MITSUBISHI ELECTRIC
Changes for the Better

機能安全とサイバーセキュリティ規格の動向

The current status of functional safety and cyber security

三菱電機　神余浩夫

Mitsubishi Electric Co. Hiroo Kanamaru

ねらい・目的

■ 講義の狙い

- 組込みシステム・制御システムの高度化・複雑化
  - 故障，不具合，ヒューマンエラーや脅威による，事故・事件のリスクが無視できなくなってきた
  - 火災，爆発，衝突，設備破損，労災，操業停止，情報漏洩…
- 安全性とセキュリティの確保が新たな課題に
  - より安全，セキュアではなく，リスクアセスメントによる十分性の説明
  - 安全性とセキュリティの両立

■ 達成目標

- 汎用規格としての機能安全とサイバーセキュリティ規格の状況を学び，自動車を含む技術動向を推察できるようになる．

■ 対象者

- 自動車分野等の機能安全またはサイバーセキュリティの基本知識を有する

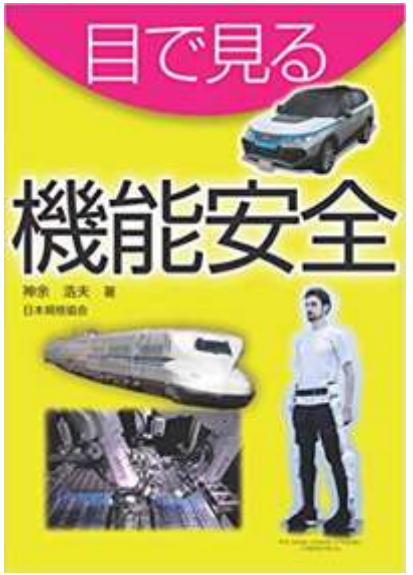
講師紹介

神余　浩夫(かなまる　ひろお)

1987　大阪大学大学院工学研究科原子力工学修士課程修了
三菱電機(株)中央研究所　入社
プラント制御システム，制御ネットワーク，高信頼システム，安全システムなどの研究・開発

2004　三菱電機(株)名古屋製作所
安全シーケンサ，安全フィールドネットワークの開発

2011　三菱電機(株)先端技術総合研究所
機能安全システム，制御システムセキュリティの研究・開発，国際標準化，人材育成
- TUV認定機能安全エキスパート(FSexp)
- IEC 61508, IEC 62443他国際エキスパート
- SICE, ISA他学会



目次

- 制御システムが抱える問題
- IEC 61508 機能安全
- IEC 62443 サイバーセキュリティ
- IEC TR 63069 機能安全とサイバーセキュリティの両立
- まとめ

制御システムが抱える問題

IoT時代の制御システム

■ IoTにより，多様な設備・システムが，人と事業者が繋がる

INFOPRISMの活用イメージ
http://www.mitsubishielectric.co.jp/news/2017/1107-a.html

制御システムの複雑化

- 1990年ごろまで
  - 各社の独自技術(クローズド技術)で作られていた
- 2000年から，最新コンピュータ技術(IT)の活用が進む
  - 汎用オペレーティングシステム(OS)，市販アプリの利用
  - インターネットワークとの接続、汎用ネットワークプロトコルの採用
  - フリーソフトウェア、オープンソース
  - 使い易さ、機能・性能、開発期間の短縮、コストダウン
- ソフトウェアの複雑化
  - 試験・評価の工数
  - 想定システムの組合せ数
  - ソフトウェアの品質
- 安全性，セキュリティ対策

ECUの搭載イメージ
[(財)日本自動車研究所 http://www.jari.or.jp/research-project/research-department/its/iso26262/]

制御ソフトウェアの安全・安心

■ 制御ソフトウェアの不具合

- 火災、爆発、衝突、墜落などの人命事故
- 停電、断水、運休、操業停止などの社会サービス停止

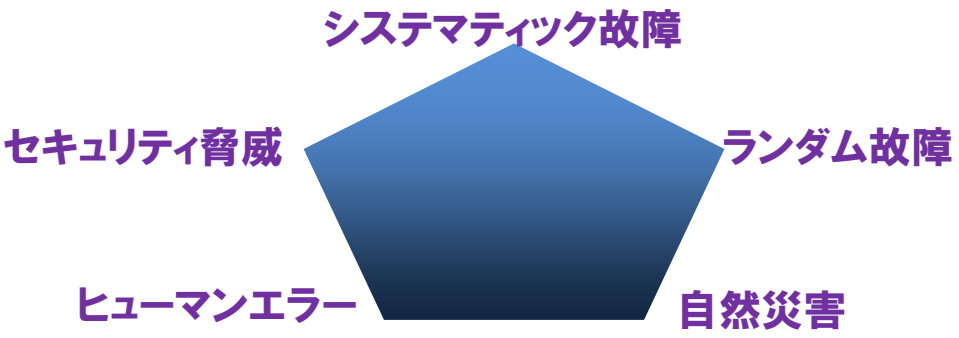
■ 制御ソフトウェアの安全・安心の保証とは？

- 対象の機械・設備はどれくらい危ない（リスク）があるのか
  - リスク=事故・事件による損害と確率（発生と回避）の関数
- リスク回避・低減のための対策を設計
  - 対策機能、時間性能、開発プロセス、故障率など
  - 設計漏れ、検討漏れ、評価漏れがないこと=トレーサビリティ
- 要求基準を国際標準化，
  規格適合性評価

自動運転事故車両
Public Domain

リスクとは

- **リスク（risk）【ISO 31000 2.1】**
  - 目的に対する不確かさの影響
  - ポジティブ，ネガティブ（安全，セキュリティではネガティブのみ扱う）
- **リスク源（risk source）【ISO 31000 2.16】**
  - それ自体又はほかとの組合せによって，リスクを生じさせる力を本来潜在的にもっている要素
- **リスク評価（risk evaluation）【ISO 31000 2.24】**
  - リスク及び／又はその大きさが，受容可能か又は許容可能かを決定するために，リスク分析の結果をリスク基準と比較するプロセス。
- **リスク対応（risk treatment）【ISO 31000 2.25】**
  - リスクを修正するプロセス。



リスク源の種類（著者オリジナル）

つながる時代の新たなリスク

- **想定しないつながりが発生する**
  - 携帯機器、家電、自動車、社会インフラなど、思いもしないつながり
- **管理されていないモノもつながる**
  - 古い機器、廃棄・中古品、ユーザ責任で追加されたモノ
- **身体や財産への危害がつながりにより波及する**
  - 特に、身体・生命・財産にへの「危害」には対策が必要
- **問題が発生してもユーザにはわかりにくい**
  - 機器が感染・故障してもすぐに被害発生しない

