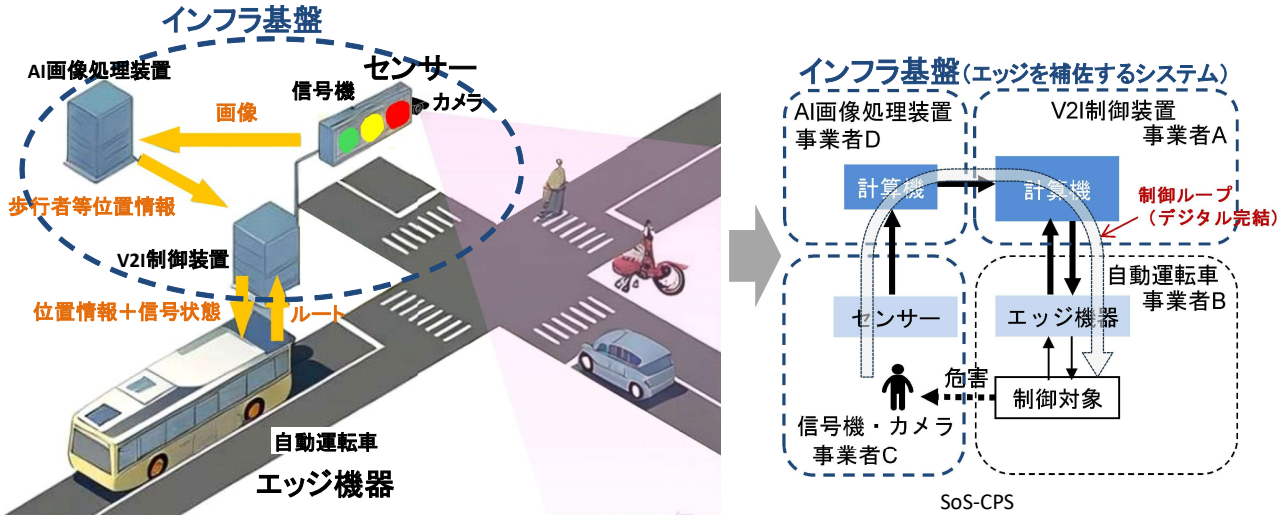


図 1.7.5　SoS-CPS におけるインフラ基盤の例

ここではエッジ機器が自動運転車であり、それを補佐するインフラ基盤が信号機、カメラ、AI 画像処理装置、V2I 制御装置である。すべてがデジタル接続され、制御ループに人が介在しないデジタル完結した CPS である。また自動運転車、道路カメラ、AI 画像処理装置、V2I 制御装置は管理事業者が異なることから SoS-CPS を構成している。

カメラは、交差点の状況を捉え AI 画像処理装置に伝送し、AI 画像処理装置は、その映像を分析することで交差点における歩行者の位置、右折車や左折車の位置を特定する。V2I 制御装置は、この位置情報と信号機の状態（赤や緑等）を自動運転車に伝送することで、自動運転車は自身のセンサーで捉えるより早く交差点の状況を認知することができ、交差点での不要な減速を行わない。これにより、安全を担保した状態で渋滞緩和が可能となる。

2 CPS および SoS-CPS のための安全性を実現する考え方

本ディスカッションペーパーにおける CPS および SoS-CPS の安全性とは、CPS および SoS-CPS を利用することによって、その構成システムの中で直接人命に関わる動作が行われるエッジ機器が、人命に危害を与えない状態を維持することを示している。この状態は、以下①②により達成されると考えられる。CPS および SoS-CPS の構成システムそれぞれが人命に対して信頼のおける安全な製作物（装置）であること、その装置が常に安全な状態に維持され、さらにより安全となる改善が行われるためにガバナンスが運用されることで成立するものと考えている。①については 2.2 項、②については 2.3 項に考え方を説明する。

① CPS および SoS-CPS の構成システムを適切な安全を備える製作物として設計する上で、CPS および SoS-CPS が関わる人命への影響度に応じて、その安全設計手法を柔軟に変えることが望ましい。

② SoS-CPS に対する計画、設計、運用のライフサイクルに対して、SoS-CPS が目的通りに機能しているかを監視するためのガバナンス、さらにガバナンスそのものが正しくなされているか監視するガバナンスが必要となる。

2.1 人命への影響度と安全設計の考え方

CPS および SoS-CPS において、その使用目的や使用方法によって人命への影響が懸念される度合いが異なる。CPS および SoS-CPS の使用目的や使用方法はさまざまであり、それらのインシデントによる安全性リスクもさまざまである。単独事業者が運営する CPS や、複数事業者が運営しそれらを接続/連携した SoS-CPS において運営管理者が存在する SoS-CPS であれば、使用目的や使用方法はある程度管理できるため、直接人命に関わる使用方法であっても普遍的な安全性を定義することはできるかもしれない。明確な運営管理者が不在の SoS-CPS においては、どのような使用目的や使用方法となるかが、想定しきることが困難となり、普遍的な安全性を定義することはできない。

つまり分類としては、①直接人命への影響がない使い方をする CPS や SoS-CPS、②単独事業者であるゆえに人命への影響を制御し極小化できる CPS、③複数事業者から構成されるも運営管理者が存在し人命への影響を制御できる SoS-CPS、④明確な運営管理者が不在であるゆえに人命への影響を制御するのが難しい SoS-CPS が存在することになる。本ディスカッションペーパーが安全設計として対象にするのは主として②③であり、直接人命への影響を制御できる CPS および SoS-CPS である。

直接人命に影響しない使い方のみの CPS および SoS-CPS においては、本ディスカッションペーパーに示す安全設計を実施する必要はない（対象外）。直接人命に影響しない CPS および SoS-CPS の例としては、図 2.1.1 に示すような金融機関の ATM システムがあげられる。人が操作するエッジ機器は、パソコン/スマホや ATM 機器であり、振込操作や引き出し操作が人命に影響（人に危害を与える）可能性はない。

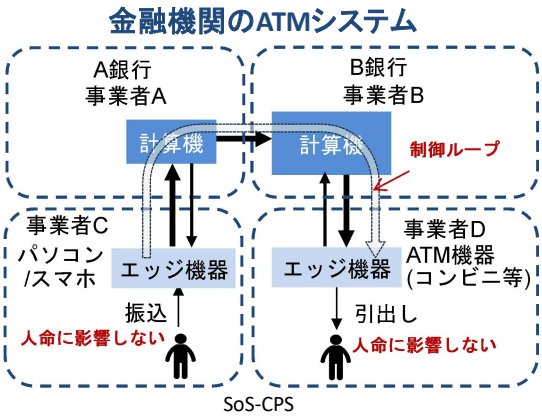


図 2.1.1　直接人命に影響しない SoS-CPS（金融機関の ATM システム）の例

④の明確な運営管理者が不在複数事業者から構成されるであるゆえに人命への影響を制御するのが難しい SoS-CPS においては、直接人命に関わる使い方をしてはならない（対象外）。

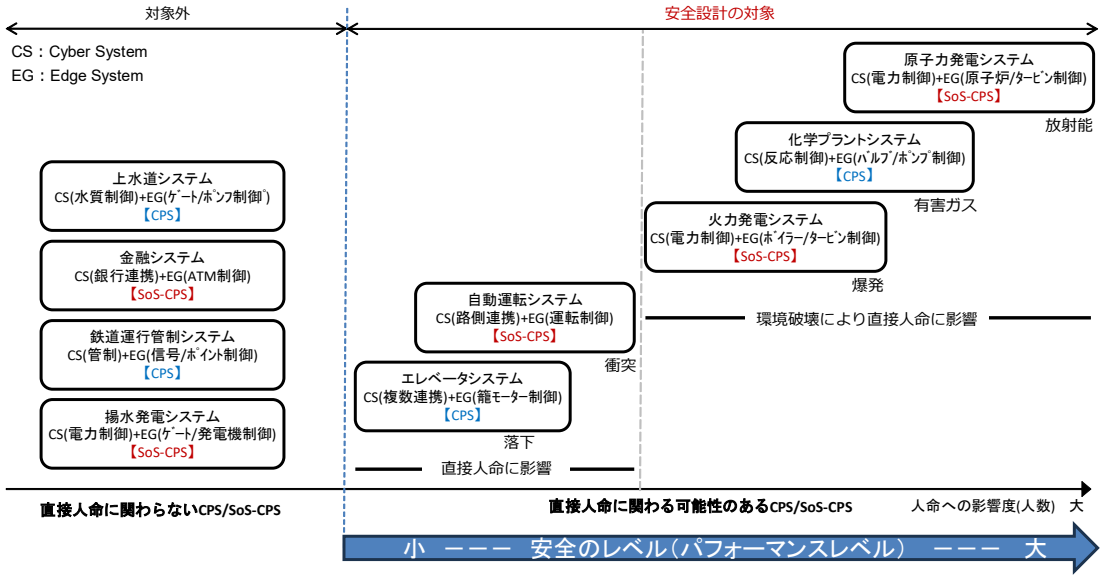


図 2.1.2　CPS および SoS-CPS の人命への影響度と安全のレベル（例）

図 2.1.2 に人命への影響度と安全のレベル（例）を示す。図右側の直接人命に関わる可能性のある CPS および SoS-CPS に対して、本ディスカッションペーパーの安全設計が適用対象となるが、ここには目的の異なったシステムがいくつか存在している。それぞれの安全設計の内容については、人命への影響度（危害を受ける人数）によって安全設計の深さを決めるレベル分けが必要と考える。つまり少人数への危害しか発生しない CPS および SoS-CPS（例えばエレベータシステム）と、大規模な人数への危害が発生する CPS および SoS-CPS（例えば原子力発電システム）では、同じ安全設計手法であるべきではないということである。具体的には機械系安全規格（ISO 13849-1）で定められているパフォーマンスレベル（PL）、機能安全規格（IEC 61508）で定められている安全度水準（SIL）、自動車機能安全規格（ISO 26262）で定められている安全度水準（ASIL）を用いることを考えている。詳細は 2.2 項および 3.1 項に示す。また CPS に比べ SoS-CPS

では複数事業者による運営になることから、CPS に加えてより考慮すべきことが多くなる。具体的にはガバナンス設計であるが詳細は 2.3 項および 4.1 項に示す。

2.2 CPS における安全設計の考え方

CPS における制御ループにおいて、安全機能をどのように分担するかを設計することが重要である。人との接点となるエッジ機器だけに安全機能を集中させると、エッジ機器近辺の局所的な情報に基づく保守的な動作しかできなくなり、結果 Society 5.0 を実現できなくなる。そこでインフラ基盤側（例えばサイバーシステム）に対しても安全設計を施しエッジ機器と協調することで、エッジ機器のセンシング範囲を超えたより広い範囲での安全動作ができるようになり、Society 5.0 を実現できるようになると考えられる。

１）エッジ機器の安全設計

CPS における構成システムのうち、人との接点であり自律して動作できるエッジ機器については、エッジ機器単体としてクローズする基本的な安全設計が必須であり（3.1 項参照）、その上でサイバーシステムとの連携の方法を設計し、サイバーシステム側の安全設計の度合いによって、エッジ機器側を追加設計することが望ましい（3.2 項、3.3 項、3.4 項参照）。

２）エッジ機器以外の構成システムの安全設計

CPS におけるエッジ機器以外の構成システムの安全設計手法は、いくつか考えられる。例えば下記①②。

① エッジ機器と同様、構成システム単位に基本的な安全設計を施し、これらを組み合わせて制御ループを構成した CPS 全体としての安全機能の過不足を調整する手法。調整は各構成システムの基本的な安全設計に対して追加設計する。2.2.1 項の図 2.2.2 を参照。

② 制御ループとして安全が担保できるように設計する手法。経済性や技術的背景などの観点から、各構成システム全てに対して安全設計ができない状態において、SoS の構築が必要になる場合がある。この場合に採用する手法である。個々の構成システムの全てに対して安全設計を求めなるものではない。安全設計されていない構成システムを人命に関わる用途の制御ループに組み込むためには、制御ループとして３つの条件を成立させる設計が必要となる。

（１）構成システムの信頼性を十分に確保する。

（２）構成システムの故障を検出する機能を安全設計して設置する。

（３）故障を検出する機能を定期的に診断する。

具体的な例を、図 2.2.1 に示す。

安全設計されていないセンサーと計算機を使って、CPS の制御ループとして安全を担保できるように設計する場合の例を、例１）～例３）の３つで説明する。

本ディスカッションペーパーでは、上記①②について説明する（①は 3 章以降で詳細を説明する）。また、本ディスカッションペーパーは、安全性についてわかり易く説明するために安全設計に焦点を絞っているが、本来システム設計する際は、システムを止めないための信頼性や可用性についても、安全性と併せて設計する必要がある。

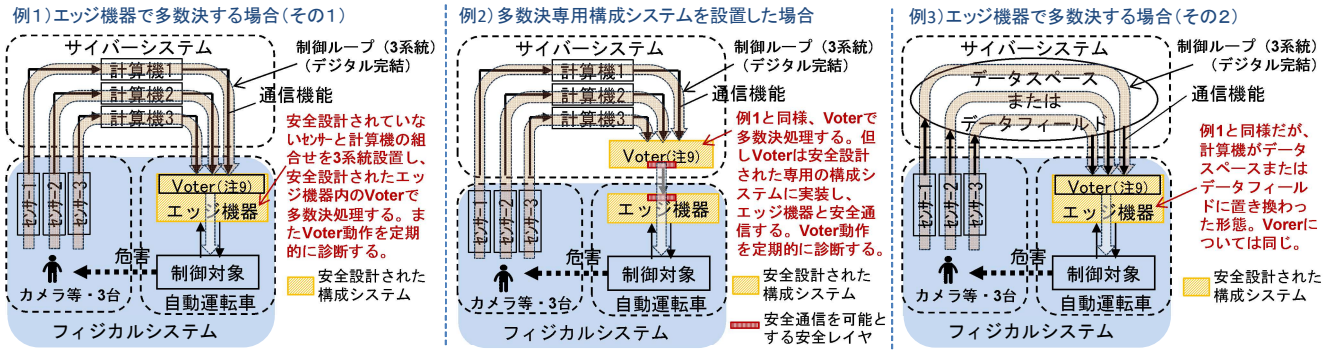


図 2.2.1　制御ループとして安全が担保できるように設計する手法の例

例１）～例３）の共通点として、

（１）に対する処置・・・センサーと計算機の組合せを 3 系統とし、それぞれの信頼性を向上している。3 系統にすることはあくまでも信頼性を向上させるためのひとつの例である。

（２）に対する処置・・・安全設計した Voter 機能で 3 系統を多数決し、故障した系統を制御ループから除外している。

（３）に対する処置・・・Voter 機能の動作が正しいかを定期的に診断している。診断周期は安全度水準（詳細は 3.1.8 項参照）によって決定する。例えば人が死亡する可能性のある制御ループでは、8 時間に一度診断（1 日の稼働時間内に 1 回実施することが目安）する等。

例１）～例３）の相違点は下記である。

例１）　は、Voter 機能を安全設計したエッジ機器内に設置した場合である。この場合、メリットはエッジ機器のみ安全設計すればよい。デメリットはサイバーシステム（計算機 1～3）とエッジ機器の間を 3 つの異なった通信機能で接続する必要があること、またエッジ機器側でセンサーや計算機の信頼性に関する設計が必要となる。

例２）　は、Voter 機能を安全設計した専用の構成システムとして設置した場合である。この場合、メリットはエッジ機器と Voter 機能とを 1 つの通信機能で接続すれば良いこと、またエッジ機器側でセンサーや計算機の信頼性に関する設計が不要となる。デメリットは、エッジ機器と Voter 機能との間で安全通信（詳細は 3.2.2 項参照）を実現する必要があること、また一般的に Voter 機能とエッジ機器の安全設計者を同じにできないため、別に準備する必要がある。

例３）　は、本質的には例１）と同じである。例１）のサイバーシステムの計算機を、データ共有する仕組み（主に静的データを扱うデータスペース、または主に動的データを扱うデータフィールド）に置き換えた場合である。データが正しく伝わる信頼性のある仕組みがあれば、データの流通の仕掛けは問わないことを意味している。

2.2.1　CPS全体を安全設計した場合の効果

CPS における安全設計の考え方は、人との接点があるフィジカルシステムを安全設計することが最も重要である。特に自律的な動作をするエッジ機器における人への危害を最小限に留めることができれば、CPS において人命に対する安全は守ることができる。しかしエッジ機器だけが安全設計されている CPS では、

エッジ機器が自律的に安全と判断できる環境内でのサービスに留まり、エッジ機器がサイバーシステムと繋がって CPS を構成し、より便利なサービスに広げることが難しくなってしまうことも事実である。この便利なサービスを実現するには、フィジカルシステムの安全設計だけでなく、CPS を構成するサイバーシステムに対しても安全設計を施すことで、CPS 全体として安全を担保できるようになるため、エッジ機器だけの安全判断から CPS 全体を使った安全判断が可能となり、より便利なサービスにすることが可能となるはずである。具体的な効果を以下に示す。

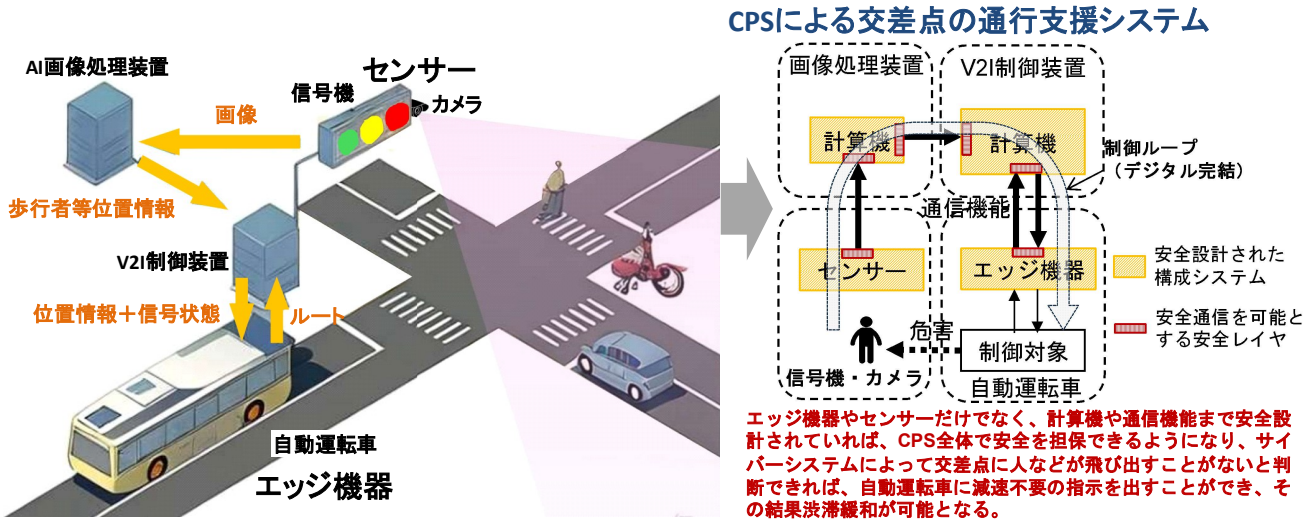


図 2.2.2　CPS 全体を安全設計した場合の効果の例

図 2.2.2 に CPS 全体を安全設計した交差点の通行支援システムにおける効果の例を示す。エッジ機器やセンサー等のフィジカルシステムの安全設計だけでなく、計算機や通信機器等のサイバーシステムに対しても安全設計を施すことで、デジタル完結した制御ループに関与するすべての構成システムが安全設計されることになり、従来はエッジ機器のみで安全判断していた運用から CPS 全体で安全判断できるようになる。これが可能になると、センサー（信号機・カメラ）で交差点付近を監視し、その情報をサイバーシステムである計算機上の画像処理によって人等が交差点に飛び出さないと判断できれば、同じく計算機上の V2I 制御装置を介してエッジ機器（自動運転車）に対して“交差点での減速不要”指示を送ることで、交差点付近での渋滞緩和が可能となる。これはエッジ機器自体では安全判断ができないが、センサー（信号機・カメラ）とサイバーシステムである計算機の組み合わせによって安全判断した結果を、エッジ機器が信用することによって実現できる運用である。

当然であるが CPS 全体として正しい安全判断をするためには、通信機能も信頼できる必要がある。しかし一般的な無線（Wi-Fi）や公衆回線（4G/5G）を使う以上、すでに普及している通信機能自体を安全設計するのは現実的ではない。そこで通信機能を情報や指示を単に伝達するだけの“土管”（IEC 61508 機能安全規格ではブラックチャネルと呼ぶ）として扱い、情報や指示に対して処理は施さない前提とする。その通信機能に対して送出する構成システムとその通信機能から受け取る構成システムの間で安全を確立した通信（以下安全通信）が実現できれば CPS 全体で安全の担保が可能となる。安全通信の一般的な実現方法は、通信機能の両端となる構成システム上に安全レイヤ（安全通信を実現するプロトコルで IEC 61508 機能安全規格で定められている）を設けることで可能となる。安全レイヤについては、3.2.2 項で詳細を説明する。

なお、画像処理等に AI 処理を利用する場合は、該当する構成システムに対する安全設計に制約が発生する。詳細は 2.2.2 項を参照のこと。

2.2.2　CPSにおける安全設計の進め方

ここでは、2.2 項２）①で示した手法（構成システム単位に基本的な安全設計を施し、これらを組み合わせて制御ループを構成した CPS 全体としての安全機能の過不足を調整する手法）で説明する。

CPS の設計において、計画当初からサイバーシステムの計算機等を含めた CPS 全体の安全設計を進めることは困難であると考えている。サイバーシステムであるクラウド（データセンター）等における現時点は、そこで使用されるサーバー、ストレージ、クラスタスイッチ等は安全設計されていない。また即日安全設計を施したものに入れ替える等、到底できるとは思えない。そのため段階を踏んで CPS の安全設計を長い期間をかけて順次進める必要があると考えている。図 2.2.3 に CPS における安全設計の進め方を示す。

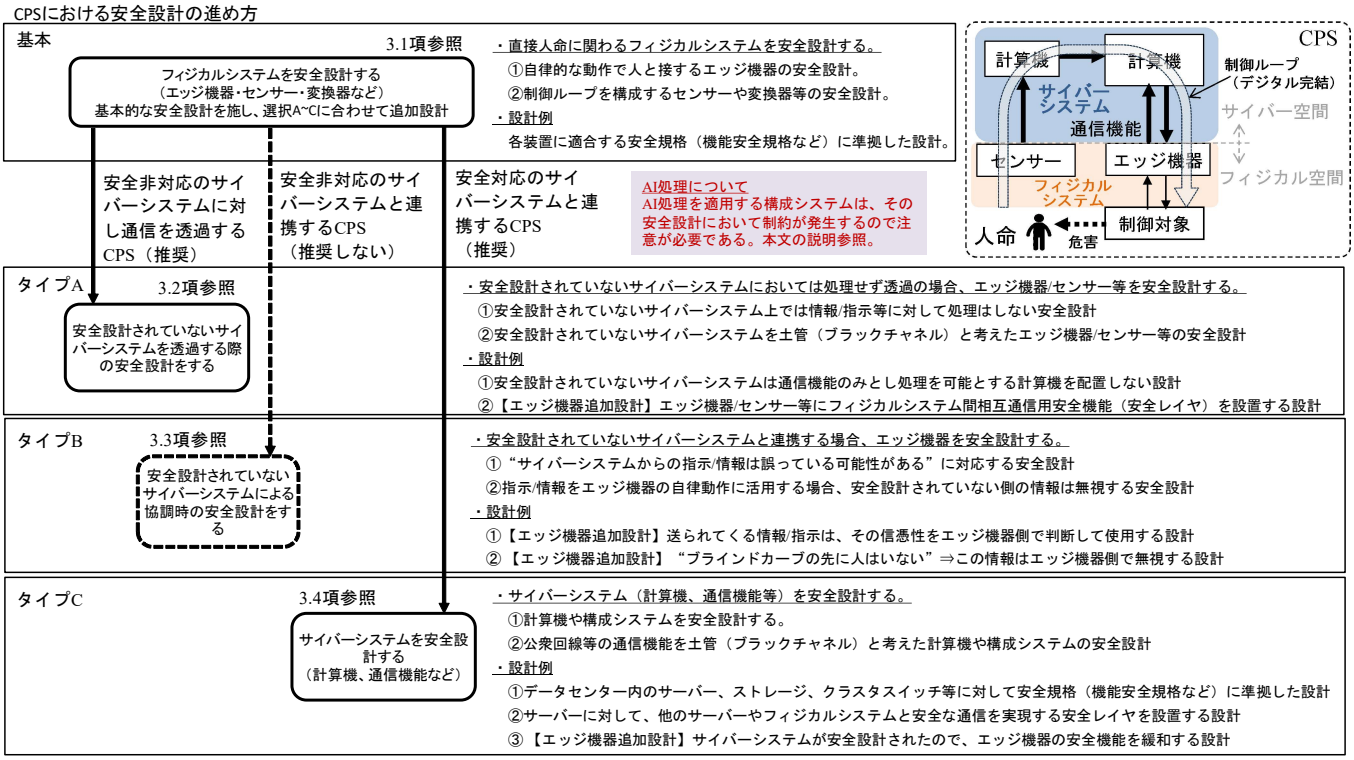


図 2.2.3　CPS における安全設計の進め方

１）基本

2.2.1 項に示したが、CPS において真っ先に安全設計するべきはフィジカルシステムであるため、基本とした。フィジカルシステムの安全設計の具体策は、エッジ機器等の開発で各事業者が実施している既存の安全性実現方法（社内品質管理、社内安全管理、PL 法遵守、製品安全規格への適合、機能安全規格への適合）と大きく違いはない（詳細は 3.1 項参照）。CPS においてフィジカルシステムのエッジ機器が安全設計されていれば、少なくとも人命の保護は可能となる。ただ CPS のうちエッジ機器だけを安全設計してもその CPS が提供できるサービス範囲はエッジ機器単体のサービス範囲と何ら変わらず CPS 構成をとる意味がない。

CPS 構成をとる以上サービス範囲を向上できることが求められるはずである。そのためタイプ A~C のいずれかの方法でサイバーシステムと接続し、それに合わせてエッジ機器の追加設計を実施する。

２）タイプ A

CPS が提供するサービスを考えたとき最も容易に提供できるサービスは、情報や指示がサイバーシステムを透過するだけで実現できるサービスであろう。つまりサイバーシステムを“土管”として扱いフィジカルシステムのセンサーとエッジ機器間で安全通信が行えるように安全設計を行う（詳細は 3.2 降参照）。こうすればサイバーシステムの計算機等は安全設計されなくてもよい。これをタイプ A としている。具体的には図 2.2.4 に示すような形態となる。

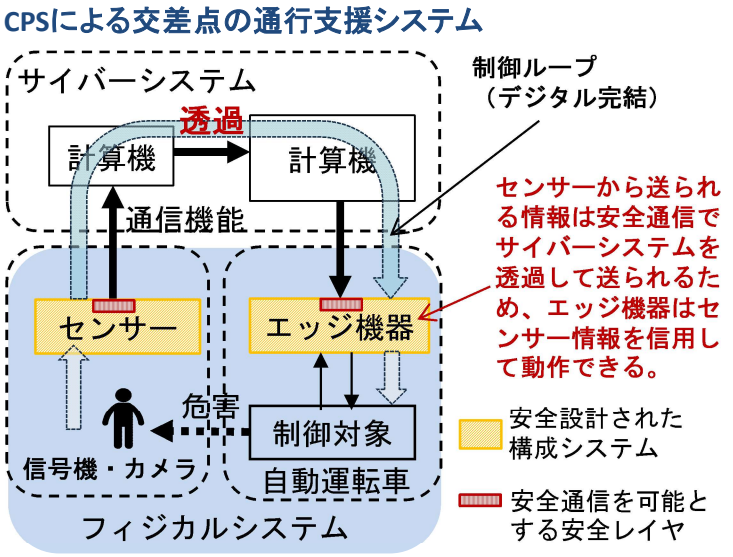


図 2.2.4　タイプ A 安全設計されていないサイバーシステムを透過する安全設計

センサー（信号機・カメラ）とエッジ機器（自動運転車）に安全レイヤを設置（追加設計）することで、この２つの間で安全通信を実現しており、サイバーシステムの計算機は処理を行わず、交差点のセンサー（信号機・カメラ）でとらえた映像をエッジ機器（自動運転車）にただ送るだけであり、エッジ機器自体が減速すべきか否かを判断する CPS である。エッジ機器はセンサー情報を信用して動作することができる。

センサー（信号機・カメラ）が安全設計され、エッジ機器との間で安全通信が実施されていれば、センサーからの情報（カメラの場合は画像等）は基本的に信頼できるものとして扱うことができる。しかし、センサー上での処理内容（例えば AI 処理等のアルゴリズム）によって、情報の信頼度が低下する可能性があり、またセンサーに対して安全設計を適用する過渡期では、安全設計の質（レベル）をすぐに必要十分に向上できないために、情報の信頼度が低下する可能性がある。そこで、センサーから送出する情報に対する信頼度を設け、情報とその信頼度を同時にエッジ機器に伝える方法が検討されている。これによりエッジ機器は信頼度を加味した情報の利用を行うことができ、その結果、エッジ機器は信頼度の低い情報を誤って利用することがなくなり、人への危害を防ぐことができる。この考え方は、RoAD to the L4（注 7）プロジェクト（RttL4）における名古屋大学の CooL4（注 8）データ連携 PF にて検討が行われている。ここでは詳細は触れないが、この信頼度を利用した SoS-CPS における事故時の責任分担の割合に使うことも検討が行われている。詳細は 2.3 項および 4 章を参照。

3）タイプ B

このタイプ B は、推奨できる使い方ではないので予め断っておく。

CPS 安全設計の過渡期にはタイプ B のような、安全設計されていないサイバーシステムとエッジ機器が協調するサービスも必要となりうると考えている。具体的には図 2.2.5 に示すような形態となる。

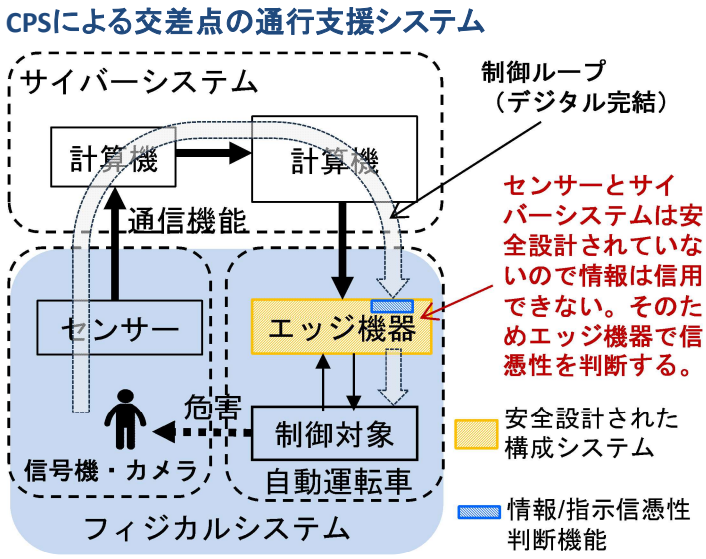


図 2.2.5　タイプ B 安全設計されていないサイバーシステムとエッジ機器が協調する安全設計

現状の安全設計されていないセンサー（信号機・カメラ）やサイバーシステム（計算機）をそのまま使うことを想定している。安全設計されていないサイバーシステムにおいて画像処理とその結果から交差点に人が存在するか否かをエッジ機器に伝送し、エッジ機器が減速すべきかを判断する CPS である。この CPS は、センサーやサイバーシステムは安全設計されていないため、そこからの情報や指示が誤っている可能性があることをエッジ機器は考慮する必要がある。つまりエッジ機器に情報や指示の信憑性を判断する機能（以下情報/指示信憑性判断機能）を設ける安全設計（追加設計）が必要になる（詳細は 3.3 項参照）。情報/指示信憑性判断機能の具体的な動作は、例えば情報が予め決めた範囲に入っているか否かで判断したり、例えば指示がエッジ機器において安全担保ができないケース（交差点には人がいないから減速するな）は無視したり、というものである。 エッジ機器は、“交差点には人がいるので早めに減速しろ”という指示は誤っていたとしてもエッジ機器をより安全に作動させることができるので、受付けても問題ないが、 “交差点には人がいないから減速しなくてよい”という指示は誤っていた場合に人命に危害が及ぶ可能性があるため、受付けてはならない。つまり CPS が目指すより便利なサービスとなるであろう“交差点での渋滞緩和”をこの CPS は実現できないことになる。

4）タイプ C

最終的にはサイバーシステムを安全設計し、CPS 全体で安全を担保したサービスを提供できることがゴールと考えている。具体的には図 2.2.6 に示すような形態となる。

