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

序

当会は、経済産業省、公益財団法人JKA及び関係団体のご協力を得て、「機械安全の標準化事業」と「機械安全の推進事業」に取り組んでおります。

これは、機械安全の国際標準化活動における国内審議団体としての使命を果たすとともに、その普及活動を通じて我が国における機械安全の確保に貢献しようとするものであります。

機械安全は、EUにおけるCEマーキング制度の発足を契機に、関連するEN規格が制定され、これに基づく国際規格化が進められるなど、世界的にもその重要性が認知されてきております。

我が国においても、平成 18 年労働安全衛生法改正による機械設備に対するリスクアセスメント等の実施、平成 24 年には残留リスク情報提供も努力義務化されるなど、機械の包括的な安全基準に関する指針が強化され、安全性確保に国際標準の考え方を取り入れた取り組みが浸透しつつあります。平成 25 年 4 月より 5 ヵ年計画で実施された第 12 次労働災害防止計画に引き続き、平成 30 年 4 月からは第 13 次労働災害防止計画が始まり、中小企業を含む多くの製造現場において安全対策が推進されることが期待されます。

現在、製造業における大きな流れとして、IoT の利活用による第 4 次産業革命が急速に活性化しようとしています。我が国においても、IoT の利活用を進め、様々なつながりにより新たな価値創出を目指す「コネクテッド・インダストリーズ」が提唱されています。我が国の機械産業においても、IoT と ICT を有効に活用し、グローバル市場での競争力を、さらに高めていくことが求められます。その際には、安全対策とともに、今までにない新しい脅威として、セキュリティの脅威に対しても十分な配慮と対策を行うことが課題と考えられています。

このような背景から、本調査研究においては、平成 29 年度より 3 ヵ年計画で、ICT 等を利用した生産システムにおける安全性確保のための調査研究を実施してまいりました。

本報告書は、3 年間の検討結果をまとめた最終報告となりますが、関係各位のご参考に寄与すれば幸甚であります。

2020 年 3 月　　一般社団法人日本機械工業連合会

会 長　大 宮 英 明

はじめに

機械安全に関しては、安全の基本概念から個別機械の安全に至るまでの技術による工学的対策を基本とする考え方が、ISO／IEC 国際標準として体系化されている。欧州から発信されたこの考え方は、今や、北南米、また、中国を含むアジア各諸国にも広がり、機械災害防止の世界的な共通認識となっている。

時代は今や IoT 時代を迎えようとしている。製造業であれば、生産システムを構成する機械やロボットや様々な装置がつながれ、デジタル情報がビッグデータとして確保され、AI により解析、診断、予測されることにより、これまでにない新しい時代の生産システムが実現することになると考えられる。しかし、そのような便利さ（ベネフィット）があるところには、これまでの機械安全では考えられていない、新たなリスクが存在している。つながる時代には、つながることによる新しい問題であるセキュリティの問題が発生する。悪意によるセキュリティの問題は、これまでは人命には関係なく情報関連の課題とされてきたが、ネットワークに接続された機械を考えると、人命に直接かかわる問題となる。人にケガをさせるのは機械を通してのエネルギーであり、安全（セーフティ）が直接関係する。セキュリティとセーフティが不可分の関係となってくる。

本事業は、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を目的としている。現状においては、セーフティはセーフティの専門家により、セキュリティはセキュリティ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に行われているとはいえない状況と思われる。本事業では、その両者の融合を図りながら、セキュリティの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してきた。

本年度の報告は 3 年間の成果をまとめたものである。

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部会

主査　向　殿　政　男

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部会　委員名簿

（敬称略、委員氏名五十音順）

	所属・職位	氏名
主　査	明治大学 名誉教授	向 殿 政 男
副主査	三菱電機(株) 先端技術総合研究所 ソリューション技術部 主席技師長	神 余 浩 夫
委　員	住友重機械工業(株) プラスチック機械事業部 成形システム部 部長	石 川　　篤
	平田機工(株) 事業本部 商品事業推進部長	木 下 博 文
	(一社)日本工作機械工業会 技術部 技術課 課長代理	笹 川 哲 平
	テュフズードジャパン(株) COM事業部 IEP部 部長	澁 谷 聡 介
	システムズエンジニアリング研究所 代表	首 藤 俊 夫
	テュフラインランドジャパン(株) 製品部 ビジネスプロモーション シニアマネージャー	杉 田 吉 広
	パナソニック(株) オートモーティブ＆インダストリアルシステムズ社 オートモーティブ開発本部 技術企画室 主務	杉 原 健 治
	(株)三菱総合研究所 科学・安全事業本部 チーフリサーチプロフェッショナル	土 屋 正 春
	(株)安川電機 品質経営推進部 規格認証センタ センタ長	中 村　　勉
	機械安全実践技術促進会 代表	畑　　幸 男
	(株)制御システム研究所 代表	森 本 賢 一
オブザーバー	内閣官房 内閣サイバーセキュリティセンター重要インフラグループ 内閣参事官	結 城 則 尚
	内閣官房 内閣サイバーセキュリティセンター重要インフラグループ 参事官補佐	細 川 尚 紀
	内閣官房 内閣サイバーセキュリティセンター重要インフラグループ 政策調査員	河 野 隆 志
	内閣官房 内閣サイバーセキュリティセンター重要インフラグループ 政策調査員	溝 添 公 一
	経済産業省 商務情報政策局 サイバーセキュリティ課 課長補佐	引 野 高 嗣
	(独法)情報処理推進機構 社会基盤センター 産業プラットフォーム部 研究員	河 合 和 哉
事務局	(一社)日本機械工業連合会 標準化推進部長	宮 崎 浩 一
	(一社)日本機械工業連合会 標準化推進部 部長代理	野 村 浩 章
	(一社)日本機械工業連合会 標準化推進部 課長	吉 田 重 雄
	エム・アール・アイ リサーチアソシエイツ(株) マネジメント事業推進部長	藪 田 尚 宏
	エム・アール・アイ リサーチアソシエイツ(株) マネジメント事業推進部 専門部長	落 合 孝 正
	エム・アール・アイ リサーチアソシエイツ(株) マネジメント事業推進部	岡 崎　　亘

	事業リーダー	
	エム・アール・アイ リサーチアソシエイツ(株) マネジメント事業推進部	畑 中 琢 哉

（2020年3月 現在）

目　次

はじめに

1. 背景と目的.....1

2. 提言.....2

3. ICT を利用した生産システムの安全性確保に関する検討.....4

4. 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.....8

5. 生産現場におけるセキュリティリスクの KY アプローチ.....18

6. 人と協調作業を行う機械におけるリスクや安全性確保の考え方.....34

7. 今後の課題.....36

参考文献.....37

おわりに

付録 A-用語の解説.....43

付録 B-セキュリティリスクアセスメント表.....46

付録 C-セキュリティリスクアセスメントの事例.....59

付録 D-生産現場におけるセキュリティリスク KY のアプローチ.....62

付録 E-生産システムのセキュリティインシデント事例.....82

付録 F-作業委託報告書（議事録等を含む）.....87

1. 背景と目的

ISO 12100 を基本安全規格とする機械安全の国際安全規格の体系が構築されてから、ほぼ 20 年の時間が経とうとしている。ISO 12100 の発行当時、この国際規格が単なる任意規格ではなく、EU の機械指令からも参照されることで国際市場に大きく影響するということが、日本の機械製造業にとって大きな驚きであり、それだけでなく、安全は第一に機械により確保するという考え方を新鮮と感じた人も多かったと考えられる。2020 年の現在においては、まだまだ完全とはいえないまでも、安全な機械の設計にはリスクアセスメントが必要であること、また安全な生産システムの構築においてもリスクアセスメントが必要とされることは、機械安全に関係する人であれば、誰もが知るところとなった。これは、これまでに実施されてきた関係各方面での様々な取り組みと、努力の成果であると考えられる。

現在、その時以上に、我が国の製造業に大きな動きが迫ってきている。それは、情報通信技術（ICT）を利用することによる、生産環境の革新である。いわゆる第 4 次産業革命である。経済産業省では、この新しい時代に、我が国の産業が目指す姿として「Connected Industries」[1]を示した。この Connected Industries は、様々なつながりによって新たな付加価値の創出や社会課題の解決をもたらすために、IoT と ICT を最大限に利用することで、製造業の革新を目指しているといえる。

グローバル化した国際市場における製造業の動きに対応して、ICT の活用により、製造業において、どのように大きなメリットを生み出すことができるのかを、考えていくことが求められている。そのために現在のビジネスの形態を、どのように変化させていくことが必要とされるのか、安全性確保の観点からどのような対応が必要とされるのか、生産環境にはどのようなリスクが登場してくる可能性があるのか、その対策として何が必要なのか、様々な点から多くの課題があげられる。

本事業では、これらの課題を共有し、我が国の機械製造業における生産環境の安全性を確保するために、必要とされる対策の方向性について検討し提言していくことを目的としている。

[1] http://www.meti.go.jp/press/2017/10/20171002012/20171002012.html

2. 提言

2017 年度の研究部会においては、機械安全の立場からセキュリティの脅威を検討するうえで基本となる考え方を議論し、整理して示した。2018 度は、2017 年度に示した考え方にさらに議論を重ねて、機械等で構成される生産システムを製造および利用する我が国の産業界に対して、「提言」として示すこととした。

「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」として、以下を示す。

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。

② セキュリティ脅威によるハザードは確定的である。

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。

2.1 新たなハザード

生産システムに対するセキュリティ脅威が、安全関連制御系の機能・性能を阻害するものであれば、それは機械安全の観点から、ハザードの一つであると考えられる。すなわち、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として見落とさないようにすることが求められる。

ISO 12100[2]に基づく機械安全の考え方の基本は、リスクアセスメントである。セキュリティ脅威への対策の検討を進めるにあたって、機械安全の対策の中で取り組んでいくためには、リスクアセスメントにより評価することが必要とされる。

機械安全のリスクアセスメントでは、最初にハザードの洗い出しを行い、そのハザードに対して、危害のひどさと発生確率の組み合わせとして、リスクを定義している。セキュリティ脅威についても、リスクアセスメントにおいて、これまでにない新たなハザードとして考え、また確実に発生するものと考えて評価を行うことが適切であると考えられる。

[2] ISO 12100:2010 Safety of machinery -- General principles for design -- Risk assessment and risk reduction（機械類の安全性－設計の一般原則－リスクアセスメント及びリスク低減）

2.2 確定的ハザード

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。そのために、セキュリティ脅威のリスク見積もりの場合には、発生確率を考えるのではなく、その脅威が実現する難易度からリスクを見積もることが必要とされる。このため、セキュリティ脅威のリスク見積もりは、セキュリティ規格（IEC 62443-2-1[3]）を参照することが求められる。

2.3 最終的な対策

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。したがって、セキュリティ脅威に対する安全対策として、安全関連ソフトウェアのみに頼った設計をすることはできない。そのため、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。

機械安全における対策の基本は、隔離と防御である。人に危害が及ばないように、ハザードから隔離するか、カバー等で防御を施せば、100%の対策を実施することは可能である。一方、セキュリティ脅威に関しては、脅威がシステム内に侵入することを 100%防御することは困難であり、被害を完全に防ぐことはできない。物理的に接続しない対策は考えられるが、前提とする ICT による利益や利便性を享受できなくなる。そのため、セキュリティ脅威への対策は、脅威をいかに早く発見し、被害を最小限に食い止める、すなわち迅速かつ確実に生産設備を停止するかにつきる。

---

[3] IEC 62443-2-1 Ed. 1.0:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program（産業用通信ネットワーク ― ネットワーク及びシステムセキュリティ ― 第 2-1 部：産業用オートメーション及び制御システムセキュリティプログラムの確立）

3. ICT を利用した生産システムの安全性確保に関する検討

3.1 つながる生産システム

製造事業者が各種の製品の生産に使用する生産システムは、技術の進歩と社会のニーズの高度化により、より複雑かつ高機能に発展を続けている。かつて、手動操作をしていた機械が自動化され、単体で使用されていた機械が搬送装置等で複数連結され、フレキシブルで複雑な動作が可能なロボットが導入され、細かな市場ニーズに応えるため多品種少量生産に対応できるように進化してきている。

この大きな進化の流れは、第 4 次産業革命と言われる世界的な産業の変革と関連する。ドイツ政府は、2011 年にインダストリー4.0（Industrie4.0）として、生産や流通の工程のデジタル化を基本とした革新的な製造業のコンセプトを示し、世界的な流れである第 4 次産業革命を推進することを、世界に対して宣言した。

我が国は、「狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く、新たな社会を指すもので、第5期科学技術基本計画において我が国が目指すべき未来社会の姿」として、Society5.0 を提唱した[4]。2017 年 3 月に、その新しい社会を目指す産業の姿として、「Connected Industries」が公表された。Connected Industries とは、データを介して、機械、技術、人など様々なものがつながることで、新たな付加価値創出と社会課題の解決を目指す産業のあり方である。Connected Industries は、大きな技術の変化である第 4 次産業革命を、社会の大きな変化である Society5.0 に結びつけるために、重要な役割を果たす[5]。

Connected Industries は、IoT（Internet of Things）の産業応用のひとつである。IoT は、既に実用化された製品、システムも多い。例えば、オフィスにおいて使用される複写機の使用状況データやメンテナンスデータは、インターネットを介してメンテナンス会社のサーバーにつながれてデータが収集され、消耗品補給や部品交換を最適化するように利用されている。また、ビルで使用される空調機器も、インターネットを介してメンテナンス会社のサーバーにつながれ、使用状況に関するデータを収集することでメンテナンスの時期を最適化するよう使用されている。また、ビル管理会社が、ビル温度の監視と空調機器の調整を遠隔で行うことも可能である。その他、家庭で使用される電気製品においても、インターネットに接続して使用することを前提とした IoT 家電が登場してきている。

---

[4] Society 5.0 とは、内閣府 https://www8.cao.go.jp/cstp/society5_0/index.html
[5] 2018 年版ものづくり白書
http://www.meti.go.jp/report/whitepaper/mono/2018/index.html

これらの「つながる」流れは、生産システムを構成する機械やロボットにおいても例外ではない。生産システムを構成する機械およびそれに取り付けられたセンサーにより、機械の動作や状態、温度等の環境、生産実績や在庫状況、インラインの試験結果や品質情報などのデータを収集し、生産管理の効率化、品質管理の最適化、保守作業の効率化を目指そうというソリューションが、現実に登場してきている。

ICT の利用による製造業へのメリットには、様々なものが考えられる。ネットワーク接続を活用したメンテナンスサービスの提供（予知保全、遠隔保全）、生産システム全てをデジタル化して仮想モデルを用いた生産ラインの最適化や生産性評価(デジタルツイン)などが検討されている。ただし、これらの新技術・新サービスは、利益と利便性を供与する一方で、セキュリティの脅威にさらされる危険性も高くなる。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しなければならない。

3.2 生産システムのセキュリティリスクの課題

生産システムをインターネットに接続する必要性は、今後も増加していくと予想される。また、生産システムを構成する制御システム等のオープン化が進んでいることもあり、生産システムのセキュリティの脅威への確実な対策が求められる。

近年では、実際にプラント等へのサイバー攻撃が発生し、セキュリティの対策は急務といわれている（付録 E 参照）。しかし、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[6]。また、生産システムを運用している事業者からは、「安全性を確保しながらセキュリティ検討をどのように進めればよいか」という課題が挙げられている [5]。さらに、セーフティ関係者の多くはセキュリティリスクへの認識が十分ではなく、セキュリティ関係者の多くは、セキュリティの脅威が機密漏えいだけでなく、健康や安全性、環境に重大な影響を及ぼすとの認識が不足している [5]。

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。

本研究部会においては、機械安全（セーフティ）の専門知識を有する有識者を中心に委員を構

---

[6] 横井ほか、エンドユーザが直面するセキュリティ対策の現状と課題－プロセスオートメーションの現場から－、計測と制御 Vol.58, No.12、計測自動制御学会、2019

成し、そこにセキュリティ分野から多くのオブザーバーを加えて、議論を行うことで、「生産システムに必要とされるセキュリティの脅威への対策の方向性」について、検討を行った。

ネットワークにつながる生産システムは、IoT システムの一種として考えることができるため、検討を進めるにあたっては、内閣サイバーセキュリティセンターが公表している「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」（以下、一般的枠組み）を検討の基本的な枠組みとした。

一般的枠組みでは、IoT システムの設計・構築・運用に関する基本原則が、表 3-1 のように示されている[7]。

表 3-1 安全な IoT システムの設計・構築・運用に関する基本原則

安全なIoTシステムの設計・構築・運用に関する基本原則	
IoTシステムの設計・構築・運用に際しては、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、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扱いの在り方を明確化する。

「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」から引用して三菱総研が作成

基本的に、システムの稼働前にセキュリティが確保されていることが確認・検証できるようにすること、基本方針の設定から運用・保守の各段階での要件を定義することが求められており、その中で

[7] 内閣サイバーセキュリティセンター、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、2016 年 8 月 26 日

リスク分析・評価を行うことが必要とされている。

研究部会では、この枠組みを基本的な考え方とし、生産システムを運用している事業者がセキュリティの脅威への対策を検討できるようにするため、機械安全の立場から「生産システムにおけるセキュリティの脅威を検討するうえで基本となる考え方」について議論した。

4. 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

生産システムの ICT 対応を行う場合、セキュリティ脅威を新たなハザード（危険源）として扱う。セキュリティ脅威が引き起こすインシデントは、情報漏洩など経済的損失を発生させるものと、安全制御系の攻撃のように人的被害に及ぶものとがある。前者は、ISO 27001 などの情報セキュリティ技術によって対策する。後者は、内閣官房サイバーセキュリティセンター(NISC)、情報処理推進機構（IPA）などから、対策のガイドが示されている。

提言にあるように、本書はセキュリティ脅威がセーフティに関わる点を重要視し、制御システムの機能喪失や機能改ざんなどを重要リスクとみなし、そのリスクアセスメントから対策立案までの進め方を解説する。

特に、セキュリティ規格に準じるとセキュリティリスクアセスメントは難易度が高いので、本書では被害の大きさと事故発生確率の評価からリスクを推定する。また、対策は、IT セキュリティ対策、安全対策および復旧対策の組合せで対応する。リスク低減には、被害の抑制とインシデントの発生確率の低減の対策が必要である。IT セキュリティ対策だけでは被害の抑制が不十分であるので、安全対策や迅速な復旧を可能とする方策を組み合わせて使用する。本書は、この 3 つのリスク低減策を独立した方策と考え、それぞれのリスク低減効果の例を示している。組合せの選択やその効果については、各自で判断してほしい。

IPA 等から出版されたガイドは、どちらかというとセキュリティ視点であったが、本書は安全リスクアセスメントを理解している機械設計者を対象とする。セキュリティに関しては多少の知識を有しているものとする。本章のリスクアセスメントおよび対策の手順を参考にして、それぞれが設計する機械の安全性（セーフティとセキュリティ）を確認してほしい。

4.1 前提となる生産システムと ICT 導入

昨年度の検討では、生産システムにおけるセキュリティ脅威を機械安全のハザードと考えて対応するために、セキュリティ脅威に対するリスクアセスメントを行う方法を検討し、リスクアセスメント表として提示した。これを用いることにより、生産システムにおけるセキュリティ脅威のリスクを把握することができると考えられ、次の段階としては、リスクが許容レベルを超える場合に、どのような対策が必要かを求めることである。

検討にあたっては、安全が確保された生産システムの事例に対して、ICT サービスを追加したモデルを想定し、セキュリティ面からの安全性分析を行った。

検討を行うための基本的なモデルとして、日本機械工業連合会が平成 28 年度までの 3 年間の

研究事業で検討した ISO 11161[8]に基づく統合生産システムのモデル[9]を一つの候補として想定している。この統合生産システムのモデルは、図 4-1 に示すとおり、鍋の蓋を製造する架空の生産ラインであり、複数のプレス等の機械と、それを接続するロボットから構成する生産ラインである。

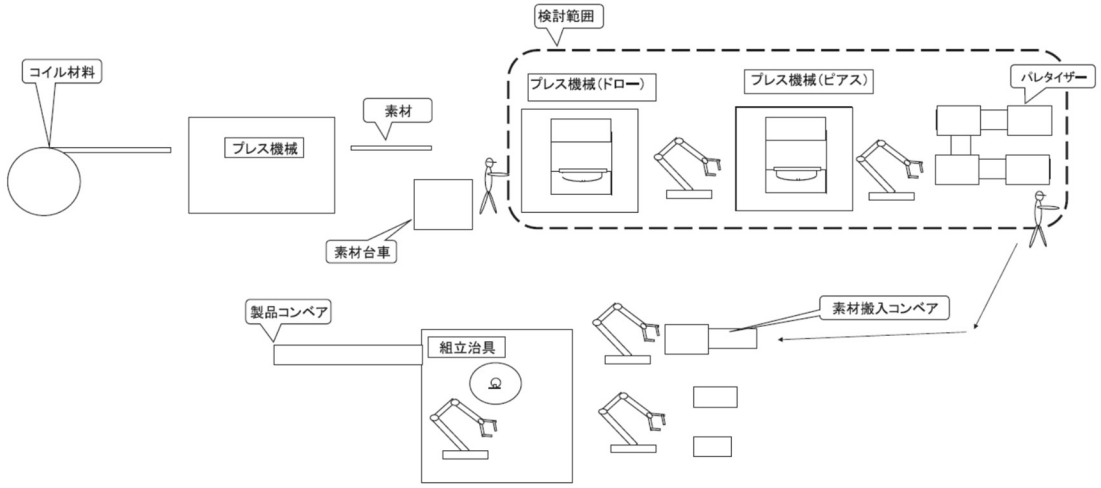


図 4-1 鍋蓋製造ライン

福田、ISO11161 に基づいた安全な生産システムの構築、安全工学 Vol.57 No.1 2018 から引用

この生産ラインにおいては、遠隔監視等の ICT の利用は想定されていないが、その他の機械安全に関する方策は、危険源、危険状態及び危険事象の洗い出しによるリスクアセスメントとその結果から許容されないリスクの低減方策まで、一連のプロセスが検討されて示されている。この生産ラインに対して、ICT を導入して遠隔監視診断等を行う機能・設備を追加する状態を想定し、セキュリティ分析を行うことで、セキュリティ脅威に対するより具体的な対処方法を、理解しやすく整理することができ、その成果は、ガイドラインとして活用することが期待できる。

4.2 リスクアセスメントの手順

(1) 概要

機械の安全性と同様、セキュリティもリスクアセスメントを実施して、許容できないリスクについてリスク低減策を講じて、セキュア(セキュリティ上の安全な状態が保たれている)な機械を設計する。セーフティもセキュリティも、対象機械システムが故障や脅威により事故や事件を起こさないこと、あ

[8] ISO 11161: 2007 Safety of machinery − Integrated manufacturing systems − Basic requirements"(機械類の安全性−統合生産システム−基本要求事項)
[9] 日本機械工業連合会 平成 28 年度 安全な生産システム構築能力向上のための調査研究報告書 http://www.jmf.or.jp/houkokusho/1505/1.html

るいは被害を最小に食い止めることを目的とする。しかし、リスクアセスメントは異なる。セーフティは、それぞれの危険源について、故障影響分析（FMEA）と故障木分析（FTA）を実施したが、セキュリティでは、機械(情報処理部)の脆弱性分析と脅威分析を行う。そしてセキュリティリスクが、機械の安全性（特に制御システムの安全関連部）に与える影響の排除（脆弱性の回避）または影響を最小限にすること（脆弱性の制限）を目的として、ここでは、機械安全のリスクアセスメント手法を習得している者を対象に、セキュリティリスクアセスメント方法について解説する。

（2） 機械類の安全性とセキュリティのリスク要素の考え方

図 4-2 と図 4-3 に機械の安全性とセキュリティのリスク要素の考え方を示す。

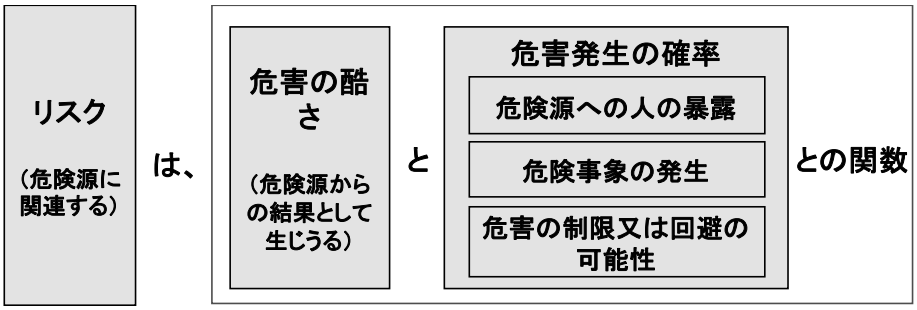


図 4-2 機械安全に関連するリスク要素

JIS B 9700 の図 3 参照

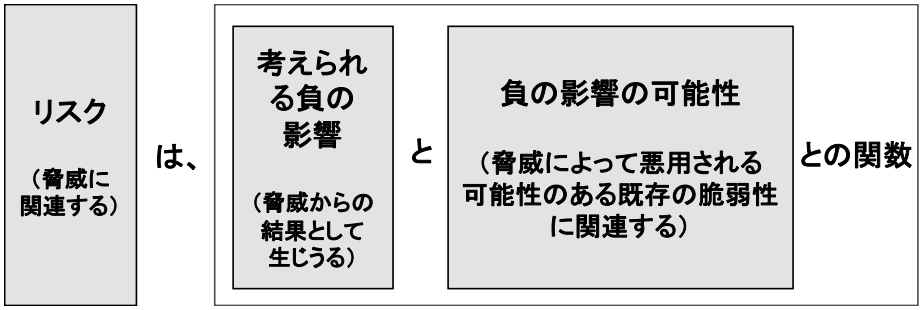


図 4-3 セキュリティに関連するリスク要素

ISO/TR 22100-4[10]の図 2 参照

[10] 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

また、図 4-4 にセキュリティによる脅威とその脅威が機械類の安全性に影響を及ぼす関係について示す。図 4-4 では、機械設計においてセキュリティが、機械類の安全性確保のためのリスク低減方策（制御システムの安全関連部）に対して影響を与え、作業者の危害に至る過程が示されている。

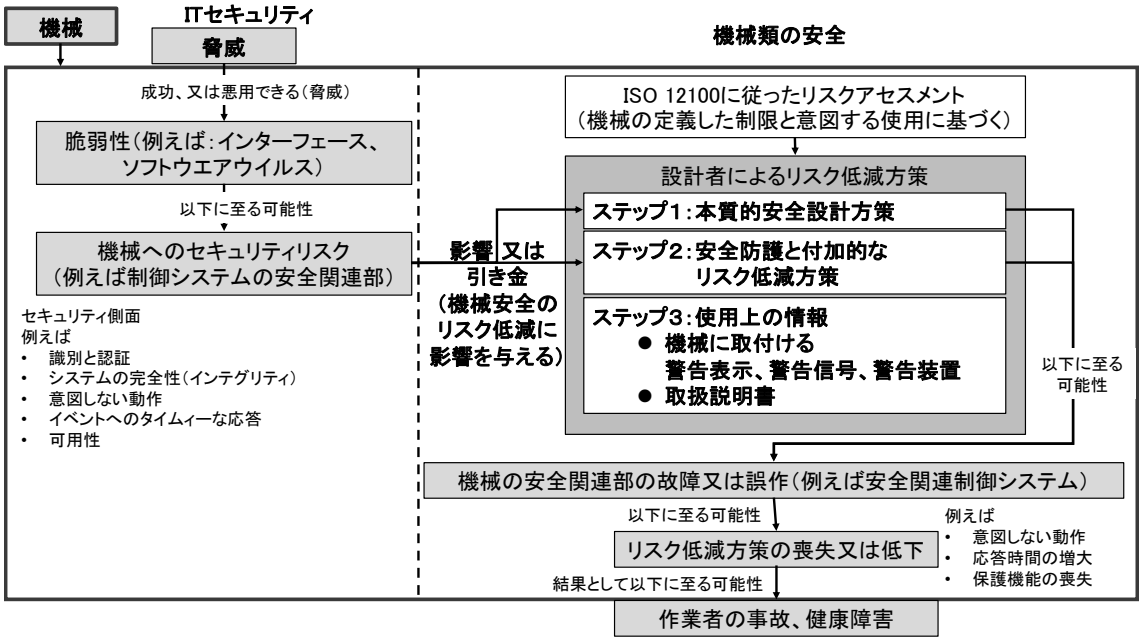


図 4-4 セキュリティと機械類の安全性の関係

ISO/TR 22100-4 の図 3 参照

セキュリティのリスクアセスメントは、図 4-4 で示したセキュリティによる機械類の安全への影響と作業者に対する危害発生のシナリオを明確にして、被害の大きさと機械安全に影響を及ぼすセキュリティインシデント（あるいは事故）の発生の可能性を見積もり、リスクを評価することである。

(3) セキュリティリスクアセスメント表

機械のセキュリティリスクアセスメント表の例を表 4-1 に示す。

表 4-1 セキュリティリスクアセスメント表の入力例（一部抜粋）

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(復旧)	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損雄	小	中	中
1.1.1.3								制御CPUがネットワーク処理兼用（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

リスクアセスメント表の横軸の各項目の内容を表 4-2 に示す。

表 4-2 リスクアセスメント表の項目名と内容

項目	内容
No	攻撃種類の番号(攻撃シナリオごとに副番を追加)
対象ソリューション	生産システムにおける被攻撃部位
ソリューション解説	対象ソリューションの解説
シナリオ	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
シナリオ解説	シナリオの追加解説
想定被害	攻撃によって発生する被害の予想
被害シナリオ	被害に至るまでの経緯、インシデントのシナリオ
被害例(脅威例)	脅威の例(攻撃方法、マルウェアなど)
脆弱性	脅威が進入する経路、感染の原因など
脅威源	最初に脅威が現れた箇所、原因
被害大きさ	この被害シナリオ(インシデント)における被害の大きさ(大/中/小の 3 値)
可能性	この被害シナリオ(インシデント)がおきる可能性(大/中/小の 3 値)
リスク	上記の被害大きさと可能性から、別表マトリックスに基づき求められたリスク
対策	脆弱性に対する対策。脆弱性を塞ぐ IT セキュリティ対策、被害を抑制する安全対策、迅速な復旧のための復旧対策の 3 種類がある。
対策(IT)	IT セキュリティ対策、ファイアウォールやホワイトリスト実行制御など
対策(安全)	インシデントによる被害を抑制する安全対策
対策(復旧)	インシデント後の速やかな復旧を行うための復旧対策
被害大きさ、可能性、リスク	それぞれの対策後のリスクの再評価、上記の同項目名と同じ

(4) セキュリティリスクアセスメントの手順

セキュリティのリスクアセスメントでは、まず、脅威に狙われるデータや設備を特定する。情報セキュリティでは、データや情報を盗聴や改ざんから防ぐことであったが、制御システムの機能や性能の喪失や劣化も、工場の操業に影響を与える。特に、制御システムの安全関連部の機能喪失や性能劣化は、作業者の保護機能が失われるので事故に直結する。データや設備は、生産システムのあるサービス(ソリューション)に帰属しているので、特定できるように該当ソリューションとそのデー

タ、設備として表に明記する。

次に、その守るべきデータや設備について、どのようなセキュリティ脅威が攻撃してくるかを分析して、攻撃シナリオを想定する。脅威の種類は、マルウェア（不具合を起こす意図で作られているソフトやプログラム）等による制御データ、プログラムの改ざん、アラームや実績データの偽造または無効化、遠隔命令によるシャットダウンや停止、トラッフィック攻撃による性能劣化、などがある。これらのシナリオに基づいて、被害の大きさを推定する。

脅威が攻撃できるためには、制御システムの脆弱性を突いて守るべきデータに到達しなければならない。そこで、それぞれの脅威が進入する制御システムの脆弱性分析を行う。脆弱性分析は、既知のあるいは容易に推定できる脆弱性に基づいて分析する。ここまでで、表中の脆弱性と脅威源までを記述する。

次に、リスクアセスメントの二つのパラメータ、被害の大きさと可能性を推定する。被害の大きさは、主に脅威による攻撃シナリオによる。生産システムの場合、制御システムの安全関連部への攻撃は人身事故に至るため被害大となる。また、高価な設備の破壊あるいは故障も被害金額が大きくなる。被害の大きさは、機械安全のリスク分析から概ね、高＝死亡・重傷事故、中＝軽傷、小＝軽微で考える。

被害発生の可能性は、脆弱性分析において、それを突く攻撃の技術的難易度と機会の多さから求める。情報セキュリティ専門家は、この可能性導出において、さらに詳細なパラメータ分析を行っていることが多い。しかし、可能性は 3~4 段階で分類されるので、詳細分析しても精度はさほど改善しない。ここでは、可能性を 3 段階として、高＝一日に何度も、中＝月に複数回、小＝年 1 回あるかないか、と考える。

セキュリティのリスクは、表 4-1 に基づいて、被害の大きさと可能性のマトリックスからリスクを導出する。ここでもリスクは 3 段階に分類されている。求められたセキュリティリスクを表 4-3 に記す。いま、リスク小を許容可能、すなわちリスク大中のシナリオは許容できないとし、リスク小となるまでセキュリティのリスク低減方策を施す。

表 4-3 セキュリティリスクのリスクマトリックス

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

4.3 リスクの低減方策

ここで、リスク低減方策として 3 つの方針がある。ひとつは、主に脆弱性を塞ぐ IT セキュリティ対策、次に事故被害を抑制する安全方策、そして攻撃後に迅速にシステムの原状回復する対策である。ほとんどの IT セキュリティ対策は、攻撃の可能性を抑えることができる。一方、安全方策とシステムの原状回復対策は、被害の大きさを抑制あるいは最小化することができる。リスク大は被害の大きさも可能性も大きいので、3 つのリスク低減方策を組み合わせて、許容可能リスクにまで低減する。表 4-1 は、3 種類のリスク低減方策をひとつずつ適用したときのリスク低減効果について記しており、合わせ技効果まで表していない。しかし、リスク低減効果の参考にはなるだろう。

リスク低減方策を実施して、改めてリスクアセスメントを行い方策後のリスクを評価し、許容可能リスク小であれば十分セキュアであるとみなす。全てのリスクが小となったとき、セキュリティ対策設計は完了する。ここまでが、表 4-1 に基づくセキュリティのリスクアセスメントの手順である。

リスク低減方策によって、他の性能が阻害される場合がある。例えば、セキュリティ強化のために暗号強度を高めると、そのぶん処理能力を取られて安全応答時間が悪化する。逆に、パスワード強化は、セキュリティはもちろんオペレータの誤操作（ヒューマンエラー）の回避にも効果がある。それぞれのセキュリティのリスク低減対策が、生産システムおよびソリューションサービスに影響あるいは阻害していないかを分析する。もし影響があれば、関連する IT セキュリティ対策を再検討する。

4.4 セキュリティ設計

ここまでのセキュリティのリスクアセスメント評価によって、生産システムおよびソリューションサービスについて実施すべきリスク低減対策、およびそのレベル要求が明らかになった。このセキュリティ要求仕様に基づいて、IT セキュリティ対策を設計する。安全方策および原状回復（エンジニアリング）対策は、安全設計やエンジニアリング設計において考慮する。

表 4-4 に機械の安全性に影響を与える可能性のあるセキュリティの脅威を回避するためのリスク低減（緩和）方策の例を示す。

表 4-4 機械の安全性に影響を与える可能性のあるセキュリティ脅威を回避するためのリスク低減（緩和）方策の例

保護領域	リスク低減（緩和）方策	機械製造者	インテグレータ	最終使用者
ITシステム（安全性に影響を与える可能性がある）への論理的/物理的アクセスの制限	ITシステム全体からの制御システムの安全関連部に関係するITシステムの物理的分離	X	X	X
	リスク低減（緩和）方策（ファイアウォール、ウイルス対策ツールなど）を備えたITシステムの提供	X	X	X
	実際の安全モードでのITシステムのリスク低減（緩和）方策の維持（例：ウイルス対策ツールの更新）			X
	ソフトウェアのアップグレードを許可する手段の提供	X	X	
	個別の認証およびアクセス制御機構（カードリーダー、物理ロックなど）の提供	X	X	
	複数の独立したレイヤーを持つネットワークトポロジ（物理的配列）の提供	X	X	
	ITシステムのユーザー権限の各個人の役割に必要な権限のみへの制限			X
	すべての未使用のポートとサービスの無効化			X
	個々のユーザーアカウントとアカウント管理の責任（例：パスワードの更新）			X
	すべての認証後の実施者/サービスの認証チェックのための手段を備えた機械の提供	X	X	
	深刻なセキュリティ攻撃の場合に機械を安全な状態にするための物理的なハードウェア手段を備えた機械の提供。（例：非常停止、シャットダウンボタン）	X	X	
	IT接続ポイント（USBまたはイーサネットソケットなど）のアクセスまたは使用の物理的制限	X	X	X
	アクセス可能なIT接続ポイント（USBまたはイーサネットソケットなど）の切断または非アクティブ化	X	X	X
	以下に関するコンポーネントメーカーの使用説明書の観察 IT接続ポイントの使用。 接続が必要な機械のライフサイクルのフェーズ。 必要な接続の期間；コンポーネントの製造元によって指定されたITインターフェイス（HW / SW）。 コンポーネントの製造元が指定または推奨するアプリケーションソフトウエアへのアクセス制限。 ；パスワードとウイルス対策ツール（オン）の使用。 インストール時、およびその後の頻繁な初期デフォルトパスワードの変更。	X	X	X
ITセキュリティインシデント（安全性に影響を与える可能性がある）の検出と対応	障害のあるITシステムコンポーネントまたは利用できないサービスを検出する機能を備えた機械の提供	X	X	
	脆弱性を監視する手段を備えた機械の提供	X	X	
	脆弱性に対する応答性と反応			X
リモート保守およびサービスの場合	リモートアクセスセッションのセットアップと終了のための手段の提供	X	X	
	リモートアクセスコマンドよりも優先される機械上の手段の提供			X
	ソフトウェアから独立したリモートでバイパスできない手段の提供	X	X	

X:方策実施者

ISO/TR 22100-4（IDT ANSI B11・TR9[11]）の表 3 より作成

[11] ANSI B11.TR9-2019 (ISO/TR 22100-4:2018 IDT) Guidance to Machinery Manufacturers for Consideration of Related IT-Security (Cyber Security) Aspects

