MITSUBISHI ELECTRIC
Changes for the Better

情報通信技術等を利用した生産システムにおける人の安全確保を実現するための調査研究

三菱電機株式会社　神余浩夫

MITSUBISHI ELECTRIC CORPORATION

0　はじめに、目次

■はじめに

- ICT等の新技術の導入は、生産システムの安全性確保に関する新たな課題・脅威を持ち込んだ。事故や事件の防止・抑制に向けた調査研究が急がれる。
- 生産システムのセキュリティリスクアセスメント調査、実施方法ガイドの策定。
- 本発表は、（一社）日本機械工業連合会が2017-20年に実施した、「情報通信技術（ICT）等を利用した生産システムにおける人の安全確保を実現するための調査研究報告書」（以下、報告書）に基づく。

■目次

1. 調査研究プロジェクトの概要
2. セーフティとセキュリティのリスク
3. 生産システムのリスクアセスメントの手順
4. まとめ

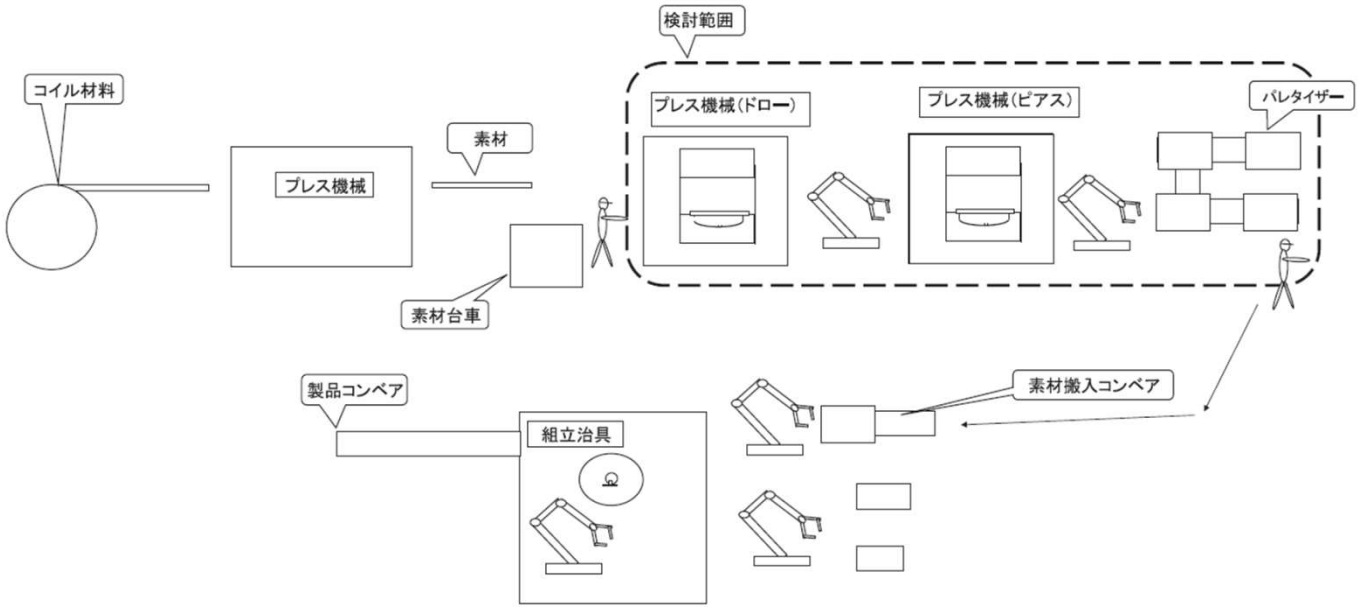
METI Journal「政策特集ロボット新潮流！ vol.5(2017/11/6)
https://meti-journal.jp/p/132/

1 調査研究プロジェクトの概要

ICTを利用した生産システムの例

■進め方

- 安全確保された事例にICTサービスを追加した生産システムを想定し、セキュリティ面からの分析を実施した。
- 鍋蓋製造ライン（日機連がH26-28年度に検討してきた、統合生産モデルの事例)
  - 複数のプレス等の機械、それを接続するロボットから構成される生産ライン

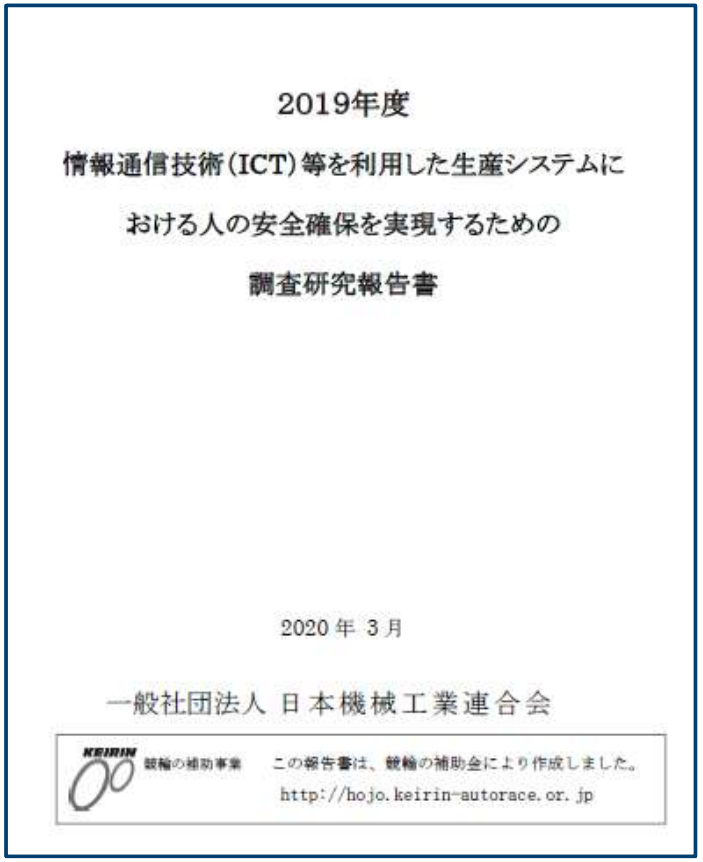


「報告書」P.9より

1.2 プロジェクト概要

■名称：情報通信技術(ICT)等を利用した生産システムにおける人の安全確保を実現するための調査研究

- 期間：2017～2020年3月
- 体制：（一社）日本機械工業連合会
- 目的：
  - IoT 時代における生産システムにおいて、これまで以上に安全性を確保し、国際競争力を維持していくために、どのようにセキュリティの脅威に対応するかを検討すること。
  - 現状においては、セーフティおよびセキュリティはそれぞれの専門家により対策が進められており、両者のコミュニケーションは十分とはいえない。
  - 本事業は、その両者の融合を図りながら、セキュリティ対策も考慮した安全な生産システム構築の進め方を検討する。