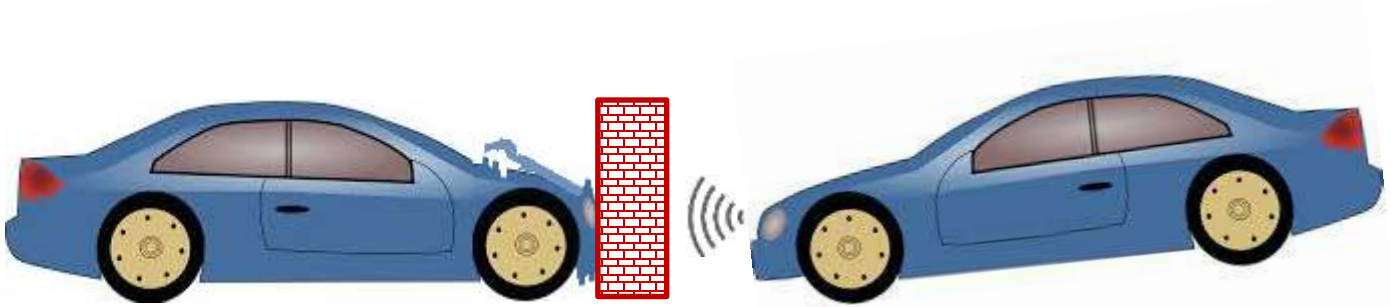
「つながる時代の開発指針」(IPA, 2016) より

MITSUBISHI ELECTRIC
Changes for the Better

IEC 61508 機能安全

機能安全とは

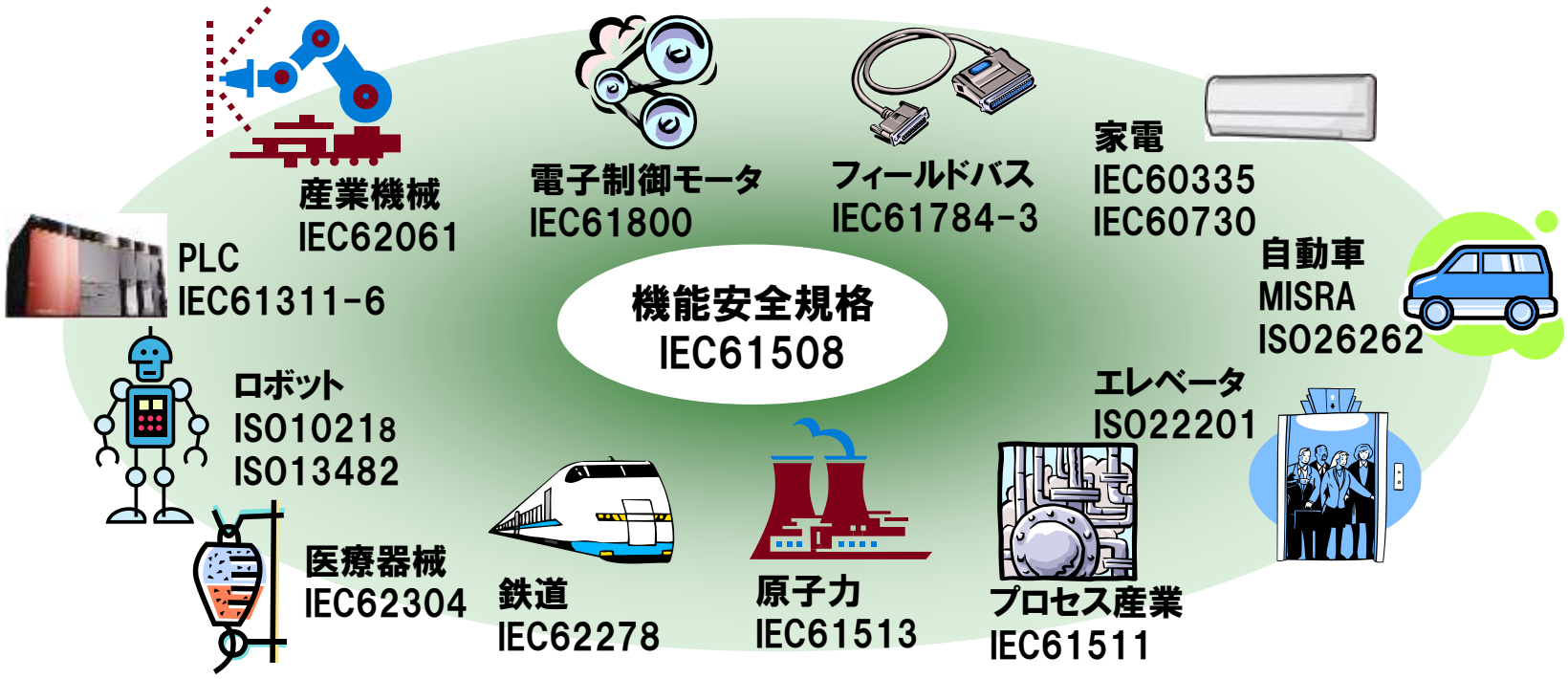
- フェールセーフ（然故障性）、フォールトアボイダンス（避故障性）
  - 故障が起きても大丈夫、危険にならない
  - そもそも故障が起きない、起きにくい
- 機能安全（Functional Safety）
  - 機能で安全を担保する（安全機能）
  - 安全制御システム＝危険を検知すれば安全状態に移行する
  - 自動ブレーキ、自動消火装置、速度超過監視、etc
- 安全制御システム
  - コンパクト（回路のソフトウェア化）、工数削減
  - きめ細かい安全制御ができる、複雑高度な安全対策が可能に



（著者オリジナル）

IEC 61508機能安全

- かつて、安全回路はハードウェア（機械的）のみで実現
  - マイコン、ソフトウェアに命を預けられない
  - 1990年代。IT技術の進歩、信頼性技術の確立
- IEC61508機能安全規格（1999, 2010, 202x）
  - 初めてのマイコン、ソフトウェアを用いた安全制御システムに対する要求事項と標準技術を規定



（著者オリジナル）

SIL(ASIL)

■ 安全機能 (Safety function) の要求レベル

- リスクアセスメントに基づく安全機能の性能要求，達成要求
- 安全機能を構築するコンポーネントの安全能力
  - SIL 1～4(IEC61508, IEC61511)
  - ASIL a～e (ISO 26262) , PL a～e (ISO 13849-1)

