平成 30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

2019 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おります。

本報告書は、2 年度目の検討結果をまとめた中間報告となりますが、関係各位のご参考に寄与すれば幸甚であります。

2019 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する。

本調査研究は 2019 年度での完了を予定しており、本年度の報告は 2 年度目の検討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)　商品事業推進部　次長	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)安川電機　品質経営推進部　規格認証部　技術統括　認証試験チームリーダ	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　基本戦略グループ　参事官補佐	大　能　直　哉
	内閣官房　内閣サイバーセキュリティセンター　基本戦略グループ　参事官補佐	白　石　哲　郎
	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
	(独法)情報処理推進機構　技術本部　ソフトウェア高信頼化センター ソフトウェアグループ　研究員	山　田　朝　彦
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
	(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)三菱総合研究所　科学・安全事業本部　研究員	高　橋　久実子

（2019年3月　現在）

目　次

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。2019 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.研究部会の開催

本調査研究の目的を達成するために、機械安全および設備安全に関する有識者から構成される情報通信技術(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)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 2018 年 7 月 13 日
- 第 2 回 2018 年 8 月 31 日
- 第 3 回 2018 年 10 月 30 日
- 第 4 回 2018 年 12 月 17 日
- 第 5 回 2019 年 2 月 4 日
- 第 6 回 2019 年 3 月 11 日

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、より複雑に高効率に発展を続けている。手動で操作され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連結され、より複雑な処理が可能なロボットが導入され、大量生産を効率的に行うだけでなく、多品種少量生産にも対応するシステムとして進化してきている。

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につながるものと考えられる。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、国の基本方針として示し、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。

我が国では、「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 が提唱された[2]。その新しい社会を目指す産業の姿として、2017 年 3 月に、我が国の産業が目指す姿として「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。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、この Connected Industries は重要な役割を果たすものと位置付けられている[3]。

現状においても、IoT（Internet of Things）を活用した例として、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共有され、消耗品補給や部品交換時期の管理を最適に行うように利用されている。また、ビルで使用される空調機器においても、空調機器が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共有することでメンテナンスのタイミングを最適化する取り組みに使用するとともに、ビル内の温度環境を適切に調整するために、温度の監視と空調機器の調整を、遠隔で行うことも可能にしている。その他、企業ではなく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

---

[2] Society 5.0 とは、内閣府 https://www8.cao.go.jp/cstp/society5_0/index.html
[3] 2018 年版ものづくり白書
http://www.meti.go.jp/report/whitepaper/mono/2018/index.html

家電が登場してきている。

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データを取得し、それらを相互につないで共有したデータを有効活用することで、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。

我が国の製造業における生産システムでは、システムを構成する機械の相互の情報交換は、かねてから行われてきたが、インターネット等の外部のオープンなネットワークへの接続は、情報漏えいの危険性から遮断されていることが通常であった。現状においても、我が国においては、原則として、生産システムのインターネットへの接続を禁止している企業は多い。

一方で、IoT、ICT の急速な技術革新を背景として、製造業においても、IoT、ICT を有効に活用することで、これまでにない新しい製造業を実現しようとする動きが世界的にも活発化しており、我が国においても、これらの取り組みを進めていくことが重要な課題となっている。経済産業省が提唱する「Connected Industries」においても、5 つの重点取り組み分野の一つとして「ものづくり・ロボティクス」があげられており、今後のグローバルな競争の中で重点的な政策を進める分野として指定されている。

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）を行ったり、生産システム全てをデジタル化して仮想モデルを構築しシミュレーションを行うことで、多品種少量生産における生産ラインの最適化を図ったり、ライン構築前に生産性の効率を評価することを可能としたり、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。ただし、そのメリットが増大するのに反して、セキュリティの脅威にさらされる危険性も高くなることは認識しておかなければならない。ICT を便利に利用していくうちに、生産システムのセキュリティのリスクが高まっている可能性がある。

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。インターネットには接続しないことを原則としていても、生産システムのどこかで、誰も認識しないうちに接続されてしまうことは、予想しておかなければならない状況になっている。

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

いるが、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といわれている[4]。また、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 [4]。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 [4]。

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と言える。

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成し、そこにセキュリティ分野から多くのオブザーバーに参加をいただき、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て設定した。

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、次の表のように示されている[5]。

[4] IPA、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

[5] 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

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と、その要件として、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、その中でリスク評価も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。

研究部会における検討の成果を次章に示す。

4. 検討成果

4.1 提言（案）の検討

昨年度の研究部会においては、研究部会における議論に基づき、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、整理して示した。今年度は、さらに議論を重ねて、昨年度示した考え方に基づき、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、以下を示す。

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。

4.1.1 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[6]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

---

[6] 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）

考えて評価を行うことが適切であると考えられる。

4.1.2 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[7]）を参照することが求められる。

4.1.3 最終的な対策

セキュリティ脅威は、安全関連制御系に影響を与える。したがって、セキュリティ脅威に対する安全対策として、安全関連制御系を採用することはできない。そのため、安全関連制御系に拠らない安全システムの安全化手段が必要とされる。最終的な対策としては、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、侵入した脅威が威力を発揮することを 100%防ぐことはできない。セキュリティ脅威からシステムを防御する物理的なカバーは存在しないためである。そのため、セキュリティ脅威への対策は、いかに早く発見し、迅速に確実にシステムを停止するかにつきると言える。また、停止するための方法としては、ソフトウェアによる制御から独立した状態のセキュリティ脅威の影響を受けないハードウェアによる方策を用いることが望ましいと考えられる。

---

[7] 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）

4.2 生産システムの ICT 対応リスクアセスメント

4.1 で示した提言の基本的な考え方にあるように、生産システムにおけるセキュリティ脅威は機械安全のハザードと考えて対応することが求められる。そのためには、セキュリティ脅威に対するリスクアセスメントを、生産システムに対して行うことが必要とされるが、その方法については、現段階では確定したものは存在していない。生産システムの ICT 対応の安全性について評価することを目的として、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の方法について検討した。

今回は、機械安全の技術者が理解しやすく取り組みやすいセキュリティ脅威のリスクアセスメントとすることを目指して、最初に ICT を利用したソリューションを設定し、そのソリューションを利用するシナリオを考え、シナリオの中で想定される被害を検討していく方法とした。

セキュリティ脅威のリスクアセスメントを行うために、セキュリティ脅威リスクアセスメントシート（以下、リスクアセスメントシート）を設定した。表 4-1 に、今年度検討したリスクアセスメントシートを示す。「a.対象ソリューション」から「i.脅威源」までの各項目は、セキュリティ脅威の状態を表現するための項目であり、その状態を明確にしたうえで、被害の大きさと可能性からリスクを求めてシートに記載することを目的としている。

表 4-1 リスクアセスメントシート

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

リスクアセスメントシートの項目名と内容を表 4-2 に示す。

表 4-3、表 4-4、表 4-5、表 4-6 に、リスクアセスメントシートの各項目に入力する内容の例を示す。

リスクアセスメントシートの項目に入力した内容に基づき、リスクアセスメントを行う。リスクアセスメントは、「被害の大きさ」と「可能性」を 3 段階で示し、その結果から表 4-7 に示すリスクマトリックスでリスクを求めることとした。

「被害の大きさ」については、人命を重視する観点から、人や機械に被害が生じた場合は「大」、工場の生産が停止した場合は「中」、工場の生産は停止しなかった場合は「小」と表現することとし

た。被害の大きさを表現するにあたって、壊滅的な被害を想定した場合には、4 段階で表現することもあるが、生産システムを前提とした場合、そのような「極大」の被害は発生すると考えられないため、今回は 3 段階で表現することとした。

一般的に IT セキュリティの対策は、実行の難易度を上げる等の対策により「可能性」を下げることはできるが、「被害の大きさ」を小さくすることはできないことを考慮して見積もることが求められる。

表 4-8 にリスク見積もり結果までを含めたリスクアセスメントシートの入力例を示す。ここでは、シナリオごとに複数の被害を想定しており、一つの被害に関して、複数の脅威源を抽出している。リスクの見積もりに関しては、被害の大きさを被害ごとに求めて、発生の可能性も検討した上で、リスクを見積もっている。

付録には、複数のソリューションについて複数のシナリオを考えた場合のリスクアセスメントシートを示す。

表 4-2 リスクアセスメントシートの項目名と内容

	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

表 4-3 対象ソリューションとソリューション解説の例

	対象ソリューション	ソリューション解説
1)	機械の遠隔監視診断	機械メーカー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。
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。

表 4-4 シナリオとシナリオ解説の例

	シナリオ	シナリオ解説
1)	生産中	動力源 ON。 機械が動作している状態。
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。
3)	現場エンジニアリング	動力源 OFF。 現場で設定の変更作業を実施している。
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。
5)	再立上げ	動力源 OFF→ON。 機械を動作状態に立ち上げる。
6)	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。
7)	部分工程の機械保全	生産中に特定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。 他の工程の動力源は ON。
8)	部分工程の変更	生産中に特定工程の機械制御の設定変更など、ソフトウェアに関係する修正が発生したケース。 IoT 機器そのものへの設定変更やエンジニアリング。 関係する工程の機械設備の動力源は OFF。 他の工程の動力源は ON。
9)	全行程の停止と変更	全行程を停止し、工程の組み換えや機械の入れ替え、設定変更などを行い、生産プロセス全体にわたる変更を行う。 全設備の動力源は OFF。

表 4-5 想定被害と被害シナリオの例

	想定被害	被害シナリオ
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。
2)	効率・品質低下	保守 PC の不正操作により、対象機械の動作パラメータが不正に変更され、気づかずに運転継続。
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。
4)	生産情報漏洩	射出成型機など、原料と機械機構、温度調整の設定や動作時間等が漏洩し、製造ノウハウが流出。
5)	不正設定	保全 PC 内部のエンジニアリングデータが書き換わっており、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）
6)	稼働中工程の生産中断	機械修理時の作業員の持ち込む PC 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。

表 4-6 脆弱性と脅威源の例

	脆弱性	脅威源
1)	PC のアップデート不足	ウィルス（感染）
2)	RDT（Remote Desk Top）による遠隔からの不正操作（誤操作）	保守員
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 故障やウィルス（感染）
4)	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）
5)	遠隔からの不正プログラムのダウンロード	ハッカー、ウィルス
6)	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
7)	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）
8)	遠隔監視用接続機器（PC 等）の管理不足	ウィルス（感染）、バックドア
9)	遠隔監視用接続機器（ルータや FW 等）の管理不足	バックドア
10)	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ーの未整備）	遠隔業者
11)	IoT データ収集機器（PC 等）の管理不足	ウィルス（感染）、バックドア
12)	管理の悪い作業用 PC からのウィルス伝搬。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
13)	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、ウィルス（感染）
14)	保全中の工程からの稼働中の工程への影響	保守 PC の誤操作・誤設定
15)	共通要因故障 共通装置の誤った停止による IoT 機能喪失 例）時刻サーバー停止、中継サーバー停止、品番管理 PC 停止	工程保守のための部分的なシステムの停止
16)	停止中工程の作業員からのリモート接続による漏洩	他の工程の作業員
17)	リモート接続	作業員
18)	不正な機器接続	作業員
19)	不要になった機器の廃棄処理の不徹底	処分業者

表 4-7 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

表 4-8 リスクアセスメントシート入力例（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	被害の大きさ	可能性	リスク
1.1	機械の遠隔監視診断	予兆保全サービスのため機械の動作データを収集する。	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。	Wannacry			中	中	中
1.1.1.1								PC のアップデート不足	ウィルス（感染）			
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			
1.1.1.3								制御 CPU がネットワーク処理兼用	工場内ＰＣ故障やウィルス（感染）			
1.1.2					効率・品質低下	保守用 PC の不正操作により対象機械の動作パラメータが不正に変更され気づかずに運転継続。	Stuxnet			中	小	中
1.1.2.1								PC のアップデート不足	ウィルス（感染）			
1.1.2.2								PLC 等の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）			
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			大	小	中
1.1.3.1								PC のアップデート不足	ウィルス（感染）			
1.1.3.2								PLC 等の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）			
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、ウィルス			

4.3 今後の検討事項

今年度の検討では、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シートとして提示した。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。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は、次年度の主な検討課題として考えている。また、これらの検討をふまえて、機械安全の技術者に対して、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もあわせて進めていくことが求められる。

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うことを考えている。

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。

---

[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

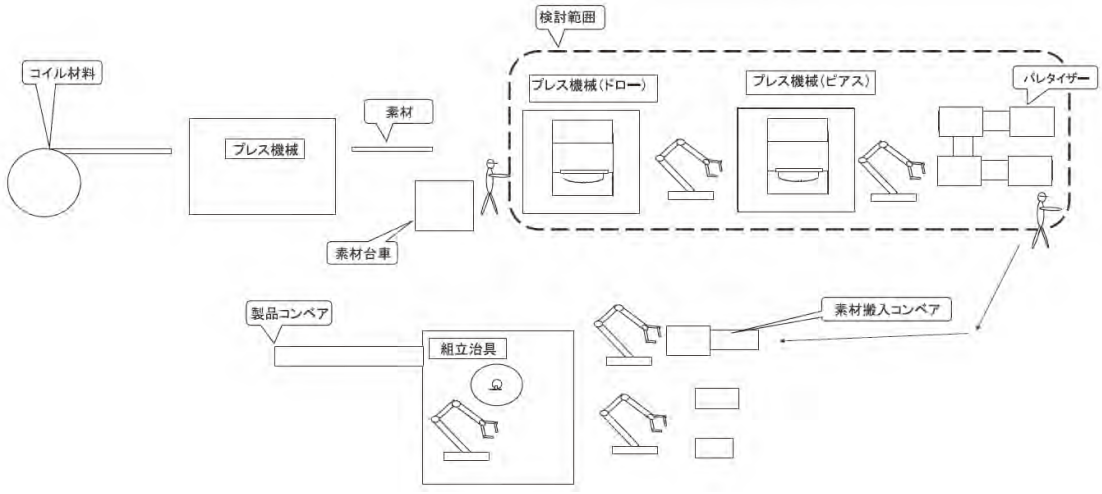


図 4-1 鍋蓋製造ライン

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。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。