2019年度

情報通信技術(ICT)等を利用した生産システムに

おける人の安全確保を実現するための

調査研究報告書

2020 年 3 月

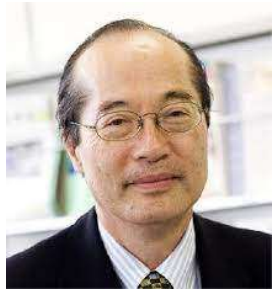
一般社団法人 日本機械工業連合会

KEIRIN 競輪の補助事業　この報告書は、競輪の補助金により作成しました。

http://hojo.keirin-autorace.or.jp

1.3 検討メンバ（2020年3月当時）

- 主査/副主査
  - 向殿政男（明治大学）、
    神余浩夫（三菱電機, IEC 61508およびIEC 62443国際メンバー、
    IEC白書"Safety in the Future"メンバー）



https://www.mukaidono.jp

- 委員：
  - 石川篤（住友重機化工業）、木下博文（平田機工）、笹川鉄平（日工会）、
    澁谷聡介（TUV-SUD）、首藤俊夫（システムズエンジニアリング研究所）、
    杉田吉広（TUV-Rheinland）、杉原健治（パナソニック）、土屋正春（MRI）、
    中村勉（安川電機）、畑幸男（ATOMS）、森本賢一（制御システム研究所）
- オブザーバ：
  - 結城則尚、細川尚紀、河野隆志、溝添公一（NISC）、引野高嗣（METI）、河合和哉（IPA）
- 事務局；
  - 宮崎浩一、野村浩章、吉田重雄（日機連）、薮田尚宏、落合孝正、岡崎亘、畑中琢哉（MRIRA）

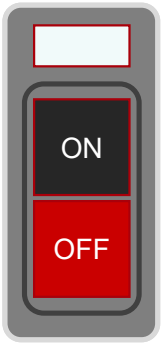
1.4 提言

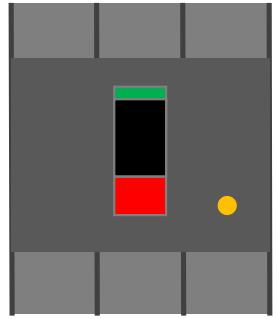
■生産設備におけるセキュリティ脅威検討の基本的な考え方

1) セキュリティ脅威は、機械安全の新たなハザードである。
   - 機械安全のリスクアセスメントにおいて、セキュリティ脅威をハザード（危険源）として見落とさない

2) セキュリティ脅威によるハザードは確定的である。
   - セキュリティ脅威は攻撃者の「悪意」によって発生するため、その発生は確率的ではなく、必ず起こりえるという点で確定的である

3) セキュリティ脅威への最終的な対策は、安全関連ソフトウェアに拠らない設備の停止である。
   - セキュリティ脅威は、安全関連の制御システム、とくにソフトウェアに影響を与えるため、安全関連ソフトウェアに拠らない機械設備の安全化手段が必要とされる
   - 例えば、安全制御系と独立したハードウェアのみによるシステムの停止が有効である。





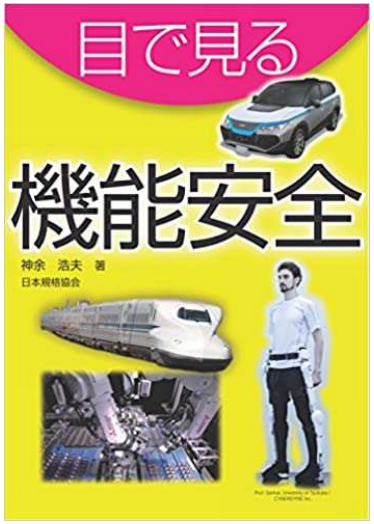
開閉器、遮断器(著者オリジナル)

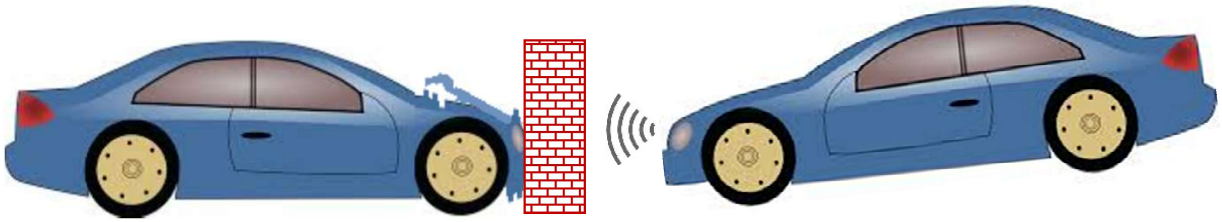
1.5 機能安全とは

■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

■機能安全(functional safety)
- 機能で安全を担保する(安全機能：safety function)
- 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