■ より高いSILを目指す…必要はない

- ギリギリ安全→コスト，操作性，性能などとのバランス

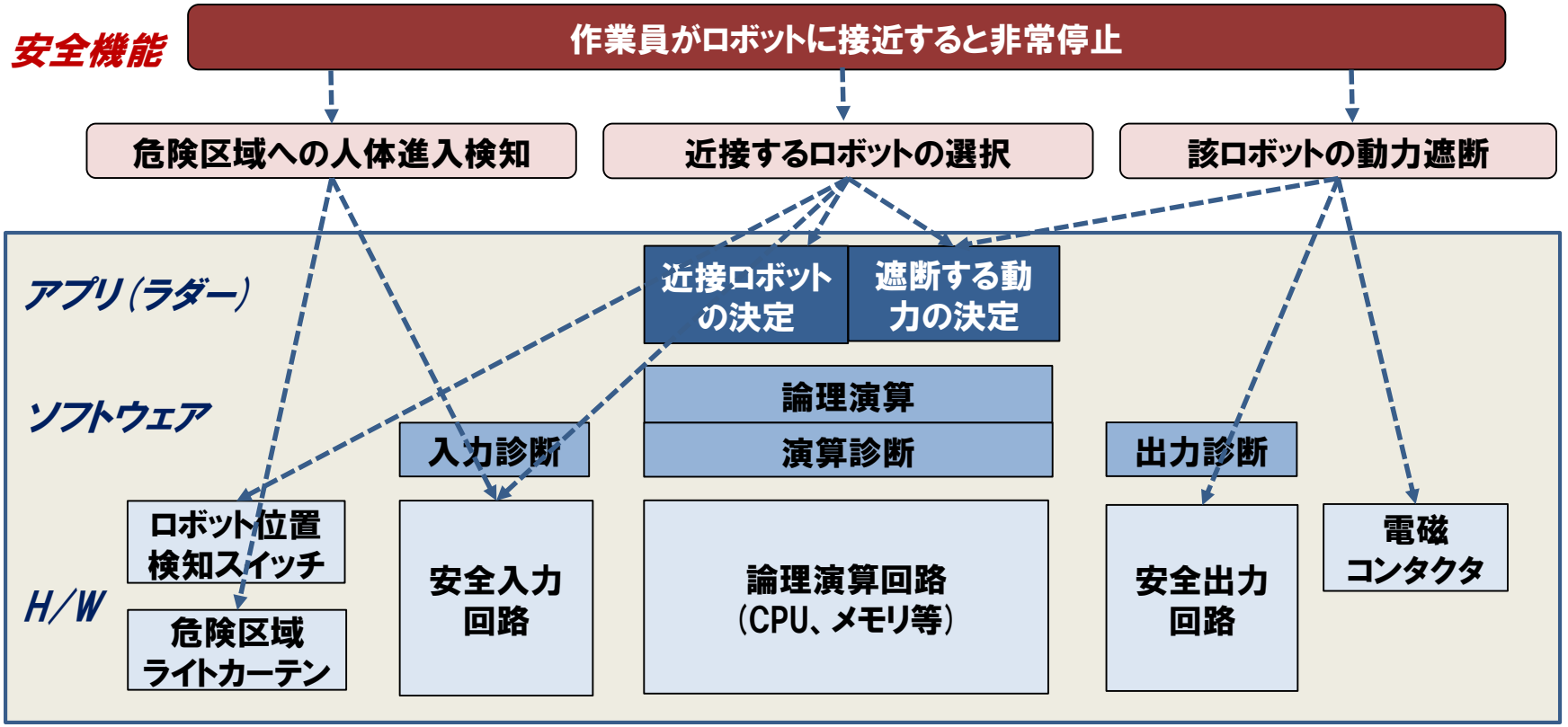
自動車機能のASIL相場感 (著者オリジナル)

ASIL A	ASIL B	ASIL C	ASIL C	ASIL D
				Airbag
	Active suspension			Power steering
	Radar cruse control		Engine management	
	Vision cluster			

機能安全の実現

■ 安全機能の分割とマッピング

- 安全機能をサブ機能に分割し、(アプリ)、ソフトウェア、ハードウェアに割り付ける。
  - 診断回路、多重化およびSIL適合機能も忘れずに



(著者オリジナル)

IEC 61508 Ed.3の議論

■ Ed.2 (2010) から10年ぶりの改訂

- **新技術の採用，要求の詳細化**
  - 用語・定義の見直し
  - サイバーセキュリティ (IEC 62443との棲み分け)
  - オフラインツールへの要求詳細化
  - プロセッサ/ASICの安全機能やマルチコア要求→Annex
  - オブジェクト指向プログラミング→Annex
  - データドリブンシステム
  - AIと機能安全→ISO TR 5469準備中
  - ヒューマンファクタ
  - 診断機能コンポーネント
  - 要員の役割，能力
  - 認証制度との連携→IEC/CAB/IECEE/CMC/WG32 機能安全
- **WD準備中→NP投票 (夏?)**

AIと機能安全

■ ISO/IEC/JTC1/SC42/WG3 (Trustworthiness of AI)

- ISO/IEC 25059 Software engineering - SQuaRE
- ISO/IEC 23849 Risk management
- ISO/IEC TR 5469 Functional safety and AI systems
  - AI技術の用途と安全性から要求レベルを規程
  - システム(アプリ), ツール, 学習データへの安全要求
  - SC42/WG3とIEC61508の共同チームにより, NP準備中

AI安全性の分類の提案例(著者オリジナル)

AI Technology Class Usage Level	Class I	Class II	Class III
Usage Level A	application of existing functional safety standards possible	limited	**Not recommended application**
Usage Level B		limited	limited
Usage Level C		limited	limited
Usage Level D	No specific functional safety requirements for AI, but safety precautions need investigation.		