5. 研究部会における議論

5.1 第 1 回研究部会

(1) 今年度の検討方針

- 生産設備をIoTでインターネットに繋げるということは、生産性・安全性の向上が可能になる、ということを前提として考える。
- 「復旧」まで含んだ検討をするかどうかについて、検討しておくべきである。「復旧」まで考慮する場合には、復旧のためのガイドラインがあると有用であると考えられる。

(2) セキュリティ脅威の検知と安全確保のあり方

- サイバーアタックを受けた際に、オペレーターがすぐに気づくことは現実的には難しい。IoT化を考慮すると、セキュリティに関するアラームの用意が必要とされる。一方で、オペレーターに知見が無いとアラームが検知しても対応が難しく、対応プロセスの教育が必要とされる。
- 現状においては、社内では、セキュリティ脅威によるリスクを検討するルールは存在していない。今後は、リスクを認識する必要があり、具体的なケーススタディの作成が必要とされる。

(3) ICT 等の活用によるサービスの影響

- ロボットメーカーだけでは、ユーザーについて把握しきることは困難である。ロボットメーカーとユーザーの両者にリスクアセスメントの専門家が必要である。またシステムインテグレーターが、両者の間の協調に寄与する必要がある。
- ビジネス上の戦略として、ICT/IoTの導入は避けられない。その一方で、顧客から情報セキュリティに関する問い合わせがあった際に、十分な知識を有しているとは言えない。

(4) 今後の検討について

- ICT/IoT を活用するシチュエーションを想定することが第一段階になるだろう。生産システムの遠隔監視、プログラムの自動書き換えなどの活用方法について想定することが必要とされる。

5.2 第 2 回研究部会

(1) 検討の視点

- 制御装置において、機能安全は部品の故障に対する確率論で検討するため、部品の故障に落とし込む。プログラムに脆弱性があったとしても、これまでは、利用者の性善説や機械エ

ンジニアの知見により運用してきた。しかし、ICT が利用されると、IT に対してリテラシーを有さない人や、悪意のある人が、脆弱性を高める使い方をする可能性がある。それについては、確率論ではなく、確定的であるとして検討する必要がある。

- ICT の利用により発生する問題においては、セキュリティとセーフティの関係を明確にするべき。体系化が求められる。

(2) 事例紹介

各委員から、ICT を利用した際の、セキュリティの検討ポイントについて、以下の事例が紹介された。

- IEC TR 63074[10]に基づき機械安全におけるセキュリティの検討ポイント
- 生産量の計画・実績のリアルタイムデータの活用による「生産実績の見える化と設備稼働率向上」
- RFID を用いた工程連携による「品質向上・ヒューマンエラーの撲滅」
- センサーを活用したコンベアのコンディションベースの「予兆メンテナンスシステム」
- 射出成型機と周辺装置の集中管理システム
- 自動車用ユニットの組立装置と周辺装置の管理システム
- 工場内搬送用の「遠隔操作による無人運転車」
- 生産工場内部の基幹ネットワークとライン制御の分離

5.3 第 3 回研究部会

(1) 機械安全の設計プロセスにおけるセキュリティ要件

- 日本機械工業連合会の研究部会により平成 28 年度まで検討された統合生産システムのモデル（鍋ふた生産システム）は、セキュリティの観点は考慮されていないため、今年度の検討例題として利用することとする。
- ISO 12100 にセキュリティの考慮を追記することは可能だろう。しかし、分析の後半で、ハザードと安全の分析方法と脆弱性・脅威分析の方法が異なることに留意する必要がある。
- セキュリティ脅威の検討を進めるにあたっては、ICT 利用の目的とサービスの内容、および接続方法を決めないと対策の検討が難しい。まずは、追加する ICT サービスを決定することが必要とされる。

[10] IEC TR 63074 ED1 Security aspects related to functional safety of safety-related control systems, IEC TC44/WG15 において開発中, 2019/06 発行予定

(2) 安全 PLC について

- 安全 PLC[11]については、普通の PLC よりもセキュリティ強度が高いと考えられているのではあれば、それは間違いではないか。
- どちらもプログラムをダウンロードして動かす、という意味では同等である。安全 PLC の安全性については、あくまでも故障率の話として理解すべきである。ネットワークに接続されれば、脆弱性は増加する。
- 安全 PLC の使用に関しては、メーカーが安全マニュアルを発行しており、安全マニュアルに従ったシステムの構築が必要とされる。

(3) セキュリティ対策の方法

- セキュリティ対策を全てソフトウェアで構築すると非常にコストがかかるため、ハードウェア対策とのハイブリッドの方法が推奨される。ハードウェアで対応した方が、コスト面で有利な場合が多い。
- 全てが確定的に動けば間違いないが、セキュリティに関しては、想定外の事象を検討する必要がある。
- 安全コントローラー等のコンポーネントは、コンポーネントとして組み込みデバイスの認証を取得しているが、使用方法を守らなければ安全ではない。PLC 等の制御機器の利用条件を示すガイドが必要とされる。

(4) 今年度の検討対象のシステム

- 安全設計における最初のリスクアセスメントは、安全機能が無いことを前提で実施する。同様に、セキュリティの場合も、セキュリティ対策機能が無い前提で検討し、攻撃された場合の被害を算出し、セキュリティレベルを決定する。
- 生産情報やメンテナンス情報を利用するため、ネットワークに接続することを前提としてリスクを検討し、対策案を考えていけばよい。
- これらの検討のプロセスがガイドラインになるのではないか。
- 基本的には、機械安全に軸足をおいて、その上でセキュリティの課題を克服していくものとする。本研究部会の成果を読む人は、機械安全に関わる人達とする。

(5) 検討の内容

- 検討の前提としては、安全部分と非安全部分はゾーニングされているということとする。ゾーニングされた上で、安全側を安全 PLC かリレーかで対策を立てることを検討する。
- 対策した結果として、安全あるいはセキュリティに影響が考えられる場合に、どちらに落とし

[11] Programmable Logic Controller

込むかというバリデーションも想定するべきだろう。

- まずは、安全 PLC をネットワークに接続するかどうかを検討する。その一方で、生産システムからのデータ収集や、安全 PLC とのデータ交換も考慮するべきであり、最低限必要とされる障壁の説明や、想定されるリスクが含まれていればよいだろう。

5.4 第 4 回研究部会

(1) まとめの方向性

- あえて最初はセキュリティを考えない構成にして、セキュリティ分析を行ったら、構成に応じてセキュリティ対策の要件が明らかになってくるという形式を考えている。
- 利用者が興味を持つ内容とすることが必要である。セキュリティ分析を行ったら、様々な問題が顕在化するというシナリオを想定する。

(2) データの提供について

- データのオーナシップを考慮しておくことが求められる。データの所有権と利用権について整理しておくことが必要。
- FA の領域では、データの所有権は、生産システムのオーナー側にあると考えられている。
- データを提供していただければ予防保全の観点から適切な交換時期を示すことができる、と提案しても、簡単にはデータの提供は認められない。工場の稼働データはノウハウと考えられており、最終的には提供されないことが多い。

(3) 安全関連部の分離

- 安全関連部が ICT の部分と分離して独立することで、安全は脅かされないという見方が基本と考えている。
- 分離した構成としていても、結果的に干渉することもあり得る、というのが現時点での世界の認識である。
- 安全重視なのか可用性重視なのかセキュリティ重視なのか、それぞれ別々に発展してきたが、つながることで境界があいまいになっている。どのように切り分けて、どこに重点を置くかを考える必要がある。
- 本研究部会のスタンスとしては、安全系が正しく設計されている前提のもとに、セキュリティ脅威により安全系が無効化する可能性に対してアセスメントを行うものとする。

5.5 第 5 回研究部会

(1) 提言案について

神余副主査から提示された提言案について議論が行われた。

- リスクが影響を与える対象を明確にした方が、読者は理解しやすい。財産が対象なのか、人が対象なのか、明確にしておくことが求められる。
- 安全制御系はハードウェアで構築するべきだという方針は、確かにそのとおりだと考えられる。
- プラントや鉄道システムでは、突然の停止は必ずしも安全につながらないが、機械安全のスコープであれば適用可能と考えられる。
- 複雑系になるほど停止は困難になると考えられるが、機械安全を対象とした場合には可能と考えられる。
- セキュリティ脅威の実現する難易度の見積もりは、機械を扱う事業者には難しい。これを、いかに簡単で使いやすいものにできるかがポイントである。

(2)「安全な生産システムの ICT 対応」について

神余副主査作成の資料（付録 A）について議論が行われた。

- IEC TR 63074 の考え方は、セキュリティとセーフティで異なるため、その考え方の違いを記載した方がわかりやすい。
- 脅威分析のいくつかのパターンを示すことで、何が起こるのかを理解できるようにする。
- 安全と資産の、どちらにフォーカスするのかを記載するべきだろう。データを含めて資産としているが、最も優先すべきは安全である。

(3) 成果のまとめかた

- セキュリティのリスクとして、具体的な事例をあげた解説が必要である。
- リスクマネジメントを理解することは難しい。一方で、安全のリスクアセスメントは、トレーニングにより対応可能と考えられる。現場で役立つものとするためには、確定論として考えて、対策を検討することが求められる。
- セーフティの分析の中に、セキュリティの観点を含める方針で検討を実施したい。
- 構造は同一であっても、作業によって被害は変わる。リスクアセスメントを行うためには、作業分析が必要と考えられる。
- 廃棄・リサイクルは対象外とする。機械の運用・作業という観点で検討する。

- セキュリティ脅威の洗い出し方を理解できるようにしてほしい。機械安全のリスクアセスメントを実施できる人であれば手が届くレベルとしてまとめたい。

5.6 第 6 回研究部会

(1) 提言について

- 神余副主査から第 5 回研究部会で示された提言案を、今年度の研究部会の提言とし、報告書に掲載することを確認した。

(2)「安全な生産システムの ICT 対応」について

セキュリティ脅威リスクアセスメントシートの案（付録 B）について議論が行われた。

- 機械安全の観点から、セキュリティの脅威に関するリスクアセスメントを実施する方法を示したい。
- 対策の方法についても検討したが、今年度は対策については検討の対象外とする。
- 対象とするソリューションを設定し、そのソリューションにおけるシナリオを考えるところからスタートする。
- 発生が予想される被害を想定し、それがどういう理由で発生するのか、どこに脆弱性が存在しているのかを洗い出す。
- 脆弱性に対して脅威源を指定し、被害の大きさ、可能性を 3 段階で表現し、リスクマトリックスから、リスクレベルを求める。
- これにより、制御用情報システムが持つ脆弱性をあぶりだすことができ、その対策を検討することができるだろう。
- 守るべきものをリストアップするところから始める方法は取り組みにくいため、今回のソリューションの設定から始める方法の方が有効と考えられる。
- セキュリティの脅威は時間が経つと進歩すると考えられる。時間が経つ内にルールは変わっていくと考えられるため、定期的な見直しが必要である。

(3) 現状と将来に向けての課題などについて

- セキュリティアタックを受けて検知された際に、生産が継続できる状況であったとすると、マネジメントの観点から、工場長はどのような判断をすべきなのか。マネジメントも含めた判断の指標の検討も必要なのではないか。
- マネジメントの観点からはコスト面が重要であるが、機械安全の観点からは、最も重要なことは人命を守ることであるという前提とした方がよいだろう。
- セキュリティは安全の制御にコンピューターが利用されるため、信頼性が関係してくる。重

要な 4 つは、リライアビリティ(信頼性)、セーフティ、セキュリティ、レジリエンスである。優先度を付けて検討していくことが求められる。

- 次年度においては、第一に対策の検討を進めることが求められる。そのうえで、トレーニングカリキュラム等への展開も検討が必要とされる。

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。

昨年度は、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。今年度は、より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。

以下に、ヒアリング調査により得られた、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のポイントを示す。

A) システムインテグレーターの役割

- ロボットは、一般的にロボットメーカーから購入してきただけでは、すぐに使用することはできない。
- 作業の対象物が何か、どのような処理を行うかによって、必要な周辺機器（ハンド等）を用意し、必要な知識をプログラミング等によりロボットにインプットすることが必要とされる。
- システムインテグレーターは、これらの役割を担っており、その中で、安全性も確保することが必要とされている。

B) アプリケーションパッケージとしての提供

- 協働ロボットは、従来の産業用ロボットの概念が適用できない製品であり、まだ新しい製品であるために、使用例の紹介も多くない。
- そのために、協働ロボットに興味を持つ製造事業者は多く、問い合わせも多数あるが、具体的な使用目的が明確になっていない場合も多いため、トライアルでの使用ができやすいように、アプリケーションパッケージとして、目的別に必要な周辺機器等を揃えて商品化して提供している。
- パッケージ導入の促進とサポートを行うため、必要な情報が入手できる協働ロボットの専用 Web サイトを構築してサポートしている。

C) 協働ロボットにおける安全性確保

- 現在、協働ロボットの活用の機運は高まっていると言える。ただし、そのメリットは、明確に認識されているとは言えないため、この状況で事故が発生した場合に、その機運が低下する恐れがあり、その点からも、安全性確保は最重点課題であると考えている。

D) 協働ロボットのメリットを生かすために

- 協働ロボットのメリットを生かすには、ロボットと作業者の衝突が発生することを、ある程度までは許容することが求められる。

- 協働ロボットについて正しく理解されていない場合には、それが許容されない。協働ロボットの安全性確保に対する企業の理解が乏しいのではないかと考えられる。

- 協働ロボットの停止を機能に組み込み、作業者との衝突を避けるように確定的に動かすことはできるが、安全である一方、協働ロボットのメリットを減らしてしまっているともいえる。