5. 生産現場におけるセキュリティリスクの KY アプローチ

5.1 セキュリティリスク KY　3 つのアプローチ

生産現場におけるセキュリティ対策のアプローチには、大きく分けて3つのアプローチがある。

1） 設備構想に基づくリスク分析

2） シナリオに基づくリスク分析

3） 気づきに基づくリスク分析

この3つのアプローチのイメージは図 5-1 に示す通りで、各アプローチの詳細を以下に記載する。

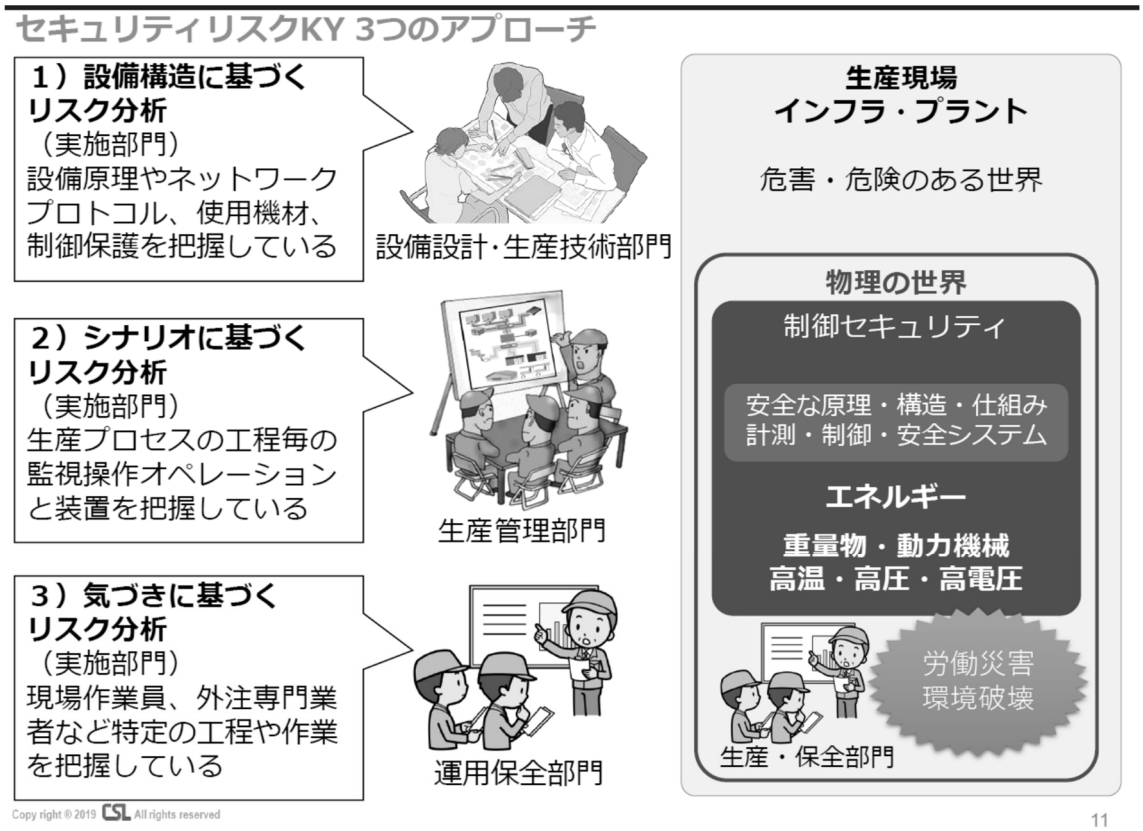


図 5-1 セキュリティリスク KY　3つのアプローチ

(1) 設備構造に基づくリスク分析

第一は、機械設備の動作原理や制御システムの詳細について熟知したメンバーによる脆弱性分析ならびに脅威分析である(以下、この2つを総称しセキュリティリスクアセスメントと呼称する)。このアプローチは、機械設備の本質的安全の観点、および機能安全の観点の災害リスクアセスメ

ントを土台とし、それらの安全の仕組みが ICT の脆弱性および ICT の脅威によってどのように脅かされるのかを評価し対策を講じるアプローチである。

具体的には機能安全の観点で設置した安全 PLC や安全防護のシステムが、通信を介して無効化されるようなケースを洗出し対策を講じる。本質的安全のアプローチ、機能安全的アプローチが適切に講じられており、かつそれらが ICT によって何ら能力が棄損されないのであれば、つまり適切に分離され独立し、ICT に影響されないのであれば、生産設備の労働災害に対するセキュリティ対策は十分であると考えることができる。

このアプローチは、抜け漏れを防ぎ確実に労働災害を防止するための方策として最も効果的なアプローチであるため、当部会として最も強く推奨する。ただし、前述の通りこのアプローチを実施するためには、生産現場で災害をもたらすすべての機械設備、動力源など、災害のポテンシャルエネルギーを持つ事物に対する動作原理や設備構造についての知識が必要であるばかりか、それらの制御処理や防護の仕組みについても十分な知識を持つメンバーが参加し、長時間にわたりリスク分析に加わることが必要となる。

新しく大規模な工場設備を建設するような場合、このような組織編成も可能かもしれないが、すでに稼働し数年経過している生産設備や、何度も工場の拡張や改造が行われ、本質的安全のポリシーや機能安全のポリシーが不明確な一般的な生産設備の現場では、そのようなメンバーが組織として維持されていない場合が多い。また安全のポリシーも文書化されずに不文律として安全ルールだけが運用されているケースがほとんどである。そのようなケースでは、本アプローチのよりどころとなる設備そのものの災害リスク分析の土台が失われていると考えられるため、たとえ外部から当事者ではない一般的な技術者、有識者をあつめたとしても、適切なセキュリティアセスメントを行うことは困難である。

このアプローチは、生産活動を行う経営層の問題として、工場建設時、または長期間の工場運営にわたって適切な投資やリスクアセスメントの維持を心がけるよう強く自戒を求めたい。

(2) シナリオに基づくリスク分析

第二は、上記のような対策が十分にできない場合の次善のアプローチである。工場設備現場が長年無災害で運営されてきた場合、その実績を今後も継続することに対して、これから行おうとする ICT 技術による現場設備への干渉がどのような負の影響を与えるのかを考察するアプローチである。

工場にある機械設備の原理や制御の詳細がわからないまでも、生産活動において必要となる現場の操作（機械の操作や、数値の入力）や監視や異常時の対処などのオペレーション、ならびに

そのシステムの現在の構成を把握するメンバーが中心となる。このメンバーに、今回 ICT によるシステム拡張を行うシステムインテグレーターが加わることでセキュリティリスクアセスメントを行う。具体的には、新しく追加する ICT 設備と既存の設備との接続点を明らかにし、その接続点周辺のコンピュータや通信装置を対象にセキュリティアセスメントを行う。

すでに生産活動が行われている場合、追加する ICT は生産活動全体の品質や効率を向上させることを目的とする場合か、または特定の機械をターゲットに保全や性能改善を目的とする場合が想定される。そのようなケースで想定されるシステム構成や通信構成、コンピュータの様態や役割はある程度絞られる。それを踏まえ、本アプローチでは設備の詳細を知らずとも、一般的なセキュリティハザードのシナリオを想定し、それを対象の設備に当てはめることで脆弱な部分や新たな脅威が発生する場所を明確化し、対策を講じる議論につなげようとするアプローチである。※このアプローチが本報告書前章のシナリオベースのアプローチである。

シナリオベースアプローチは、生産現場のオペレーションの主任技術者と、今回追加する ICT 設備（IOT 設備）を設置するベンダーで実施することができるため、すでに稼働している生産現場ではより現実的なアプローチであろう。

このアプローチは、機械や設備の原理や制御や保護システムについての詳細な知見が無くても可能である一方、現状のオペレーションにかかわる監視や操作のシステム、表示や警報のシステムのネットワーク構成やソフトウェア構成についての全体把握が必要となる。なぜならば、新たに追加する ICT 装置（IOT 装置）が、制御や保護のどの部分のネットワークに接続されるのか、それによって影響を受けるシステムはどの範囲か、つまり変化点がわかなければ、影響を受けるオペレーションの範囲が判定できないからである。

生産設備が古くても、ある程度大掛かりな設備を工場が保有する場合には、会社として選任者が継続してシステムの維持保全を行っているケースが多いため、このアプローチは実行可能であろう。しかしさらに規模の小さな工場現場では、メーカから購入した機械設備をその時々の運用に併せて、現場の操業担当者が直接改造したりネットワークや PLC を取り付けたりすることで日々のオペレーションを実現しているケースがある。このような場合、それぞれのラインの現場の担当者だけが知っている設備情報が多くなる。現場のシステムを知るのが工場操業の担当者そのもののため、リスクアセスメントのミーティングに、長時間それら現場担当者を拘束することは操業を停止するなどの影響が避けられず、現実的ではないケースが想定される。

（3）気づきに基づくリスク分析

上記のように生産現場のオペレーションを担う担当者そのものが、オペレーションに必要なパソ

コンや PLC などに改造を施すなど、現場設備の制御や保護、システムに対する知見が組織として維持保全されていない場合を想定したアプローチを考える必要がある。このようなケースでは、担当者を長時間リスクアセスメントで拘束することは、生産現場を止めることにつながるため現実的ではない。また担当者本人も、システムの詳細は社外の業者に依頼しており、前述のアプローチのようなセキュリティインシデントのシナリオを独自に想定することも難しいかもしれない。

第三のアプローチは、日常の生産活動におけるRKY（リスク・危険・予知）活動の一環として、毎日問題意識を共有し考える時間をすこしずつ設け、これから行う実際の作業に直結した問題を現場で繰り返し見直すことにより、セキュリティリスクに関する気づきを得ようとするものである。

このアプローチは、第一の本質安全・機能安全からのアプローチと異なり、設備の根本原理や制御や保護の構造をベースにするものではないため、高度な工学的なアプローチとはなりえない。また第二のアプローチのように、ICT の知識に基づく分析でもない。しかしながら、労働災害を防止する安全活動の一環であることを強く意識づけることができれば、現場の担当者自身が自分の命や健康への影響に引き付けて考えることとなり、専門的な脆弱性の発見以外にも、パスワードの付箋紙での貼付けや、USB の持ち込みの抜け穴など、業務プロセス上の脆弱性をも見つけることにもつながる効果が期待できる。また若い新人技術者が日常の SNS などで伝わるセキュリティ事件を伝えながら、ベテラン作業者とコミュニケーションすることで、現場の課題の発見につながる可能性も期待できる。

このアプローチの実行のためには、毎日の RKY 活動のように、毎日繰り返し自分の問題であることを、それが労働災害につながることを強く意識づけることが肝要である。このため、本調査研究会では、労働災害防止のために現場で唱和される 6 か条をイメージし、セキュリティリスク 8 か条を提唱する。これらは制御システムにおけるセキュリティリスクを考える際の主な脆弱性を抽象的に表現したものである。毎朝の朝礼や RKY の場面で、安全の誓いの唱和同様、この 8 カ条を唱和し、そのうえでこれから実施する作業の問題点を皆で短時間でもディスカッションするのが本アプローチである。

これらの抽象的な脆弱性のキーワードを、自分たちのこれからの作業に引き付けて、どのような危険を予知できるのか、毎日の現場で繰り返し行えば、自分たちがすぐに改善できる対処は行い、現場担当者では解決できそうにない問題に気付いた際は、現場から管理部門や経営者に問題を上申し、より大きな活動に広げるきっかけとなることを期待したい。その気づきは専門的なものである必要はない。8 か条に書かれてある言葉を引用し、「だったら、今回の作業のこのパソコンは大丈夫か？」と、現場作業員レベルが自問自答することを想定している。

直接的な漏洩の被害を受ける情報が保管されている場所と異なり、生産現場の労働災害に結び付く制御セキュリティリスクは、実際に現場作業に携わらない、携わった経験のない管理部門や

経営者には感覚的に理解できない部分が多い。その一方でセキュリティ対して一番心配しているのは管理職であり経営者でもある。

このような現場担当者が行う、作業員の身近なレベルの RKY を通して現場と管理部門を結び、安全とセキュリティの関係性、問題意識を共有することは、大掛かりで高価なセキュリティ対策の装置を購入するよりも効果が高いのではないだろうか。

5.2 生産現場のセキュリティリスク 8 か条

一、パスワードは	ばれる。
一、無線 Wi-Fi は	侵入される。
一、ソフトウェアは	乗っ取られる。
一、コンピュータも通信も	間違える。
一、ＰＬＣも	改ざんされる。
一、通信は悪事も障害も	伝える。
一、脅迫ウイルスで	生産が止まる。
一、バックアップなければ	復元なし。

自分の安全は自分で守ります！よし！

図 5-2 生産現場のセキュリティリスク 8 か条

(1)パスワードはいつかばれる

現場におけるパソコンなどの装置は、個人の所有物ではない。このため個人が記憶するパスワードによるセキュリティ確保は生産現場では効果が薄い。緊急操作のたび、シフト交代のたびにパスワードを担当間で伝える必要性があり秘匿には限界がある。現場のパソコンなどの装置すべてに個人個人を区別特定するアカウントとパスワードを記憶させることも技術的には可能であるが、結局は使用者のモラルに大きく依存する。一人が付箋紙に貼るなどすれば、セキュリティ対策として意味を持たない。また現場のパソコンは使われていない状態の PC も多い。オフィスの会議室にパソコンがぽつんと置かれているのは不自然だが、現場にパソコンがぽつんと置いてあっても違和感がない。業務系パソコンの様に個人に紐づく管理ではなく、パソコン資産そのものにデジタル証明書を埋め込むなど、個体を識別する機能を搭載することも検討すべき課題である。

この条文を踏まえた現場の RKY として、たとえば長期間固定化したパスワードを変更するという

対策が出されたり、物理的な施錠の必要性に気付くことを期待したい。

(2)Wi-Fi は侵入される

Wi-Fi にはある程度のセキュリティ対策は施すことができる。SSID そのものを見せないようにすることや、MAC アドレスの制限、パスワードの定期的な変更なども効果があるとされる。ただしこれらは不特定多数がワンタイムで接続することを想定したセキュリティであり、設備として何年も常時使用する生産現場では効果が限定的である。

常時昼夜を問わず通信をしている現場では、無線電波に含まれているやり取りのデータパケットに SSID や MAC アドレスなどのデータが含まれており、長時間観測すれば解析は容易である。またMACアドレスを成り済ます技術は市販されている。そもそも生産現場で制御機器やPLCをWi-Fi で接続している場合、SSID やパスワードの文字列を変更する作業は、接続する PLC や端末すべてを適切に変更することが必要となる。ダウンタイムが発生し、また変更に失敗した場合に極めて深刻な影響を生産に及ぼす変更は頻繁には実施できない。

設備や生産ラインのレイアウトが頻繁な生産現場では、制御ネットワークへの Wi-Fi 使用はとても便利である。しかし生産現場での Wi-Fi の安易な使用は、流れる情報に容易にアクセスを許し制御セキュリティのリスクが高まる可能性について十分留意するべきである。

たとえば 2000 年オーストラリアの下水処理場では、地方自治体の不採用に恨みを持った犯人が、無線 LAN 経由で施設内の弁を操作する SCADA にアクセスし、汚水を河川に流出させた。無線による不正操作は機械の故障と区別がつきにくい。この事件も発覚まで 2 カ月かかっている。生産設備で使用される制御用通信は、市販されている PLC や SCADA ソフトを使用することが多いが、それらは通信コマンドや文法が公開されているものが多い。機密漏洩の観点では重要度の低い設備制御の通信データであっても、機械設備に影響を与える可能性を考慮した場合、データが漏洩する事態は避けるべきである。Wi-Fi の適切な使用が求められるケースである。

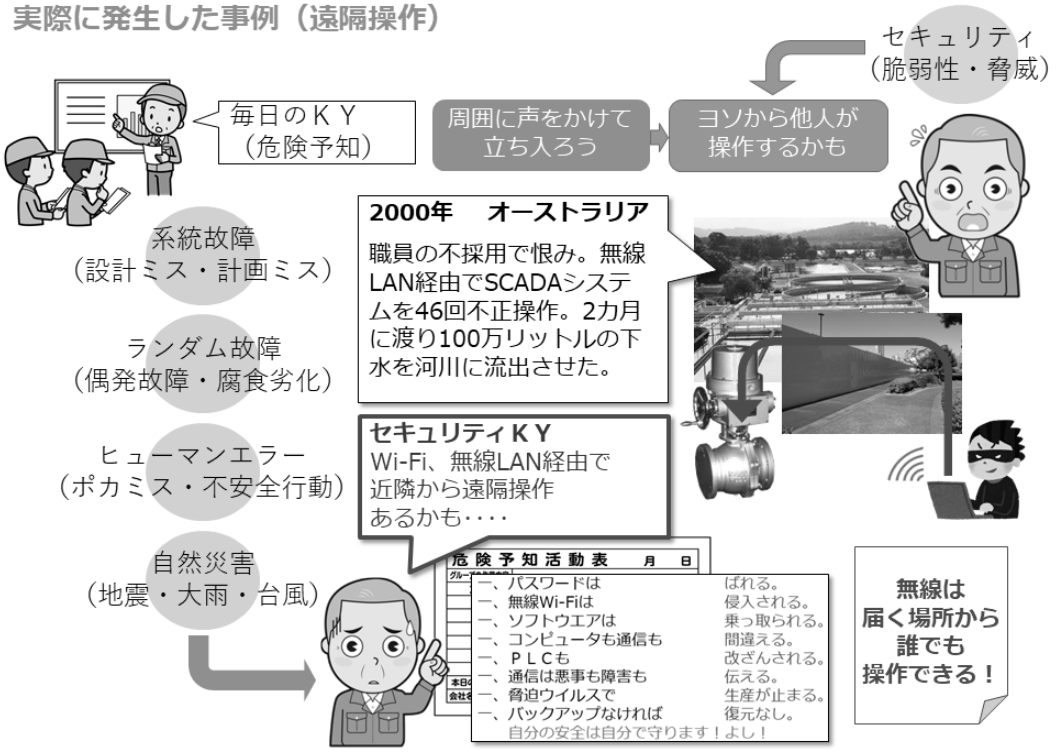


図 5-3 実際に発生した事例（遠隔操作）

Wi-Fi では SSID とパスワードを組み合わせたセキュリティ以外にも、前述のデジタル証明書の技術を用いた、EPA-TLS という技術がある。これを使用することで、予めデジタル証明書をインストールしたパソコンだけが Wi-Fi に接続できるような制限を設けることができる。生産現場で Wi-Fi を使用する際は検討を推奨する。

本条項に基づく RKY によって、Wi-Fi を用いる範囲を限定し、重要性が高いシステムや安全に関係するシステムでは、有線接続に振り替えるなどの問題意識が提案されることを期待したい。また Wi-Fi が接続されているネットワークと、ネットワークそのものを分離することも検討を促したい。また SSID のパスワードの変更作業の実施も毎朝の RKY で周知することは、作業による通信障害（パスワード変更から漏れた機器が接続できなくなるトラブル）の発生可能性を低減させることも期待したい。

(3)ソフトウェアは乗っ取られる

Windows のような OS に、不正なプログラムとしてインストールされるようなウイルスは、ホワイトリスト制御など、許可されたプログラムだけが起動できる手立てで感染や発病を防止することができる。しかし、そもそも起動を許可したソフトウェアが乗っ取られる場合は、そのプログラムの動作メモリー

の内部で不正な処理が行われるため、ウイルス検知ソフトなど、プログラムの外から監視するセキュリティ対策では不正に気付くことは難しい。乗っ取りというと SF 映画のような事態を想像するが、実際の事例では、そのパソコン内部に保存されているパスワードなどのアカウント情報を、特定のインターネットのサーバーにひそかに転送したり、インターネットから不正なプログラム(ウイルス)をひそかにダウンロードするなどがあげられる。地味に思えるが、それを起点にさらなる悪意のある活動に広がる可能性があり注意を要する。

ソフトウェアの乗っ取りに悪用されるかもしれないソフトウェア製品の脆弱性は毎週のように発見されている。脆弱性とは、製品のプログラムミスではないが(直接的な機能不良ではないが)、うっかり間違った操作をしたり悪用すれば想定外の動作をそのソフトウェアに行わせることができるソフトウェアの設計上の弱点のことである。Word や Excel のような大手のソフトウェア製品でもあり得るし、近所のベンダーが開発したプログラムでも乗っ取られる可能性がある。ローカルなプログラマーが作成したプログラムをわざわざ解析して乗っ取るなど、海外のハッカーが労力をかけるはずはなかろうと考えるがそうではない。IoT 関連のプログラマーの多くは、Microsoft 社のプログラム開発環境言語「. net(ドットネット)」を用いて開発している。この言語をもちいると、簡易な用語を記載するだけで、予め Microsoft 社が用意した処理を「.net」プログラムが解釈し CPU で実行する。この「.net」を実行するソフトウェアそのものにも乗っ取られる可能性のある脆弱性が見つかっており、頻繁に Microsoft 社は OS のセキュリティアップデートを呼び掛けている。すなわち、「.net」を用いたプログラム開発を業者に委託すれば、世界中の悪意のあるハッカーから、「.net」の脆弱性を用いて乗っ取りを実行し、他の会社や政府機関を攻撃する手足として悪用される可能性がある。

このような脆弱性は OS やソフトウェア製品をアップデートするしか対策はない。Windows OS やアプリケーションを生産現場で用いる際は、「便利になるから」「処理が速くなるから」「画面が大きくなるから」更新するという意識を捨て、「毎週見つかる脆弱性を改善するには更新しかない」と強く意識し、古い OS のパソコンが現場にあることは、イコール、「古くて劣化したワイヤーで荷物をつっている」位に危険な事だと啓発することが重要である。朝の RKY で認識を共有すれば、いかに古くてアップデートされていないパソコンが多いことが判るだろう。それが作業者の危険につながることを周知することで、現場から繰り返し強く意見や要望がでることにより、経営者の更新投資に対する意識も変化することにつながると期待したい。

(4)コンピュータも通信も間違える

日常的につかうパソコンやメールでは、海外など何千キロも離れた地点とファイルをやり取りしており、データが化けたり抜け落ちたりを感じることはない。このようなことから、現代の通信技術は特別信頼性が高いように一般的に思われるが、生産現場では特別な仕組みを用意しない限り、流れ

るデータのそれほどの信頼性はないことに注意すべきである。

メールやホームページの閲覧で、欠落なくデータがやってくるように感じるのは、データに欠落やエラーがある場合、再度の送信を要求する仕組みが経路の途中に細かく設置されているからである。生産現場でも、通信処理の周期が遅くてもよいシステムでは、このような仕組みを使うことはある。例えば工場長に昨日の実績を画面表示するような「見える化」処理には通信のエラーにより再送信する機能が備わっている可能性が高い。

しかしそのような「見える化」のために現場の PLC やセンサーからデータを高速で集約している場所、設備に近ければ近いほど、送信処理は1回ぽっきりのケースが多い。すなわち欠落したりエラーになると、前回の値で補完したり0を埋めるなどの処理が行われる。慎重な設計がなされた制御システムでは、エラーになったデータエリアに、数字ではない文字を埋めるなどの配慮をする。平均値を算出するなどの演算では、エラー文字のデータを母数から排除して統計計算を行うためである。多くの IoT の処理では、通信やメモリーのエラーで不正な値になると前回の値や0を使用することが多く、統計計算の信頼性は極端に劣化することが多い。そのような間違えたデータが 1 秒（1個）あれば、60 秒（60 個）の平均値は信頼置けなくなることは容易に想像できる。

これは、生産現場の制御装置では、高速のデータをリアルタイムで処理をしており、1 回（連続する毎秒データの内のどこかの1秒）が欠落しても、制御処理にそれほど影響を与えない特性があるからである。このようなデータの信頼性に対する処理の違いから、想定外のデータや結果が表示されることがありうる。電流や電圧を経由して数値を表示していた時代は、おかしな数値は故障であると直ちに考えたが、最新のパソコンの画面にグラフィカルに値が表示された場合、その数値の信頼性に疑いを持つことが難しい。またその結果、制御や保護の動作が異常になることもありうる。コンピュータは壊れたり、おかしな振舞いをするという前提で、労働災害に向き合う必要がある。画面に「停止中」の表示がされていても、深刻な労働災害が発生する可能性があるのであれば、コンピュータ画面の表示を危険エリアの立ち入りの基準にするのではなく、電源の切断の操作を各作業員が行ってから立ち入るルールにするなど、万一のコンピュータの誤動作を想定したオペレーションルールを作るべきである。

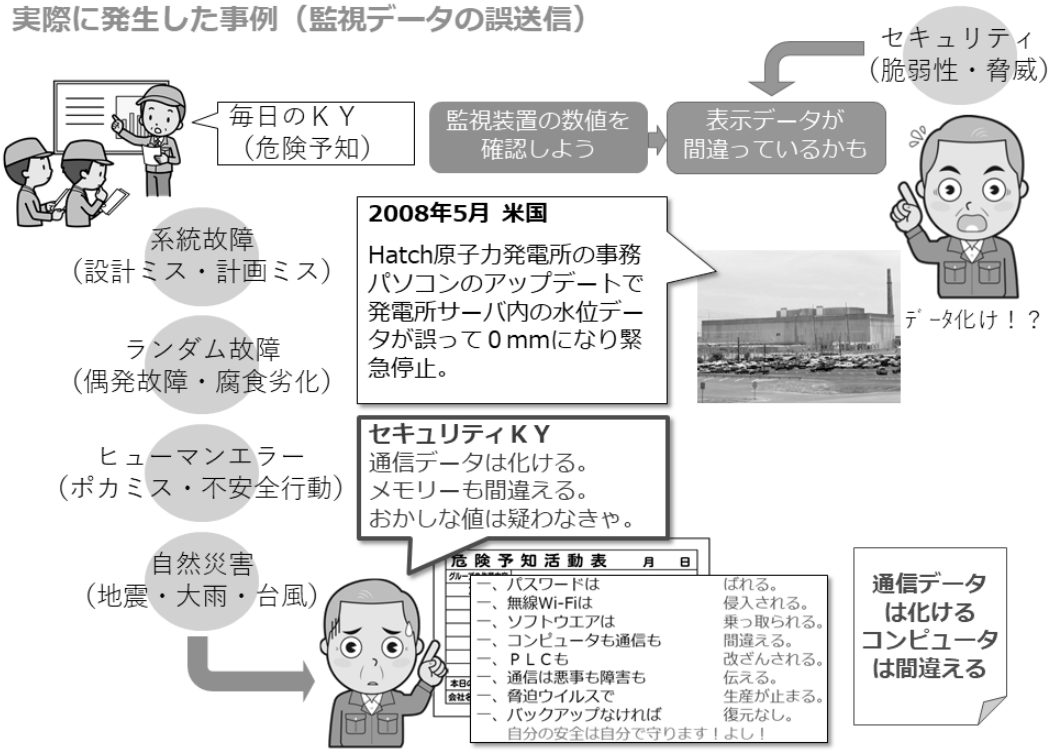


図 5-4 実際に発生した事例(監視データの誤送信)

過去に発生したトラブルでは、表示されたモータの回転方向が実際の現場遮断器と異なっており、意図しない方向に機械設備が動作したという事故がある。運用者がモータの動作方向を切り替える操作を与えた際の「切替え完了」の表示が、末端の遮断器の機械的な状態に基づくのではなく、経路の通信コンピュータが「切り替え信号を遮断器に信号出力した」という処理のアンサーバックであったために発生している。遮断器に至る信号線が劣化切断しており、通信コンピュータが信号出力処理を完了しても、遮断器そのものは切り替わっていなかった。このような「指令は出力した」というコンピュータの処理完了を設備の状態変更完了として表示するケースは多い。設備や機械の動作状態の変更を確認するためには、センサーを機械設備に新たに取り付け信号を読み込む装置を追加するなどコストがかかるからである。安全にかかわる判断が、コンピュータや通信に依存しすぎていないか、現場作業者とともに改めて RKY すべき事例である。

新しい設備や機械を設置する際は、制御と安全は分離し、かつ安全にかかわる表示やスイッチには冗長化対策や、前述の例でいえば末端の遮断器の動作状態をスイッチで別で読み込むなど慎重な設計を施す。しかし既存の機械設備を IoT と称して改造しながら便利な運用になるように拡張した場合、リスク分析が不足することで、結果的に災害が起こりやすい回路となっている可能性がある。現場 RKY をすることで、このような安全にかかわる信号や表示が適切なソースを持ってい

るのか、現場の運用に照らして見直すことを期待したい。

(5)PLC も改ざんされる

機械制御の PLC そのものは特殊な OS が使用されているケースが多く、それが一般的なハッキングの脅威にさらされるリスクはそれほど高くないと予想できる。しかしどのような特殊な制御コンピュータも、保守をしてパラメータや制御回路を変更したりバックアップを行うメンテナンス用端末は Windows 端末を用いるケースがほとんどである。このような場合、保守パソコンが乗っ取られたり改ざんされることで、間接的に PLC に搭載しているラダープログラムが書き換わったり入出力信号モジュールの信号変換倍数パラメータが不正に書き換わるなどし、異常な制御を行うことが想定される。

イランの核施設の遠心分離機を破壊した Stuxnet では、USB または WEB からパソコンに感染したウイルスが、遠心分離機の回転数制御を行う PLC の保守パソコンのプログラムを悪用し、不正な回転数制御プログラムを設定したと考えられている。

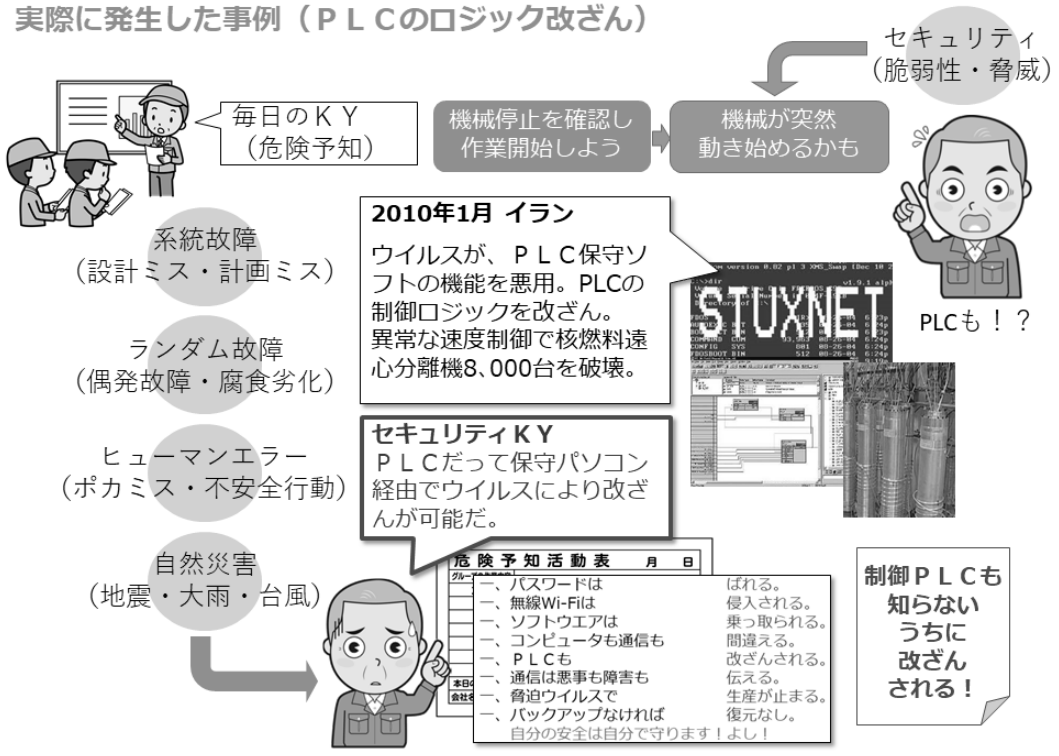


図 5-5 実際に発生した事例(PLC のロジック改ざん)

このような対策には一つには保守用のパソコンはネットワークに常時はつながず、電源を切断しておくことが最も容易な対策ではある。PLC へのログインパスワードをパソコンに記憶させないなど

の細かい対策も重要である。また PLC が納入された際のデフォルトのパスワードは必ず変更することも効果がある。PLC 本体に物理的な鍵でエンジニアリングやダウンロード機能のロックをする機能がある場合は必ず施錠し、エンジニアリングをする端末から物理的に遮断しておくことが望ましい。不正なプログラムがダウンロードされていないか、設備停止の際は予めバックアップしておいたラダープログラムと PLC 内のプログラムを比較するなど、制御プログラムの健全性を確認する作業を行うことは効果が高い。

安全を確保するための PLC のプログラムは、常時又は頻繁に動作するものではないため、改ざんされたことに気づき難い。すなわち、障害が潜在化しやすく、いざという時に適切に働かず、大きな災害につながる。本条項の RKY によって、現場の PLC や安全にかかわるシステムの設定やプログラムをバックアップと比較することを意識すれば、ハッカーやウイルスによる改竄のほか、誤操作や EMC によるパラメータ初期化などによる設定変更に対しても、潜在的な不安全状態に気付くきっかけとなることが期待できる。

(6)通信は悪事も障害も伝える

通信経路はハッカーが侵入する経路になったり、ウイルスが外部に情報を漏洩させる経路として使われるが、生産現場において通信経路は電気的なノイズ、EMC も含めたコンピュータ障害の原因やその影響を伝播させ他のコンピュータに影響を与える経路にもなりえる点を十分に認識し、IoT 時代のシステム構築をするべきである。

業務系と異なり、生産現場では大きなモータが起動停止することでサージも大きく発生する。理想的にはそのような電磁誘導系の設備と PLC や IOT パソコンは異なる変圧器の電源を使用してほしいし、感電防止の保安接地(アース)と信号シールドのための計装接地極とは別な接地極を使用すべきであるが、現実では大手メーカの工場も、変圧器が動力設備と制御計装設備で共通であることのみならず、保安用接地と計装接地の区別がついていない工場現場が多い。

このような場合、サージがイーサネットの信号線やシールド線の経路をたどって遠くの PLC のリセットを発生するなど、シールドそのものがアンテナとなり現場機器が EMC の影響を受ける可能性がある。一般に EMC の影響による障害は、原因を発見し改善することが極めて難しい。何年にもわたり不可思議な現象として向き合う必要がある。製造機械と一体で納められる制御機器は、動力からの影響なども考慮し繰り返し ECM 対策を行い製品化することが一般的である。しかし IOT で機械設備を横断したネットワークを工場運営側が独自に敷設した場合、データを集めるという機能にのみ着目するため、このような電磁系の障害に対する対策が不足することが多い。業務系の通信設備のインテグレータには、このような障害に対する知見が不足した業者が多く、オフィスのOA機器の設置と同じ感覚で、ノイズフィルタもサージアブソーバもなしに生産設備の現場にネットワー

ク機器を設置してしまう。注意が必要である。

また電気的なだけではなく論理的な障害も伝達することがある。過去に海外の発電所で発生した例では、制御ネットワークに接続された通信機器の電源装置がサージにより故障したことで、通信機器への直流電源ラインにのるリップルが過大となったことが原因となり、通信機器のイーサネット IC が故障し、ネットワーク上に膨大な量の ARP パケット（通常はパソコンなどをネットワークに接続するなどのごくまれなタイミングで極短時間やり取りされる通信装置間の通信処理）が発生し、接続している制御機器を麻痺させ制御不能となったケースがある。同様な例に IP パケットが大量に発生し、重要な設備の制御システムを停止させた海外の事例もある。これらはネットワークストームと呼ばれ、意味のないデータが大量に発生し送出されることで、接続している制御機器の処理を麻痺させることで大きな災害を引き起こす。ネットワークが機能安全における共通要因故障となりうる点を考慮すべきケースである。

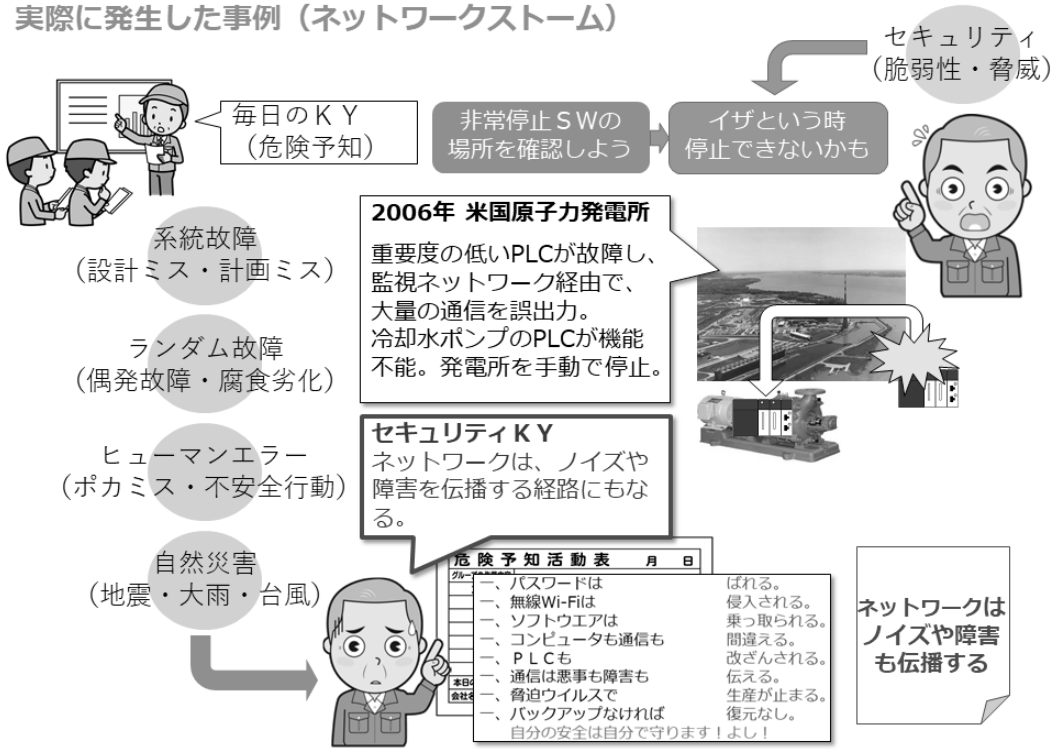


図 5-6 実際に発生した事例（ネットワークストーム）

もっと上位のファイルのやり取りの階層でも通信経路が問題となる場合が多い。共有フォルダがウイルスを運ぶ経路になりえるからである。業務系では、個人が保有する PC の共有フォルダは、会社サーバーにつながる形態がほとんどである。共有フォルダの実態はそもそも会社サーバー側にしかなく、個人の PC で感染した不正なファイルがあっても、サーバーの共有フォルダに移動し

た段階で検閲され無害化されることが多い。

一方で生産現場においてパソコンは、サーバーとクライアントいう厳格な構成ではなく、経路の途中にゲートウェイパソコン、集約パソコン、処理パソコンなどのように、処理段階に応じて分割されていることが多く、それらすべてが網目状にまたは数珠つなぎ的に共有フォルダでファイルを共有しているケースがある。そのようなケースでは、業務系のサーバー／クライアント型のシステムとは異なり、伝達経路が複雑で、ウイルスの伝達経路となった場合、駆除や対策を 1 か所で行っても他の PC より再び感染する可能性が常にあり、対策に時間を要することが予想される。

生産現場では極力 Windows の共有フォルダは使用を禁止することを推奨する。また通信も経路上に IP マスカレードの装置を入れるなど通信処理が一方通行になるような工夫を推奨する。