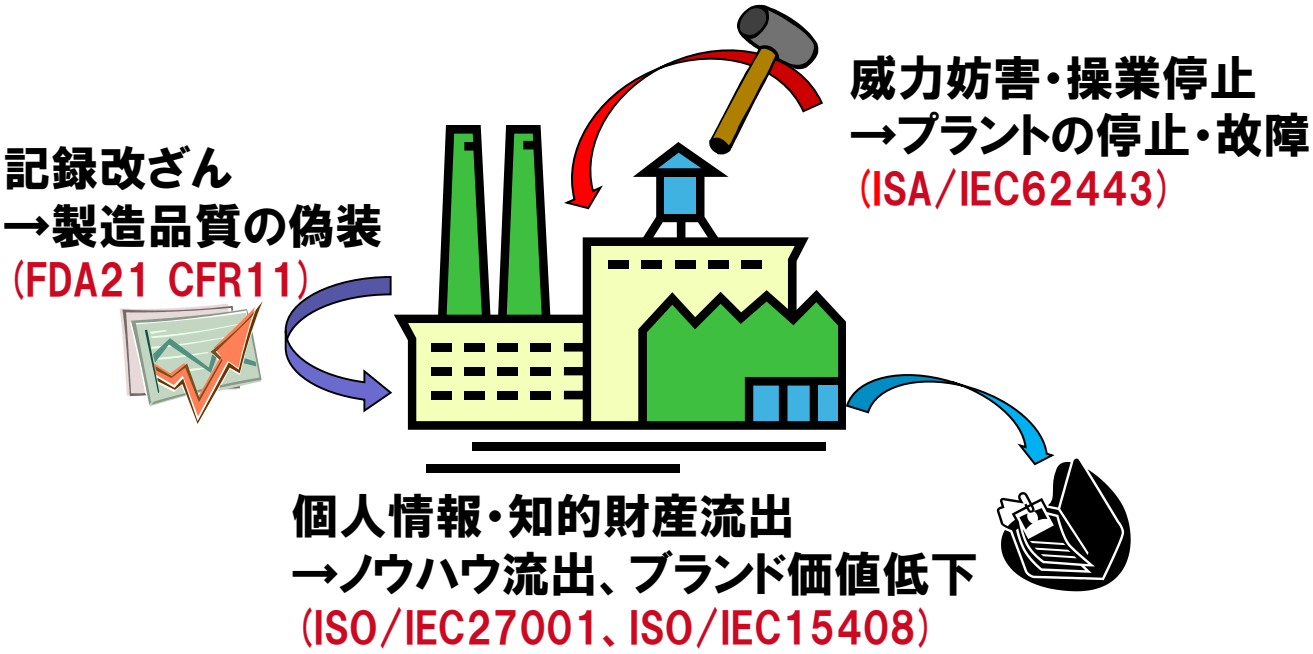
MITSUBISHI ELECTRIC
Changes for the Better

IEC 62443 サイバーセキュリティ

制御システムのセキュリティ

■ 工場・プラントのセキュリティ

- 個人情報・知的財産の流出→情報セキュリティによる対策
- 製造品質記録の改ざん（医薬食品）→電子署名・バリデーション
- 威力妨害・操業停止→制御セキュリティ規格
  - 社会インフラの場合、情報漏洩よりも事故や操業停止のほうが、社会的影響が大きい
    →情報セキュリティとはリスク分析が異なる



（著者オリジナル）

4.2 情報セキュリティと制御セキュリティ

■ 制御システムの特徴

- 10年以上使用される＝数年で入れ替えできない
- 簡単にリブートできない、止められない＝セキュリティパッチ？
- 組み込みソフトウェアを更新できないことが多い
- 機械設備の運転員・保全員は、セキュリティをよく知らない

■ 守るべき対象と目的が異なる

- 情報セキュリティ
  - プライバシー情報、企業秘密、金融データetc.
  - 情報漏洩、盗聴、改ざん、データ破壊
- 制御セキュリティ
  - 制御システムプログラム、アラーム情報、プロセス入出力etc.
  - プログラム/パラメータ書換、リモート操作、サービスダウン

（著者オリジナル）

制御セキュリティ規格

■ 国際自動制御学会 (ISA)