- ロボットを停止させずに、作業者と柔軟に連携させることが、協働ロボットのメリットを生かした導入の基本的な考え方であるが、その実現は簡単ではない。メリットを生かす思い切った運用は、現在ではあまり行われているとは言えない。

E) 協働ロボットの活用に向けて

- 海外の自動車メーカー等では、日本よりも積極的に協働ロボットの利用を推進しているようである。

- 国内の大手企業でも、協働ロボットのメリットを認識しているが、現状においては、効果的に導入するための周辺環境の整備段階にあるとみられる。適切に使用するためには、ハンドや周囲の状況を認識するセンサー等を新たに開発する部分もあり、積極的な利用が進むには、まだ時間が必要であると考えられる。

- 労働安全上の要求から、作業者とロボットが衝突する可能性については、これまでに許された前例がないため、企業としても、それを認めることに関しては非常に慎重であり、導入が進まない理由の一つになっているとも考えられる。

F) 協働ロボットの認証取得

- システムインテグレーターとして、複数のメーカーの協働ロボットを取り扱っているが、いずれの協働ロボットも、ロボットの機能に対して認証を取得している。

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。

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

平成 30 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　2019 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

付　録

付録 A-安全な生産システムの ICT 対応（神余副主査資料）

付録 B-セキュリティ脅威リスクアセスメントシート

付録 C-作業委託報告書（議事録等を含む）

付録 A-安全な生産システムの ICT 対応（神余副主査資料）

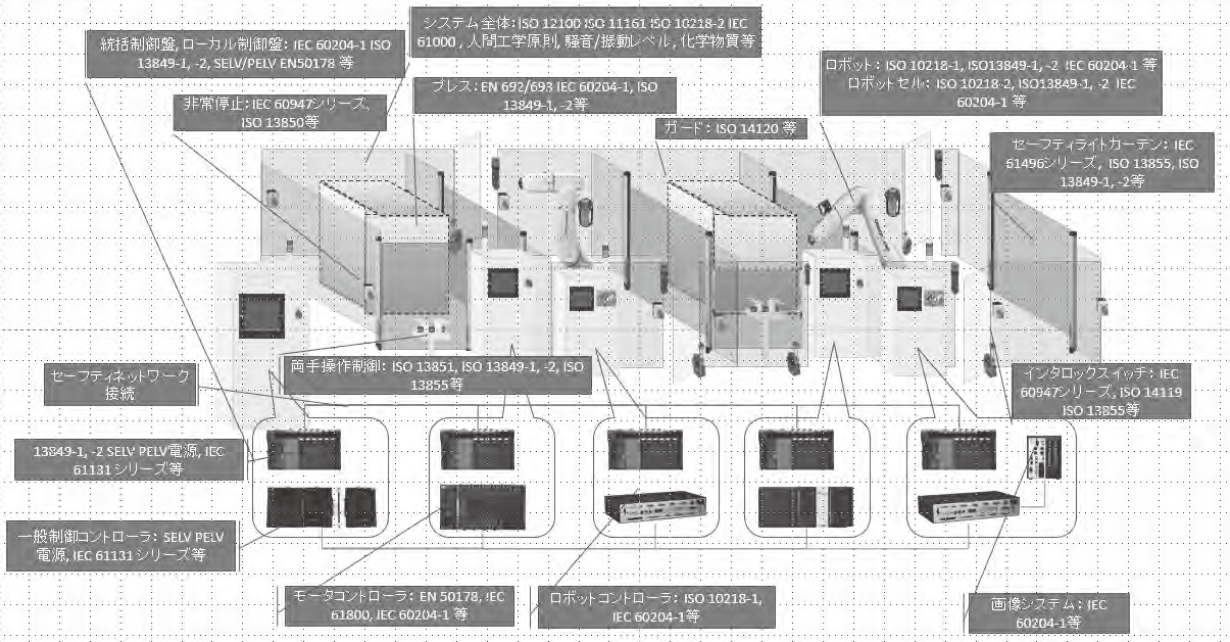
安全な生産システムの ICT対応(案)

目的・手法

- 目的
  - ICT導入した生産システムの安全性について検討するため、安全な生産システム事例にICTサービスを追加して、セキュリティ面からの安全性分析を行う。
- 手法
  - H28年成果の「安全な生産システム検討」のFMSをもとに、リモート診断監視を行う機能・設備を追加する。
  - この設備について、IEC 62443に基づくセキュリティ分析を行う。特に、安全性への影響を分析する。
    - 安全制御系の分析は、IEC TR 63074に基づく。
  - 安全機能を損なわないようなセキュリティ対策の実施までを行う。

安全機器/制御機器配置イメージ

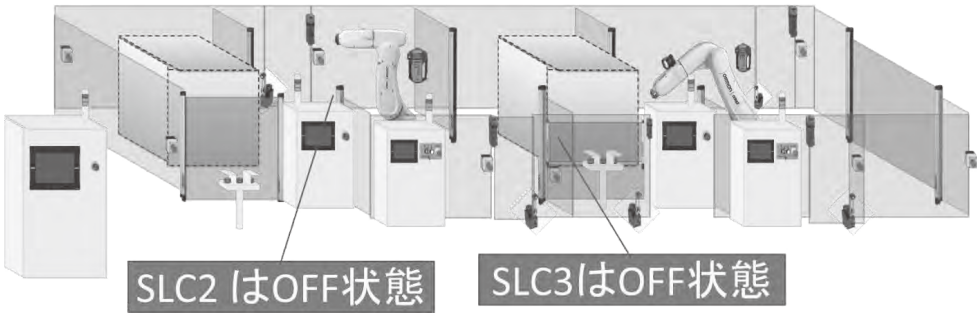
関連規格*と各安全機器/制御機器配置イメージ（例示）



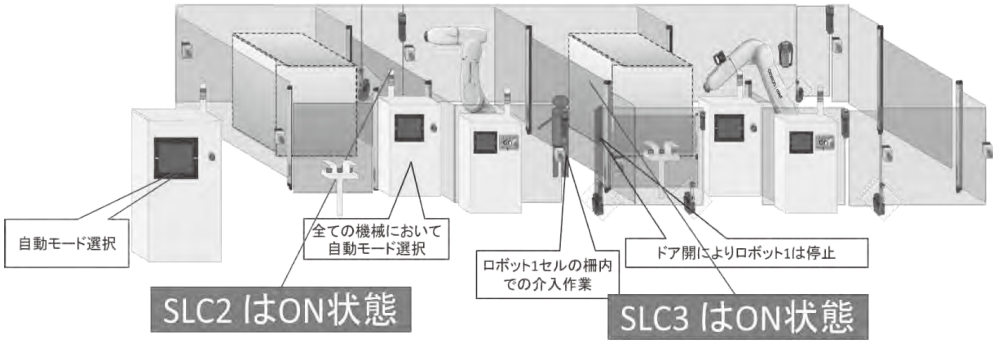
*記載の安全規格類はあくまで例示であり、これらが全てと言うわけではない。

動作例(柵内ライトカーテン)

自動運転中



ロボット1の介入作業時

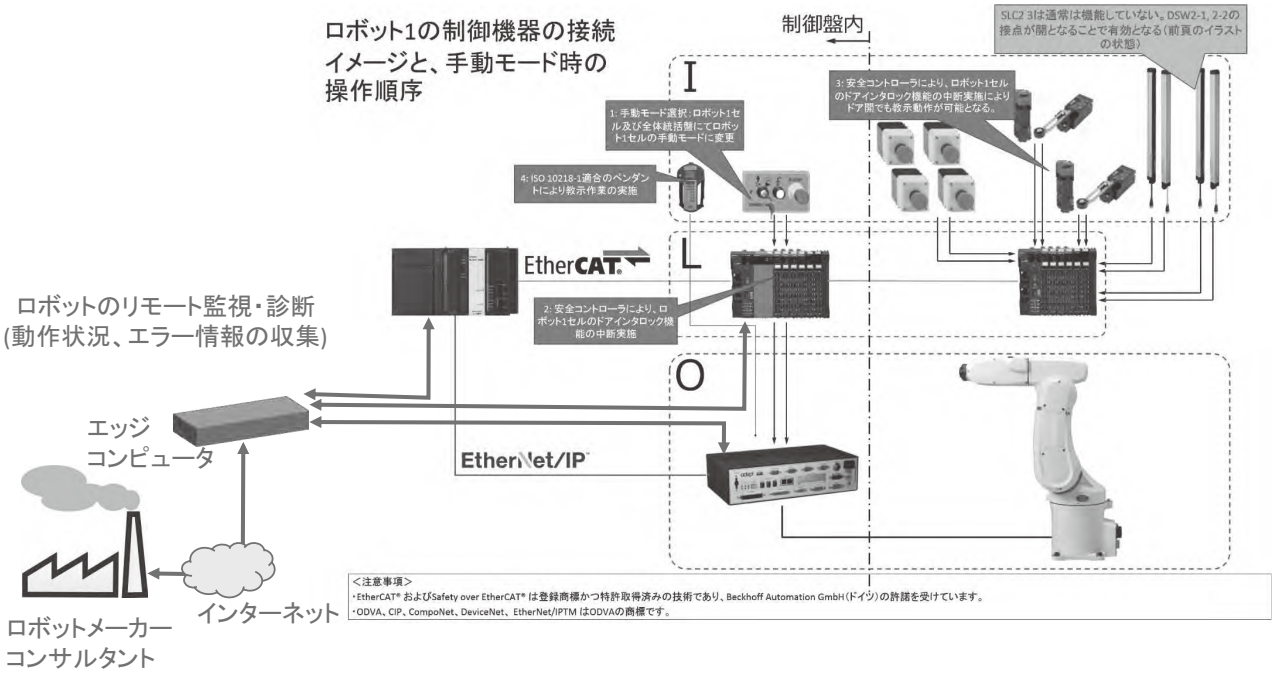


ロボットのリモート監視診断

- ロボットメーカーがロボット状態を監視
  - エラーやチョコ停などを監視→故障等への迅速な対応
  - 消費電力、速度、位置などの変化を監視→モータや構造(重量バランス)の劣化
  - ティーチング動作とシミュレーションの比較→ティーチングへのアドバイス

  - 一日数回、ロボットコントローラからデータ送信。
  - 問題解決時には、ロボットメーカからコマンド送ってデータを取る→双方向通信
  - ロボットだけでなく、生産システムの状態いろいろとるなら、データ纏めにエッジコンピューティングが欲しい

ロボットのリモート監視診断の構成

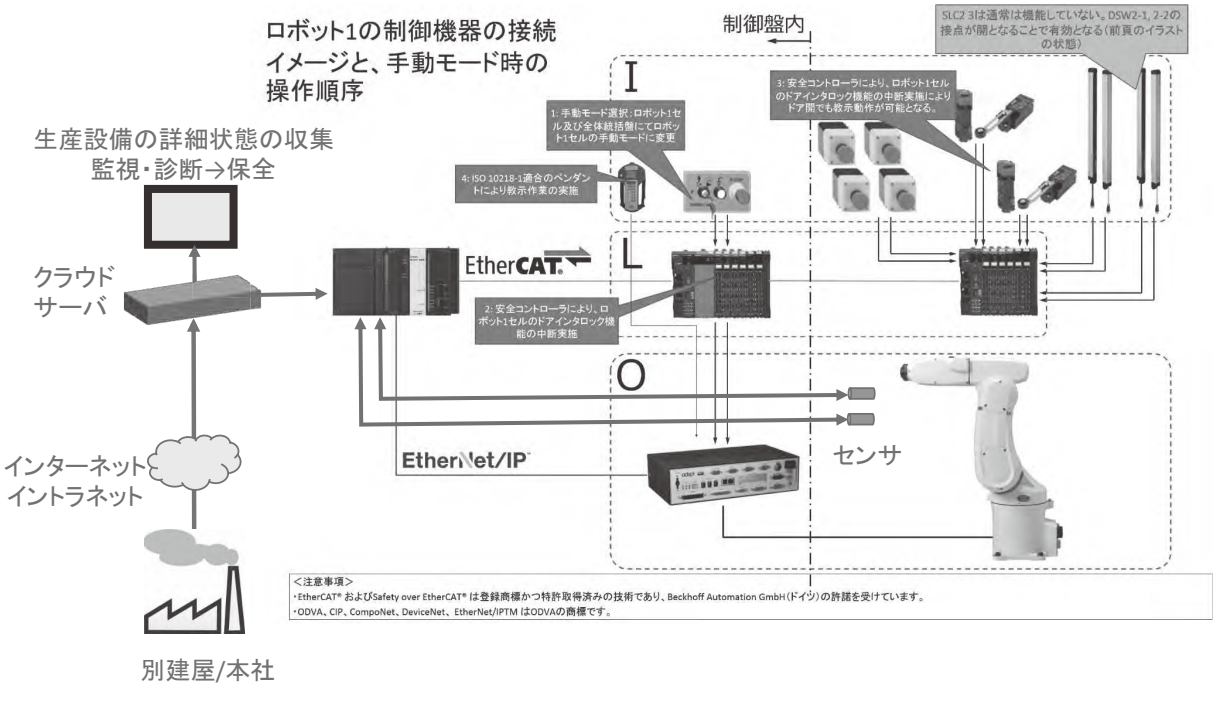


生産設備の品質管理（工場内クラウド）

- 生産設備の品質管理（状態管理）
  - 設備の細かいところの状態（クリアランス，スリップ率など）を計測し，保全係が監視し必要に応じて生産設備の保全を行う。
  - 工場内にクラウドを立ててデータ集積・分析

  - 生産設備の各種センサーから，クラウドに常時データ転送（数秒～数十秒に1回＝タスクまたはロット単位で）→単方向通信
  - センサは設備当たり数点～数十点
  - クラウドデータ（分析画面）を，工場外からもアクセス可能（見るだけ）
    →クラウドサーバが踏み台になる可能性あり