EMC レベルでもパケットレベルでも、さらに OS によるファイル共有のレベルでも、通信は有効な情報だけではなく、障害の原因や障害そのものも伝達する経路となることを周知し、本条項の RKY の際には、不用意にネットワークを接続している箇所はないのか改めて現場を見直すきっかけとなることを期待したい。

(7) 脅迫ウイルスで生産が止まる

海外の事例でも近年脅迫ウイルスが増加している。実際に金銭を要求するケースもあるが、そのふりをしながらも実際は解除する方法がなく、実質的には操業停止を狙ったテロと思えるウイルスも発見されている。また高度な脅迫ウイルスは、市販のセキュリティ製品を回避する方法を持つウイルスも発見されている。

脅迫ウイルスは、パソコンのハードディスクを強制的に暗号化し画面をロックして使用不能にしつつ、画面に金銭を要求数する文字を表示する。個人のパソコンが被害にあった場合、自分が作ったファイルや文書がすべてアクセスできなくなり、とてもつらい思いをする。

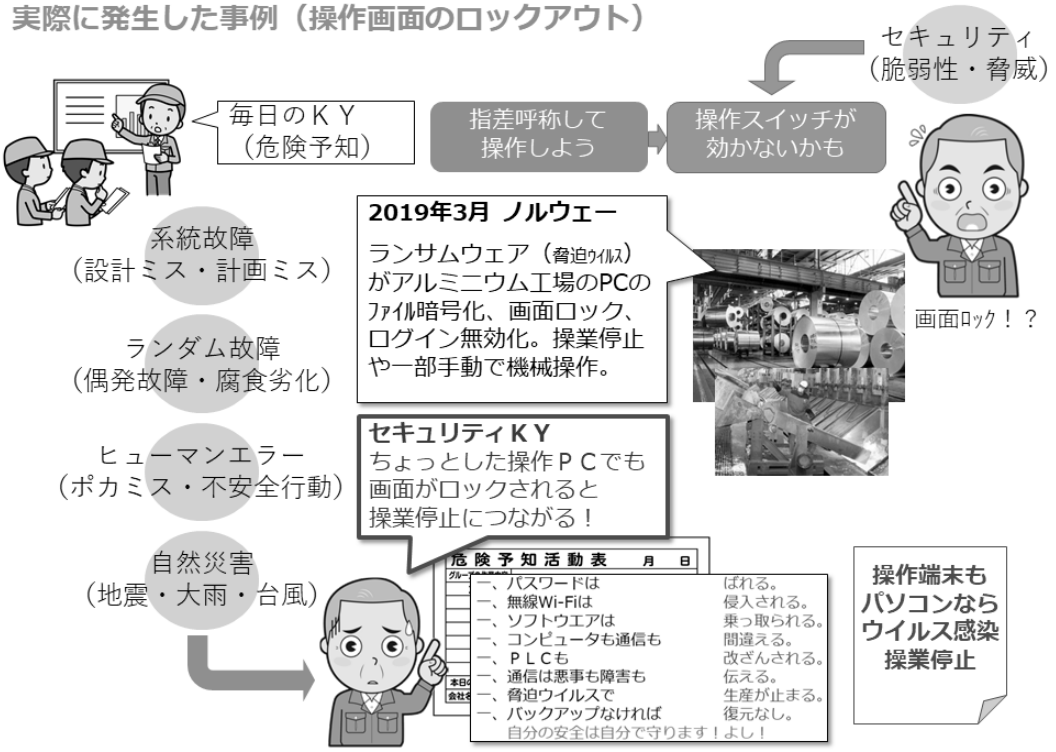


図 5-7 実際に発生した事例（操作画面のロックアウト）

生産現場では、特別に重要なファイルがハードディスクに無くても、画面がロックされるだけでも大きな被害が予想される。たとえば生産ラインのアンドンやタクトを知らせる表示装置の画面がロックされたり、品番のバーコードを印刷するプリンターのパソコンがロックされるだけで、生産活動を中断せざるを得ない可能性が高い。脅迫ウイルスは、ハードディスクに大切なデータが入っていなくても、生産現場では深刻な被害を生むこと十分に周知し、万一にもウイルスに感染しないように心がけるべきである。

(8)バックアップなければ復元なし

業務系では、定期的に夜間にサーバデータのバックアップを取ることは一般的である。しかし生産現場では、様々なコンピュータがあるにもかかわらず、バックアップ取得がおろそかになりがちである。これは連続的に使用する装置であり、また表示だけ、通信だけの処理パソコンも多くあるため、キーボードやマウスで、ファイルをバックアップ操作する行為ができないケースもあるためである。

生産現場でウイルス感染した場合、復旧に時間がかかる理由の一つに、システムのバックアップが適切に保存されていないケースが多い。たとえば業務系であれば、マイドキュメントの Word や Excel ファイルをバックアップしておけば、万一手元のパソコンが被害にあっても、新しいパソコン

が入手できれば、すぐに該当の Word ファイルや Excel ファイルを開き作業することができ、大きな問題は感じない。

しかし生産現場で使われているパソコンで動作しているプログラムが、どのような設定ファイルを必要としているのか、マイドキュメントのフォルダだけをバックアップしておけば問題ないのかは、そのシステムを構築したベンダーやプログラマーの指示に従う必要がある。制御関連に必要なファイルの多くは、C ドライブ直下に専用のフォルダを用意していることも多い。また、新しいパソコンに復元した場合、その最新の Windows で、数年前に業務委託して開発したプログムをインストールできるのか不明である。最新版のプログラムがインストールできても、バックアップした古いデータファイルを読み込めるかは不明な場合もある。このようなことから、重要な装置であればファイルだけではなく、動作させるパソコン本体も含めてバックアップを用意しておく必要がある。データも、OS も含めたバックアップは 1 年に一回、毎日の作業結果を反映するバックアップは毎日、などのように、範囲に応じてバックアップを取得するインターバルも設定するべきである。さらに言えば、防災訓練同様、1 年に 1 度は、そのような事態を想定した復元の予行演習をすることも推奨したい。すべての現場システムを一度に復元する訓練をすることは、生産現場の負担が大きいが、毎年訓練対象を決めて取り組むことが可能であろう。

業務系では情報として「文書」が保護されることを目的としてバックアップを行うが、生産現場においては目の前で動作しているシステムを復元するためにバックアップを行う。データファイルだけではなく、重要なシステムであればハードウェアすなわちパソコン本体そのものも予備を保管しておく必要がある。前述のような脅迫ウイルスに感染し発病した場合、バックアップの備えをしていなければ、システムを復元することは難しい。

この条項に基づく RKY によって、バックアップや予備品の準備がないシステムはないか、生産設備としてクリティカルなシステムにそのような抜けはないのか、気づきにつながることを期待したい。

(9) 自分の安全は自分で守ります

以上コンピュータや通信が引き起こしかねないリスク(脆弱性)の代表的なものを列記した。
現場での作業前には、毎日必ず本 8 項目を唱和し、その日の作業に関係するシステムを想像し、RKY ボードに懸案事項や、注意事項を記載し、関係者で共有することを推奨する。対策には現場の担当者だけでは難しい場合もある。管理者は、より上層部に問題意識を訴えセキュリティのインシデントが、労働災害につながらないようにするべきである。

その第一歩が、現場の作業員ひとりひとりの気づきあること認識し、自分の安全を守ることと同列に、セキュリティリスクを洗い出し対策する力を続けることが大切である。

6. 人と協調作業を行う機械におけるリスクや安全性確保の考え方

現在、ICT を利用した生産システムの革新、また人と機械の間の物理的なバリア等を撤去し、人と機械が協調して作業を行うロボット等が出現してきており、生産システムに対する考え方のパラダイムシフトが起ころうとしている。このような生産システムの新しい時代において、これまでの安全性確保の考え方や技術だけでは対応が困難な状況に対して、現状の課題と今後の方向性についての検討の一環として、人と協調作業を行う機械におけるリスクや安全性確保の検討を行うにあたり、協働ロボットの開発と利用状況について調査を行った。

2017 度は、協働ロボットの設計開発の側面から、長年にわたって産業用ロボットを開発してきた我が国の製造事業者で、協働ロボットの開発にも実績を有する企業のロボット開発本部に対して、ヒアリング調査を行った。2018 年度は、利用の側面からの状況について把握するために、協働ロボットを利用したシステム構築を担当するシステムインテグレーターに対して、協働ロボットを利用したシステム構築における安全性確保の考え方についてヒアリング調査を行った。

2019 年度は、ロボットに関する安全資格制度や協調安全ロボットシステム事例について、公開情報に基づきトピックスを整理した。

(1)ロボット安全資格制度

世界の産業用ロボット販売台数は 2017 年には全世界で推定 35 万台(うち日本製ロボットは 20 万台)まで増加している[12]。産業用ロボットに関する安全については、ISO 10218(2011)に対応して、国内規格の JIS B 8433(2015)「ロボット及びロボット装置−産業用協働ロボットのための安全要求事項−」が改訂発効されている[13]。また、産業用ロボット運用時の安全、つまり製造業等の事業者が行うべき安全管理やマネジメントは、労働安全衛生法や労働安全マネジメント規格 ISO 45001 で規定されている[14]。さらに、人とロボットが連携し安全環境を確保する協調安全〈Safety2.0〉の新しいコンセプトも提唱されている[15]。

今後、協働ロボットなど、産業用ロボットの適用がさまざまな形態に発展していく中で、労災事故防止のためには、ロボットメーカー、システムインテグレーター、エンドユーザが、リスクアセスメントやリスク低減手法を互いに共有し、安全確保のために連携することが重要となる。

---

12 経済産業省・第1回 ロボットによる社会変革推進会議資料 3:「ロボットを取り巻く環境変化等について」2019 年 5 月 8 日

13中央労働災害防止協会「機能安全活用実践マニュアル ロボットシステム編」(平成 29 年度厚生労働省委託機能安全を活用した機械設備の安全対策の推進事業)平成 30 年 3 月

14 同上

15 向殿政男・日本機械工業連合会・浜離宮朝日ホール講演会「機械安全に係わる新たな動き」、「機械と人間との協調安全に向けて」2017 年 3 月 9 日

このような背景から、ロボットシステムの安全性確保に必要な知識、能力を保有することを認証する要員認証制度として、一般社団法人セーフティグローバル推進機構（IGSAP）が 2018 年度に「ロボットセーフティアセッサ資格制度」を創設している。これは一般社団法人日本電気制御機器工業会（NECA）の機械安全全般をカバーしているセーフティアセッサ資格制度をベースに、ロボットシステムの安全に関する知識の保有を付帯して認証するものであり、日本認証株式会社が制度運営を行っている[16]。試験内容は、ロボットの安全規格(JIS B 8433-1, JIS B8433-2 および TS B0033)とロボットの安全関連部の設計・構築に関する知識(製品知識を含む)となる[17]。

（2）協調安全ロボットシステム事例

上記のロボットセーフティアセッサ資格を多数保有する IDEC グループ（IDEC ファクトリーソリューションズ株式会社）では、生産性と安全性を両立する「協調安全ロボット」システムインテグレーターとして生産現場向けのソリューションを提供している。

2014 年の規制緩和に伴い、産業用ロボットが安全柵なしに作業者と協働することが可能になり、リスクアセスメントに基づいた安全方策を講ずることにより、人とロボットの作業領域が分断されることなく、協調・協働できるようになった。

IDEC グループが所有する協調安全ロボットテクニカルセンターは、協働ロボット導入の活用方法や安全なシステム構築方策を提供するための活動拠点として、以下のような主要な協働ロボットや産業用ロボットを使用した安全柵なしのシステムを見学できる[18]。

KUKA（ドイツ）：繊細な組立て作業用の軽量構造ロボット。可搬重量7kg の LBR iiwa 7 R800

JAKA（中国）：低価格が特徴。可搬重量 7kg の Zu7、12kg の Zu12 の 2 機種

Universal Robots（デンマーク）：生産ラインの変更にもスムーズに対応できる UR-3/-5/-10

安川電機（日本）：外部からあらかじめ設定した制限値を超える力を検出すると自動で停止する「人協働モード」を備えている MOTOMAN-HC10

ファナック（日本）：小型協働ロボット CR-7iAL

三菱電機（日本）：オプションにより安全柵なしで人と協働できる協働ロボット化が可能な高回転・高トルク出力の MELFA RV-7F

MiR（デンマーク）：人や障害物を自動的に回避し自律走行することが可能な積載重量 100kg の MiR100 と積載重量 1000kg の MiR1000 の 2 機種

16 一般社団法人セーフティグローバル推進機構、一般社団法人日本電気制御機器工業会、日本認証株式会社の各 HP より

17 日本認証株式会社 HP より

18 IDEC 協調安全ロボットテクニカルセンターHP より

7. 今後の課題

生産システムに ICT を導入すると、新たにセキュリティ脅威が発生する。脅威は、情報漏洩委だけでなく、工場の操業妨害や機械の安全性にまで影響を与える。そのため、生産システムの技術者は、安全面まで考慮したセキュリティ対策を余儀なくされる。本書では、機械安全のリスクアセスメントを理解している技術者に向けて、セキュリティのリスク分析および対策の検討方法について、解説した。

しかし、残念ながら本書だけでセキュリティと安全対策に十分な知識が得られるわけではない。生産システムのセキュリティに関しては、IEC 62443 等の標準に従わなければならないし、もちろん ISO 12100 や ISO 13849-1 機械安全規格にも適合しなければならない。また、セキュリティ分析と対策立案には、セキュリティ脅威や脆弱性の知識、最新の対策技術等の知見が必要である。これらの制御システムセキュリティに関する知見や教科書は、IPA などから出版されているので、そちらを参考にしてほしい。もし、生産システムのセキュリティに関するセミナーやカリキュラムを、機械系工業会に求められるなら、今後の検討課題としたい。

また、本書ではセキュリティリスク分析と対策のいくつかの事例について解説したが、対象とした生産システムも脅威もごく一部であり、脅威や脆弱性と対策について網羅的な分析と列挙を行ったわけではない。セキュリティリスクアセスメントも安全リスクアセスメントと同様、機械システムの使用方法や制限に強く依存する。従って、安全でセキュアな ICT 技術導入のためには、機械種類や ICT サービス・サブシステムごとに、典型的なセキュリティ分析と対策例を示した分野事例(ケーススタディ)が出版され多くの技術者に参照されることが望ましい。分野事例集の作成には時間を要するが、我々の将来課題として検討したい。

参考文献

ISO

ISO 12100: 2010: Safety of machinery - General principles for design — Risk assessment and risk reduction

ISO 11161: 2007: Safety of machinery - Integrated manufacturing systems – Basic requirements

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

ISO 31000:2018 Risk management — Guidelines

IEC

IEC TS 62443-1-1:2009: Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models

IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program

IEC TR 62443-3-1:2009: Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems

IEC 62443-3-3:2013: Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

IEC/TR63074: 2019: Safety of machinery - Security aspects related to functional safety of safety-related control systems

ISO/IEC

ISO/IEC 27001: 2013:　Information technology - Security techniques - Information security management systems - Requirements

ISO/IEC 30147(開発中): Information technology - Internet of things - Methodology for trustworthiness of IoT system/service

ISO/IEC ガイド

Guide 51: 2014: Safety aspects — Guidelines for their inclusion in standard

関連団体発行文書

経済産業省

2018 年版ものづくり白書 2018 年 5 月 29 日

(https://www.meti.go.jp/report/whitepaper/mono/2018/honbun_pdf/index.html)

2019 年版ものづくり白書 2019 年 6 月 11 日

(https://www.meti.go.jp/report/whitepaper/mono/2019/honbun_pdf/index.html)

第 1 回 ロボットによる社会変革推進会議 資料 3 「ロボットを取り巻く環境変化等について」

2019 年 5 月 8 日

(https://www.meti.go.jp/shingikai/mono_info_service/robot_shakaihenkaku/pdf/001_03_00.pdf)

内閣府

第 5 期科学技術基本計画（Society 5.0） 2016 年 1 月 22 日

(https://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf)

内閣サイバーセキュリティ センター(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 2016 年 8 月 26 日

(https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf)又は

(https://www.nisc.go.jp/materials/index.html)

日本電気協会 電気用品調査委員会

遠隔操作に対する技術基準の解釈の追加要望 2013 年 3 月 8 日

(http://www.eam-rc.jp/pdf/result/remote.pdf)

遠隔操作採用時のリスクアセスメント手順書 ～家庭用エアコンの事例～ 2019 年 11 月 18 日

(http://www.eam-rc.jp/pdf/result/remote_risc_asses.pdf)

中央労働災害防止協会

機能安全活用実践マニュアル ロボットシステム編 2018 年 3 月

(https://www.mhlw.go.jp/file/06-Seisakujouhou-11300000-Roudoukijunkyokuanzeneiseibu/0000197860.pdf)
よくわかるリスクアセスメント―グローバルスタンダードの安全を構築する
向殿政男(著) 2017 年 11 月
安全設計の基本概念―ISO/IEC Guide51(JIS Z 8051)、ISO 12100(JIS B 9700) (安全の国際規格)、向殿政男(監修) 2007 年 5 月

IPA – 独立行政法人情報処理推進機構
制御システム セーフティ・セキュリティ要件検討ガイド 基本編 第 1 版 2018 年 3 月
(https://www.ipa.go.jp/files/000064728.pdf)
制御システム セーフティ・セキュリティ要件検討ガイド ケーススタディ編 第 1 版 2018 年 3 月 (https://www.ipa.go.jp/files/000064729.pdf)

日本機械工業連合会
メーカのための機械工業界リスクアセスメントガイドライン 2010 年 3 月 31 日
(http://www.jmf.or.jp/japanese/standard/pdf/hyojun_guideline.pdf)
安全な生産システムの構築能力向上のための調査研究報告書 2017 年 3 月
(http://www.jmf.or.jp/content/files/houkokusho/28nendo/28jigyo_01s.pdf)
講演会「機械安全に係わる新たな動き」講演資料
「機械と人間との協調安全に向けて」向殿政男 2017 年 3 月 9 日
(http://www.jmf.or.jp/content/files/hyoujunka/syu3109_h01.pdf)

NIST - National Institute of Standards and Technology
NISTIR 8183 Rev. 1: Cybersecurity Framework Version 1.1 Manufacturing Profile Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (2020) (https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1-draft.pdf)
NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (2019)
(https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf)

ANSI －American National Standards Institute

B11.TR9-2019 : Guidance to Machinery Manufacturers for Consideration of Related IT-Security (Cyber Security) Aspects

お わ り に

ここ 20 数年の間の情報通信技術の発展と普及により、情報の流れ方とスピードが大きく変わり、製造業に限らず仕事の進め方は、大きく変化してきた。最近は、PC やスマートフォンのような情報機器に限らず、様々なものがネットワークに接続されてきている。これらのいわゆる IoT の拡大により、今まで以上に急速なスピードで、新しい情報技術の利用が進んでいくものと考えられる。あまりの急激な変化により、その複雑さが限度を超えて、人間がコントロールできる境界を遥かに超えてしまうことについても検討が必要とされる。

機械製造業においても、一連の統合生産システムはロボットを含む複数の機械装置で構成され、相互にネットワークで接続することで生産情報の共有とコントロールが行われる世界になってきている。その接続は、工場内にとどまらず、事業所間、あるいは企業間での情報交換・共有に利用されるようになり、グローバルな生産体制の一部を形成する時代が、すぐそこに迫ってきていると考えられる。そのような時代においても、安全性（セーフティ）の確保は第一に考えられなければならないが、複雑な情報ネットワークのどこかに、少しでもセキュリティの問題が存在していると、それは従来には存在しなかったリスクとして、生産システムの安全性を大きく低下させる可能性を有している。

本事業では、そのような生産システムの安全性に関わるセキュリティの問題への対応を、セーフティとの両立を図りつつ確保していくための方策を検討するために、「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部会」（以下、研究部会）を設置し検討を行った。今回の活動が、日本における機械安全レベルの向上に、多少なりとも貢献することができれば幸いである。

研究部会の主査、副主査並びに委員の方々に深く感謝するとともに、今後の活動につきましても同様のご協力をお願いする次第です。

付　録

付録 A-用語の解説

付録 B-セキュリティリスクアセスメント表

付録 C-セキュリティリスクアセスメントの事例

付録 D-生産現場におけるセキュリティリスク KY のアプローチ

付録 E-生産システムのセキュリティインシデント事例

付録 F-作業委託報告書（議事録等を含む）

付録 A-用語の解説

生産システムにおけるセキュリティの脅威を検討するにあたって、関連する用語および基本概念を明確にする。基本的に既存の JIS 等の用語定義と同じであるが、ここでは「安全」をセーフティとセキュリティの両方のリスクが許容可能であると定義している。

(1)リスク

危害の発生確率と危害のひどさとの組合せ[JIS B 9700:2013 3.10]

注　人が利用・使用する機械・設備・システムにおいて発生する事故の「被害の発生頻度と被害のひどさ」から導かれる値(レベル)

(2)リスクアセスメント

リスク分析及びリスク評価を含む全てのプロセス。[JIS B 9700:2013 3.17]

例　事故のシナリオや発生メカニズム分析から、該当箇所(ハザード)のリスクを推定すること

(3)許容可能なリスク

現在の社会の価値観に基づいて，与えられた状況下で，受け入れられるリスクのレベル[JIS Z 8051:2015 3.15]

注　関係者がその機械・設備等から得られる便益や利益を考慮して、リスク低減の手段を設けずに引き受けることができるリスクのレベル。関係者の業界、地域および時代によって、許容可能なレベルは変わる。

(4)リスク低減方策、保護方策

ハザードを除去するか，又はリスクを低減させるための手段又は行為。[JIS Z 8051:2015 3.13]

注　一般に、工学的あるいは運用的手段によって、リスクを許容可能な程度まで低減すること

(5)セーフティ(防災)

許容不可能なリスクがないこと。[JIS Z 8051:2015 3.14]

注　上記定義は一般的な安全に関する定義であるが、ここでは偶発的または経年的な機械の故障、(悪意のない)ヒューマンエラーや自然災害等によるリスクに限定する

(6)セキュリティ(防犯)

情報の機密性，完全性及び可用性を維持すること。 [JIS Q 28000:2019 3.28]

注 さらに，真正性，責任追跡性，否認防止，信頼性などの特性を維持することを含めることもある。

注　本書では、セーフティとの対比のために、悪意を持った人的行為および影響、意図したヒューマンエラーや犯罪行為によるリスクが許容可能であることを意味する。以下の定義に準じる。

- prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system [IEC] 62443-1-1:2009 3.2.99 e)]

(7)安全

セーフティ(防災)とセキュリティ(防犯)の両方のリスクが許容可能であること。[original]

注　この語のみ、他の規格の「安全(safety)」とは違う意味で用いる。対応する英語は(safety and security)である。

付録 B-セキュリティ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(運旧)	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損雄	小	中	中
1.1.1.3								制御CPUがネットワーク処理兼用（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

1.1.3					人的被害 装置損壊	安全保護装置が無効化され、保護機構が喪失する。	Triton/Trisis			高	小	中				高	小	中
1.1.3.1								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）			高	小(無)	中
													EXEのホワイトリスト制御			高	小(無)	中
														安全保護装置の代替装置(バックアップ)を設置		中	小	中
															Windows環境の再インストールとバックアップ	高	小(無)	中
															定期的なエンジツールのアップデート	高	小(無)	中
1.1.3.2								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（全台）			高	小(無)	中
													EXEのホワイトリスト制御			高	小(無)	中
														安全保護装置の代替装置(バックアップ)を設置		中	小	中
															定期的なエンジツールのアップデート	高	小(無)	中
															定期的な制御システムパラメータのレビュー	高	小(無)	中
1.1.3.3								遠隔からの不正プログラムのダウンロード	ハッカー ウイルス				FireWall (IPフィルタ)設置			高	小(無)	中
														安全保護装置の代替装置(バックアップ)を設置		中	小	中
															定期的な制御システムパラメータのレビュー	高	小(無)	中
															遠隔操作の禁止	**小**	**小(無)**	**小**
1.1.4					生産情報漏洩	射出成型機など原料と機械機構や温度調整の設定や動作時間が漏洩し製造ノウハウが流出。	中国ファーウェイ（笑）			小	小	小				小	小	小
1.1.4.1								インターネットなど外部につながる伝達経路	ウィルス（感染） 通信装置そのもの				ネットワークを多層分離し、FWやフィルタを設置。流出パケットを常時監視。	既存の設備で後から対策するするのは難しい。（コストがかかる。）専門技術者が必要。	インターネットにつなげる末端には最低FWを入れて特定のIPアドレス（認証済みドメイン）のみへの送受信に限定する。			
1.1.4.2								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） ホワイトリスト制御	アップデートもホワイトリストも別装置での準備が必要。（コストが高い）	定期的なウイルスチェック（全台）			
1.2			遠隔接続（監視）	動力源ON。機械の動作状態を通信によって遠隔地に送信している。														
1.2.1					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	高	高				中	高	高
1.2.1.1								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	中	中
													EXEのホワイトリスト制御			中	小	中
														なし		中	高	高
															Windows環境の再インストールとバックアップ	小	高	中

1.2.1.2								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	中	中
													FireWall設置			中	中	中
														RDT禁止		小	小	小
															RDT操作のundo網羅	小	高	中
1.2.1.3								制御CPUがネットワーク処理兼用（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	中	中
														外部ネットワーク遮断		小	高	中
															ネットワーク遮断後の別回線使用	小	高	中
1.2.1.4								遠隔監視用接続機器（パソコン等）の管理不足	ウイルス（感染）				定期的なWindowsアップデート（全台）			中	中	中
													EXEのホワイトリスト制御			中	小	中
														なし		中	高	高
															Windows環境の再インストールとバックアップ	小	高	中
															定期的なエンジツールのアップデート	中	中	中
1.2.2					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	高	高				中	高	高
1.2.2.1								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	中	中
													EXEのホワイトリスト制御			中	小	中
														なし		中	高	高
															Windows環境の再インストールとバックアップ	小	高	中
1.2.2.2								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（全台）			中	中	中
													EXEのホワイトリスト制御			中	小	中
														安全保護装置の代替装置(バックアップ)を設置		小	高	中
															定期的なエンジツールのアップデート	中	中	中
															定期的な制御システムパラメータのレビュー	中	中	中
1.2.2.3								保護装置CPUがネットワーク処理兼用（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	中	中
														外部ネットワーク遮断		小	高	中
															ネットワーク遮断後の別回線使用	小	高	中
1.2.2.4								遠隔監視用接続機器（パソコン等）の管理不足	ウイルス（感染）バックドア				定期的なWindowsアップデート（全台）			中	中	中
													EXEのホワイトリスト制御			中	小	中
														なし		中	高	高
															Windows環境の再インストールとバックアップ	小	高	中
															定期的なエンジツールのアップデート	中	中	中

1.2.3					人的被害 装置損壊	安全保護装置が無効化され、保護機構が喪失する。	Triton/Trisis			高	高	高				高	高	高
1.2.3.1								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）			高	中	高
													EXEのホワイトリスト制御			高	中	高
														安全保護装置の代替装置(バックアップ)を設置		小	高	中
															Windows環境の再インストールとバックアップ	小	高	中
															定期的なエンジツールのアップデート	中	中	中
1.2.3.2								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（全台）			高	中	高
													EXEのホワイトリスト制御			高	中	高
														安全保護装置の代替装置(バックアップ)を設置		小	高	高
															定期的なエンジツールのアップデート	小	中	中
															定期的な制御システムパラメータのレビュー	中	中	中
1.2.3.3								保護装置CPUがネットワーク処理兼用（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			高	小	中
														外部ネットワーク遮断		小	高	中
															ネットワーク遮断後の別回線使用	小	高	中
1.2.3.4								遠隔からの不正プログラムのダウンロード	ハッカー ウイルス				FireWall (IPフィルタ)設置			高	小	中
														安全保護装置の代替装置(バックアップ)を設置		小	高	高
															定期的な制御システムパラメータのレビュー	中	中	高
															遠隔操作の禁止	**小**	**小**	**小**
1.2.3.5								遠隔監視用接続機器（パソコン等）の管理不足	ウイルス（感染） バックドア				定期的な Windowsアップデート（全台）			高	中	高
													EXEのホワイトリスト制御			高	中	高
														なし		高	高	高
															Windows環境の再インストールとバックアップ	小	高	中
															定期的なエンジツールのアップデート	中	中	中
1.2.4					生産情報漏洩	射出成型機など原料と機械機構や温度調整の設定や動作時間が漏洩し製造ノウハウが流出。	中国ファーウェイ（英）			小	中	中				小	中	中
1.2.4.1								インターネットなど外部につながる伝達経路	ウィルス（感染） 通信装置そのもの				対称ゾーンを深層部に配置 (Zone Conduit)			小	小	小
													Firewall設置 (IPフィルタ)			小	小	小
													IDSによる監視			小	小	小
														制御システムへのアクセス制御		小	小	小
															エンジニアリングのアクセス制御設定	小	小	小

1.2.4.2								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）			小	小	小
													EXEのホワイトリスト制御			小	小	小
														安全保護装置の代替装置(バックアップ)を設置		小	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	小	小	小
1.2.4.3								遠隔監視用接続機器（パソコン等）の管理不足	ウイルス（感染） バックドア				定期的なWindowsアップデート（全台）			小	小	小
													EXEのホワイトリスト制御			小	小	小
														なし		小	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	小	小	小
1.2.4.4								遠隔監視用接続機器（ルータやFWなど）の管理不足	バックドア				定期的なF/Wアップデート			小	小	小
													定期的な設定確認/変更			小	小	小
														なし		小	中	中
															なし	小	中	中
1.3			現場エンジニアリング	動力源OFF。現場で設定を変更作業を実施している。														
1.3.1					生産情報漏洩	射出成型機など原料と機械機構や温度調整の設定や動作時間が漏洩し製造ノウハウが流出。	中国ファーウェイ（笑）			小	小	小				小	小	小
1.3.1.1								インターネットなど外部につながる伝達経路	ウィルス（感染） 通信装置そのもの				ネットワークを多層分離し、FWやフィルタを設置。流出パケットを常時監視。	既存の設備で後から対策するするのは難しい。（コストがかかる。）専門技術者が必要。	インターネットにつながる末端には最低FWを入れて特定のIPアドレス（認証済みドメイン）のみへの送受信に限定する。			
1.3.1.2								保全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） ホワイトリスト制御	アップデートもホワイトリストも別装置での準備が必要。（コストが高い）	定期的なウイルスチェック（全台）			
1.3.2					不正設定	保全パソコン内部のエンジニアリングデータがすでに書き換わっており、保守の際に現場装置を書き換えてしまう。（インシデントは立ち上げ時に発覚）	Stuxnet			中	中	中				中	中	中
1.3.2.1								保全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	中
														安全保護装置の代替装置(バックアップ)を設置		小	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	小	中	中
1.3.2.2								エンジニアリングデータのバックアップ管理が不完全	ウィルス（感染） 保守員（誤操作）				なし			中	中	中
														なし		中	中	中
															エンジニアリングデータの自動バックアップ	小	中	中
															エンジニアリングのログ分析	小	中	中

1.4			遠隔接続（変更）	動力源OFF。遠隔地からの指令でデータ送信や変更作業を実施している。													
1.4.1					生産情報漏洩	射出成型機など原料と機械機構や温度調整の設定や動作時間が漏洩し製造ノウハウが流出。	中国ファーウェイ（笑）			小	中	中				小	中	中
1.4.1.1								インターネットなど外部につながる伝達経路	ウィルス（感染） 通信装置そのもの				対称ゾーンを深層部に配置(Zone Conduit)			小	小	小
													Firewall設置(IPフィルタ)			小	小	小
													IDSによる監視			小	小	小
														制御システムへのアクセス制御		小	小	小
															エンジニアリングのアクセス制御設定	小	小	小
1.4.1.2								保全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）			小	小	小
													EXEのホワイトリスト制御			小	小	小
														安全保護装置の代替装置(バックアップ)を設置		小	小	小
															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	小	小	小
1.4.1.3								遠隔監視用接続機器（パソコン等）の管理不足	ウイルス（感染） バックドア				定期的なWindowsアップデート（全台）			小	小	小
													EXEのホワイトリスト制御			小	小	小
														なし		小	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	小	小	小
1.4.1.4								遠隔監視用接続機器（ルータやFWなど）の管理不足	バックドア				定期的なF/Wアップデート			小	小	小
													定期的な設定確認/変更			小	小	小
														なし		小	中	中
															なし	小	中	中
1.4.1.5								遠隔からの業者ログインのルールの未整備（セキュリティポリシの未整備）	遠隔業者				アクセス制御装置の設定			小	小	小
													IDSによる監視			小	小	小
														なし		小	中	中
															エンジニアリングのアクセス制御設定	小	小	小
															エンジニアリングのログ分析	小	小	小
1.4.2					不正設定	保全パソコン内部のエンジニアリングデータがすでに書き換わっており、保守の際に現場装置を書き換えてしまう。（インシデントは立ち上げ時に発覚）	Stuxnet			中	中	中				中	中	中
1.4.2.1								保全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	中
														安全保護装置の代替装置(バックアップ)を設置		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	中	中

1.4.2.2								エンジニアリングデータのバックアップ管理が不完全	ウィルス（感染） 保守員（誤操作）				なし			中	中	中
														なし		中	中	中
															エンジニアリングデータの自動バックアップ	小	中	中
															エンジニアリングのログ分析	中	小	中
1.4.2.3								遠隔監視用接続機器（パソコン等）の管理不足	ウイルス（感染） バックドア				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	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
1.4.2.4								遠隔監視用接続機器（ルータやFWなど）の管理不足	バックドア				定期的なF/Wアップデート			中	小	中
													定期的な設定確認/変更			中	小	中
														なし		中	中	中
															なし	中	中	中
1.4.2.5								遠隔からの業者ログインのルールの未整備（セキュリティポリシの未整備）	遠隔業者				アクセス制御装置の設定			中	小	中
													IDSによる監視			中	小	中
														なし		中	中	中
															エンジニアリングのアクセス制御設定	中	小	中
															エンジニアリングのログ分析	中	小	中
1.5			再立上げ	動力源OFF→ON。機械を動作状態に立ち上げる。														
1.5.1					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				中	中	中
1.5.1.1								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	中
														安全保護装置の代替装置(バックアップ)を設置		小	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
1.5.1.2								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網雄	小	中	中
1.5.1.3								制御CPUがネットワーク処理兼用（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

1.5.2					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	中	中				中	中	中
1.5.2.1								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	中
														安全保護装置の代替装置(バックアップ)を設置		小	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
1.5.2.2								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
1.5.3					人的被害 装置損壊	安全保護装置が無効化され、保護機構が喪失する。	Triton/Trisis			高	小	中				高	小	中
1.5.3.1								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）			高	小(無)	中
													EXEのホワイトリスト制御			高	小(無)	中
														安全保護装置の代替装置(バックアップ)を設置		小	小	小
															Windows環境の再インストールとバックアップ	小	小	小
															定期的なエンジツールのアップデート	高	小(無)	中
1.5.3.2								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			高	小(無)	中
													EXEのホワイトリスト制御			高	小(無)	中
														なし		高	小	中
															定期的なエンジツールのアップデート	高	小	中
															定期的な制御システムパラメータのレビュー	高	小	中
1.5.3.3								遠隔からの不正プログラムのダウンロード	ハッカー ウイルス				FireWall (IPフィルタ)設置			高	小(無)	中
														安全保護装置の代替装置(バックアップ)を設置		小	小	小
															定期的な制御システムパラメータのレビュー	高	小(無)	中
															遠隔操作の禁止	小	小	小
1.5.4					生産情報漏洩	射出成型機など原料と機械機構や温度調整の設定や動作時間が漏洩し製造ノウハウが流出。	中国ファーウェイ（笑）			小	小	小				小	小	小
1.5.4.1								インターネットなど外部につながる伝達経路	ウィルス（感染） 通信装置そのもの				ネットワークを多層分離し、FWやフィルタを設置。流出パケットを常時監視。	既存の設備で後から対策するするのは難しい。（コストがかかる。）専門技術者が必要。	インターネットにつなげる末端には最低FWを入れて特定のIPアドレス（認証済みドメイン）のみへの送受信に限定する。			
1.5.4.2								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） ホワイトリスト制御	アップデートもホワイトリストも別装置での準備が必要。（コストが高い）	定期的なウイルスチェック（全台）			

2	生産効率化品質向上	複数の生産機械やセンサーを結び生産情報を統合。工程毎の品質データや検査結果を品番などによりトレースする。生産情報は遠隔地でさらに大きな情報と統合され見える化される。															
2.1			生産中（モニタリング）	いずれか１つの工程の生産プロセスが動作している状態。検査装置などから生産情報が送信されている。													
2.1.1					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				中	中	中
2.1.1.1								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	中
														安全保護装置の代替装置(バックアップ)を設置		小	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
2.1.1.2								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網雄	小	中	中
2.1.2								制御CPUがネットワーク処理兼用（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
2.1.1.3								IOTデータ収集機器（パソコン等）の管理不足	ウイルス（感染）				定期的なIOTファームウェアアップデート			中	小	中
													IOT機器へのアクセス制御(ルータ等)			中	小	中
														なし		中	中	中
															なし	中	中	中
2.1.1.4								管理の悪い工程からのウイルス伝搬。 EMCノイズ伝搬による不正停止	他の工程のPC 他の工程の通信機器				定期的なWindows設定の確認。			中	小	中
													FireWall設置			中	小	中
														EMC対策		中	小	中
															Windows環境の再インストールとバックアップ	小	中	中
2.1.2					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	中	中				中	中	中
2.1.2.1								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	中
														安全保護装置の代替装置(バックアップ)を設置		小	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

2.1.2.2								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	小	中	中
															定期的な制御システムパラメータのレビュー	中	小	中
2.1.2.3								保護装置CPUがネットワーク処理兼用（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
2.1.2.4								IOTデータ収集機器（パソコン等）の管理不足	ウイルス（感染）				定期的なIOTファームウェアアップデート			中	小	中
													IOT機器へのアクセス制御(ルータ等)			中	小	中
														なし		中	中	中
															なし	中	中	中
2.1.2.5								管理の悪い工程からのウイルス伝搬。 EMCノイズ伝搬による不正停止	他の工程のPC 他の工程の通信機器				定期的なWindows設定の確認。			中	小	中
													FireWall設置			中	小	中
														EMC対策		中	小	中
															Windows環境の再インストールとバックアップ	小	中	中
2.1.3					人的被害 装置損壊	安全保護装置が無効化され、保護機構が喪失する。	Triton/Trisis			高	小	中				高	小	中
2.1.3.1								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）			高	小(無)	中
													EXEのホワイトリスト制御			高	小(無)	中
														安全保護装置の代替装置(バックアップ)を設置		小	小	小
															Windows環境の再インストールとバックアップ	小	小	小
															定期的なエンジツールのアップデート	高	小(無)	中
2.1.3.2								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			高	小(無)	中
													EXEのホワイトリスト制御			高	小(無)	中
														なし		高	小	中
															定期的なエンジツールのアップデート	高	小(無)	中
															定期的な制御システムパラメータのレビュー	高	小(無)	中
2.1.3.3								保護装置CPUがネットワーク処理兼用（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			高	小(無)	中
														外部ネットワーク遮断		小	小	小
															ネットワーク遮断後の別回線使用	小	小	小