- 2002年10月、ISA S99制御システムセキュリティ委員会発足

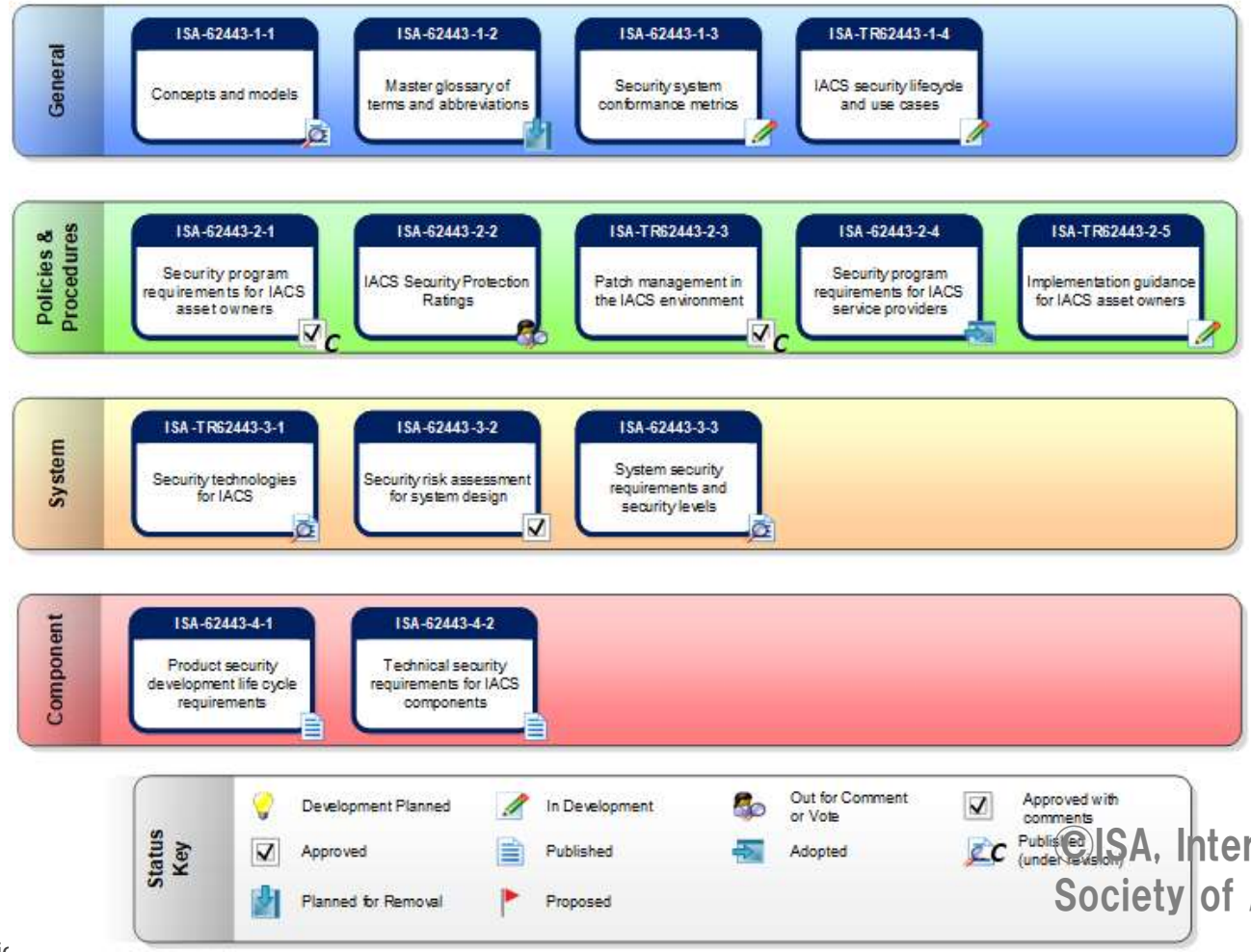
■ IEC/ISA 62443　制御システムセキュリティ規格

一般

ポリシー

システム

コンポーネント



制御セキュリティ規格の最新状況

- IEC 62443（TC65/WG10）
  - TF roadmap
    - ACSECから制御セキュリティの水平規格作成の検討指示
  - PNW TS 65-827　Rules for IEC 62443 Profiles
    - 産業分野規格を作成するための指針
  - PNW TS 65-828
    - Security evaluation methodology for IEC 62443 – Part 2-4: Security program requirements for IACS service providers
    - Maturity Levelの評価基準
  - PNW TS 65-829
    - Security evaluation methodology for IEC 62443 – Part 4-2: Technical security requirements for IACS components
    - 制御機器のセキュリティ機能の評価基準
- IEC/CAB/IECEECMC/WG 31 Cyber Security
  - OD-2061 IEC 62443に基づくセキュリティ認証制度

自動車分野のセキュリティ

UNECE WP29 GRVAサイバーセキュリティ法

- 国連欧州経済委員　自動車基準調和世界フォーラム
- 自動車のサイバーセキュリティとソフトウェアアップデートに関する国際基準（2020年6月）
  - 開発組織への要求（CSMS），S/W機能要求

ISO/TC22/SC32

- WG8　Functional safety
  - ISO 26262 Functional safety, ISO 21448 SOTIF
- WG11 Cyber security
  - ISO TS 5112 Guidelines for auditing cybersecurity engineering
- WG12 Software update
  - ISO 24089 Software update engineering
  - ISO 21434 Cybersecurity engineering
- WG13 Safety and cybersecurity for automated road vehicles
  - ISO TS 5083 Design, V&V

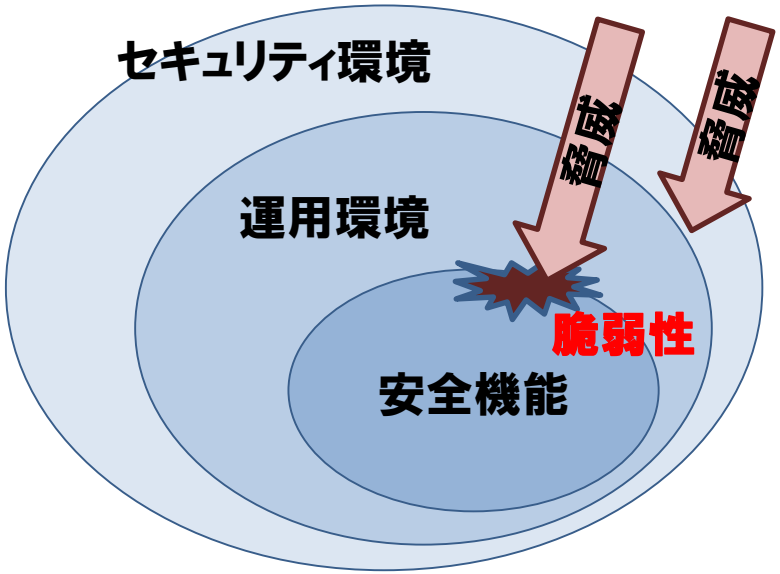
MITSUBISHI ELECTRIC
Changes for the Better

IEC TR 63069 機能安全とサイバーセキュリティの両立

制御システムの抱えるリスク

■ 安全とセキュリティの要求

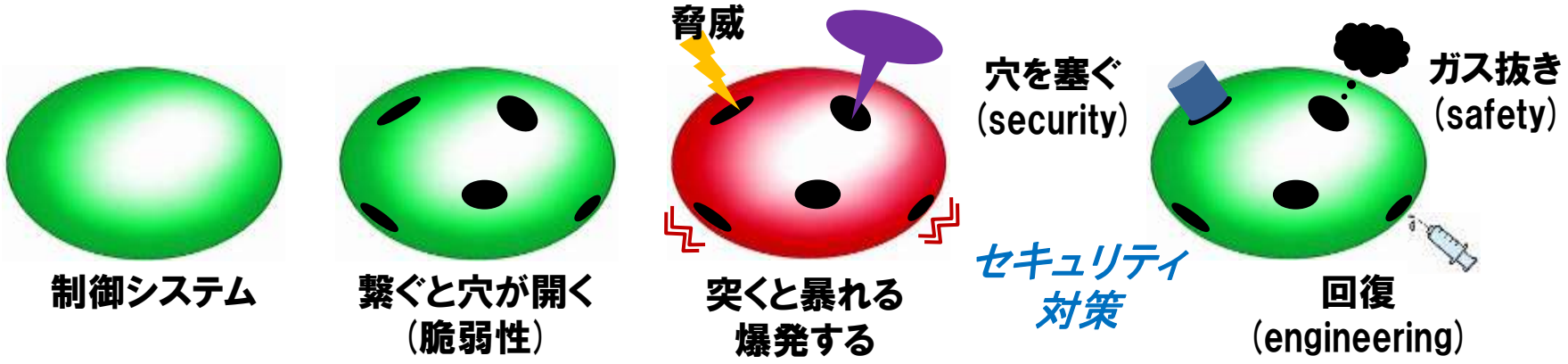
- 制御システムに起きる事象を想定し，対策
  - 自然災害，機械の故障，ヒューマンエラー，サイバー攻撃など
- セキュリティ脅威による被害（事故）の発生
  - システム外からの脅威が，セキュリティ環境（対策含む），運用環境の脆弱性を通り抜けて，安全機能を無効化あるいは劣化させる
  - 安全機能の喪失＝事故リスクが高まる
- 制御システムの安全とセキュリティの両立