ロボットのリモート監視診断の構成



付録 B-セキュリティ脅威リスクアセスメントシート

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
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）			
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			
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			
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
1.1.2.1								パソコンのアップデート不足	ウィルス（感染）			
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）			
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			大	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）			
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）			
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			
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	H社			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			
1.1.4.2								パソコンのアップデート不足	ウィルス（感染）			
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	大	大
1.2.1.1								パソコンのアップデート不足	ウィルス（感染）			
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			
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）			
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）			

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	大	大
1.2.2.1								パソコンのアップデート不足	ウィルス（感染）			
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）			
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			
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			
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			大	大	大
1.2.3.1								パソコンのアップデート不足	ウィルス（感染）			
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）			
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			
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			
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			
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。	H社			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			
1.2.4.2								パソコンのアップデート不足	ウィルス（感染）			
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			
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			
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。	H社			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			
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）			
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

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）			
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）			
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。	H社			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			
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）			
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			
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			
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			
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
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）			
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）			
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			
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			
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			
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
1.5.1.1								パソコンのアップデート不足	ウィルス（感染）			
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			
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）			
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
1.5.2.1								パソコンのアップデート不足	ウィルス（感染）			
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）			
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			大	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）			
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）			
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			
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。	H社			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			
1.5.4.2								パソコンのアップデート不足	ウィルス（感染）			
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
2.1.1.1								パソコンのアップデート不足	ウィルス（感染）			
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			
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）			
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）			
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			
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
2.1.2.1								パソコンのアップデート不足	ウィルス（感染）			
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）			
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）			
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） バックドア			
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			
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			大	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）			
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）			

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）			
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			
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			
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			
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	H社			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			
2.1.4.2								パソコンのアップデート不足	ウィルス（感染）			
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			
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			
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
2.2.1.1								管理の悪い作業用PC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			
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			
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
2.2.2.1								管理の悪い作業用PC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			
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			
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			
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			大	中	大
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）			
2.2.3.2								管理の悪い作業用PC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			
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			

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			
2.2.4					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。	H社			小	小	小
2.2.4.1								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			
2.2.4.2								停止中工程の作業員からのリモート接続による漏洩	他の工程の作業員			
2.3			部分工程の変更	生産中に、特定の工程の機械制御の設定変更などソフトウェアに関係する修正が発生したケース。IOT機器そのものへの設定変更やエンジニアリング。関係する工程の機械設備の動力源はOFF。他の工程はON。								
2.3.1					可動中工程の生産中断	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
2.3.1.1								パソコンのアップデート不足	ウィルス（感染）			
2.3.1.2								RDT（Remote Desk Top）による遠隔からの不正操作（誤操作）	保守員			
2.3.1.3								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）			
2.3.1.4								IOTデータ収集機器（パソコン等）の管理不足	ウイルス（感染）			
2.3.1.5								管理の悪い作業用PC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			
2.3.1.6								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			
2.3.2					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
2.3.2.1								パソコンのアップデート不足	ウィルス（感染）			
2.3.2.2								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）			
2.3.2.3								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）			
2.3.2.4								IOTデータ収集機器（パソコン等）の管理不足	ウイルス（感染） バックドア			
2.3.2.5								管理の悪い作業用PC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			
2.3.2.6								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			
2.3.2.7								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			
2.3.3					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			大	中	大

2.3.3.1								パソコンのアップデート不足	ウィルス（感染）			
2.3.3.2								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）			
2.3.3.3								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）			
2.3.3.4								管理の悪い作業用PC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			
2.3.3.5								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			
2.3.3.6								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			
2.3.4					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。	H社			小	小	小
2.3.4.1								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			
2.3.4.2								パソコンのアップデート不足	ウィルス（感染）			
2.3.4.3								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			
2.3.4.4								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			
2.3.4.5								停止中工程の作業員からのリモート接続による漏洩	他の工程の作業員			
2.4			全工程の停止と変更	全工程を停止し、工程の組み換えや機械の入替え、設定変更などを行い、生産プロセス全体に亘る変更を行う。全設備の動力源はOFF。								
2.4.1					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。	H社			小	小	小
2.4.1.1								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			
2.4.1.2								パソコンのアップデート不足	ウィルス（感染）			
2.4.1.3								IOTデータ収集機器（パソコン等）の管理不足	ウイルス（感染） バックドア			
2.4.1.4								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			
2.4.1.5								リモート接続	作業員			
2.4.1.6								不正な機器接続	作業員			
2.4.1.7								不要になった機器の廃棄処理の不徹底	処分業者			

付録 C-作業委託報告書（議事録等を含む）

平成 30 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

平成 31 年 2 月

株 式 会 社　三 菱 総 合 研 究 所

目　次

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。

- 研究部会の議論のための調査と資料作成
- 研究部会での議論を整理した議事録案作成

2. 研究部会の開催

本調査研究の目的を達成するために、機械安全および設備安全に関する有識者から構成される情報通信技術（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）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 平成 30 年 7 月 13 日
- 第 2 回 平成 30 年 8 月 31 日
- 第 3 回 平成 30 年 10 月 30 日
- 第 4 回 平成 30 年 12 月 17 日
- 第 5 回 平成 31 年 2 月 4 日
- 第 6 回 平成 31 年 3 月 11 日

3. 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
- IoT 技術事例調査

作成した資料を、付録 A に示す。

4. 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 B に示す。

付　録

A 研究部会資料

B 議事録

A 研究部会資料

A-1 第 1 回研究部会用資料

A-2 第 2 回研究部会用資料

A-3 第 3 回研究部会用資料

A-4 IoT 技術事例調査

平成３０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

2018年7月13日

1. 平成29年度の検討成果確認

「**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**」として、以下の3項目に整理した。

	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
1-1	セキュリティの脅威は機械安全におけるハザードを生じる新たな因子
1-2	セキュリティの脅威から生じるハザードは「偶発的」ハザードであり、確実に発生するものと考える
1-3	セキュリティの脅威への最終的な対策は「停止」

今後の検討事項として、以下の2項目を示した。

	今後の検討事項
2-1	設計・構築・運用の各段階における要件の明確化
2-2	ガイドラインの作成検討

2. 今年度の検討の進め方

1）設計・構築・運用の各段階での要件の明確化

- 機　安全技術者の視点から、要件を整理することが必要。
- 具体的な生産システムのモデルを対象とした検討が有効。（ケーススタディ）
- 検討にあたっては、具体的なICT利用のパターンを想定。
  - 生産効率の向上
  - 遠　地からの管理
  - 受注・生産・在庫の状況をリアルタイムで　握し生産管理を最適化
  - 予知保全の実現
- 検討の切り口として「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-」を参
  。

2）ガイドライン作成検討におけるポイント

- ガイドライン使用者の想定。
  - オペレーター、生産管理、生産技術
  - インテグレーター、生産システムの設計者、機　の設計者
  - 情報システムの関係者
- 機　安全国際標準の考え方を基本とする。
  - ハザードを　出した後にリスクアセスメントでリスクを　握
  - セキュリティの　：　はハザードとして考慮
- 最終的な対策は機　の「停止」
  - セキュリティの　：　が発見された際に自動的に「停止」は可能か
  - 限定的な運転の継続は許さないのか
  - セキュリティの　：　の排除の方法および体制等については、　存のガイドラインを参考に

3. 研究部会の成果のイメージ [昨年度研究部会資料再掲]

研究部会における検討（２年間）の成果をどのように形にするか、具体的なイメージ（目標）の検討が必要。

- 具体的なイメージを持つことで、目的を明確に共有しやすくなり、検討の活性化が期待される。
- 以下にイメージの例を示す。特に順番に実施するものでものなく、これらにこだわるものでもない。

A 問題点リスト	■ 現状で考えられる問題点をリストアップ ■ 業界に向けた注意換気	■ 工場の生産システムにICT等を利用することによるメリットを提示 ■ ICT等の利用により発生が考えられる　：　等について解説 ■　：　へ対応するために参考とすべき情報をリストアップ
B Q&Aリスト	■ ICT等の利用に関するQ&Aリスト ■ 国内製造事業者向け	■ 現状において、ICT等の利用により発生する可能性がある問題点をリストアップ ■ 製造事業者の立場のQuestionに対するAnswerを作成（以下、例） ■ 生産設備をネットで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？
C ガイドライン	■ ICT等利用の際のチェックリスト ■ ICT等利用時の注意点を読み物に	■ 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 ■ 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、導入方法、安全性対策、運用課題等を、読み物として作成（書籍化）
D 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事故宣言する活動の推進 ■ 自己宣言のための要件を公表するとともに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

7. 参考資料

- 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、内閣サイバーセキュリティセンター、平成28年8月26日
  https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf
- IPA　がる世界の開発指針　第２版
  https://www.ipa.go.jp/sec/publish/tn16-002.html
- 制御システムのセキュリティリスク分　ガイド ～セキュリティ対策におけるリスク分　実施のススメ～
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
- 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）（ケーススタディ編）
  https://www.ipa.go.jp/sec/reports/20180319.html
- EU・ドイツにおけるIoT製品にかかるサイバーセキュリティ規制の動向
  https://ec.europa.eu/digital-single-market/en/policies/cybersecurity
  VDMA Cybersecurity integrated part of a Single European Market
- Platform Industrie(PI) 4.0におけるセキュリティの考え方
  http://www.vdmashop.de/refs/Leitf_I40_Security_En_LR_neu.pdf
  INDUSTRIE 4.0 SECURITY GUIDELINES
  https://ec.europa.eu/futurium/en/system/files/ged/a3-jochem-platform_industrie_4.0_security_of_networked_systems.pdf
  IT security in Industrie 4.0 First steps towards secure production_GUIDELINE
  Industrie 4.0 Security Guidelines Recommendations for actions
  IT Security in Industrie 4.0 Action fields for operators
- 米国におけるサイバーセキュリティ政策
  NIST SP800-171
  DFARS Clause252.204-7012
- NIST SP800-30 Risk Management Guide for Information Technology Systems
  https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01

<参考-1> 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）

- Step0 安全設計経緯の確認
  - 0-1 検討システムの事業上のリスクを確認
  - 0-2 検討システムの概要を確認
- Step1 事業者のセキュリティ検討
  - 1-1 セキュリティ方針・計画の策定、SuC（System under Consideration）識別
  - 1-2 セキュリティリスク分析
  - 1-3 セーフティへの影響確認
- Step2 インテグレーターのセキュリティ検討
  - 2-1 事業者からの要求事項の確認
  - 2-2 セキュリティリスク分析
  - 2-3 リスク評価
- Step3 セキュリティ対策の立案と残存リスク評価
  - 3-1 セキュリティ対策の立案
  - 3-2 セーフティへの影響確認
- Step4 全妥当性確認
- Step5 運用・保守・修理

＜参考-1＞ 日機連 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

ISO 11161に基づく統合生産システム（以下、生産システム）の安全設計プロセス

1. 生産システムの安全要求事項の確認	● 安全要求事項の確認するとともに、適用する規格を確認する。
2. 生産する製品の仕様と製造条件の決定	● 製造する製品の形状、材質、構造などの製品仕様および生産量を決定する。 ● 製造ライン仕様書（ユーザー要求）の作成
3. 工程分析 3..1 初期工程分析－空間設計	● 材料から製品までの製造工程を分析し、必要設備を決定する。 ● 各工程での生産財、製造設備（単体機械）の必要機械性能・仕様（ユーティリティを含む）を決定する。 ● 各設備における大まかな人の配置を決定する。
3..2 中期工程分析－ライン構想	● 各工程での定常作業・非定常作業を検討する。 ● 各設備（単体機械）における段取・設定・調整・生産作業内容の定常作業手順を決定する。 ● 段取時、トラブル処理などの非定常作業での人の介入を洗い出す。
3..3 後期工程分析－危険源同定その1	● 機械機能とレイアウトが決定した段階での、単体機械、コンポーネント、それらの組み合わせによる危険源を同定する。
4. リスクアセスメント	● 機械機能とレイアウトが決定した段階でのリスクアセスメントを行い、リスク低減方策を決定する。
5. 作業分析と作業ゾーンの切り分け	● 各機械設備に対して各作業者がどのような作業に関わるかを決定する。 ● 決定した作業にしたがい機械設備全体を作業ごとのゾーンに切り分ける。 ● 全作業ゾーンにおいて、各作業者と各作業のかかわりを整理し、ゾーン間の関連を洗い出す。
6. 作業ゾーンにおける危険源同定 その2	● 各作業ゾーンを通過して別の作業ゾーンへの人および設備の侵入を考慮した場合の危険源同定を行う。
7. 生産システムのリスクアセスメント	● 全体のリスクアセスメントとリスク低減方策を決定する。
8. 安全機能の制御範囲の決定（各運転モード）	● 全体のリスクアセスメントの結果に基づくリスク低減方策（モード・インターロック・非常停止等）の西予範囲を決定、整理する。
9. 生産システムの妥当性確認（リスクアセスメント）	● 生産システムを構築した際の各設備の保護法策の改造、追加の保護方策の妥当性確認を実施する。 ● 生産システムの安全戦略の妥当性確認の技術ファイルを作成し、保管する。
10. 生産システムの運用	