2.1.3.4								遠隔からの不正プログラムのダウンロード	ハッカー ウイルス				FireWall (IPフィルタ)設置			高	小(無)	中
														安全保護装置の代替装置(バックアップ)を設置		小	小	小
															定期的な制御システムパラメータのレビュー	高	小(無)	中
															遠隔操作の禁止	小	小	小
2.1.3.5								IOTデータ収集機器（パソコン等）の管理不足	ウイルス（感染） バックドア				定期的なIOTファームウェアアップデート			高	小(無)	中
													IOT機器へのアクセス制御(ルータ等)			高	小(無)	中
														なし		高	小	中
															なし	高	小	中
2.1.3.6								管理の悪い工程からのウイルス伝搬。 EMCノイズ伝搬による不正停止	他の工程のPC 他の工程の通信機器				定期的なWindows設定の確認。			高	小(無)	中
													FireWall設置			高	小(無)	中
														EMC対策		高	小(無)	中
															Windows環境の再インストールとバックアップ	小	小	小
2.1.4					生産情報漏洩	射出成型機など原料と機械機構や温度調整の設定や動作時間が漏洩し製造ノウハウが流出。	中国ファーウェイ（英）			小	小	小				小	小	小
2.1.4.1								インターネットなど外部につながる伝達経路	ウィルス（感染） 通信装置そのもの				ネットワークを多層分離し、FWやフィルタを設置。流出パケットを常時監視。	既存の設備で後から対策するするのは難しい。（コストがかかる。）専門技術者が必要。	インターネットにつなげる末端には最低FWを入れて特定のIPアドレス（認証済みドメイン）のみへの送受信に限定する。			
2.1.4.2								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） ホワイトリスト制御	アップデートもホワイトリストも別装置での準備が必要。（コストが高い）	定期的なウイルスチェック（全台）			
2.1.4.3								IOTデータ収集機器（パソコン等）の管理不足	ウイルス（感染） バックドア				定期的なWindowsアップデート（全台） ホワイトリスト制御	アップデートもホワイトリストも別装置での準備が必要。（コストが高い）	定期的なウイルスチェック（全台）			
2.1.4.4								IOTデータ収集機器（（ルータやFWなど）の管理不足	バックドア				定期的な通信機器（ルータやFW)のアップデートと設定の確認	専門の技術者が必要。	定期的に接続パスワードなどを変更する			
2.2			部分工程の機械保全	生産中に、特定の工程の機械の修理や交換が発生したケース。関係する工程の機械設備の動力源はOFF。他の工程はON。														
2.2.1					可動中工程の生産中断	機械修理時の作業員の持ち込むパソコンや、作業中のＥＭＣノイズ、物理的な工事の影響が他の工程に影響して生産が中断する。	Wannacry			中	中	中				中	中	中
2.2.1.1								管理の悪い工程からのウイルス伝搬。 EMCノイズ伝搬による不正停止	他の工程のPC 他の工程の通信機器				定期的なWindows設定の確認。			中	小	中
													FireWall設置			中	小	中
														EMC対策		中	小	中
															Windows環境の再インストールとバックアップ	小	中	中
2.2.1.2								保全中の工程からの稼働中の工程への影響	保守パソコン 誤操作、誤設定				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	中
													Firewall設置			中	小	中
														稼働中工程の安全対策		小	中	中
															Windows環境の再インストールとバックアップ	小	中	中

2.2.2					効率品質低下	機械修理時の作業員が持ち込む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	中	中				中	中	中
2.2.2.1								管理の悪い工程からのウイルス伝搬。 EMCノイズ伝搬による不正停止	他の工程のPC 他の工程の通信機器				定期的な Windows設定の 確認。			中	小	中
													FireWall設置			中	小	中
														EMC対策		中	小	中
															Windows環境の 再インストール とバックアップ	小	中	中
2.2.2.2								保全中の工程からの稼働中の工程への影響	保守パソコン 誤操作、誤設定				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	中
													Firewall設置			中	小	中
														稼働中工程の安 全対策		小	中	中
															Windows環境の 再インストール とバックアップ	小	中	中
2.2.2.3								共通要因故障。共通装置の誤った停止によるIOT機能の喪失（例）時刻ｻｰﾊﾞの停止、中継サーバの停止、品番管理ＰＣの停止	工程保守のための部分的なシステムの停止				定期的なIOT機 器・PCのソフト ウェアアップ デート			中	小	中
													サーバー多重化			小	中	中
														なし		中	中	中
															再立ち上げ(設定 不要)	小	中	中
2.2.3					人的被害 装置損壊	機械修理時の作業員の持ち込むパソコンや、作業中のＥＭＣノイズ、物理的な工事の影響安全保護装置が無効化され、保護機構が喪失する。	Triton/Trisis			高	中	高				高	中	高
2.2.3.1								保護装置CPUがネットワーク処理兼用（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			高	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
2.2.3.2								管理の悪い工程からのウイルス伝搬。 EMCノイズ伝搬による不正停止	他の工程のPC 他の工程の通信機器				定期的な Windows設定の 確認。			高	小	中
													FireWall設置			高	小	中
														EMC対策		高	小	中
															Windows環境の 再インストール とバックアップ	小	中	中
2.2.3.3								保全中の工程からの稼働中の工程への影響	保守パソコン 誤操作、誤設定				定期的な Windowsアップ デート（全台）			高	小	中
													EXEのホワイト リスト制御			高	小	中
													Firewall設置			高	小	中
														稼働中工程の安 全対策		小	中	中
															Windows環境の 再インストール とバックアップ	小	中	中
2.2.3.4								共通要因故障。共通装置の誤った停止によるIOT機能の喪失（例）時刻ｻｰﾊﾞの停止、中継サーバの停止、品番管理ＰＣの停止	工程保守のための部分的なシステムの停止				定期的なIOT機 器・PCのソフト ウェアアップ デート			高	小	中
													サーバー多重化			小	中	中
														なし		高	中	高
															再立ち上げ(設定 不要)	小	中	中

付録 C-セキュリティリスクアセスメントの事例

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。																
1.2			遠隔接続（監視）	動力源ON。機械の動作状態を通信によって遠隔地に送信している。														
1.2.1					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	高	高				中	高	高
1.2.1.2								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	中	中
													FireWall設置			中	中	中
														RDT禁止		小	小	小
															RDT操作のundo網羅	小	高	中
1.2.1.3								制御CPUがネットワーク処理兼用（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	中	中
														外部ネットワーク遮断		小	高	中
															ネットワーク遮断後の別回線使用	小	高	中
1.2.1.4								遠隔監視用接続機器（パソコン等）の管理不足	ウイルス（感染）				定期的なWindowsアップデート（全台）			中	中	中
													EXEのホワイトリスト制御			中	小	中
														なし		中	高	高
															Windows環境の再インストールとバックアップ	小	高	中
															定期的なエンジンツールのアップデート	中	中	中
1.2.3					人的被害 装置損壊	安全保護装置が無効化され、保護機構が喪失する。	Triton/Trisis			高	高	高				高	高	高
1.2.3.2								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（全台）			高	中	高
													EXEのホワイトリスト制御			高	中	高
														安全保護装置の代替装置(バックアップ)を設置		小	高	高
															定期的なエンジンツールのアップデート	小	中	中
															定期的な制御システムパラメータのレビュー	中	中	中
1.2.3.4								遠隔からの不正プログラムのダウンロード	ハッカー ウイルス				FireWall (IPフィルタ)設置			高	小	中
														安全保護装置の代替装置(バックアップ)を設置		小	高	高
															定期的な制御システムパラメータのレビュー	中	中	高
															遠隔操作の禁止	**小**	**小**	**小**
1.2.3.5								遠隔監視用接続機器（パソコン等）の管理不足	ウイルス（感染） バックドア				定期的なWindowsアップデート（全台）			高	中	高
													EXEのホワイトリスト制御			高	中	高
														なし		高	高	高
															Windows環境の再インストールとバックアップ	小	高	中
															定期的なエンジンツールのアップデート	中	中	中

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(復旧)	被害大きさ	可能性	リスク
2	生産効率化品質向上	複数の生産機械やセンサーを結び生産情報を統合。工程毎の品質データや検査結果を品番などにより トレースする。生産情報は遠隔地でさらに大きな情報と統合され見える化される。																
2.1			生産中（モニタリング）	いずれか１つの工程の生産プロセスが動作している状態。検査装置などから生産情報が送信されている。														
2.1.1					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				中	中	中
2.1.1.2								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 網雄	小	中	中
2.1.1.3								制御CPUがネットワーク処理兼用（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
2.1.1.4								IOTデータ収集機器（パソコン等）の管理不足	ウイルス（感染）				定期的なIOTファームウェアアップデート			中	小	中
													IOT機器へのアクセス制御(ルータ等)			中	小	中
														なし		中	中	中
															なし	中	中	中
2.1.1.5								管理の悪い工程からのウイルス伝搬。EMCノイズ伝搬による不正停止	他の工程のPC 他の工程の通信機器				定期的なWindows設定の確認。			中	小	中
													FireWall設置			中	小	中
														EMC対策		中	小	中
															Windows環境の再インストールとバックアップ	小	中	中
2.2			部分工程の機械保全	生産中に、特定の工程の機械の修理や交換が発生したケース。関係する工程の機械設備の動力源はOFF。他の工程はON。														
2.2.3					人的被害 装置損壊	機械修理時の作業員の持ち込むパソコンや、作業中のＥＭＣノイズ、物理的な工事の影響安全保護装置が無効化され、保護機構が喪失する。	Triton/Trisis			高	中	高				高	中	高
2.2.3.3								保全中の工程からの稼働中の工程への影響	保守パソコン 誤操作、誤設定				定期的なWindowsアップデート（全台）			高	小	中
													EXEのホワイトリスト制御			高	小	中
													Firewall設置			高	小	中
														稼働中工程の安全対策		小	中	中
															Windows環境の再インストールとバックアップ	小	中	中
2.2.3.4								共通要因故障。共通装置の誤った停止によるIOT機能の喪失（例）時刻ｻｰﾊﾞの停止、中継サーバの停止、品番管理ＰＣの停止	工程保守のための部分的なシステムの停止				定期的なIOT機器・PCのソフトウェアアップデート			高	小	中
													サーバー多重化			小	中	中
														なし		高	中	高
															再立ち上げ(設定不要)	小	中	中

付録 D-生産現場におけるセキュリティリスク KY のアプローチ

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部会

生産現場におけるセキュリティリスクＫＹのアプローチ

（改４）2020年3月2日
（株）制御システム研究所
森本 賢一

（一社）日本機械工業連合会

現場のセキュリティってなんだろう

毎日のＫＹ
（危険予知）

系統故障
（設計ミス・計画ミス）

ランダム故障
（偶発故障・腐食劣化）

ヒューマンエラー
（ポカミス・不安全行動）

自然災害
（地震・大雨・台風）

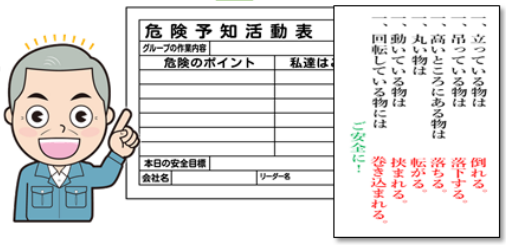
周囲に声をかけて立ち入ろう

機械停止を確認し作業開始しよう

指差呼称して操作しよう

監視装置の数値を確認しよう

非常停止ＳＷの場所を確認しよう



Copy right © 2019 CSL All rights reserved

安全の対策が台無しになるかも

毎日のＫＹ
（危険予知）

系統故障
（設計ミス・計画ミス）

ランダム故障
（偶発故障・腐食劣化）

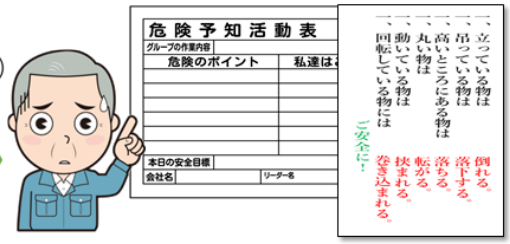
ヒューマンエラー
（ポカミス・不安全行動）

自然災害
（地震・大雨・台風）

セキュリティ
（脆弱性・脅威）

周囲に声をかけて立ち入ろう	ヨソから他人が操作するかも
機械停止を確認し作業開始しよう	機械が突然動き始めるかも
指差呼称して操作しよう	操作スイッチが効かないかも
監視装置の数値を確認しよう	表示データが間違っているかも
非常停止ＳＷの場所を確認しよう	イザという時停止できないかも

本当！？



実際に発生した事例（遠隔操作）

毎日のＫＹ
（危険予知）

系統故障
（設計ミス・計画ミス）

ランダム故障
（偶発故障・腐食劣化）

ヒューマンエラー
（ポカミス・不安全行動）

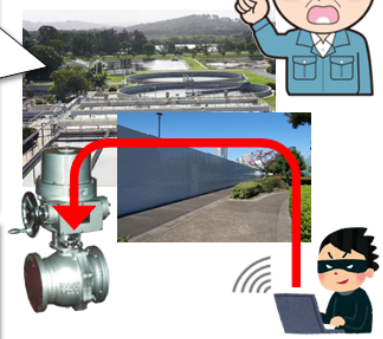
自然災害
（地震・大雨・台風）

セキュリティ
（脆弱性・脅威）

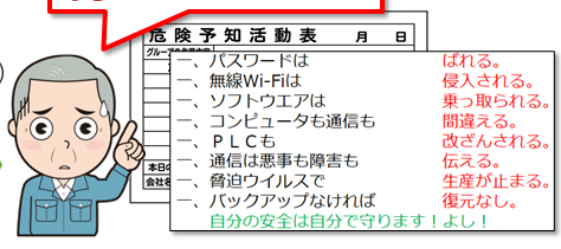
周囲に声をかけて立ち入ろう	ヨソから他人が操作するかも

2000年　オーストラリア

職員の不採用で恨み。無線LAN経由でSCADAシステムを46回不正操作。2カ月に渡り100万リットルの下水を河川に流出させた。



セキュリティＫＹ
Wi-Fi、無線LAN経由で
近隣から遠隔操作
あるかも・・・・



**無線は
届く場所から
誰でも
操作できる！**

実際に発生した事例（ＰＬＣのロジック改ざん）

セキュリティ
（脆弱性・脅威）

毎日のＫＹ
（危険予知）

機械停止を確認し
作業開始しよう

機械が突然
動き始めるかも

PLCも！？

系統故障
（設計ミス・計画ミス）

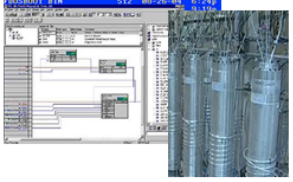
ランダム故障
（偶発故障・腐食劣化）

ヒューマンエラー
（ポカミス・不安全行動）

自然災害
（地震・大雨・台風）

2010年1月 イラン

ウイルスが、ＰＬＣ保守ソフトの機能を悪用。PLCの制御ロジックを改ざん。異常な速度制御で核燃料遠心分離機8、000台を破壊。



セキュリティＫＹ
ＰＬＣだって保守パソコン経由でウイルスにより改ざんが可能だ。

危険予知活動表　月　日

一、パスワードは	ばれる。
一、無線Wi-Fiは	侵入される。
一、ソフトウエアは	乗っ取られる。
一、コンピュータも通信も	間違える。
一、ＰＬＣも	改ざんされる。
一、通信は悪事も障害も	伝える。
一、脅迫ウイルスで	生産が止まる。
一、バックアップなければ	復元なし。

自分の安全は自分で守ります！よし！

制御ＰＬＣも知らないうちに改ざんされる！

実際に発生した事例（操作画面のロックアウト）

セキュリティ
（脆弱性・脅威）

毎日のＫＹ
（危険予知）

指差呼称して
操作しよう

操作スイッチが
効かないかも

画面ﾛｯｸ！？

系統故障
（設計ミス・計画ミス）

ランダム故障
（偶発故障・腐食劣化）

ヒューマンエラー
（ポカミス・不安全行動）

自然災害
（地震・大雨・台風）

2019年3月 ノルウェー

ランサムウェア（脅迫ｳｨﾙｽ）がアルミニウム工場のPCのﾌｧｲﾙ暗号化、画面ロック、ログイン無効化。操業停止や一部手動で機械操作。

セキュリティＫＹ
ちょっとした操作ＰＣでも画面がロックされると操業停止につながる！

危険予知活動表　月　日

一、パスワードは	ばれる。
一、無線Wi-Fiは	侵入される。
一、ソフトウエアは	乗っ取られる。
一、コンピュータも通信も	間違える。
一、ＰＬＣも	改ざんされる。
一、通信は悪事も障害も	伝える。
一、脅迫ウイルスで	生産が止まる。
一、バックアップなければ	復元なし。

自分の安全は自分で守ります！よし！

操作端末もパソコンならウイルス感染操業停止

実際に発生した事例（監視データの誤送信）

セキュリティ
（脆弱性・脅威）

毎日のＫＹ
（危険予知）

監視装置の数値を
確認しよう

表示データが
間違っているかも

ﾃﾞｰﾀ化け！？

系統故障
（設計ミス・計画ミス）

ランダム故障
（偶発故障・腐食劣化）

ヒューマンエラー
（ポカミス・不安全行動）

自然災害
（地震・大雨・台風）

2008年5月 米国

Hatch原子力発電所の事務パソコンのアップデートで発電所サーバ内の水位データが誤って０mmになり緊急停止。

セキュリティＫＹ
通信データは化ける。
メモリーも間違える。
おかしな値は疑わなきゃ。

危険予知活動表　月　日

一、パスワードは	ばれる。
一、無線Wi-Fiは	侵入される。
一、ソフトウエアは	乗っ取られる。
一、コンピュータも通信も	間違える。
一、ＰＬＣも	改ざんされる。
一、通信は悪事も障害も	伝える。
一、脅迫ウイルスで	生産が止まる。
一、バックアップなければ	復元なし。

自分の安全は自分で守ります！よし！

**通信データは化ける
コンピュータは間違える**

実際に発生した事例（ネットワークストーム）

セキュリティ
（脆弱性・脅威）

毎日のＫＹ
（危険予知）

非常停止ＳＷの
場所を確認しよう

イザという時
停止できないかも

系統故障
（設計ミス・計画ミス）

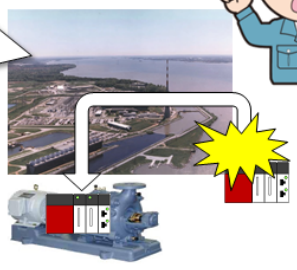
ランダム故障
（偶発故障・腐食劣化）

ヒューマンエラー
（ポカミス・不安全行動）

自然災害
（地震・大雨・台風）

2006年 米国原子力発電所

重要度の低いPLCが故障し、監視ネットワーク経由で、大量の通信を誤出力。冷却水ポンプのPLCが機能不能。発電所を手動で停止。



セキュリティＫＹ
ネットワークは、ノイズや障害を伝播する経路にもなる。

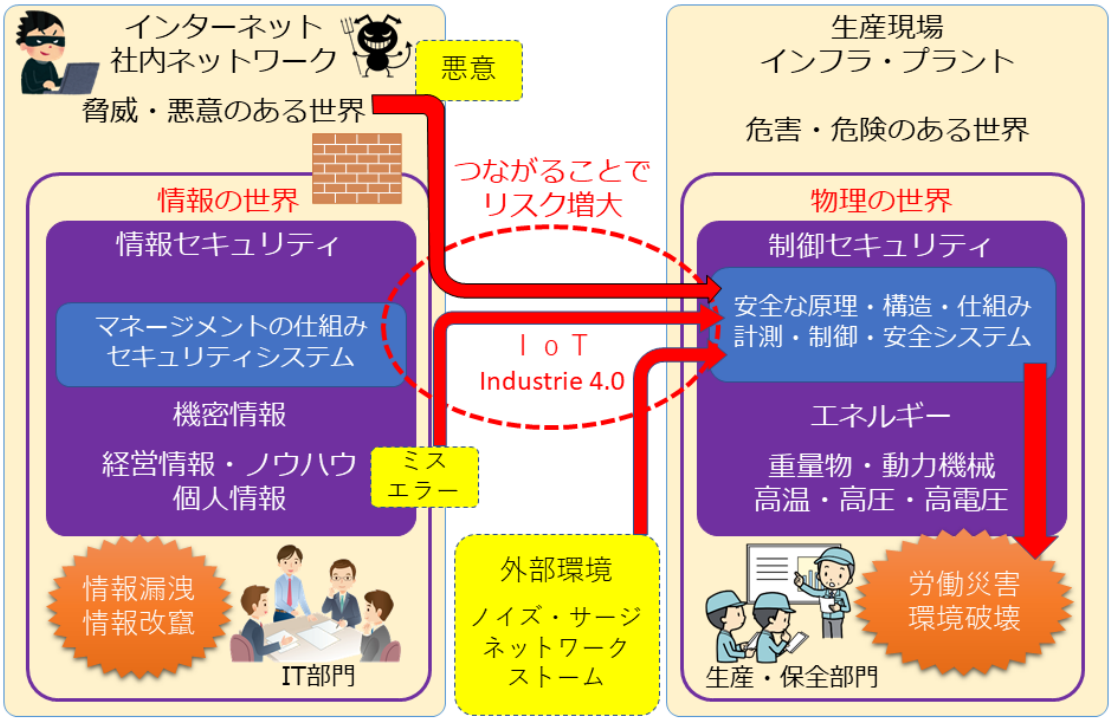
危険予知活動表　月　日

一、パスワードは	ばれる。
一、無線Wi-Fiは	侵入される。
一、ソフトウエアは	乗っ取られる。
一、コンピュータも通信も	間違える。
一、ＰＬＣも	改ざんされる。
一、通信は悪事も障害も	伝える。
一、脅迫ウイルスで	生産が止まる。
一、バックアップなければ	復元なし。

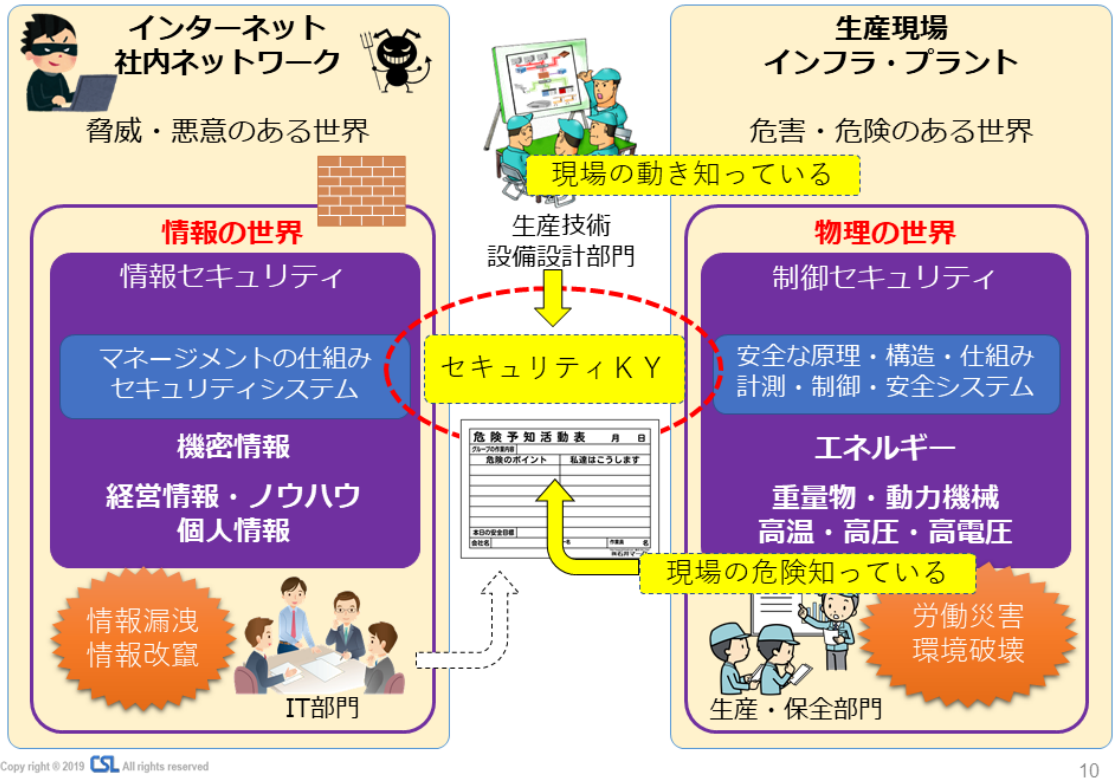
自分の安全は自分で守ります！よし！

**ネットワークは
ノイズや障害
も伝播する**

現場のセキュリティリスクが高まるわけ



現場のセキュリティリスクＫＹの実行者



セキュリティリスクKY 3つのアプローチ

1）設備構造に基づくリスク分析
（実施部門）
設備原理やネットワークプロトコル、使用機材、制御保護を把握している

設備設計･生産技術部門

2）シナリオに基づくリスク分析
（実施部門）
生産プロセスの工程毎の監視操作オペレーションと装置を把握している

生産管理部門

3）気づきに基づくリスク分析
（実施部門）
現場作業員、外注専門業者など特定の工程や作業を把握している

運用保全部門

生産現場
インフラ・プラント

危害・危険のある世界

物理の世界

制御セキュリティ

安全な原理・構造・仕組み
計測・制御・安全システム

エネルギー

重量物・動力機械
高温・高圧・高電圧

労働災害
環境破壊

生産・保全部門

セキュリティリスクKY 3つのアプローチ

1）設備構造に基づくリスク分析
（実施部門）
設備原理やネットワークプロトコル、使用機材、制御保護を把握している

設備設計･生産技術部門

2）シナリオに基づくリスク分析
（実施部門）
生産プロセスの工程毎の監視操作オペレーションと装置を把握している

生産管理部門

3）気づきに基づくリスク分析
（実施部門）
現場作業員、外注専門業者など特定の工程や作業を把握している

生産・保全部門

生産現場
インフラ・プラント

危害・危険のある世界

物理の世界

制御セキュリティ

安全な原理・構造・仕組み
計測・制御・安全システム

エネルギー

重量物・動力機械
高温・高圧・高電圧

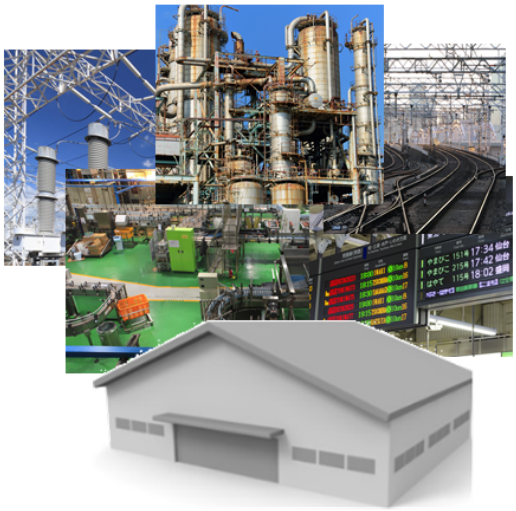
労働災害
環境破壊

生産・保全部門

1）生産設備の構造に基づく　セキュリティーリスクＫＹ

取組のステップ

設備の危険な状態や部位を洗い出す
コンピュータに頼らない安全対策を行う
↓
制御機器、ネットワークを把握する
↓
ネットワークを整理・分離する
↓
脆弱性・脅威分析をして対策を施す
↓
業務規程・技術基準を整備
啓蒙教育を継続する



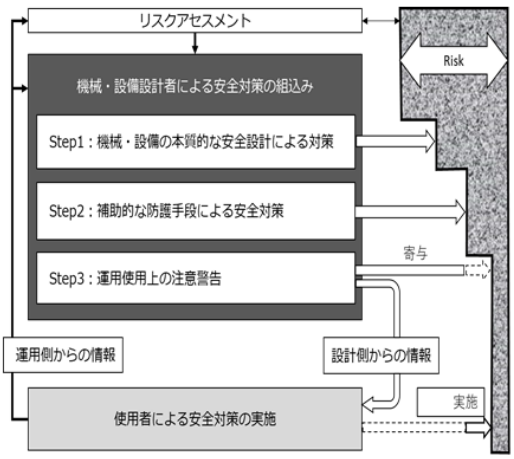
機械設備やプラント機器、その危険な状態（ハザード）を特定し安全対策や制御が、どのような原理や機器で行われているのか把握しましょう。

1）生産設備の構造に基づく　セキュリティーリスクＫＹ

取組のステップ

設備の危険な状態や部位を洗い出す
コンピュータに頼らない安全対策を行う
↓
制御機器、ネットワークを把握する
↓
ネットワークを整理・分離する
↓
脆弱性・脅威分析をして対策を施す
↓
業務規程・技術基準を整備
啓蒙教育を継続する

ISO 12100 リスクアセスメントの原則



コンピュータに頼らない安全対策が大切です。コンピュータなしの安全対策がしっかりしていれば、セキュリティ対策は容易になります。IoT時代だからこそ、今一度見直しましょう。

1）生産設備の構造に基づく　セキュリティーリスクＫＹ

取組のステップ

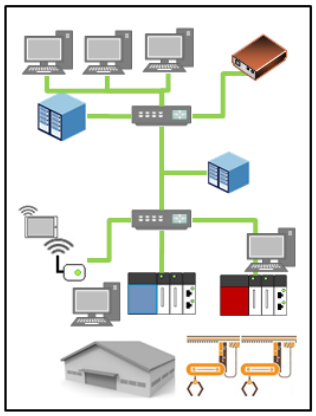
設備の危険な状態や部位を洗い出す
コンピュータに頼らない安全対策を行う

制御機器、ネットワークを把握する

ネットワークを整理・分離する

脆弱性・脅威分析をして対策を施す

業務規程・技術基準を整備
啓蒙教育を継続する



PLCやパソコン、モバイルルータ、構内モデムなどの機材や、有線LANやWi-Fi、LTE回線など、管理部門を横断的に調査し、現場にあるネットワークの全体像を把握しましょう。試験用IoT機器もセキュリティの対象です。

1）生産設備の構造に基づく　セキュリティーリスクＫＹ

取組のステップ

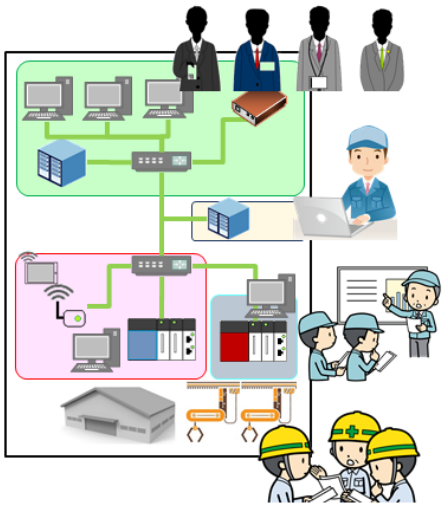
設備の危険な状態や部位を洗い出す
コンピュータに頼らない安全対策を行う

制御機器、ネットワークを把握する

ネットワークを整理・分離する

脆弱性・脅威分析をして対策を施す

業務規程・技術基準を整備
啓蒙教育を継続する



用途や設備の重要度、関与する人員構成が違う機器がつながるネットワークを区別しましょう。技術的に分離で来ていなくても、現場の意図を明確にします。レイアウト変更や外注化など運用が変わった際にも見直します。

1）生産設備の構造に基づく　セキュリティーリスクＫＹ

取組のステップ

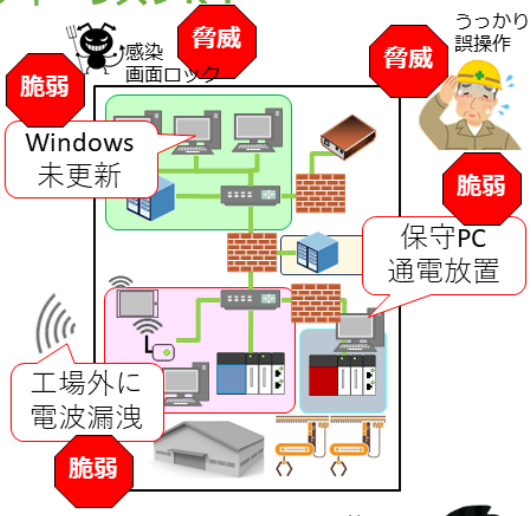
設備の危険な状態や部位を洗い出す
コンピュータに頼らない安全対策を行う

制御機器、ネットワークを把握する

ネットワークを整理・分離する

脆弱性・脅威分析をして対策を施す

業務規程・技術基準を整備
啓蒙教育を継続する



セキュリティリスク
＝ 脆弱性 × 脅威 × 被害程度

・脆弱性は見つけて穴をふさぎます。
・脅威は想定し発生可能性を小さくします。
・万一の被害を小さくする準備をします。

1）生産設備の構造に基づく　セキュリティーリスクＫＹ

取組のステップ

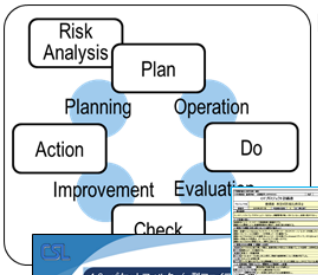
設備の危険な状態や部位を洗い出す
コンピュータに頼らない安全対策を行う

制御機器、ネットワークを把握する

ネットワークを整理・分離する

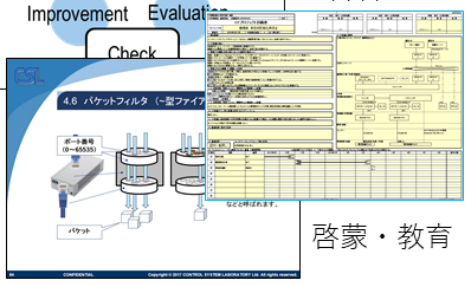
脆弱性・脅威分析をして対策を施す

業務規程・技術基準を整備
啓蒙教育を継続する



PDCAサイクルの構築

帳票・記録
文書管理



啓蒙・教育

取り決めた対策は、全体のルールに展開します。また現場のIoTによるカイゼンは今後も常に続きます。
セキュリティに配慮した、IoTの取り組みができるように、
常に啓蒙と教育をつづけます。

セキュリティリスクKY 3つのアプローチ

1）設備構造に基づく
リスク分析
（実施部門）
設備原理やネットワーク
プロトコル、使用機材、
制御保護を把握している

設備設計･生産技術部門

2）シナリオに基づく
リスク分析
（実施部門）
生産プロセスの工程毎の
監視操作オペレーション
と装置を把握している

生産管理部門

3）気づきに基づく
リスク分析
（実施部門）
現場作業員、外注専門業
者など特定の工程や作業
を把握している

生産・保全部門

生産現場
インフラ・プラント

危害・危険のある世界

物理の世界

制御セキュリティ

安全な原理・構造・仕組み
計測・制御・安全システム

エネルギー

重量物・動力機械
高温・高圧・高電圧

労働災害
環境破壊

生産・保全部門

2）シナリオに基づく　セキュリティーリスクＫＹ

取組のステップ

IoTの目的や機能を明確化
1）機械保守のためのIoT
2）品質等設備横断のIoT

⇩

運用シナリオを想定
被害シナリオを想定

⇩

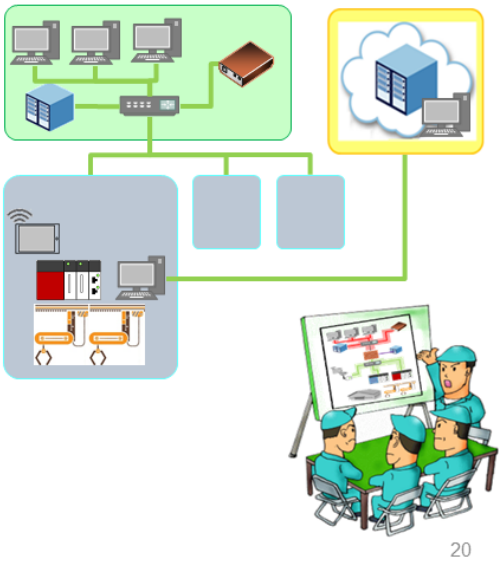
被害と発生可能性分析し、対策を施す

⇩

業務規程・技術基準を整備
啓蒙教育を継続する

生産現場のIoTシステムは、
目的や機能によって使用する機
材や構造が類似します。
詳細なシステムが判らない場合、
機能や目的を明確化して
被害シナリオを想定し、被害や
発生可能性を分析します。