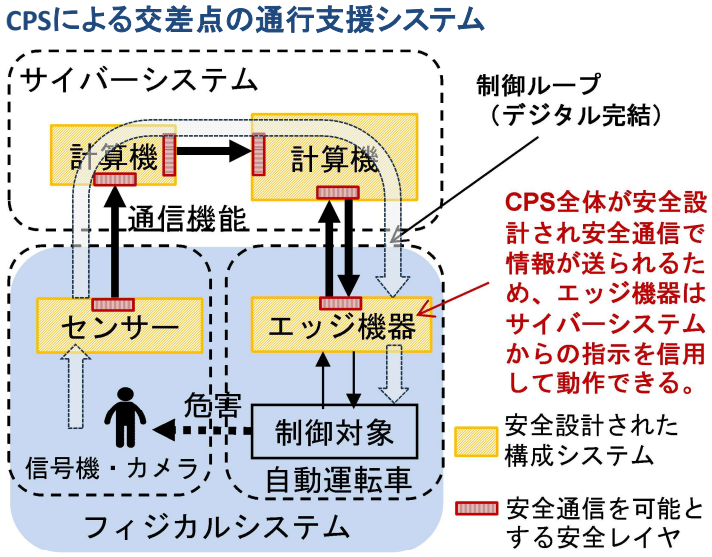


図 2.2.6　タイプ C　サイバーシステムの安全設計

サイバーシステムの計算機等の安全設計は、フィジカルシステムの安全設計と基本は同じであり、既存の安全性実現方法（社内品質管理、社内安全管理、PL 法遵守、製品安全規格への適合、機能安全規格への適合）となる（詳細は 3.4 項参照）。しかしサイバーシステムの通信機能（公衆回線 4G/5G、Wi-Fi、各社光回線等のすでに多く普及している通信網）に対して今後安全設計を施していくのは現実的ではない。もちろん専用回線を準備し、安全設計することは不可能ではないが、例えば IEC 61508 機能安全規格を満足させることは非常に難しい。そこで選択 A 同様に、通信機能に対して安全通信を実施することで対処するのが一般的である。通信機能の両端に安全レイヤを設置（エッジ機器とセンサーに追加設計）する手法である。これによりエッジ機器はサイバーシステムからの指示を信用して動作できるようになり、エッジ機器の安全機能を緩和させる追加設計を施すことで、より効率的な動作ができるようになる。

５）AI 処理の安全設計について

AI 処理を実施する構成システムは、現時点完全な安全設計（規格通りの安全設計）ができない。例えば画像処理等サイバーシステムの計算機等において AI 処理を行う場合、AI 処理結果の正しさ（CPS としての安全担保に対して信頼できる結果か否か）を判断するのが非常に難しいためである。現在 IEC 61508 機能安全規格 Ed.3 にて規格化される予定の AI に対する対処方法を WG（IEC TC65/SC65A/JWG21）にて検討中であるが、まだ正式に規格化されていない。従って AI 処理を CPS に導入する場合には、AI の処理手法や結果の信憑性判断方法を上記 WG に確認する等した上で、CPS 設計者および SoS-CPS 設計者において十分レビューして適用を決定する必要がある。さらに、タイプ A でも説明したが、AI 処理結果に対する信頼度を付加する方法も検討されている。　AI 処理の安全設計については、3.4.3 項を参照のこと。

2.3 異なった事業者で構成される CPS（SoS-CPS）における安全設計の考え方

異なった事業者で構成される CPS（SoS-CPS）における安全設計の考え方の基本を図 2.3.1 に示す。本図は SoS-CPS の構成の違いによって、人命に関わる用途へ適用（安全用途）できるか否かの考え方を示したものである。詳細は 4 章を参照。

図 2.3.1 中において、〇は適用可能、△は制約付きで適用可能、×は適用不可を示す。

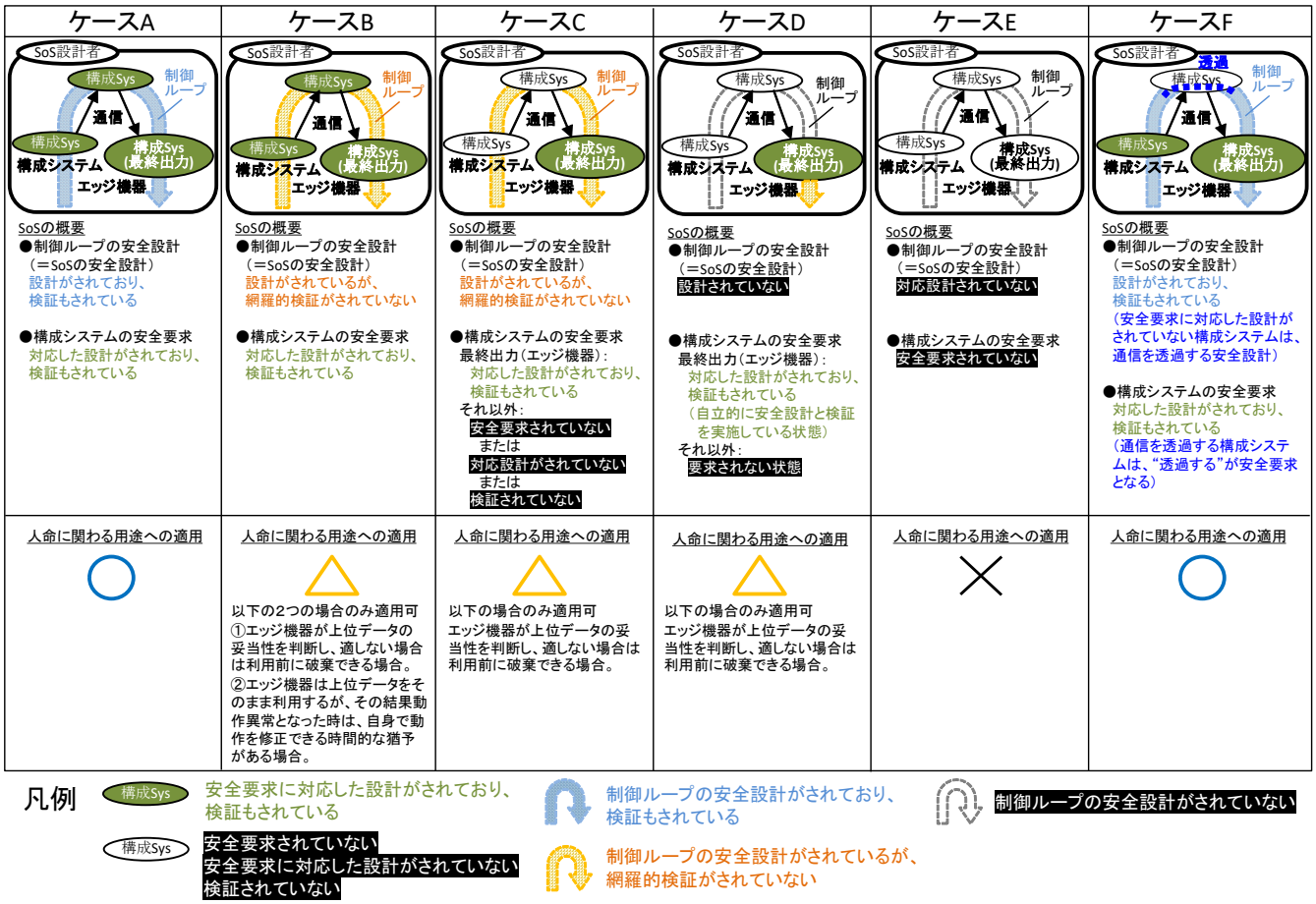


図 2.3.1　SoS-CPS における安全用途への適用の考え方

3 CPS の安全設計

本章では、2.1 項および 2.2 項で説明した、直接人命に関わる CPS における安全設計の考え方に対して、その詳細について説明する。はじめに CPS におけるフィジカルシステムの安全設計について 3.1 項で説明する。2 点目にフィジカルシステムの構成システム間（サイバーシステムは透過）で安全を担保する設計について 3.2 項で説明する。3 点目に安全設計されていないサイバーシステムとフィジカルシステムを協調運転する際、フィジカルシステム側に追加で考慮すべき安全設計について 3.3 項で説明する。最後に CPS におけるサイバーシステムの安全設計について 3.4 項で説明する。

3.1 フィジカルシステムの安全設計

CPS の構成システムにおいて、直接人命に関わる可能性のあるフィジカルシステム（センサーやエッジ機器等）を安全設計することが、CPS の安全設計においては基本となる。3.1 項では、フィジカルシステムの安全設計の具体策について説明する。2.2.2 項の手順 1 でも説明したが、フィジカルシステムの安全設計の具体策は、センサーやエッジ機器等の開発で各事業者が製品開発で実施している既存の安全性実現方法（社内品質管理、社内安全管理、PL 法遵守、製品安全規格への適合、機能安全規格への適合）そのものである。従って読者がこのような安全設計の具体策を理解されているのであれば、本 3.1 項は読み飛ばして頂いて問題ない。

3.1.1 CPSの基本構成とフィジカルシステムの位置づけ

CPS の基本構成を図 3.1.1 に示す。フィジカルシステムのセンサーやエッジ機器等は、人が存在する空間であるフィジカル空間に位置され、サイバーシステムの計算機（クラウド等）と通信機能で接続される。計算機が近くに設置される場合は、通信機能は有線、Wi-Fi またはローカル無線等になるであろうが、計算機がクラウドの場合は、一般的にフィジカルシステムとサイバーシステムのクラウドとは遠距離にあるため、通信機能は公衆回線（4G や 5G 等）が使用される場合が多い。

CPS として正常運用できなくなった場合に発生する人命への危害の大きさは、CPS によって異なる。それゆえ、すべての CPS に対して闇雲に強固な安全性を施す必要はなく、CPS の目的に応じて必要な安全性が実現できるように、それぞれの CPS の性質を考慮した上で、フィジカルシステムに対して、例えば ISO 13849-1 機械安全規格に従うならばパフォーマンスレベル（PL）、例えば IEC 61508 機能安全規格や ISO 26262 自動車の機能安全規格に従うならば安全度水準（SIL や ASIL）を設定し、それに従った安全設計を実施する。

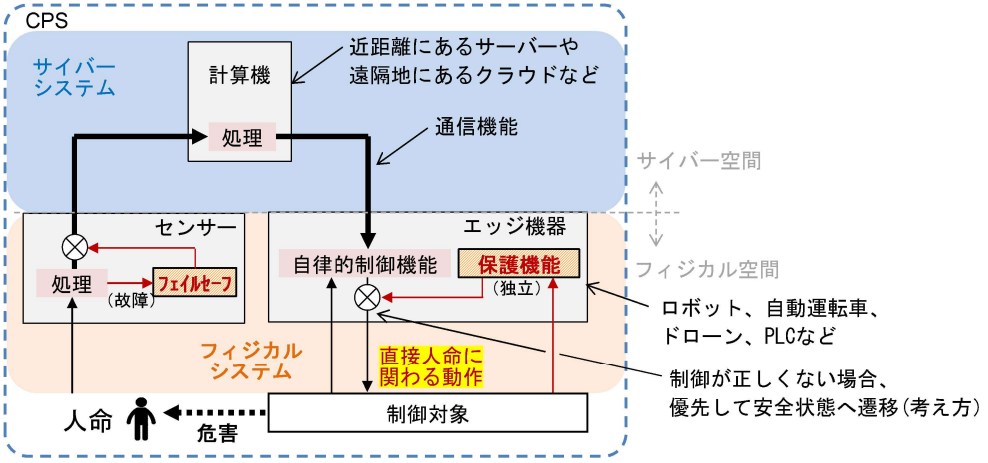


図 3.1.1　CPS の基本構成

3.1.2　フィジカルシステムにおける安全設計の基本

フィジカルシステムにおける安全設計の基本は、フィジカルシステムの各構成システムによる処理や制御が機能不全になった場合、フェイルセーフ機能や保護機能が確実に作動し、人へ危害を与えないように決められた時間内に“安全状態（3.1.3 項参照）”へ遷移させるように設計することである。この“安全状態”とは、フィジカルシステム（エッジ機器）が制御対象に出力する値を、制御対象が危険側の動作をしないように安全状態に固定される値とすることある。安全状態に固定される具体的な値は、エッジ機器と制御対象の間で事前に取り決めしておく。一般的な例は、エッジ機器からの出力をオフ（切断）し、信号線をハイインピーダンスにすることで、制御対象は安全状態に固定されるというような使い方である。出力をオフすることが最も簡単で確実（例えば停電時にも出力オフは容易にできる）である。

エッジ機器の自律的な制御機能に対しては、独立した保護機能を設置すべきである。独立した保護機能によって安全状態に遷移できる場合は、保護機能のみに安全設計を施し、自律的な制御機能に対しては安全設計を施す必要はない。安全状態が複雑であり保護機能だけでは安全状態に遷移させることができない場合は、自律的な制御機能と協力して安全状態に遷移させる必要がある。このケースでは、自律的な制御機能に対しても安全設計が必要となる。

フィジカルシステムのエッジ機器以外（自律的な制御を行わない機器）における構成システム（例えばセンサー等）においては、処理機能が故障した際にフェイルセーフ機能が働くように処理機能も含めて、安全規格に準拠した安全設計が必要である。

１）例１：センサーの安全設計

例えば、センサーの安全設計は以下を満足する必要がある。図 3.1.2 参照。

① センサーの処理機能が不全の場合にセンサーを安全状態に遷移させるフェイルセーフ機能を装備する。

② 処理機能とフェイルセーフ機能は独立関係にできないため、両方を安全設計する（注３）。

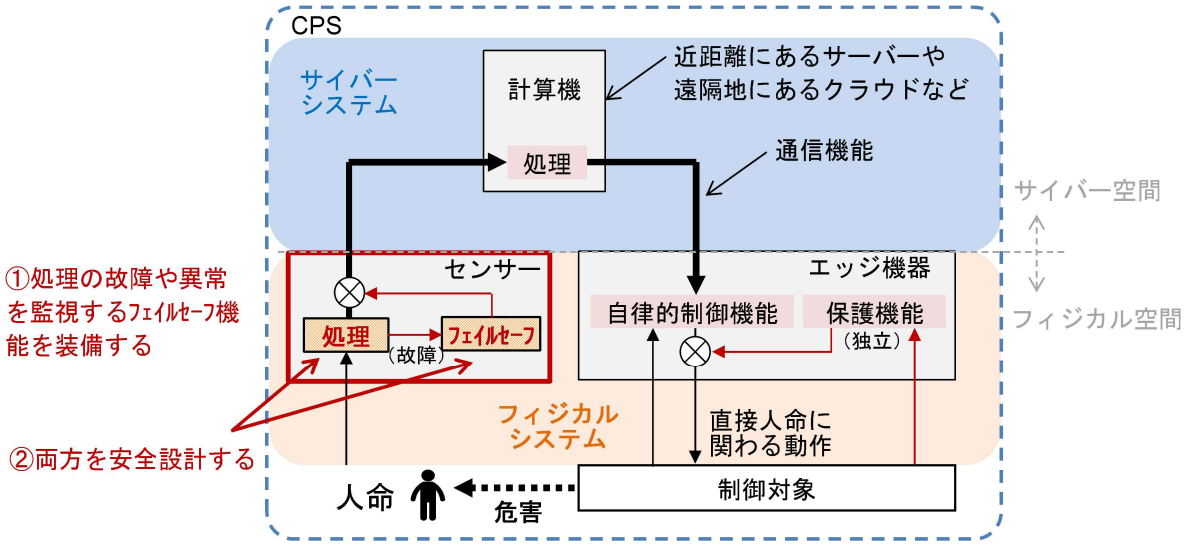


図 3.1.2　センサーの安全設計例

2）例 2：エッジ機器の安全設計

例えば、エッジ機器は以下を満足する必要がある。エッジ機器は自律的に動作する機能をもつことから、フィジカルシステムの構成システムの中でも人に危害を与える可能性が大きいため、安全設計は以下を満足する必要がある。図 3.1.3 参照。

③　自律的な制御機能が機能不全の場合にエッジ機器を安全状態にする保護機能を装備する。

④　保護機能は自律的な制御機能と独立性を保つ（注４）（直接人命に関わるため独立性は必須）。

⑤　保護機能を安全設計する。

⑥　自律的な制御機能に対し目的に応じて（注５）、安全設計する。

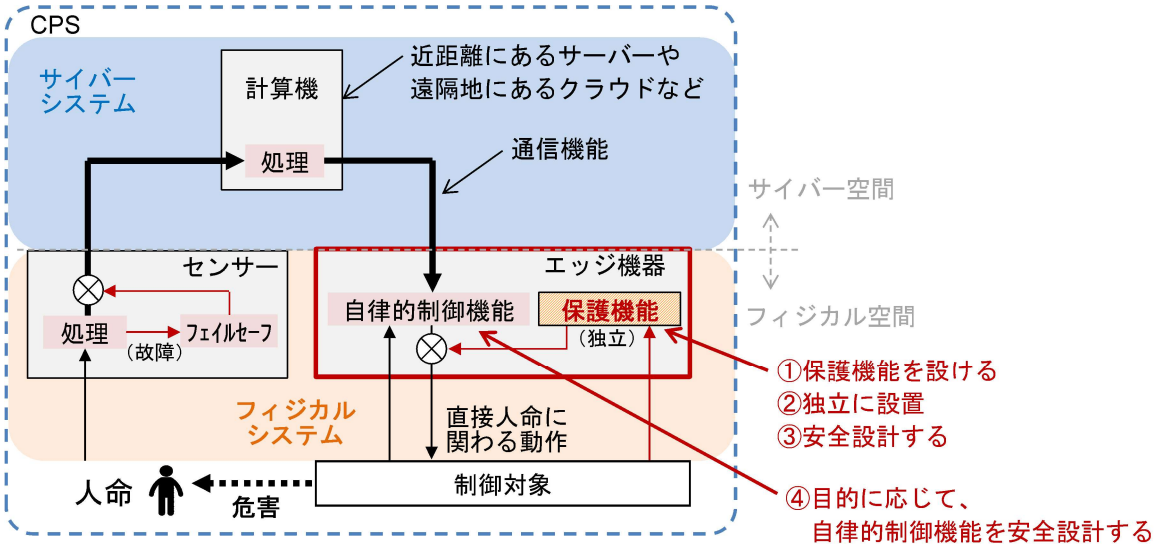


図 3.1.3　エッジ機器の安全設計例

3.1.3　安全状態の定義

安全設計を進めるためには、まず CPS における安全状態を定義する必要がある。CPS における安全状態とは、安全設計されたフィジカルシステムが、人命に危害を与えないように予め定義した状態に遷移したことを意味する。つまり CPS における安全状態＝フィジカルシステムの安全状態であり、フィジカルシステムによって人命を保護している状態である。従って状況に応じて安全状態が異なるため、CPS の目的に応じたリスク分析を十分に行った上で、フィジカルシステムにおける構成システム（センサーやエッジ機器等）に対して、それぞれ安全状態を決める必要がある。

フィジカルシステムが安全状態に遷移するのは次のいずれかである。

① 安全設計した保護機能が働いたとき（自律的な制御機能の動作が異常であることを保護機能が検出したとき）
② 安全設計した保護機能が故障したとき（保護機能が自身の故障を検出したとき）
③ 安全設計したセンサー等の処理部とフェイルセーフ機能が故障したとき。
④ 安全設計したエッジ機器の自律的な制御機能が故障したとき。

いずれも、予め定義した“安全と考えられる状態”に、決められた時間内に遷移させる。

安全状態の一例を以下に説明する。（あくまでも例であり、状況に応じて異なる場合がある）

・センサーの場合、サイバーシステムに誤ったデータを送出しないように送信を停止した状態。
・自動運転車の場合、人や他車の通行を妨げない場所に自車を退避し停止した状態。
・ロボットの場合、一般的にはその場で停止した状態。
・ドローンの場合、人の居ない場所に退避させた状態（地上か空中かは問わない）。
・原子炉の場合、放射能漏れないよう制御棒挿入状態かつ原子炉冷却状態かつ発電用蒸気弁閉鎖状態。

3.1.4　エッジ機器の保護機能と自律的な制御機能の役割

エッジ機器は自律的に動作する機能をもつことから、フィジカルシステムの構成システムの中でも人に危害を与える可能性が高いため、個別に安全設計の考え方を説明する。

エッジ機器の保護機能は、人への危害を防ぐための最終手段であるため、パフォーマンスレベル（PL）や安全度水準（SIL や ASIL）が比較的高い安全設計が必要となる。

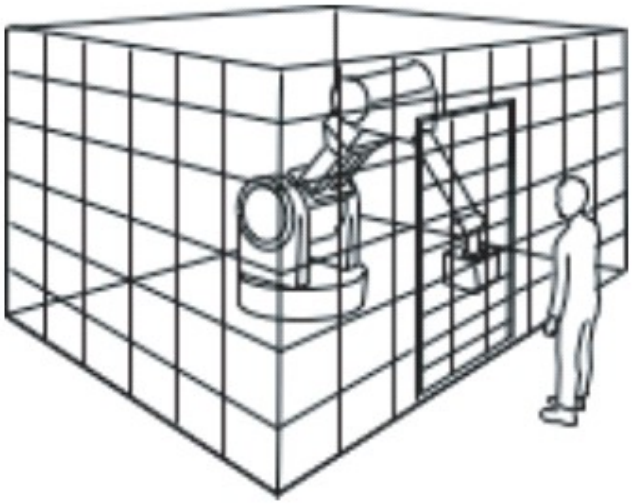
自律的な制御機能は、安全設計が不要な一般の制御機能と、安全設計が必要な安全に関わる制御機能に分かれる。考え方は、保護機能のみで定義した安全状態に遷移させることができる場合は、制御機能に対して安全設計は不要となり、一般の制御機能として扱う。それに対し、定義した安全状態に遷移させるために保護機能と制御機能の連携が必要な場合は、制御機能に対しても安全設計が必要となり、安全に関わる制御機能として扱う。安全に関わる制御機能は、その制御対象の性質によって（用途に応じて）安全設計のパフォーマンスレベル（PL）や安全度水準（SIL や ASIL）は保護機能よりも低くて問題ない場合がある。

１）役割の例

① 例１：エッジ機器が工作用ロボットの場合

工作用ロボットをエッジ機器とした場合、限定されたエリアの中にロボットを設置することができれば、ロボットの保護機能によってエリアに人が侵入したことを検知しロボットを瞬時に停止させる（人とロボットの距離が十分ある段階で保護機能が働く）ことができるので、ロボット自体を動作させるための自律的な制御機能に対して安全設計は必要ない。この場合の自律的な制御機能は一般の制御機能の扱いとなる。ただし、人が誤って限定されたエリアに侵入できないよう、また侵入したことを保護機能が確実に検出できるように、図 3.1.4 の通り柵等を設置することが原則となる。

限定されたエリア（柵）の設置



出典：平成29年度　厚生労働省委託 中央労働災害防止協会
機能安全を導入した産業用ロボットシステムの安全関連システムの設計
URL： https://www.mhlw.go.jp/new-info/kobetu/roudou/gyousei/anzen/dl/180320-2.pdf

図 3.1.4　限定されたエリアを設けて安全を確保

② 例２：エッジ機器が自動運転車の場合

自動運転車をエッジ機器とした場合、自律的な走行制御機能が故障した際に、保護機能である補助ブレーキ機能等によって停止することは可能である。しかし一般的に自動運転車の安全状態は、その場で停止することではなく（停止すると後続車に衝突されるリスクがあり人に危害が及ぶことがある）、人や他車の通行を妨げない場所に自車をすみやかに退避し停止することだと考えられる。つまり安全状態に遷移させるためには、保護機能である補助ブレーキ機能等だけでなく、自律的な制御機能であるステアリング制御機能、アクセル制御機能、アンチロックブレーキ機能等と連携して行うことが必要となる。従ってこれらの自律的な制御機能に対しても安全設計を考慮する必要があり、安全に関わる制御機能として扱う。

表 3.1.1 に、エッジ機器の保護機能と自律的な制御機能（安全に関わる制御機能、一般の制御機能）の役割について説明する。

表 3.1.1　保護機能と自律的な制御機能の役割

	項目	保護機能 （安全設計が必要）	自律的な制御機能	
			安全に関わる制御機能 （安全設計が必要）	一般の制御機能 （安全設計は不要）
1	用途	人への危害を防止	人命に関わる制御 （保護機能と連携する必要あり）	人命に関わらない制御 （但し保護機能が作動している条件下）
2	担当機能	自律的な制御機能に優先して動作し、エッジ機器を積極的に安全状態に遷移させる機能	保護機能と連携して安全性をより高めるために必要な安全関連制御機能。用途（人命への影響度）に応じた安全設計が必要。	限定されたエリア内で動作する工作用ロボットなど、独立した保護機能が作動している条件下で人への危害の可能性がない制御。安全設計は不要。

2）代表的リスクと対応する安全設計

エッジ機器における保護機能、自律的な制御機能（安全に関わる制御機能、一般の制御機能）について、安全設計を行う上で考慮する観点からの代表的リスクと対応策について、表 3.1.2 に説明する。

表 3.1.2　代表的リスクと安全設計による対応策

	項目	代表的リスク	保護機能 （安全設計が必要）	自律的な制御機能	
				安全に関わる制御機能 （安全設計が必要）	一般の制御機能 (安全設計は不要)
1	システムの外的要因への対処	人への危害	・本質安全の設計（人が立ち入れない構造、爆発的/即効的な反応が無い、耐火、等） ・フェイルセーフな設計 3.1.6項参照 （予め決めた時間内に予め決めた安全側へ挙動、等）	・フェイルセーフ設計 3.1.6項参照 （予め決めた時間内に予め決めた安全側へ挙動）	・保護機能がある前提で制限なし ・但し安全設計は不要であるがファイルセーフ的な考慮は可能な限り実装したい 3.1.6項参照
2		人による起因	・誤操作誤不動作が起きない フールプルーフ設計 3.1.7項参照 （カバー付きの目立つ大型非常ボタンの採用、等）	・誤操作誤不動作が起きない フールプルーフ設計 3.1.7項参照 （操作監視画面の視認性や操作器具の配置や形状への配慮、等）	・保護機能がある前提で制限なし ・但し安全設計は不要であるがフールプルーフ的な考慮は可能な限り実装したい 3.1.7項参照
3		サイバー攻撃	・原則として（外部接続しない）独立した設計 そのため影響を受けない 3.1.5項参照	・制御セキュリティを考慮した設計 （IEC 62443やISA-Secureの要求、被攻撃時も誤動作誤不動作なく、安全制御機能を継続など）セキュリティ参照	・保護機能がある前提で制限なし
4		テロ行為	・十分なフィジカルセキュリティを設計 ・適用分野によっては、テロ攻撃（航空機や車両などの突入、爆発物、ガス・放射線、等）に耐える要求に対応した設計 セキュリティ参照	同左	・保護機能がある前提で制限なし
5		自然災害	・必要により、大規模な自然災害（竜巻、洪水、津波、なだれ、火災、放射能、等）でも機能を失わない（設置場所、動力等の）設計	・軽微な自然災害（地震、台風等）では機能を失わない（設置場所、動力等の）設計	・保護機能がある前提で制限なし
6	システムの内的要因への対処	計算機（クラウドなど）の故障、 計算機とエッジ間の通信の故障	・保護機能と計算機（クラウド等）は原則接続しない設計（独立した設計）3.1.5項参照	・安全設計されていない計算機指示（クラウド等からの指示）の妥当性を確認する設計 （保護機能が有効な範囲の指示のみ受け入れ） ・処理結果の妥当性を確認する設計 （計算機指示の処理結果が現状と矛盾ない場合のみ制御実行）3.3項参照	・保護機能がある前提で制限なし
7		保護機能の故障	・フェイルセーフ設計 3.1.6項参照 ・極力シンプルに設計	―	―
8		安全に関わる制御機能の故障・遅延	・制御機能と保護機能の同時機能喪失を防ぐ独立設計（動力、設備、場所、等） ・同じ原因で保護動作が必要な事象を検知失敗しないよう、制御システムと別原理（別のセンシング事象、等）により設計 3.1.5項参照	・フェイルセーフ設計 3.1.6項参照	―
9		一般制御システムの故障・遅延	・制御機能と保護機能の同時機能喪失を防ぐ独立設計（動力、設備、場所、等） ・同じ原因で保護動作が必要な事象を検知失敗しないよう、制御システムと別原理（別のセンシング事象、等）により設計 3.1.5項参照	―	・保護機能がある前提で制限なし ・但し安全設計は不要であるがファイルセーフ的な考慮は可能な限り実装したい 3.1.6項参照
10		設計不十分・バグ	・安全設計（安全規格等に準拠した設計）3.1.8項参照	同左 3.1.8項参照	・事業者における品質水準を満足した設計（事業者における設計基準の適用）
11		検証不十分・ミス	・合理的に想定・推定されるリスクへの対処を設計し、正しく設計構築されたことを第三者が検証 ・事故原因や再発防止の施策の特定ができるログ・トレースを装備		

表 3.1.2 において、重要と考えられる対応策（保護機能の独立、フェイルセーフ、フールプルーフ、安全規格等の適用）についての詳細を 3.1.5 項～3.1.8 項に、安全設計されていないサイバーシステム（計算機やクラウド等）から指示を受ける場合についての詳細を 3.3 項に、それぞれ説明する。また要約した設計指針を下記に説明する。

(1) 保護機能の設計指針

① 十分に安全なプロセスで構築する（安全規格等に準拠した設計を推奨する）
② 規定時間内に定義した安全状態（停止の場合が多い）になるように、積極的に作動させる（フェイルセーフ設計）
③ ミス操作、誤信号入力等に対し十分なフールプルーフを考慮する
④ 制御機能と保護機能が同時に機能喪失しないよう共通部を持たない別装置として構築する（状態を監視する検知機能が同時に失敗しないよう別原理でセンシングする）
⑤ サイバーシステムの計算機（クラウド等）と接続しない（指示を受けない。独立で判断し動作する。）

(2) 安全に関わる制御機能の設計指針

① 十分に安全なプロセスで構築する（安全規格等に準拠した設計を推奨する）
② 故障等制御機能喪失時、制御対象に悪影響を与えないよう、規定時間内に定義した安全状態（安全と定義した出力値）に遷移する（フェイルセーフ設計）
③ ミス操作、誤信号入力等に対し十分なフールプルーフを考慮する
④ 安全設計されていないサイバーシステムの計算機（クラウド等）や通信機能の故障を考慮して、指示や処理結果の妥当性を判断する

(3) 一般的な制御機能の設計指針

① 保護機能が独立して装備される条件下では、安全設計は不要であるが、以下のことを考慮する
② 可能な限りフェイルセーフ的な考慮を実装
③ 可能な限りフールプルーフ的な考慮を実装
④ 事業者の品質水準を満足した設計

3.1.5 エッジ機器における保護機能の分離

自律的な制御機能と保護機能が同時に機能を喪失することが無いように、図 3.1.5 に説明するように保護機能を独立に構築する。

① 独立すべき内容は、エッジ機器の制御対象の性質によるが、例えば使用部品、設置場所、センサー、給電ルート、設計者、評価/検証者等である。潜在的不良（バグ含む）や物理的な故障等共通要因故障を排除する目的である。
② 保護機能は、自律的な制御機能に優先して作動する設計とする。
③ 自律的な制御機能と保護機能を装備するエッジ機器は、確実な動作を実行できるように、可能な限り設備等の近傍に設置することが望ましい。
④ 保護機能はサイバーシステム等と接続してはならない。独立系として動作する必要がある。

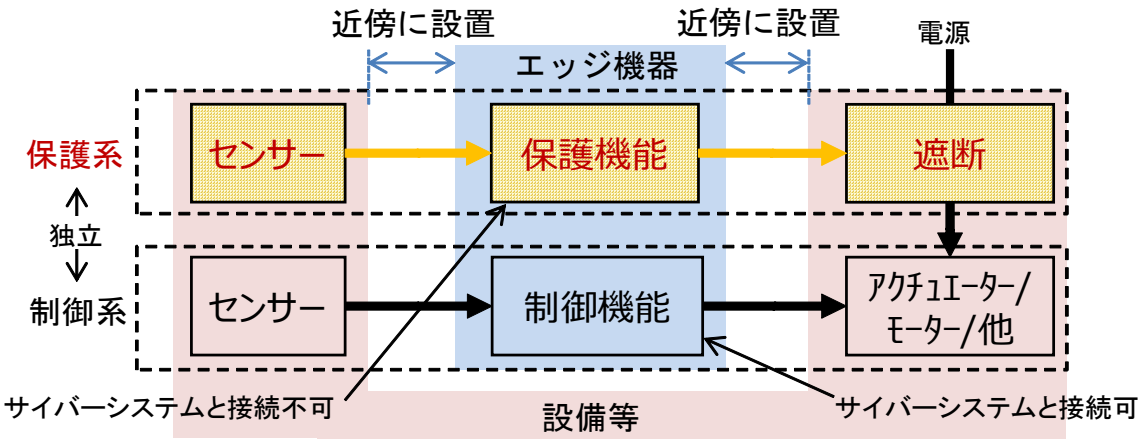


図 3.1.5　保護機能と制御機能を独立に構築した例

3.1.6　フェイルセーフ設計

フェイルセーフ設計とは、装置やそれを構成する部品は必ず壊れることを前提とし、故障時や異常発生時に安全状態へ遷移させることで、人に危害を与えないようにシステムを構築する設計方法である。 わかりやすい例では、踏切遮断機が故障した場合 、重力により自ら遮断かんが降りてくる（自重降下）機構を設けることで踏切通行者の安全を確保している。図 3.1.6 にフェイルセーフ設計の考え方をロジック表記で示す。