＜参考-2＞ 生産システム構築の観点からみたセキュリティ要件

生産システムの安全設計プロセス	IPA　がる世界の開発指針　第２版
1. 生産システムの安全要求事項の確認	[指針1]安全安心の基本方針を策定する [指針2]安全安心のための体制・人材を見直す [指針3]内部不正やミスに備える
2. 生産する製品の仕様と製造条件の決定	[指針4]守るべきものを特定する
3. 工程分析 3..1 初期工程分析－空間設計 3..2 中期工程分析－ライン構想 3..3 後期工程分析－危険源同定その1	[指針5]つながることによるリスクを想定する [指針6]つながりで波及するリスクを想定する [指針7]物理的なリスクを認識する
4. リスクアセスメント	[指針8]個々でも全体でも守れる設計をする
5. 作業分析と作業ゾーンの切り分け	[指針9]繋がる相手に迷惑をかけない設計をする
6. 作業ゾーンにおける危険源同定 その2 7. 生産システムのリスクアセスメント	[指針10]安全安心を実現する設計の整合性をとる [指針11]不特定の相手とつなげられても安全安心を確保できる設計をする
8. 安全機能の制御範囲の決定（各運転モード）	
9. 生産システムの妥当性確認（リスクアセスメント）	[指針12]安全安心を実現する設計の検証・評価を行う
10. 生産システムの運用	[指針13]自身がどのような状態かを把握し、記録する機能を設ける [指針14]時間が経っても安全安心を維持する機能を設ける [指針15]出荷後もIoTリスクを把握し、情報発信する [指針16]出荷後の関係事業者に守ってもらいたいことを伝える [指針17]つながることによるリスクを一般利用者に知ってもらう

<参考-3> 生産システム構築の観点からみたセキュリティ要件

生産システムの安全設計プロセス	INDUSTRIE 4.0 SECURITY GUIDELINES
1. 生産システムの安全要求事項の確認	15. Determining security requirements for vendors and suppliers ベンダおよびサプライヤのセキュリティ要件の決定 17. Developer training on security セキュリティに関する開発者トレーニング
2. 生産する製品の仕様と製造条件の決定	
3. 工程分析 3..1 初期工程分析－空間設計 3..2 中期工程分析－ライン構想 3..3 後期工程分析－危険源同定その1	4. Using secure protocols 安全なプロトコルの使用 5. Safeguarding wireless technologies ワイヤレス技術の保護 6. Secure remote service 安全なリモートサービス 14. Cryptography 暗号化
4. リスクアセスメント	1. Risk analysis リスクアナリシス 10. Adapting and testing components コンポーネントの適合とテスト 11. Foregoing unnecessary component functions 不要なコンポーネントの機能 12. Component hardening コンポーネント強化
5. 作業分析と作業ゾーンの切り分け	2. Network segmentation ネットワークセグメンテーション 3. User accounts, credentials, authentication and authorization ユーザーアカウント、資格情報、認証と承認
6. 作業ゾーンにおける危険源同定 その2	13. Isolation techniques within the machine/virtualization マシン/仮想化における分離テクニック
7. 生産システムのリスクアセスメント	1. Risk analysis リスクアナリシス
8. 安全機能の制御範囲の決定（各運転モード）	
9. 生産システムの妥当性確認（リスクアセスメント）	1. Risk analysis リスクアナリシス 16. Documentation ドキュメンテーション
10. 生産システムの運用	7. Monitoring and recognizing attacks 攻撃の監視と認識 8. Recovery plan 復旧計画 9. Secure product lifecycle 製品ライフサイクルの確保

9

平成３０年度 ICT等を利用した安全確保に関する調査検討
第2回研究部会用資料

2018年8月31日

1. 第1回研究部会の議論

① 今年度の方針

- 昨年度提案の研究部会の成果イメージについて　ね合意を得た。
  - 想定するシステム・使用者毎に類型化したガイドラインの作成
  - 　もが理解しやすいフレーズを使用した業界宣言

② セキュリティの脅威の検知から安全確保のあり方の検討方針（以下、ご意見）

- 異常検知から対応（復旧）までのプロセスを検討対象とするか。
- サプライチェーン上の様々な主体の連携を前提とした検討が必要ではないか。
- 具体的なケーススタディの作成が必要ではないか。

③ ICT等の活用によるサービス、事業環境の変化

- 各ステークホルダーが担うべき責任　囲、検討対象とするリスクの　囲の明確化
- IoT等の先進技術活用したプレイヤーが拡大している現状　握の必要性

④ 生産システムにおけるセキュリティの脅威の考え方（以下、ご意見）

- 保護対象は性能、機能、データと多　に渡るため、保護対象の検討から開始すべき。
- 機能安全により安全性が担保されている状況がサイバーアタックによって破られるという考え方はどうか。
- 設計段階から、セキュリティ・安全の対策の両輪での検討が必要であることを前提とすべき。

2. 事例の共有

- 第一回研究部会で依頼した「ICT事例　介フォーム」に基づき各社の推進する事例を共有する。
- 今回集約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　」～「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　握
  - 企業横並びに比　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　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

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	

3. 本検討部会（8/31）の論点

本検討部会において議論すべき点を示す。

①　研究部会の成果

- 本検討部会の成果（次　参　）について具体的にゴールとなるイメージの共有・確定

②　成果の要件

- 作成する成果物に含むべき事項の検討

（例）ガイドライン

- 設計段階で本質的に実施すべき事項の整理
- 設計段階から制御が破　したとき（セキュリティ起因）の想定すべき状況　等

③　安全確保のあり方　※本日共有した事例に基づき検討

- 踏まえるべき事業環境・サービスの変化
- 具体的なケーススタディの選定
- 安全確保の検討対象・　囲の特定
  - サプライチェーン上の主体のだれを、異常検知から対応までのどこまでを検討するか　等
- セキュリティの　：　により想定すべき発生事象

（再掲）研究部会の成果のイメージ

研究部会における検討（２年間）の成果をどのように形にするか、具体的なイメージ（目標）の検討が必要。

- 具体的なイメージを持つことで、目的を明確に共有しやすくなり、検討の活性化が期待される。
- 以下にイメージの例を示す。特に順番に実施するものでものなく、これらにこだわるものでもない。

A 問題点リスト	■ 現状で考えられる問題点をリストアップ ■ 業界に向けた注意換気	■ 工場の生産システムにICT等を利用することによるメリットを提示 ■ ICT等の利用により発生が考えられる ： 等について解説 ■ ： へ対応するために参考とすべき情報をリストアップ
B Q&Aリスト	■ ICT等の利用に関するQ&Aリスト ■ 国内製造事業者向け	■ 現状において、ICT等の利用により発生する可能性がある問題点をリストアップ ■ 製造事業者の立場のQuestionに対するAnswerを作成（以下、例） 　■ 生産設備をネットで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？
C ガイドライン	■ ICT等利用の際のチェックリスト ■ ICT等利用時の注意点を読み物に	■ 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 ■ 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、導入方法、安全性対策、運用課題等を、読み物として作成（書籍化）
D 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事故宣言する活動の推進 ■ 自己宣言のための要件を公表するとともに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

平成３０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

ガイドラインの構成案

2018年10月30日

ガイドラインの基本構成

1.	まえがき	生産システムとICTについて
2.	ICT利用の目的	ICT利用の目的とメリットについて
3.	セキュリティの脅威による被害	生産システムにおいて、どのような被害が想定されるか
4.	セキュリティリスク分析の方法	セキュリティリスク分析に関して、参考資料の内容を紹介
5.	セキュリティの脅威に対する基本的考え方	機械安全の立場からセキュリティの脅威に対する基本的な考え方とは
6.	統合生産システムへの適用検討	ISO 11161に基づく統合生産システムの安全設計プロセスへの適用を検討 - エネルギーを持つシステムの安全確保の対策として検討すべき項目を整理
7.	あとがき	ICT活用の心構え
付録	参考文献	

ガイドラインの内容

2. ICT利用の目的

●ICT利用の目的と期待されるメリットについて

- 生産効率の向上
- 遠隔地からの管理・操業
- 受注・生産・在庫の状況をリアルタイムで把握し生産管理を最適化
- 予知保全の実現（性能劣化の監視、停止前の部品交換）
- 品質の履歴管理
- ヒューマンエラーの撲滅（RFIDによる工程管理と連携）
- 生産量の計画と実績をリアルタイムで見える化
- 稼働率低下の原因対策と対応
- エネルギー消費量の見える化

ガイドラインの内容

3. セキュリティの脅威による被害

●生産システムにおいてセキュリティの脅威により、どのような被害が想定されるかを、具体的に示す。セキュリティリスク分析を行うための参考とする。

- 制御パラメーター（ロボット、搬送システム等）の変更による暴走発生
- 悪意による遠隔操作
- 実績データの改ざんによる生産性低下・ライン停止
- 意図せぬ機械動作による挟まれ・巻き込まれ

脅威の識別 （脅威の観点例）

■セキュリティ脅威を導き出す際の観点例を以下に示します。

通信妨害		
	輻輳	DoS攻撃
	遮断	物理的に切断（ケーブル切断）
	電波妨害	遮蔽物設置、同一周波数帯使用し通信妨害
不正アクセス		
	盗聴	情報が傍受・窃取され盗用、悪用される
	情報窃取	ID/PW情報、データ、設定情報等窃取
	機能・サービスの低下、停止	情報の書換、削除等により機能が低下・停止
改ざん		
	不正データ設定	不正なシステム設定値に変更される
	不正コマンド・メッセージ発行	正しくないコマンド、メッセージを送信し不正動作をさせる
	ログ消去・喪失	操作履歴を消去、改ざんし追跡不能状態にする
脆弱性利用		
	脆弱性露見	脆弱性を悪用される
	不正中継	悪意のあるアクセスの踏み台として利用される
物理的脅威		
	盗難・紛失	機器、装置が盗み出される
	破壊	機器、装置が破壊され動作不能になる
	保守・廃棄時の窃取	保守作業、廃棄時に機器から不正に情報を取出す
誤操作		
	誤操作、・設定	操作者の誤った操作、設定による脅威の発現
ウィルス感染		
	ウィルス感染	ウィルス感染した機器、記憶媒体により感染する脅威

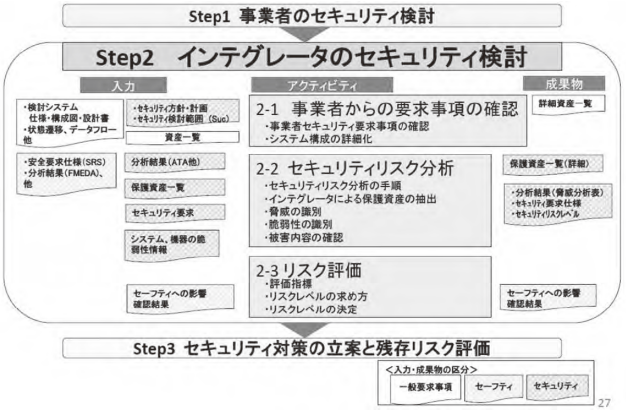
IPA：制御システム セーフティ・セキュリティ要件検討ガイド –ケーススタディ編- P.36

ガイドラインの内容

4. セキュリティリスク分析の方法

●セキュリティとセーフティの関係を踏まえ体系的な整理を行ったうえで、セキュリティリスク分析の方法として、参考資料の内容を紹介

- 事業者による資産明確化
- ZC（ゾーン・コンジット）分析
- 保護資産の抽出
- 影響度・発生可能性評価
- セキュリティ要求の抽出
- インテグレーターによる保護資産の抽出
- 脅威の識別
- 脆弱性の識別
- 被害内容の確認



引用元：IPA：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- P.16（左） P.27（右）

ガイドラインの内容

5. セキュリティの脅威に対する基本的考え方

●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」を示す。（引用元：平成29 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）

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	
1-1	セキュリティの脅威は機械安全におけるハザードを生じる新たな因子
1-2	セキュリティの脅威から生じるハザードは「偶発的」ハザードであり、確実に発生するものと考える
1-3	セキュリティの脅威への最終的な対策は「停止」

- ISO 12100 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。セキュリティの脅威への対策の検討を進めるにあたっても、機械安全の対策と一体となって取り組んでいくためには、リスクアセスメントの中で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、危害の重要度と発生確率の組み合わせとして、リスクを定義している。セキュリティの脅威については、リスクアセスメントにおいて、偶発的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思われる。ただし、セキュリティの脅威から生じるハザードは、従来とは異なり「悪意」という特徴を有している。セキュリティの脅威には、何かしらの「悪意」が存在し、その「意図」を持って近づいてくるという点が大きな特徴である。その特徴のために、対策として何を考えなければならないのかは、今後、検討していくことが求められる。
- ハザードとしてセキュリティの脅威を考えたならば、リスクアセスメントの次の段階としては、そのハザードのリスクを求めることになる。リスクは危害の程度と発生確率の組み合わせで求めるが、危害の程度については、セキュリティの脅威により、何が発生するかを想定し、推定することができる。一方、発生確率に関しては、部品の劣化や磨耗等に起因する偶発的なハザードのように確率で表現できるものではなく、確実に発生するものと考えて、その脅威に応じて発生する被害の程度を見積もることが適切と考えられる。従って、セキュリティの脅威から生じるハザードの発生確率に関しては、常に「100%」と考えることが安全側の思考方法として適切であるといえる。
- 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、セキュリティの脅威に関しては、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、侵入した脅威が威力を発揮することを100%防ぐことはできない。セキュリティの脅威からシステムを防御する物理的なカバーは存在しないためである。そのため、セキュリティの脅威への対策は、いかに早く発見し、迅速に確実にシステムを停止するかにつきると考えられる。また、停止するための方法としては、ソフトウェアによる制御から独立した状態のセキュリティの脅威の影響を受けないハードウェアによる方策を用いることが望ましいと考えられる。