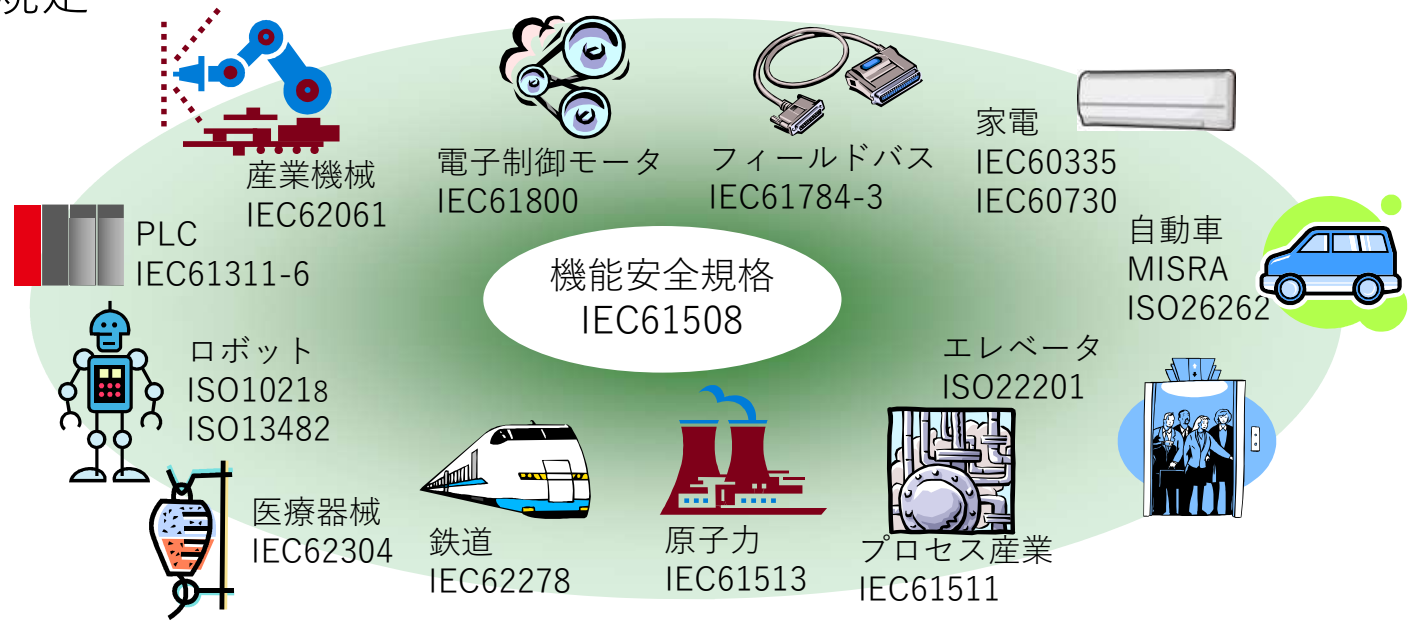


（著者オリジナル）

1.6 機能安全：機能安全規格

■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

■IEC 61508機能安全規格(1999) (Ed.2:2010, Ed.3:2023)
- 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)

2 セーフティとセキュリティのリスク

2.1 安全リスクとセキュリティリスク

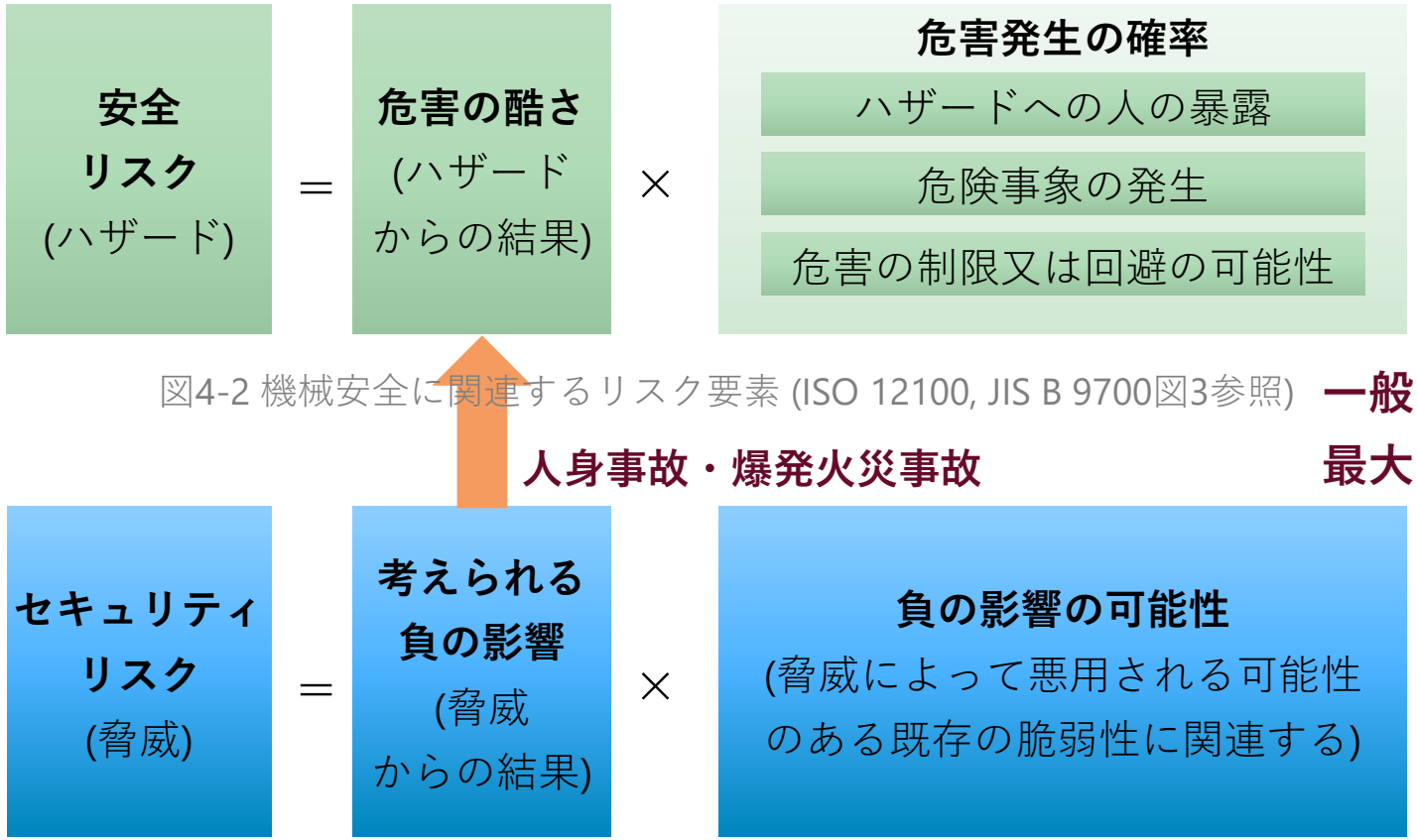


図4-2 機械安全に関連するリスク要素 (ISO 12100, JIS B 9700図3参照)

一般に，安全関連が最大リスクとなる

図4-3 セキュリティに関連するリスク要素 (ISO TR 22100-4図2参照)

ISO/TR 22100-4: Safety of machinery - Relationship with ISO 12100 - Part 4:Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

「報告書」P.10より

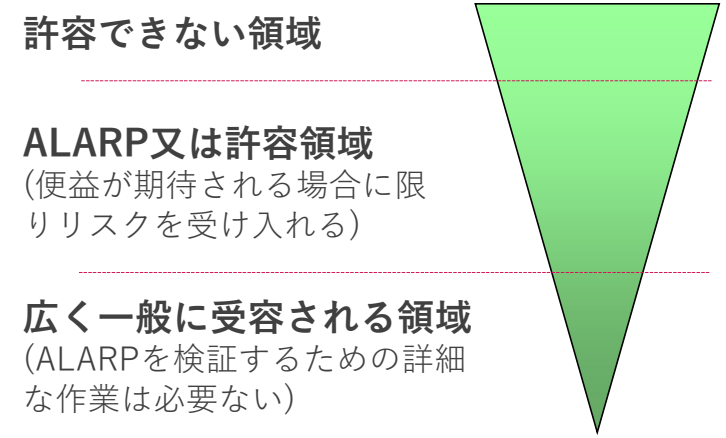
2.2 リスクアセスメント

■セキュリティリスク

- ICT を生産システムに導入する際には、セキュリティリスクを考慮する。
- 大きなセキュリティリスクは，人身事故や爆発火災など「被害の大きな事故」
- 安全関連部（機能安全）は，サイバー脅威に晒される＝セキュリティリスク