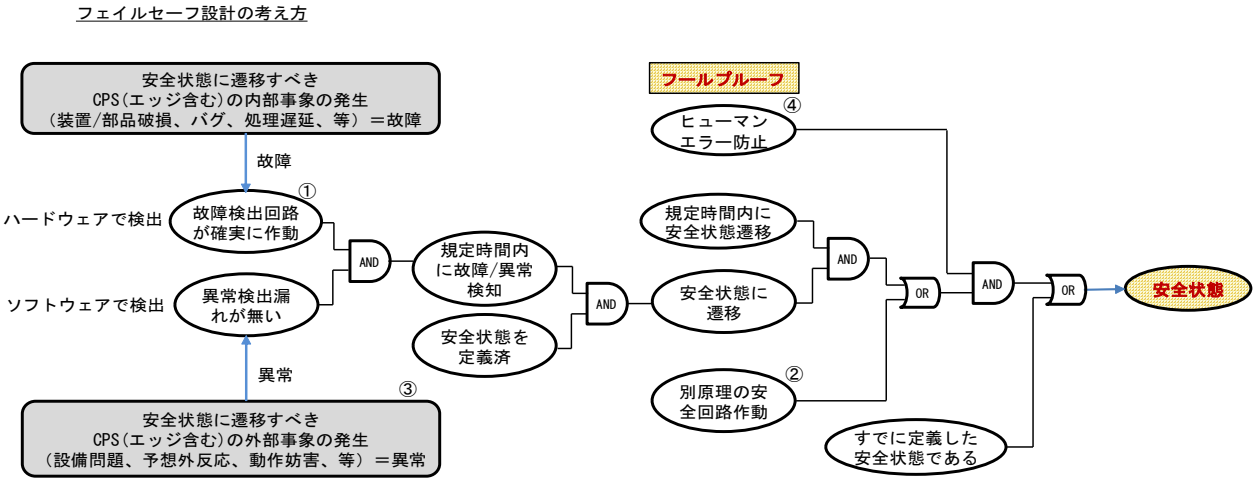


図 3.1.6　フェイルセーフ設計の考え方のロジック表記

図中の AND 条件がすべて成立した時に、エッジ機器が安全状態であることを表している。安全規格によれば、正しく制御ができている期間を安全状態には含めない。停止することが安全と定義したエッジ機器では、制御が続行される期間は停止ができていない（危険状態である）ためである。従って、安全状態であるためには、電源 OFF 状態等すでに定義した安全状態にあるか、故障または異常が発生しすべての AND 条件が成立した時となる。このロジックの AND 条件のそれぞれは、設計にミスが許されない。ミスがあれば永遠に安全状態に遷移しない。

故障はエッジ機器内部で発生した事象（ハザード）を意味し、異常はエッジ機器外部で発生した事象（ハザード）を意味している。故障も異常も確実に検出できて初めて安全状態になる。漏れがあっては安全状態とは言えない。確実に検出しても規定時間内に検出できなければ意味がない。同様にせっかく安全状態に遷移しても規定時間内に遷移できなければ意味がない。

① 故障検出回路が確実に動作する割合が安全規格で定義される PFH や PFHd に含まれるので、故障検出回路の故障を FMEDA に含めて計算する。パフォーマンスレベル（PL）や安全度水準（SIL や ASIL）が高い場合は、故障検出回路に診断回路を付加させて確実性を向上させる。この場合診断回路さらに診断する必要はない。診断回路の故障確率は PFH や PFHd には含まないため。

② 万が一安全状態に遷移できなかった場合を想定し、パフォーマンスレベル（PL）や安全度水準（SIL や ASIL）が高い必要のあるエッジ機器においては、別の原理で安全状態に遷移する他の手段（バックアップ）を準備することが望ましい。

③ エッジ機器の外部事象である異常の定義は、どこまで想定できるかと、その発生確率で決める。

④ ヒューマンエラー防止を考慮する。但し完全に防止することはできないので十分条件ではない。

3.1.7　フールプルーフ設計

フールプルーフ設計とは、人がミスをしようとしてもできないようにする工夫を盛り込んだ設計である。フールとは「愚者」、プルーフは「耐える」という意味がある。 図 3.1.7 にフールプルーフの具体例を示す。 考え方は、出来るだけミスできないようにすることである。完全にミスを防ぐことはできない。

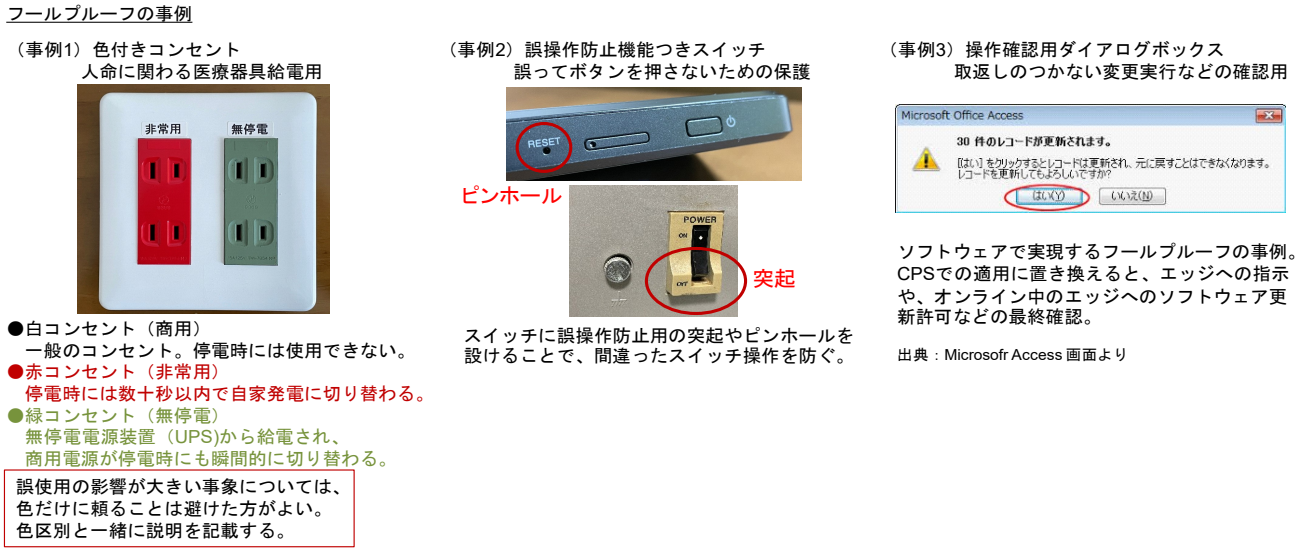


図 3.1.7　フールプルーフの具体例

1） 事例 1：色付きコンセント

コンセントに色を付けることで、停電に対処した給電ができるか否かを判断できるようにしている。医療機関等の人命に関わる医療器具の給電用として使用する。

商用電源のコンセントは一般的に白色だが、商用電源が停電時に数十秒以内に自家発電に切り替わるコンセントは赤色（非常用）表示となる。また瞬時に切り替わり停電が発生しないコンセントは緑色（無停電）表示となる。

2） 事例 2：誤操作防止機能つきスイッチ

操作ボタンが誤って押されないように、ピンホールの奥にスイッチを設ける手法や、誤ってスイッチを切られないように、OFF 側に突起を設ける手法で、スイッチの操作誤りを防止する。意思のない操作（誤って触れる、モノが当たる、等）から防護する。

3） 事例 3：操作確認用ダイアログボックス

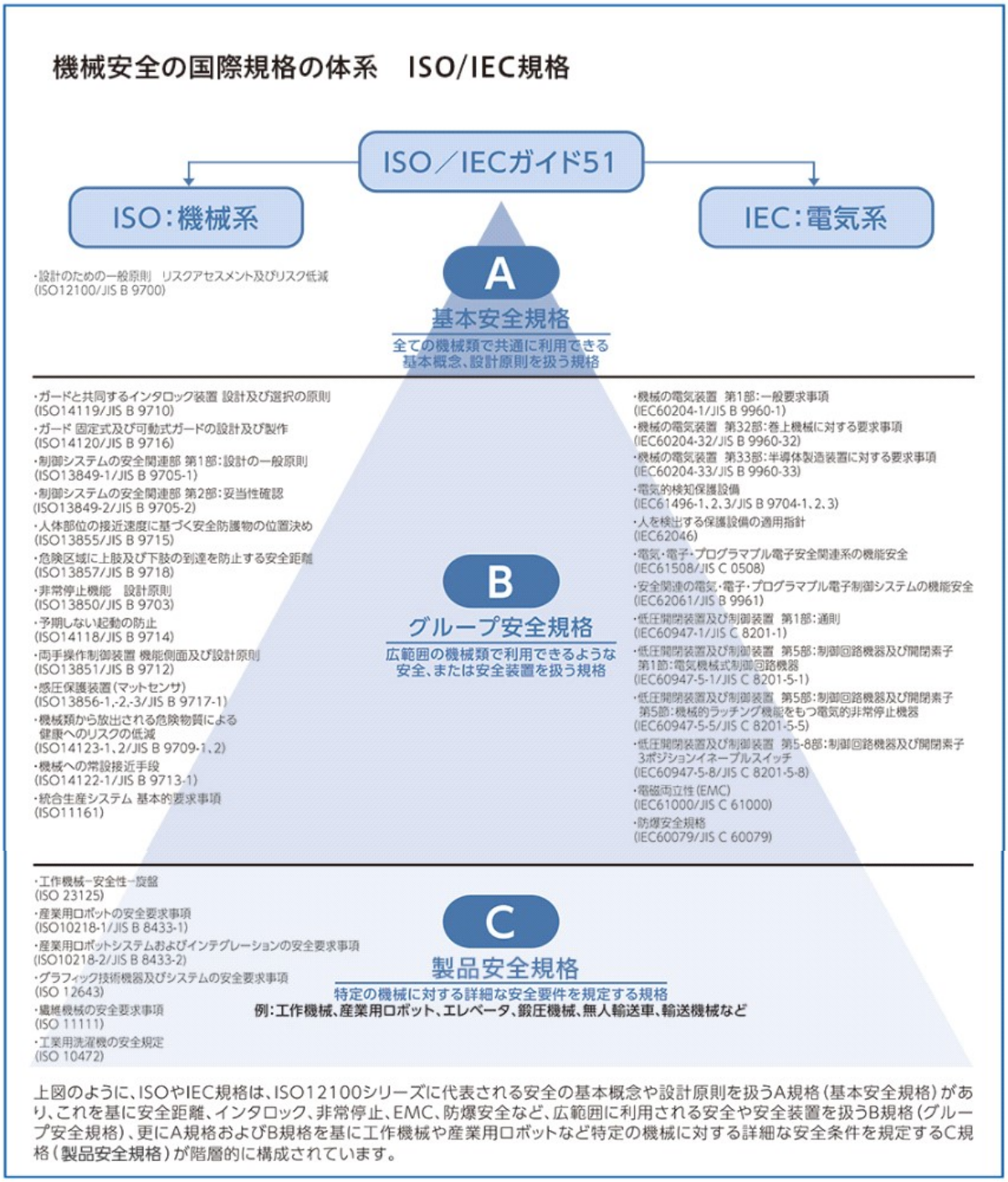
ソフトウェアで実現する誤操作防止の例で、取り返しのつかない操作（例えば変更作業等）の最終確認用として使用する。例えば、オンライン中のエッジ機器へのソフトウェア更新許可の確認等に使用する。

人によって感知できる色覚が異なることから、誤使用の影響が大きい事象については、色だけに頼ることは避けた方がよい。

3.1.8 安全規格に準拠した設計

人に危害を与えないようにフィジカルシステム（センサーやエッジ機器）を設計するためには、独自の設計手法や判断（事業者の品質水準や設計基準だけ）で設計するのではなく、世の中に知られている安全規格等に準拠して設計することを推奨する。理由は、事故が発生した際、オープンな規準ではない独自の設計手法等では、第三者への説明の十分性（説明責任）が難しいと考えられるためである。また安全規格に準拠した進め方が正しいか否かを、認証機関等で検証（受査）することを推奨する。以下に安全規格に準拠して設計する際の代表的な考え方を説明する。詳細は規格書等を参照のこと。

安全規格はアンブレラ体系で構成されている。安全規格の最上位に位置するガイド 51（ISO/IEC GUIDE 51、日本では JIS Z 8051）では、安全とは、人・財産・環境に対し許容できないリスクがない状態としているが、本ディスカッションペーパーにおいては、1.5.3 項で説明した通り、安全の定義として「人命への許容できないリスクがない状態」とした。財産と環境は敢えて除外している。人に危害を与えないという概念から、本ディスカッションペーパーにおいては機械安全を参考として説明している。図 3.1.8 に機械安全の国際規格体系を説明する。



出典：安全に関する国際規格（ISO/IEC）(idec.com)

図 3.1.8　機械安全の国際規格体系

進め方としては、ガイド 51 を参照してから、フィジカルシステムの各構成システムの性質にあった安全規格を適用すればよい。また厚生労働省は、機能安全活用ガイドを発行しており、図 3.1.9 に説明するような体系で参照することを推奨している。例えばエッジ機器の安全設計は、図中の赤色部分の手順で実施することを推奨する。

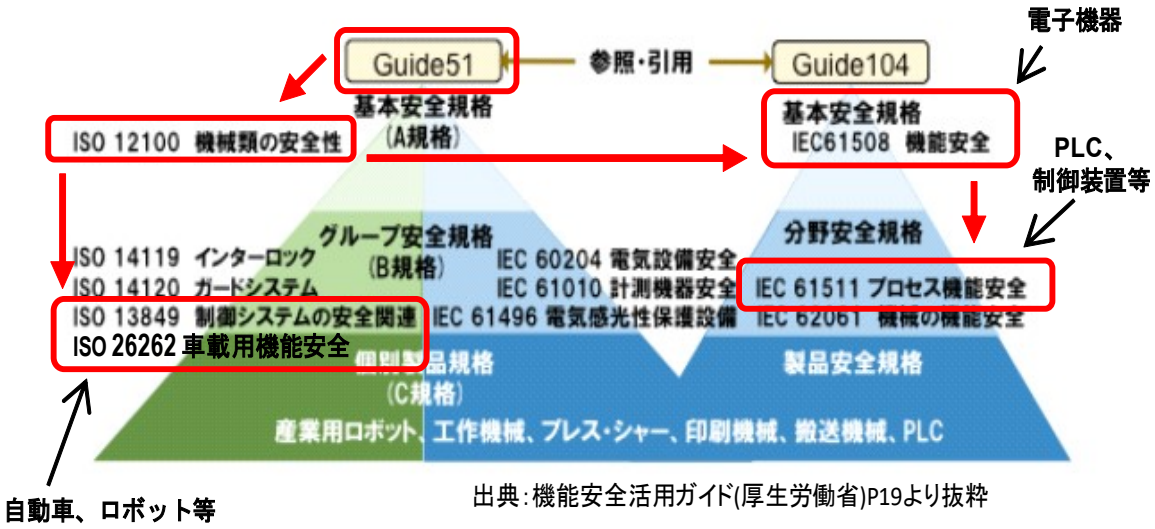


図 3.1.9　エッジ機器の安全設計の参照順番の具体例（一例）

例えば機械系の自動車関連は ISO 26262 を参照、ロボットは ISO 13849-1 を参照、電子機器系の PLC（プログラマブルロジックコントローラ）や制御装置は IEC 61511 を参照等。そして電子機器を使用するエッジ機器全体については併せて IEC 61508 を参照するといった具合である。

安全設計の詳細な進め方は、各安全規格を参照して頂きたい。各規格共通して重要な項目（以下）については、本ディスカッションペーパーでも説明する。

① リスクアセスメント
② パフォーマンスレベル（PL）や安全度水準（SIL や ASIL）の設定
③ システマティック故障とランダムハードウェア故障の考慮
④ 第三者検証

なお、ISO や IEC の安全規格に限らず、日本政府からもロボット等に対するする安全ガイドラインが発行されている。これらの安全ガイドラインは、おおよそリスクアセスメントと事故が発生した際の運用について説明されている。ISO や IEC の安全規格に説明されているパフォーマンスレベル（PL）や安全度水準（SIL や ASIL）等の定義について、またリスクの低減策についての説明はない。表 3.1.3 に国内安全ガイドライン一覧を示すので、併せて参照のこと。

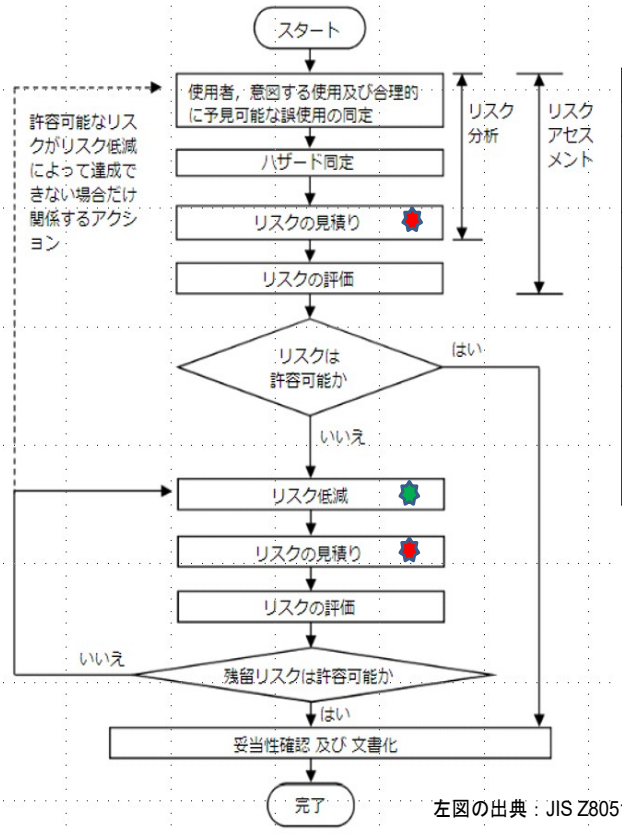
表 3.1.3　国内における安全ガイドライン（一例）

No	種類	安全ガイドライン	発行元	URL	適用範囲	備考
1	ロボット	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（第一版）	ロボット革命・産業 IoT イニシアティブ協議会 Robot Revolution & Industrial IoT Initiative	ロボット革命イニシアティブ｜生活支援ﾛﾎﾞｯﾄ及びﾛﾎﾞｯﾄｼｽﾃﾑの安全性確保に関するｶﾞｲﾄﾞﾗｲﾝ(第一版)／ｻﾌﾞWG報告書 公開の件 (jmfrri.gr.jp	製造、実証実験、販売、管理	（注6）
2		次世代ロボット安全性確保ガイドライン	経済産業省	次世代ロボット安全性確保ガイドライン（案）(esh.co.jp)	設計、製造、輸入、設置、管理、修理、販売	
3		自律移動型駅サービスロボットの安全性確保に関するガイドライン	JRMA 一般社団法人 日本鉄道車両機械技術協会	自律移動型駅サービスロボットの安全性確保に関するガイドライン (rma.or.jp)	開発、製造、設置、管理、使用	
4		食品工場における協働ロボット運用時の安全性確保ガイドライン	農林水産省	seisansei-53.pdf (maff.go.jp)	運用	
5	自動運転車	自動運転車の安全技術ガイドライン	国土交通省	001253665.pdf (mlit.go.jp)	開発（安全要件定義）レベル3/レベル4	
6		農業機械の自動走行に関する安全性確保ガイドライン	農林水産省	220328-1.pdf (maff.go.jp)	設計、製造、輸入、販売、設置、管理、使用、修理	
7	無人航空機	無人航空機の安全な飛行のためのガイドライン	国土交通省	31533.pdf (city.ishikari.hokkaido.jp)	運用（飛行）	
8	機能安全	機能安全活用実践マニュアル ロボットシステム編	厚生労働省	0000197860.pdf (mhlw.go.jp)	市販の産業用ロボットに対する機能安全の導入	

1）リスクアセスメント

安全設計における最初のステップは、フィジカルシステムが関わる全対象範囲を定義して、その対象範囲に対してリスクアセスメント（潜在する危険を明確化（ハザードの固定）、リスク見積り、リスク評価）を行う。その後、各構成システム（エッジ機器やセンサー等）自体についてリスクアセスメントを行う。このリスクアセスメントの手順は、図 3.1.8 や図 3.1.9 に示す安全規格アンブレラ構成のグループ安全規格（B 規格）に、各分野としてそれぞれ説明されているが、要点は基本安全規格（A 規格）の ISO/IEC (JIS Z8051) Guide 51 に説明されている。図 3.1.10 にリスクアセスメントおよびリスク低減の反復プロセスと参照規格を示す。

ISO/IEC (JIS Z8051) Guide 51 リスクアセスメントおよびリスク低減の反復プロセス



リスクの見積およびリスク低減のための参照規格

項目	参照規格
安全側面への導入指針	ISO/IEC Guide 51 (JIS Z8051)
リスクアセスメントガイド	IEC Guide 116（低電圧規格) ISO 12100 (JIS B9700、機械) など
ハザード固定 (ハザード源の固定/特定方法)	規格やガイドはない
リスク見積手法	MIL-STD-882E R-Map 厚生労働省　危険性または有害性等の調査等に関する指針 など
リスク低減手法	IEC 61508 (電気/電子、基本機能安全規格) ISO 13849 (機械、個別機能安全) ISO 26262 (自動車、個別機能安全) IEC 61511 (産業/計装、個別機能安全) など

左図の出典：JIS Z8051 Guide 51(2014)　図2-リスクアセスメントおよびリスク低減の反復プロセス

図 3.1.10　リスクアセスメントおよびリスク低減の反復プロセスと参照規格

ISO/IEC (JIS Z8051) Guide 51 によれば、リスク分析の範囲は、ハザードの固定およびリスクの見積りと定義しており、リスクアセスメントの範囲は、リスク分析およびリスクの評価と定義している。リスクアセスメントを終えた結果、リスクが許容範囲であるか否かを判定することが重要となる。これを誤ると以降の安全設計の意味がなくなってしまうことに注意。

リスクが許容範囲でなければ、リスク低減を実施して、低減後のリスク見積りと評価を行い、残留リスクが許容範囲か否かの判定を行う。これも同様に重要であり、誤ると安全設計に抜けが発生する。残留リスクが許容範囲になるまで反復してリスク低減を行う。リスク低減の手法は、各分野別の安全規格（B 規格）に従うことを推奨する。

ALARP の適用

リスクが許容範囲であるか否かの判断は、リスク低減手法にかける代償とのバランスが重要となる。あまりにも高額になる低減手法を採用しても助けられる人命の数が少ない場合は、その低減策は実施しなくてもよい。これを許容できるリスクとして取り扱う考え方が ALARP である。つまり、合理的に実現可能な範囲でリスクを最小限とする考え方が（As Low As Reasonably Practicable = ALARP)である。図 3.1.11 に示す。

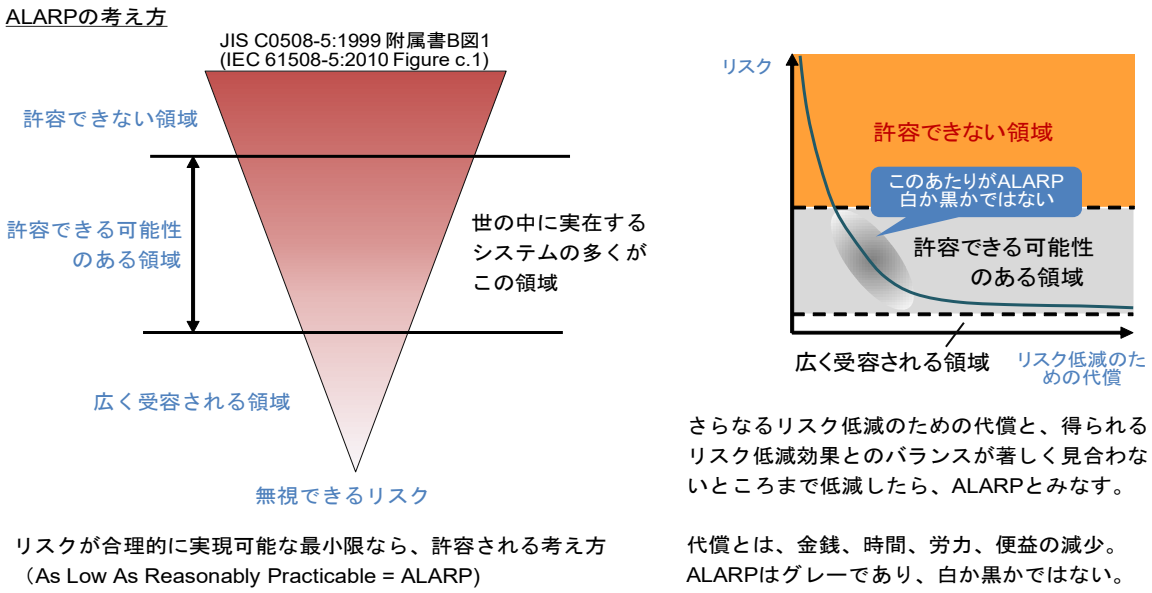


図 3.1.11　ALARP の考え方

世の中に実在するシステムの多くが、許容できる可能性のある領域に位置しており、さらなるリスク低減のための代償と、得られるリスク低減効果のバランスが著しく見合わなくなったところで、ALARP とみなして、低減手法での対策をやめる。代償とは、金銭、時間、労力、便益の減少である。ALARP はグレーであり、白か黒かではない。

２）パフォーマンスレベル（PL）や安全度水準（SIL や ASIL）の設定

フィジカルシステムの対象となる範囲のリスクアセスメントを行った結果に従い、安全要求事項を決定する。安全要求事項の中でも重要なことは、その目的や想定される危険の度合い、規模、使用頻度等から、これに必要なパフォーマンスレベル（PL・ISO 13849-1）、安全度水準（SIL・IEC 61508 や ASIL・ISO26262）等を制御の性質や分野別で設定し、必要な作動信頼性を決めることである。

このパフォーマンスレベル（PL）や安全度水準（SIL や ASIL）を設定し、規格で定義されている内容（具体的には、危険側故障確率 [故障した際に人に危害を与えてしまう確率・ISO 13849-1 では PFHd、IEC 61508 では PFH] 等）を満足するように、リスク低減の設計を行う。図 3.1.12 に ISO 13849-1 で規定されているリスクによる安全機能の対するパフォーマンスレベル(PL)の設定方法（一例）を説明する。

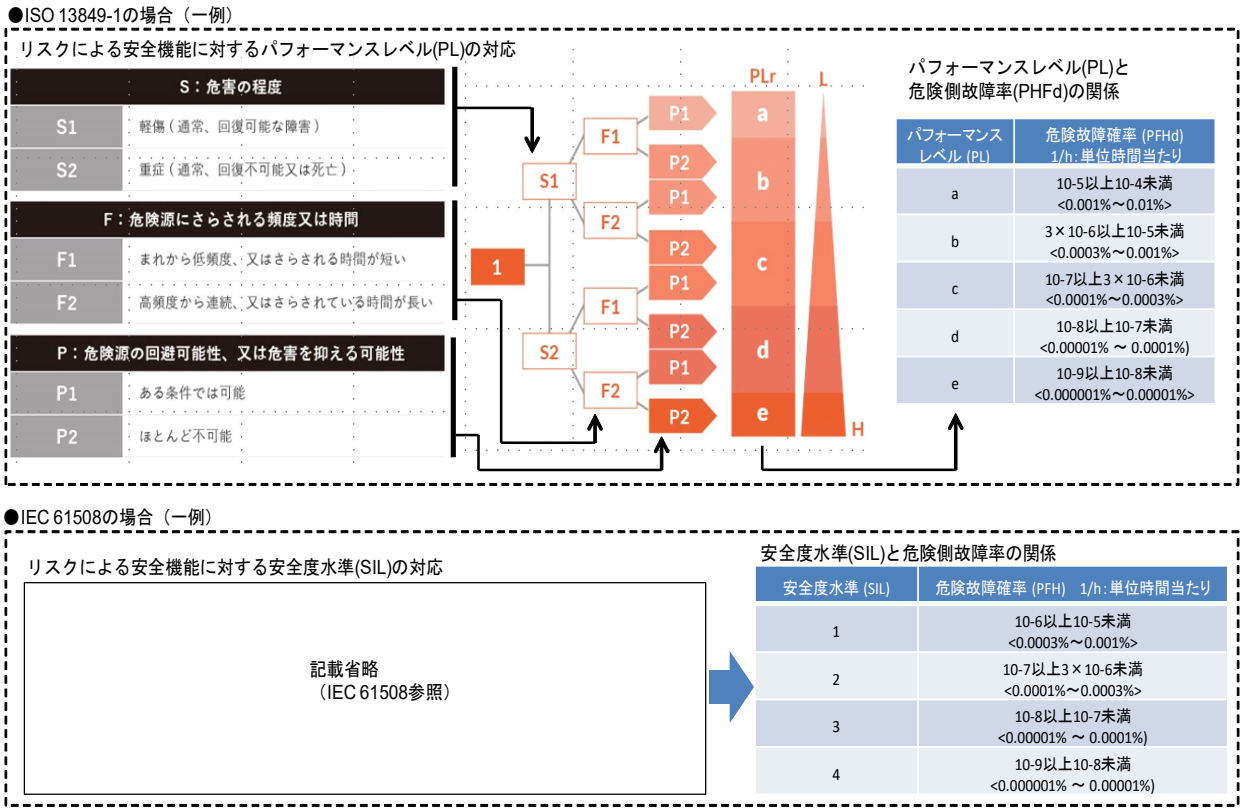


図 3.1.12　ISO 13849-1 におけるパフォーマンスレベルの設定方法

ISO 13849-1 では、リスクを S（危害の程度）、F（危険源にさらされる頻度）、P（危険源の回避可能性）の３つの定量的な内容に分けて、それに対応する安全機能のパフォーマンスレベル（PL）を設定する。安全機能は、パフォーマンスレベル（PL）に応じた危険側故障率(PFHd)を満足する必要があり、リスク低減のための安全設計が必要となる。

IEC61508 でも同様である。パフォーマンスレベル（PL）に対応する安全度水準（SIL）を設定する。安全度水準（SIL）に応じた危険側故障率(PFH)を満足する必要があり、リスク低減のための安全設計が必要となる。

３）システマティック故障とランダムハードウェア故障の考慮

リスク低減の手法は大きく 2 つの故障について対処することで成立する。１つはシステマティック故障を抑える安全設計、もう１つはランダムハードウェア故障を検出して安全状態に遷移させる安全設計である。ソフトウェアには故障という概念はない。バグという概念はあるが、バグは開発プロセスを厳格に実施することで防ぐことができるという解釈から、システマティック故障に分類される。図 3.1.13 に２つの故障の考え方を説明する。

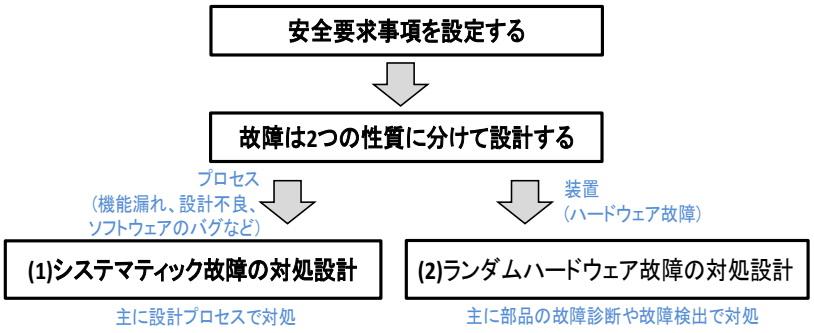


図 3.1.13　システマティック故障とランダムハードウェア故障の対処設計

安全要求事項（Safety Requirements Specification＝SRS と呼ぶ場合が多い）を設定し、それを実現するために 2 つの性質の故障について対処する設計を計画する。

(1) システマティック故障の対処設計

1 つ目の性質は、機能漏れ、設計不良、ソフトウェアのバグ等開発途中で入り込む不具合であり、これをシステマティック故障と呼ぶ。システマティック故障の具体的な対処設計は、開発プロセスを厳格に運用することである。具体的には V モデル設計を適用すること、および V&V（Verification & Validation）を実施することである。図 3.1.14 の左側に安全設計における V モデル設計と V&V を示す。本ディスカッションペーパーで適用する V モデル設計は、安全のための V モデル設計として、IEC 61508 機能安全規格から引用している。そのため、一般的なシステム（システムエンジニアリング）に適用する V モデル設計とは表現が異なっていることに注意。