ガイドラインの内容

日機連 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

6. 統合生産システムへの適用検討

ISO 11161に基づく統合生産システム（以下、生産システム）の安全設計プロセス

1. 生産システムの安全要求事項の確認	● 安全要求事項の確認するとともに、適用する規格を確認する。
2. 生産する製品の仕様と製造条件の決定	● 製造する製品の形状、材質、構造などの製品仕様および生産量を決定する。 ● 製造ライン仕様書（ユーザー要求）の作成
3. 工程分析 3..1 初期工程分析－空間設計	● 材料から製品までの製造工程を分析し、必要設備を決定する。 ● 各工程での生産財、製造設備（単体機械）の必要機械性能・仕様（ユーティリティを含む）を決定する。 ● 各設備における大まかな人の配置を決定する。
3..2 中期工程分析－ライン構想	● 各工程での定常作業・非定常作業を検討する。 ● 各設備（単体機械）における段取・設定・調整・生産作業内容の定常作業手順を決定する。 ● 段取時、トラブル処理などの非定常作業での人の介入を洗い出す。
3..3 後期工程分析－危険源同定その1	● 機械機能とレイアウトが決定した段階での、単体機械、コンポーネント、それらの組み合わせによる危険源を同定する。
4. リスクアセスメント	● 機械機能とレイアウトが決定した段階でのリスクアセスメントを行い、リスク低減方策を決定する。
5. 作業分析と作業ゾーンの切り分け	● 各機械設備に対して各作業者がどのような作業に関わるかを決定する。 ● 決定した作業にしたがい機械設備全体を作業ごとのゾーンに切り分ける。 ● 全作業ゾーンにおいて、各作業者と各作業のかかわりを整理し、ゾーン間の関連を洗い出す。
6. 作業ゾーンにおける危険源同定 その2	● 各作業ゾーンを通過して別の作業ゾーンへの人および設備の侵入を考慮した場合の危険源同定を行う。
7. 生産システムのリスクアセスメント	● 全体のリスクアセスメントとリスク低減方策を決定する。
8. 安全機能の制御範囲の決定（各運転モード）	● 全体のリスクアセスメントの結果に基づくリスク低減方策（モード・インターロック・非常停止等）の制御範囲を決定、整理する。
9. 生産システムの妥当性確認（リスクアセスメント）	● 生産システムを構築した際の各設備の保護法策の改造、追加の保護方策の妥当性確認を実施する。 ● 生産システムの安全戦略の妥当性確認の技術ファイルを作成し、保管する。
10. 生産システムの運用	

6. 統合生産システムへの適用検討

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）

- Step0 安全設計経緯の確認
  - 0-1 検討システムの事業上のリスクを確認
  - 0-2 検討システムの概要を確認
- Step1 事業者のセキュリティ検討
  - 1-1 セキュリティ方針・計画の策定、SuC（System under Consideration）識別
  - 1-2 セキュリティリスク分析
  - 1-3 セーフティへの影響確認
- Step2 インテグレーターのセキュリティ検討
  - 2-1 事業者からの要求事項の確認
  - 2-2 セキュリティリスク分析
  - 2-3 リスク評価
- Step3 セキュリティ対策の立案と残存リスク評価
  - 3-1 セキュリティ対策の立案
  - 3-2 セーフティへの影響確認
- Step4 全妥当性確認
- Step5 運用・保守・修理

ガイドラインの内容

6. 統合生産システムへの適用検討

●エネルギーを持つシステムの安全確保の対策として検討すべき項目の整理

- 他分野も含めた事例調査を行い、生産ラインに適用した場合に機能的に機械に持たせるべき仕組みを検討し、技術的に検討しなければならない項目を整理する。

用途・目的		説明	対策例
防御	初期侵入段階	攻撃の最上流（初期段階）における、外部との接続点を介したネットワーク経由の攻撃、あるいはシステム（サーバ・操作端末・機器等）設置場所への攻撃者の物理的侵入を防止する目的で実装される対策。 また、攻撃者（内部犯行者を含む）による、システム（サーバ・操作端末・機器等）への不正ログイン等を防止する目的で実装される対策。	ファイアウォール（FW）、IPS、 アンチウイルス、 パッチ適用、脆弱性回避、 通信相手の認証、操作者認証、 入退管理
	内部侵攻・拡散段階	システム（サーバ・操作端末・機器等）への侵入を果たした攻撃者（人間あるいは不正プログラム）による、内部の情報収集や侵入範囲拡大（侵入したシステム内部での拡大及び他のシステムへの拡散）を防止する目的で実装される対策。	セグメント分割／ゾーニング、 APT対策ツール、 アクセス制御、 ホワイトリストによるプロセスの起動制限
	目的遂行段階	「情報窃取」「データ改ざん」「制御乗っ取り」「システム破壊」等、攻撃者による最終目的の実現を防止する目的で実装される対策	重要操作の承認、 データ暗号化、データ署名、 フェールセーフ設計
検知		攻撃の実施、あるいは攻撃の成功による被害の発生を早期に検知することを目的に実装される対策。	IDS、アンチウイルス、APT対策ツール、 統合ログ管理システム、 機器異常検知、機器死活監視、 入退管理、侵入センサ
被害把握		攻撃の成功による被害や影響範囲の把握を目的に実装される対策。あるいは、監査における証跡提示のため、攻撃内容の詳細の把握等を目的に実装される対策	ログ収集・分析、 統合ログ管理システム
事業継続		攻撃の成功による被害を最小限に留めるために実装される対策。あるいは、サービスの継続、被害の早期復旧を実現することを目的に実装される対策	データバックアップ、冗長化、 暗号鍵更新、 フェールセーフ設計

IPA：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- P.49

6. 統合生産システムへの適用検討

生産システムの安全設計プロセス	制御システム セーフティ・セキュリティ要件検討ガイド
1. 生産システムの安全要求事項の確認	Step0 安全設計経緯の確認 0-1 検討システムの事業上のリスクを確認 ● 事業リスクの確認 ● 安全基本方針の確認
2. 生産する製品の仕様と製造条件の決定	Step1 事業者のセキュリティ検討 1-1 セキュリティ方針・計画の策定、SuC識別 0-2 検討システムの概要を確認 ● 概要 ● 関係者 ● ライフサイクル ● 安全対策の経緯 ● デフォルトのセキュリティ機能
3. 工程分析 3..1 初期工程分析－空間設計 3..2 中期工程分析－ライン構想 3..3 後期工程分析－危険源同定その1	1-2 セキュリティリスク分析 ● 事業者による資産明確化 ● ZC（ゾーン・コンジット）分割 ● 保護資産の抽出 ● 影響度・発生可能性評価 ● セキュリティ要求の抽出 1-3 セーフティへの影響確認 Step2 インテグレーターのセキュリティ検討
4. リスクアセスメント	2-1 事業者からの要求事項の確認 ● 事業者セキュリティ要求事項の確認 ● システム構成の詳細化
5. 作業分析と作業ゾーンの切り分け	2-2 セキュリティリスク分析 ● インテグレーターによる保護資産の抽出 ● 脅威の識別 ● 脆弱性の識別 ● 被害内容の確認
6. 作業ゾーンにおける危険源同定 その2 7. 生産システムのリスクアセスメント	Step3 セキュリティ対策の立案と残存リスク評価 3-1 セキュリティ対策の立案 ● 対策立案と残存リスク評価 2-3 リスク評価 ● 評価指標 ● リスクレベルの求め方 ● リスクレベルの決定
8. 安全機能の制御範囲の決定（各運転モード）	3-2 セーフティへの影響確認 ● 確認事項 ● 影響有無の確認
9. 生産システムの妥当性確認（リスクアセスメント）	Step4 全妥当性確認
10. 生産システムの運用	Step5 運用・保守・修理

研究部会の成果のイメージ [昨年度研究部会資料再掲]

研究部会における検討（２年間）の成果をどのように形にするか、具体的なイメージ（目標）の検討が必要。

- 具体的なイメージを持つことで、目的を明確に共有しやすくなり、検討の活性化が期待される。
- 以下にイメージの例を示す。特に順番に実施するものでものなく、これらにこだわるものでもない。

A 問題点リスト	■ 現状で考えられる問題点をリストアップ ■ 業界に向けた注意換気	■ 工場の生産システムにICT等を利用することによるメリットを提示 ■ ICT等の利用により発生が考えられる脅威等について解説 ■ 脅威へ対応するために参考とすべき情報をリストアップ
B Q&Aリスト	■ ICT等の利用に関するQ&Aリスト ■ 国内製造事業者向け	■ 現状において、ICT等の利用により発生する可能性がある問題点をリストアップ ■ 製造事業者の立場のQuestionに対するAnswerを作成（以下、例） 　■ 生産設備をネットで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？
C ガイドライン	■ ICT等利用の際のチェックリスト ■ ICT等利用時の注意点を読み物に	■ 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 ■ 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、導入方法、安全性対策、運用課題等を、読み物として作成（書籍化）
D 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事故宣言する活動の推進 ■ 自己宣言のための要件を公表するとともに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

参考資料

- 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、内閣サイバーセキュリティセンター、平成28年8月26日
  https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf
- IPA 繋がる世界の開発指針　第２版
  https://www.ipa.go.jp/sec/publish/tn16-002.html
- 制御システムのセキュリティリスク分析ガイド ～セキュリティ対策におけるリスク分析実施のススメ～
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
- 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）（ケーススタディ編）
  https://www.ipa.go.jp/sec/reports/20180319.html
- EU・ドイツにおけるIoT製品にかかるサイバーセキュリティ規制の動向
  https://ec.europa.eu/digital-single-market/en/policies/cybersecurity
  VDMA Cybersecurity integrated part of a Single European Market
- Platform Industrie(PI) 4.0におけるセキュリティの考え方
  http://www.vdmashop.de/refs/Leitf_I40_Security_En_LR_neu.pdf
  INDUSTRIE 4.0 SECURITY GUIDELINES
  https://ec.europa.eu/futurium/en/system/files/ged/a3-jochem-platform_industrie_4.0_security_of_networked_systems.pdf
  IT security in Industrie 4.0 First steps towards secure production_GUIDELINE
  Industrie 4.0 Security Guidelines Recommendations for actions
  IT Security in Industrie 4.0 Action fields for operators
- 米国におけるサイバーセキュリティ政策
  NIST SP800-171
  DFARS Clause252.204-7012
- NIST SP800-30 Risk Management Guide for Information Technology Systems
  https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01

<参考-1> 生産システム構築の観点からみたセキュリティ要件

生産システムの安全設計プロセス	IPA 繋がる世界の開発指針　第２版
1. 生産システムの安全要求事項の確認	[指針1]安全安心の基本方針を策定する [指針2]安全安心のための体制・人材を見直す [指針3]内部不正やミスに備える
2. 生産する製品の仕様と製造条件の決定	[指針4]守るべきものを特定する
3. 工程分析 3..1 初期工程分析－空間設計 3..2 中期工程分析－ライン構想 3..3 後期工程分析－危険源同定その1	[指針5]つながることによるリスクを想定する [指針6]つながりで波及するリスクを想定する [指針7]物理的なリスクを認識する
4. リスクアセスメント	[指針8]個々でも全体でも守れる設計をする
5. 作業分析と作業ゾーンの切り分け	[指針9]繋がる相手に迷惑をかけない設計をする
6. 作業ゾーンにおける危険源同定 その2 7. 生産システムのリスクアセスメント	[指針10]安全安心を実現する設計の整合性をとる [指針11]不特定の相手とつなげられても安全安心を確保できる設計をする
8. 安全機能の制御範囲の決定（各運転モード）	
9. 生産システムの妥当性確認（リスクアセスメント）	[指針12]安全安心を実現する設計の検証・評価を行う
10. 生産システムの運用	[指針13]自身がどのような状態かを把握し、記録する機能を設ける [指針14]時間が経っても安全安心を維持する機能を設ける [指針15]出荷後もIoTリスクを把握し、情報発信する [指針16]出荷後の関係事業者に守ってもらいたいことを伝える [指針17]つながることによるリスクを一般利用者に知ってもらう

<参考-2> 生産システム構築の観点からみたセキュリティ要件

生産システムの安全設計プロセス	INDUSTRIE 4.0 SECURITY GUIDELINES
1. 生産システムの安全要求事項の確認	15. Determining security requirements for vendors and suppliers ベンダおよびサプライヤのセキュリティ要件の決定 17. Developer training on security セキュリティに関する開発者トレーニング
2. 生産する製品の仕様と製造条件の決定	
3. 工程分析 3..1 初期工程分析－空間設計 3..2 中期工程分析－ライン構想 3..3 後期工程分析－危険源同定その1	4. Using secure protocols 安全なプロトコルの使用 5. Safeguarding wireless technologies ワイヤレス技術の保護 6. Secure remote service 安全なリモートサービス 14. Cryptography 暗号化
4. リスクアセスメント	1. Risk analysis リスクアナリシス 10. Adapting and testing components コンポーネントの適合とテスト 11. Foregoing unnecessary component functions 不要なコンポーネントの機能 12. Component hardening コンポーネント強化
5. 作業分析と作業ゾーンの切り分け	2. Network segmentation ネットワークセグメンテーション 3. User accounts, credentials, authentication and authorization ユーザーアカウント、資格情報、認証と承認
6. 作業ゾーンにおける危険源同定 その2	13. Isolation techniques within the machine/virtualization マシン/仮想化における分離テクニック
7. 生産システムのリスクアセスメント	1. Risk analysis リスクアナリシス
8. 安全機能の制御範囲の決定（各運転モード）	
9. 生産システムの妥当性確認（リスクアセスメント）	1. Risk analysis リスクアナリシス 16. Documentation ドキュメンテーション
10. 生産システムの運用	7. Monitoring and recognizing attacks 攻撃の監視と認識 8. Recovery plan 復旧計画 9. Secure product lifecycle 製品ライフサイクルの確保