目的や機能でシステムを想定



2）シナリオに基づく　セキュリティーリスクＫＹ

取組のステップ

IoTの目的や機能を明確化
1）機械保守のためのIoT
2）品質等設備横断のIoT

↓

運用シナリオを想定
被害シナリオを想定

↓

被害と発生可能性分析し、対策を施す

↓

業務規程・技術基準を整備
啓蒙教育を継続する

このようなIoTの特徴は･･･

機械の運転データを得るため、制御PLCへの接続があり得ます。

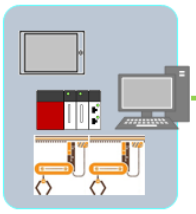
クラウドのAIなど工場外への接続があり得ます。

■想定機能

設備機械を予兆保守するために制御PLCからデータ収集しクラウド等で予兆解析

■想定IoTシステム

・制御PLC
・PLC保守用PC
・機械操作パネル
・外部との接続



2）シナリオに基づく　セキュリティーリスクＫＹ

取組のステップ

IoTの目的や機能を明確化
1）機械保守のためのIoT
2）品質等設備横断のIoT

↓

運用シナリオを想定
被害シナリオを想定

↓

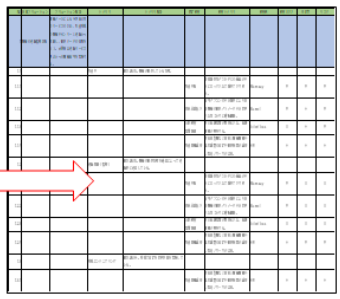
被害と発生可能性分析し、対策を施す

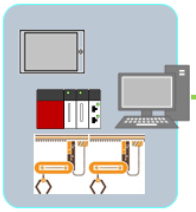
↓

業務規程・技術基準を整備
啓蒙教育を継続する

日機連の資料を参考に
運用シナリオ、被害シナリオを参考にして、必要な対策を抽出します。
想定被害を加えてもよいです。

■想定シナリオ（別紙参照）





2）シナリオに基づく　セキュリティーリスクＫＹ

取組のステップ

IoTの目的や機能を明確化
1）機械保守のためのIoT
2）品質等設備横断のIoT

↓

運用シナリオを想定
被害シナリオを想定

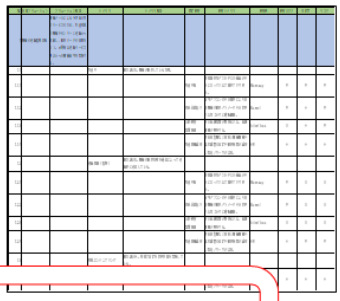
↓

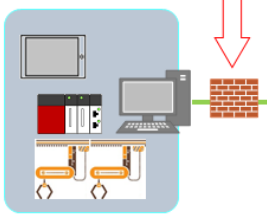
被害と発生可能性分析し、対策を施す

↓

業務規程・技術基準を整備
啓蒙教育を継続する

■想定シナリオ（別紙参照）





日機連の資料を参考に
抽出した対策を実施します。

2）シナリオに基づく　セキュリティーリスクＫＹ

取組のステップ

IoTの目的や機能を明確化
1）機械保守のためのIoT
2）品質等設備横断のIoT

↓

運用シナリオを想定
被害シナリオを想定

↓

被害と発生可能性分析し、対策を施す

↓

業務規程・技術基準を整備
啓蒙教育を継続する

このようなIoTの特徴は･･･

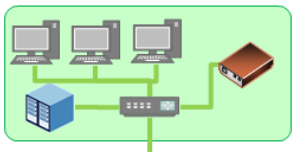
工程や設備を横断するネットワークの相互接続があり得ます。

管理部門との接続など業務部門との接続があり得ます。

■想定機能

設備を横断的に結び、生産状態を監視またはカイゼン指令を出す

■想定IoTシステム



・制御PLC
・PLC保守用PC
・操作パネル
・工場横断接続
・部門間接続

別な工程・設備

2）シナリオに基づく　セキュリティーリスクＫＹ

取組のステップ

IoTの目的や機能を明確化
1）機械保守のためのIoT
2）品質等設備横断のIoT

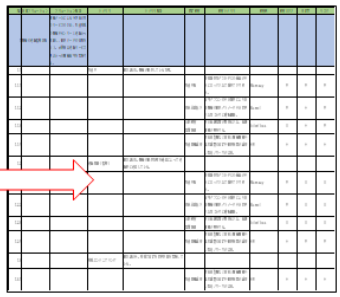
運用シナリオを想定
被害シナリオを想定

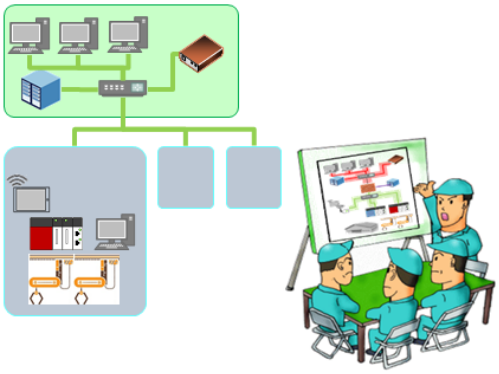
被害と発生可能性分析し、対策を施す

業務規程・技術基準を整備
啓蒙教育を継続する

日機連の資料を参考に
運用シナリオ、被害シナリオを
参考にして、必要な対策を抽出
します。
想定被害を加えてもよいです。

■想定シナリオ（別紙参照）





25

2）シナリオに基づく　セキュリティーリスクＫＹ

取組のステップ

IoTの目的や機能を明確化
1）機械保守のためのIoT
2）品質等設備横断のIoT

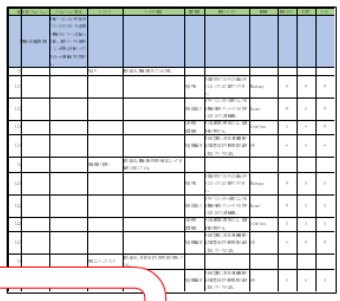
運用シナリオを想定
被害シナリオを想定

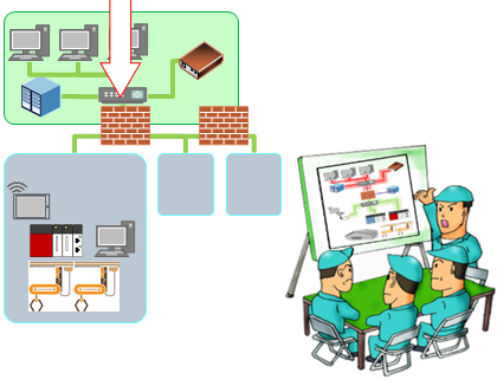
被害と発生可能性分析し、対策を施す

業務規程・技術基準を整備
啓蒙教育を継続する

日機連の資料を参考に
抽出した対策を実施します。

■想定シナリオ（別紙参照）





26

2）シナリオに基づく　セキュリティーリスクＫＹ

取組のステップ

IoTの目的や機能を明確化
1）機械保守のためのIoT
2）品質等設備横断のIoT

↓

運用シナリオを想定
被害シナリオを想定

↓

被害と発生可能性分析し、対策を施す

↓

業務規程・技術基準を整備
啓蒙教育を継続する

PDCAサイクルの構築

帳票・記録
文書管理

啓蒙・教育

取り決めた対策は、全体のルールに展開します。また現場のIoTによるカイゼンは今後も常に続きます。
セキュリティに配慮した、IoTの取り組みができるように、
常に啓蒙と教育をつづけます。

セキュリティリスクKY 3つのアプローチ

1）設備構造に基づく
リスク分析
（実施部門）
設備原理やネットワーク
プロトコル、使用機材、
制御保護を把握している

設備設計･生産技術部門

2）シナリオに基づく
リスク分析
（実施部門）
生産プロセスの工程毎の
監視操作オペレーション
と装置を把握している

生産管理部門

3）気づきに基づく
リスク分析
（実施部門）
現場作業員、外注専門業
者など特定の工程や作業
を把握している

生産・保全部門

生産現場
インフラ・プラント

危害・危険のある世界

物理の世界

制御セキュリティ

安全な原理・構造・仕組み
計測・制御・安全システム

エネルギー

重量物・動力機械
高温・高圧・高電圧

労働災害
環境破壊

生産・保全部門

3）気づきに基づく　セキュリティーリスクＫＹ

一、立っている物は　倒れる。
一、吊っている物は　落下する。
一、高いところにある物は　落ちる。
一、丸い物は　転がる。
一、動いている物は　挟まれる。
一、回転している物には　巻き込まれる。
ご安全に！

危険予知活動表　月　日

グループの作業内容	
危険のポイント	私達はこうします
本日の安全目標	
会社名 / リーダー名 / 作業員　名	

指差呼称マーク

現場で皆で、セキュリティリスクＫＹ

手順や準備
注意や気づき

当てはまる運用や
準備不足はないかな

一、パスワードは　ばれる。
一、無線Wi-Fiは　侵入される。
一、ソフトウエアは　乗っ取られる。
一、コンピュータも通信も　間違える。
一、ＰＬＣも　改ざんされる。
一、通信は悪事も障害も　伝える。
一、脅迫ウイルスで　生産が止まる。
一、バックアップなければ　復元なし。
自分の安全は自分で守ります！よし！

生産現場
インフラ・プラント

危害・危険のある世界

物理の世界

制御セキュリティ

安全な原理・構造・仕組み
計測・制御・安全システム

エネルギー

重量物・動力機械
高温・高圧・高電圧

労働災害
環境破壊

生産・保全部門

気づきに基づく　セキュリティリスクＫＹ　８項目

一、パスワードは　ばれる。
一、無線Wi-Fiは　侵入される。
一、ソフトウエアは　乗っ取られる。
一、コンピュータも通信も　間違える。
一、ＰＬＣも　改ざんされる。
一、通信は悪事も障害も　伝える。
一、脅迫ウイルスで　生産が止まる。
一、バックアップなければ　復元なし。
自分の安全は自分で守ります！よし！

項目	パスワードはいつかばれる
こころ	パスワードによるセキュリティはしょぼい
重点施策	デフォルトのパスワードは使わない（変更する）
	パスワードは付箋紙に書かない
	みんなで共有するパスワードは定期的に変更する
	二段階認証や個人認証と組み合わせる
	デジタル証明書を活用する（クライアント認証）

気づきに基づく　セキュリティリスクＫＹ　８項目

一、パスワードは	ばれる。
一、無線Wi-Fiは	侵入される。
一、ソフトウエアは	乗っ取られる。
一、コンピュータも通信も	間違える。
一、ＰＬＣも	改ざんされる。
一、通信は悪事も障害も	伝える。
一、脅迫ウイルスで	生産が止まる。
一、バックアップなければ	復元なし。

自分の安全は自分で守ります！よし！

項目	**Wi-Fiは侵入される**
こころ	Wi-Fiのセキュリティはしょぼい
重点施策	MACｱﾄﾞﾚｽ制限、SSIDステルスで安心しない
	パスワード方式は定期的に変更できない通信には使わない
	制御や安全のネットワークとは分離する
	設定や操作の通信には使わない。（表示のみに使用）
	デジタル証明書を活用する（クライアント認証）

気づきに基づく　セキュリティリスクＫＹ　８項目

一、パスワードは	ばれる。
一、無線Wi-Fiは	侵入される。
一、ソフトウエアは	乗っ取られる。
一、コンピュータも通信も	間違える。
一、ＰＬＣも	改ざんされる。
一、通信は悪事も障害も	伝える。
一、脅迫ウイルスで	生産が止まる。
一、バックアップなければ	復元なし。

自分の安全は自分で守ります！よし！

項目	**ソフトウェアは乗っ取られる**
こころ	OSやソフトウェアの脆弱性はつぎつぎに発見されている。
重点施策	使わないOfficeアプリは現場ＰＣには入れない
	できるだけ現場ＰＣには、Officeアプリは入れない
	Windowsアップデートは予算化して必ず取り組む
	マクロやVBAを有効化したファイルは現場に持ち込み禁止

気づきに基づく　セキュリティリスクＫＹ　８項目

一、パスワードは　ばれる。
一、無線Wi-Fiは　侵入される。
一、ソフトウエアは　乗っ取られる。
一、コンピュータも通信も　間違える。
一、ＰＬＣも　改ざんされる。
一、通信は悪事も障害も　伝える。
一、脅迫ウイルスで　生産が止まる。
一、バックアップなければ　復元なし。
自分の安全は自分で守ります！よし！

項目	コンピュータも通信もバカになる
こころ	コンピュータや通信機器にもエラーや故障は発生する
重点施策	安全にかかわるデータや信号には入力検査回路を必ずいれる
	除外や遮断をする場所を明確にしておく ・コンピュータのシャットダウン・再起動要領の明確化 ・通信経路の遮断要領の明確化
	重要設備、危険な機械の起動停止は手動スイッチをつける
	多重化した重要設備を同じネットワークにつながない
	安全にかかわる装置はネットワークにつながない

（一社）日本機械工業連合会

気づきに基づく　セキュリティリスクＫＹ　８項目

一、パスワードは　ばれる。
一、無線Wi-Fiは　侵入される。
一、ソフトウエアは　乗っ取られる。
一、コンピュータも通信も　間違える。
一、ＰＬＣも　改ざんされる。
一、通信は悪事も障害も　伝える。
一、脅迫ウイルスで　生産が止まる。
一、バックアップなければ　復元なし。
自分の安全は自分で守ります！よし！

項目	ＰＬＣも改ざんされる
こころ	ＰＬＣロジックの改ざんは発見が難しい。見落としがち。
重点施策	定期的にロジックのバックアップと比較検査する
	ＰＬＣの保守パソコンは不使用時電源を切っておく
	常時運用パソコンにロジック変更機能をインストールしない
	パスワードはパソコンに記憶させない
	デフォルトのパスワードは使用しない（変更する）
	ＰＬＣのエンジ可キーは必ず施錠する

気づきに基づく　セキュリティリスクＫＹ　８項目

一、パスワードは　ばれる。
一、無線Wi-Fiは　侵入される。
一、ソフトウエアは　乗っ取られる。
一、コンピュータも通信も　間違える。
一、ＰＬＣも　改ざんされる。
一、通信は悪事も障害も　伝える。
一、脅迫ウイルスで　生産が止まる。
一、バックアップなければ　復元なし。
自分の安全は自分で守ります！よし！

項目	通信は悪事も障害も伝える
こころ	ネットワークは想定外のトラブルの伝播経路になりえる
重点施策	ネットワーク接続図は常に更新しておく
	万一の際にネットワークを遮断する場所を決めておく
	設備や工程ごとにネットワーク分離を励行する
	・異なるネットワークアドレスを使用する（ルータ）
	・決まった通信方式以外を遮断する（ポートフィルタ）
	・Windowsの共有フォルダ使用しない
	・ＩＰマスカレードの使用を励行する

（一社）日本機械工業連合会

気づきに基づく　セキュリティリスクＫＹ　８項目

一、パスワードは　ばれる。
一、無線Wi-Fiは　侵入される。
一、ソフトウエアは　乗っ取られる。
一、コンピュータも通信も　間違える。
一、ＰＬＣも　改ざんされる。
一、通信は悪事も障害も　伝える。
一、脅迫ウイルスで　生産が止まる。
一、バックアップなければ　復元なし。
自分の安全は自分で守ります！よし！

項目	脅迫ウイルスで生産が止まる
こころ	現場のパソコンでも常にウイルス感染の恐れがあると心得る
重点施策	現場のどこにパソコンがあるのか、台帳管理を徹底する。
	現場のパソコンは定期的にウイルス検査を行う
	業者の持ち込パソコンのウイルス検査は確実に行う
	ウイルス検査は最新のパターンファイルで行う
	持ち込んだＵＳＢ器具は使わない（不使用ＵＳＢをふさぐ）
	不使用のイーサネットポートはふさぐ
	ホワイトリスト制御を設定する

気づきに基づく　セキュリティリスクＫＹ　８項目

一、パスワードは　ばれる。
一、無線Wi-Fiは　侵入される。
一、ソフトウエアは　乗っ取られる。
一、コンピュータも通信も　間違える。
一、ＰＬＣも　改ざんされる。
一、通信は悪事も障害も　伝える。
一、脅迫ウイルスで　生産が止まる。
一、バックアップなければ　復元なし。
自分の安全は自分で守ります！よし！

項目	**バックアップなければ復元なし**
こころ	消去や改ざん強制暗号化に備えたバックアップは不可欠
重点施策	ＰＣ、ＰＬＣ、通信機器、すべての機器はバックアップ
	・購入時のバックアップ（ＯＳのみ、デフォルト設定）
	・システムのバックアップ（アプリ機能の復元）
	・可変データのバックアップ（設定やロジックの復元）
	・上記種類と期間を決めてバックアップを行う
	バックアップデータが読めるかメディアを定期的に検査する
	バックアップから復元する訓練を定期的に行う

気づきに基づく　セキュリティリスクＫＹ　８項目

一、パスワードは　ばれる。
一、無線Wi-Fiは　侵入される。
一、ソフトウエアは　乗っ取られる。
一、コンピュータも通信も　間違える。
一、ＰＬＣも　改ざんされる。
一、通信は悪事も障害も　伝える。
一、脅迫ウイルスで　生産が止まる。
一、バックアップなければ　復元なし。
自分の安全は自分で守ります！よし！

項目	**自分の安全は自分で守ります**
こころ	現場のセキュリティリスクは、我が身のためだと考える
重点施策	現場の全員が定期的にセキュリティについて学ぶ
	セキュリティリスクＫＹ8項目を毎朝唱和する
	毎朝のＫＹに必ず１つセキュリティリスクを加える
	設備導入時には、セキュリティリスク審査を行う
	セキュリティリスク審査が未完の設備は注文許可をしない
	ＩｏＴの投資vs効果にはセキュリティ対策費も含める
	セキュリティ対策費がもったいないと感じるIoTは入れない

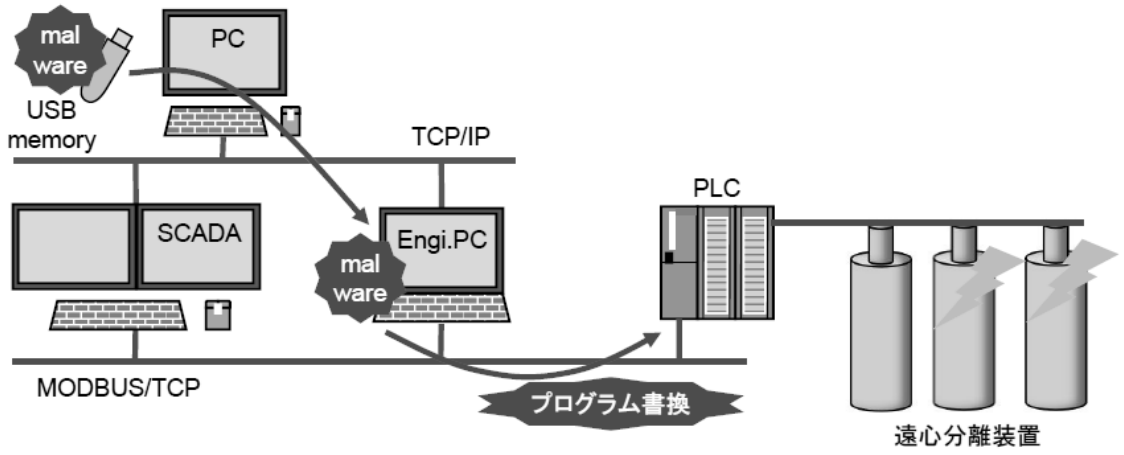
付録 E-生産システムのセキュリティインシデント事例

既に、生産設備の制御システムに対するセキュリティ脅威が報告されている。ここでは、代表的なものを解説する。

(1) Stuxnet

2011 年に、イランのウラン濃縮工場の遠心分離装置数千台が回転異常によって破損した。遠心分離装置を制御する PLC のアプリケーションプログラムとアラーム設定値が、マルウェア Stuxnet により書き換えられたことが原因である。何者かが持ち込んだ USB メモリーに仕込まれた Stuxnet は、制御システムのパソコンに順次感染を拡大した。目標 PLC のエンジニアリングツールに到達すると発症、すなわち目標 PLC のプログラムとパラメータを書き換えた。これで遠心分離装置は異常回転によって破損したが、アラームがあがらないため原因追及が遅れた。

本件は、クローズドシステムである PLC が直接攻撃された世界初の事件であり、これを受けて各国政府は制御システムのサイバーセキュリティ対策に乗り出すことになった。



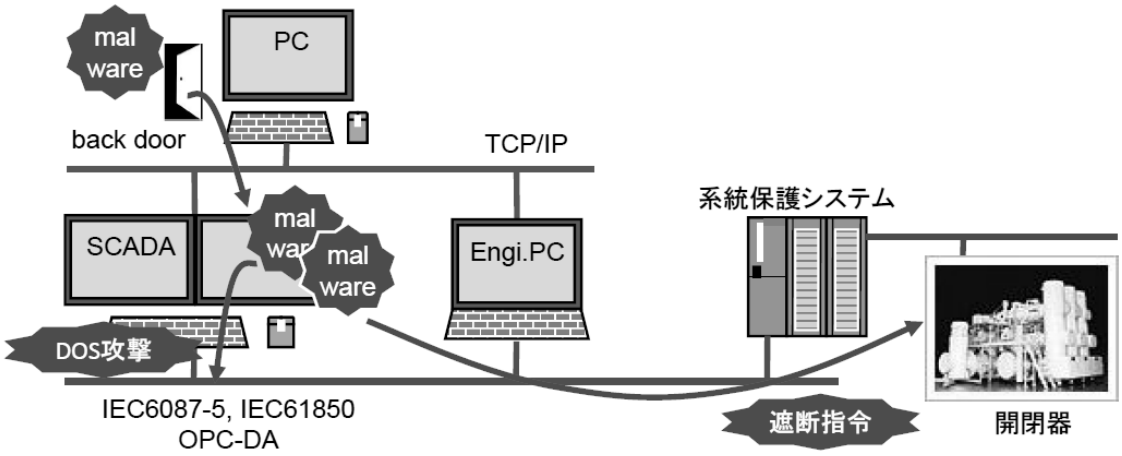
付図 E-1 Stuxnet によるウラン濃縮工場攻撃例

(2) BlackEnergy, Industroyer

2015 年 12 月、ウクライナで大規模停電が発生した。インターネット経由で電力系統制御システムの SCADA に感染したマルウェア BlackEnergy が、系統保護システムの脆弱性をついて開閉器を遮断したことが停電を引き起こした。同時に電話システムなど関連サブシステムに DoS 攻撃(過負荷トラフィック)を行い、停電復旧を妨害した。2016 年 12 月にも、同じくウクライナで同様の大規模停電が発生した。前年度とは異なるマルウェア Industroyer が、インターネットからバックドアを開けて系統保護システムに侵入し、開閉器を遮断した.Industroyer は複数の制御プロトコルに対応し、モジュール構成により多様な攻撃が可能である。

サイバー攻撃が大規模停電を起こした初のめての事件であり、これを受けて各国はエネルギー

分野のサイバーセキュリティ対策を強化した。

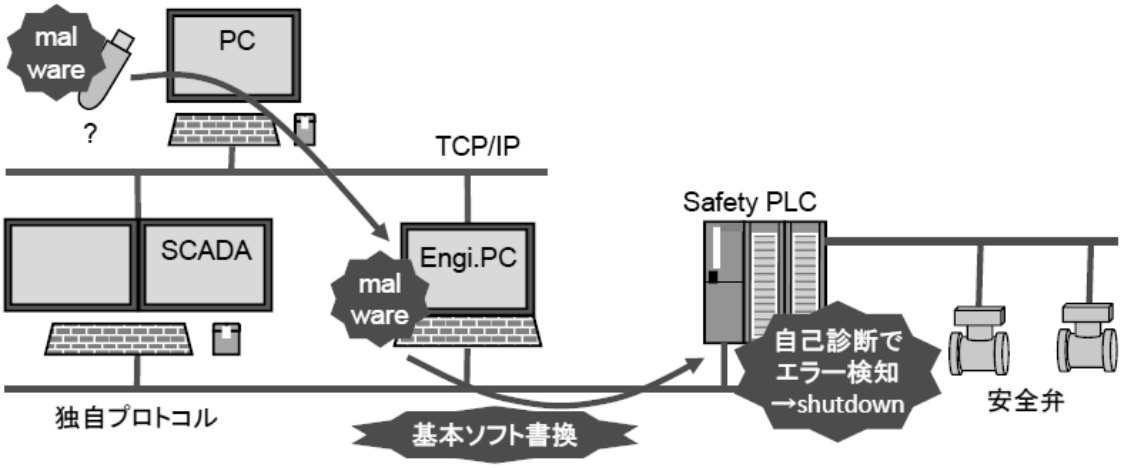


付図 E-2 Industroyer の電力系統制御システム攻撃例

(3) Triton (HatMan)

2017 年、サウジアラビアの石油化学プラントが緊急シャットダウンした。エンジニアリングツールに感染したマルウェア Triton（HatMan）が、安全計装 PLC の基本ソフト（ファームウェア）を書換えようとした。この書換えは不完全であったため、三重系構成の安全計装 PLC の自己診断（基本ソフトの不一致）に引っ掛かり、安全計装 PLC は停止した。しかし、安全 PLC が停止すると、プラントは運転継続できないので、プラント全体がシャットダウンした。侵入経路は不明である。

過去の PLC に対する攻撃は、ユーザが作成するアプリケーションプログラムまたはパラメータの書き換えであったが、本件は安全計装 PLC の基本ソフトを攻撃した初の事件である。この事件後、PLC ベンダーは基本ソフトの保護対策を強化した。また、ユーザ／インテグレータは、安全制御計のセキュリティ対策に乗り出した。



付図 E-3 Triton（HatMan)の安全制御攻撃例

(4) Wannacry

2017 年 6 月、国内の自動車工場がマルウェア Wannacry に感染し、工場の生産設備用パソコンが動作不能となり生産設備が停止し、2 日間約千台の自動車生産に影響した。Wannacry は、パソコン内のファイルを暗号化してその解除のために身代金を要求するマルウェアであり、2016 年 5 月にメールを介して世界的に流行した。被害に遭った会社の情報部門は、その時点で情報システムに関して全社的対策を進めていたが、生産部門の古いパソコンまで管理が届いていなかった。

同マルウェアによる工場の生産システム停止は、台湾の半導体工場などの複数例が報告されている。情報システム向けのマルウェアが、工場生産を停止できる実例である。

付図 E-4 Wannacry の警告ダイアログ

(ニュージーランド政府　サイバーセキュリティ通信統合局(NJCCIC)より)

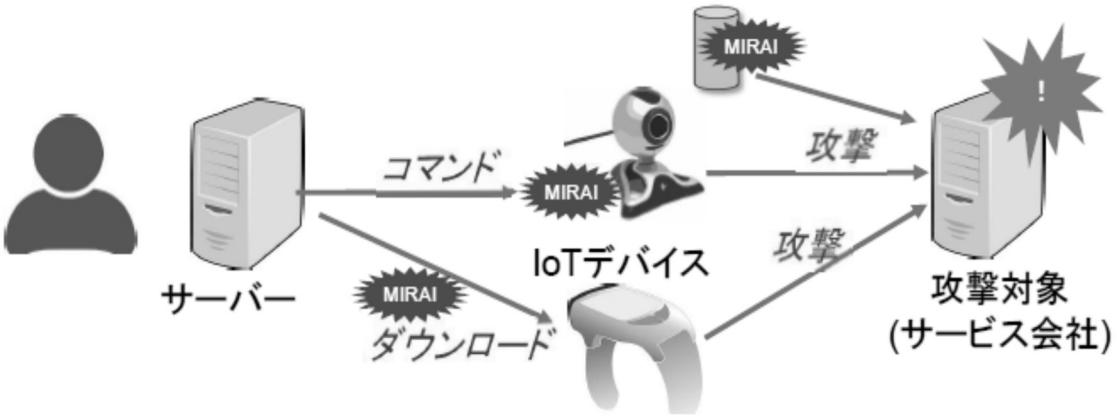
(5) MIRAI

2016 年 9 月、あるセキュリティジャーナリストのブログが DoS 攻撃(過負荷攻撃)を受け、彼のブログがしばらく見えなくなった。この攻撃は、Linux ベースの IoT デバイスに感染するマルウェア MIRAI による。MIRAI に感染した多数のデバイス(監視カメラ、携帯情報機器等)が、犯人の攻撃指令によって一斉に攻撃対象のサーバーに問い合わせして、DoS 攻撃となった。

同年 10 月には、別の DNS サービス会社が MIRAI に感染した 10 万台以上のデバイスから

DoS 攻撃を受け、多くの商用サービスが停止した。

MIRAI は、デバイス所有者が気付かぬうちに彼のデバイスに感染するため、所有者は自分が攻撃に加担していることに気が付かない。そのため、攻撃を防御する、あるいは感染から復旧することは難しい。



付図 E-5 MIRAI による DoS 攻撃

付録 F-作業委託報告書（議事録等を含む）

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における作業委託
報告書

2020 年 2 月

エム・アール・アイリサーチアソシエイツ株式会社

目 次

1. はじめに 90
2. 研究部会の開催 91
3. 議事録の作成 92
4. 研究部会資料の作成 93

付録

1. はじめに

（一社）日本機械工業連合会（以下、日機連）が設置する「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部会」（以下、研究部会）の検討を支援するために、以下の作業を行った。

① 研究部会での議論を整理した議事録案作成
② 研究部会の議論のための資料作成

以上

2. 研究部会の開催

本調査研究の目的を達成するために、機械安全及び設備安全に関する有識者から構成される研究部会を組織し、以下に示す 6 回の研究部会を開催し、検討を行った。

- 第 1 回　2019 年　6 月　4 日
- 第 2 回　2019 年　7 月 22 日
- 第 3 回　2019 年　9 月 19 日
- 第 4 回　2019 年 11 月 20 日
- 第 5 回　2020 年　1 月 20 日
- 第 6 回　2020 年　3 月 11 日

3. 議事録の作成

各研究部会での議論を整理した議事録を作成し、提出した。作成した議事録を付録 F1 に示す。

4. 研究部会資料の作成

研究部会での議論のための資料として以下の資料を作成した。

- 第 1 回研究部会用資料
- 第 2 回研究部会用資料
- 第 3 回研究部会用資料
- 第 4 回研究部会用資料

作成した資料を付録 F2 に示す。

付録

F1 議事録

F2 研究部会資料

付録 F1 議事録

<table>
<tr><td colspan="3">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部会
第１回　議事録</td><td>作 成
エム・アール・アイ
リサーチアソシエイツ</td></tr>
<tr><td>開 催 日 時</td><td colspan="2">2019 年 6 月 4（火）　15:00~17:00　　開 催 場 所</td><td>ステーション
コンファレンス東京</td></tr>
<tr><td rowspan="3">出 席 者
（敬称略）</td><td>委員</td><td colspan="2">向殿（明治大学）、神余（三菱電機㈱）、石川（住友重機工業㈱）、木下（平田機工㈱）、笹川（(一社）日本工作機械工業会）、澁谷（テュフズードジャパン㈱）、首藤（システムズエンジニアリング研究所）、杉原（パナソニック㈱）、土屋（㈱三菱総合研究所）、畑（機械安全実践技術促進会）、森本（㈱制御システム研究所）</td></tr>
<tr><td>オブザーバ</td><td colspan="2">結城、河野（内閣官房 内閣サイバーセキュリティセンター）、引野（経済産業省）</td></tr>
<tr><td>事務局</td><td colspan="2">宮崎、野村、吉田（(一社）日本機械工業連合会）、藪田、岡崎、畑中（エム・アール・アイ　リサーチアソシエイツ㈱）</td></tr>
</table>

計 20 名

1. 開会

事務局及び主査より開会挨拶を行った。

2. 平成 30 年度の成果及び 2019 年度の討議範囲について

事務局による資料（第 1 回研究部会用資料）に基づく説明後、以下の議論があった。

- 今年度の課題について意見を伺いたい。【向殿】
  - 今年度は、IT セキュリティ対策よりもレジリエンスに重点を置き、昨年度の結果に基づき対策の検討を行うことを想定している。リスクアセスメントやリスクマップを作成する人材に対してセキュリティの啓発に繋がる資料を作成できれば、本事業の目的達成と考えている。【神余】
  - IT セキュリティ対策は、基本的に IT セキュリティの専門家に任せる立場とする。【向殿】

- IPA のガイドライン等では IT 系の対策から先に記述されるが、企業投資の観点からは復旧に対する優先度の方が高いと考えられる。【神余】

- ボーイング 737MAX やシーサイドラインの事故の根底にあるものは、コンピュータによる設計によって本来の基本安全設計が劣後し、頼るべき機能安全が意図通りに機能せず事故に至ったことと考えられる。オーナーズコントロールの効かない IT 機器は便利だが、最終的な安全はエンドポイント側で確保するという原則が崩れてきている。【結城】
  - IT 側の検討がセーフティに関わる場合には、機械側のセーフティの検討で対応する。そのため、IT 側との接点は押さえておく必要があると考える。【向殿】

- 当初は外部環境に繋げることをやめる案があった中で、安全に繋げるという方向性で検討を行い提言としてまとめた。提言としては弱いという印象を持った。【結城】
- 世間に知られなければ効果が無い。【神余】
- 今年度の成果として提言をまとめ、世間に発表することとしたい。【向殿】

- IT のネットワーク機器のベンダー・代理店は自身の分野に関しては理解している。それらを用いることで利便性のみを謳ってネットワーク等を構築する SE が第 3 極として存在する。機械の専門家が安全と TLC を区別しても、気付いたら繋がれている可能性があり、町工場への啓発、もしくは、SE に対する牽制ができなければ安全の確保は困難ではないか。【森本】
- 現状と課題を整理してはどうか。【結城】
- メーカ向けの IEC 62443-4 シリーズは良いが、インテグレータ向けの IEC 62443-3 シリーズはユーザが SE に丸投げする日本の実態に即していない。【神余】

- シーサイドラインの事故は、クリティカルな装置の異常に対する対策が本質安全に則っていないために起きたと言える。【森本】
- 本来は本質安全がある大前提の上に機能安全があるべきであるが、本質安全を無視してコンピュータでのみ制御しようとすると、今回のような事故が起きる。セキュリティの問題が生じても人命が失われないように安全を確保するためにはどうするか。【向殿】
- 人は間違える・機械は壊われる・ソフトは騙されるが、それでも安全を確保することがゴールである。【神余】
- エンドポイント側で対策を行うしかない。【畑】
- 機能安全が浸透しソフト指向になったときに、機械安全のプリンシプルを守るべきであるが実態は異なっている。なおかつ、中間の役割である日本のインテグレータは機械安全を理解していない。機能安全が浸透しソフト指向になり本質的にあったものが変質し、本来と異なる形になってきたことを例示し、本来あるべきプリンシプルを今年度の成果として示すのはどうか。【首藤】
- 異論は無い。【向殿】
- IEC/TC44 が担当する IEC TR 63074、ISO/TC199 が担当する ISO TR 22100-4 に対して、日本からカウンターを挙げていくことに意味がある。【神余】
- メーカ側（ハードウェア）からセキュリティ側・インテグレータ側に方針を提示できるようなマニュアル・ガイドラインがあれば良い。【向殿】
- 作成するガイドラインを、ISO、IEC に日本からの提案として示すこともできる。日本の考え方が欧州で認められなければ、設計変更を行わなければ輸出できなくなる。【神余】
- 良い提案だと思う。日機連が行ってきたことにセキュリティの考え方を加え、インテグレータがどのように関与すべきかを明確にできると良い。【畑】

オブザーバによる持参資料に基づく説明後、以下の議論があった。

- システムメソッドとは、セキュリティバイデザインに相当することの理解が、進んでいない実態がある。コンピュータ設計による機能安全が強くなり、伝統的な機械安全が軽視される傾向にあることが最近のトレンドである。【結城】
  - 基本的な安全設計思想を無くしてしまった。機械安全が軽視されつつある傾向に対する警鐘を機械の専門家の立場から提言すべきではないか。【結城】
  - コンピュータの進歩によって、安全の思想を理解していない IT の専門家が設計を行うようになり、機械の専門家が当然と考えていることが軽視されつつある。【向殿】
  - 提言を行うのであれば、リスクが存在するという前提を明示した方が良い。【森本】
  - ISO/IEC 27001 のリスクは誰でもできるが、システムやユースケースの知見が必要とされる部分については機械の専門家の出番と考えている。その点においては、IT の専門家と機械の専門家は融合できる。【結城】
  - 物理空間の安全は機械の専門家で確保したい。【向殿】

- 提言を社会に公表することについてはどうか。【向殿】
  - 異論は無い。ただし、提言だけでなく、証拠・理由を事例という形でまとめ提示したい。人は事例に関心が向かう。【宮崎】
  - 根拠の明確化は必要と理解している。報告書には提言とその根拠を記述する。提言は学会や日本工学アカデミー等の第三者機関から公表することも一案である。【向殿】
  - コンピュータの進歩によって機能安全の概念ができたことで、本来あった機械安全が変質してきた。例えば、具体的な事例を根拠として示し提言に繋げられれば良い。【首藤】
  - 自動車の機能安全（ISO 26262）には本質安全があまり含まれていないため、機能安全のみで安全確保する方向に進んでいる。普通の機械であれば本質安全の上に機能安全がある。【向殿】
  - このことが最も重要な発信内容である。機能安全は便利で素晴らしい。しかし、やるべきことをやった上で初めて機能安全が確保される。【向殿】

- 事例とは事故のものという理解で良いか。【森本】
  - 本質安全設計の重要性に係る事例は首藤委員のアイデアを採用したい。これだけやられていないから考えましょうといった内容で良い。【宮崎】
  - 事例はある程度の数がほしい。やってみたという事例は稀なはず。【神余】
  - 考察でも良いだろう。【宮崎】
  - 可能な範囲で各社の事例を提示できないか。【神余】

- 参考情報だが、生産システムのエンドユーザに、ネットに繋ぎたいか聞いたところ、No との回答だった。保守点検を目的としたメーカとしては繋ぎたいという立場である。エンドユーザは、外部環境へは未接続で良いが、ソフト化して利便性は向上させてほしいと考えている。【木下】
  - 実装面における課題が、メーカとエンドユーザとの間で異なることによって生じるトラブルは、良い事例になる。【結城】

- 米国有識者からビューロクラシーリスクが、リスクの中で最も厄介であると聞いた。【結城】
  - ブロックチェーンも完璧ではないと専門家から伺った。そのとき、人命が失われなければ良い。【杉原】
  - 繋がることで生じるセキュリティの問題から、人命を守ることがセーフティの基本概念である。【向殿】
  - 外部から繋ぐこと自体をナンセンスと考えるか。最低でもプロファイルを変更できるルータを用い、ブロックできる物理的手段を備えることを望ましいと考えるか。落としどころをどうするか。【森本】
  - 正解は 1 つではなく幅があると考えている。今回の対策としては、IT、フィジカルセキュリティ、物理側の安全といった場合分けによる複数のパターンが必要なのではないか。【神余】
  - 繋げた場合における、方法、脅威への対策、残留するリスクをまとめるという理解で良いか。【向殿】
  - どんなリスクがあるかを分かり易く伝えることではないか。【森本】
  - リスクに対するアプローチと、システムの感染を前提として復旧に力を入れるという考え方もある。【森本】
  - 抽出された全てのリスクに対して対策を行うのではなく、許容されないリスクに対して、行うべき対策の種類や、リスク発生の予防となり得る設計方法の指針を作成するのではないか。【結城】
  - その通り。1 つのシステムでも複数の対策がある。【神余】
  - リスクは時間とともに変容することも対策を難しくする要因だろう。【結城】
  - その通りである。IEC 61508 にはセーフティ監査とセキュリティ監査をシンクロできればという議論がある。【神余】
  - IT と OT のハイブリッドシステムになる際には、全体を俯瞰できる人材が必要になる。JASA の委員会とコラボレーションすれば良いものができそう。【結城】

- 投資対象をどこにするか。セキュリティ対策への投資より、トラブルが起きることを前提にレジリエンスに投資する考え方もある。繋がなくても実はリスクがある。繋げた場合のリスクもある。これらのリスクを示す必要がある。【向殿】

- セーフティの基本的な考え方における機能安全の位置付けと、機能安全が表立つことで機械安全の本質が忘れられがちになっている事故事例を示す。繋げることによるセキュリティの考え方・対応方法を示す。エンドユーザがインテグレータに示す仕様書作成の一助となるようなガイドラインを、日機連の報告書として提示できれば良い。【向殿】
  - 今年度は事例が沢山あるとしか言えないのではないかと考える。リスクアセスメントはある程度 1 本化できるが、ウェイトの置き方次第で対策は複数存在する。【神余】
  - 入口は誤作動のみである。誤作動の要因はサイバーアタック、バグ、EMC ノイズのいずれかで、その結果どうするかだけである。【杉原】