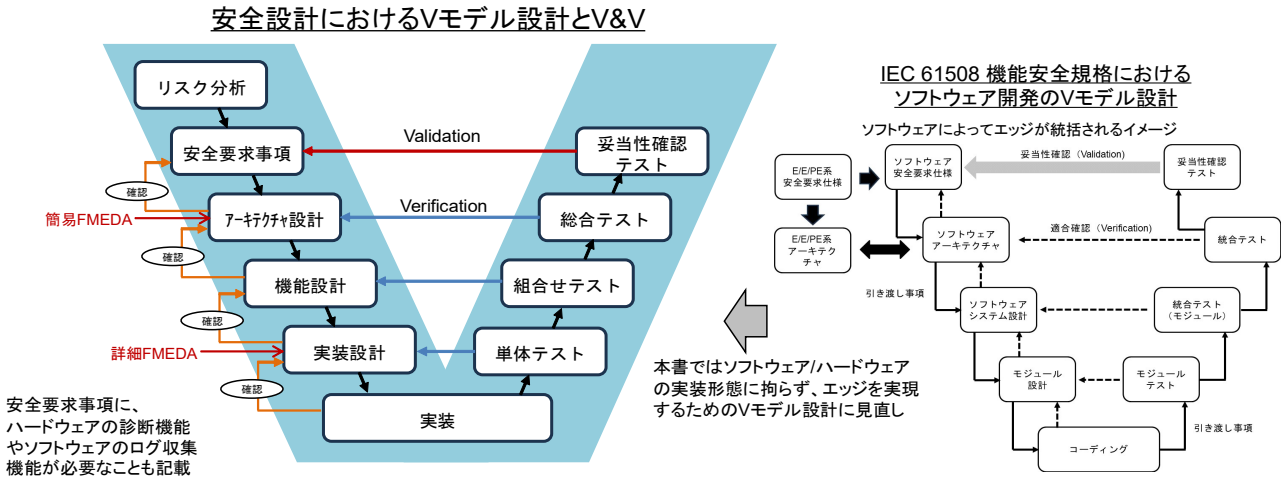


図 3.1.14　安全設計における V モデル設計と V&V

V モデル設計は、V の字の左辺で設計し、右辺で検証と妥当性を確認する考え方である。左辺の設計は上（上流）から下（下流）へ実施するが、下流の設計が 1 つ上流の設計に対して仕様の抜けや発生がないかを確認する手順が入る。また左辺では、安全機能（制御機能や異常検出機能）に加えて、直接的な安全機能で

はないが安全動作に重要な機能（例えば異常検出機能の診断機能やソフトウェアのログ収集機能）の設計も考慮するべきである（安全要求事項に含まれるべき）。

右辺の検証は下から上へ実施する。この時右辺のテスト結果が該当する左辺の設計通りになっていることを検証（Verification）する。右辺の最上位では左辺の安全要求事項の妥当性を確認（Validation）する。

図 3.1.14 の左側に示す安全設計における V モデル設計は、右側に示す IEC 61508 機能安全規格におけるソフトウェア開発の V モデル設計をモチーフにしており、ソフトウェア/ハードウェアの実装形態に拘らず、フィジカルシステムの各構成システムを実現するための V モデルに見直ししたものである。IEC 61508 機能安全規格の V モデル設計は、各構成システムの中核はソフトウェアで統括されているという前提からソフトウェア開発の V モデル設計となっている。安全を実現する各構成システムは、ソフトウェアを使わずハードウェアだけでも構築は可能であるため、本ディスカッションペーパーではソフトウェア/ハードウェアの実装形態に拘らない V モデル設計としている。

a.　V モデル左辺の要素説明

① リスク分析：[IEC 61508 機能安全規格においては規定なし]

フィジカルシステムの各構成システムが人に対して危害を与えるリスクを分析する。またリスクを回避する手段、リスクを許容範囲内に低減する手段、残留リスクを明確化する。

② 安全要求事項：[IEC 61508 機能安全規格においてはソフトウェア安全要求事項]

適用法規、パフォーマンスレベル（PL）や安全度水準（SIL や ASIL）、許容範囲、予見される誤使用、危険源や危険事象の同定、リスクの低減方法、残留リスク、使われ方の前提、等を明示する。

③ アーキテクチャ設計：[IEC 61508 機能安全規格においてはソフトウェアアーキテクチャ]

フィジカルシステムの各構成システムのアーキテクチャを設計するフェーズであるが、アーキテクチャを決めるには大まかな機能や実装制限についても考慮する必要がある。

④ 機能設計：[IEC 61508 機能安全規格においてはソフトウェアシステム設計]

アーキテクチャ設計で検討した大まかな機能について、モジュール分割やブロック分割、詳細な機能割り当て、処理仕様、入出力規定、等を設計する。

⑤ 実装設計：[IEC 61508 機能安全規格においてはモジュール設計]

アーキテクチャ設計で検討した実装制限を守りながら、機能設計で決定したモジュールやブロックの処理仕様や入出力規定に対して、具体的に実現（実装）できる実ロジックを設計する。

b.　V モデル右辺の要素説明

① 単体テスト：[IEC 61508 機能安全規格においてはモジュールテスト]

実装設計において実現したモジュールやブロックの処理仕様や入出力規定の実ロジックに対して、モジュール単体やブロック単体の機能を確認するテストを実施する。

② 組合せテスト：[IEC 61508 機能安全規格においては総合モジュールテスト]

単体テストで確認済のモジュールやブロックの実ロジックを、複数接続し、機能の組み合わせを確認するテストを実施する。

③ 総合テスト：[IEC 61508 機能安全規格と同じ]

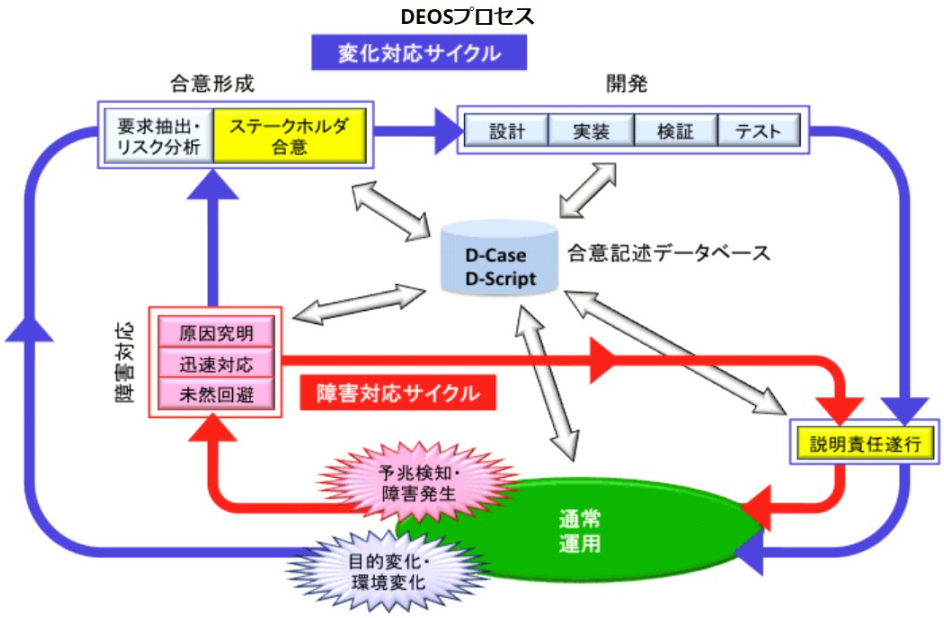
組合せテストで確認済のモジュールやブロックの実ロジックを使ってエッジを構成し、アーキテクチャ設計で規定した動作が実現できているかを確認するテストを実施する。

④　妥当性確認テスト：[IEC 61508 機能安全規格と同じ]

フィジカルシステムの各構成要素として製作された実物に対して、安全要求事項が満足できているか、妥当性を確認するテストを実施する。

c.　DEOS プロセス（IEC 62853）について

システマティック故障の対処設計として V モデルの例を説明したが、これは構成システムの開発（設計・実装・検証など）に対しての手順を示したものであるが、事業者は構成システムのライフサイクルを通して対処すべきであり、開発だけでなく、運用や障害対応（保守）についても考える必要がある。特に CPS におけるフィジカルシステムの場合、システムがネットワークによりつながることで、これまで以上に他のシステムからの影響（干渉）を受けやすい状況になるため、多様なステークホルダーがシステムに関わる必要がでてくる。このような予測困難で動的な変化にさらされる環境下において、多様なステークホルダーが関わる中でディペンダビリティを確保するということをいかに確実におこなっていくか。このような課題に答えるために図 3.1.15 に示す DEOS（IEC 62853・Open Systems Dependability [OSD]）という考え方が生まれた。



出典：プロセス | DEOSの技術 | DEOS　http://deos.or.jp/technology/process-j.html

図 3.1.15　DEOS プロセス

事業者は構成システムに対して、以下の DEOS プロセスを適用することが望ましい。

反復的アプローチ

- 目的や環境の変化に対してシステムを継続的に変更して行くための変化対応サイクル
- 障害に対して迅速に対応するための障害対応サイクル
- 障害対応サイクルから変化対応サイクルへのパス

(2)　ランダムハードウェア故障の対処設計

2つ目の性質は、ハードウェア特有の壊れることによる故障であり、これをランダムハードウェア故障と呼ぶ。装置やそれを構成する部品（いずれも機能として表現）が壊れることは防げないため、壊れたことを確実に検出できるようにし、検出したら安全状態へ遷移させる設計を実施する。ランダムハードウェア故障の具体的な対処設計は、FMEDA（Failure Modes, Effects, and Diagnostic Analysis）を実施して、故障モードを明確化した上で、故障を検出する回路を敷き詰める設計となる。故障検出のカバー率は、パフォーマンスレベル（PL）や安全度水準（SIL や ASIL）等で設定した値から決定される。重要なのは、故障を検出した際に、エッジを規定時間内に安全状態に遷移できることである。この規定時間や安全状態の定義は、安全要求事項に含まれる。図 3.1.16 に故障検出による安全状態遷移のイメージを示す。

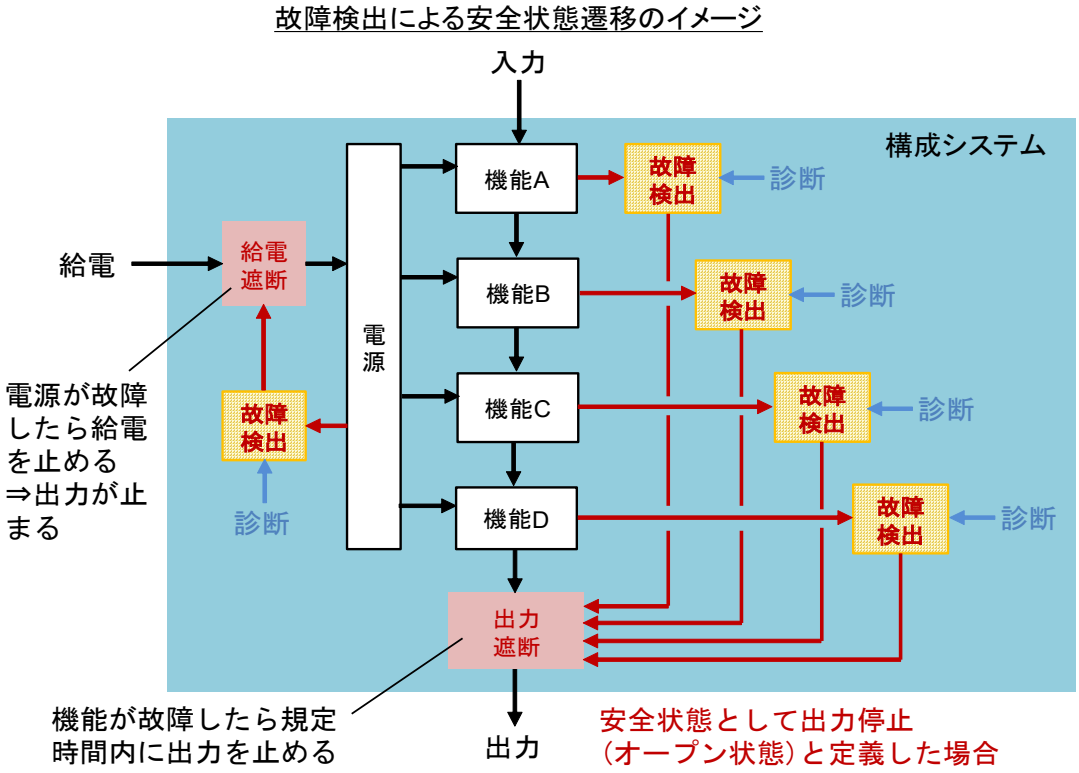


図 3.1.16　故障検出による安全状態遷移のイメージ

ハードウェアで構成される電源や機能等は、故障を前提に安全設計する。故障を検出するには故障検出回路が必要であり、機能ごとに検出回路を配置するのが一般的である。機能が大きすぎると検出率が下がる傾向になるため、パフォーマンスレベル（PL）や安全度水準（SIL や ASIL）で定義される検出率を達成できない場合は、機能をさらに細分化して検出回路増やして配置する必要がある。また故障検出回路が必要な時に作動するように、定期的に診断を実施することも必要である。

検出率を求めるには FMEDA を実施する。詳細な FMEDA は実装が決まらないと実施できないが、それでは設計がクローズしないため、図 3.1.14 に示す V モデル左辺の基本設計（アーキテクチャ設計）で簡易的な FMEDA を実施し、概ね検出率を確保できたアーキテクチャで詳細設計を進める。最終的に詳細設計において詳細な FMEDA を実施することで検出率を満足し、設計をクローズする。

安全状態として出力停止（オープン状態）と定義した場合、例えば電源が故障しても各機能が故障しても、最終的に出力遮断回路で出力が停止するように設計する。電源が故障した場合は、給電を遮断することで間接的に出力が停止するので問題ない。このように故障を検出した際は、規定時間内に安全状態へ遷移さ

せる設計が必要である。注意点すべきは、故障の検出時間と出力の安全状態遷移時間の両方が規定時間に含まれることである。

4） 第三者検証

フィジカルシステムの各構成システムにおける安全要求事項（重要度、想定される危険の程度、関係者の要望等）を達成するために、リスクアセスメント、設計、実装、テストが十分かつ正しく実施されているかについて、第三者による検証や認証を実施する。

具体的には、安全設計における V モデル設計に従った第三者検証が行われる。V モデルに沿って設計されているかの検証と、V モデルの各要素に対して検証する。表 3.1.4 に V モデル設計における第三者検証の観点を示す。

表 3.1.4　V モデル設計における第三者検証の観点

No	Vモデル設計の要素	監査・認証の観点
1	リスクの分析	リスクアセスメントの不十分（網羅性、十分性等）
2	安全要求事項	リスクへの対処の網羅性、十分性
3	基本設計(ｱｰｷﾃｸﾁｬ設計)	安全要求事項への対応の網羅性、妥当性、十分性
4	機能設計	基本設計の網羅性、十分性
5	詳細設計	機能設計の網羅性、十分性
6	実装	詳細設計の実現の網羅性、妥当性、十分性
7	単体テスト	詳細設計内容の検証の網羅性、妥当性、十分性
8	組合せ手素地	機能設計内容の検証の網羅性、妥当性、十分性
9	総合テスト	基本設計内容の検証の検証網羅性、妥当性、十分性
10	妥当性確認	安全要求事項の妥当性

観点としてはほぼ共通であり、網羅性、妥当性、十分性である。可能であれば、アーキテクチャ決定段階において、進め方が正しいかを確認するコンセプト検証を受査することを推奨する。また設計終盤で第三者検証が問題なく終了すれば、期限付きの Qualification が発行され、実証実験等に参画できる体制を目指す。市場投入や販売には、認証を義務づけた体制を目指す。この場合は期限付き Certification が発行される。検証や認証が完了した後においても、維持/更新を目的に定期的な第三者受査を義務づけた体制を目指す。

3.1.9　製品安全の実装

製品安全（プロダクトセーフティ）とは、製品に内在するハザードにより危害をもたらすリスクを、製品内部で低減することである。それに対し機能安全（ファンクショナルセーフティ）とは、制御機能内の保護機能で低減し切れない内在残存リスクを、制御機能外に設置した独立の保護機能で低減する。図 3.1.17 に製品安全と機能安全のちがいを記載する。

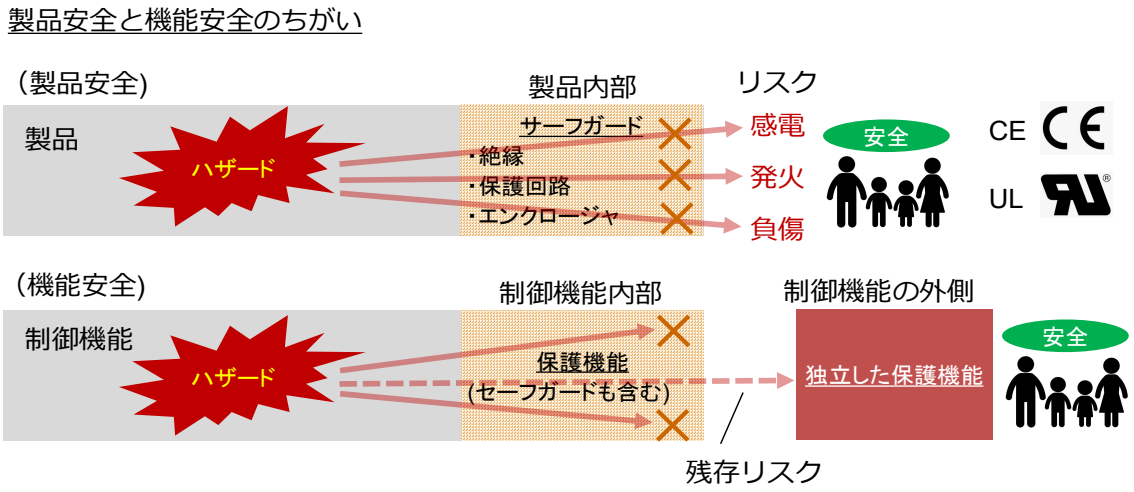


図 3.1.17　製品安全と機能安全のちがい

人命を保護するための安全設計というと、機能安全を思い描く場合が多いが、製品安全に対処することも必須である。製品安全は、セーフガードという機能（絶縁、保護回路、エンクロージャ等）で製品内のハザードによる人命への危害を防ぐ機能であり、製品内部に設置される必要がある。これを設置することで感電、発火、負傷等を防ぐことができる。多くの製品は、CE や UL 等で認証を受けている。

3.1.10　安全設計と信頼性設計の関係

信頼性とは、機器・設備等のアイテムが、与えられた条件の下で、与えられた期間、要求機能を遂行できる能力をいう。これらを満足する設計が信頼性設計。

安全性とは、人への危害の危険性が許容可能な水準に抑えられている状態をいう。これらを満足する設計が安全設計。

信頼性設計と安全設計は、図 3.1.18 に記載する通り密な関係にある。

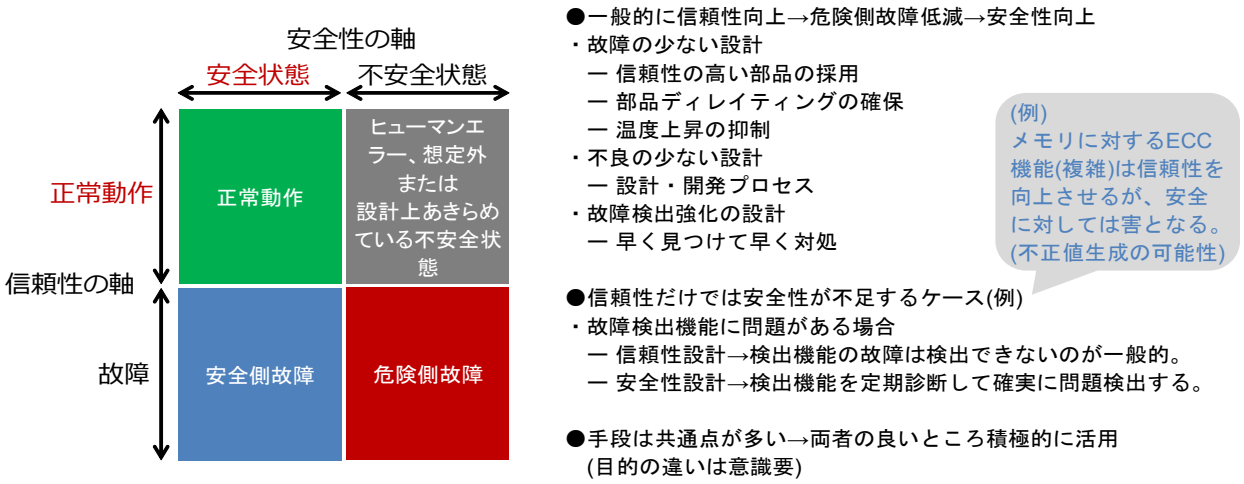


図 3.1.18　安全設計と信頼性設計の関係

一般的に信頼性を向上させると安全性における危険側故障が低減し、その結果安全性が向上するので、信頼性と安全性は非常に密な関係にあるといえる。信頼性においては、故障の少ない設計、不良の少ない設計、故障検出強化の設計の 3 本柱が重視され、それを信頼性設計としている。

信頼性設計だけでは安全性が不足することが考えられる。例えば故障検出機能に問題がある場合、信頼性設計においては検出機能の故障までは検出しないのが一般的なため、安全設計では故障検出機能の定期診断まで行う。またソフトエラーの対処に信頼性の 1 つである可用性を向上するため、ECC（Error Correcting Code）を使用するケースが多いが、この機能は複雑であるため、安全性に対しては害となる。不正値を生成する可能性があるため。ECC を用いる場合は、CRC（Cycle Redundancy Check）コード等と併用することが安全規格では義務づけられている。

3.1.11 安全設計とセキュリティ設計の関係

サイバーセキュリティの対応であるセキュリティ設計は、フィジカルシステムの構成システム外部の脅威（攻撃、侵入、異常入力、異常操作など）に対する防御機能（セキュリティ機能）を実現することが目的である（外部からシステムに危害を与えない）。それに対して安全設計は、構成システム内部の故障（ランダムハードウェアフォルトやシステマティックフォルトなど）によるシステム外部へ危害に対しての防御機能（安全機能）を実現することが主な目的である（危害をシステムの外部に及ぼさない）が、さらにセキュリティ設計における残存リスクの脅威に対する防御にも対応する。共通点はどちらも制御対象の意図しない動作を引き起こさないように防御する設計である。図 3.1.19 にセキュリティ設計と安全設計の関係を記載する。

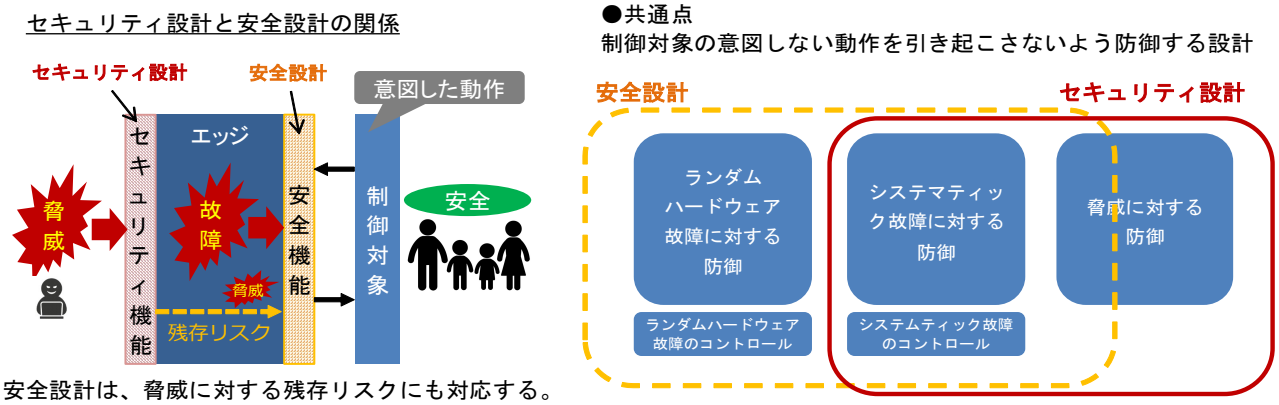


図 3.1.19　安全設計とセキュリティ設計の関係

想定した脅威であるならセキュリティ機能で防御しきれるが、残存リスクである想定できない脅威であった場合、セキュリティ機能で防御できない場合がある。この場合、構成システム内部に対して脅威が侵入することになるが、この結果は構成システムの機能異常として現れ、安全機能によって検出され、最終的には安全状態へ遷移することで制御対象である人命を保護する。

セキュリティ設計は、脅威に対する防御機能を実現することであるが、その設計プロセスは厳格であることが IEC 62443-4-1/2 などの制御システムセキュリティ規格で規定されており、システマティック故障に対する防御機能の実現も併せもつ。それに対して安全設計は、ランダムハードウェア故障に対する防御機能と

システマティック故障に対する防御機能を実現するが、セキュリティ設計の残存リスクである脅威に対しても防御機能が実現される。

3.1.12 安全設計の進め方

フィジカルシステムに対する安全設計には、安全規格に規定される項目（代表的な項目としては 3.1.5 項～3.1.11 項で記載）以外にも必要と考えられる項目が存在する。例えば障害時の復旧や保守に関する内容、障害や事故の解析のためのログやトレースの採取の実施など。

そのため、3.1.4 項 2）に示す代表的なリスクに対して漏れがないように進めるために、図 3.1.20 に示す通り、安全設計を 3 つの階層に分けて考えると進めやすいかもしれない。

安全設計を3つの階層に分けて考え進める。
階層1：どのような設計をすれば安全なのかを定義する
階層2：定義した安全設計において考慮すべきことを決める
階層3：定義した安全設計の具体策・仕掛けを決める

図 3.1.20　安全設計の 3 つの階層

1）階層 1：どのような設計をすれば安全なのかを定義する

フィジカルシステムの各構成システムに対して、一般的に以下の内容を実現することが安全と考えられるが、あくまでも一例であるので、各構成システムに応じて定義する。

① 誤動作/誤不動作が起きにくい設計
② 誤動作/誤不動作を起こす可能性のあるリスクを回避する設計
③ 誤動作/誤不動作が発生しても人に危害を与えない設計
④ 誤動作/誤不動作を起こした要因を特定できる設計
⑤ 誤動作/誤不動作後、短時間に復旧できる設計
⑥ 事故(人への危害)に対処できる設計
⑦ ヒヤリハットに対処できる設計
⑧ 上記 7 つに対して満足した設計になっているかの検証

2）階層 2：定義した安全設計において考慮すべきことを決める

上記①から⑧の安全設計を実現するために、どのような考慮が必要か、表 3.1.5 に説明する。

表 3.1.5　安全設計において考慮すべきこと

階層1 どのような設計をすれば安全なのかを定義する（例）	階層2 定義した安全設計において考慮すべきことを決める（例）
①誤動作/誤不動作がそもそも起きにくい設計	①-1 故障が少ない設計
	①-2 コンパクトな造り
②誤動作/誤不動作を起こす可能性のある リスクを回避する設計	②-1 リスクアセスメントによるリスク低減手法の立案
	②-2 システマティック故障の考慮（機能要件漏れ、設計不良、バグ）
	②-3 ランダムハードウェア故障の考慮（部品故障、装置故障）
	②-4 ハードウェアへの外部からの影響 （停電、断線、ノイズ、ソフトエラー、誤操作、不正アクセス）
	②-5 ソフトウェアへの非安全処理からの影響と外部からの影響
③誤動作/誤不動作が発生しても人や設備に 危害を与えない設計	③-1 安全状態の定義
	③-2 故障(残留したバグ含む)を規定時間内に検出
	③-3 故障検出により安全状態へ遷移
④誤動作/誤不動作を起こした要因を特定できる設計	④-1 解析のためのログやトレース情報を採取
⑤誤動作/誤不動作後、短時間に復旧できる設計	⑤-1 規定時間内に復旧
	⑤-2 バックアップがある場合は規定時間内に運用切替
⑥事故(人や設備への危害)に対処できる設計	⑥-1 事故の前後の情報を採取
⑦ヒヤリハットに対処できる設計	⑦-1 事故ではないが平常時と違う挙動の前後の情報を採取
⑧上記７つを満足した設計になっているかの検証	⑧-1 第三者検証

3）階層 3：定義した安全設計の具体策・仕掛けを決める

階層 2 で決めた考慮すべき内容①-1 から⑧-1 について、具体策・仕掛けの例を表 3.1.6 に記載する。

表 3.1.6　安全設計の具体策・仕掛けの例

階層2 定義した安全設計において考慮すべきことを決める（例）	階層3 安全設計の具体策・仕掛けの例
①-1 故障が少ない設計（信頼性設計）(3.1.10項)	・故障率の小さい装置/部品の採用 ・十分なディレーティングの確保 ・温度上昇の抑制
①-2 コンパクトな実装	・部品点数が少ない構成 ・小規模なタスクまたは単純な機能の組み合わせ ・検証のしやすい機能構成
②-1 リスクアセスメントによるリスク低減手法の立案	・ハザード源の固定/特定 ・リスクの見積りと評価 ・リスク低減手法に安全規格を適用/立案
②-2 システマティック故障の考慮 （機能要件漏、設計不良、バグ）	・Vモデル設計、V&Vの実施 ・要件に対する十分な妥当性確認（Validation） ・要件トレーサビリティの実施(Vモデル左辺上下の確認) ・十分な検証（Verification）（Vモデル左辺と右辺の関係）
②-3 ランダムハードウェア故障の考慮 （部品故障、装置故障）	・製品安全の実装(3.1.9項) ・故障検出機能/回路の実装 ・故障検出機能/回路の定期的な診断 ・安全機能と非安全機能の物理的な分離 ・非安全機能から安全機能へのアクセス禁止 ・共通要因故障への対応
②-4 ハードウェアへの外部からの影響 （停電、断線、ノイズ、ソフトエラー、誤操作、不正アクセス）	・停電：多重化電源、UPS、バッテリー保護など ・断線：ケーブルの保護、安全レイヤの実装(3.2.2項) ・ノイズ：ケーブルのシールドなど、安全レイヤの実装(3.2.2項) ・ソフトエラー：誤り検出の実装、[エラー訂正機能の実装] ・誤操作：フールプルーフ設計 ・不正アクセス：フィジカルセキュリティ対応
②-5 ソフトウェアへの非安全処理からの影響と外部からの影響	・安全機能と非安全機能のリソース分離（メモリ分離など） ・非安全機能から安全機能へのアクセス禁止 ・安全機能のハードウェアによる異常検出(WDT、処理順番) ・セキュリティ対応(3.1.11項)
③-1 安全状態の定義	・人や設備を保護する状態（エッジの停止が多い）を定義
③-2 故障(残留したバグ含む)を規定時間内に検出	・PLやSILに応じた故障見逃し許容率(FIT)の設定 ・FMEDAによる故障見逃し率の算出 ・エッジ内通信は安全レイヤ(3.2.2項)による故障率の除外適用 ・故障見逃し許容率以上について故障検出機能/回路の実装 ・規定時間を遵守した検出機能の実装
③-3 故障検出により規定時間内に安全状態へ遷移	・故障検出時にエッジ出力/挙動として安全状態値とする ・規定時間を遵守した遷移機能の実装
④-1 解析のためのログやトレース情報を採取	・誤動作/誤不動作要因解析ができるログ/トレースの採取 ・誤動作/誤不動作要因が短時間で解析できる仕掛け ・要因を元に対策ができる仕掛け
⑤-1 規定時間内に復旧	・アプリケーションに応じた復旧規定時間の設定 ・復旧手順の明確化と保守部品の整備 ・規定時間が短い場合は、可用性（多重化構成）の考慮 ・遠隔でのプログラム修正が行える機能の考慮
⑤-2 バックアップがある場合は規定時間内に運用切替	・最低限の機能を維持するバックアップシステムの考慮 ・最低限の機能明確化
⑥-1 事故の前後の情報を採取	・タイムスタンプ付きの画像、前後30秒程度採取 ・制御指示情報、入力値/出力値情報のログ ・絶対時刻への同期
⑦-1 事故ではないが平常時と違う挙動の前後の情報を採取	・ヒアリハット条件明確化（平常時と違う挙動の検出は？） ・明確化した条件で⑥-1と同じ対処（明確化ができるか疑問）
⑧-1 第三者検証	・設計上流段階でのコンセプト/アーキテクチャ検証 ・設計終盤での検証(Qualification)・・・実証実験可 ・設計完了時の認証(Certification)・・・市場投入・販売可

3.2　安全設計されていないサイバーシステムを透過する安全設計

CPS を直接人命に関わる使い方で運用するために、サイバーシステムを安全設計することは理想である。しかし 2.2.2 項で説明した通り、現時点では困難であるため、当面は別の代替案を考慮する必要がある。その一つの案として、安全設計されていないサイバーシステムを土管のように単なる伝送パイプ（IEC 61508 機能安全規格ではブラックチャネルと呼ぶ）として扱い、データをサイバーシステムに流すだけで加工は一切しない使い方である。安全設計されていないサイバーシステムの両端に位置する安全設計されたフィジカルシステムが、送受信するデータの安全性を担保する実装方法である。これを本ディスカッションペーパーではサイバーシステムを透過するという表現で以下説明する。