■リスクアセスメント（リスク分析、リスク低減）

- 守るべき情報資産、設備資産、生命・環境
- 脅威による攻撃・被害シナリオ
  →被害規模とその確率→セキュリティリスク見積
- リスク評価：リスクは許容(tolerable)できるか
  - 残留リスクが許容できるまでリスク低減方策を講じる
- 全ての残留リスクが許容レベル以下＝安全/セキュア



ALARP(As Low As Reasonably Practicable)
著者オリジナル

2.3 セーフティに関するセキュリティリスク

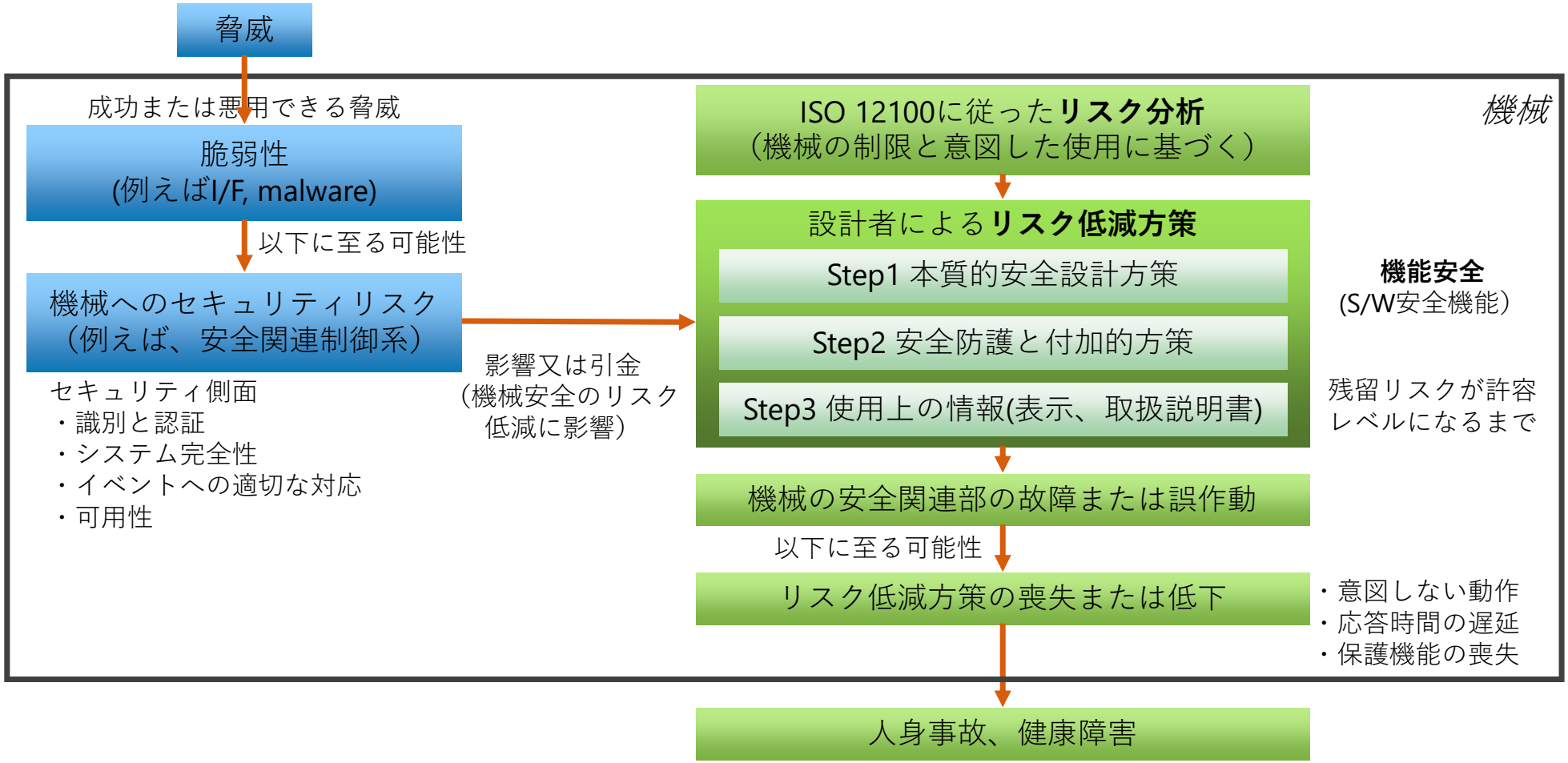
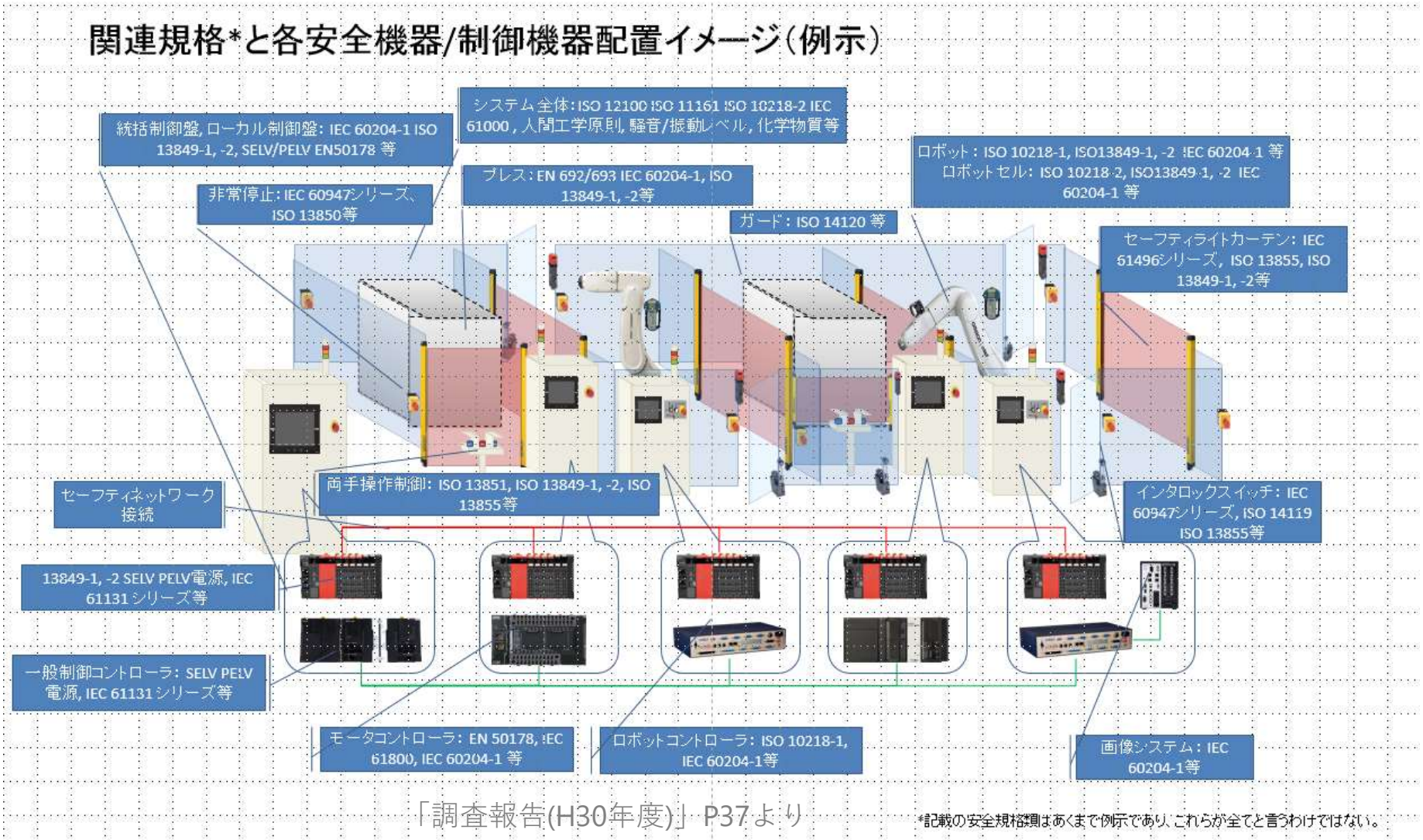