IoT技術事例（WEB調査）

2018/12/17 MRI

大分類	中分類	事業者名	技術の名称	技術の概要	参考資料／別添資料／URLなど
状態監視保全技術	センシング	横河電機	配管腐食センサー	配管周囲の磁界を利用して配管の減肉を非接触で計測するセンサのプロトタイプを開発し、顧客プラントで実証実験を実施	https://www.yokogawa.co.jp/about/yokogawa/rd/inv_center/pcm/
		ＮＥＣ	圧電式振動センサ	幅広い周波数帯域の振動を従来比20倍の感度でリアルタイムに収集可能 詳細は、こちらをご確認ください。http://jpn.nec.com/techrep/journal/g12/n02/pdf/120215.pdf	https://premium.ipros.jp/nec-tokin/catalog/detail/327467/
		富士通	「ODMA予兆監視モデルfor光ファイバー温度測定」	光ファイバーを用いて、機器や設備の温度を検知し、トラブルの予兆を把握する。温度の変化を時間的にAI自動監視させることで、高度な自動異常検知が可能となる。ガス漏れや腐食、稼動異常という問題を温度という切り口で高度に大規模に監視する技術。	http://www.fujitsu.com/jp/solutions/business-technology/intelligent-data-services/ba/product/operational-data-management-and-analytics/sing-monitoring-model-for-optical-fiber-temperature-measurement-solution/
		富士通	LPWA対応・電池交換不要の世界最小センサーデバイス	温度センサーで測定した温度に合わせて電波送信のタイミングを制御する技術開発により、電力を効率よく利用することができ、電波送信に必要となる蓄電素子を半減することが可能となっている。 電源確保や電源ケーブル増設が困難な場所でも、本センサーデバイスを置くだけで測定データの取得が可能となるため、IoTシステムの導入や運用管理などをメンテナンスフリーで実現できる。	http://pr.fujitsu.com/jp/news/2017/12/4-1.html
		ＮＥＣ	ＶｏｉｃｅＤｏ音声認識	紙帳票を使っていた工場での製品検査、プラント設備の巡視点検などの業務を、音声認識によるハンズフリー入力や合成音声による作業指示に置き換え、現場作業の正確性/効率を向上する。	https://www.nec-solutioninnovators.co.jp/sl/sitework/ https://jpn.nec.com/techrep/journal/g10/n01/pdf/10
	IoT技術基盤／クラウド技術	東芝	Chip to Cloud(C2C)	各デバイスに組み込まれたエージェントソフトウェアが、クラウドに上げるべきデータか、あるいは現場で処理すべきデータかを機器側で判断し、必要な情報のみをクラウドに送る	http://www.toshiba.co.jp/iot/power/entry/2016/2016_003.htm
		東芝	samrt EDA	さまざまなセンサーやデータソースからデータを収集、デバイス管理・制御、リアルタイムな異常検知をするためのIoT基盤	http://www.toshiba.co.jp/cl/pro/smarteda-cloud/index_j.htm
		三菱電機	スマート制御クラウドサービス	IoT及びM2M技術を利用して、複数の家電製品や産業用機器の遠隔制御、稼働モニタリング、エネルギー管理などを実行できるシステム	http://www.mitsubishielectric.co.jp/business/itsolution/ondemand/diaplanet/index.html
	機械学習技術	ＮＥＣ	RAPID機械学習	高速・軽量な動作を特長とするディープラーニング技術。画像・テキスト・数値データなどを分析可能であり、多種多様な業務に適用できる。	https://jpn.nec.com/ai/analyze/rapid.html?
		ＮＥＣ	異種混合学習技術	多種多様なデータから、簡単に複数のデータのパターンを自動で場合分け。状況に応じた最適な規則性を選択する、NEC独自のアルゴリズム	https://jpn.nec.com/ai/analyze/pattern.html?
		東芝	故障予知・監視フレームワーク	故障発生時期やタイミングを予測、ログデータやセンサデータから故障に至る事象パターンの抽出、リアルタイム監視により業務効率やサービスレベルの向上、事象の順序だけでなく時間間隔も含めた事象パターンの抽出、故障予兆検知ソリューションを手軽に実現	http://www.toshiba.co.jp/cl/pro/bigdatapf/lineup/index_j.htm
	故障予兆診断	ＮＥＣ	インバリアント分析技術	大規模・複雑なシステムに設置された多数のセンサから大量の時系列データを収集・分析し、通常時に存在するセンサ間の不変的な関係性（インバリアント）をモデル化する。	https://jpn.nec.com/ai/analyze/invariant.html?
		IBM	IBM Analyzer for Correlational Data (ANACONDA)	IBMにおける機械学習研究と応用	http://ibisml.org/archive/ibisml010/2012_IBISML-Ide_distribution.pdf センサーデーター分析ソフトを活用した異常検知システム活用法 - 解析エンジン概要とその分析事例 http://classnk-rd.com/pdf/katsudou201211_C1.pdf
		日立	機械故障予兆診断ソリューション	設備から収集したセンサーデータを解析し、設備の「いつもと違う」を検知する。また、過去のセンサーデータや故障履歴情報を解析し、将来の故障時期予測を行う。	http://www.hitachi-power-solutions.com/product-site/predictive/index.html
		NTTコム	不明	NTTコムの深層学習技術を活用して、三井化学のガス製品工場内に設置されたガス濃度センサーの故障検知	http://itpro.nikkeibp.co.jp/atcl/column/14/346926/111000695/?mln
	原因究明・運転ノウハウ蓄積	東芝	ものづくり情報プラットフォーム（Meister DigitalTwin［マイスター デジタルツイ	豊富なものづくりの経験から導き出された汎用的なデータモデルと、社会インフラシステム構築で実績のある統合ビッグデータソリューション(GridDBなど)を活用することにより、製造から運転・保守までのライフサイクルでの多種多様なデータを、高速に関連付け、リアルタイムに蓄積することができる情報プラットフォーム	http://www.toshiba.co.jp/cl/news/news201603_08.htm
	状態監視システム（ソフトウェアパッケージ）	IBM	IBM Predictive Maintenance Quality（PMQ）	工場やビジネスの運用に悪影響を与える可能性のある、資産の信頼性に関するリスクを特定し、管理するための機械学習と分析を運用データに適用する。	平成２６年度石油精製環境分析・情報提供事業 ビッグデータ解析手法による製油所安定操業対策 （T1, T4参照） http://www.meti.go.jp/meti_lib/report/2015fy/00099
		富士通	ヒューマンセントリックエンジン（HCE）	各種センサーから24時間絶えず得た情報をもとに計算を実行し、意味のある情報に変えてクラウドへ送るといった一連の処理において、徹底的な省電力を実現	http://jp.fujitsu.com/solutions/business-technology/iot/download/pdf/iot_whitepaper201411.p
		三浦工業	オンライン・メンテナンス	顧客が使用しているボイラーに埋め込んだセンサーから得られるデータを通信会社の回線を介して収集し、同社のオンラインセンターで職員が画面を見ながら稼働状態を監視して、異常が感知されれば、まずユーザーに電話して対処方法を伝え、それでも無理な場合にはメンテナンス要員が現地に急行する。	http://www.nikkei.com/article/DGXMZO05617390T00C16A8X13000/

大分類	中分類	事業者名	技術の名称	技術の概要	参考資料／別添資料／URLなど
現場作業支援システム	保守支援解析支援	ＮＥＣ	画像認識・超解像技術	カメラを変えずに画像処理によって低解像画像を高解像度化	http://jpn.nec.com/ad/onlinetv/rd/srt_h.html
		富士通	FUJITSU IoT Solution UBIQUITOUSWARE	人や物の状態・状況・周囲の環境をセンシングし、データ提供を行うIoTパッケージ。ユビキタスウェア製品として、バイタルセンシングバンド、ヘッドマウントディスプレイ(8-3)などがある。	http://www.fmworld.net/biz/uware/ http://www.itmedia.co.jp/smartjapan/articles/1605/23/news025.html
		三菱電機	AR技術を活用した設備検査システム	タブレット端末のカメラで変圧設備など検査対象の製品を写すだけで、必要な点検項目を表示。	http://www.nikkei.com/article/DGXMZO03540940T10C16A6X91000/
		CEC	スマートロガー	ウェアラブル端末のスマートウォッチを活用して、工場の労働生産性向上につなげる作業動態分析ソリューション。位置情報や作業者の動作情報をきめ細かく収集・デジタルデータ化することで、顧客は「熟練作業・ノウハウの蓄積」「作業者のバラツキ解消」「ムダのない作業順序や最適な動作」に向けた改善に取り組みやすくなり、生産性向上や不良発	https://iotnews.jp/archives/20644
		日立	高効率生産モデル	膨大なデータを人工知能（ＡＩ）で解析し、最も効率が良い作業方法を導き出す。ＩＣタグやカメラを使って装置や製品だけでなく、ヒトの動きも捉えるのが特徴。すでに電力機器の生産期間半減に成功しており、新システムを社外にも売り込む。	http://www.hitachi.co.jp/New/cnews/month/2016/10/1025.html
	ウェアラブルデバイス	NTTデータ	スマートグラス	産現場で各種機器を利用しているユーザー側の機器オペレーター自身がスマートグラスを装着し、遠隔地にいる機器メーカーの保守サービス員からの指示・サポートだけでメンテナンスを実施する。この取り組みにより、機器メーカー側は保守サービス員を派遣する負担が減り、またユーザー側は現場の機器オペレーターのノウハウレベルに左右されず機器の早期復旧が可能になり、双方メリットを享受出来ることが期待される。	https://www.newson.co.jp/new-information/newsrelease/410-20170703release.html
		富士電機	ウェアラブル型遠隔作業支援パッケージ	遠隔からのビジュアルな指示による作業を実現し、ベテラン技術者視点で作業品質を確保する。点検、修理箇所を遠隔でビジュアルに指示することが可能。	http://www.fujielectric.co.jp/products/service/service_menu/cloud_04.html
		富士通	FUJITSU IoT Solution UBIQUITOUSWARE ヘッドマウントディスプレイ(HMD)	現場作業向けの企業用ヘッドマウントディスプレイ。付属のウェアラブルキーボードや音声コマンドにより、作業マニュアルのページめくりや数値入力、カメラ撮影などの本体操作も可能	http://pr.fujitsu.com/jp/news/2015/05/11-1.html
		NTTコミュニケーションズ	hitoe	着るだけで生体情報の連続計測ができる機能素材。NTTコムが独自開発したクラウドベースの安全管理システムを利用し、熱ストレス推定や疲労推定、リラックス度推定などの分析・通知が低コストで可能	https://zuuonline.com/archives/50715 http://businessnetwork.jp/Detail/tabid/65/artid/4121/Default.aspx
		Google	Google Glass	新型のものは小型化し、他のメガネに取り付けるクリップオンタイプになる模様(新型のものについて、詳細なスペックや価格等は明らかにされていない)	http://japanese.engadget.com/2015/07/30/google-glass-atom/
		VUZIX (ビュージックス)	M100スマートグラス	シースルーではないため、視野が限定されるが、メガネとの併用可能	http://monoist.atmarkit.co.jp/mn/articles/1408/11/news018_3.html
		VUZIX (ビュージックス)	STAR1200XL-D	メガネ型の為AR用機器としての利用が可能。眼鏡との併用が不可能と思われる	http://monoist.atmarkit.co.jp/mn/articles/1408/11/news018_3.html
		セイコーエプソン	MOVERIO(モベリオ) BT-200	メガネ型の為AR用機器としての利用が可能。タッチパッド・バッテリーを外出しして軽量化	http://monoist.atmarkit.co.jp/mn/articles/1408/11/news018_3.html
		東芝	リストバンド型生体センサー	センサーは2週間連続で使用可能で、腕に装着するだけで連続したデータを計測できる。さらに、その日の体調に合わせた作業量の負荷調整などができるよう、個人のライフログデータを現場管理者のタブレットや職場のPCなどに収集・管理・閲覧できるシステムを東芝が開発	http://monoist.atmarkit.co.jp/mn/articles/1509/07/news021.html
		AgX	スマートヘルメット	作業員の健康状態などをスマートフォンやタブレット端末などから確認。脳波、温湿度、加速度センサーなどを備え、取得した情報はクラウド上に送信して解析を行う。結果は「リラックス度合」「集中力」などの単位として、タブレット端末上	http://monoist.atmarkit.co.jp/mn/articles/1601/18/news045.html
		日立	Doctor Cloud／巡回・点検支援システム	現場作業者は、作業ナビゲーションの確認をハンズフリーで行えるとともに、接写可能な点検カメラを活用して見えにくい箇所も撮影・確認できることから、保守・点検・建設作業の効率・安全性向上が図れる。また、国内外の複数拠点間で同時通信が行えることから、遠隔地からの効率的な作業指示を可能にした。	http://www.hitachi-ics.co.jp/product/newsrel/2015-09_doctor.html
		京セラ	スマートグラス遠隔モニタリングシステム	作業者と管理者で映像と音声を共有、管理者の指示などをグラスに表示。 メガソーラーの運用・保守業務での確認作業でトライアル利用を開始。	http://www.kccs.co.jp/special/1504/
		NTT	多種センサを活用した工場内作業者支援	処理基盤一式をWoTエンジンとして提供。 ・工場内でカメラとセンサを連携させた一括監視　・作業者の状況確認や作業支援 ・本社部門、複数工場との情報連携　・ネットサービス、サプライチェーンとの連携	http://www.ntt.co.jp/RD/active/201602/jp/pf/pdf/A-23_j.pdf
	作業支援システム	ＮＥＣ	巡視・保守点検システム SmartMaintenance（スマートメンテナンス）	現場作業者～管理者向け機能がOne packageとなって点検業務全域をサポート	http://jpn.nec.com/engsl/pro/smartmainte/
		新日鉄住金	製造現場の見守りシステム	携帯端末で得た作業者の位置や心拍数、動作などの情報をインターネット上のプラットフォームに蓄積し、現場から離れた管理センターで情報を一元的に把握。データを通じて外部から安全を見守ることで、現場作業員が１人での作業や高所作業をより安全にこなせるようにする。	http://www.japanmetaldaily.com/metal/2016/steel_news_20160707_1.html
		日立	Doctor Cloud／巡回・点検支援システム	現場作業者は、作業ナビゲーションの確認をハンズフリーで行えるとともに、接写可能な点検カメラを活用して見えにくい箇所も撮影・確認できることから、保守・点検・建設作業の効率・安全性向上が図れる。また、国内外の複数拠点間で同時通信が行えることから、遠隔地からの効率的な作業指示を可能にした。	http://www.hitachi-ics.co.jp/product/newsrel/2015-09_doctor.html
		京セラ	スマートグラス遠隔モニタリングシステム	作業者と管理者で映像と音声を共有、管理者の指示などをグラスに表示。 メガソーラーの運用・保守業務での確認作業でトライアル利用を開始。	http://www.kccs.co.jp/special/1504/
	セキュリティ	ＮＥＣ	顔認証技術	顔認識技術を活用した認証により、登録した人間のみが計器室の操作端末にスムーズかつ安全にアクセス可能に	http://jpn.nec.com/biometrics/face/