3.2.1　具体的な実現方法

交差点における自動運転車の通行支援システムを CPS で構成した場合を例にして、サイバーシステムを透過する実現方法を説明する。図 3.2.1 の左側はシステムのイメージ図である。センサー（信号機・カメラ）で捉えた歩行者等の位置情報から交差点をこれから通行するエッジ機器（自動運転車）に対して減速するか否かの指示を路側にある装置（サイバーシステム）を通して出力し、渋滞を緩和させることを目的とするシステムである。

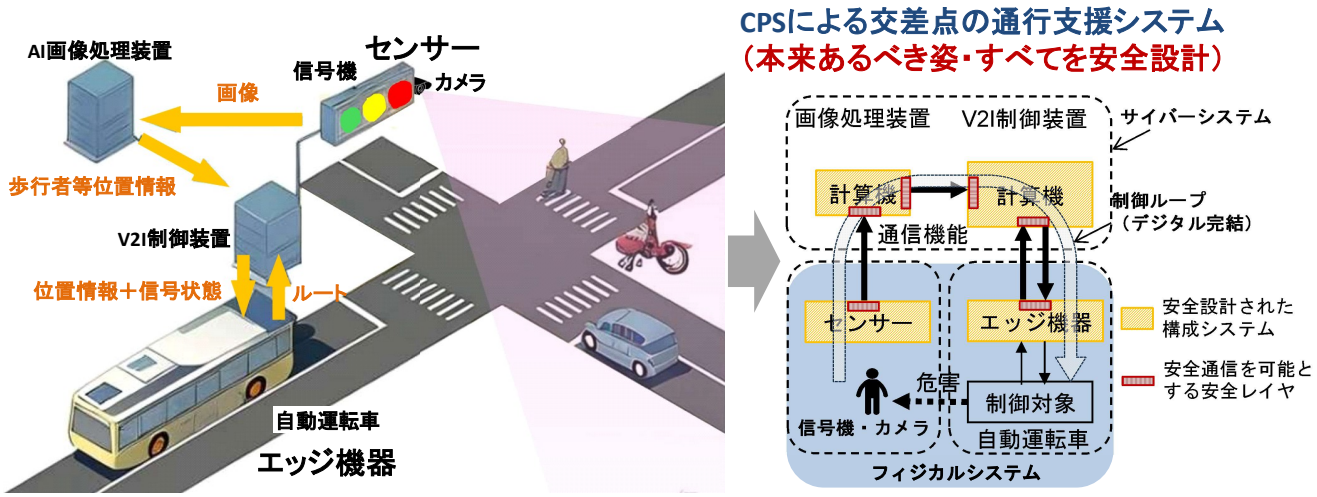


図 3.2.1　CPS による交差点の通行支援システムの例

図 3.2.1 の右側はこの CPS のブロック図である。本来であればサイバーシステムである計算機等に対しても安全設計されていることが望ましいが、これが実現困難であるため、図 3.2.2 に示すように安全設計されていない安全設計されていないなサイバーシステムを透過させることで、CPS 全体として安全を担保する手法である。

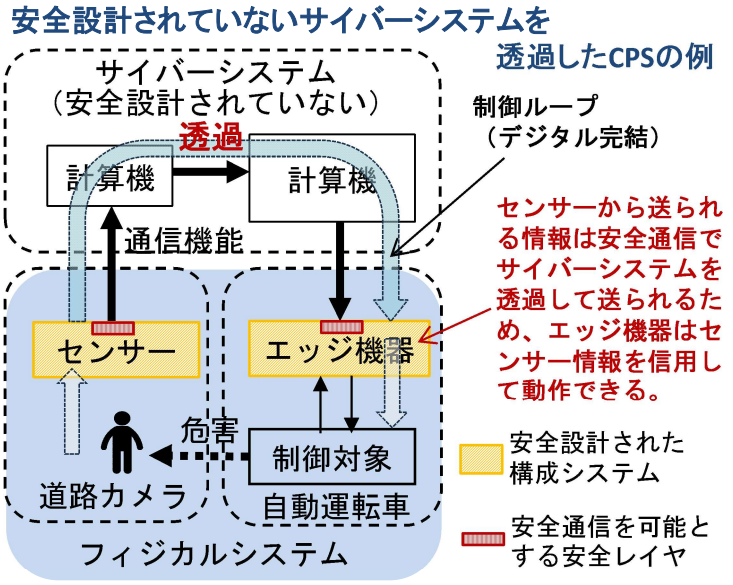


図 3.2.2　安全設計されていないサイバーシステムを透過する実現方法

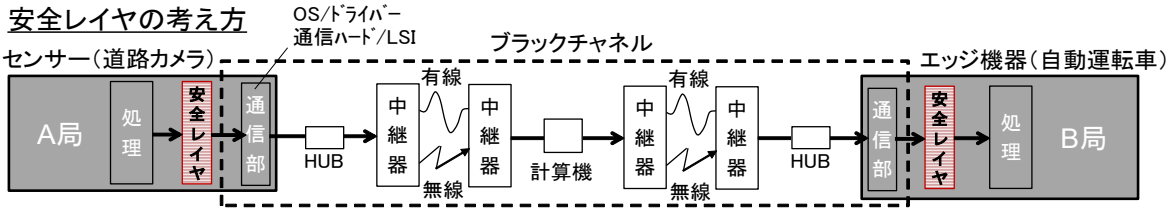
CPS として安全を担保するには、安全設計されていないサイバーシステムの計算機等は、センサーから上がってくる情報に一切加工処理を施さないで透過し、エッジ機器へそのまま情報を伝達する必要がある。つまり図 3.2.1 の右側のサイバーシステムで実施されていた画像処理はできないことになる。従って画像処理の機能を安全設計されたセンサー（信号機・カメラ）またはエッジ機器（自動運転車）に移設する必要がある。これが 1 つ目の制約となるが、クラウドや計算機等を安全設計するより遥かに現実性があると考えられる。具体的な移設方法については本ディスカッションペーパーでは説明を省略する。

サイバーシステムを透過するための 2 つ目の制約は、サイバーシステムにおいて一切の加工処理がないことを証明する必要があり、それを実施する安全通信が必須となることである。安全通信は一般的には安全レイヤ（安全通信を実現するプロトコルで IEC 61508 機能安全規格で定められている）を実装することで実現する場合が多い。3.2.2 項で説明する。

3.2.2　安全レイヤ（安全通信）

安全レイヤとは安全通信を実現する手法の 1 つで、通信において発生する可能性のある 8 つのエラーに対処できる機能（レイヤ）を有することで、通信路のうち安全レイヤで囲まれた内側を土管のような単なる伝送パイプ（ブラックチャネルと呼び、通信路として安全設計を省略可能な範囲）として扱うことができる手法である。図 3.2.3 に安全レイヤの考え方を記載する。

【注意】機能安全規格（IEC 61508）における安全通信の原則は、送信者は受信者からの応答を確認して通信が成立する。応答のない通信手段は安全通信と認められない。推奨する通信手段は、Peer to Peer または P2P とも表現するが、1 対 1 通信である。ブロードキャスト方式やマルチキャスト方式は、応答のない場合、安全通信に使用することはできない。複数の受信者に同じ内容を伝送する場合は、受信者ごとに P2P で伝送するか、ブロードキャスト方式やマルチキャスト方式で全受信者に一斉伝送し、後から応答だけを各受信者から個別に受け取る方法が考えられる。



8つのエラーに対処するレイヤ

No	エラー種別	安全レイヤにおける対応策の例
1	劣化	応答メッセージ、エラー検出符号、二連送、など
2	意図しない繰り返し	通し番号、タイムスタンプ、二連送、など
3	誤った順序	通し番号、タイムスタンプ、二連送、など
4	消失	応答メッセージ、通し番号、二連送、など
5	受容できない遅延	タイムアウト、タイムスタンプ、など
6	挿入	通し番号、タイムスタンプ、アドレス明示、応答メッセージ、二連送、など
7	偽装	アドレス明示、応答メッセージ、など
8	アドレス誤り	アドレス明示、など

図 3.2.3　安全レイヤの考え方

A 局（例えばセンサー）と B 局（例えばエッジ機器）の通信を安全通信に対応させる場合、通信路途中に介在する機能や媒体（通信部、サイバーシステムの計算機、HUB、中継器、有線/無線など）をすべて安全設計する必要が発生し、現実的ではない。そこで一般的な通信で発生する可能性のある 8 つのエラーを検出できる機能（安全レイヤ）を A 局と B 局にそれぞれ対向して実装することで、通信路途中に介在する機能や媒体の安全設計を省略する。エラーの検出能力は、IEC 61508 機能安全規格等で定められており、適用するパフォーマンスレベル（PL）や安全度水準（SIL や ASIL）によって異なる。8 つのエラーは、劣化、意図しない繰り返し、誤った順序、消失、受容できない遅延、挿入、偽装、アドレス誤りである。これらが発生したことを各エラーの対処策で検出し、一般的には可用性対応（リトライ、回線切り替えなど）を行う。可用性対処ができない場合は、A 局および B 局を定義した安全状態へ遷移させる運用となる。通信回線が 4G や 5G 等の公衆回線の場合、専用回線と比べて回線エラーとなる可能性が高いため、A 局や B 局が安全状態に遷移する頻度が高くなると考えられる。このようなケースでは、公衆回線の多重化およびダイバーシティ化（例えば D 社回線と A 社回線の二重化回線）による可用性の確保も重要である。

3.2.3　データに対する信頼度

フィジカルシステムの構成システムであるセンサー（信号機・カメラ）を安全設計したとて、送出するデータ（映像、画像処理を搭載していればその結果による指示、等）が 100%正しいとは限らない。本来なら 100%を目指すべきであるが、アナログ系が介在する場合のデジタル化に伴う量子化誤差、画像処理などや AI が関与する場合のアルゴリズム起因、動画データのフレーム抜け、近未来を予測したデータ等を考慮すると、そのデータの信頼度は 100%にならない場合が多い（AI 処理に対する安全設計については、3.4.2 項参照）。信頼度が 100%でないデータを送られたエッジ機器等の対処については先行して検討されている取り組みがある。RoAD to the L4（注 7）のテーマ 4 である CooL4（注 8）プロジェクトでは、安全設計したセンサーからのデータに信頼度を付加してエッジ機器へ伝送する手法を検討している。データとその信頼度を受け取ったエッジ機器は、データに対して信頼度に応じた処理を実施することで、安全性を担保している。

データに対する信頼度は、送出する側の構成システム（この例ではセンサー）を安全設計して初めて有効となる。そうでないと信頼度の数値そのものを信用できなくなる。図 3.2.4 に近未来を予測した指示を出す例を示す。

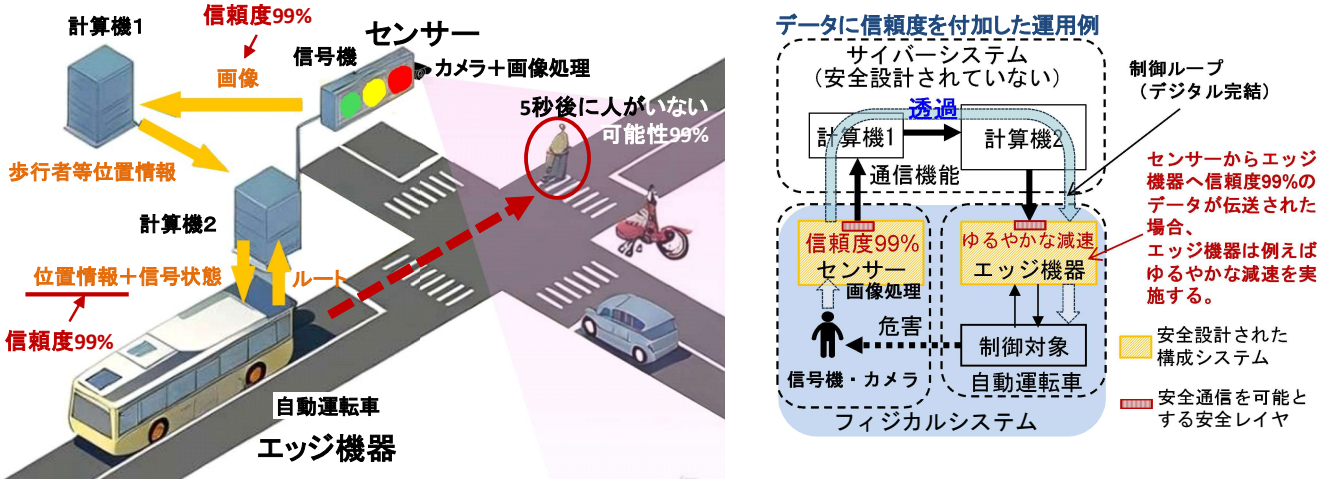


図 3.2.4　データに信頼度を付加した運用例

画像処理機能を装備したセンサー（信号機とカメラ）は、エッジ機器（自動運転車）が 5 秒後に通過する横断歩道に人がいない可能性を、画像処理のアルゴリズム起因精度を差し引いた信頼度 99%でエッジ機器に伝送した（センサーは安全設計されているため、それ以外での信頼度低下はない前提）。その指示を受けたエッジ機器は、信頼度 99%を考慮し、ゆるやかな減速を始めた。また、もし 90%程度の信頼度であった場合（あくまでも例として）は、エッジ機器はいつでも停止できる速度まで比較的急な減速を開始する。このような運用になると考えられる。

安全の担保だけであれば、制御のためのパラメータとして信頼度を使用することになるが、事故が発生した際は、信頼度を基準にその責任分担の割合を決めるという考え方もできる。

3.3　安全設計されていないサイバーシステムによる協調運用に対処した安全設計

最初に断っておくが、本 3.3 項で説明する安全設計は推奨しない。

サイバーシステムを安全設計することなく、CPS の安全を担保する 2 つ目の案として、安全設計されていないサイバーシステムに対して制約を設けてフィジカルシステムを協調運用させる方法である。これはやむなく運用する場合の設計であることを強調しておく。社会が目指すシステムは、インフラ基盤との協調により達成できるエコな環境の実現であり、例えば自動運転においては渋滞がない効率化された交通システムであり、これを実現するにはフィジカルシステムの安全担保だけでは達成できず、時にはインフラ基盤の指示を信用してフィジカルシステムの安全性能を緩める必要がある。しかしそれはデンフラの基盤安全設計が達成できた後の話である。

3.3.1　協調するための課題

安全設計されていないサイバーシステムからの指示は信頼できない。従って協調運用においては、サイバーシステムを使うことでフィジカルシステムの安全性をより高める運用に限定し、フィジカルシステムの安全性能を緩める運用は実施すべきでない。つまり、安全設計されていないサイバーシステムからの指示によって、フィジカルシステムの安全機能が解除や緩和されてしまうような運用は避けるべきである。

1）危険な協調運用の例

（例）ブラインドカーブの向こうは“障害物なし”を信じ、減速せず渋滞緩和させる使い方

ブライドカーブの通過時に、カーブの向こう側の状態がわからない場合、エッジ機器である自動運転車は徐行通行が必要になり通行の効率性が損なわれる（渋滞の発生）。そこで、カーブの向こう側をセンサーである道路カメラで監視し、対向車等の障害物が無いことを自動運転車に通知すれば、徐行が不要にできそうに考えられる。しかし現状は、センサー（道路カメラ）、サイバーシステム（画像処理の計算機、通信機能等）の安全設計ができていない。サイバーシステムからの“障害物なし”という危険側の情報をエッジ機器はそのまま運用に利用することは避けるべきである。図 3.3.1 参照。

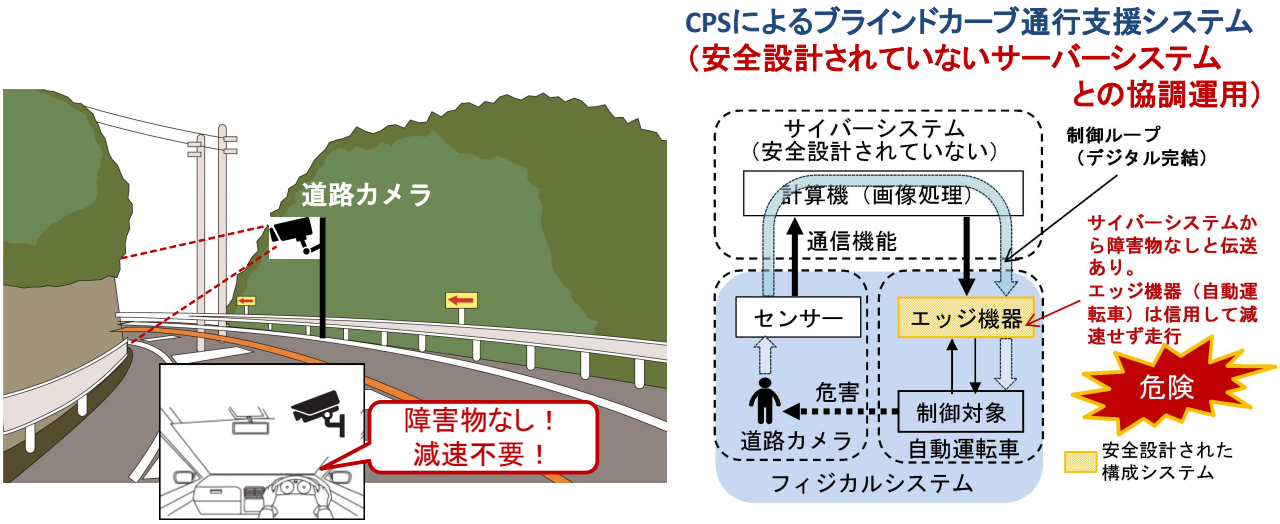


図 3.3.1　ブラインドカーブ通行支援システムの危険な運用例

2） 安全な協調運用の例

（例）ブラインドカーブの向こうは“障害物あり”として、早めの減速で安全を確保する使い方

センサーである道路カメラが“障害物あり”を通信で伝えてきた場合に、通常エッジ機器である自動運転車が減速開始するポイントより手前での事前減速が可能となり、事故のリスクを減らすことができ、安全性が向上できる。センサーやサイバーシステムが安全設計されていない場合でも、エッジ機器は安全を向上する指示には従うことができる。しかしこの運用はサイバーシステムからの安全重視に対する指示のみ受け入れる特性をもつため、社会が目指すエコなシステムを実現できるわけではなく、エッジ機器である自動運転車のさらなる性能向上化で道路カメラやサイバーシステムは不要となる可能性があり、普及は考えられない。図 3.3.2 参照。

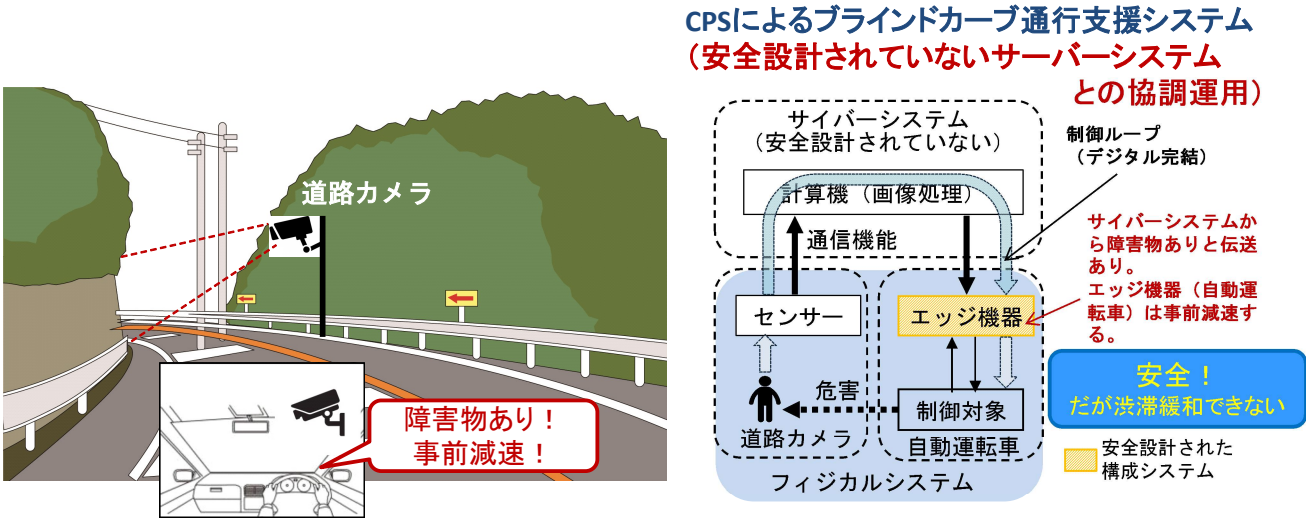
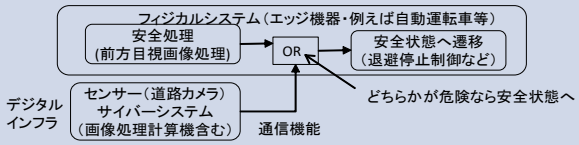
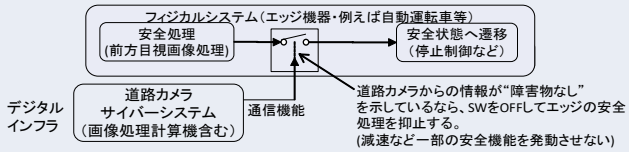


図 3.3.2　ブラインドカーブ通行支援システムの安全な運用例

3） 協調運転における要点

以上の例のように、安全設計されていないサイバーシステムと協調運転する場合の要点は、表 3.3.1 に示す通りである。

表 3.3.1　協調運用における安全設計の要点

No.	協調目的	協調運用の例	協調運用時の安全設計	運用可否
1	フィジカルシステムの安全性向上	図3.3.2参照	センサーである道路カメラとサイバーシステムの協調により、フィジカルシステムのエッジ機器が具備する安全機能をより強化する運用。 	可 （推奨しない） 安全設計として成立する
2	フィジカルシステム動作の効率向上	図3.3.1参照	センサーである道路カメラとサイバーシステムの協調により、フィジカルシステムのエッジ機器が具備する安全機能を緩めて走行効率を向上する運用。 	否 （運用禁止） 安全設計として成立しない

3.3.2　フィジカルシステムにおける対処方法

安全設計されていないサイバーシステムからフィジカルシステムのエッジ機器に対して指示を行う場合、サイバーシステムの故障やバグなどで誤作動し、正しい指示をエッジ機器等が得られない場合が考えられる。そのためエッジ機器はその指示を鵜呑みにせず、以下の確認を行う必要があると考えられる。確認の結果、問題がなければ指示に従った制御に移行する。図 3.3.3 参照。

① エッジ機器等自体が装備する保護機能の能力を超えた指示でないことを確認する。確認の結果問題があった場合は、指示を無視する。

② 保護機能の能力以内の指示であっても、現状態と矛盾しない指示であることを確認する。確認の結果、問題があった場合は、指示を無視する。

③ サイバーシステムからの指示を逐次プロファイリングし、最新の指示とプロファイリングした結果とを照らし合わせ、総合的に指示が正しいか否かを判断する。判断の結果、問題があった場合は、指示を無視する。

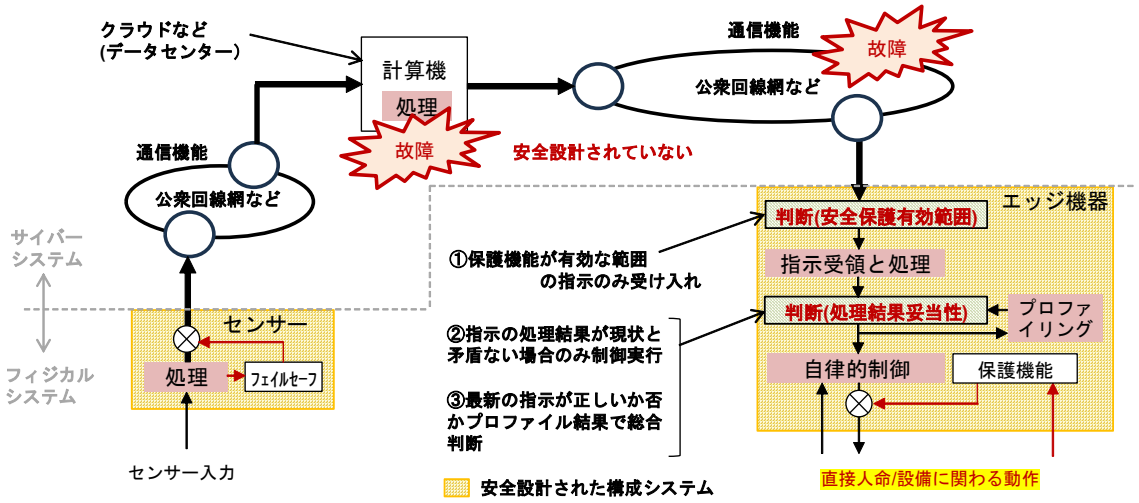


図 3.3.3　サイバーシステムからの指示に対処する考え方

例えば、エッジ機器等が自動運転車の場合、人との距離が 10m の状況下において、サイバーシステムから道路に障害物なしで加速する指示が来た。この場合、エッジ機器の自動運転車は保護機能であるブレーキシステムで人命を守ることはできないと判断し、この指示を無視する。

3.3.3　サイバーシステムにおける対処方法

サイバーシステムに対する安全設計ができない状況下においても、サイバーシステムの信頼性を極力向上させるための努力は必要であり、可能な範囲で信頼性設計を実施する必要がある。例えば、フィジカルシステムのエッジ機器に対する指示をサイバーシステムの構成システムである計算機が出力する際に、その指示の正当性確認を計算機自体が実施するような設計である。図 3.3.4 参照。

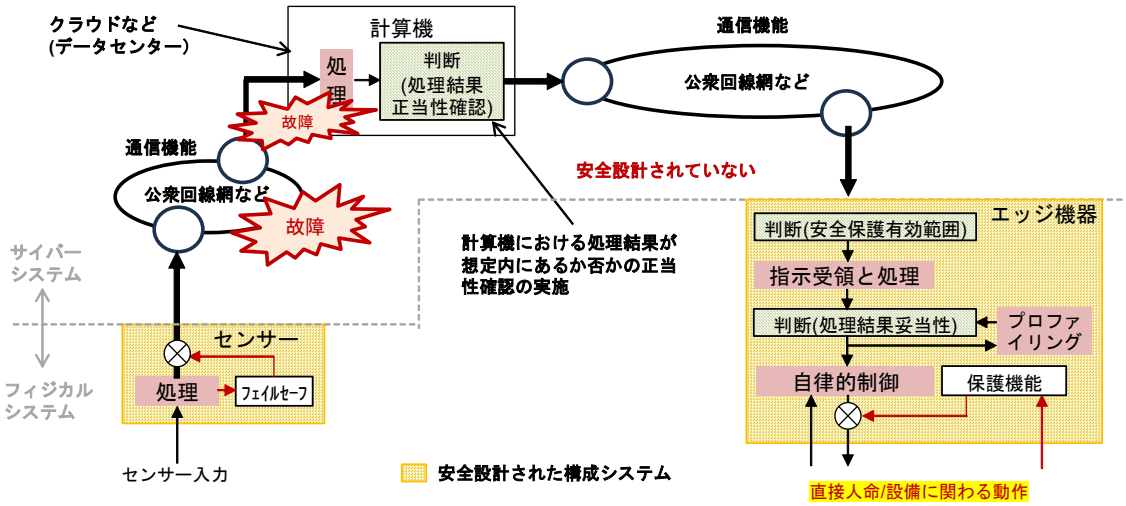


図 3.3.4　指示に対する正当性確認を計算機自体が行う信頼性設計の例

3.3.2 項で説明した通り、サイバーシステムの故障による誤指示の可能性を考慮して、指示の妥当性を判断する機能をエッジ機器に必要とするが、さらなる安全性の向上を目的に、例えば、指示を出力する計算機自体がその指示の正当性を確認してから出力する信頼性設計が考えられる。

3.4　サイバーシステムの安全設計

CPS を直接人命に関わる使い方で運用するために、サイバーシステムを安全設計することは理想である。この理想を将来的に実現するために、サイバーシステムにおける安全設計について 3.4 項で説明する。

3.4.1　IoT“つながる世界の開発指針”をCPSの安全設計に適用

“つながる世界の開発指針”は、IoT 分野で既に明確にされている。CPS は IoT に加え、仮想世界のサイバーシステムで分析・解析された結果を現実世界のフィジカルシステムにフィードバックするものである。このため、CPS の安全設計の要点は、１）フィジカルシステムであるエッジ機器の最終出力部（人との接点）において確実に安全を担保すること（3.1 項で説明）、２）エッジ機器が人に危害を与えないように、サイバーシステムにおける処理の連鎖によるフィードバック（指示）を正しく出力すること、の２点である。つまりサイバーシステムの安全設計の要点は、後者の２）である。図 3.4.1 参照。

つながる世界の開発指針一覧

	大項目	指針	
方針	3.1 つながる世界の安全安心に企業として取り組む	指針 1	安全安心の基本方針を策定する
		指針 2	安全安心のための体制・人材を見直す
		指針 3	内部不正やミスに備える
分析	3.2 つながる世界のリスクを認識する	指針 4	守るべきものを特定する
		指針 5	つながることによるリスクを想定する
		指針 6	つながりで波及するリスクを想定する
		指針 7	物理的なリスクを認識する
設計	3.3 守るべきものを守る設計を考える	指針 8	個々でも全体でも守れる設計をする
		指針 9	つながる相手に迷惑をかけない設計をする
		指針 10	安全安心を実現する設計の整合性をとる
		指針 11	不特定の相手とつなげられても安全安心を確保できる設計をする
		指針 12	安全安心を実現する設計の検証・評価を行う
保守	3.4 市場に出た後も守る設計を考える	指針 13	自身がどのような状態かを把握し、記録する機能を設ける
		指針 14	時間が経っても安全安心を維持する機能を設ける
運用	3.5 関係者と一緒に守る	指針 15	出荷後も IoT リスクを把握し、情報発信する
		指針 16	出荷後の関係事業者に守ってもらいたいことを伝える
		指針 17	つながることによるリスクを一般利用者に知ってもらう

出典：IEC 62853と「つながる世界の開発指針」
Open Systems Dependabilityの観点からの考察（SEC journal Vol.14 No.1 Aug. 2018）

CPSの安全設計においても、IoT分野についてまとめられた左表の指針に則り、フィジカルシステムへの効能毎にサイバーシステムの安全設計を実施する。特に、フィジカルシステムにフィードバック（指示）する観点から、フィジカルシステムでの危険の発現を防止、フィジカルシステムに誤った指示をしない、について配慮が必要である。

また、フィジカルシステムであるエッジ機器の保護機能発動を抑制するような運用となる場合は、CPSにおける安全責任主体者がCPSの安全設計や安全ガバナンス設計を実施し、危険発現時の対処に責任を持ち、これを実現する必要がある。また、サイバーシステムの構成システムである計算機（クラウド等）、通信機能（公衆回線等）、AI処理機能等に対する厳格な安全設計が必要である。

図 3.4.1　IoT 分野における“つながる世界の開発指針”を CPS の安全設計に適用

１）フィジカルシステムにおいて危険の発現を防止

3.1 項の再掲である。詳細は 3.1 項 フィジカルシステムの安全設計を参照のこと。

CPS として人の安全を守ることが重要だが、たとえ CPS の各構成システムが、CPS から切離され単独運用になった場合においても、人命に対する許容できない危険が発現しないよう、特にフィジカルシステムのエッジ機器において、人への危害の発生を防止することが最優先の設計となる。

２）フィジカルシステムであるエッジ機器に対し誤ったフィードバック（指示）をしない

3. 4 項 サイバーシステムの安全設計における真骨頂である。

サイバーシステムの構成システムである計算機や通信機能等による処理不備や処理遅延など、誤った処理による指示、鮮度不足の指示、フィジカルシステムが理解できない解像度や精度の指示、セキュアでない処理で生成された指示、AI アルゴリズム不良で生成された指示、等の誤指示や偽指示をフィジカルシステムへフィードバックしない安全設計が必要である。