IEC TR 63069より

セキュリティ対策と安全対策

- **機能安全はセキュリティ脅威に晒される**
  - 攻撃を受けた場合，人身事故リスク大
- **制御システムのリスクアセスメントと対策**
  - 脅威が脆弱性をつつくと，被害（事故）が発生
  - リスク低減対策
    - ITセキュリティ：脆弱性を塞ぐ，脅威シナリオ確率を下げる
    - セーフティ：被害規模（爆発，破損，傷害等）を抑制
    - エンジニアリング：迅速に正常操業に回復
  - セキュリティとセーフティは密に結合

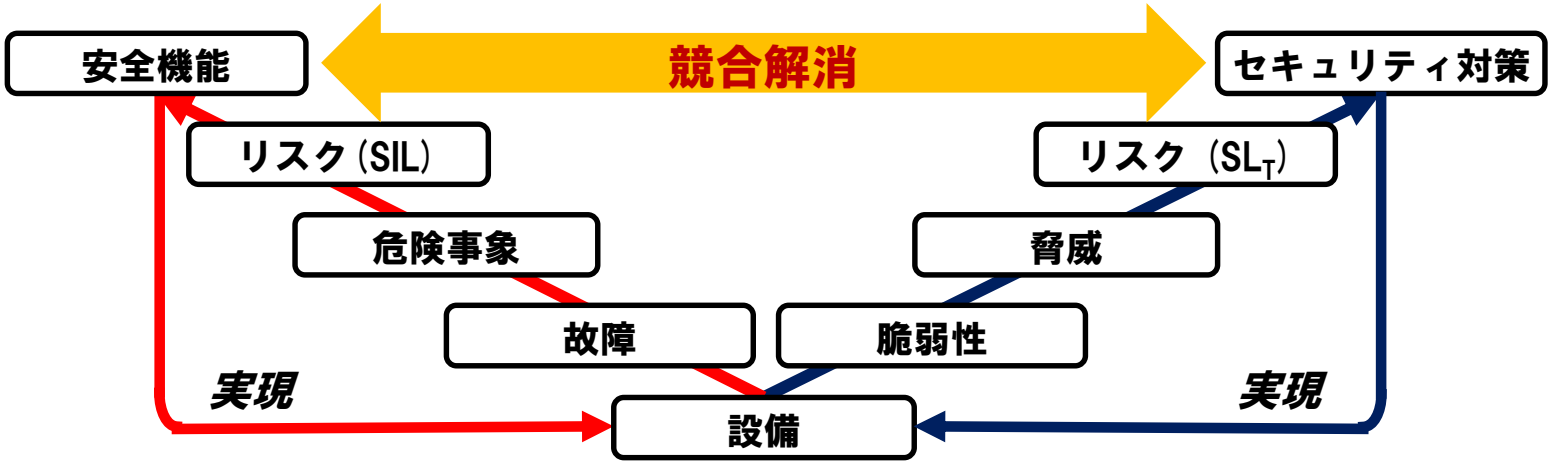


著者オリジナル

機能安全と制御セキュリティの両立

■ 機能安全と制御セキュリティの共通点と差異

- **似ているが差異も多い**
  - 安全リスク分析とセキュリティリスク分析は視点が違う
  - 長年使い込んだソフトウェアは安全とみなされる（Proven in Use）が，セキュリティ的には脆弱性になる．セキュリティパッチは安全か？
- **同じ製品・システムが、両方に適合しなければならない**
  - 規格に矛盾、競合があってはならない
  - ふたつの開発プロセスが業務規程（ISO 9001）に展開できるか

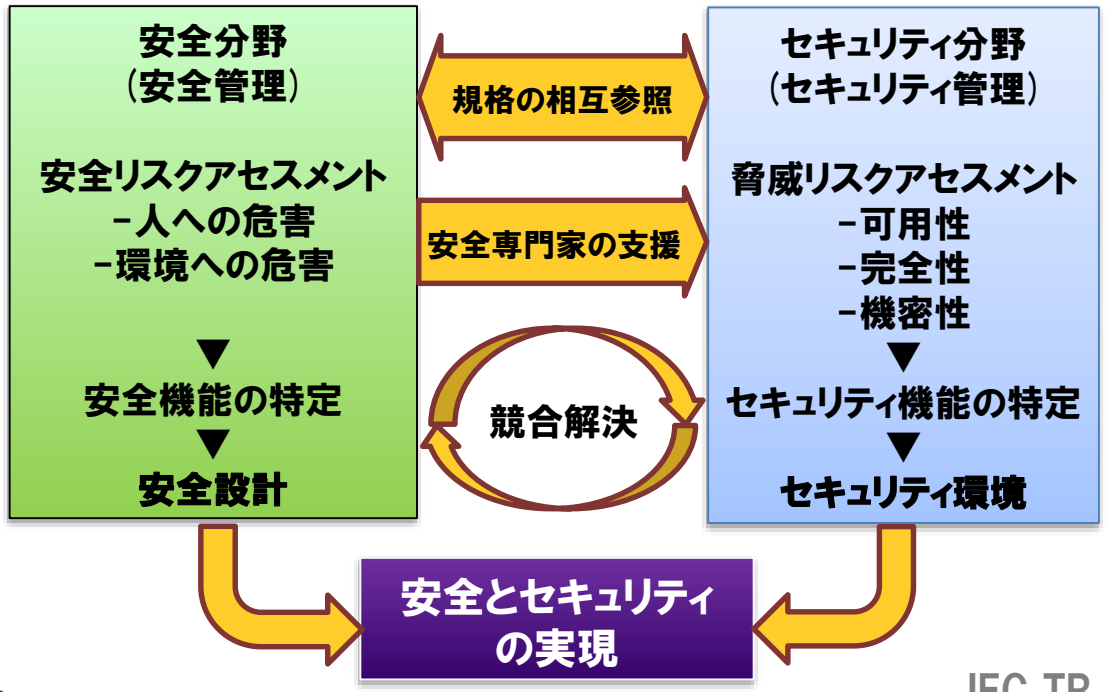


著者オリジナル

安全・セキュリティシステム設計手順

■ IEC TR 63069 機能安全とセキュリティの連携フレームワーク

- 安全とセキュリティふたつの分野について，並列に分析・設計
- 両者が規格 (IEC 61508, IEC 62443) に基づいて分析
- 両者間の競合
  - 実現方法，性能，構成，運用方法など
  - システム仕様として統合，実現