- セキュリティはハザードの１つに過ぎない。【向殿】
- 機械の専門家はゴール（機械）があるため概念を理解できるが、IT の専門家は機械と IT を別物と考えている。【神余】
- 最後は合わせるが、アプローチとしては両者が噛み合わない前提で検討を進める。【結城】
- 今回の議論で、かなり方向性は決まったと考えられる。【向殿】

- 具体の事例、IPA のガイドライン等を収集し、それらを理解した上で本会の狙いどころを検討し、リスクアセスメントを手分けして実施することになる。9 月頃までは様々な答えを収集する。【神余】
- 確定論的回答でなければならないか。確率論的回答でも構わないか。【杉原】
- 対策は確定論である。原因の発生には双方あり得る。【神余】
- 原因から入るか。セキュリティ面には様々な要素があるため、原因から入ると分からなくなる。結果保証（安全）からの方が絞りやすい。【結城】
- IT よりレジリエンスに重点を置き議論することになるだろう。【神余】
- FA や OT といわれる現場でセキュリティ対策と称して行われている対策を収集するという理解で良いか。【森本】

- 次回の部会では、各自が収集した事例に基づき表の項目について議論する。【向殿】
- ゴールは IT の専門家ではなく日機連のユーザが活用できることとする。【神余】
- 機械安全の人命を守るという大前提に対するハザードの 1 つとして、繋がることで様々なウイルスや悪意が入り込むことによって人命が失われる可能性があり、これを如何に防ぐか。入らなせない対策と入った後の対策といった切り分けで十分ではないか。【向殿】
- 機械の専門家は制御系を信用していないため機械だけで安全性を保障する設計を行う。その逆もまた、然りだろう。【神余】
- ゼロトラストの時代に入ったと言える。日本も米国のサイバーの政策は全てゼロトラストに基づき動いている。【結城】

- 議論を伺い、複数モデルの検討は難しいのではないかと感じた。モデルを 1 つに絞って対策のパターンを検討することでも良い。【宮崎】
- 鍋蓋ラインだけで、例えば、セキュリティを重視するパターンや、ある程度リスクに寛容なパターン等といった十分な検討ができるか。【向殿】
- 原因は１つかもしれないが、取れる対策は複数あるというイメージである。【宮崎】
- 複数ラインの検討を行うのではなく 1 つのラインに対する複数の対策を検討した上で、総合的な検討（レジリエンス、ファイアーウォール、ログ解析等）を行う。【神余】

- トレーニングカリキュラムに関しては誰にどのレベルになってもらうかが見えない。【神余】
- 必ずしもトレーニングカリキュラムまで検討が進まなくても良いかもしれない。【宮崎】
- カリキュラムの作成は困難だが、必要な人材についてまとめたい。【神余】
- トレーニングは副主査の意見を採用したい。【宮崎】

- 対象等の大枠のみ検討することとしたい。具体はどこかに任せたい。【向殿】
- 機械の専門家が最低限知っておくべきものになるべきである。【神余】
- ユーザが発注する際にインテグレータの質を評価できる軸だけでも良い。【森本】

3. 次回の日程等について

次回の調査研究部会は、7 月 22 日（月）13：30～16：00 に決定した。

各委員は、次回の調査部会までに、実際に行われている対策や事故事例、IPA のガイドラインといった資料等を収集する。

4. 本日の総括

- 今年度目指す成果（案）について

- 機械の専門家の立場から人命を守る機械安全への提言を公表
- 提言の根拠とした事例から得られた対策・コスト等の検討をまとめた報告書を公表
- 機械の専門家の立場から人命を守る機械安全に資するために必要な人材を定義

以上

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部会 第２回　議事録			作 成
			エム・アール・アイ リサーチアソシエイツ
開 催 日 時	2019 年 7 月 22（月） 13:30~16:00	開 催 場 所	ステーション コンファレンス東京
出 席 者 （敬称略）	委員	向殿（明治大学）、神余（三菱電機㈱）、石川（住友重機工業㈱）、木下（平田機工㈱）、笹川（(一社）日本工作機械工業会）、杉田（テュフライインランドジャパン㈱）、首藤（システムズエンジニアリング研究所）、杉原（パナソニック㈱）、土屋（㈱三菱総合研究所）、畑（機械安全実践技術促進会）、森本（㈱制御システム研究所）	
	オブザーバ	結城（内閣官房 内閣サイバーセキュリティセンター）、引野（経済産業省 商務情報政策局）	
	事務局	宮崎、野村、吉田（(一社）日本機械工業連合会）、薮田、岡崎、畑中（エム・アール・アイ　リサーチアソシエイツ㈱）	

計 19 名

1. 開会

事務局及び主査より開会挨拶を行った。

- 本部会は、セーフティの専門家としての立場からセキュリティを考慮した ICT を利用した生産システムの安全確保についての考え方の提案を行う意義のある研究である。最終年度である今年度も着実に成果をまとめ外部に発信するべく引き続き協力をお願いしたい。【向殿】

2. 2019 年度の討議範囲、成果について

事務局による資料（第 2 回研究部会用資料）に基づく説明後、以下の議論があった。

- 機械における ICT の使い方としては、クラウドの利用もしくは工場内に閉環境を構築してネットワークを利用する程度に限られることが昨年度の工場視察や議論を通じて結論付けられ、これを前提としたシステム構成に基づきリスクアセスメントの検討を行った。今年度は IT、安全、物理といった各要素に振って検討した対策を検討することを想定しており、ベストプラクティス・ケーススタディのような検討結果を成果として提示することになる。【神余】
  - 機械の専門家の立場から最終的な人の安全が守るための考え方の提案を行うことが、本部会の意図するところである。【結城】
  - 機械の専門家としてできる検討は、IT の対策としてはゲートウェイ、フィルタリング程度に限られるため、安全及びレジリエンスの側面になる。【神余】
  - 米国で可決された National Defense Authorization Act(米国国防権限法 2019)でも、サイバー攻撃で問題が生じた場合には、最終的には手動に切り替えることが提言されている。

本部会の成果も同様の考え方を大前提としたものにすべきである。【結城】
- 機能安全はセキュリティ脅威に対して万全ではないため、最終的には電源を切る術を残しておく必要がある。【神余】
- 生産システムにICTを利用する上での安全確保の基本概念として、最終的には手動で電源を切るという考え方を提言の前提として提示した方が良い。【向殿】

- 重要なことはICTを過信しないことである。【神余】
- ICT の利便性は享受するが、不確実性・蓋然性があり得るため、エンドポイントである機械側で安全対策を考慮する必要がある。【結城】
- 機能安全設計を考える前に本質安全を確保しておくことが最重要ポイントである。機械安全における安全設計の考え方が無視されている。【向殿】
- 繋げたことによるリスクを検討することが良いのではないか。【畑】
- 異論は無い。【神余】
- 検討を行う上での思想をまとめることも必要と考える。【向殿】

- 昨年度に検討を行った鍋蓋製造ラインにおける制御システム想定及びICTによる外部接続を前提として、存在する脆弱性と対策の方向性を、ガイドラインのような形で今年度の成果として提示できれば良いと考える。【杉原】
- ガイドラインは、リスクアセスメント、カウンターメジャーのどちらの立ち位置を想定しているか。前者はガイドラインとして提示が可能であるが、後者はケースバイケースであり、事例として提示は可能だがガイドラインとして提示が可能か疑問である。【神余】
- 全てのシナリオからモデルとして 1 つの対策を提示することは困難だが、例えば、シナリオ単位にケースを 1 つ特定すれば対策の検討が可能ではないか。【森本】
- IT、安全、レジリエンスのそれぞれに寄った極端な対策を提示しつつ、実際に対策を行うバランスポイントは利用者側（例えば、工場）で判断してもらうような形を想定しており、今後の部会においてケース毎に検討を行う担当者を決めたい。【神余】
- 検討を行うベースは昨年度のリスクアセスメントシートという理解で良いか。【森本】
- 良い。【神余】
- 議論を聞いていると委員のリスクに対する定義が曖昧な印象がある。リスクとは目的に対する不確かさの度合いであり、部会における定義付けが必要である。【結城】
- 機械安全のリスクアセスメントに考え方を合わせようとしている。【神余】
- ケースによって求められる対策が異なる。FA で考えられるテーマ（遠隔監視、生産効率化）で、人的被害と品質低下のリスクを被害シナリオとして区分し脅威と脆弱性の検討を行った。【森本】
- 安全が何に対するものか明確にする必要がある。【畑】
- ICT 利用のリスクは社会不安等を含め様々存在するが、生産システムの安全を考える場合には人命の安全に割り切って考えることとした。人命の場合には ISO/IEC ガイド 51、社会全体の場合には ISO 31000 で定義されるリスクがある。リスクの階層を理解した上で ISO/IEC ガイド 51 に基づきセキュリティとセーフティの考え方を検討してきた。基本原

理（3 ステップメソッド）の中で ICT 利用を考える場合には、ステップ 2（機能安全に相当）の前に本質安全を確保するという基本概念が重要である。【向殿】
- 提言の手前にある基本的な考え方、前提条件を提示する必要があると考える。【神余】
- ICT 利用の生産システムにおける安全の基本原則を提示することは分かり易く、将来に向けた良い提案になる。【向殿】
- 基本原則が押さえられた上で対策例を提示し、選択は利用者側で行う。【神余】

- 安全学の観点からボーイング 737、シーサイドラインの事故事例を提示しても良いのではないか。大前提があれば具体例の提示は有益と考える。【向殿】

- 安全関連部、非安全関連部を理解し両者を区分できる設計者は、実際の設計現場にほぼいないのが実情である。また、改訂等の変遷を経て一層理解しにくいものになっている。両者を規定することが本部会の議論でも重要と考えている。【石川】
- 重要であることに異論は無い。読者層として日機連の機械安全リスクアセスメントを理解している者を想定しているが、日機連の想定を踏まえたい。【神余】
- IT の専門家だけでなく経営層や役人に理解してもらう必要があると考えている。【結城】
- 不可侵な部分、考え方が提示されれば読者にとっては分かり易いだろう。【石川】

- 機械安全の最も重要な思想がないがしろにされた結果として事故が発生している。付加的な機能安全で本質安全をカバーできると考えられつつある傾向に問題がある。【向殿】
- 機能安全が広義に解釈されるようになった。【結城】
- 機能の定義が先になされるべきである。機能安全で全ての安全が確保可能と社会が考えるようになりつつある。人を守るには物理的に止める手段を設けることが、従来の本質安全による設計の思想であった。【向殿】
- オブジェクティブの明確化が重要である。何を繋がれても機械側で人の安全を確保するが、クラウド等へのセキュリティ対策は IT の専門家に任せる。【結城】
- 電源を切ること（工場停止）によって発生する損失よりも、人の安全確保が重要であることを基本原則としたい。【神余】
- 経営層のリスクマネジメントの視点としては利益優先もあり得る。【向殿】
- 基本原則として提示する必要がある。【神余】
- 経営層は ISO 31000 を意識しており、基本原則の提示は重要と考える。【石川】
- 本部会が対象とするリスクが何であるかを明確にする必要がある。【結城】

- 日機連が行ってきた機械安全のリスクより広義のリスクを扱う方向性で議論が進んでいる。日機連としての考えはどうか。【神余】
- 計画段階では、IT の危うさを理解した上で機械の専門家が ICT を活用できるようにすることを想定し、IT の専門家の想定はあまりしていなかった。【宮崎】

- 報告書骨子（案）の提言の上位に位置付けられる理念・原則にあたる論文・文献に基づき

本部会としての理念・原則（案）を、スライド 1 枚程度にまとめたい。【神余】

- 結果のまとめ方については、新たなシステムではなく昨年度の検討結果に基づきリスク対策を検討していきたい。【神余】
  - サプライチェーンリスクの検討は行わないか。【結城】
  - 検討しない。【神余】
  - サプライチェーンリスクに取り組むのであれば、次年度以降の委員会で検討すべき内容と考える。【向殿】
  - リスクの要素としては考慮すべきではないか。リスクの外枠を明確にした上で、本部会の検討対象とするリスクにフォーカスすれば読者が理解し易くなるだろう。【結城】
  - 考えるべき問題として指摘することは良い。【神余】

- ステークホルダ（経営者、ユーザ等）によって取るべき異なる対策をどこまで検討するかを議論する必要があると考えている。例えば、IEC 62443-4-1 だけでも開発者・検証者・全体のセキュアな開発プロセスのオーディターといった人物が登場する。来年度以降に教育カリキュラム等の開発を行うのであれば、細かく検討することは来年度以降の調査研究の出口に繋がると考える。【神余】
  - プロセスを考慮して業務を遂行するためには能力のある担当者を育成する必要がある。製造業で品質向上を目的に現場改善を行う担当者にはセキュリティに対する知見が無い。リスクから安全を確保するためのプロセスや能力についての定義が必要である。【森本】
  - IEC 62443 もしくは IEC/TC44 を活用すれば良いと考えている。本部会から TC44 に対する提案（例えば、IEC TR 63074 のアップデート）を行うことも良い。【神余】
  - 中小企業がリスクアセスメントを行い適切なカウンターメジャーを選択できるようにすることを目標とすることも 1 つの案である。ただし、中小企業が必要としているか否かは不透明である。【神余】

- 本部会としては、トップの人材を育成しても意味が無い。【神余】
  - ICT の基礎力を有せずに製品が活用されるような現場への教育にフォーカスすべきと考える。【結城】
  - リスクアセスメントができること、及び、カウンターメジャーが取れる基礎的な知識が身に着けられれば十分であると考えている。【神余】
  - 3 ステップメソッドに立ち返ることが重要である。【結城】
  - 今年度の成果としては、具体のシステムによる対策及び整理ができれば良い。【森本】
  - 異論は無い。人の教育にはベースとなる規格を調査する必要がある。【神余】
  - 人の教育は後回しにすることとしたい。【向殿】

- 提言の上位に理念・原則を入れる。提言に対する根拠としては事例を想定していたが、具体的なイメージはあるか。【神余】
  - 機械安全の根拠としては ISO 12100 ではないか。ICT 環境下での機械安全を改めてどうす

るか。【結城】
- ガイドラインとしては既に発行されている IEC 62443 に従うことになるが、中小企業への適用は困難である。【神余】
- 中小企業を対象とするならば、ISO 12100（基本安全規格）、ISO/IEC 27000（情報セキュリティ規格群）、IEC 62443（制御システムセキュリティ）に基づき、機械安全を確保しつつある程度低コストで実現可能な対策を幾つか選択することになる。まとめ方としては、3 つのカテゴリ毎に選択した典型的な対策を鍋蓋製造ラインもしくはトラブル事例等に適用し、対策を行うことの効果を検討する。最終的に何を選択するかは現場次第である。【森本】
- ガイドラインは事例を相当数検討しなければできないだろう。【向殿】
- 性能規定の解釈を作ることと理解している。【結城】
- その通りである。対策と参照すべき規格の明確化ができれば良い。【神余】
- ユーザに対して啓発を行うのであれば、インテグリティを乱すようなランダム故障についても記述した方が良いだろう。【森本】
- 異論は無い。【神余】

- システムを考える上でのセキュリティのチェックリストがあると良いのではないか。【畑】
- IEC 62443 には記述があまり無い。【神余】
- IEC TR 63074 を分かり易く解釈できると良い。【畑】
- 分野が異なると対策も異なる。ある程度決め打ちした代表的なパターンを提示しなければ業界は動かない。まずは選択できる範囲を作りたい。【神余】
- 設計者がセキュリティの検討を行う上で考慮すべき項目を明確にできれば良い。【畑】
- 本質安全を踏まえて安全・非安全を区分した設計を行い、安全系にネットワークを接続しないことを、回答としてガイドラインに記述することも 1 つの案である。まずは、並列に並べることで安全・非安全という世界観を知らしめることが重要ではないか。【森本】
- 共通して必要な対策は、ファイアーウォールによる不要なパケットの切断、バックアップの構築、電源の切断の 3 つ程度ではないかと考えている。【神余】

- 安全関連部は繋がないという考え方が示されたが、可能性として繋がる構成である場合に、検知や切り離すことはできるか。【首藤】
- 切ることが本質安全に近いアプローチである。繋ぐ必要がある場合には機能によるセキュリティ（パケット計測装置やホワイトリストの導入、ネットワークの分離等）に頼らざるを得ない。対策の実施で脅威に対するリスクは低減が可能であるが、コストバランスが重要であり、特に中小企業が受け入れ易い対策と効果を具体に提示したい。【森本】

- 対策が機能安全に寄った時にインテグリティを高めればある確率で大丈夫という議論だけで製品化を行う流れが最近強くなりつつある印象があるが、本部会で、機能安全のインテグリティにまで踏み込んだ提言を行う必要があるかは疑問である。中小企業は、機能安全のインテグリティまで意識したシステム設計を行っていないだろう。【森本】

- 自動運転中に攻撃を受けた場合には、不可能かもしれないが G センサ（アナログ）が挙動の異常を検知したことでソフトウェアを介さずに急ブレーキをかける。ロボットの場合は、危険か否かの判別ができない時点で検知しようがないのではないか。ウイルスに侵されないアナログセンサは科学的に不可能と思う。【杉原】
- 対策が可能な機械設備もあれば、複雑なロボットであれば機能安全のインテグリティによる対策が必要になる。【森本】
- 考えるのはあくまでも読者として想定する中小企業である。【神余】
- 汎用生産設備において安全 PLC をネットワークに繋げる必要が無いことは提示した方が良いのではないか。【杉田】
- 例えば、機械のテンション等の設定が必要なのであれば安全パラメータを入力する必要がある。【神余】

- 手動の概念を明確にした方が良い。【森本】
- 遠隔手動と現場手動が異なることは明確にすべきである。【結城】
- 主電源断路装置を必ず設けるということである。【杉原】

- 設計思想が現場の経緯で多少揺らぐことはあり得るだろう。あるべき論を提示すると使い勝手が悪くなるため、対策の優先度や事前に行うべき対策等が提示できると良い。【森本】
- パターン毎（IT、安全、復旧程度）の対策を洗い出し、議論を開始したいと考えている。そのために、次回の部会ではパターン毎の担当者を割り当てられると良い。【神余】
- 例えば、各自で対策を 3 つ程度検討し、次回の部会で議論を行うことはどうか。【森本】
- 昨年度のリスクアセスメントシートに基づき、各自が選択した 3 つのリスクに対していずれかの立場（カテゴリ）で各々1 つ程度の対策を検討してほしい。次回の部会で、各自の対策の検討結果に基づき議論を行い、カテゴリ毎の役割分担を決定したい。【神余】

- 最終的には、昨年度のリスク焦る面とシートに、カウンターメジャー・参照規格・再 RA の結果が示されれば、対象とする中小企業にとって有益なものができる。【神余】

- まずは、各自の主観で対策を検討した上で、次回の部会での議論を通じて対策の優先度の個人差を埋めていけば今後の検討が進む。カバレッジ範囲が広くなるように整理したいと考えている。【神余】

3. 次回の日程等について

次回の調査研究部会は、9 月 19 日（木）13：30～16：00 に決定した。

4. 今度の作業について

- 宿題事項
- 報告書骨子（案）提言の上位に位置付けられる理念・原則にあたる論文・文献があれば、

本部会関係者に共有する。【向殿主査】

- 向殿主査から共有された論文・文献に基づき報告書に提示する理念・原則（案）を、スライド 1 枚程度にまとめる。【神余副主査】
- 昨年度のセキュリティ脅威リスクアセスメントシートに基づき対策の検討を行い、リスク対策記入フォームに検討結果を記入し、第 3 回研究部会の前までに事務局に提出する。【全委員】
- 対策を検討する難しさを体感することが目的なので、リストから数件選んで記入すればよい。【神余副主査】

- アクションプラン及び決定事項

- 昨年度の本研究部会で検討したセキュリティ脅威リスクアセスメントシートに基づき、対策（IT、安全、復旧の 3 カテゴリ）を検討する。
- 第 3 回研究部会では各委員の検討結果に基づき議論を行い、議論を踏まえた上で、対策カテゴリ毎の検討担当者を決定する。
- 本研究部会において生産システムの企画等の実務担当者が備えるべき能力等の整理を行うか否かについては、現時点では未定とする。

※対策のカテゴリは今後の議論を踏まえて修正される可能性がある。

以上

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部会 第３回　議事録			作 成
			エム・アール・アイ リサーチアソシエイツ
開 催 日 時	2019 年 9 月 19（木） 13:30~16:00	開 催 場 所	ステーション コンファレンス東京
出 席 者 （敬称略）	委員	向殿（明治大学）、神余（三菱電機㈱）、石川（住友重機工業㈱）、木下（平田機工㈱）、登山（テュフーズドジャパン）、杉田（テュフラインランドジャパン㈱）、首藤（システムズエンジニアリング研究所）、杉原（パナソニック㈱）、土屋（㈱三菱総合研究所）、畑（機械安全実践技術促進会）、森本（㈱制御ｊシステム研究所）	
	オブザーバ	結城、細川、河野、溝添（内閣官房 内閣サイバーセキュリティセンター）、河合（情報処理推進機構）	
	事務局	宮崎、野村、吉田（(一社）日本機械工業連合会）、薮田、岡崎（エム・アール・アイ　リサーチアソシエイツ㈱）	

計 21 名

1. 開会

事務局及び主査より開会挨拶を行った。

2. 2019 年度の討議範囲、成果について

事務局による資料（第 3 回研究部会用資料）に基づく説明後、以下の議論があった。

- 事務局から提案された報告書の構成（案）に異論は無いか。【向殿】
- 今年度まとめる報告書は、3ヵ年分の成果をまとめた形式とする必要があるか。【神余】
- 過年度の報告書では議論の過程が記述されている。最終年度の報告書では成果をまとめたものとしてほしい。【宮崎】
- 報告書だけでは現場が活用できないため、別冊を用意するのではなかったか。【結城】
- 3ヵ年の検討成果をガイドとしてまとめられれば良い。【宮崎】
- 成果が与える影響力を念頭に置き報告書をまとめていきたい。【向殿】

3. セーフティとセキュリティの基本的な考え方について

神余副主査によるセーフティとセキュリティの基本的な考え方の案についての説明後、以下の議論があった。

- 提案されたセーフティとセキュリティの考え方について意見はあるか。【向殿】
- 安全な状態にするという目的の観点から検討することに異論は無い。日本ではセーフティもセキュリティも安全と解釈されることが多く、好ましくない状況から守るという同義と捉えられる。【結城】
- セーフティとセキュリティを包含する安全の英語はあるか。【向殿】

- Surety ではないか。機械の専門家が捉える安全の方がより広義であるため、ISO/IEC ガイド 51 だけでなく ISO 31000 の要素が必要となる。【結城】
- セーフティとセキュリティにおけるリスクアセスメントの方法論は異なるが、概念としては同一と捉えて、双方が維持されている状態の表現方法を検討した。【神余】
- セーフティとセキュリティ、アベイラビリティと信頼性、レジリエンスの概念を含む新たな言葉を作りたい。Surety は人間系も含めた意であるか。【向殿】
- Surety について、米国では、核物質防護で使われている。【結城】
- 標準化組織においては Trustworthy が使用されている。【河合】
- 安全に信頼・信用の概念を含めるか。安全の議論が必要ではないか。【向殿】

- 本研究部会においては、セーフティを生産システムで人が怪我をしないことと定義した上で、本質安全による安全確保を第一義的に行うとして、ICT を利用する場合には、ICT による安全担保の仕掛けが阻害されるようなハザードを要因としてセキュリティを検討した。セキュリティを、本質安全・機能安全を阻害するハザード要因の 1 つと捉えた方が、過去からの議論と整合する。セーフティとセキュリティを、同一概念に基づいて同じ目標を持ったシチュエーションの相違と捉えると、本質安全と機能安全として確保すべき安全をどのように考えるか。【森本】
- 副主査からの提案は、原因に悪意があるか否かで区分した考え方と理解している。【向殿】
- 現在のリスクは複雑系であるが故に様々な原因があるが結果は 1 つであり、結果から捉えた方が対策を検討しやすい。近年のインシデントは、セーフティとセキュリティ双方を含む複合要因によって発生しており、人的側面・偶発的側面・意図的側面による発生要因が存在する。【結城】
- 実際に発生した全ての事故には、マネジメント・人間的側面・技術的側面が含まれる発生要因が存在する。【向殿】
- これまで行ってきた議論の範疇を、より広義に検討することを意識した。AI を含む ICT 等の新技術を利用する際に、これらの新技術をどこまで信用するかを課題と捉えて、想定外が起こり得る場合、最後には切り離すことによる安全確保が必要と考えた。【神余】

- 初見の読者に対して、最終的に電源を切る手段を残すことをどこまで訴求するか。【神余】
- 本研究部会では生産システムを念頭に置き、システムがより複雑化する中で、機械の専門家の立場から、被害系を、人命を最優先に財産、環境等へ拡張するという安全確保の概念を定義した上で検討を行ってきた。【向殿】
- 研究部会の報告書としては生産システムにおける人の安全に限定される。検討においては将来を踏まえて行うことの必要性は理解している。【宮崎】
- 電源を切る手段を設けることを前提としつつ、必要な機能安全まで喪失されない仕組みを構築する必要があることを提示したい。【神余】
- セーフティは原因から被害を特定可能だが、セキュリティは FTA 的に追わなければ被害を起こす事象を特定できない。【畑】
- 次年度以降、対象とする中小企業にセキュリティリスクアセスメントや対策を教育するた

めの検討を行うのであれば、アナロジーが必要と考えている。【神余】
- IEC/TR63074（機械類の安全性についての安全関連制御システムの機能安全に関するセキュリティ側面の技術報告書）との関係性等を総合的に提示する必要がある。【畑】
- セーフティと同様の概念であることは提示したい。【神余】
- 通常使用及びリスクアセスメントが容易に可能な範囲内の誤使用をセーフティの領域、予見不可能な範囲の使用をセキュリティの領域と理解している。【杉原】
- 従来、予見不可能として無視していた想定外を想定して対策を検討する必要がある。意図せず USB を PC に接続して発生した事故が、悪意のある人に仕組まれたものであれば、ヒューマンエラーではなくセキュリティに該当すると考えられ、想定事象として対策を検討する必要がある。セキュリティを想定できない事象と捉えることには違和感がある。【神余】
- 生産システムにおける ICT 等の利用を検討する上での基本的な考え方を、より広範に捉えた際の考え方をどう定義するか。【向殿】
- 過去の議論は範囲が限定的であったが、原則を考える上ではより広範な議論を行うことが有効と考えた。今後の議論を通じて、日機連の立場を踏まえた考え方をまとめ、提言の上位概念として提示するか、用語の定義として提示するかを決定したい。【神余】

- セキュリティの概念には、悪意を持つ存在が意図する行為をどう防ぐかが含まれる。【向殿】

- 対策を事象の発生後に行う行為、方策を事象の発生前に行う行為と捉えている。【向殿】
- 方策はカウンターメジャー、対策はインシデントレスポンスとなる。【神余】

- 研究部会での議論を通じて、根拠の明確化と想定される反論への対応ができれば、考え方を日本から世界に発信できる可能性を秘めている。研究部会の検討範囲をより広範に捉え抽象化して分類し、可能であれば適用範囲を拡大するための一例としての検討を行っていることを理解してほしい。【向殿】

4. リスク対策の検討結果について

石川委員によるリスク対策の検討結果についての説明後、以下の議論があった。

- 対策の実行前後で被害の大きさと可能性に変化は無いと判断されたにもかかわらず、リスクの大きさを「中」から「小」とした意図を教えてほしい。【神余】
- ネットワークに接続された安全シーケンサが、対策の実行で接続が切断されることによるリスクが下がると考えて「中」から「小」と評価した。【石川】
- 被害の大きさは変化しないが、可能性は下がったと考えることができる。【向殿】
- リスクマトリクスへの指標の追加について議論する必要がある。【神余】
- 現状の 3 段階評価のリスクマトリクスを用いると、被害の大きさが「大」の場合に、リスクを「小」と評価することには違和感がある。【宮崎】
- 機器の状態によっても危険度は変化するため、仕組みとして対応できるようなまとめ方が必要ではないか。【結城】

- 対策は、IT セキュリティ、被害を小さくする安全、早期復旧の 3 種類程度に区分されると考えている。ガイドは、中小企業が現場に合わせて対策の実行が可能になるような形式とする。石川委員から提示された対策は、安全にフォーカスしたものと理解している。【神余】
- 研究部会としてはネットワークへの接続を前提に議論を行うと理解しているが、安全関連部は接続しないという極端な対策を提示した。リードオンリーであれば安全関連部を接続しても問題は無いが、リードライトでは制約を設けた方が中小企業にとっての理解が平易であると考えた。【石川】
- 資産管理不足が原因でワームが閉環境に侵入した結果、3 日間業務が停止した事例がある。対策のターゲットは製品ベースという理解で良いか。【結城】
- 昨年度に検討した鍋蓋製造ラインのリスクアセスメントに基づいて、各委員が対策を検討することが今回の趣旨である。【神余】
- 海外メーカのある車種で起こった安全関連部のバグは、カーナビ経由で侵入されたことが原因である。車のような閉環境内であっても安全関連部が他のシステムと接続されていると安全関連部へのアクセスが可能になる。【石川】
- 監視だけのラインでも内部で通信があれば侵入される可能性がある。【向殿】
- ソフトウェアが異常な動作をする可能性がある場合、接続する設計は行ってほしくないと考えている。【森本】
- 接続しなければ利便性の向上を図れないという要求がある。イーサネットには接続するがインターネットには接続させないといった対応が現実的ではないか。【木下】
- 例えば、直接接続されない設計を行い、アップロードしたプログラムの妥当性を確認するプロセスが存在すれば、被害の大きさは「大」ではなく「小またはゼロ」と評価されるという理解で良いか。【杉田】
- 可能性がゼロになることはあり得ない。【向殿】
- ハザードの除外という概念がセキュリティにあるかを懸念している。【神余】
- 例えば、現場でメンテナンス用のコンピュータを接続したことで発生したインシデントをサイバーセキュリティとするか疑問だが、利用者のためには、ネットワークに接続しないシステムに対する考え方を明確に提示する必要がある。【杉田】
- 人への被害の大きさは機械との接触度合いによるため、機械自体の有する危険度に落とし込まなければならない。【畑】
- 例えば、モニタ情報の共有をフィルム写真で行うといったローテクであれば、サイバーアタックを回避できる。安全関連部のメンテナンスが一般化されていない現状において、物理的な対策だけでなく、機器使用や無効化のルール設定等の手順、プロセスがガイドとして整備されると、設計者にとっての有用性が高まると考えている。【石川】
- 技術による安全方策ではなく仕組みや手順や管理に任せる安全がある。【向殿】

- 対策には、確率を下げる IT セキュリティ、被害を小さくするレジリエンス及びセーフティがある。マネジメントはどちらに属するか。マネジメントによる対策が有効であることは自明ではあるが、教育する際に、効果を説明できる必要がある。【神余】
- リスクの低減、回避、移転、保有のいずれかに収束するのではないか。【結城】

- 例えば、バックアップを保存するプロセスが機能していれば早期の復旧が可能になり、被害を小さくできる。一方で、USB の管理といった発生自体を防ぐためのプロセスであれば可能性を下げられる。人が関与するためテーマ次第ではないか。【森本】
- IEC 62443 から、セキュリティレベルの概念に、ルールの順守や組織のセキュリティレベルが与える影響といったユーザの側面を含める提案がなされていること、及び、セーフティにも安全文化の概念があることからも、マネジメントを成果に含めたいと考えている。【神余】
- 一般的な機械リスクのうちの 1 つとして情報技術のセキュリティリスクが加わると考えれば、3 ステップメソッドのような本質安全、残留リスクに対するセキュリティ対策を体系的にまとめやすい。【石川】
- セキュリティの脆弱性分析の観点からは、確定的な原因が無い場合でも、より広範に検討して想定外を無くすことができれば良いと考えている。【森本】

木下委員によるリスク対策の検討結果についての説明後、以下の議論があった。

- 被害の大きさが対策の実行前後で変化しない場合にリスクを下がったと判断するためには、可能性が大きく下がる必要がある。また、被害の大きさが「大」のセキュリティ脅威を、IT セキュリティによる手法のみでは下げることはできない。【神余】
- 対策の十分性を担保するようなパラメータを追加する必要がある。【畑】

- ICT も含めた新技術をシステムに採用するにあたっては、リスクアセスメントを実施した上での対策の検討が必要であることを提示したい。【神余】
- 安全に関わるシステム・装置に ICT 等を利用する場合、リスクアセスメントの実施と対策の検討を経なければ直接接続してはならないことを共通の考え方としたい。【向殿】
- 単一障害で安全性が損なわれるといった協調性の無い設計がなされることは従来あまり考えられなかったのではないか。【結城】
- フェールセーフという安全確認型の構造が主流になりつつあるためだろう。【向殿】
- 安全 PLC や安全関連部でトラブルが発生した場合の代替策は、現場では必ず用意されている。【神余】

- ICT 等の利用が前提であるためサイバーセキュリティに対する問題を検討するが、対策にはローテクが必須と考えている。【神余】

- 事例は、IT セキュリティ、セーフティ、レジリエンスの領域毎にまとめる。マネジメントについては今後の検討が必要である。現場に即した対策を検討する上で、バランスの重要性を提示したい。【神余】
- 世界的な EC サイト・Web サービスを運営する会社において発生した制御系システムに起因する大規模障害の事例は研究部会の検討に有用ではないか。フルデジタルでフェールセーフ設計を実装することは困難であり、経済性も劣ると思われる。【結城】

- 可能であれば事例としての活用を検討したい。【神余】

森本委員によるリスク対策の検討結果についての説明後、以下の議論があった。

- 松竹梅のレベルの判断基準は難易度、コストのいずれか。【神余】
- 双方が含まれている。【森本】

- 松竹梅のレベルで可能性あるいは被害の大きさが変化することはあるか。【神余】
- 可能性は「小」の中でより細分化される程度に変化すると考えている。【森本】
- 対策にはコストが掛かることの説明について検討している。最も効果的な対策が、様々な対策を組み合わせることで実現可能な場合において、難易度とコストのバランスを考慮する際にコストの捉え方をどうするか。【神余】
- 企業規模に応じた記載が妥当ではないか。【森本】

- ウイルスに感染した場合に自動周知、自動切断を行うような機能が必要ではないか。【木下】
- セキュリティかマルウェアかを疑うのは一般的に最後であり、感知は困難である。【神余】
- 例えば、プラントでは通常開放しないブローバルブを、現場判断を優先して行うことがある。現場の判断を優先する必要がある場合、見える化が重要と考えている。【森本】
- 異常が無いのに警告が発せられる場合と異常があるにもかかわらず警告が発せられない場合の 2 パターンがある。後者では、プラントを検査して初めて発覚する。例えば、プラント運転員のマニュアルにおいて、原因の 1 つとしてセキュリティへの考慮が初期段階に記載されていれば、発覚は早くなる。【神余】
- 今回の対象はコンシューマユースではなく、現場に人がいる環境下での ICT 利用であるため、柔軟性のある考え方が良いと考えている。【結城】
- 企業に過剰な負担を強いる対策では導入が促進されないが、実際には知恵と工夫次第でリーズナブルに対策が可能になることを提示したい。【神余】
- 最低限のガイドを成果として提示して、企業毎に現場に即したレベルの対策を立案してもらえれば良い。【河合】

- 従来は人を間違える存在として仕組みから排除しようとする傾向にあったが、今後は、人をシステムの重要なファクターと位置付け、能力の高い人を認証して積極的に活用すべき時代になると考える。【向殿】
- 人の経験や能力を評価する資格制度も検討されている。IEC 62443-4-1 においても従事する人の能力に関する記述があり、人の力量管理については、IECEE/ CMC /WG 34 及び Personnel Competence が検討を進めている。人の能力に関する仕組みを構築したい。【神余】
- IEC 62443-3 においても人の力量によって実施可能な対策が区別されている。【森本】
- ISO/IEC ガイド 51 におけるリスクベースの議論とは整合しないが、IEC 62443-2-3 において議論されている同じセキュリティシステムであってもマジョリティレベルの高い組織

によって構築されたシステムの方が、より高いレベルになるという考え方を含めたい。【神余】

- これまでの IT リスクへの対策の延長として ICT 等を利用することによる新たなリスクへの対策を検討した方が、現場に浸透しやすい。【結城】
- より広義に解釈しつつ、研究部会の成果としては、生産システムにおける場合を提示できれば良い。【向殿】
- 海外の現場にみられるようなマニュアル主義に対して、現場主義の優秀な人が多い日本の特徴を生かし、現場主義に基づいた現場を実現するために必要なリスクヘッジを行う提言がまとまれば良い。【森本】
- 異論は無い。【神余】

- 悪意とは人が意図することであるから、人間系を含めて議論しなければセキュリティを網羅できない。【向殿】
- ISO/IEC ガイド 51 のリスクは時間変化を考慮していないこと、マネジメントの概念を含める必要性の 2 点から、協調安全ベースの新しい概念が必要と考えている。【神余】

- 再リスク評価を加味したリスクアセスメントを早期に試行したい。対策カテゴリ毎の担当者については候補者と個別に相談したい。【神余】
- 多くの中小企業にはキーマンが存在しない。簡単な対処の方法が浮かばない【溝添】
- 必要な対策は、従来の対策の延長線上という安心感を醸成できることが望ましい。【結城】
- 当社ではユーザ責任として、「機械始動時にインターロックが効くか否か確認すること」と取扱説明書に記載している。原始的ではあるがウイルスで無効化されていないことを確認する方策としては有効な一案ではないか。【石川】
- 安全、セキュリティの双方から求められる極めて重要な方策の 1 つである。【神余】
- 本日の議論を行った方策はメーカ側の責務であると認識している。【石川】
- 現在のセキュリティシステムに、安全確認を行い正常に動作することを人に知らせる方策は無いか。【向殿】
- セーフティ側で機能安全等の改訂作業を行っているが、安全機能の無効化確認は機能安全の規格には明記されていない。攻撃によって安全機能が阻害される可能性がある場合、定期的に安全関連部を確認することが安全監査の観点から必要である。【神余】
- セキュリティも現場の危険予知記録（RKY）のように平易な表現で確認できると良い。【森本】

5. 次回の日程等ついて

次回の調査研究部会は、11 月 20 日（水）13：30～16：00 に決定した。

6. 今後の作業ついて

- アクションプラン及び決定事項
- セーフティとセキュリティの基本的な考え方について意見等がある場合には、研究部会関

係者にメールで共有する。

- 次回研究部会までに昨年度の本研究部会によるセキュリティ脅威リスクアセスメントシートに基づき、方策及び対策（IT、安全、復旧の 3 カテゴリ）を検討する。カテゴリ毎の担当については副主査から個別に相談を行う。