3.4.2　セキュリティの考慮

単独事業者でクローズする CPS であっても、公衆回線等を使用する場合は、図 3.4.2 に示すような、なりすましやサイバー攻撃の可能性が出てくる。

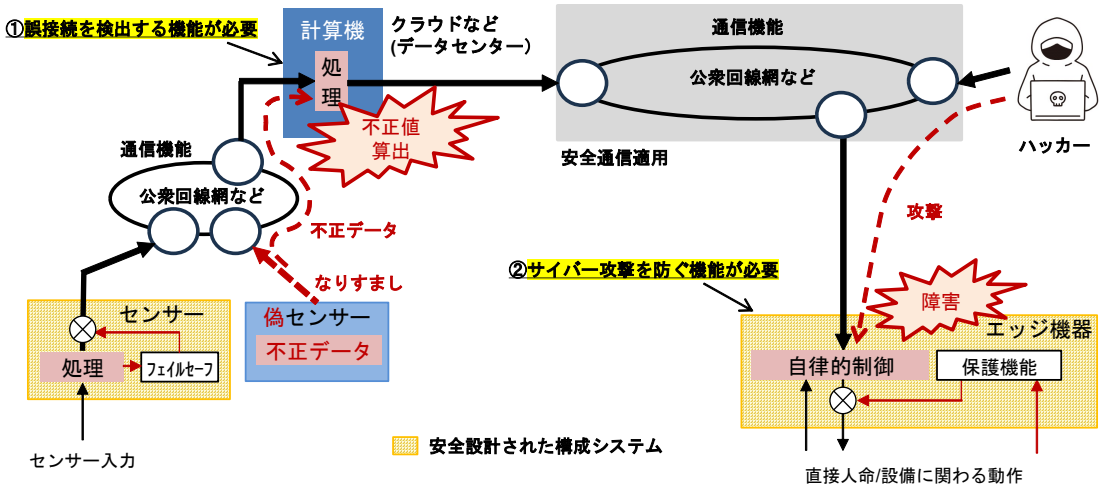


図 3.4.2　CPS におけるセキュリティ対策の必要性

なりすましに対応するには、誤接続を検出する機能（①）が例えば計算機やエッジ機器に必要となる。これはセキュリティ対策に見えるが、実際のところは安全設計の一部として IEC61508 機能安全規格に記載がある。具体的には 3.2.2 項で説明した安全レイヤによって検出することが可能となる。このセキュリティ的な目的のためにも、また公衆回線を土管のような単なる伝送パイプ（ブラックチャネル）として扱うためにも、サイバーシステムおよびフィジカルシステムに安全通信を適用し、安全レイヤを実装することが不可欠である。

サイバー攻撃に対応するには、サイバー攻撃を防ぐ機能（②）が例えば計算機やエッジ機器に必要となる。このレベルになると例えば IEC 62443 制御セキュリティ規格に準拠したセキュリティ設計が必要となるが、それでも 3.1.11 項で説明したように、安全設計がしっかりされていれば、セキュリティ設計に脆弱性が見つかり攻撃が成功した場合でも、エッジ機器に搭載された保護機能によってエッジ機器自体の制御不具合を検知し、人への危害を防止するために安全状態へ遷移できる。つまり目標である安全の担保は達成できる。

3.4.3　AI処理に対する安全設計

2.2.2 項(5)に IEC 61508 機能安全規格 Ed.3 にて規格化される予定の AI に対する安全設計について概況を示したが、以下に WG（IEC TC65/SC65A/JWG21）にて検討中のドラフト案について概要を説明する。現状規格化されている IEC 61508 機能安全規格 Ed.2（IEC 61508-3:2010 Table A.2 No5）においては、AI 処理を故障診断に対して使用することは認めているが、それ以外に適用することは推奨していないため、現時点においては、AI 処理を用いた CPS は、第三者によって認められる安全設計として確立した状態で開発することはできない。Ed.3 のリリースを待つ必要がある。

１） WG（IEC TC65/SC65A/JWG21）で想定している Ed.3 向け AI 処理の適用範囲

以下の３種の適用を想定している。

① AI 処理を安全間連系に使う

直接人命に関わる制御における制御ループの中に AI 処理を組み込む使い方である。例えば、フィジカルシステムのセンサーであるカメラ等に画像認識等として AI 処理を組み込む場合、サイバーシステムの計算機に判断処理等として AI 処理を組み込む場合、フィジカルシステムのエッジ機器に判断処理等として AI 処理を組み込む場合、等が主な使い方となる。

② AI 処理に安全間連系を付加する

AI 処理を中心としたシステムの中に直接人命に関わる制御を組み込む使い方である。例えば AI 処理がシステムの中核を成して指示を作り出しエッジ機器等を操る場合、等が使い方となる。

③ AI 処理をクリティカルシステムの開発・検証に使う

直接人命に関わる制御装置の開発や検証に AI 処理を使う、つまり開発プロセスとして AI 処理を適用するという使い方である。例えば、適用規格の翻訳を AI 処理で行う場合、機能仕様書を AI 処理で生成する場合、テスト項目や期待値を AI 処理で生成する場合、等が使い方となる。

２） AI 処理に対する安全設計手法の Ed.3 への提案

AI 処理自体は安全設計できないという考え方で生まれた AI 処理の安全設計手法を Ed.3 へ提案中である。

安全設計されていない AI 処理の結果を安全設計された検証機能で比較を行い、結果が安全担保できると考えられる範囲に入っている時だけ出力を許可する手法である。具体的には図 3.4.3 に示す通りである。

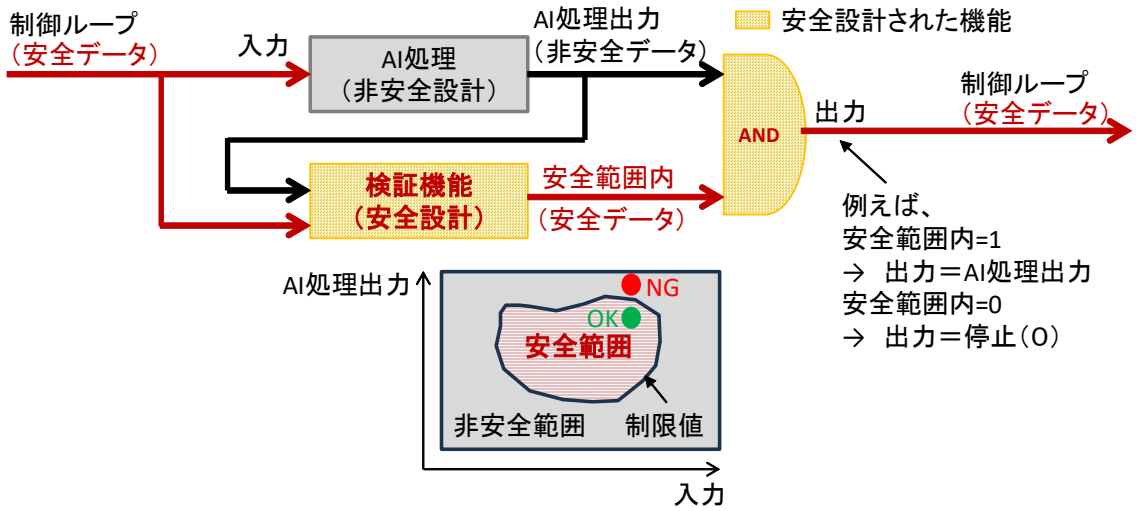


図 3.4.3　AI 処理の安全設計手法

もし検証機能の結果が安全範囲内に入っていないときは、出力を定義した安全状態に遷移させる。上図の例の場合は、AND 機能によって出力停止（0 を出力）することで安全状態に遷移させている。検証機能と AND 機能は安全設計されている必要があり、3.1.8 項 3）（2）で説明した通り、これらの機能には正しく動作するかを確認する診断が定期的に必要となる。

この手法の場合、検証機能における安全範囲（制限値）が安全を左右する基準値となるが、この制限値は予め人によって予想した値以外にも AI という特性から想定外の値が安全範囲内になる場合があり得る。結果を見ないとわからないということであり、この想定外の値を新しい制限値として見直す手法の例を以下に説明する。

３） 検証機能における制限値の見直し手法（例）

図 3.4.4 は、AI 処理によるごみ焼却ボイラー制御の例である。従来のボイラー制御は、プログラミングされた燃焼制御が行われており、制限値も事前計算によって決められている。しかしこのプログラミングが最適な燃焼効率であるとは限らない。AI 処理によって燃焼効率が向上する可能性がある。逆に言えばどのような制御を実施すれば更なる効率向上が可能になるか、やってみないとわからない（AI 処理特有の性質）。

検証機能の制限値の初期値は、プログラミングによる燃焼制御と同じ制限値（事前計算によって決定）を使うしかないが、この値を使い続けると燃焼効率をさらに向上する制御ができなくなる可能性がある。一時的に事前に決めた制限値を超えたからといって、すぐに安全状態に遷移させるのではなく、ボイラーの状態を確認しながらその AI 処理が燃焼制御として 1 つの有効な挙動であるなら、新しい制限値のパターンであることを検証機能が学習しアップデートすることで、より優れた制御が可能となる。無論、AI 処理も同時に学習していく。

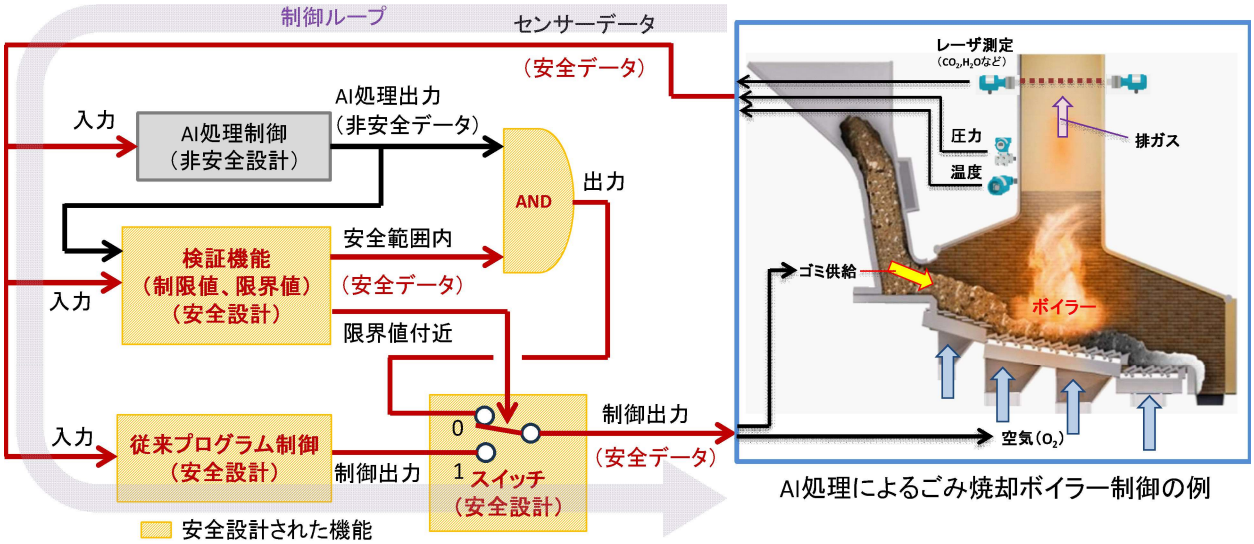


図 3.4.4　AI 処理によるボイラー制御の例

もし検証機能がボイラーの限界値に近づいたと判断した場合は、スイッチへ 1 を出力し、AI 処理による制御を切り離し、従来プログラム制御による制御出力に切り替える。これによりボイラー制御に可用性を持たせている。

検証機能における制限値の学習は、図 3.4.5 のような考え方で実施できる。

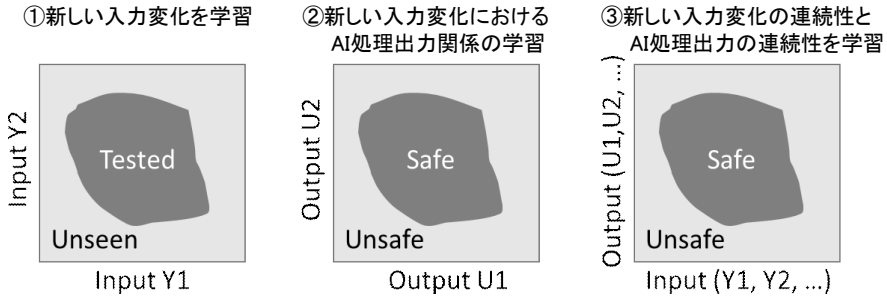


図 3.4.5　制限値の学習の例

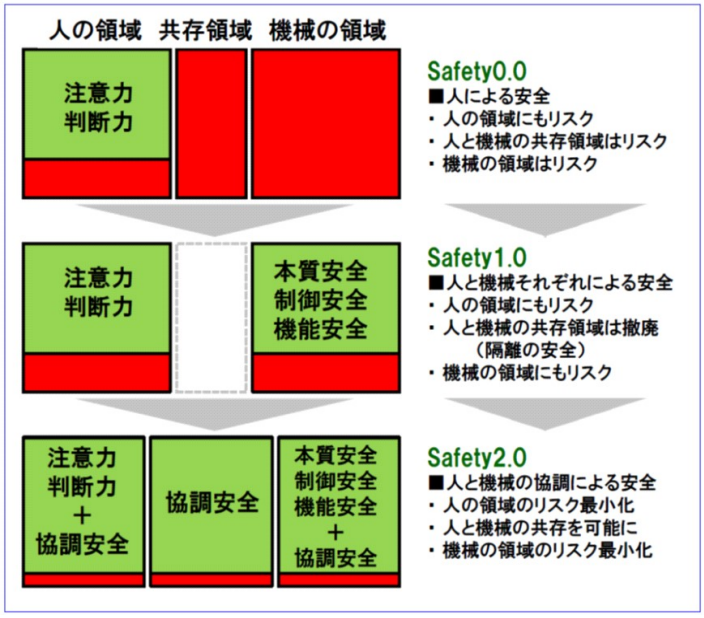
検証機能の入力となるセンサーデータが、Y1 から Y2 に変化したようなケースが今までにない挙動である場合、これをテスト的な入力状態と捉え（図中の①）、その時の AI 処理の出力が U1 から U2 になった結果、制限値内（安全範囲内）にあるかどうか（図中の②）、またそれらの連続的な入力（Y1、Y2、・・・）とそれに対する AI 処理の連続的な出力（U1、U2・・・）の関係が一連のボイラー制御として制限値内（安全範囲内）で成立するかどうか、を判断しながら学習していく方法である。

3.4.4　協調安全（Safety 2.0）を考慮した安全設計

いずれは協調安全（Safety 2.0）を考慮した CPS の安全設計について説明したいと考えているが、本ディスカッションペーパーの今回の版においては、協調安全（Safety 2.0）の概要だけに留めておく。

協調安全（Safety 2.0）とは、IoT 時代に合わせた日本発祥の新しい安全に対する考え方である。IoT と AI 処理を組み合わせる（CPS に AI 処理を適用する）ことにより、直接人命に関わる制御において人とエッジ機器である機械の共存に対するリスクを軽減できる考え方である。図 3.4.6 参照

。



出典：「IoT時代の新しい安全『Safety2.0』の全貌」https://www.ipa.go.jp/files/000062789.pdf

図 3.4.6　協調安全（Safety 2.0）の考え方

従来の安全（Safety 1.0）の考え方は、直接人命に関わる制御において、人と機械を干渉させない（距離をおく）ことで安全を担保する設計手法であった。しかしそれでは社会が目指すエコなシステムを創造することができない。例えば、エッジ機器である自動運転車は、人がいない専用レーンを走ることが目標ではなく、一般道の交差点、商店街の中、等、人が多数存在する中を人と一緒に走行できるエコなシステムを目指しているからである。そこで考案されたのが協調安全（Safety 2.0）である。

協調安全（Safety 2.0）は、AI 処理の力を借りて、人が機械と干渉しそうになった時、機械を止めるという安全対策から、できるだけ止めないという安全対策へ移行させることを主体としている。例えば図 3.4.7 に示すような使い方を提案している。

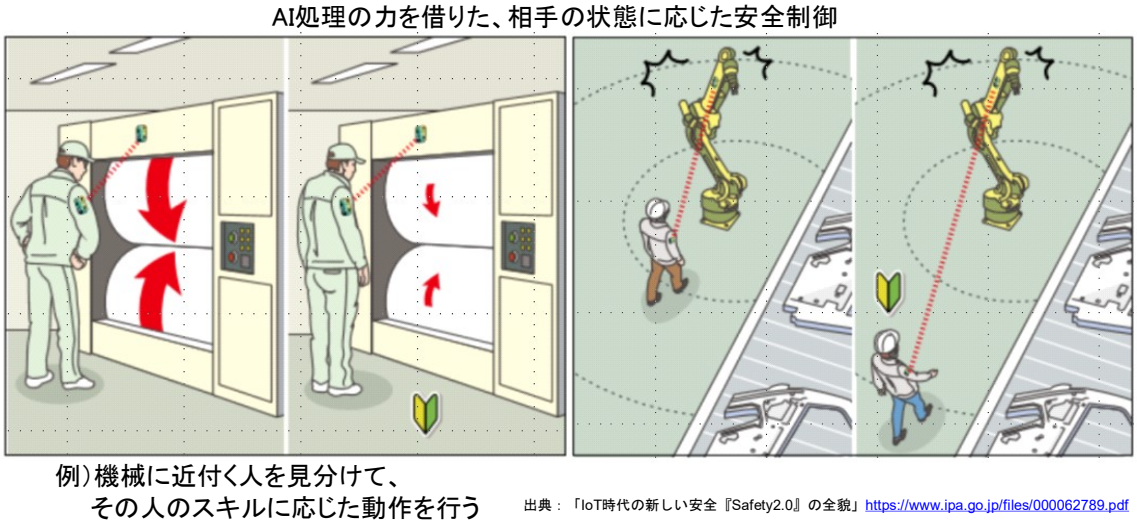


図 3.4.7　相手の状態に応じた安全制御

機械に近づこうとする人がいた場合、AI 処理によって近づく人のスキルを判断し、スキルが低ければ即停止するが、スキルが高ければよほど近づかない限り動作し続ける、という使い方である。

協調安全（Safety 2.0）は、現在 IEC SyC/SM における ahG7 ワーキングによって進められている。ahG7 は、Collaborative Safety for Smart Manufacturing（スマートマニュファクチャリングのための協調安全）というテーマで規格化を進めている。詳細は、IEC ahG 7 Dashboard > Structure: Subcommittee(s) and/or Working Group(s), Membership, Officers, Liaisons 参照。

3.4.5　共生安全を考慮した安全設計

いずれは共生安全を考慮した CPS の安全設計について説明したいと考えているが、本ディスカッションペーパーの今回の版においては、共生安全の概要だけに留めておく。

共生安全とは、協調安全（Safety 2.0）の拡張的な考え方であり、協調安全（Safety 2.0）において人とエッジである自律機械が接触する原因となる行動計画や安全ルールを改修することを目的とする安全設計の考え方である。図 3.4.8 参照。

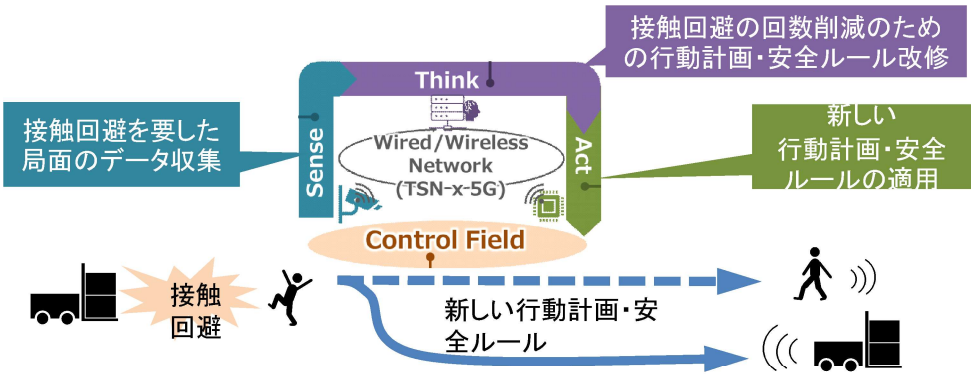


図 3.4.8　共生安全の考え方

接触回避を要した局面のデータ（ヒアリハット的データ）を収集することで、接触回避の回数を削減するための行動計画や安全ルールを改修し、実際の現場に対してアップデートした新しい行動計画や安全ルールを適用することができる。これにより、異種システム混在環境での安全性向上、接触回避の回数を削減することで効率向上と安心が実現できる。例えば図 3.4.9 に示すような使い方を想定している。

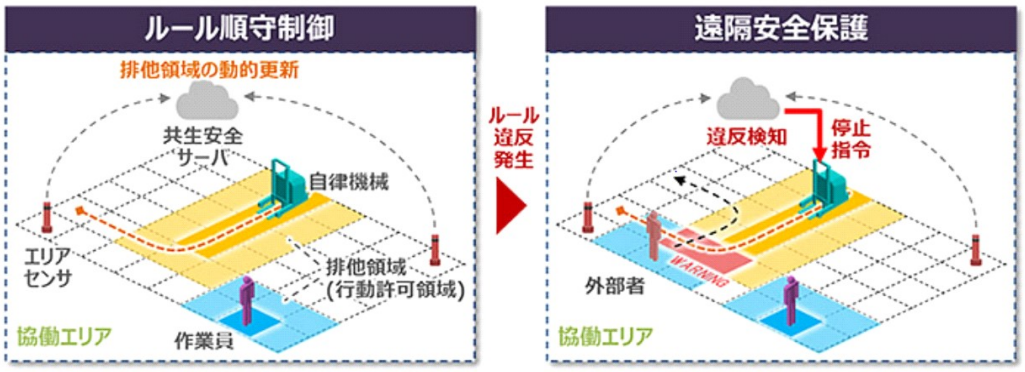


図 3.4.9　作業全体最適を実現する CPS の例

システムの安全検証が可能なシミュレーション技術を用いて、作業エリアに対してルールを適用した際の安全性や作業効率を評価する。策定したルールに対し、人と自律機械の現在および将来予測される位置の情報を用いて、サイバーシステムである計算機が移動を許可する範囲（以後、排他領域）を自律機械に割り当てることでルールを順守させる。計算機は作業エリア内の人と自律機械の行動範囲をグリッド状に管理し、センサーからの情報により排他領域を動的に更新しながら、排他領域外に自律機械が出ないように制御する。

自律機械やシステムの異常により自律機械が排他領域外に出る、あるいは、自律機械が移動するグリッドの範囲内に外部者が侵入する（ルール違反する）ことが予測された場合に、計算機が自律機械に対し迅速に停止指令を出す。

この例におけるサイバーシステムの計算機とフィジカルシステムのエッジ機器（自律機械）は、安全設計されている必要がある。また計算機上で協調安全（Safety 2.0）を実行するための AI 処理に対しても安全設計が必要となる。

共生安全（Symbiotic Safety）は日本企業によって研究が進められており、国際標準化中の協調安全（Safety 2.0）IEC SyC/SM ahG7 の拡張規格として、国際標準化を進めている。

3.4.6　計算機に対する安全設計

サイバーシステムの計算機は、直接人命に関わる制御の一部に加担する（その制御ループに加入する）構成（図 3.4.10 参照）で使用する場合、安全設計が必要となる。計算機の安全設計は、エッジ機器の自律的制御機能に対する安全設計と基本は同じである（詳細は 3.1 項を参照）。唯一異なる点は、計算機はエッジ機器と異なり直接的な人との接触がないことである。つまり計算機に独立した保護機能は必要なく、計算機が常に正しい処理結果を出力できるように安全設計することで、計算機の安全は担保できる。

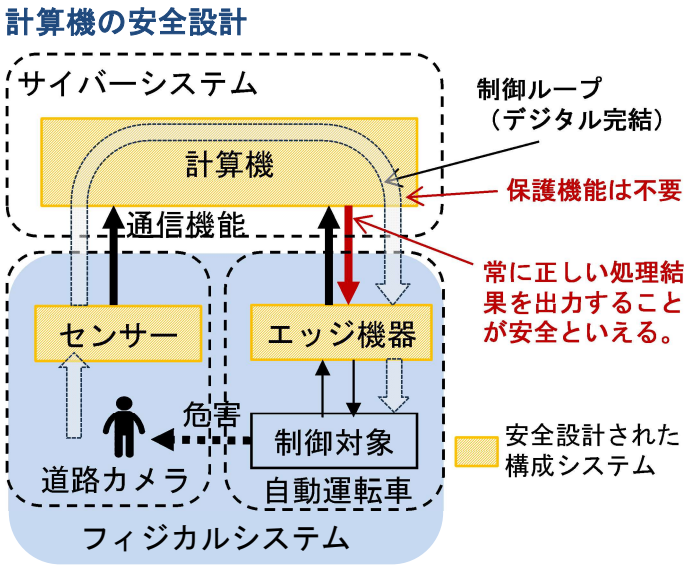


図 3.4.10　計算機の安全設計

しかし、現時点の技術では、計算機を安全設計することは難しい。特にクラウドやデータセンターの計算機の特長である並列演算処理を保ちつつ安全設計を実装することが困難なためである。図 3.4.11 に計算機の基本構成例を示す。計算機はハードウェアとしてプロセッサ、メモリ、ストレージ（SSD 等）、バス、LAN、電源装置等の各機能から構成され、その上でソフトウェアである BIOS/ドライバー、OS、ミドルウェア、アプケーションの各機能が動作する。この構成に対して、各機能を機能安全規格（IEC 61508）に準拠するように安全設計した場合の例を説明する。

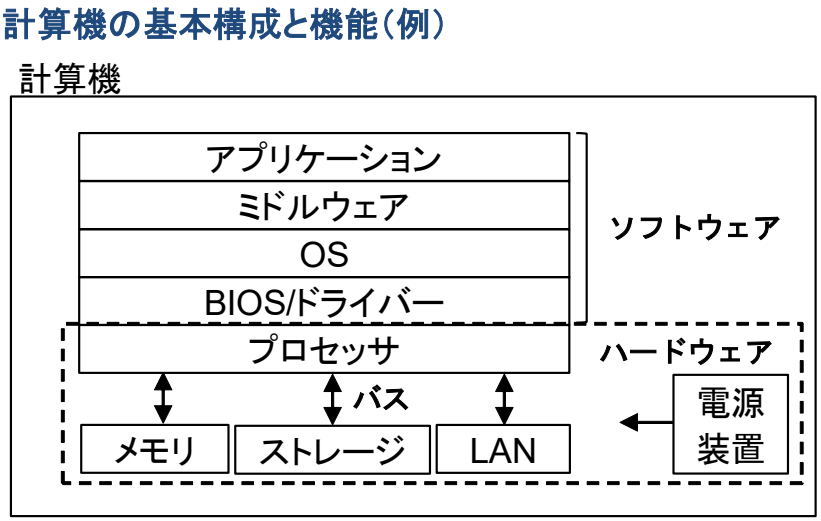


図 3.4.11　計算機の基本構成と機能（例）

1）ハードウェアに対する安全設計の例

（1）　プロセッサ

プロセッサメーカーが設計したものを部品として調達して計算機に組み込む形態が一般的となるため、計算機を設計する製造者から見たプロセッサはブラックボックスである。そのためプロセッサに対する安全設計の例としては、プロセッサの処理結果が正しいか否かをプロセッサの外側で常時チェックする機能を設置する考え方である。この場合、チェック機能にはバグなどのシステマティック故障があってはならないため、ホワイトボックスで安全設計する必要があり、チェック機能が正しく動作しているかを定期的に診断する必要がある。図 3.4.12 にプロセッサの安全設計例について示す。

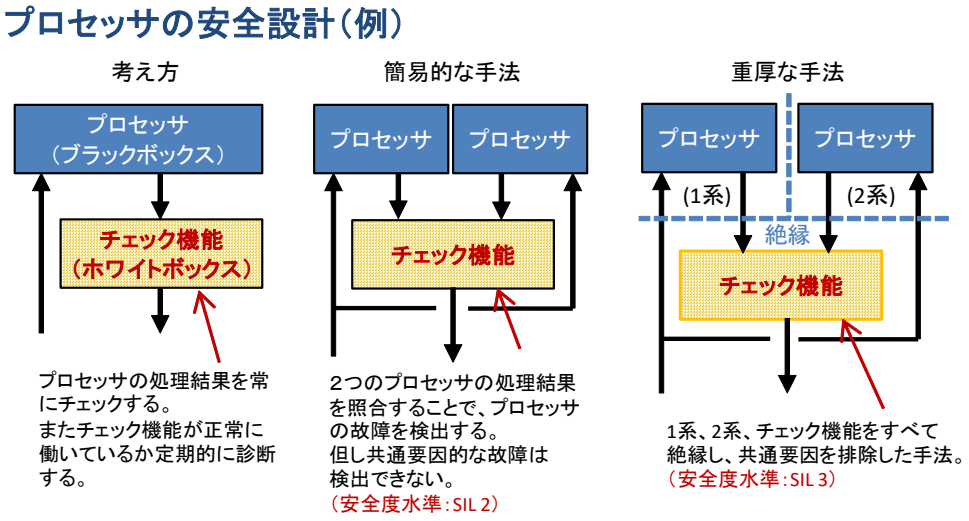


図 3.4.12　プロセッサの安全設計（例）

簡易的な手法では、同じプロセッサを並べてチェック機能で処理結果を照合する。但し、プロセッサ以外の回路（電源、発振器、配線エリア等）が共通であるため、それらの共通要因故障をこの手法では検出できない場合がある。よって安全度水準 SIL 2 までが適用を許される。

重厚な手法では、各プロセッサとチェック機能をすべて絶縁し、共通の電源、共通の回路、共通な配線エリアを存在させないことで共通要因故障を排除する。安全度水準 SIL 3 までが適用を許される。

実際にこのような安全設計を実装するのは難しい。簡単な構造のプロセッサであれば２つのプロセッサの同期も可能と思えるが、高速で構造も複雑なプロセッサでは同期させることが困難と考えられる。各プロセッサメーカーから機能安全規格に準拠したプロセッサがリリースされるようになったので、これを使う方法も考えられる。しかし現時点においては、クラウド等で使用する並列演算を主目的としたプロセッサは存在しない。エッジ機器（自動運転車等）用途に開発された組み込み向けプロセッサが主であるため、一部のクラウドではこれらのプロセッサを計算機に使用して安全を担保し、自動運転車のエミュレーション等を行わせているに留まっている。以下に一例であるが、機能安全規格に対応したプロセッサを記載する。

① arm Cortex-R5F
② arm Cortex-A78AE
③ AMD Zynq UltraScale+ MPSoC
④ ルネサス R-Car V3U
⑤ NVIDIA DRIVE Xavier

（２） メモリ

プロセッサ同様、メモリ素子（以下メモリ）もブラックボックスである。そのためメモリに対する安全設計の例としては、メモリから読み出したデータが正しいか否かをメモリの外側で常時チェックする機能を設置する考え方である。この場合、チェック機能にはバグなどのシステマティック故障があってはならないため、ホワイトボックスで安全設計する必要があり、チェック機能が正しく動作しているかを定期的に診断する必要がある。

中性子線によってメモリ内容が化けてしまう事象をソフトエラーと呼んでいるが、ソフトエラーに対処するために ECC（Error Correction Code）機能を実装する場合が多い。しかし ECC 機能は誤ったデータを訂正する（生成ともいえる）機能を持っているため、機能安全規格では安全ではない機能とされている（可用性と安全性は別である）。従って ECC を使う場合は、CRC（Cyclic Redundancy Check）などの冗長コードと併用することが必要とされている。図 3.4.13 にメモリの安全設計例について示す。

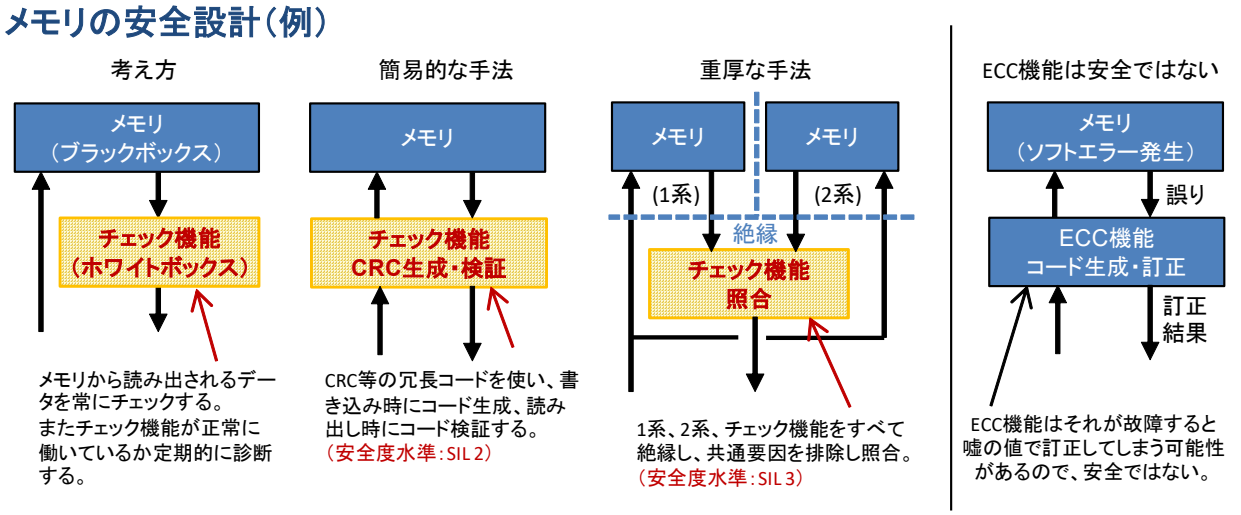


図 3.4.13　メモリの安全設計（例）

簡易的な手法では、CRC 等の冗長コードを使用し、メモリに書き込む際に CRC コードを生成し、読み出し時に CRC コードを検証する。CRC は複数ビットの誤りを検出するのに適しているが完全ではない。よって安全度水準 SIL 2 までが適用を許される。