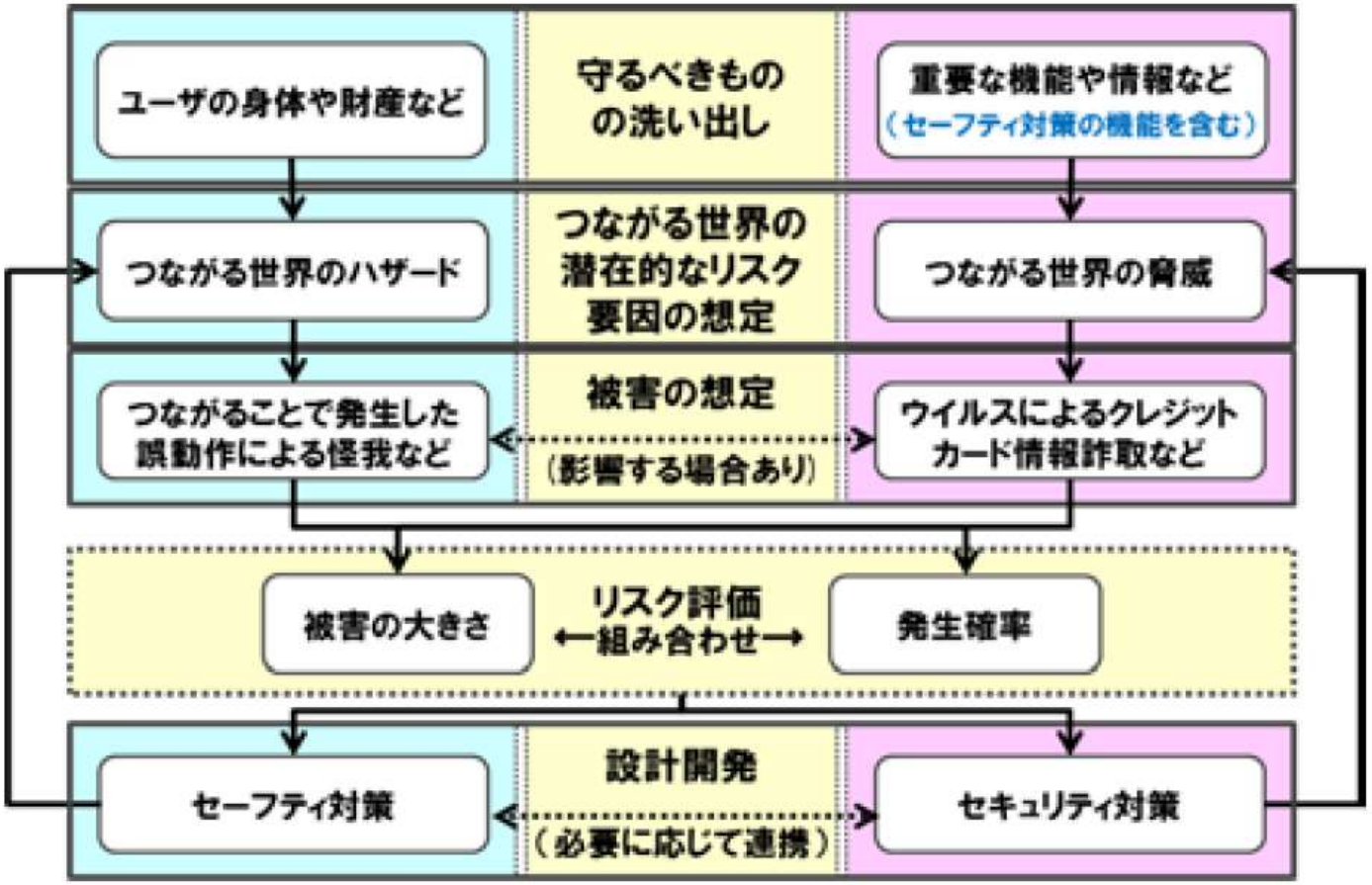


IEC TR 63069より

5.5 リスク分析の手順

■ つながる世界のセーフティ、セキュリティのリスク分析と対策

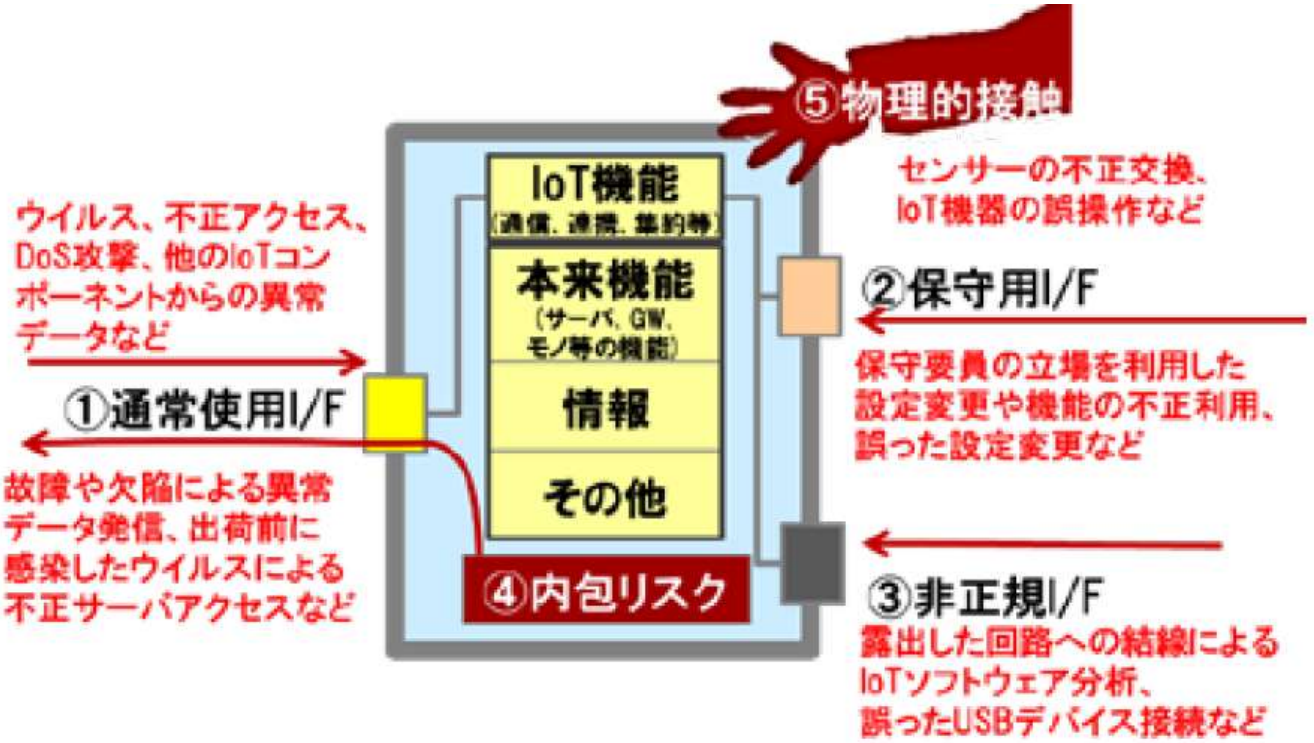
- 大きなリスク（被害大かつ高確率）を見逃さない
- セーフティ対策とセキュリティ対策のバランス