以上

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部会 第 4 回　議事録			作 成	
			エム・アール・アイ リサーチアソシエイツ	
開 催 日 時	2019 年 11 月 20 日（水）　13:30~16:00		開 催 場 所	TKP 東京駅セントラルカンファレンスセンター
出 席 者 （敬称略）	委員	向殿（明治大学）、神余（三菱電機㈱）、石川（住友重機工業㈱）、木下（平田機工㈱）、澁谷（テュフーズドジャパン）、首藤（システムズエンジニアリング研究所）、杉原（パナソニック㈱）、土屋（㈱三菱総合研究所）、畑（機械安全実践技術促進会）、森本（㈱制御ｊシステム研究所）		
	オブザーバ	結城、細川、河野、溝添（内閣官房 内閣サイバーセキュリティセンター）		
	事務局	宮崎、野村、吉田（（一社）日本機械工業連合会）、岡崎、畑中（エム・アール・アイ　リサーチアソシエイツ㈱）		

計 19 名

1. 開会

事務局及び主査より開会挨拶を行った。

2. 基本的な考え方について

事務局による資料（第 4 回研究部会用資料）に基づく説明後、以下の議論があった。

- 自然災害、悪意のある行為、悪意のないミス・故障等の事故といった 3 つの概念での区分が適当ではないか。【向殿】
  - 内部故障や自然災害も含めたアベイラビリティを阻害する全てを対象にしている。自然災害による被害を緩和する観点から検討する場合、セーフティ、セキュリティとも同様になりつつある。現状の考え方とセーフティとセキュリティの間に差異が無くなった際の考え方の中間段階が必要ではないか。【結城】
  - 人命、社会的安定性、財産といった結果系から区分する方法もある。原因系、結果系の双方から検討を進めた場合でも交差点は存在する。【向殿】
  - 原因系を整理軸をとして、検討においては、システマティック故障・故障、ヒューマンエラー、自然災害、サイバー脅威の 5 つに区分した。【神余】

- 機械安全の専門家がサイバー脅威への対策を検討する際に、脅威のインパクトや加えるべき変更点を検討する方が、既存システムとの親和性が高い。既存システムを全て変更することは不可能である。【結城】
  - 自然災害、ヒューマンエラーへの検討は、工場の所長や作業者によってある程度行われて

おり、ICT によって新たに発現するサイバー脅威への対策を提示できれば、読者が分かりやすい。【森本】

- 実務的観点には最も分かりやすい方法であるが、学術的観点からは、概念からトップダウンで分類するイメージを持っている。研究部会では、原因系・結果系による区分で議論を進めているが、将来的には学術的なまとめ方が可能なイメージがあると良い。【向殿】
- 今年度の研究成果としては、生産システムに ICT を活用する上での提言をまとめる必要がある。システマティック故障、故障、ヒューマンエラー、自然災害は、従来から対策が行われてきた分野であり、サイバー脅威は従来の対策に加えてプラスアルファの検討が必要な分野である。対応すべき事項は、サイバーをキーワードとして起こり得る事象から検討した方が良いだろう。【森本】

- サイバー脅威が存在する場合に、既に現場で検討、実行されてきた故障やヒューマンエラーといったリスクへの対策に与える影響、新たに検討すべき対策は何であるかを機械の専門家の立場からまとめると現場に浸透しやすいと考える。【向殿】

3. リスク対策の検討について

神余副主査によるセーフティとセキュリティの基本的な考え方についての説明後、以下の議論があった。

- セキュリティ脅威リスクアセスメントシートを提示する必然性が理解できない。脅威分析の結果から考えられる複数の対策を提示した上で、対策毎のリスクアセスメント結果が提示されるべきではないか。【結城】
- セキュリティ脅威リスクアセスメントシートは、特定のシステム・環境ではなく、遠隔監視等の機能をネットワーク接続した際に想定される一般的なトラブル（シナリオ）に基づいて検討を行ったものであるため、脅威分析の対象は分からない。【森本】
- セキュリティ脅威リスクアセスメントシートを用いた示し方は、対策の網羅性の観点から有効と感じた。ある 1 つの対策を実行すれば、その他の対策による効果を同時に得られるものがあるのではないか。また、対策が脅威とリンクしていないため、読者に全ての対策が必要と誤解される可能性があるのではないか。【首藤】
- NIST サイバーセキュリティフレームワークでは、資産やビジネス環境、リスク等の特定を行った上で防御・検知・対処・復旧を決定する。実際には、企業や組織の特性に合わせたプロファイリングにより対策等が調整される。プロファイリングをせずに検討を行うことに違和感がある。【結城】

- 研究成果として提示する対策の粒度は、洗い出した個別具体のものか、検討によってある程度まとめられたものか。【森本】
- 対象、使用方法によってリスクアセスメントの評価結果は変わるため、提示する対策はサンプルの位置付けと考えている。例えば、単独の対策ではリスクを小にできない場合、被害の大きさと発生可能性の双方を小にする対策を組み合わせる必要がある。被害の大きさ

を小さくするためには、IT による対策ではなく、セーフティやエンジニアリングによる対策が重要であることを説明したいと考えている。提示する対策の中から、読者が現場に応じて選択してほしい。【神余】

- 例えば、広報が行う SNS が起因となって現場がウイルス等に感染するといった状況も考えられる。想定脅威が不明確なまま検討を進めても十分な対策が提示できるのか。【結城】
- コンサルティングの経験上、現場の危険予知記録（RKY）を行う担当者が SNS やフィッシングの脅威を理解して想定することはできないだろう。【森本】
- 研究部会によるセキュリティ脅威リスクアセスメントシートの検討過程を説明する必要がある。【結城】
- セキュリティ脅威リスクアセスメントシートは、読者がリスク分析を行う際のナレッジの位置付けと理解している。【森本】
- 対策によってリスクを小とするためには、各現場に即した複数の対策による合わせ技が必要である。ただし、各現場の特色を否定するものではなく、例えば、安全の意識が高い現場では IT 系の対策のみで十分ということはあり得るだろう。【神余】
- サイバーセキュリティに対する取組の各現場のゴールを設定した上でのプロファイリングが必要になる。通常の現場ではリタンダンシーがあり、サイバー攻撃によって直ちに生産が停止するは少ないこと、及び、サイバーセキュリティにおける予防（prevention）、軽減（mitigation）、回復（recovery）、の説明が必要と考える。【結城】
- 検討開始当初は回復（recovery）とは復旧と考えていたが、復旧でもエンジニアリングツールのアップデートといった予防的対策がある。【神余】

- セキュリティ脅威リスクアセスメントシートの作成意図、使用方法を説明したい。【神余】
- ガイドを読み進める中で、セキュリティ脅威リスクアセスメントシートを理解できるような説明があれば良い。【向殿】

- 各対策の方法の説明が必要と考えている。また、イーサネットのセキュリティホールを塞ぐといった内容も含めることができていない。【神余】
- 例えば、国内金融機関のオンラインシステムが国外で運用・管理されているような場合についてはどうか。【杉原】
- サプライチェーンリスクはサイバー脅威に含まれる。【結城】
- 研究部会ではスコープ外としている。【神余】
- 機材の導入で十分といった意識が独り歩きするような提言にはすべきでない。【森本】
- 研究部会ではサプライチェーンに対する全ての脅威には対応できないが、リスクの提示は必要と考える。【向殿】
- ガイドでは、昨年度資料の再掲、セキュリティ脅威リスクアセスメントシートの読み方、対策毎の手法を説明するとともに、サプライチェーンの検討の必要性は議論を踏まえて可能な範囲で含めたい。【神余】
- セキュリティ脅威リスクアセスメントシートに基づいて不足している対策を検討してはどうか。【森本】

- 日機連の研究部会であることを踏まえた現場に即した検討を行いたい。【神余】
- フェールセーフのもとに安全が確保可能なことを前提に、セキュリティ脅威に対するリスクを許容できるレベルにまで低減が可能、かつ、現場が容易に活用できる典型的な対策をまとめたい。【向殿】

- 来年度以降のミッションは、今年度の研究成果であるスクアセスメント手法を伝導することと考えている。対象者は、脆弱性や脅威、機械のリスクアセスメントを理解しているレベルを想定している。【神余】

- 最低限実行すべき対策のみを提示するのであれば、脆弱性をパソコンに起因するものに限定するといった単純化も有効ではないか。セキュリティ脅威は、ウイルス感染か、悪意のある社員による行為程度に限定される。中小企業の現場を念頭にシナリオの検討を行うか。【森本】
- 現場にシャドーIT が無いこと、制御機器パラメータに変更がされていないこと等の確認は、機械、IT でも同様に必要な項目といえる。日本にしかできない対策は提言として価値がある。【神余】

- 提示する対策は、可能な範囲で具体の対策と有効性を提示した方が良い。【森本】
- 機械、IT による対策 20 個程度であるが、有効性は、状況に応じて優劣がある。【神余】
- セーフティの対策が制御システムに寄った検討であるため、柵の設置といった物理セキュリティ寄りの対策の追加が必要と認識している。なお、物理セキュリティの対策は、機械システムの構造に遡及する必要がある。【神余】
- 機械安全の考え方を提示できれば良い。【畑】
- 安全に係るカウンターメジャーの幅を広くしたい。現場では既に行われている安全対策が多く、対策の追加は不要となる場合が多いと想定している。機械の専門家の立場からは、各現場が最低限行うべき対策を例示したい。脅威分析と脆弱性分析の組み合わせに応じた対策例を提示することはどうか。【神余】

- ソフトウェアによる機能安全の概念が浸透して以降、人の機械への接近に支障がないとする傾向が生まれた。ポイントは、ウイルス等によるソフトウェアの異常を、正常なバージョンに復帰させるような仕組みではないか。【杉原】
- IEC TR 63069（2019 年版）では、機能安全と制御セキュリティの両立が図られている。当該規格では、機能安全側で行った設計情報をセキュリティ側に展開することが示されている。【神余】
- ICT における機械安全へのセキュリティの関連性を明確化する必要がある。【畑】
- 機械安全による安全確保を省略して機能安全による安全確保のみで設計を行わないことが、設計における最も重要な考え方である。【杉原】

- 機械的に本質安全を確保する重要性に異論はないが、ロボットはほぼ電子回路のみである

ため非現実的ではないか。【畑】
- ロボットがアタックされた際には、システム全体の遮断よりも、檻で囲う、または、動作を止めるような物理的な対策が重要ではないか。【杉原】
- ICT を使った際の本質安全の確保方法を検討すべき時期にある。安全を確認できるとき以外は ICT の利用を認めないといった方法になるのではないかと予想している。【向殿】
- 人の近傍で動作可能なロボットを前提にする場合、例えば、接近前にスリープモードであることを確認することが、現場の危険予知（KY）になる。【森本】
- ハードと人の関連性は重要な議論である。【結城】

- 被害シナリオを人の安全確保の観点において分類すれば、対策を絞り込むことが可能ではないか。人命を最優先とする考え方と、財産の安全確保（工場停止や情報漏洩のリスク）はスコープ外であるという研究部会の前提を明示した方が良い。【石川】
- リスクが大のセキュリティ脅威が人命に関わるリスクに該当し、検討対象にしている。【神余】
- プロファイリングによるゴールの設定が必要である。日本の産業界が発展しない理由は、過去からの継続を疑問視しないため、プロファイリングをできないからである。プロファイリングにはトップのコミットメントが必要である。【結城】
- 日本の産業界は改善・改良を重視した結果として新規設計を行う思想が疎かにされた結果、リスクアセスメントができなくなった。また、妥当性確認（validation）ができないため、安全要求仕様（Safety Requirements Specification）を作成できない。【神余】

- セーフティのリスクアセスメントの理解を前提にすれば、人命に関わるセキュリティ脅威に対して新たに行う必要がある対策は多くない。【神余】
- 提言はシンプルにまとめられると考えている。接続することのリスク、対策が必要なことに気付いていない IOT 担当者は世の中に多い。【石川】
- 人命に関わる最低限の安全確保が必要という前提と、プロファイリングは企業が自由に行うものであることを提示した方が良い。将来に継承できる考え方を作りたい。【結城】
- 現場で応用されるような対策であれば進化は可能だろう。プロファイリングの実践方法を日機連から現場にどう伝導するか。【森本】
- プロファイリングは企業の価値観に委ねられるが、研究部会としては安全を最優先に考える。【向殿】

- 日機連からの提言として発信する場合、サイバーを、故障の原因の 1 つか、安全の前提を阻害する要因と捉えるか。【森本】
- 後者の方が伝わりやすいのでないか。IEC TR 63074 では、機能安全のセキュリティが考慮すべき事項として扱われている。提言として発信すべき内容は、研究部会の報告書が対象とする読者層の活用方法によって異なる。セキュリティ対策のケーススタディとして、例えば、あるシステムにおける脅威分析、脆弱性分析の結果として抽出された人命に関わるセキュリティ脅威への対策は、被害の大きさを小さくするセーフティとレジリエンスに

よる対策、及び、被害の発生可能性を低くするITによる対策の合わせ技が必要であることを提示したい。【神余】

- 物理セキュリティが十分検討されていない対策は、ITセキュリティによる対策に留まったものといえる。【森本】
- 物理セキュリティを検討する意義は大きいが、評価・分析方法がないため、研究部会のスコープ外としている。ただし、入退室管理といった通常行われている対策は、記述しても良い。【神余】
- 異論はない。想定する脅威レベルは、IEC 62443におけるセキュリティレベルを対象とすれば良いのではないか。悪意がある社員の存在は想定して検討すれば良い。【森本】
- テロの検討は不要である。【向殿】
- 解雇された元社員による社内ネットワークへの侵入は、実際のサイバーインシデントでも起こっている。【神余】
- 研究部会の特徴としては、人を危害が及ぶ状況から守るために最終的には電源を切断するとしている点にあることから、今年度に検討しているセキュリティ脅威リスクアセスメントシートを、セーフティを含めたものに改訂できないか検討したい。【神余】

4. 成果とりまとめに向けた検討について

- セキュリティ脅威リスクアセスメントシートをブラッシュアップ(重要箇所の抽出)する。シートの見方、使用方法を文書化する。【神余】

- ブラッシュアップされたセキュリティ脅威リスクアセスメントシートに基づいて、森本委員には、説明方法を検討してほしい。【神余】
- 現場が分かりやすい言葉(KYに繋がるようなキーワード)を検討したい。安全を阻害する可能性のあるセキュリティの脆弱性と脅威を検討したい。【森本】

- 畑委員、杉原委員には、セーフティやレジリエンスの方法を検討してほしい。提言すべき内容があれば検討をお願いしたい。一般的な現場では多くの対策が既に実行されていることから、ICTを導入するハードルが高くないことを読者が理解することが重要である。【神余】
- 安全と考えているシステムでも、ICT の導入にあたっては点検が必要といった内容が、キーワードになる。【森本】
- IT化による新たなシステムリスクについては検討してほしい。【結城】
- シャドーITが典型例である。日本であれば、スマートフォンをロッカーに収納するといったルールが有効に機能する。【神余】
- ネットワーク接続による動作を想定していなかった機械が、遠隔操作が可能になった場合、従来の安全対策が無効になる。ネットワーク接続はメリットだけではない。【結城】

- 漫画は若手社員でも読みやすく効果がある。読みやすい工夫を取り入れても良いのではな

いか。【杉原】
- 人に危害が加わることを想像できると分かりやくなるだろう。【森本】
- 対策は、スマホのロッカー収納や機器の動作を遅くするといった単純な内容である。設備の復旧方法をどう検討するか。【神余】
- 復旧の検討には時間が必要だろう。【森本】
- エンジニアリングソフトに問題が無ければバックアップから復旧できるが、ソフトウェアが被害を受けている場合には、OS からフルインストールすることが最も安全である。また、バックアップを用意していない工場もある。【神余】
- 通信インターフェース盤内のパソコンが感染源となった場合には、コンソールによる復旧はできず、ネットワークセグメントを全て外す必要がある。【森本】
- セーフティの装置が故障した場合でも、代替手段（人を見張り役にする等）によって被害を小さくできることを提示したい。【神余】

5. 次回の日程等ついて

次回の調査研究部会は、1 月 20 日（月）13：30～16：00 に決定した。

6. 今後の作業ついて

- 宿題事項
  - セキュリティ脅威リスクアセスメントシートを部会の議論を踏まえて見直しを行った上で、関係者（委員、オブザーバ）に展開する。【神余】
  - セキュリティ脅威リスクアセスメントシートの見方、使用方法を文書化する。【神余】
  - セキュリティ脅威リスクアセスメントシートの説明方法を検討する。【森本】
  - 現場が分かり易い言葉（KY に繋がるようなキーワード）を検討する。【森本】
  - 例示するセキュリティの脆弱性、脅威を検討する。【森本】
  - セキュリティ脅威リスクアセスメントシートに基づいて、セーフティとレジリエンスを検討する。【杉原、畑】
  - セーフティとレジリエンスの検討を通じて提示すべき提言があれば検討する。【杉原、畑】

以上

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部会 第 5 回　議事録			作 成	
			エム・アール・アイ リサーチアソシエイツ	
開 催 日 時	2020 年 1 月 20 日（月）　13:30~16:00		開 催 場 所	ステーションコンファレンス東京・503A 会議室
出 席 者 （敬称略）	委員	向殿（明治大学）、神余（三菱電機㈱）、石川（住友重機工業㈱）、木下（平田機工㈱）、首藤（システムズエンジニアリング研究所）、杉原（パナソニック㈱）、土屋（㈱三菱総合研究所）、畑（機械安全実践技術促進会）、森本（㈱制御システム研究所）		
	オブザーバ	結城、河野、溝添（内閣官房 内閣サイバーセキュリティセンター）		
	事務局	宮崎、野村、吉田（(一社）日本機械工業連合会）、薮田、岡崎、落合（エム・アール・アイ　リサーチアソシエイツ㈱）		

計 18 名

配布資料

資料 1:前回議事録(案)

資料 2:リスクアセスメント表の解説

資料 3:第 X 章　セキュリティリスクアセスメントの手順

資料 4:生産現場におけるセキュリティリスク KY のアプローチ(案)

資料 5:ANSI B11.TR9(IDT ISO/TR22100-4)で示されている機械の安全性に影響を与える可能性のある IT セキュリティの脅威を避けるためのリスク低減(緩和)方策の例

資料 6:ANSI B11.TR9(IDT ISO/TR22100-4)Guidace to Machinery Manufactures for Consideration of Related IT-Security (Cyber Security) Aspects
関連する IT セキュリティ(サイバーセキュリティ)の側面を考慮するための機械メーカーへのガイダンス

1.　開会

事務局及び主査より開会挨拶を行った。

議事録は特にコメントが無ければこれで FIX したい。

2.　報告書全体のイメージ共有

第 4 回研究部会用資料の調査研究報告書の骨子（案）に基づく説明後、以下の議論があった。

- 全体的な構成や提言は従来のまま変えないということにしたい。昨年度はリスク分析までだったが、今年度はリスク低減対策まで行い、解説的な利用ガイドが目玉になっている。このガイドを考える上で機械安全の ISO12100 に対して、ISO/TR22100 シリーズでセキュ

リティ関連があるが、両者は内容的に似ている。本日はガイドについて議論したい。【神余】

- ISO/TR 22100 は、三層構造の ABC のどれにあたるか。【杉原】
- リスクの考え方（基本概念）を A、提言（規格）が B、利用ガイド（リスクへの対応方法）が C であろう。【向殿、杉原、畑】
- 業界としては機械産業なので、機械毎を入れてもよいのではないか。プレス機、半導体製造装置等の法令で決まっているものとそうでないもの。しかし、機械安全になってしまう。【杉原、向殿】
- 個別の機械は難しいので、工場全体等統合化した全体を対象にする。【神余】

- 利用ガイドの章立てのイメージを作れるとよい。これまでを振り返ると以下のようになる。このような内容のガイド前に、ISO/TR 22100 やセキュリティリスク KY の資料が来るのかどうかを議論したい。【神余】

- 1 年目：ICT 使うと何が問題になるのか～やはりリスクはサイバーセキュリティである。
- 2 年目：具体的なアプリケーションシステムで使い方を考えた。工場内のデータがクラウド内にある例と、業者構築の IoT 例の 2 つを想定して、リスクが高い後者のリスクアセスメント(RA)を行った。パラメータが多く、被害の大きさと可能性をざっくり評価した。
- 3 年目：対策は人によって違う。IT セキュリティ、安全対策、レジリエンスの 3 つの合わせ技でいけるのかどうかを検討した。どれをどう選ぶのかはエンドユーザであり、シナリオが多いので、規模が大きくなった。RA の方法論を説明することが大事である。

- 資料 4 は、本来リスク分析はプロファイルが必要だが、整理のために作成してみた。【森本】
- ガイドは注目されているので、よりわかりやすく記載したい。【神余】
- 報告書出口の花形は資料 2 の表である。その前に背景になる資料 4～6 がある。【森本、神余】

- 資料 2、3 の説明【神余】

資料 2 の箇条書きの文章は資料 3 として書き直したものである。EXCEL はセキュリティリスクアセスメントを 2 つの例題について作成している。資料 3 はこの作成手順を記載している。

- 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部会のため、本提言の被害は人命（人体）に対するもので、財産事案や工場の操業停止までは拡大することはできるが、入れない方が良い。【向殿、神余、杉原、森本】
- 人命の安全レベルを上げるための対策や安全確保には復旧はあっても良い。機械設備に被害が及ぶことも入れるべきではないか。復旧段階では安全系再点検は必要である。セーフティを人命に制約するかどうか。ネットワークとしての共通要因故障と思えば復旧も対策も入る。【向殿、神余、杉原、森本、畑】
- 手順の前の機械の安全やセキュリティなどの上位概念を入れるべきか否か。【神余】
- サイバー攻撃を受けた場合も含めていかなる場合も安全であることが重要である。【杉原】

- 序章か概念に生産中断は除外していることを記載した方が良い。人命を守ることがメインテーマであり、従属テーマとは分離すべきである。【石川、神余】
- 対策が 3 種類（セキュリティ対策、安全対策、復旧対策）独立で記載しているが、実際にはそれらの合わせ技でないとリスクは下がらない。【神余】
- 可能性（高、中、小）について誰がどうジャッジするのか。回数だけではピンとこないのでわかりやすい指標が必要ではないか。【森本】
- ランサムウェアなどの新しい脅威はどう評価するか。【神余】
- 4 番目の安全対策（IT セキュリティ対策）は、素人がイメージを作りづらい。安全系をきちんと守る、すなわち機械安全や機能安全を守るためにネットワークから遮断する、と記載した方がイメージがわくのではないか。【森本】
- 機械安全の基本原則をセキュリティに使っているだけである。何かあったら全停止、緊急ボタンを押すと関連する部分だけ物理的に停止、3 重防護コンピュータシステム。3 段論法。【杉原】
- 安全のところに停止、遮断が入っている。また、IT、安全、の順番で良い。【向殿】
- 停止は機械式か、インバーターか、あるいはブレーキか。【首藤】
- 物理的に停止の場合には制御やインターネットには無関係に停止する。【向殿】
- 機能安全には頼らずに、いきなり機能停止（物理的な遮断）を提言に入れる。【神余】
- 組織のプロファイリング＝目的によってリスクが変わる。【結城】
- 守るべき対策は、当面は生命・人命である。【向殿】
- 安全第一、品質第二、稼働（利益）は第三である。【杉原、向殿】
- セキュリティ対策への考え方は、機械製造者（メーカー）側、使用者（ユーザー）側の両方をバランス良く想定した対応であるべき。【結城、石川、向殿、森本、畑】
- 固有名詞はどこまで出すかは検討が必要。【神余】

- 資料 6 の説明【畑】
- 機械類の安全性と IT-セキュリティの関係の図の ISO12100 に従った RA フローで、ステップ 3 の機械が PC になったら左（機械へのセキュリティリスク）から→がステップ 3 にも入るだろう。【畑、杉原、森本】

- 資料 4 の説明【森本】
- この内容をガイドとは違う次元で本文に入れるか否か。詳細は付録で。【神余】
- P11 の「セキュリティリスク KY 3 つのアプローチ」で、KY（危険予知）はオペレーションでステップ 3)のみの話である。ただ、ステップ 3)だけを言うのはバランスが欠ける。ステップ 3)からステップ 1)、2)へのフィードバックが必要である。これはいわゆる使用者と設計者の間のリスクコミュニケーションである。【森本、神余、結城】
- この資料の使い方はガイド（手順）の最後にする。【神余】
- 2 月末までにドラフトを集約して、3 月の最後の部会で確認したい。【岡崎】

3. 次回の日程等ついて

最後の調査研究部会は、3 月 11 日（水）10：00～12：30（場所は同じ）に決定した。

4. 今後の作業ついて

- 宿題事項
- 本日資料提出の 3 名は、本日のコメントについて資料の見直しを行う。
- 1 章 基本的概念・前提、2 章 提言　については別途すり合わせを行う。3 章 利用ガイド（対策・事例等）は、わかりやすく記載する。
- 畑様には資料 6 の概要文を記載頂く。
- 期限は 2 月末

以上

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部会 第 6 回　議事録			作 成
			エム・アール・アイ リサーチアソシエイツ
開 催 日 時	2020 年 3 月 11 日（水）　10:00~12:00	開 催 場 所	サピアタワーステーションコンファレンス東京
出 席 者 （敬称略）	委員	向殿（明治大学）、神余（三菱電機㈱）、杉原（パナソニック㈱）、杉田（テュフラインランドジャパン㈱）、首藤（システムズエンジニアリング研究所）、杉原（パナソニック㈱）、澁谷（テュフズードジャパン㈱）、畑（機械安全実践技術促進会）、森本（㈱制御ｊシステム研究所）	
	オブザーバ	結城、細川、河野、溝添（内閣官房 内閣サイバーセキュリティセンター）	
	事務局	宮崎、野村、吉田（（一社）日本機械工業連合会）、岡崎、落合（エム・アール・アイ　リサーチアソシエイツ㈱）	

計 18 名

配布資料

資料 1:前回議事録(案)

資料 2:平成 31 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(案)、A3 セキュリティリスクアセスメントの事例表

資料 3: 第 5 回研究部会用資料「生産現場におけるセキュリティリスク KY のアプローチ(案)」

資料 4: 月刊「計装」掲載記事抜粋

1. 開会

事務局及び主査より開会挨拶を行った。

議事録はコメントがあれば吉田まで連絡されたい。

2. 報告書全体のまとめ方

資料 2 の概要説明後、以下の議論があった。

- 付録 D、E は必要か。【神余】
- 抜粋して要点は本文に入れたので不要ではないか。参考文献の位置づけである。【畑、神余】

- 付録 F はどうか。【神余】
- ランサムウェアは書いた方が良いだろう。安全計装システム(SIS)を標的とした TRITON など、制御セキュリティの事例を中心に 5 つくらい。資料 4 などをベースに神余がまとめる。【向殿、細川、畑、神余】

- 4.1 基本概念、4.2 提言について。【神余】
  - (4)リスク低減（安全対策）は、再発防止の観点から、安全方策との使い分けが必要である。【向殿、細川】
  - 許容可能とは、どういうものか事例を記載しなくてよいか。【首藤】
  - ゼロリスクとか絶対安全は無いという観点から定義を書くくらいまででではないか。【向殿、細川、結城】
  - 用語の定義や引用文献／参考文献リストは必要ではないか。【向殿、神余】
  - 用語集は後ろで良いのではないか。【細川】
  - セキュリティ対策はソフトウェアだけではなく、ハードウェアも必要であろう。【畑、首藤】
  - 提言における「生産システム」は「生産設備」とするべきではないか。システムはコンピュータの中にあるソフトウェアではないか。【森本】
  - セキュリティの影響を受けないシステムのポンチ絵を入れると良いのではないか。【首藤】
  - 情報技術（IT）や運用技術（OT）ではなく、情報通信技術(ICT)にすると受け入れやすい面がある。【 神余】
  - セキュリティ脅威とは、サイバーセキュリティ（サイバーアタック）のことであり、テロセキュリティのことではない。【細川、神余、向殿】
  - IT セキュリティよりも、サイバーセキュリティの方が情報やヒューマンファクタも含むため広義である。【細川】
  - リスクアセスメントの定義などは正しいかどうか。【杉原】
  - 定義は前に持っていき、用語と参考文献は後ろに持っていく。4.3 からはシナリオベースでさっと読めるようにする。【神余】
  - 4.2.2 確定的ハザードの前提として制御の観点から ICT 共通原因故障かどうかを考えるべきか。【森本】　具体的な記載方法が難しい。【神余】

- 4.5 今後の検討事項について。【神余】
  - 町工場の方が読んでわかるレベルにしたり、具体的なグッドプラクティスや啓もうを入れ込むべきか。【神余】

- 報告書作成の進め方について。【神余】
  - 今回の議論の内容を基に報告書（案）を修正し最終版としてまとめる。【事務局】
  - 提言は文章を見直して 3 章に入れる。4 章の用語集は巻末へ移動し、参考文献も追加する。参考文献は杉田委員にお願いしたい。
  - 4.2.1～4.2.3 は前の章に追加する。4.2.3 の最後に安全関連系とそれ以外の関係がわかるブロック図を入れる。
  - 4.3 ではセキュリティをサイバーセキュリティで統一する。MRA 担当。
  - 4.5 は別の章を立てる。
  - 今後の課題を 6.2 の後ろにして、その前に実際の手順、考え方、実例を入れる。
  - 付録は、D、E なしで、F は追加する。
  - サマリー文章が固いので、読みやすくする。

- アクションアイテムを展開する。MRA 担当。

3. 調査研究部会のまとめ

- 3 年間かけて面白い議論ができた。セキュリティを救うのはセーフティの文化であり、両者一体でこそ利用が広がる展開になろう。被害の対象は人命であるが、その後は財産事案、サービス停止などもある。また利用者によって価値観も異なる。人間も機械も一緒に安全やセキュリティを考え、日本から発信していく必要がある。【向殿、神余、細川】
- 今後に向けて、導入事例や障害事例、グッドプラクティスなどを業界として集めていく事が良いのではないか。【河合、向殿、神余】

以上

付録 F2 研究部会資料

2019年度 第１回 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部会

第1回研究部会用資料

2019年6月4日

1. 昨年度（平成３０年度）の検討成果確認

機械等で構成される生産システムを製造および利用する我が国の産業界に対する「**提言：生産システムにおけるセキュリティ脅威検討の基本的な考え方**」として、以下を示した。

生産システム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。
②	セキュリティ脅威によるハザードは確定的である。
③	セキュリティ脅威への最終的な対策は、安全関連制御系に拠らないシステムの停止である。

機械安全の技術者が理解しやすく取り組みやすい生産システムにおけるセキュリティ脅威に対するリスクアセスメントを行う方法を検討し、「**リスクアセスメントシート**」として提示した。

No.	a.対象ソリューション	b.ソリューション解説	c.シナリオ	d.シナリオ解説	e.想定被害	f.被害シナリオ	g.被害例	h.脆弱性	i.脅威源	被害の大きさ	可能性	リスク

	項目名	内容
a.	対象ソリューション	リスクアセスメントの対象とするICTを利用したソリューション
b.	ソリューション解説	a.対象ソリューションについての説明
c.	シナリオ	アセスメントの対象とする生産システムの状態
d.	シナリオ解説	c.シナリオの説明
e.	想定被害	c.シナリオにおいてセキュリティの脅威により想定される被害
f.	被害シナリオ	e.想定被害にいたるシナリオ
g.	被害例	実際に発生した類似の被害
h.	脆弱性	e.想定被害をもたらす脆弱性。1つの想定被害に複数の脆弱性あり。
i.	脅威源	h.脆弱性を攻撃して被害を発生させる脅威源

1. 昨年度（平成３０年度）の検討成果確認

今後の検討事項として、以下の3項目を示した。

今後の検討事項	
1-1	リスクが許容レベルを超える場合に必要な対策の検討
1-2	1-1の対策を行うにあたり必要とされる、対策の効果、コスト、システムへの影響等に関する総合的な検討
1-3	1-2の検討を踏まえ、機械安全の技術者に対するセキュリティ脅威の対策に向けたトレーニングカリキュラムの構築に向けた検討

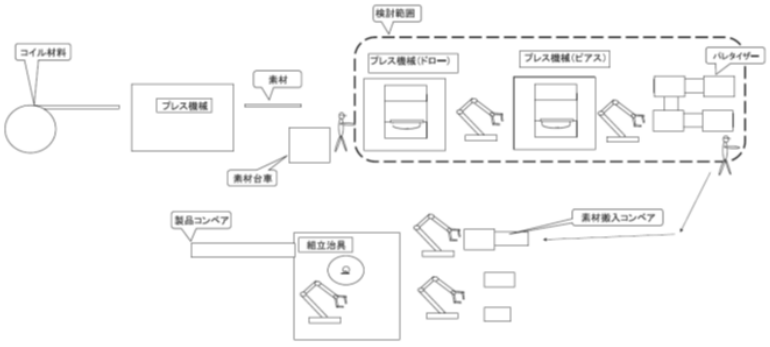
- 検討にあたっては、安全が確保された生産システムの事例に対して、ICTサービスを追加したモデル（例えば次ページ）を想定し、セキュリティ面からの安全性分析を行う。
- 一連のプロセスが検討されたモデルにてセキュリティ分析を行うことで、セキュリティ脅威に対する具体的な対処方法を理解しやすく整理することができ、その成果は、ガイドラインとして活用することが期待される。

1. 昨年度（平成３０年度）の検討成果確認

参考：

日本機械工業連合会が平成28年度までの3年間の研究事業で検討したISO 11161(*1)に基づく統合生産システムのモデル(*2)

- この統合生産システムのモデルは、下図に示すとおり、鍋の蓋を製造する架空の生産ラインであり、複数のプレス等の機械と、それを接続する3台のロボットから構成する生産ラインである。
- 機械安全に関する対策は、ハザードの洗い出しからリスクアセスメント、その結果から許容されないリスクの対策まで、一連のプロセスが検討されて示されている。



福田、ISO11161 に基づいた安全な生産システムの構築、安全工学 Vol.57 No.1 2018から引用

*1：ISO 11161: 2007 Safety of machinery — Integrated manufacturing systems — Basic requirements"
（機械類の安全性－統合生産システム－基本要求事項）
*2：日本機械工業連合会 平成28年度 安全な生産システム構築能力向上のための調査研究報告書
http://www.jmf.or.jp/houkokusho/1505/1.html

2. 今年度の重点課題と検討の進め方（案）

- 重点課題

1-1 リスクが許容レベルを超える場合に必要な対策の検討

- セキュリティ脅威へのリスクアセスメント・対策（事前対策）の検討のみならず、今年度は新たに、攻撃を受けた後の復旧作業等（事後対策）の検討を行う想定。
- 前頁の統合生産システム（以下、鍋蓋製造ライン）に加え、他の複数ラインで対策の検討を行う想定。

1-2 対策の効果、コスト、システムへの影響等に関する総合的な検討

- 以下の順序で検討を進めることを想定。
  - ① 1-1の検討を踏まえつつ、鍋蓋製造ラインを含めた複数ラインにてセキュリティ分析を実施。
  - ② セキュリティ分析した内容を解説として記載することを試行。
  - ③ 共通項目の洗い出し、代表的なものを整備。（ガイドラインやトレーニングのコンテンツ候補）

- その他の課題

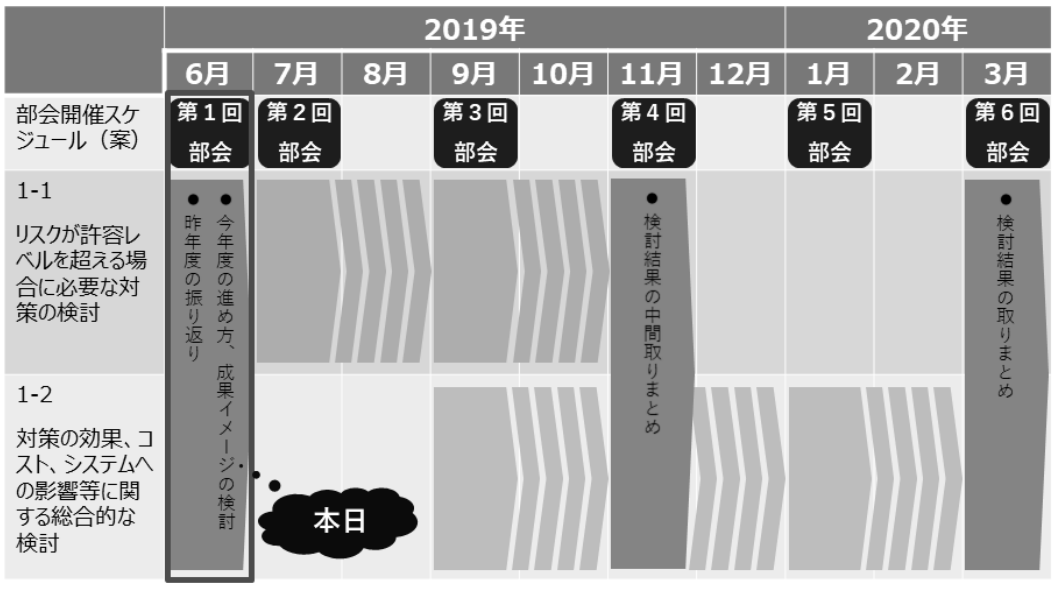
1-3 機械安全の技術者に対するセキュリティ脅威の対策に向けたトレーニングカリキュラムの構築に向けた検討

- 実施する場合、以下の順序で検討を進めることを想定。
  - ① 1-2の検討を踏まえ、トレーニングカリキュラム案を作成。
  - ② トレーニングを試行。
  - ③ ②を踏まえ、代表的なものをガイドライン、トレーニングのコンテンツ、カリキュラムとして整備。

MRI Research Associates Inc.

2. 今年度の重点課題と検討の進め方（案）

昨年度と同様に全６回の部会を予定している。想定する検討スケジュール（案）を以下に示す。



3．研究部会の成果イメージ（案）

3カ年の研究部会における検討の成果イメージを以下に示す。具体的な成果イメージは部会での検討が必要。

- これまでの検討成果を取りまとめることが必要。

これまでの成果	業界発信	■ ICT等の利用に伴うセキュリティ脅威に対する考え方の提言	■ 生産システム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。 ② セキュリティ脅威によるハザードは確定的である。 ③ セキュリティ脅威への最終的な対策は、安全関連制御系に拠らないシステムの停止である。
	事例研究	■ 起こり得るハザードの検討 ■ リスクアセスメント方法の検討、実施	■ リスクアセスメントシート （対象ICTソリューション：機械の遠隔監視診断、生産効率化品質向上）
今年度の成果イメージ（案）			■ リスクアセスメントシート （鍋蓋製造ライン＋複数ライン）
	ガイドライン	■ ICT等利用の際のチェックリスト ■ ICT等の利用に関するQ&Aリスト ■ ICT等利用時の注意点をレポートに	■ 国内製造事業者が生産システムにICT等を利用する際に、注意すべき点についてチェックリストとして整理 ■ 国内製造事業者の立場のQuestionに対するAnswerを作成（以下、例） ■ 生産設備をネットワークに接続するメリットは何ですか？ ■ 外部のインテグレーターと生産設備を接続しても問題ないでしょうか？ ■ あるいは、ICT等の生産システム適用に関して、目的、メリット、想定リスク、導入方法、安全性対策、運用課題、システム復旧等を、レポートとして作成
	業界宣言	■ ICT等利用を安全に効果的に使用するための業界としての宣言	■ ICT等の生産システム適用にあたり、安全性確保を対応した企業であることを自己宣言する活動の推進、自己宣言のための要件を公表 ■ 自己宣言した企業をリストアップ ■ 具体的な導入事例を公開

MRI Research Associates Inc.