図4-4 セキュリティと機械類の安全性の関係
（ISO/TR 22100-4 図3参照）

「報告書」P.11より

2.4 安全制御系の構成例



「調査報告(H30年度)」P37より

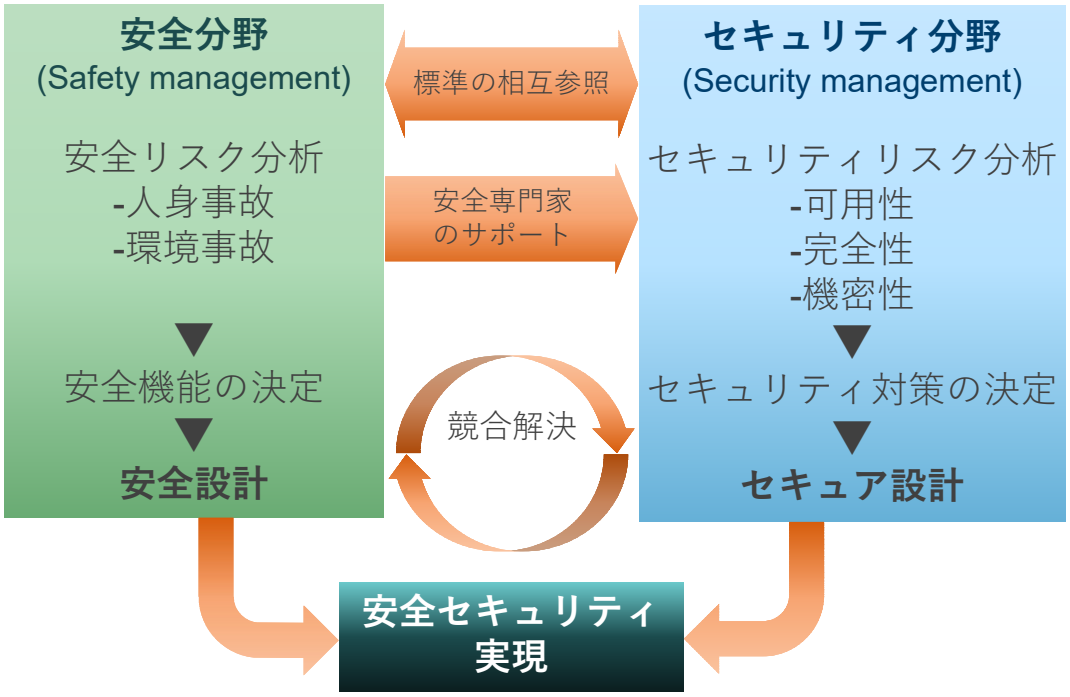
*記載の安全規格類はあくまで例示であり、これらが全てと言うわけではない。

2.5 リスク分析とリスク低減

■リスク分析
- 安全とセキュリティ分析は並行に
  - 脅威/脆弱性分析、故障/事象分析
- 安全制御系の追加→セキュリティ分析

■リスク低減
- すべてのリスクを許容レベルに
- 安全対策、セキュリティ対策の実現

■実現仕様の評価
- 安全とセキュリティの競合解決
  - CPUやメモリの取り合い、操作性



安全とセキュリティのリスク分析から機能実現
(IEC TR 63069 Framework for functional safety and security Figure4)
を参考に著者作成

2.6 安全なIoTシステムの設計/構築/運用の基本原則

- IoTシステムの設計/構築/運用に関しては、セキュリティを事前に考慮する**セキュリティ・バイ・デザイン**を基本原則として、これが確保されていることが当該システムの稼働前に確認・検証できる仕組みが求められる。その際、IoTシステムのセキュリティ確保のための要件として、基本方針の設定、リスク評価、システム設計、システム構築、運用・保守の**各段階で求められる要件を定義**することが必要である。その際、以下の項目について明確化することが必要である。

a) IoTシステムについて、範囲、対象を含めた定義を改めて明確にするとともに、IoTシステムが多岐にわたることから、リスクを踏まえたシステムの特性に基づく分類を行い、その結果に応じた対応を明確化する。
b) IoTシステムに係る情報の機密性、完全性及び可用性の確保並びにモノの動作に係る利用者等に対する**安全確保**に必要な要件を明確化する。
c) 機能保証の制定を含め、確実な動作の確保、障害発生時の**迅速なサービス回復**に必要な要件を明確化する。
d) その上で、接続されるモノ及び使用するネットワークに求められる**安全確保水準**（法令要求、慣習要求）を明確化する。
e) 接続されるモノ及びネットワークの故障、サイバー攻撃等が発生しても機密性、完全性、可用性、安全性の各項目が確保されるとともに、障害発生時の**迅速なサービス復旧**を行うことを明確化する。
f) IoTシステムに関する責任分界点、情報の所有権に関する議論を含めたデータの取り扱いの在り方を明確化する。￥