つながる世界のハザードと脅威の想定、リスク分析及び対策
（IPA「つながる世界の開発指針」より）

■ リスク個所の整理と脅威・ハザード分析

- IoTコンポーネントの「守るべきもの」に対して、脅威やハザードを想定するとともに、どの場所で発生しうるかを整理した。
- 想定した脅威やハザードが発生しうる箇所（リスク箇所）と、リスク箇所に想定される脅威やハザードの例。



IoTコンポーネントに対する脅威やハザードの例
（IPA「つながる世界の開発指針」より）

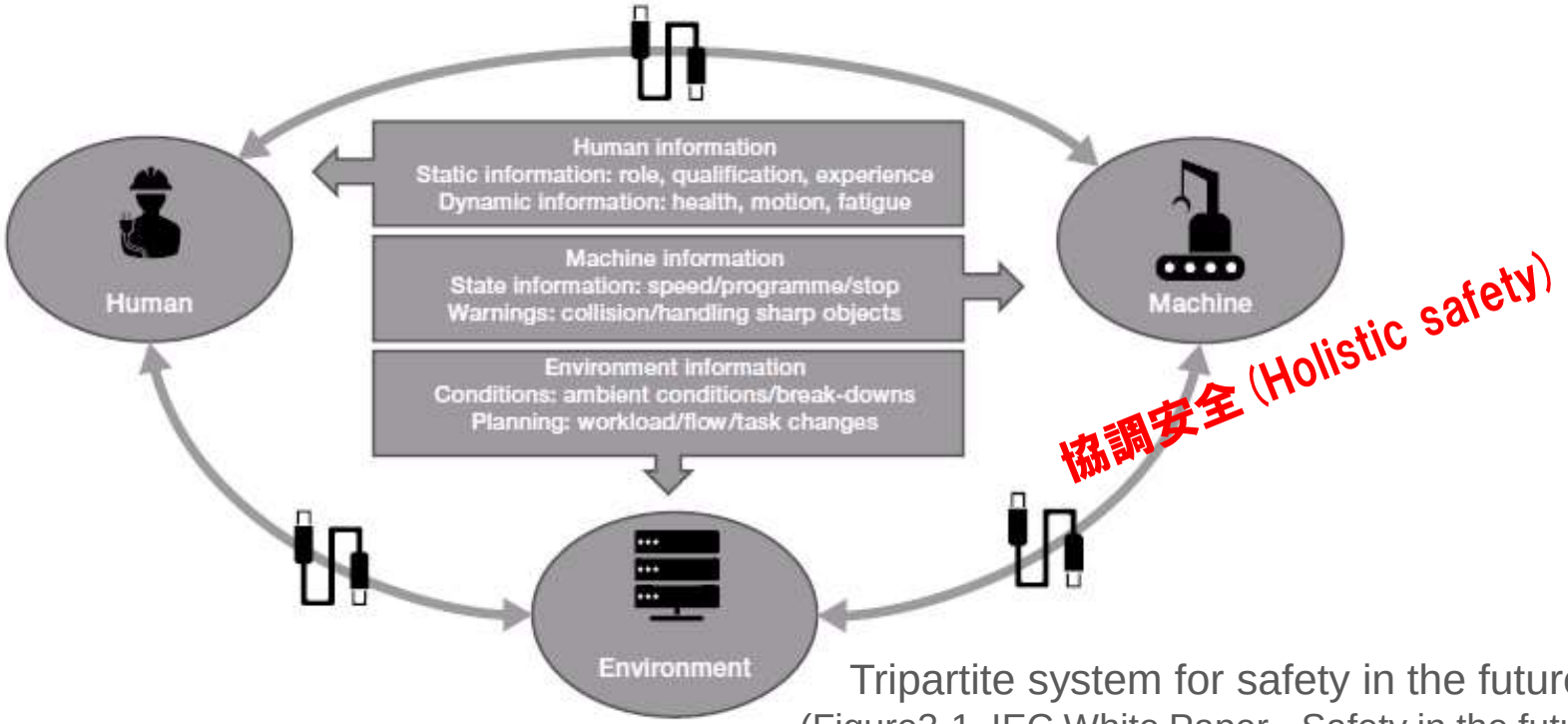
まとめ

まとめ

- **複雑高度化する制御システム**
  - セーフティ，セキュリティ確保が新たな課題
- **IEC 61508 機能安全**
  - ソフトウェアによる安全機能の実現，SIL要求，開発プロセス要求
  - Ed.3改訂提案=2021年，AIと機能安全
- **IEC 62443 サイバーセキュリティ**
  - 制御システムのセキュリティ対策，リスク分析，SL要求
  - 13/15編発行，3編追加，水平規格化
- **IEC TR 63069　安全とセキュリティの両立**
  - 制御システムのリスク分析，安全/セキュリティ対策の両立
  - 新規提案（改訂?）=2021年
- **自動車（全体）の安全とセキュリティの両立**
  - ISO TS 5083 Safety and cybersecurity for automated driving

IEC白書 Safety in the Future

- **IEC白書（市場戦略評議会MSBが発行）**
  - IECが今後注力する技術分野の調査報告
- **Safety in the future: 2020/11月**
  - 自動運転、協働ロボットなど新技術分野の安全概念の提言
  - 人、機械、組織の連携による三位一体アプローチ
  - 標準、規格適合性、教育制度の整備



Tripartite system for safety in the future
(Figure3-1, IEC White Paper - Safety in the future)