２０１９年度 第２回 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部会

第２回研究部会用資料

2019年7月22日

1. 第１回研究部会（6月4日開催）の振り返り

- 平成３０年度の成果について
  - ✓ 生産システムにおけるセキュリティ脅威検討の基本的な考え方
  - ✓ リスクアセスメントシート
  - ✓ 今後の検討事項
- ２０１９年度における討議範囲について
  - ✓ 今後の検討事項を踏まえ、事務局が検討の進め方（案）を提示し議論

●重点課題

1-1 リスクが許容レベルを超える場合に必要な対策の検討

- セキュリティ脅威へのリスクアセスメント・対策（事前対策）の検討のみならず、今年度は新たに、攻撃を受けた後の復旧作業等（事後対策）の検討を行う想定。
- 統合生産システム（以下、鍋蓋製造ライン）に加え、他の複数ラインで対策の検討を行う想定。

1-2 対策の効果、コスト、システムへの影響等に関する総合的な検討

- 以下の順序で検討を進めることを想定。
  - ① 1-1の検討を踏まえつつ、鍋蓋製造ラインを含めた複数ラインにてセキュリティ分析を実施。
  - ② セキュリティ分析した内容を解説として記載することを試行。
  - ③ 共通項目の洗い出し、代表的なものを整備。（ガイドラインやトレーニングのコンテンツ候補）

●その他の課題

1-3 機械安全の技術者に対するセキュリティ脅威の対策に向けたトレーニングカリキュラムの構築に向けた検討

- 実施する場合、以下の順序で検討を進めることを想定。
  - ① 1-2の検討を踏まえ、トレーニングカリキュラム案を作成。
  - ② トレーニングを試行。
  - ③ ②を踏まえ、代表的なものをガイドライン、トレーニングのコンテンツ、カリキュラムとして整備。

MRI Research Associates Inc.

1. 第１回研究部会（6月4日開催）の振り返り

- 今年度の検討方針
  1. 鍋蓋製造ラインに則り、セキュリティ脅威への予防的対応（事前対策）、及び、攻撃を受けた後の復旧作業等の対応（事後対策）を、複数パターン検討
  2. FA・OTにおける事例（各社による検討、公開情報、事故）、及び、ガイドライン等を収集し、生産システムにおけるICT利用のメリット等を整理
  3. 日機連の会員をはじめとした企業の生産システムの企画等の実務担当者が、備えておくべきICTの検討・導入・運用に係り必要な知見、並びに、能力を整理
- 今年度に目指す成果（案）

  機械の専門家の立場から、
  - ✓「提言： ICTを利用する生産システムにおいて人を守るあるべき機械安全」を公表
  - ✓「事例等から得られたICT利用に係るセキュリティ対策の検討結果をまとめた報告書」を公表
  - ✓「人を守る機械安全の確保を担う生産システムの企画等の実務担当者像」を整理

1. 第１回研究部会（6月4日開催）の振り返り

- ご参考（議論のサマリ）

（重点課題）

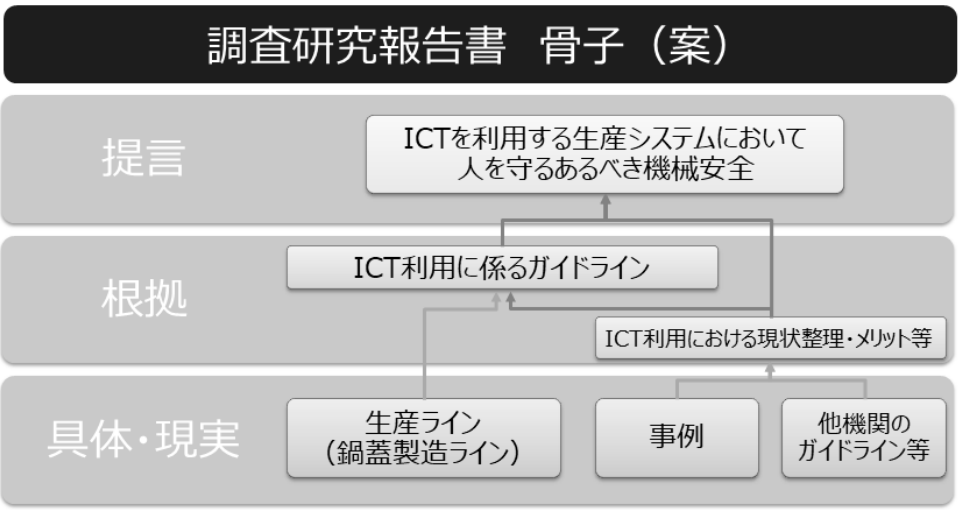
- ✓ コンピュータの進歩によって機能安全の概念ができたことで、本来あった機械安全が変質してきた。具体的な事例を根拠として示し提言に繋げられれば良い
- ✓ セーフティの基本的な考え方における機能安全の位置付けと、機能安全が表立つことで機械安全の本質が忘れられがちになっている事故事例、繋げることによるセキュリティの考え方・対応方法を示す
- ✓ リスクアセスメントはある程度1本化できるが、ウェイトの置き方次第で対策は複数存在する
- ✓ 抽出された全てのリスクに対して対策を行うのではなく、許容されないリスクに対して、行うべき対策の種類や、リスク発生の予防となり得る設計方法の指針を作成する
- ✓ 日機連が行ってきたことにセキュリティの考え方を加え、インテグレータがどのように関与すべきかを明確にできると良い
- ✓ 1つのラインに対する複数の対策を検討した上で、総合的な検討（レジリエンス、ファイアウォール、ログ解析等）を行う
- ✓ 今年度の成果として提言をまとめ、世間に発表する

（その他の課題）

- ✓ 必ずしもトレーニングカリキュラムまで検討が進まなくても良いかもしれない
- ✓ トレーニングカリキュラムに関しては誰にどのレベルになってもらうかが見えない。カリキュラムの作成は困難だが、必要な人材についてまとめたい
- ✓ 対象等の大枠のみ検討することとしたい。具体はどこかに任せたい
- ✓ 機械の専門家が最低限知っておくべきものになるべきである
- ✓ ユーザが発注する際にインテグレータの質を評価できる軸だけでも良い

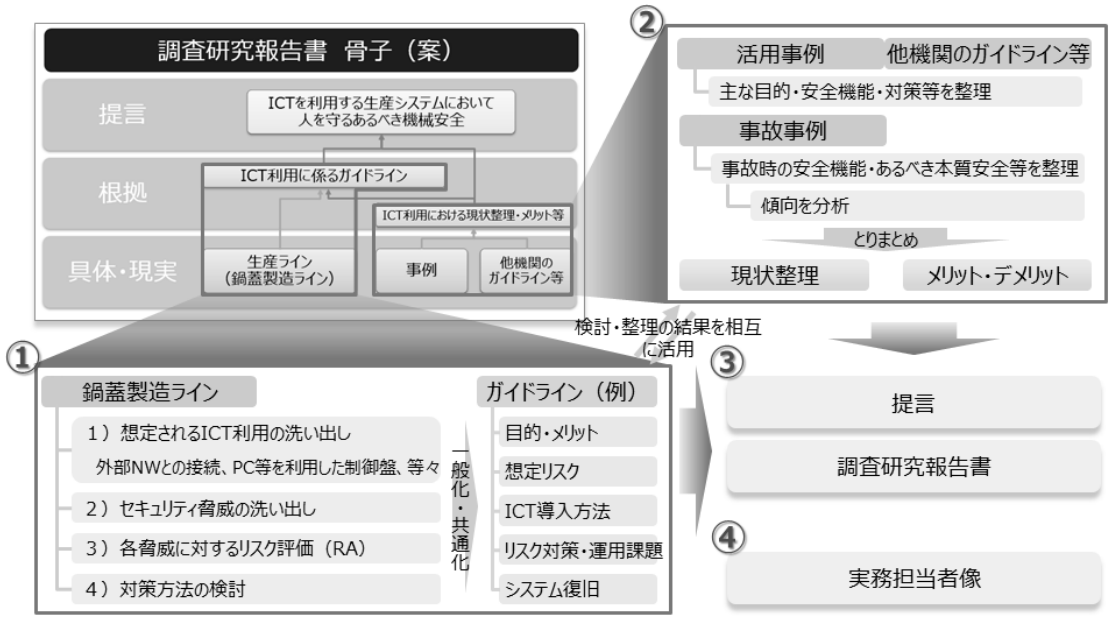
2. 研究部会における検討の進め方・成果のとりまとめ（案）

検討の成果としてまとめられる調査研究報告書の骨子（案）を以下に示す。



2. 研究部会における検討の進め方・成果のとりまとめ（案）

今年度の研究部会では、①具体の生産ライン（鍋蓋製造ライン）の検討を踏まえたICT利用に係るガイドラインの作成と並行して、②現実の事例等に基づきICT利用のメリット等を整理し、提言・報告書としてとりまとめる。



MRI Research Associates Inc.

2. 研究部会における検討の進め方・成果のとりまとめ（案）

第2回研究部会（本日）の検討内容（案）を以下に示す。

① 鍋蓋製造ラインにおける検討
- 1）想定されるICT利用の洗い出し
  （必要に応じて検討対象範囲の選定）
- 2）セキュリティ脅威の洗い出し
- 3）各脅威に対するリスク評価（RA）
- 4）対策の検討

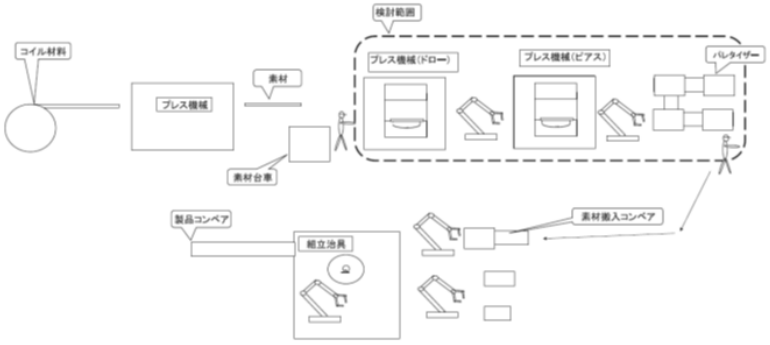
② 収集すべき事例等の検討
（紹介を含む場合あり）

3. 鍋蓋製造ラインにおける検討（案）

参考：

日本機械工業連合会が平成28年度までの3年間の研究事業で検討したISO 11161(*1)に基づく統合生産システムのモデル(*2)

- この統合生産システムのモデルは、下図に示すとおり、鍋の蓋を製造する架空の生産ラインであり、複数のプレス等の機械と、それを接続する3台のロボットから構成する生産ラインである。
- 機械安全に関する対策は、ハザードの洗い出しからリスクアセスメント、その結果から許容されないリスクの対策まで、一連のプロセスが検討されて示されている。



福田、ISO11161 に基づいた安全な生産システムの構築、安全工学 Vol.57 No.1 2018から引用

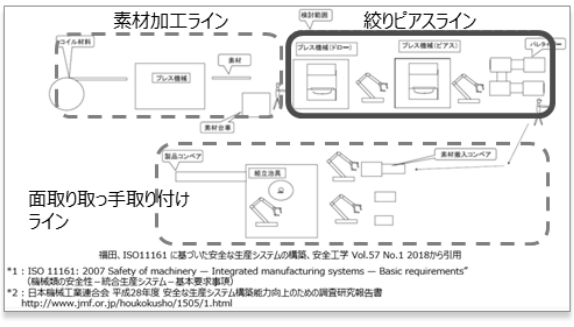
*1：ISO 11161: 2007 Safety of machinery — Integrated manufacturing systems — Basic requirements"
（機械類の安全性－統合生産システム－基本要求事項）
*2：日本機械工業連合会 平成28年度 安全な生産システム構築能力向上のための調査研究報告書
http://www.jmf.or.jp/houkokusho/1505/1.html

3. 鍋蓋製造ラインにおける検討（案）

参考：

日本機械工業連合会が平成28年度の研究事業『安全な生産システムの構築能力向上のための調査研究』において検討した絞りピアスライン（赤枠内）のシステム構成(*2)

- 絞りピアスラインのシステム構成



福田、ISO11161 に基づいた安全な生産システムの構築、安全工学 Vol.57 No.1 2018から引用

*1：ISO 11161: 2007 Safety of machinery — Integrated manufacturing systems — Basic requirements"
（機械類の安全性－統合生産システム－基本要求事項）
*2：日本機械工業連合会 平成28年度 安全な生産システム構築能力向上のための調査研究報告書
http://www.jmf.or.jp/houkokusho/1505/1.html

機械 或いは部品	動力源 および定格情報	機械機能	機械間協調作業	人の介入	安全に関連する改造事項	その他
絞りプレス	200Vac 3Φ 50Hz 空気圧 0.4MPa 加圧能力 600kN (60t)	円盤を鍋蓋形状にプレスにより加工. 寸動. 安全一工程. 自動運転モード	ロボット1とのインタロック	金型交換. 材料投入. 清掃	石側面固定ガード取外し	
ロボット1	200Vac 3Φ 50Hz 真空圧 90kPa	絞りプレスにより加工された素材をピアスプレスに搬送. 調整(教示)モード. 自動運転モード	絞りプレス. ピアスプレス. ロボット2とのインタロック	パットの交換. 清掃. 教示		
ピアスプレス	200Vac 3Φ 50Hz 空気圧 0.4MPa 加圧能力 600kN (60t)	鍋蓋形状の中心に取手取付穴をプレスで開ける. 寸動. 安全一工程. 自動運転モード	ロボット1, 2とのインタロック	金型交換. 材料投入. 清掃. スクラップ取り出し	左右側面固定ガード取外し	
ロボット2	200Vac 3Φ 50Hz 真空圧 90kPa	ピアスプレスにより加工された素材を製品パレットに搬送. 調整(教示)モード. 自動運転モード	ピアスプレス. 積込装置. ロボット1とのインタロック	パットの交換. 清掃. 教示		
積込装置	200Vac 3Φ 50Hz 空気圧 0.4MPa	製品パレットの移載. 排出. 個別操作モード. 自動運転モード	ロボット2とのインタロック	空パレットの挿入. 満載パレットの搬出. 清掃		

*2：日本機械工業連合会 平成28年度 安全な生産システム構築能力向上のための調査研究報告書
http://www.jmf.or.jp/houkokusho/1505/1.html

3. 鍋蓋製造ラインにおける検討（案）

参考：

絞りピアスラインの工程 (*2)

- 絞りピアスラインのシステム構成及びユーティリティ

1. 円形に打ち抜かれた素材を，手作業で絞り加工プレスに投入する
2. 絞り加工され凹型となった素材を搬送ロボットが次のピアスプレスに搬送する
3. ピアスプレスで穴あけ加工をする
4. 穴あけ加工された素材を搬送ロボットがパレタイザにある製品パレットへと並べていく
5. 製品パレットが満杯になれば，パレタイザがこのパレットを排出する
6. 排出されたパレットは作業者が次工程の面取り取っ手取り付けラインへと運ぶ

*2：日本機械工業連合会 平成28年度 安全な生産システム構築能力向上のための調査研究報告書
http://www.jmf.or.jp/houkokusho/1505/1.html

3. 鍋蓋製造ラインにおける検討（案）

参考：

絞りピアスラインのユーティリティ(*2)

- 絞りピアスラインに使用する設備へ供給するユーティリティ（動力条件

IMS 内に存在する機械	ユーティリティ	設置現場準備	接続方法(Interface)
絞りプレス	電気	200Vac 3φ 50Hz	プレス制御盤の主幹遮断器一次側へ直結
	圧空	0．4MPa	プレス受入れコネクター
ロボット1	電気	200Vac 3φ 50Hz	ロボット制御盤の主幹遮断器一次側へ直結
	真空	90kPa	ロボット本体受入れコネクター
ピアスプレス	電気	200Vac 3φ 50Hz	プレス制御盤の主幹遮断器一次側へ直結
	圧空	0．4MPa	プレス受入れコネクター
ロボット2	電気	200Vac 3φ 50Hz	ロボット制御盤の主幹遮断器一次側へ直結
	真空	90kPa	ロボット本体受入れコネクター
積込装置	電気	200Vac 3φ 50Hz	積込装置制御盤の主幹遮断器一次側へ直結
	圧空	0．4MPa	積込装置エアーセットコネクター

*2：日本機械工業連合会 平成28年度 安全な生産システム構築能力向上のための調査研究報告書
http://www.jmf.or.jp/houkokusho/1505/1.html

4.事例の収集（案）

- 事務局で用意する「ICT事例紹介フォーム（案）」に基づき、各社の推進する事例、公開情報から得られる事例や考察等を収集する。
- 収集された事例を活用し、特に以下の点を検討する。
  - 「機能・サービス呼称」～「ICTの主な利用」に基づき、事業環境・サービスの変化について把握
  - 企業横並びに比較し、想定される被害と主な安全機能に基づき、不十分な点の抽出
  - 想定されるセキュリティハザードの具体化
  - 対策の具体化（現実的な観点から）

ICT事例紹介フォーム（案）

機能・サービス 呼称	
ICTパターン	□生産効率向上　□遠隔地からの管理・操業　□管理チェーン最適化　□予防保全
想定災害	
範囲	□機械と人のサービス　□機械と機械のシステム　□機械単体　□部材・電子装置
登場人物	□オーナ　□オペレータ　□労働者　□インテグレータ　□機械メーカ　□部材・電子装置メーカ
ICTの主な目的（最大3件）	・ ・ ・
主な安全機能	・ ・ ・
想定される セキュリティハザード ※本欄は協議後整理	・ ・ ・
対策	

クラウドや広域通信網 サービスの具体化	
制御システムを連結した システム設備	
機械や装置の振舞い制御	
動力源の制御制限	

4.事例の収集（案）

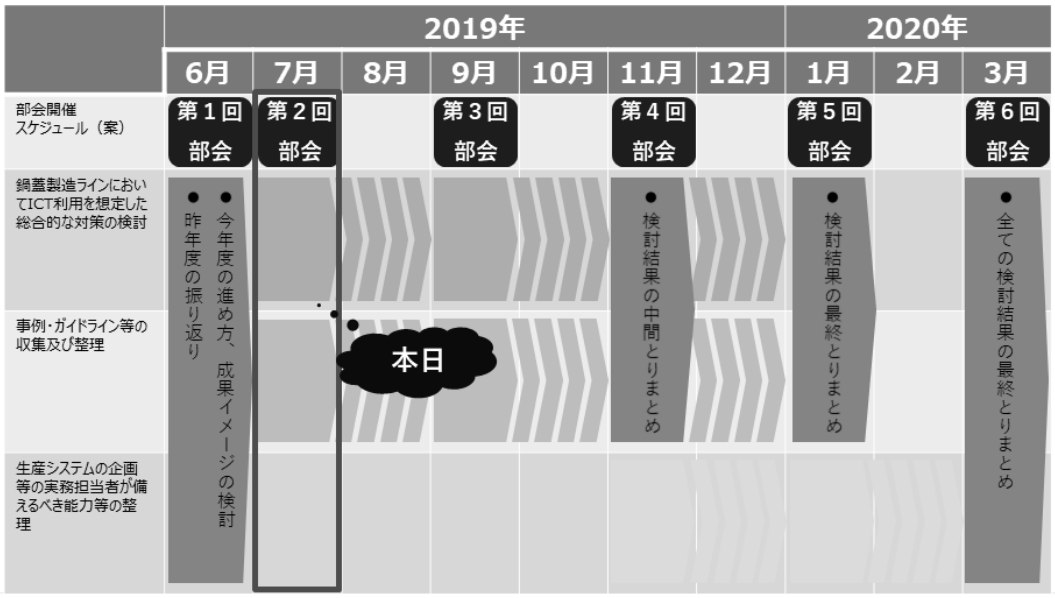
- 事務局で用意する「事故事例紹介フォーム（案）」に基づき本質安全の軽視による事故事例を収集する。
- 収集された事例を活用し、特に以下の点を検討する。
  - 本質安全の代替として確保されている機能安全について把握
  - 事故時の本質安全と本来備えられるべき本質安全とのギャップを抽出し傾向を分析

事故事例紹介フォーム（案）

事故の概要	
事故のカテゴリー	□ 製品の使用時　□ 生産の現場　□ その他
事故の原因	
原因の背景と考えられる事象（根本原因）	
事故時の機能安全	・ ・ ・
事故時の本質安全	
本来備えられるべき本質安全（事故時とのギャップ）	
事故後に取られた対策（あれば）、または、 対策の方向性	

今年度の重点課題と検討の進め方（案）

第1回研究部会の議論を踏まえて、想定する検討スケジュール（案）を改訂し以下に示す。



MRI Research Associates Inc.

２０１９年度 第３回 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部会

第３回研究部会用資料

2019年9月19日

1. 第２回研究部会（7月22日開催）の振り返り

1. 本研究部会における基本的概念・前提
   - ✓ 本研究部会では、ICT等を利用した生産システムにおけるリスクのうち特に人命に関わるものに対して、ISO/IECガイド51に基づき機械の専門家の立場からセキュリティとセーフティの考え方を検討してきた
   - ✓ 人の安全確保は、電源を切ること（工場停止）によって発生する損失よりも重要と考える
   - ✓ 最終的には手動で電源を切ることができる手段を設けることが、生産システムにICT等を利用する上での人の安全確保における前提とする
   - ✓ ICT等の利用を考える場合には、3ステップメソッドにおけるステップ2の前に本質的安全を確保するという基本概念が重要である
   - ✓ 汎用生産設備において安全PLCをネットワークに繋げる必要が無いことは提示した方が良いのではないか

2. 成果のとりまとめ
   - ✓ 基本原則を踏まえた上で、IT、安全、復旧のそれぞれに寄った対策を提示し、実際に対策を行う場合のバランスポイントは、利用者側（例えば、工場）で判断してもらうような形式で成果をまとめることを想定する
   - ✓ 安全学の観点から過去に発生した事故事例を提示しても良いのではないか
   - ✓ セキュリティ脅威に対するカウンターメジャー・参照規格・対策後の再リスクアセスメントの結果が示されることは、対象と想定する中小企業にとって有益と考える

3. その他の課題
   - ✓ トレーニングカリキュラム等の検討は、今後、カリキュラムの対象者等が具体化された後に改めて再考することにしたい

2. 研究部会における成果のとりまとめ（案）

前回の研究部会における議論を踏まえた調査研究報告書の骨子（案）を以下に示す。

調査研究報告書　骨子（案）

基本的概念・前提	✓ 研究部会による検討の基礎となる考え方
提言	✓ ICTを利用する生産システムにおいて人を守るあるべき機械安全
利用ガイド（対策・事例等）	✓ 生産システムにICT等を利用する際の検討等に資する情報

2. 研究部会における成果のとりまとめ（案）

研究部会による検討の基礎となる基本的概念・前提の概要（例）を示す。

概要（例）

（基本的概念）

- ✓ 人の安全確保は、被害への対処によって発生し得る損失等（例えば、工場停止）よりも優先される

・・・・

（前提）

- ✓ 安全及びリスクとは、ISO/IECガイド51において定義されるものを指す
- ✓ 安全な機械設備とは、手動で電源を切る機能を有する設備である

・・・・

2. 研究部会における成果のとりまとめ（案）

研究部会の成果として発信する提言の概要（例）示す。

概要（例）

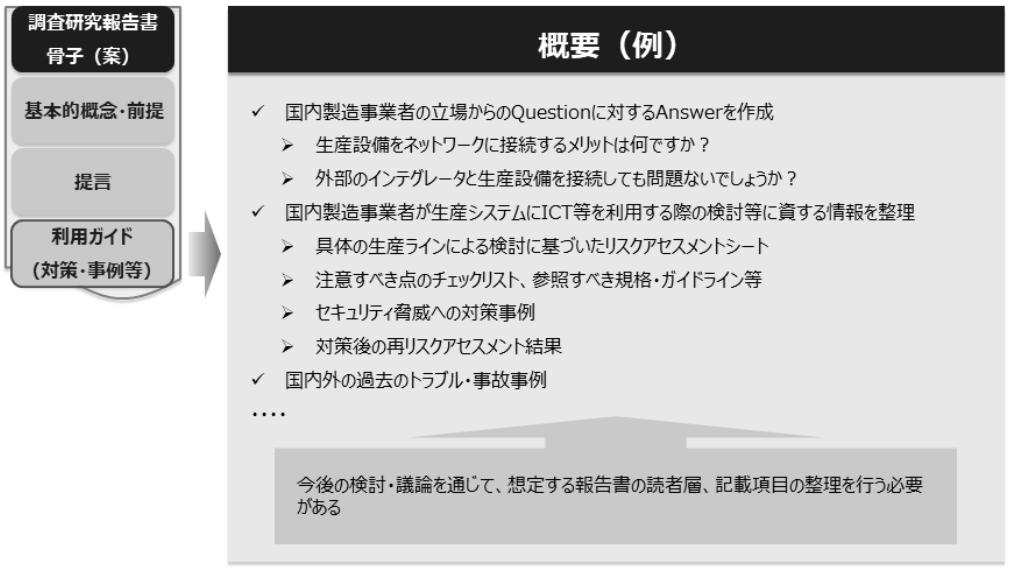
- ✓ 『ICTを利用する生産システムにおいて人を守るあるべき機械安全』を、具体による検討結果に基づき提言として提示

『提言』としてとりまとめを行う上では、研究部会による検討・議論を踏まえて読者層の立場を意識したものにすることが考えられる

（例： 経営/マネジメント層、機械設計者、機械設備管理者、工場オペレータ、等）

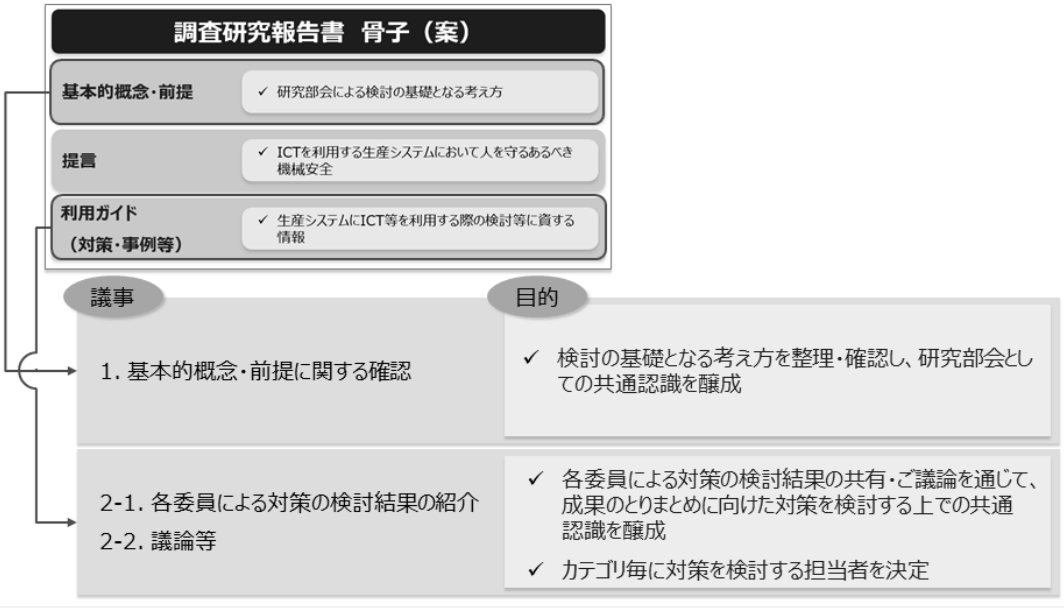
2. 研究部会における成果のとりまとめ（案）

研究部会の検討結果としてとりまとめられる利用ガイド（対策・事例等）の概要（例）を示す。



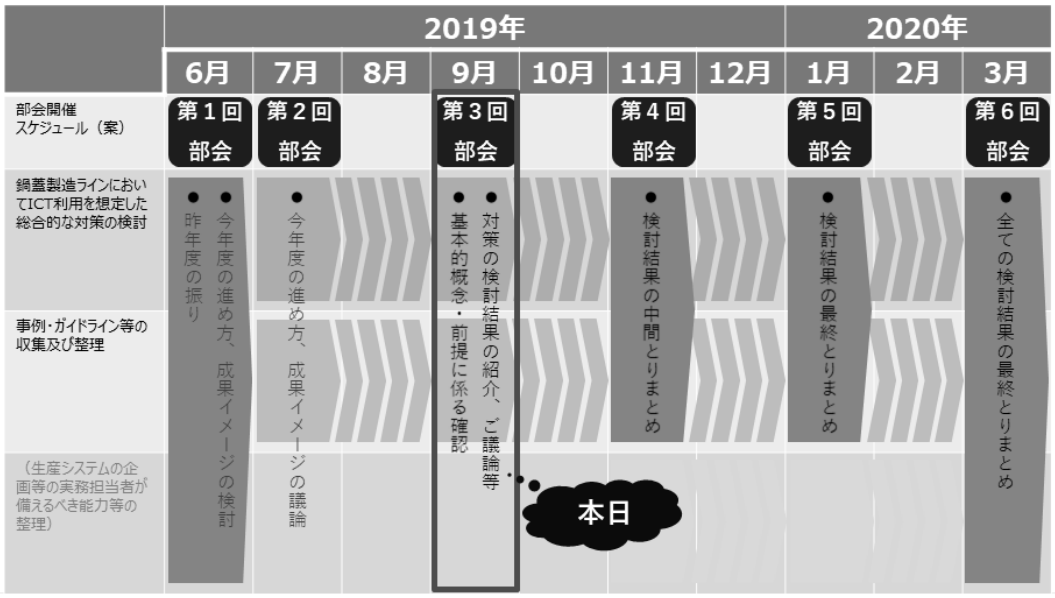
3. 本日の進め方と目的

研究部会の検討結果としてとりまとめられる利用ガイド（対策・事例等）の概要（例）を示す。



4.今年度の重点課題と検討の進め方（案）

想定する検討スケジュール（案）を以下に示す。



MRI Research Associates Inc.

２０１９年度 第４回 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部会

第４回研究部会用資料

2019年11月20日

1. 第3回研究部会（9月19日開催）の振り返り

1. セーフティとセキュリティの基本的な考え方

●第3回研究部会にて、副主査からご提出いただいた内容を転記

- ✓ リスクとは、人が利用・使用する機械・設備・システムにおいて発生する事故の「被害の発生頻度と被害のひどさ」から導かれる値である
- ✓ 事故のシナリオや発生メカニズム分析から、該当箇所のリスクを推定することをリスクアセスメントという
- ✓ リスクが許容できるとは、関係者がその機械・設備等から得られる便益や利益を考慮して、リスクを負うことを選択できることである。関係者の業界、地域および時代によって、許容できるレベルは変わる
- ✓ 安全対策とは、工学的あるいは運用的手段によってリスクを許容できる範囲に低減すること
- ✓ セーフティとは防災、すなわち偶発的または経年的な機械の故障、(悪意のない)ヒューマンエラーや自然災害等によるリスクが許容できる範囲になること
- ✓ セキュリティとは防犯、すなわち悪意を持った人的行為および影響、意図したヒューマンエラーや犯罪行為によるリスクが許容できる範囲にあること

研究部会による「セーフティ」と「セキュリティ」の考え方

- ✓ 安全とは、セーフティ(防災)とセキュリティ(防犯)のリスクが許容できる範囲であること
- ✓ ICT等の新技術を適用する場合、利便性だけでなくリスクの許容性(安全性)についても議論すること
- ✓ ICT等の新技術を無効化することで(例えば電源オフ)、安全な状態が確保できる手段を残すこと

MRI Research Associates Inc.

1. 第3回研究部会（9月19日開催）の振り返り

1. セーフティとセキュリティの基本的な考え方

- ✓ AIを含むICT等の新技術を利用する際のセーフティとセキュリティの考え方には、セーフティとセキュリティ、アベイラビリティ(可用性)と信頼性、レジリエンスの概念を包含する新たな表現を考えたい
- ✓ 今後は、これまで予見不可能として無視していた想定外の事象を、想定して対策を検討することが必要
- ✓ AIを含むICT等の新技術を利用する際に、これらの新技術をどこまで信用するかを課題と捉えて、想定外が起こり得る場合、最後には切り離すことによる安全確保が必要

2. リスク対策の事例紹介

- ✓ ICT等の利用に伴うリスクへの対策とは、既に各現場で行われているITセキュリティリスクに対する対策の延長線上にあるもの
- ✓ IT、安全、復旧の3カテゴリに加えて、マネジメントの検討が必要
- ✓ リスクの発生可能性がゼロになることはない。対策の実行によってリスクは、低減・回避・移転・保有のいずれかに収束
- ✓ リスクアセスメントによって識別されたリスクへの対策後におけるリスクの再評価・効果の測定を行うためには、過年度に研究部会で検討された指標（リスクマトリクス）の発生確率を細分化することが必要

3. 本日の進め方

本日の研究部会における検討項目、論点を示す。

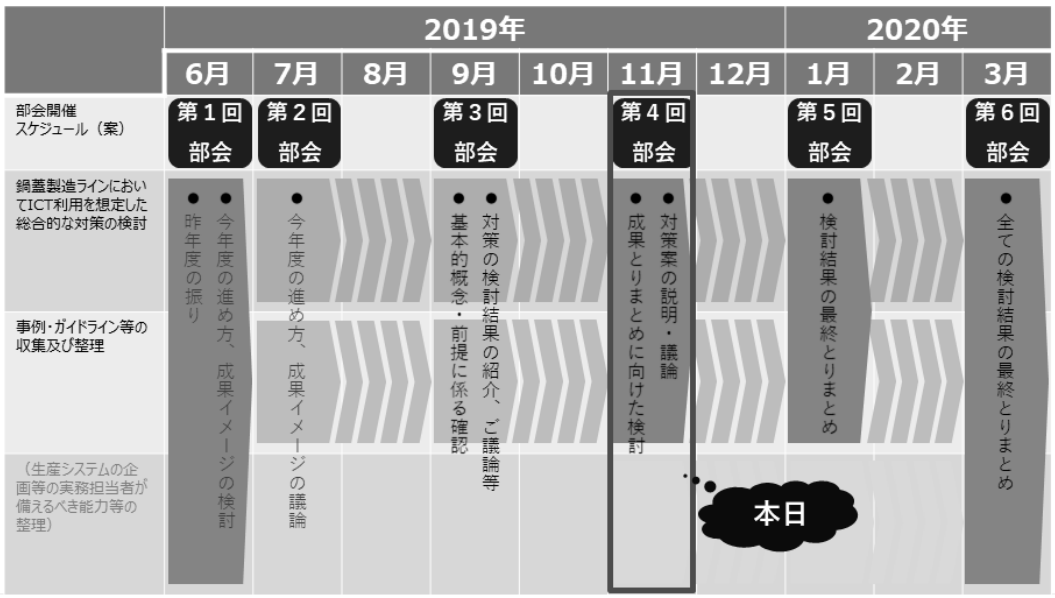
① リスク対策の検討
- IT、安全、復旧の各対策案の説明、議論
  - ✓ 効果の視点による分類
  - ✓ 対策の組み合せ
  - ✓ 脅威の種類

② 成果とりまとめに向けた検討
- 読者層の想定
  - ✓ 例えば、機械設計者、機械設備管理者、工場オペレータ、経営/マネジメント層
- 今年度の提言
  - ✓ 昨年度の提言に、基本的概念・前提、及び、今年度の検討結果を踏まえて内容を追加
- 利用ガイドの具体化
  - ✓ 主要コンテンツ案
    - ① ICTの導入・利用時に注意すべき点（チェックリスト）、検討のプロセス、参照すべき基準・ガイドライン等
    - ② リスク対策（過年度に実施した具体のラインにおける検討結果、IT・安全・復旧毎の対策集）
    - ③ 対策後の再リスクアセスメント結果（再リスクアセスメントシート）
  - ✓ 読者が対策の取り方・留意等をイメージできるような内容

4

4.今年度の重点課題と検討の進め方（案）

想定する検討スケジュール（案）を以下に示す。



5

（再掲）研究部会における成果のとりまとめイメージ

前回の研究部会における議論を踏まえた調査研究報告書の骨子（案）を以下に示す。

調査研究報告書　骨子（案）

基本的概念・前提	✓ 研究部会による検討の基礎となる考え方
提言	✓ ICTを利用する生産システムにおいて人を守るあるべき機械安全
利用ガイド（対策・事例等）	✓ 生産システムにICT等を利用する際の検討等に資する情報

（再掲）研究部会における成果のとりまとめイメージ

研究部会による検討の基礎となる基本的概念・前提の概要（例）を示す。

概要（例）

（基本的概念）
- ✓ セーフティとセキュリティの基本的な考え方を提示

・・・・

（前提）
- ✓ 安全及びリスクとは、ISO/IECガイド51で定義されるものを指す
- ✓ 安全な機械設備とは、手動で電源を切る機能を有する設備である

・・・・

（再掲）研究部会における成果のとりまとめイメージ

研究部会の成果として発信する提言の概要（例）示す。

概要（例）

- ✓ 今年度の本研究部会における検討過程（要旨の整理）を提示
- ✓ 『ICTを利用する生産システムにおいて人を守るあるべき機械安全』を、提言として提示

『提言』としてとりまとめを行う上では、研究部会による検討・議論を踏まえて読者層の立場を意識したものにすることが考えられる

（例： 経営/マネジメント層、機械設計者、機械設備管理者、工場オペレータ、等）

（再掲）研究部会における成果のとりまとめイメージ

研究部会の検討結果としてとりまとめられる利用ガイド（対策・事例等）の概要（例）を示す。

概要（例）

- ✓ 国内製造事業者の立場からのQuestionに対するAnswerを作成
  - ➢ 生産設備をネットワークに接続するメリットは何ですか？
  - ➢ 外部のインテグレータと生産設備を接続しても問題ないでしょうか？
- ✓ 国内製造事業者が生産システムにICT等を利用する際の検討等に資する情報を整理
  - ➢ 具体の生産ラインによる検討に基づいたリスクアセスメントシート
  - ➢ 注意すべき点のチェックリスト、参照すべき規格・ガイドライン等
  - ➢ セキュリティ脅威への対策事例
  - ➢ 対策後の再リスクアセスメント結果
- ✓ 国内外の過去のトラブル・事故事例

・・・・

今後の検討・議論を通じて、想定する報告書の読者層、記載項目の整理を行う必要がある

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

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

発　行　2020 年 3 月
発行者　一般社団法人日本機械工業連合会
〒105-0011
東京都港区芝公園三丁目 5 番 8 号
電話 ： 03-3434-9436