重厚な手法では、CRC などの冗長コードは使用せずメモリを 2 つ用意しチェック機能で読み出し時にデータを照合する。各メモリとチェック機能をすべて絶縁し、共通の電源、共通の回路、共通な配線エリアも存在させないことで共通要因故障を排除している。安全度水準 SIL 3 までが適用を許される。

プロセッサとメモリを組み合わせた形を 1 つの系として、1 系と 2 系の照合をストレージや通信などの I/O に出力する際に行う手法も考えられる。しかしこの方法は効率がよさそうに見えるが、系間の同期が問題となり、実装の難易度は高い。また高速処理には向かない。

（3）　ストレージ

メモリと同じ考え方である。図 3.4.14 は、図 3.4.13 のメモリをストレージに置き換えた構成となる。

ストレージには可用性のための RAID（Redundant Arrays of Inexpensive Disks）という手法があるが、RAID は機能安全規格では安全ではない機能とされている（可用性と安全性は別である）。これはメモリの ECC と同じ考え方である。RAID を適用した安全設計をするには、RAID そのものをホワイトボックスで安全設計するか、RAID の外側でチェック機能を置くかのいずれかであるが、いずれにしても難易度は高い。

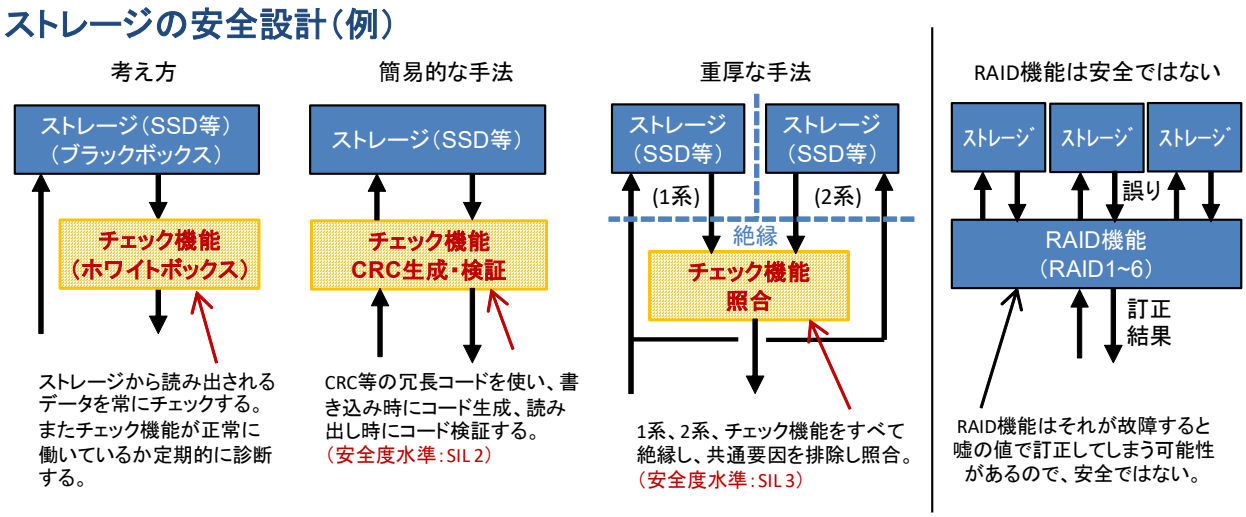


図 3.4.14　ストレージの安全設計（例）

（4）　バス

DDR、PCIe、SATA 等のバス（インタフェースとも呼ばれる）についてもプロセッサやメモリと同じで、規格化されたブラックボックスであることが一般的である。プロセッサやメモリと同様にバス個別にチェック機能を外側に設けることもできるが効率が悪い。例えばメモリと DDR バスを繋いだその外側でチェック機能を設置するのがよい。同様にストレージと SATA バスを繋いだその外側でチェック機能を設置、通信と PCIe バスを繋いだその外側でチェック機能を設置、といった具合である。図 3.4.15 に例を示す。この形態であれば、各機能が正常でもバスが故障すれば異常を検出できる。

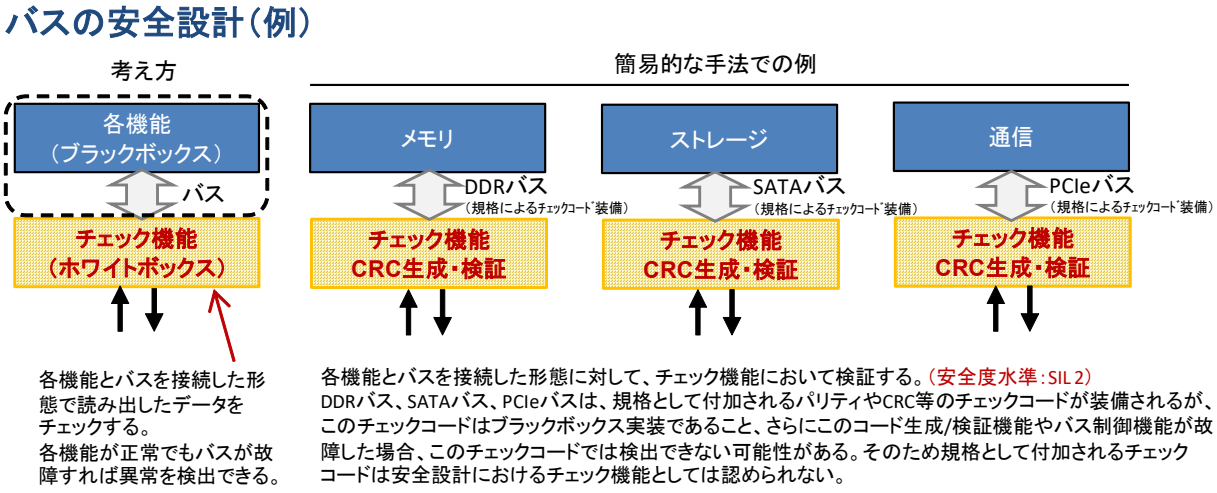


図 3.4.15　バスの安全設計（例）

注意すべき点は、DDR バス、SATA バス、PCIe バス等の規格として付加されるチェックコード（パリティや CRC 等）はブラックボックス実装（チップメーカーでの実装）であり、さらにこのコード生成/検証機能やバス制御機能が故障した場合、このチェックコードでは検出できない可能性がある。そのため規格として付加されるチェックコードは安全設計におけるチェック機能としては認められない。それとは別にその外側

でホワイトボックス設計したチェック機能が必要である。つまり、例えば PCIe バスでは、結果的に PCIe バスの CRC コードに加えてチェック機能の CRC コードの 2 重のコードが必要となる。

（５） LAN

LAN についてもバスと同じで、規格化されたブラックボックスであることが一般的である。しかし LAN 等の通信に対する安全設計は、機能安全規格においてその手法が安全通信として専用に規格化されており、それは“安全レイヤ”を実装することである。安全レイヤについては、3.2.2 項を参照。

現時点において、一般的な LAN である 1GLAN や 10GLAN に対する安全レイヤをハードウェアで装備する製品はないと考えられるため、プロセッサ上のソフトウェアで安全レイヤを実現するしかないが、安全レイヤは非常に重いプロトコルであるため、通信性能は期待できない。

（６） 電源装置

電源装置は、人体に危害を加える可能性のある高電圧を扱うため、まず製品安全規格（UL、CE 等）に準拠する必要がある。製品安全については 3.1.9 を参照。また製品安全とは別に機能安全規格についても準拠する必要があり、その主な内容は以下の 3 点である。図 3.4.16 参照。

① SELV 回路の実装
② 二次側電圧の常時チェック
③ 二次側電流の常時チェック

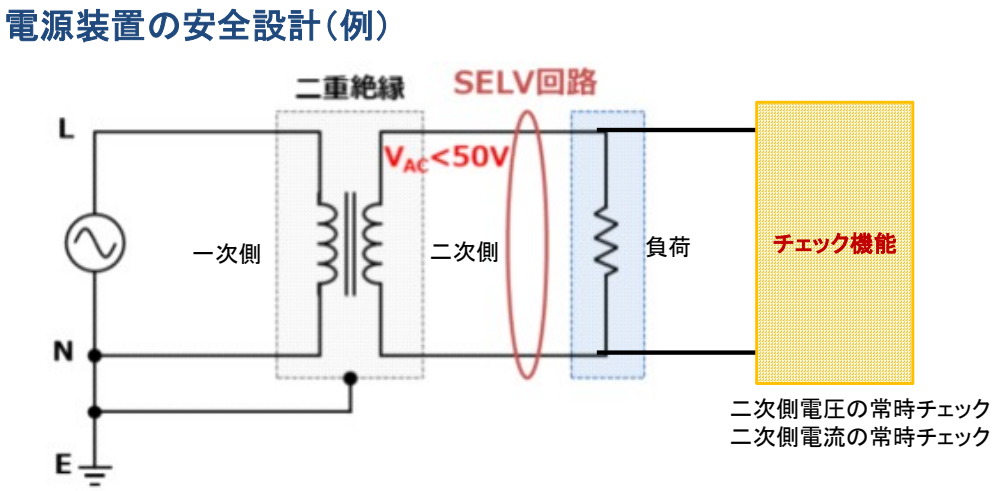


図 3.4.16 電源装置の安全設計（例）

① SELV 回路の実装

SELV（Safety Extra Low Voltage）回路は、電源装置の単一故障（1 点故障）が発生した際に、二次側出力に AC50V、DC120V 以上の電圧が印加されないようにする回路であり、安全設計には実装が不可欠である。また一次側と二次側が二重絶縁されている必要があり、二次側の出力は接地されないことが条件となる。安全度水準 SIL 2 と SIL3 で実装が求められる。

② 二次側電圧の常時チェック

負荷が正常に動作できる電圧の範囲を超えていないか常時チェックする機能であり、チェック機能が正常に働いているかを定期的に診断する必要がある。電源装置が機能安全規格に準拠していない（ブラックボックス製品）場合は、チェック機能は電源装置二次側出力の外側に設置する必要があり、ホワイトボックスでの安全設計が必要となる。

負荷が正常に動作できる電圧の範囲は、最低動作電圧と最大動作電圧の２つがあるが、安全度水準 SIL 2 においては、最低動作電圧以下を検出できればよい。過電圧検出については一般的に電源装置側で保護回路を装備しているため、それに頼る形でも良いとされている。最低動作電圧は負荷に依存するため、電源装置側の検出回路は当てにできないという理由である。SIL 3 においては、最低動作電圧以下および最大動作電圧以上の両方を検出できなければならない。

③ 二次側電流の常時チェック

負荷が正常動作していると考えられる状態の電流範囲を超えていないか常時チェックする機能であり、チェック機能が正常に働いているかを定期的に診断する必要がある。電源装置が機能安全規格に準拠していない（ブラックボックス製品）場合は、チェック機能は電源装置二次側出力と負荷の間に設置する必要があり、ホワイトボックスでの安全設計が必要となる。

負荷が正常動作していると考えられる状態の電流範囲は、最低動作電流と最大動作電流の２つがあるが、安全度水準 SIL 2 においては、最大動作電流以上（要は過電流）を検出できればよい。SIL 3 においては、最低動作電圧以下および最高動作電圧以上の両方を検出できなければならない。負荷が電流を計画通りに消費しないという状態も機能的に安全が担保できていないと解釈する。

２） ソフトウェアに対する安全設計の例

機能安全規格では実現性がない安全設計は求めていない。すべてのソフトウェアに対して安全設計を求めているわけではなく、例えば BIOS/ドライバー、アプリケーションへの安全設計は不要としている。ドライバーや BIOS は、装置メーカが提供する場合が多く、計算機設計者がホワイトボックスで開発することが困難とされているためである。従ってドライバーや BIOS の処理結果が正しいか否かを OS が判断する安全設計としている。アプリケーションはユーザーが開発する場合が多く、ユーザーに安全設計を強要するのは困難とされているためである。従ってアプリケーションの動作をミドルウェアによって監視する安全設計としている。

（１） ソフトウェア共通（一例）

OS やミドルウェアに対して共通な安全設計手法について一例を説明する。機能安全規格で細かく手法が規定されているうちの代表的なものである。

① 割込みの使用制限

基本的には割り込みを使用しないことが推奨される。安全とされるソフトウェアは、計画した順番に計画した処理時間で動作することが求められるため、割り込みはこれを崩してしまうためである。

② ポインタの使用制限

レジスタやメモリの格納位置、プログラムのジャンプ先やコール先等、はポインタでなく直接指定をすることが推奨される。ポインタ値が壊れると格納位置やジャンプ先が誤ることになり、正しいデータの参照、正しい位置へのデータ書き込み、正しいプログラムの実行が出来なくなり、その結果正しい制御ができなくなる可能性があるためである。

③ サブルーチンの使用制限

スタックポインタが壊れると正しい位置に戻れなくなる可能性があるため、サブルーチンを使用しないことが推奨される。

④ モジュール化

ソフトウェアを小さな機能に分割して、各機能を小さなモジュール化することが推奨される。小さなという意味は、人間が容易に理解できる構造であるということである。これにより潜在的なバグ発生を防ぐ効果がある。

⑤ ダイバースプログラム

同じ機能のプログラムを異なった設計でＮ個準備する。入力をＮ個で処理し、結果を比較して妥当性を判断することが推奨されている。

⑥ 時間的監視

タスクの処理時間を計測することが推奨されている。計画通りの処理時間ではなく、極めて速いまたは極めて遅い場合には正しく処理されていない可能性が高いためである。時間はソフトウェアの動作に影響しないハードウェアによる計測が必要である。

⑦ 論理的監視

タスクの処理順番を監視することが推奨されている。計画通りの処理順番でなくなった場合には正しく処理されていない可能性が高いためである。タスクに番号をつけ、番号通りに動作しているかをソフトウェアの処理に影響しないハードウェアによる確認が必要である。

⑧ タスク間のデータ受け渡し監視

データの整合性チェック、データのロックと排他制御、データロギングと監視等を実施することが推奨されている。データの整合性チェックは、タスク間で受け渡されるデータに対して、データサイズやデータ型の検証、データ範囲のチェック、不正値の検出などを実施する。データのロックと排他制御は、同時に複数のタスクからアクセスされる可能性のある共有データへのアクセスを制御するために、タスクが共有データにアクセスする前にロックを獲得し、操作が完了したらロックを解放する。データロギングと監視は、タスク間のデータ受け渡しを監視するために、データの送信元や宛先、タイムスタンプなどの情報を記録することで、データの問題を追跡・解析ができるようにする。これ以外にも、キューイングやバッファリング、データ一貫性の確保、等を実装することが推奨されている。ここでは説明を省略する。

⑨ 安全プログラムと一般プラグラムの分離

すべてが安全プログラムであれば必要はないが、一般的なIT処理を行う一般プログラムと、直接人命に関わる制御を行う安全プログラムを、１つの計算機で実行する場合は、一般プログラムが安全プログラム領域にアクセスできないように、メモリ上のプログラムやデータの保存エリアを分離することが推奨されている。このためには、安全プログラムの領域を他のプログラムがアクセスできないように、アクセスプロテクトすることが必要である。書き込みだけをプロテクトする一般のメモリプロテクトでは、リードアクセスが可能となり、一般プログラムが暴走した場合に安全プログラム領域へのアクセス負荷が上がり、安全プログ

ラムが計画した処理時間で動作できなくなる。そこでアクセスそのものをできないようにするプロテクトが必要である。これはソフトウェアの処理に影響しないハードウェアで実現する必要がある。

（２） OS（一例）

OS はハードウェアおよびミドルウェアと連携した安全設計が必要となる。安全設計における OS の役目は、ハードウェアの安全機能と連携して安全設計手法を実現する、ハードウェアと連携してソフトウェア共通の安全設計手法を提供する、BIOS/ドライバーの処理結果が正しいか監視する、ミドルウェアの動作を監視する、等である。

① ハードウェアの安全機能と連携して安全設計手法を実現

OS は直接ハードウェアにアクセスする位置付けであるため、ハードウェアの安全機能と連携して安全設計手法を実現する。例えば、前述したプロセッサ、メモリ、ストレージ等のチェック機能に対する診断処理の実施、LAN のための安全レイヤの実行、メモリエリアのパトロール（例えばビットウォーク）等である。

② ハードウェアと連携してソフトウェア共通の安全設計手法を提供

前述したソフトウェア共通の安全設計手法のうち、時間的監視、論理的監視、アクセスプロテクトについてハードウェアと連携して実現する。

③ BIOS/ドライバーの監視

BIOS/ドライバーはブラックボックスであるため、OS はそれらから返されるデータに対して、データサイズやデータ型の検証、データ範囲のチェック、不正値の検出、応答時間の監視等の整合性チェックを実施する。

④ ミドルウェアの監視

ミドルウェアは安全設計されるため、ミドルウェアからのハードウェアアクセス要求に関するデータの整合性チェック等は不要となるが（ミドルウェア側で実施）、ミドルウェアの安全設計のための連携は必要となる。例えばミドルウェアの動作に対する時間的監視、論理的監視、アクセスプロテクト等は OS のタスクを使うことになる。

（３） ミドルウェア（一例）

ミドルウェアは OS と連携した安全設計が必要となる。安全設計におけるミドルウェアの役目は、3 言語を処理する、アプリケーションの処理結果が正しいか監視する、等である。

① 3 言語の処理

機能安全規格においては、アプリケーションを C 言語等で開発することが禁止されている。C 言語等は非常に拡張性や自由度が高く、例えばハードウェアを直接アクセスするコーディングも可能である。つまりハードウェアの動作に対して直接影響を与える（例えばアクセスを集中させ処理速度を低下させる）プログラムが可能であり、非安全とされている。機能安全規格においては、IEC 61131 で規格化されている 5 言語（LD、FBD、SFC、ST、IL）のうちグラフィカルユーザーインタフェースをもつ 3 言語（LD、FBD、SFC）をアプリケーションで使用することを推奨している。この 3 言語（最低 1 言語）をミドルウェアとして安全設計した上でアプリケーションに提供する。

② アプリケーションの監視

3 言語によってアプリケーションが記述されることによって、アプリケーションの監視が実現する。ミドルウェアが安全設計されることで、アプリケーションを設計するユーザーは、安全設計について考慮せずとも安全なプログラミングが実現できることになる。ただし 3 言語は処理性能や機能に限界があるため、例えば高速化演算処理や AI 処理には、安全設計を施したカスタム FBD 等の開発が必要となる。

以上、計算機における安全設計の概要を説明したが、現時点において、このような安全設計を、仮想化環境を実現するソフトウェアやクラスタスイッチ等を使って複数の計算機（クラスタ）を並列演算させるクラウド（データセンター）の各計算機に適用することは、極めて困難である。現時点で検討されている安全設計を適用した計算機は、自動運転車等（安全設計されるエッジ機器）で採用されるプロセッサ、SoC、OS 等をベースにしたクラウド向け計算機であり、安全設計が難しい並列演算による運用は検討されていない。単独チップにおける性能を追求することで安全対応を可能としている。

3.4.7　通信機能に対する安全設計

サイバーシステムの計算機とフィジカルシステムのエッジ機器等を接続する通信機能は、小規模な無線通信（V2I 通信：760MHz/5.8GHz/5.9GHz 帯等）やローカル 5G 等、さらに一般的な公衆回線（V2N 通信：4G、5G 等）を使用することが考えられる。小規模な無線通信や公衆回線は有線回線と比べ、場所を選ばない通信ができるという特長をもつが、いずれも無線であることから通信品質が劣ることや、公衆回線ではレイテンシが劣るというデメリットも持ち合わせている。これらを使用して安全通信を実現するために、すでに普及している無線通信機器や大規模な公衆回線機器に対して安全設計を施すことは現実的ではない。そこで機能安全規格に示されるように、無線通信機器や公衆回線機器はそのままに、その両端に安全レイヤを追加実装することで安全通信を実現する。この手法が通信機能に対する安全設計である。安全レイヤについては、3.2.2 項を参照。

【注意】ブロードキャスト方式やマルチキャスト方式は、受信元からの応答がない場合、安全通信に使用することはできない（安全通信とは認められない）。詳細は 3.2.2 項（安全レイヤ）参照。

4 SoS-CPS の安全設計

4.1 構成の違いによる安全用途への適用可否の考え方

SoS-CPS の構成について、SoS-CPS が全体として実現する制御ループについて、及び SoS を構成する構成システムが安全の要求を満たす範囲の組み合わせにより、その安全用途への適否を考慮必要である。安全用途への適用可否について図 4.1.1 にまとめた。図 4.1.1 中において、〇は適用可能、△は制約付きで適用可能、×は適用不可を示す。

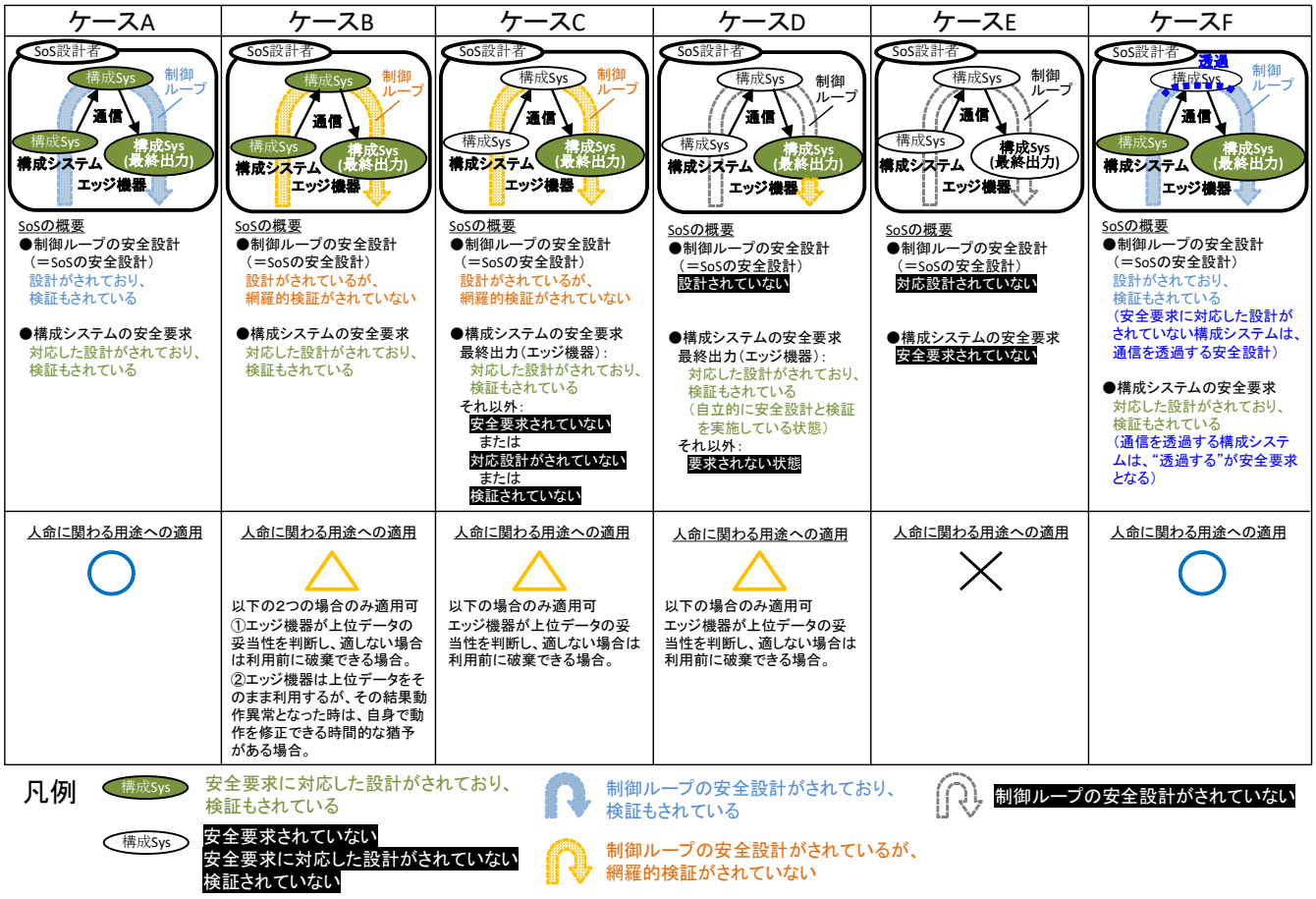


図 4.1.1　SoS-CPS における安全用途への適用の考え方

・ケース A

SoS-CPS の制御ループに対する安全設計がされており、検証もされている。また構成システムの安全要求に対して、対応する設計がされており、検証もされている。

⇒安全用途への適用は可能である。

本構成の安全設計の考え方の詳細は 3.4 章（サイバーシステムの安全設計）参照。

なお、2.2 項 2）で説明した②の設計手法は、このケース A に属する。

・ケース B

SoS-CPS の制御ループに対する安全設計はされているが、網羅的な検証がされていない。また構成システムの安全要求に対して、対応する設計がされており、検証もされている。

⇒安全用途への適用は制約付きで可能である。以下の制約①または②を満足する場合は適用可能である。

制約①：制御ループの最終段であるエッジ機器において、制御ループの上流が出力するデータの妥当性を判断し、適さない場合はデータを利用する前に破棄できる機能を有する場合。

制約②：制御ループの最終段であるエッジ機器において、制御ループの上流が出力するデータをそのまま利用するが、その結果動作異常となった場合は、自身の安全機能によって正しい動作に修正できる時間的な猶予がある場合。

制約①で使用する場合、エッジ機器は、制御ループの上流が出力するデータを信用できないと判断する場合が多くなると予想され、本来の目的や施したいサービスが実現できない可能性が高くなると推測される。

制約②で使用する場合の運用例を図 4.1.2 に示す。

本構成の安全設計の考え方の詳細は 3.3 章（安全設計されていないサイバーシステムによる協調運用に対処した安全設計）参照。

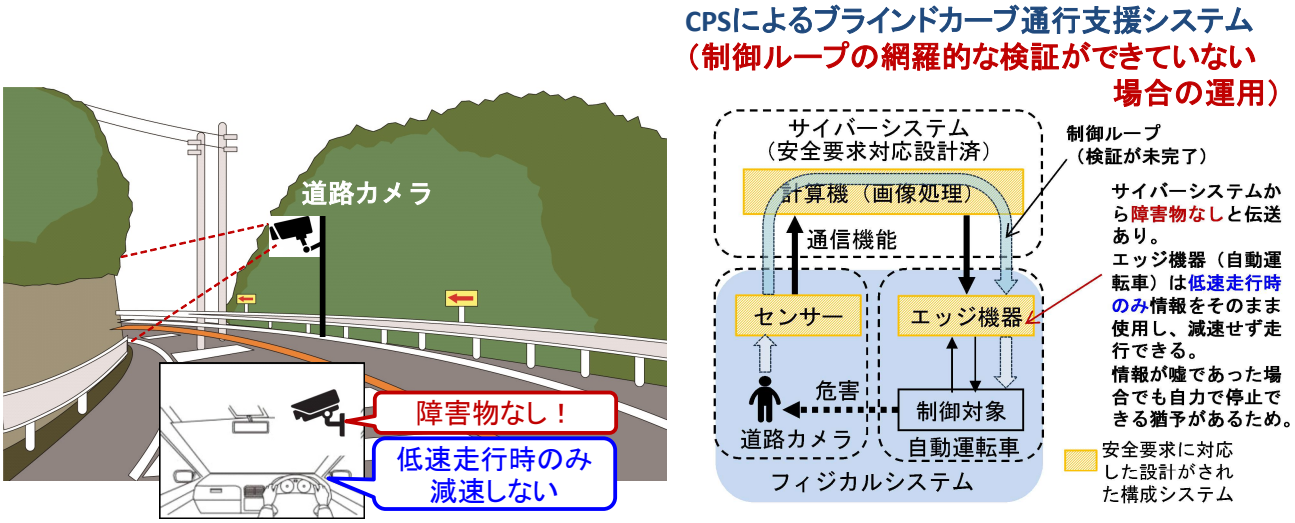


図 4.1.2　制約②における運用例

制御ループの網羅的な検証ができていない場合、エッジ機器（自動運転車）が低速で走行している場合に限って、サイバーシステムからの情報をそのまま利用してもよい。道路カメラが捉えた情報を、計算機が障害物なしと判断し自動運転車に伝送した場合、自動運転車はその情報が嘘であった場合でも人命に危害を及ぼすことなく停止できる低速走行時のみ、計算機からの情報をそのまま利用して動作を行うことができる。その結果、もし道路上に人が存在しても、自動運転車の安全機能で人に接触することなく停止することができるためである。

・ケース C

SoS-CPS の制御ループに対する安全設計はされているが、網羅的な検証がされていない。また構成システムの安全要求に対して、最終出力であるエッジ機器については、対応する設計がされており、検証もされ

ているが、その他の構成システムについては、安全要求されていない、または対応した設計がされていない、または検証されていない、のいずれかの場合。

⇒安全用途への適用は制約付きで可能である。制約は以下の通り。

制約：制御ループの最終段であるエッジ機器において、制御ループの上流が出力するデータの妥当性を判断し、適さない場合はデータを利用する前に破棄できる機能を有する場合。

本構成の場合、ケース B の制約①と同様、本来の目的や施したいサービスが実現できない可能性が高くなると推測される。

本構成の安全設計の考え方の詳細は 3.3 章（安全設計されていないサイバーシステムによる協調運用に対処した安全設計）参照。

・ケース D

SoS-CPS の制御ループに対する安全設計はされていない。従って構成システムに対する安全要求はない。但し制御ループの最終段であるエッジ機器だけが自立的に安全設計と検証を済ませている。

⇒安全用途への適用は制約付きで可能である。制約は以下の通り。

制約：制御ループの最終段であるエッジ機器において、制御ループの上流が出力するデータの妥当性を判断し、適さない場合はデータを利用する前に破棄できる機能を有する場合。

本構成の場合、ケース B の制約①と同様、本来の目的や施したいサービスが実現できない可能性が高くなると推測される。

本構成の安全設計の考え方の詳細は 3.3 章（安全設計されていないサイバーシステムによる協調運用に対処した安全設計）参照。

・ケース E

SoS-CPS の制御ループに対する安全設計はされていない。従って構成システムに対する安全要求はない。

⇒対象外であり、安全用途への適用は不可である。

・ケース F

SoS-CPS の制御ループに対する安全設計がされており、検証もされている。また構成システムの安全要求に対して、対応する設計がされており、検証もされている。

ケース A との違いは、安全要求に対応した設計がされていない構成システムに対して、通信を透過させるという制御ループに対する安全設計を行っていることである。

※通信を透過　：　上流から受けたデータを加工せずにそのまま下流に流す（転送する）こと。

⇒安全用途への適用は可能である。

本構成の安全設計の考え方の詳細は 3.2 章（安全設計されていないサイバーシステムを透過する安全設計）参照。

4.2　社会実装促進の課題

前述のケース B、C、D は、実質的に CPS の制御ループの最終出力を実施する事業者に責が偏ってしまう面がある。極端な例を挙げれば、自動運転を支援する路側のシステム等からの情報を参考に自動運転車が自

動運転する場合に、路側のシステム等からの情報を使うか使わないか判断したり、その結果発生したトラブルを回避する責任は自動運転車のみにあるということである。

これについては、路側のシステムなど CPS の制御ループを構成する構成システムが守るべきルールとそれを実効あるものにするためのガバナンスを設計し、真に実効するようにすることによって（たとえば、3.2 項に前述したようにシステム側からの信号に信頼度を付加の方法なども提案されている。）、障害発現時に責を適切に分担できるようにするなどできれば、事業者の取るべきリスクが限定できるようになり、利便性や快適性の社会実装が加速する可能性があると考えられる。

また、合わせてクラウドや通信回線などのサイバーシステムについても、その出力が人命へのリスクの可能性を帯びる SoS-CPS では、より安全なサイバーシステムによる実現がなされるようになれば、さらにエッジ機器の事業者の負担が減り社会実装が促進されるであろう。

5 SoS-CPS の安全ガバナンス

社会課題の解決に際し、不確実性を含んだシステムを活用していくことが検討される中では、そのシステムが社会に与えるリスクを抑えつつ継続的な改善を図ることで、諸外国に遅れることなく新技術を使った SoS-CPS の社会実装とそのブラッシュアップを図っていくことが求められていくと考えている。そのためには SoS-CPS を適切にガバナンスする必要がある。

ここでは、システム設計開発する立場からガバナンスで実施が求められるであろうことを想定し記載した。

5.1 SoS-CPS の安全ガバナンスの考え方

SoS-CPS、CPS の安全要求を満たすシステムの設計について３章まで説明してきた。しかし、SoS-CPS では創発性リスクの発現や事業者が複数存在する構成になるゆえに許容できないリスクの残存が避けられない。このため、SoS-CPS の安全を確保し維持するためのガバナンスについて検討する。