NISC「安全なIoTシステムのためのセキュリティに関する一般的枠組み」より引用
「報告書」P6より

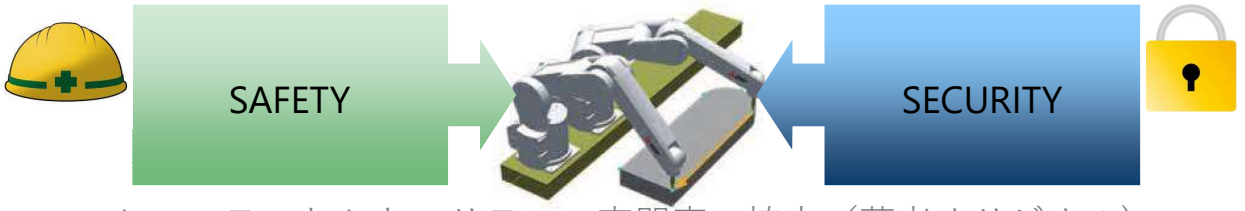
2.7 セーフティとセキュリティの課題

■ICT生産システムのセーフティとセキュリティの対策

- 両方のリスクアセスメント、対策立案と相互影響の分析

■現状の課題

- 生産システムの現場では、「セーフティとセキュリティ双方に精通した技術者が極めて少ない」、「セキュリティ要件を実現した場合、安全要件に及ぼす影響をどう考えたらよいのかわからない」という課題に直面している。
- 生産システムにおけるセキュリティの脅威の対策を進めるには、セーフティとセキュリティの専門家が協力することが必要と考えられるが、現状においては、セーフティとセキュリティの専門家が連携して取り組む段階には達していない。