単一事業者による CPS なら十分なリスク想定が可能であるが実現に複数の事業者が関わる SoS-CPS では、想定外のリスクが残る可能性が高い。一般に SoS では、構成システムの運営者の違いによる適用技術や運営ルールなどの違いによるリスク（注１０）や、構成システムそのものでは問題にならなくとも SoS として組合せ動作した場合に顕在化する創発性のリスクなど予め設計で対処できないリスクがある（注１１）と指摘されている。

また、ここまで CPS としての入力から制御出力のループを含んでいたり、それ自体を構成していたりする SoS として SoS-CPS という記載をしてきており、また４章でも SoS-CPS を念頭において必要なガバナンスを検討していくが、CPS を含まないあるいは CPS ではなかった SoS でもシステムの拡張や発展により SoS-CPS になっていくことが想像できる。このため、多くの SoS について、CPS への発展を見越した安全の設計が為されることを期待し、4 章では、あえて SoS として表記し検討していくことにする。

5.1.1 SoSの安全ガバナンスリファレンスモデル

本項では、京都大学大学院法政策共同研究センターとの共同研究で得た成果をもとに、図 5.1.1 で安全ガバナンスリファレンスモデルを説明する。

2010 年代の中頃からビッグデータとディープラーニングを用いた AI の実装が 飛躍的に進むと、それに伴って世界中で SoS ガバナンスに関する議論が大きな盛り上がりをみせた。その中には、自動運転や医療の場面における法規制の話、プ ライバシーや公平性に関する話など、様々なものが入り混じっている。 これらの範囲は膨大で、それぞれを細かく追っていってもきりがないし、その 動きも速いため、仮に追いついたとしても、またすぐに状況は変わってしまう。 そこで重要なのは、SoS ガバナンスの全体像を正しく理解することである。SoS ガバナンスの枠組みを、以下のように整理する。

「SoS ガバナンスの目的」とは、基本的人権・民主主義・経済成長・サステナ ビリティなど、最終的に SoS ガバナンスによって達成すべき基本的な価値である。これらは SoS の利用の有無にかかわらず重要な価値だが、SoS の文脈においてこれ を実現するためには、安全性やセキュリティ、プライバシーや透明性など、とく に配慮すべき要素がある。これが「基本原則」と呼ばれるものである。 これらの価値や原則は、一次的には SoS の構成要素の提供者による「システムのガバナンス」を通じて達成される。そのうえで、各

システムのガバナンスについて法律で何を求めるのか、問題が生じた際の責任をどう分配するかといった、社会制度についても考えなければならない。

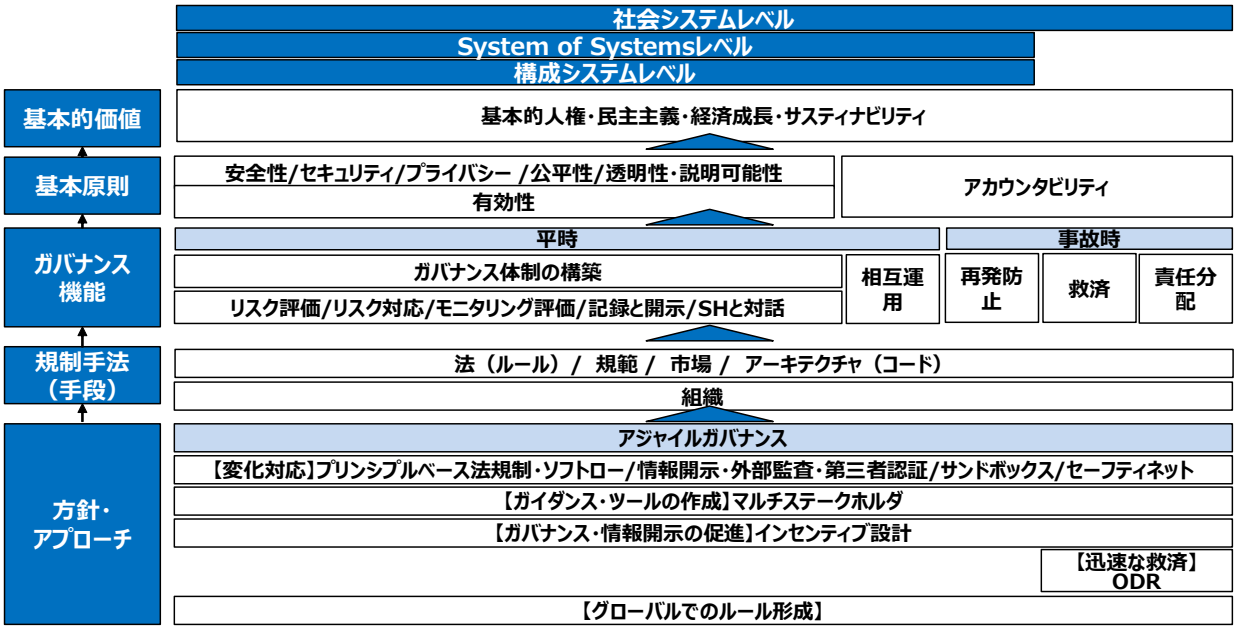


図 5.1.1　ガバナンスリファレンスモデル

このガバナンスリファレンスモデルは、社会システム、System of Systems、構成システムの各レベルで考慮すべきこととして整理され、設計すべき対象のガバナンス機能について、例えば救済や責任分担などは社会としてデザインされることが望ましいものとして整理されている。

また、ガバナンスとしてはアジャイル・ガバナンスをアプローチとして実現するよう整理している。

また、実際に実施するにあたっての具体的な規制方法やアプローチについては、実適用時に具体検討することとし、本ディスカッションペーパーでは取り扱わない。

5.1.2　アジャイル・ガバナンス

Society5.0 におけるガバナンスの在り方として、経済産業省によるアジャイル・ガバナンスの取組みがある。

ここでは以下のように述べられている。『Society5.0 では、我々の社会基盤となるサイバー・フィジカルシステム（CPS）が複雑かつ急速に変化し、予想困難かつ統制困難なものとなっていく。

このような社会をガバナンスしていくにあたっては、予め一定のルールや手順を設定しておくアプローチではなく、一定の終局目標 中核的価値 具体的目標「ゴール」をステークホルダで共有し、そのゴールに向けて、柔軟かつ臨機応変なガバナンスを行っていくようなアプローチが求められる。

しかし、この「ゴール」自体も、CPS の技術の発展やそれがもたらす社会状態の変動と共に常に変化しつづけるものであり、事前に一義的に定めることができない。

こうした社会の変化を踏まえると、Society5.0 のガバナンスモデルは、常に変化する環境とゴールを踏まえ、最適な解決策を見直し続けるものであることが必要である。そのためには、ゴールや手段が予め設定されている固定的なガバナンスモデルを適用することは、妥当ではないと考えられる。我々が目指すべき

は、様々な社会システムにおいて、「環境・リスク分析」「ゴール設定」「システムデザイン」「運用」「評価」「改善」といったサイクルを、マルチステークホルダーで継続的かつ高速に回転させていくガバナンスモデルであると考えられる。

このようなガバナンスモデルを、本報告書において「アジャイル・ガバナンス」と呼ぶ。これを図示すると、図 5.1.2 のようになる（以上は GAVERNANCE INNOVATION Ver.2 報告書から抜粋）』

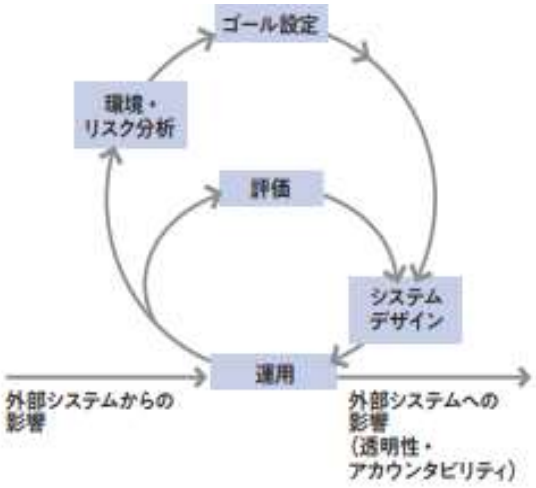


図 5.1.2　アジャイル・ガバナンス

5.1.3　システム側のリスク対応とガバナンスの対応

SoS は SoS 自身及び構成システムの安全リスクのマネジメントを行うだけでなく、それらが適切に実行され社会に受容されるために、どの様にガバナンスされるべきかステークホルダや規制当局と協力し、情報の非対称性もふまえて検討する必要がある。

ここではシステムのリスクについて、システム自体の構造（アーキテクチャ）の観点からのリスクと、システム運用（平時オペレーション）の観点からのリスクを列挙し、システムが一般的に取るリスク対応の手段について検討した。

また併せて、そのシステムにおいて不具合が発生した場合のオペレーションが適切になされないリスクも記載した。これは SoS が社会システムの一部として機能し、インフラとして位置付けられていく際に、社会に与える影響を抑えつつ継続的に改善していく上で必要なものとして設定した。

例えば通勤電車の運行におけるトラブルで、その復旧が出来ない場合は駅ホームに大量の人が溢れることで次なる危険に繋がることが想定される。そういった不具合発生時のリスクの連鎖を抑えることを考慮した。

この表において、システムの実施するリスク対応について記載しているものの、SoS 創発特性をふまえると、どの項目をどこまでの水準で対処すればシステムとしての責任を果たしたと認められるのか、定義することは難しい。

そのため、「ガバナンスの要求定義」として、ガバナンスがシステムに求める範囲についてステークホルダや規制当局と協議・合意すべきと考えられる事項の一案を図 5.1.3 に示した。

縦軸にシステムの安全に関して想定されるリスクを置き、横軸にシステム設計とガバナンス設計を置く。システム側でリスクへの対処を行うことを原則とするが、安全の徹底を図る上で、ガバナンス側での対応が求

められる場合がある。その際、ガバナンス側での対処はシステムに依存することも想定され、システム側とガバナンス側が連携してガバナンス要求事項を取り決め、その後のガバナンスアーキテクチャをガバナンス側で設計することを想定した。それぞれの行の隣り合ったセルにおいてシステムリスクとリスク対応、ガバナンス対応とが関係するものとして表記している。

「システムとステークホルダとでの検討事項」は「リスク評価とガバナンス対象の特定」から始める。システムの生み出すリスクを評価し、「システムが実施するリスク対応」のうち、何を必須事項として求められるのかを定義した上で、その対象項目の具体的な範囲・水準を検討することを想定した。

そこで定義した項目が実行されるために必要なガバナンス機能（体制構築や、インセンティブ・サンクションの設定、モニタリング等）と、実施手段（例えば認定認証制度、IT システム利用、市場原理など）についても設計される必要がある。ただし、この機能・実現手段には様々な選択肢が存在すること、また SoS が社会システムの中においてガバナンスされる想定であることから、一部機能は例示したものの具体的なガバナンス方法の設計は法学や経済学、規制当局などの専門家による検討の範囲とした。

「ガバナンスの要求定義」においては、「安全確保の仕様が特定される場合」（業界標準など拠り所にすべきものがある場合）と「安全確保の仕様が特定されない場合」（適用すべき標準などを特定できない場合や複数選択肢があり統制する必要がない場合）とに分けている。また併せて、事前に規制すべきものと、事後に規制すべきものに分けることもできる。これらの設定次第でリスク対応コストや参入障壁の高低などが変わるものの、システムに関する情報・知識が十分に共有されないことには適切な検討が難しいと考えられることから、システム提供側からも積極的な議論・働きかけを行うことが重要である。

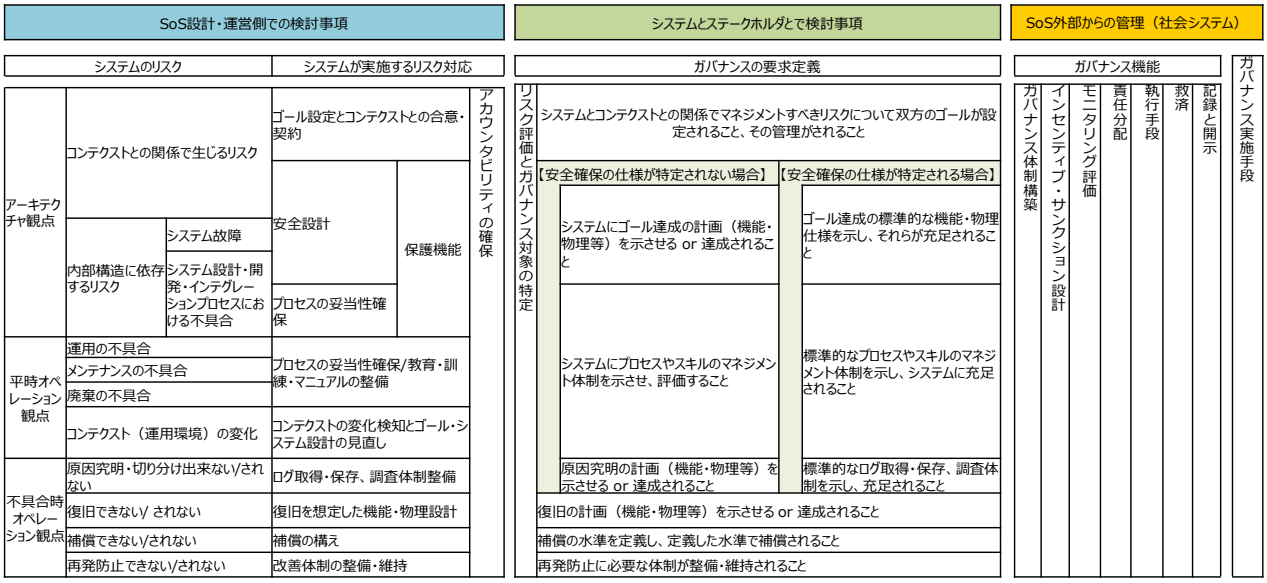


図 5.1.3　ガバナンスの要求定義

5.2 SoS-CPS のガバナンスの体制と機能の検討例

「はじめに」で安全サイドでは守りの視点「リスク回避」、そして開発・革新を実現していくために攻めの視点「リスク許容、の両にらみが設計の基本的なスタンスになる。そうした「攻め」と「守り」の形をどのように作るかということが、技術革新、技術開発競争が起きている時代の経営をする上でガバナンスの設計として重要である。とした。

また、事業者それぞれに分割された範囲で実現する価値しか提供しないシステムや製品であれば、モノづくりの不具合で事故が発生した場合の作り込みが、調達、開発・設計、製造、検査のいずれの部署に原因があっても対外的には、事業者等のそうした関連部署にモノづくりを要請している事業者のマネジメントの問題となる。その最終的な対応の責任は、そのオペレーションを行う経営陣にあるとされる。一方で、複数の事業者によるシステムが連携し CPS として機能していく SoS では、そのような考えに留まれなくなり、事業者を社会に置き換えた時にどのようにしていくべきなのか考えなければならなくなる。という問題意識を共有した。

ここでは、社会が実施するオペレーションの一つの具体例は、「攻め」と「守り」の形をどのように作るかのために、個々の事業者が行うオペレーションに求め、それが有効に機能するように管理するガバナンスであると考え、前述の「ガバナンスの要求定義」から以下の①～⑦について、これを実施するためのガバナンス機能と体制構築の一例を検討してみる。

① 「攻め」と「守り」の形をどのようにするか、すなわち、システムとコンテクストとの関係でマネジメントすべきリスクについて双方のゴールが設定され、合意することである。
② システムにゴール達成の計画（機能・物理等）を示し 達成される（安全の要求を満たして運用されていることを SoS としてモニタリングし示す）ようにする。
③ システムにプロセスやスキルのマネジメント体制を示させ、評価（安全の要求を満たして運用できるように相互運用条件や管理ルールを設定）し守られるようにする。
④ SoS では障害発生時に個システムでは対処（原因究明、再発防止など）できないことがあるので、障害が発生した時に障害の原因究明を実施できるようにする。
⑤ 障害からの復旧が出来るようにする。
⑥ 障害の再発防止を通じて安全性の改善を継続する。
⑦ 迅速な被害者救済の為の仕組みを持つ（⑦は社会システムとして整備されるものとし、ここでは検討範囲外にした）

5.2.1 SoS-CPSにおける安全のロール例

これを検討するために単純化したロール図を図 5.2.1 に示す。
このロール図はシステム提供する側のステークホルダの機能を整理するものである。

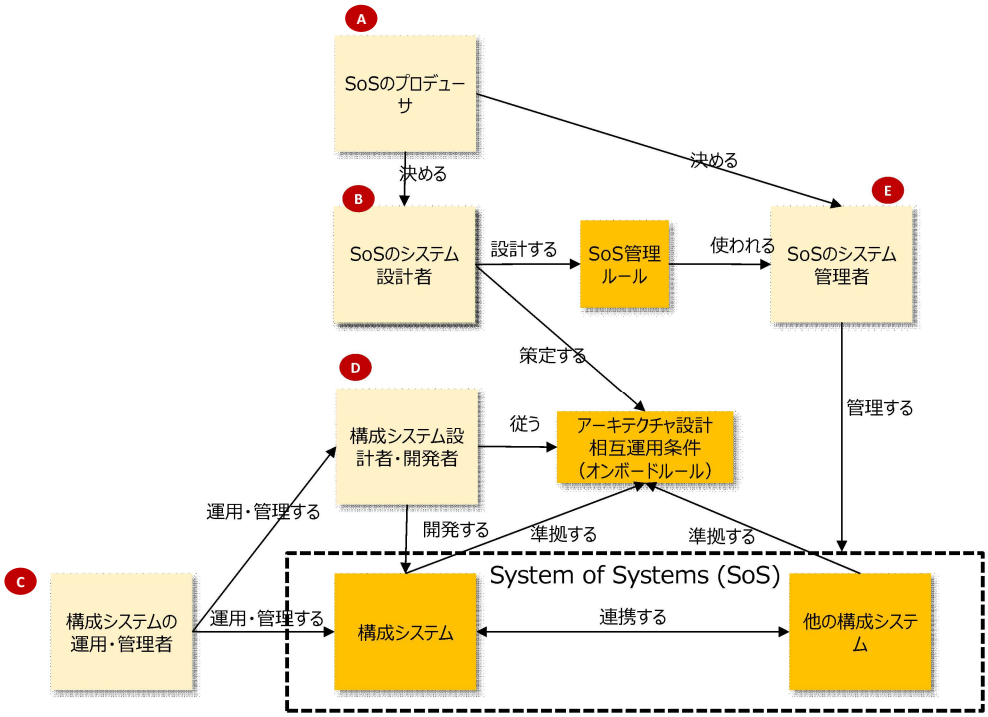


図 5.2.1　SoS における安全のロール例

また、各ステークホルダのロール内での機能を下記する。

1) SoS のプロデューサ A とは、ここではなんらかの目的をもって SoS を創造しようとする者という意味で使っている。例えば SoS をもって事業をしようとする主体者が居れば、もちろんこの者もプロデューサになり得る。
   SoS のプロデューサ A は SoS のシステム設計者 B と SoS のシステム管理者 C を決める。
   また、SoS の安全の要求について、規制省庁などの外部のステークホルダと合意し、これに基づく設計を SoS のシステム設計者 B に指示する。
2) SoS のシステム設計者 B は、SoS のアーキテクチャと管理ルールを設計し、これを公開する。
3) 構成システムの運用・管理者 C は SoS のアーキテクチャ設計を参照・理解し、自己の構成システムの設計者・開発者 D を指示・管理する。また。構築された構成システムを運用・管理する。
4) 構成システム設計者・開発者 D は SoS 全体アーキテクチャを理解しこれに従い構成システムを開発する。SoS の各構成システムは相互運用条件に則ることにより連携し機能を果たすことができるようになる。
5) SoS のシステム管理者 E は、複数の構成システムが連携し、SoS としての機能を果たす（ここでは安全を達成する）ための管理を実施する。

次に、管理者は複数の機能を持つので、判り易さの為に機能を細分化し例を図 5.2.2 に示す。

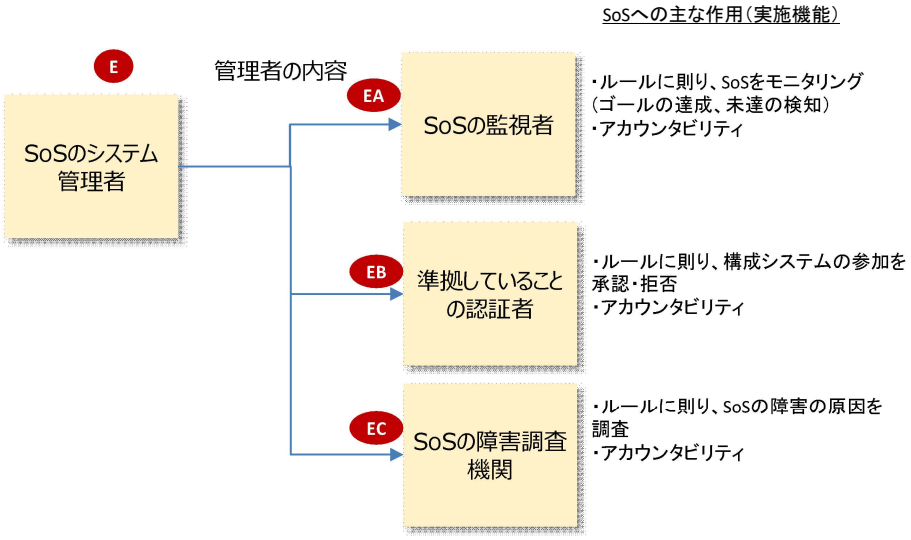


図 5.2.2　SoS における安全のロール例（管理者の実施機能の細分化）

SoS のシステム管理者は大きく３つの管理を実施する。

１） SoS の監視者

ルールに則り、SoS のモニタリングを実施し、SoS の環境変化の検知や、SoS の安全ゴール（許容されるリスクを守った運用）の達成や未達の検知をし、これの外部のステークホルダへのアカウンタビリティを果たす。

２） 準拠していることの承認者

構成システムの SoS への参加をルールに則り承認する、あるいは拒否する。

この実施について外部のステークホルダへのアカウンタビリティを実施する。

３）SoS の障害調査者

ルールに則り、SoS の障害の原因調査をする。その経過や結果について外部のステークホルダへのアカウンタビリティを実施する。

この管理機能は SoS 内の事業者や SoS 内で独立した管理者が実施するのか、社会レベルの体制で実施するのかのようなことは、SoS の社会への影響の大きさなどによって変わってくるので、4.1.3 で前述したようにガバナンス側とシステム側が議論して決めていくべきである。

5.2.2　システム側の対処機能のアロケーション検討例

前述のガバナンスの要求定義へのシステム側の対応について、システム側の対処を整理し、機能のアロケーション例を検討した。

これを表 5.2.1 に示す。SoS として設計されると思われるガバナンス機能について、これが正しく機能しているかをガバナンスする機能、①～⑤が必要になる。これは規制側で実施するなど SoS の外側から実施することが必要と考えられる。

① SoS 設計（安全達成の計画など）の妥当性の認証

SoS の設計において安全ゴールを達成するための計画、これを実現するための SoS のリスク想定や対処、検証などの設計妥当性及び適用される開発プロセスや管理のプロセスなど妥当性を認証する。また、障害からの復旧ができる設計、必要な記録が残るなど障害原因が究明できる設計になっていることもこの設計妥当性の中には含まれる。（構成システムの設計の認証についても同様であるが、本ディスカッションペーパーでは説明省略する）

② モニタリングの公正な実施を審査

運用中のモニタリングによる安全のゴール達成評価について、公正に実施されているかを審査する。

③ 準拠していることの認証が公正公平に実施されていることを審査

オンボードの可否の認証、これに問題がある場合に市場排除や改善指示をする判断が公正公平に実施されていることを審査する。

④ 障害原因の調査・究明が公正公平に実施されていることを審査

障害原因の調査・究明が公正に実施されているか、SoS の各構成システムにとって判断は公平か、を審査する。加えて、原因究明に至ったもの至らなかったものなど障害原因調査の達成の評価を実施する。

⑤ 復旧や再発防止の実施の評価

SoS の障害の再発防止についての実施体制整備・維持及び実績（対策済、未対策など）を評価する。また、SoS の復旧の実績（可否や復旧までの時間など）を評価する。

表 5.2.1 システム側対処機能のアロケーション例

ガバナンスの要求定義	No	対処のための機能や環境、ルール（案）	ガバナンスを実施する者(案)												
			A	B	①	C	D	EA	②	EB	③	EC	④	⑤
			SoSのプロデューサ	SoSのシステム設計者	SoS設計(安全達成の計画など)の妥当性を認証する者	構成システムの運用・管理者	構成システム設計者・開発者	SoSのシステム管理者（SoSの監視者）	モニタリングの公正な実施を審査	SoSのシステム管理者（準拠していることの認証者）	準拠していることの認証が公正公平なことを審査	SoSのシステム管理者（SoSの事故調査機関）	障害原因の調査・究明が公正公平に実施されていることを審査	復旧や再発防止の実施を評価する者
リスクとゴールが設定され管理がされること	1	安全ゴールを含む安全のSLAのステークホルダ合意	○											
	2	コンテクストの変化など環境変化を検知し見直す機能	○											
システムにゴール達成の計画（機能・物理等）を示させる or 達成されること ゴール達成の標準的な機能・物理仕様を示し、それらが充足されること システムにプロセスやスキルのマネジメント体制を示させ、評価すること 標準的なプロセスやスキルのマネジメント体制を示し、システムに充足されること	3	SoSの設計者の決定	○											
	4	SoSの管理者の決定	○											
	5	業界のガイドライン等の則るべき標準を合意する		○										
	6	SoSのシステム設計		○										
	7	SoSの管理ルールの設計(プロセスやスキルマネジメントを含む)		○										
	8	構成システムの設計者を選定し、構成システムの安全の要求を開示する機能				○								
	9	構成システムの設計					○							
	10	構成システムオンボード（SoS加入）可否の審査判断機能								○				
	11	SoSのシステム設計の審査機能			○									
	12	構成システムの設計の妥当性の開示機能					○							
	13	構成システムの安全要求の達成を開示する機能				○								
	14	モニタリングし安全の達成を事後審査する機能						○						
	15	モニタリングの公正公平な実施を審査する機能							○					
	16	安全のゴールが未達の場合に市場排除や改善指示の判断機能								○				
	17	オンボードの可否審査、市場排除や改善指示の判断が公正公平に実施されていることを審査する機能									○			
障害の原因究明の計画（機能・物理等）を示させる or 達成されること 標準的なログ取得・保存、調査体制を示し、充足されること	18	SoSの障害発生時の原因調査できるようにする（調査用情報収集、調査など）設計		○										
	19	SoSの障害原因の調査・究明する機能										○		
	20	SoSの障害原因についての再発防止箇所を決め、対処を要請する機能		○										
	21	SoSの障害原因の調査・究明が公正公平に実施されていることを審査する機能											○	
	22	SoSの障害調査及びUnknown検知について説明責任を果たす機能										○		
	23	SoSの障害原因調査の実績を評価する機能											○	
復旧の計画（機能・物理等）を示させる or 達成されること	24	SoSの障害発生時の復旧のための設計		○										
	25	SoSの復旧の実績（可否や復旧までの時間など）を評価する機能												○
再発防止に必要な体制が整備・維持されること	26	SoSの障害が再発防止なされるようにする設計		○										
	27	SoSの障害の再発防止についての実施体制整備・維持及び実績（対策済、未対策など）を評価する機能												○

5.2.3　コラム　『SoSにおけるに安全に関するロール(想定例)』

図 5.2.3 に SoS における安全に関するロールについて、一例を想定検討した。

例えば「路側機器による自動運転支援の SoS を作る」と言うような、何の為の SoS を作るのか具体的に〇〇を実現しろと言い出すのが SoS のプロデューサ A。プロデューサ A はこの SoS が達成すべき安全のゴール（許容できるリスク）を規制官庁などステークホルダと合意して示す。

SoS の設計者 B はこれを受けて SoS のアーキテクチャを設計し、SoS の内部のステークホルダに開示する。この設計には例えば、構成システム間のインタフェースや安全にオンボードできるようにするオンボード時の検証ルールなどのような相互運用条件などの技術的設計事項の他、これに適用すべき開発プロセスなども含まれる必要がある。また、これに合わせて SoS を正しく機能させ維持するために SoS の管理ルールも設計される必要がある。

構成システム設計者・開発者 D は SoS のアーキテクチャ設計に従い構成システムを設計開発する。構成システム運用・管理者 C は SoS のアーキテクチャ特に相互運用条件に準拠し運用管理し、他の構成システムと連携することで SoS を構成する

SoS のシステム管理者 E は SoS の管理ルールに則り SoS のモニタリング（特に安全のゴールの達成・未達成）を実施し、SoS が安全のゴールを達成しながら運用されていることの評価とアカウンタビリティを実施する。また、SoS を構成する構成システムが SoS のアーキテクチャに則り開発運用されていることを認証し、オンボードの許可拒否をする。障害や障害予兆の発生時にはこの原因究明と再発防止要否及び責任所在(分担)の判断を実施する。

また、SoS の管理ルール設計にあたっては、迅速に実施済みの被害者救済や再発防止の為の費用などについて、明らかになった責任所在により清算されるなどの仕組みも必要になっていくと推定している。

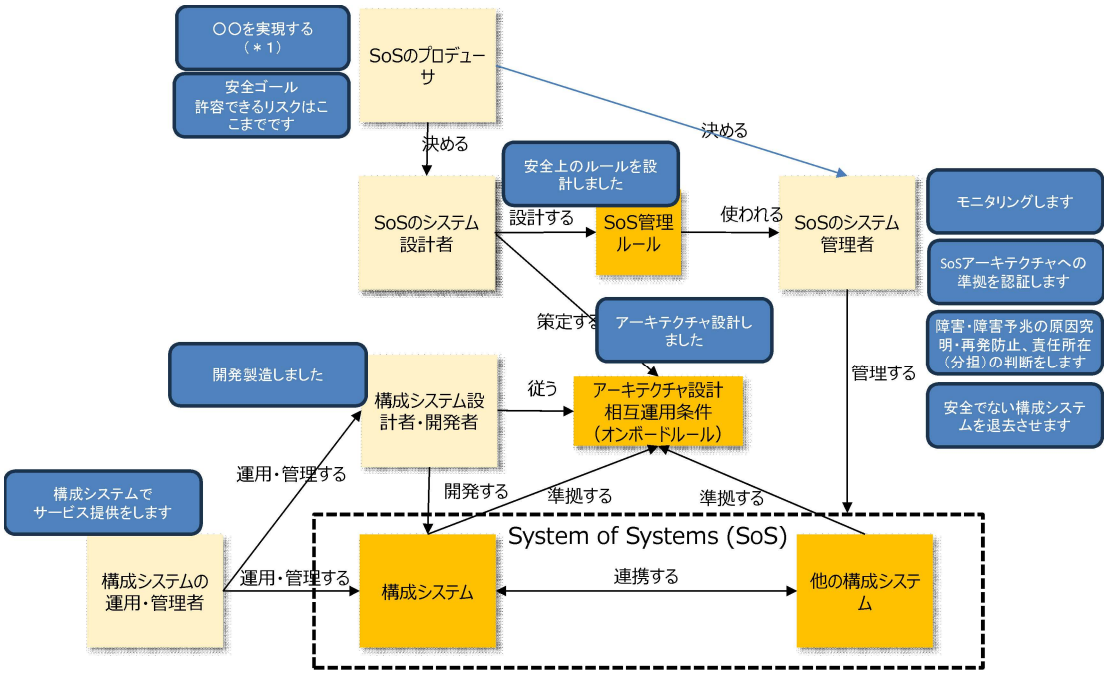


図 5.2.3　SoS における安全のロール図（利用想定例）

6　あとがき

本ディスカッションペーパーは、SoS とその構成システムにおいて、安全性をどのように作って行くか、検討・整理してきたものである。

安全性確保のために、全てのリスクを想定し、これに対処していくことが一般的であり、従来はこの考え方により安全設計を行ってきた。一方で、近年著しく技術進歩した OSS 、クラウド、AI など安全設計されていない構成要素を使わずにシステムを構築すると、技術進歩に付随するイノベーションを迅速に実現することを否定してしまう可能性、またサイバー空間を介してフィジカル空間を結び実現される人間中心社会の取組みを否定してしまう可能性、さらに経済成長の取組みを否定してしまう可能性がある。管理と運用が独立した複数のシステムが連携し機能し、かつ安全性を継続的に実現していくためにどうすべきか、今後、議論が必要となる。

本ディスカッションペーパーでは SoS とその構成システムの安全の要求を満たす設計やガバナンスについて検討してきた。安全設計については保守的な設計の中ではどうしてそのようにしているのかの設計思想もできるだけ記載するようにした。安全の要求を満たす設計を検討する時に参考にしていただければ幸いである。ガバナンスについては検討が「WHAT：何を設計すべきか？」止まりであり、「HOW：どうやって実現するか？」を十分に議論するところまでには至らなかったので、具体事例でのさらなる検討が必要と考えている。

はじめにで記載した通り。Society5.0 の実現に向け継続的にディスカッションされることを期待し、たたき台として資することを期待し、現時点の議論で作成した本ディスカッションペーパーを公開したものである。

2025 年 3 月末日