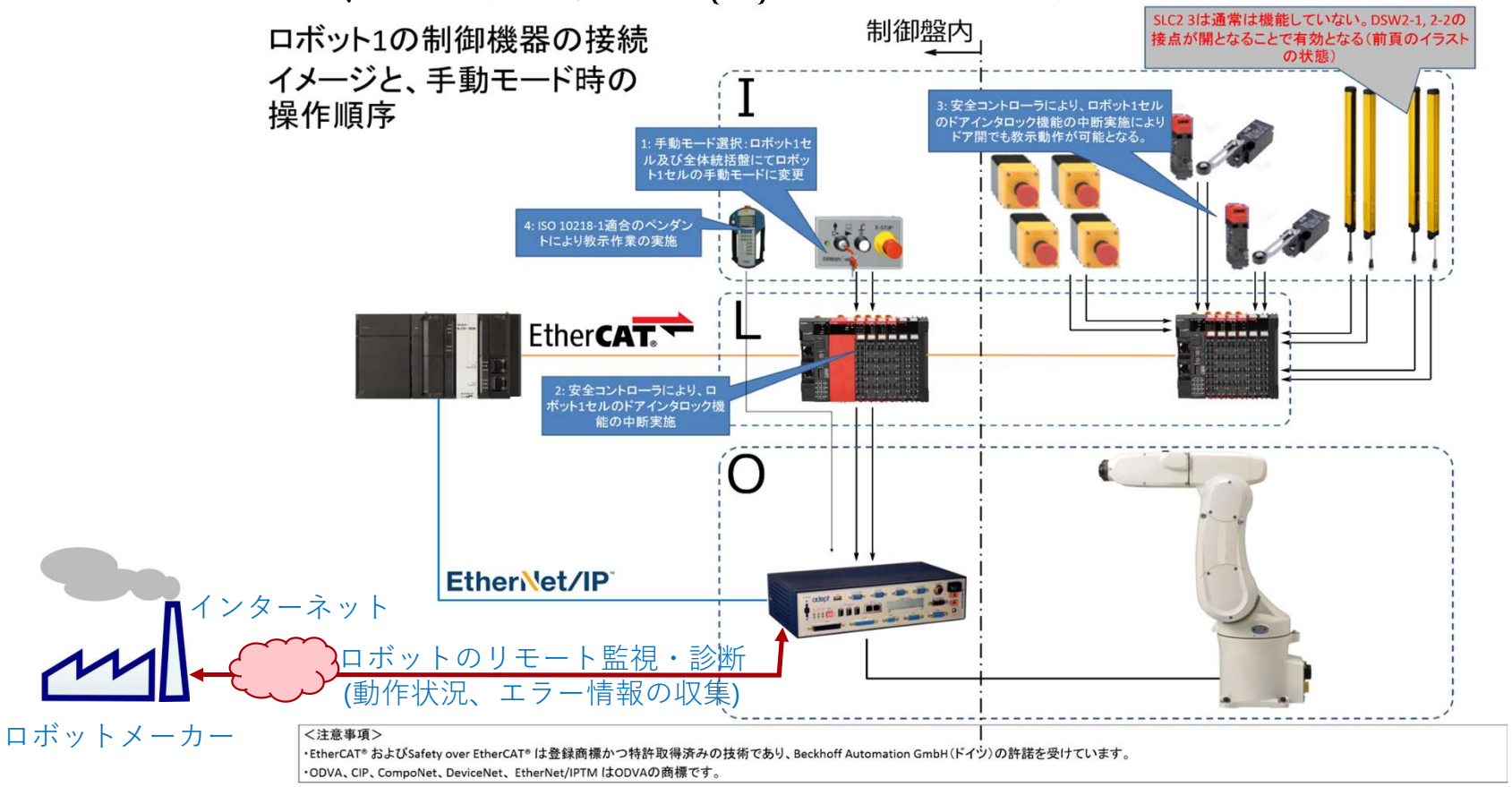
セーフティとセキュリティの専門家の協力（著者オリジナル）

3 生産システムのセキュリティリスクアセスメントの手順

3.1 システム構成例（リモート監視診断）

■ロボットのリモート監視診断の構成例

● ロボットメーカー、コンサルタント(SI)のリモートアクセス

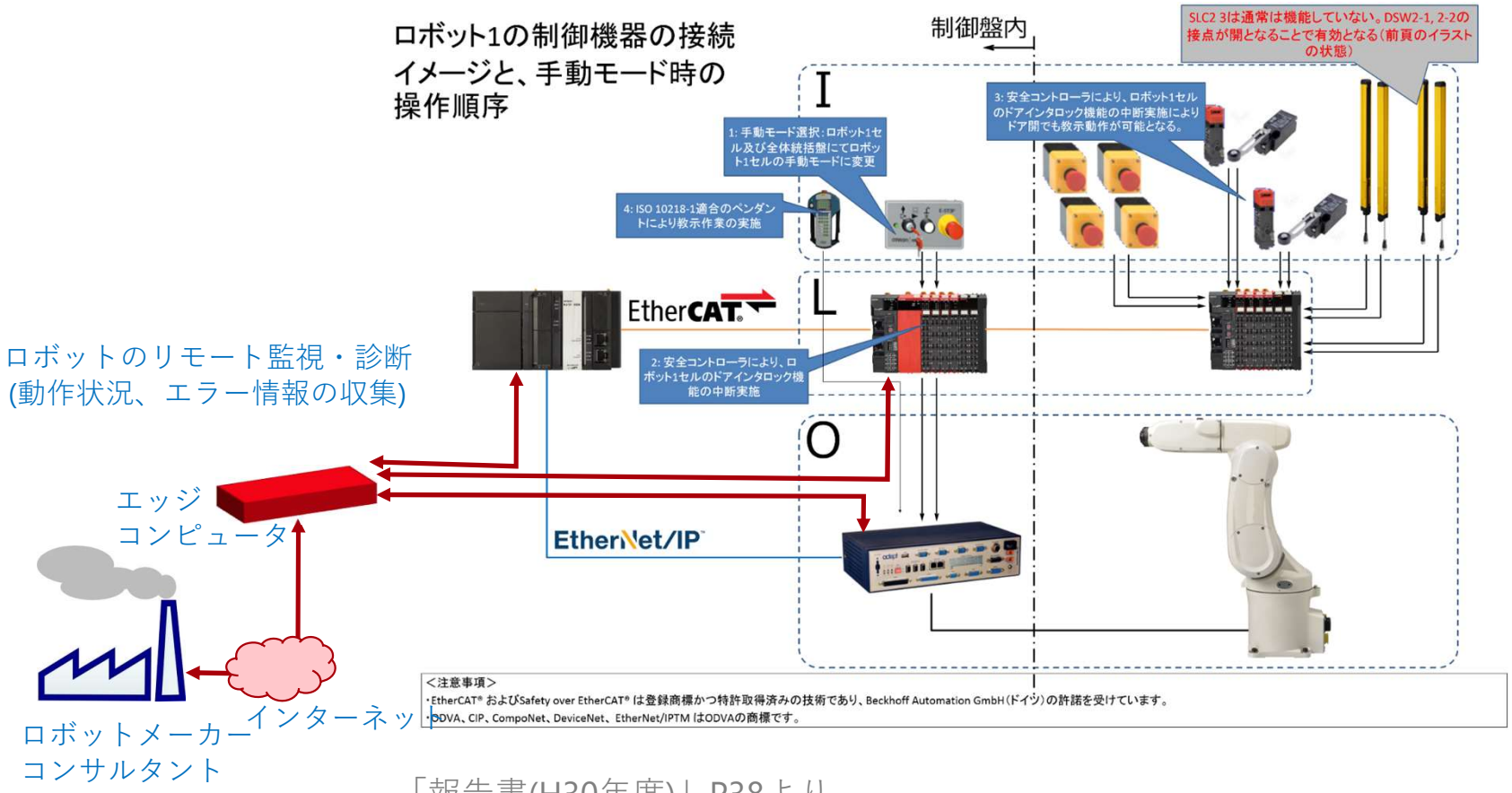


「報告書(H30年度)」P37より

3.2 システム構成例（所内クラウド）

■ロボットのリモート監視診断の構成例

● 工場内にクラウドサーバを設置し、社外からアクセス



「報告書(H30年度)」P38より

3.3 リスクアセスメント表

NO	対象ソリューション	ソリューション解説	シナリオ	シナリオ解説	想定被害	被害シナリオ	被害例	脆弱性	脅威源	被害大きさ	可能性	リスク	対策(IT)	対策(安全)	対策(運用)	被害大きさ	可能性	リスク
1	機械の遠隔監視診断	機械メーカによる予兆保全等のサービスのため、生産現場の機械やセンサーと遠隔から接続し、動作データの収取を行う。必要時は遠隔サービス拠点からの機械保守を実施する。																
1.1			生産中	動力源ON。機械が動作している状態。														
1.1.1					生産中断	現場操作用パネルＰＣの画面が不正にロックされて操作できず停止。	Wannacry			中	中	中						
1.1.1.1								パソコンのアップデート不足	ウィルス（感染）				定期的なWindowsアップデート（全台）			中	小	中
													EXEのホワイトリスト制御			中	小(無)	中
														なし		中	中	中
															Windows環境の再インストールとバックアップ	小	中	中
1.1.1.2								RDT（Remote Desk Top）による遠隔からの不正操作（誤操作）	保守員				定期的なWindows設定の確認。			中	小	中
													FireWall設置			中	小	中
														RDT禁止		小	小	小
															RDT操作のundo機能	小	中	中
1.1.1.3								制御CPUがネットワーク処理専用（DoS攻撃に弱い）	工場内ＰＣ故障やウイルス（感染）からのDoS攻撃				FireWall (IPフィルタ)設置			中	小	中
														外部ネットワーク遮断		小	中	中
															ネットワーク遮断後の別回線使用	小	中	中
1.1.2					効率品質低下	保守パソコンの不正操作により対象機械の動作パラメータ不正変更され気づかずに運転継続。	Stuxnet			中	小	中				中	小	中
1.1.2.1								パソコンのアップデート不足	ウィルス（感染）				定期的なWindowsアップデート（全台）			中	小	中
													EXEのホワイトリスト制御			中	小(無)	中
														なし		中	中	中
															Windows環境の再インストールとバックアップ	小	中	中
															定期的なエンジツールのアップデート	中	小	中
1.1.2.2								ＰＬＣなど制御システムのソフトウェアアップデート不足	ウィルス（感染）				定期的なWindowsアップデート			中	小	中
													EXEのホワイトリスト制御			中	小	中
														なし		中	中	中
															定期的なエンジツールのアップデート	中	小	中
															定期的な制御システムパラメータのレビュー	中	小	中

「調査報告」P.12より

3.4 リスクアセスメント表

No	対象ソリューション	ソリューション解説	シナリオ	シナリオ解説	想定被害	被害シナリオ	被害例(脅威例)
攻撃種類番号	生産システムにおける被攻撃部位	-	対象ソリューションの動作状況、または攻撃を受けた状況	-	攻撃によって発生する被害の予想	被害に至るまでの経緯、インシデントのシナリオ	脅威の例（攻撃方法、マルウェアなど）
1.1.1	遠隔監視		生産中	機械動作	生産中断	HMI-PCがロック	Wannacry

攻撃対象

人身事故、操業停止、環境汚染など

		リスク評価			対策			リスク再評価		
脆弱性	脅威源	被害大きさ	可能性	リスク	対策(IT)	対策(安全)	対策(復旧)	被害大きさ	可能性	リスク
脅威が進入する経路、感染の原因など	最初に脅威が現れた箇所、原因	小/中/大	小/中/大	小/中/大	ITセキュリティ対策，FWやホワイトリスト実行制御など	インシデントによる事故被害を抑制する安全対策	インシデント後の速やかな復旧のための対策			
RDTによる遠隔から不正操作	保守員	中	中	中	FW設置 Windowsの設定確認			中	小	中
						RDT停止		小	小	小
							RDT操作のundo機能	小	中	中

再評価して効果を確認

被害と可能性を小/中/大で評価
→分析を詳細化しすぎない

		被害の大きさ		
		大	中	小
可能性	大	大	大	中
	中	大	中	中
	小	中	中	小

合わせ技でリスク低減

「調査報告」P13, P14より

4 まとめ

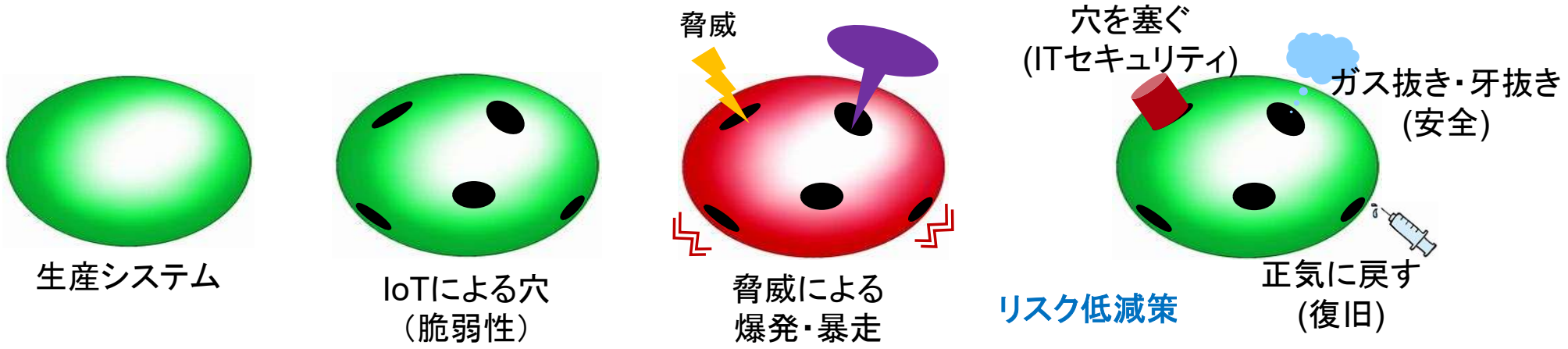
4.1 まとめ

■ICT生産システムの新たなセキュリティ脅威

- 情報漏洩だけでなく、操業妨害や人身事故を考慮→安全制御系が最大リスク

■リスク分析とリスク低減

- セーフティ/セキュリティリスク＝被害規模×事象確率
- リスク低減＝被害抑制（安全、復旧）と確率低減（ITセキュリティ）の合わせ技
- リスクアセスメント表の拡張提案



セキュリティリスク低減方策(筆者オリジナル)

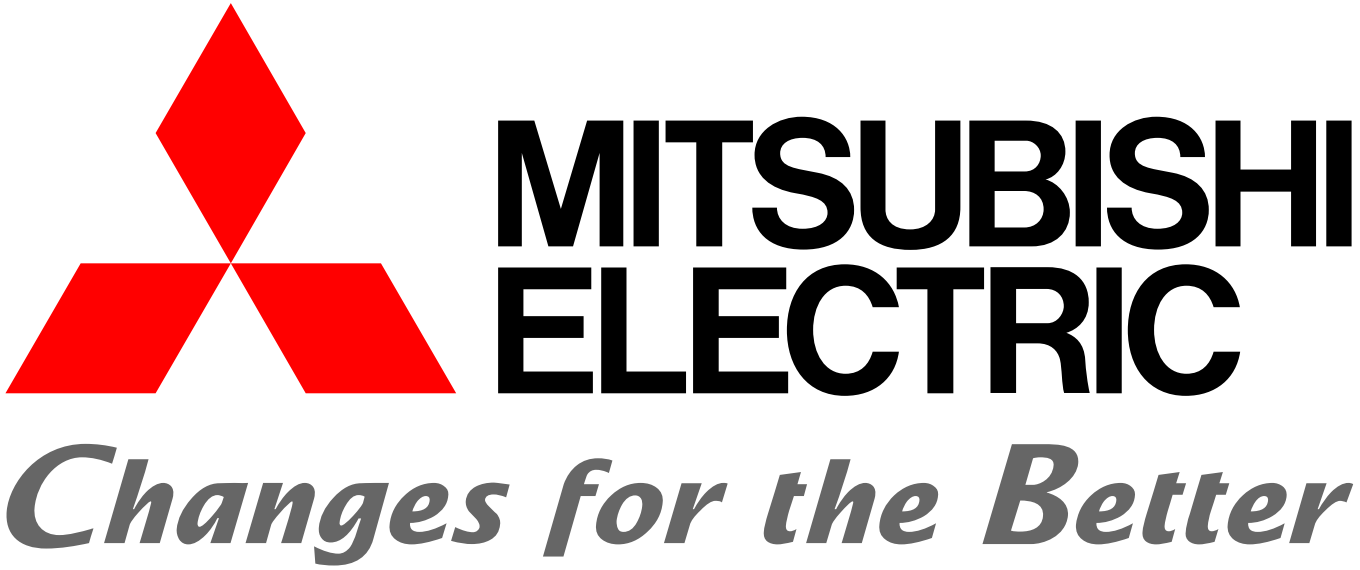
4.2 セーフティとセキュリティの標準化

■セーフティとセキュリティの標準化

- セキュリティとセーフティの両立
  - IEC TR 63069:2019 Framework for functional safety and security
    →TS化に向けて作業中
- cyber/physical safety and security (未検討)
  - 4種類の対策を効果的に組み合わせることで、安全・セキュアで、コスト・操作性に優れたシステムを構築できる

cyber/physical とsafety/securityの標準化状況（著者オリジナル）

	safety	safety & security	security
cyber	機能安全(IEC 61508) OT安全	機能安全とセキュリティのフレームワーク(IEC TR 63069) 機械の安全制御系のセキュリティ側面(IEC TR 63074)	制御セキュリティ(IEC 62443) OTセキュリティ
physical	機械の安全性(ISO 12100) 機械安全全般	--	物理セキュリティ(ISO 27001) 入退室管理、監視カメラ他


MITSUBISHI
ELECTRIC
Changes for the Better