参考：経済産業省「平成２８年度 IoT推進のための新産業モデル創出基盤整備事業（自主保安高度化に向けた実証事業）」（MRI受託受託欧）

B 議事録

平成30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			作　　成
			三菱総合研究所
開催日時	2018年7月13日(金) 10:00~12:30	開催場所	ステーションコンファレンス東京 402C+D 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(住友重機械工業㈱)、木下(平田機工㈱)、杉田(テュフラインランドジャパン㈱)、杉原(パナソニック㈱)、中村(㈱安川電機)、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	白石(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)、河合、山田((独)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)、首藤、高橋(三菱総合研究所)	

計18名

1．開会

事務局より挨拶を行い、主査、副主査、委員より自己紹介を頂いた。

2．事業概要

事務局の資料1に基づく説明後、以下の議論があった。

今年度の方針

- 生産設備をIoTでインターネットに繋がるということは生産性・安全性の向上が可能となったということを前提とする。【向殿】
- 資料1のP3「2．今年度の検討の進め方」について。「最終的な対策は機械の「停止」」との記載があるが、「復旧」まで含んだ検討をするかどうか認識を合わせるべきである。「復旧」まで考慮する場合は、「PLC にバックアップを策定しておく」などの復旧に関するガイドラインがあると有用なのではないか。【神余】
- 想定するシステム・使用者を特定し類型化を行い、ガイドラインは作成すべきである。【山田】
- 研究部会の成果イメージにある業界宣言を行う場合は、誰もが容易に理解可能なフレーズを使用すべきである。【神余】

セキュリティの脅威の検知から安全確保のあり方の検討方針

- サイバーアタックを受けた際に、すぐにオペレーターが気付くことは現実的に困難である。機器の挙動の異変を検知するアラームは、プレスオートメーションの場合、①オペレーターが対応可能なプロセス異常、②メーカーのみ対応可能なシステムエラーの2つに現状分類される。IoT化を考慮すると、③セキュリティに関するアラームを位置付ける必要がある。【神余】
  - 一方で、③セキュリティに関するアラームがオペレーターに検知されたとしても、セキ

ュリティの知見がないため対応は困難である。異変検知から対応までのプロセスに沿った教育が必要である。【神余】

- プロセスプラントの場合、相互インターロックがある。インターロックを含めた設計を行うことは設備信頼性にメーカーが責任を持つということを意味し、設計段階からプラント技術者とインターロック技術者の間の調整が必要となる。ファクトリーオートメーションも同じ状況となると考えている。【森本】
  - 制御システム全体の仕組みを整理する必要がある。【畑】
- 安全確保とは、「停止」と「隔離」を確立し、危険源を取り去ることである。また、周囲にその機器がサイバー攻撃を受けた状態であることを周知することも重要な対応の一つである。【杉原】
- 自社ではインターネットに設備を繋ぐ際のリスク等を検討することを規定するルールはない。現在、この類の事故は未発生だがリスクは認識する必要があり、具体的なケーススタディの作成は必要だと考えている。【石川】
  - 機器をインターネットに繋ぐ際には、性能を検討する必要がある。本委員会の議題としても性能規定を検討したい。【畑】
  - 病院内で使用されるホスピーという歩行ロボットを例に挙げると、時速 4km 以下と制限をかけている。しかし、最大出力で突っ込んだ際を考慮すると圧迫死の可能性はある。機器の最大エネルギー量と最大リスクを前提として、サイバー攻撃の影響を考えるべきである。【杉原】
  - 本質安全を確立する必要がある。エネルギーを減少させた機器とするか、構造を考えるべき。【向殿】
  - サイバーアタックを受けた場合、システムの多重系が機能しない可能性も考慮にいれて安全確保を検討するべきである。【畑】
  - セキュリティの観点からサイバーアタックからの防御は検討できるが、サイバーアタックによる影響の損害についてはセーフティの観点となる。【神余】
- ソフトのエラー・バグとサイバーアタックは区別できるか。【向殿】
  - 見分けることは困難である。【杉原】

<u>ICT 等の活用によるサービス、事業環境の変化</u>

- 半完成品を作っているため、販売後にどのような使用方法、使用環境となるのかの想定には限界がある。リスクはどの範囲を対象として検討するべきなのかを考えるべきなのか。現状の対策として危険表示しかできない。【中村】
  - ロボットメーカーはユーザーについて把握しきることは困難。ユーザー側にもリスクアセスメント専門家が必要であるし、システムインテグレーターがメーカーとユーザー間の協調に寄与すべきである。【向殿】
  - ケーススタディの種類をより多く検討する必要がある。【神余】
  - ケーススタディは、ロボットレンタル等の新たなビジネスへの指針となる。【中村】
  - メーカーがどこまで責任を持つのか。自動車業界についても責任の所在が論点となっている。【向殿】

- 各ステークホルダーの責任の範囲については、契約のあり方について議論すべきなのではないか。【山田】
- 生産システムのプレイヤーが拡大している現状を認識したうえで検討するべきである。例えば、セーフティに関する知識のない生産現場に関わる担当者が協働ロボットを制御盤の組み立てに活用するなど。【石川】
- インターネット接続が前提となっていない機器が勝手に繋げられている状況が多々ある。【河合】

- 自社（平田機工㈱）で推進しているコグニティブファクトリーを次回紹介する。【木下】
  - 自社（住友重機械工業㈱）でもNECのツールを活用し、インターネットと接続する方針を決定した。ビジネス上の戦略として、IoT化は避けられない。一方で、顧客から機械設計者に対し情報セキュリティに質問が集中しているが、回答できる知識を持っていないため混乱が起きている。【石川】

<u>生産システムにおけるセキュリティの脅威の考え方</u>

- サイバーアタックは、シングルフォルトかダブルフォルトか。機械安全はシングルフォルトを前提として検討しており、安全の定量化が可能。【中村】
- イベントツリーで検討すべき適切な範囲とは。保護対象は性能、機能、データと多岐に渡るため、保護対象の検討から開始したい。【神余】
- サイバーセキュリティは確率論ではなく、偶発的なハザードとして考慮すべきである。【首藤】
  - 脅威を実現するための難易度によって確率は変わる。【神余】
- システム思考に基づくシステムエンジニアリングが根付いていないため、システムインテグレーターの資格に盛込むべきである。【首藤】
- システム構成はセキュリティ・バイ・デザインとして考えるべきではないか。【首藤】
- 自動車業界については、国際連合議案で安全性とセキュリティガイドラインが示されている。【杉原】
  - 生産システムの場合の発生可能性のある事象を想定するのがポイントだろう。【向殿】
  - 車はエネルギーの最大出力に至った場合、100人分の生命に脅威を与えることができる。設備は従業員等の生命身体にどの程度脅威を与えることができるのか明確にしたい。【杉原】
  - 具体例から検討を開始する。【首藤】
  - 機能安全により安全性が担保されている状況がサイバーアタックによって破られるという考え方はどうか。【河合】
  - 安全機能の阻害をポイントとしたらどうか。【神余】
  - 制御安全、システム安全の3ステップメソッドの2番目のところ。そこをやられるかどうか、安全機能が果たせるかどうか。【向殿】
  - インテグレートされた場合の機能安全は次の検討事項とすべきである。【森本】
- 設備・機器デザインの段階からセキュリティリスクをどの程度考慮しているのかも明確にはなっていない。【向殿】
  - 設計段階から、セキュリティ・安全の対策の両輪での検討が必要である。【神余】

- セーフティは協調領域であり、信頼性は競争領域である。【杉原】
- ユーザーとメーカーの間でリスクコミュニケーションを成り立たせる必要がある。【神余】

次回調査研究部会に向けて

- ICT を活用するシチュエーションを想定することが第一段階となる。遠隔操作、プログラムの自動書き換え、遠隔監視など活用の想定案を全員で持ち寄ってはどうか。【畑】
  - モデルの検討にはステークホルダー整理も必要である。【神余】
  - 標準形を事務局が作成し、委員に展開してほしい。IPA ケーススタディ編・基本編が参考になるのではないか。【向殿】

３．その他

次回の調査研究部会は、８月３１日（金）１０：００に決定した。次回の調査部会で、ICT を活用するシチュエーションを各自想定した資料を収集することとなった。

以上

平成30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(案)			作　　成
			三菱総合研究所
開催日時	2018年8月31日(金) 10:00~12:30	開催場所	ステーションコンファレンス東京・602B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(住友重機械工業㈱)、木下(平田機工㈱)、杉田(テュフラインランドジャパン㈱)、杉原(パナソニック㈱)、中村(㈱安川電機)、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)、山田(IPA)、穴田(テュフズードジャパン㈱・今回限り)	
	事務局	宮崎、野村、吉田((一社)日本機械工業連合会)、首藤、土屋、高橋(三菱総合研究所)	

計19名

1．開会

事務局より挨拶を行った。

2．第2回研究部会の進め方

事務局の資料4に基づく説明後、以下の議論があった。

- セキュリティアタックが機能安全を破るという前提に基づき、本質安全のあり方を検討する方針について議論したい。【向殿】
  - セキュリティに3STEPはない。【神余】
- 保安対策が機能していることを踏えれば、サイバー起因で言われるような事故は起きない。と言うのは、サイバーセキュリティから産業保安が語られる場合、冗長性安全設計や保安体制を考慮していない場合が多く見受けられるからである。セキュリティは不具合の起因事象のひとつでしかない。想定外も想定するというISO 31000:2009のリスクに対する考え方の延長線上で考えれば、通常の安全に関する考え方が適用できる。セキュリティにおける安全思想として多重防護は今のところないようだ。【結城】
- 制御装置においては、機能安全は部品の故障に対する確率論で検討する。部品の故障率として落とし込む。今までは、プログラムに脆弱性があったとしても利用者の性善説や機械屋さんの知見に依って運用してきた。しかし、IoTの場合は、ソフトウエア、ITに対するリテラシーを有さない人や悪意のある人が脆弱性を高めるような使い方をする状況も発生する。それは確率論ではなく確定的であることとして検討を進めるべきである。【森本】
  - 脆弱性もひとつの不具合と考える方が良い。1980-90 年代のソフトシーケンス導入後、最近のプラントの現場では動作原理を十分理解できていない従業員がみられている。【結城】
  - また、IEC 60950(IT機器の安全性)が要求する信頼性は高くはない。しかし、理解せずに規格の使用範囲を超えて使用しているのが現状。適切な設計を判断できるかどうか、

サプライチェーンリスク・信頼性を検討し適切な素材を選定できるか、適切な維持運用（問題発生を迅速に検知・対処できるか等）をできるかどうかがポイントとなるのではないか。【結城】

- ICT を製造ラインに入れて発生する問題において、セキュリティとセーフティの関係を明確にすべきではないか。セーフティは人命に対する脅威を議論とするが、セキュリティは生産性も検討対象となり、体系化が必要だと認識している。【向殿】

- 故障・バグは、ある意味誤差範囲のようなものと想定されるが、セキュリティの攻撃というのは、完全に想定しているような動きではないので、誤差範囲で考えられるようなものではないのではないか。【山田】
  - それは、設計の問題に帰着する。今回のようなセキュリティの問題は、脆弱性に対して、意図を持って攻撃してくるので、設計（デザイン）で対応しなければ防げない。【向殿】
  - 米国の事例では、デュポンの工場で化学プラントの反応速度の速いリアクターの制御用 PLC に検証されないパッチを当て、PLC の動作緩慢により、リアクターが破裂し、死亡につながった例が報告されるなど、サイバーで人身災害が生じるようになってきている。日本の化学プラントの設計では、物理的手段による安全停止装置を確保したうえで、ソフトシーケンスを適用すると聞いている。【結城】
  - それがセキュリティバイデザインではないか。【山田】
  - 想定される不具合を考える範囲にサイバーという要素が含まれたということ。【結城】
  - 物理的なことを理解してロジックを組んでいるのか。【向殿】
- セキュリティと機能安全を統合する IEC 規格がある。セキュリティ・セーフティの検討を行っても、矛盾等が発生する。【神余】
  - 安全装置のインテグリティが落ちることも考慮すべきである。【森本】
  - 工場レベルだと、大きなファイヤーウォールなどセキュリティを先に考える場合もある。セキュリティとセーフティのどちらを先にかんがえるかは状況による。【神余】
  - 機械について、故障モードを全て解析 FMEA で実施して対策をしている。当然そういう設計段階で発生事象を考慮した上で対応していることを前提として良いのではないか。【畑】
  - オーナーズコントロールが効く、効かないという点も考慮する必要がある。【結城】
- FMEA において、異常に大きい値が入力された場合なども想定しているのか。【畑】
  - ソフトウエアでは、異常値が入った場合というリミテーションは想定されている。現象面として出てくるのは故障か物理量の異常かになる。【森本】
  - 結果にコミットするアプローチを検討すべきである。【結城】
- 物理量が異常値になったときの安全対策は。【首藤】
  - 異常については、本質安全の対策、圧力計器の PLC で対策を行っている。【森本】
  - 異常値を強制的に設定された場合に、PLC も犯されていた場合はどうするのか。【首藤】
  - PLC で守れないものも想定する。【畑】
  - セキュリティかセーフティかという議論よりも、安全機能が犯された状況を想定することが重要なのではないか。【首藤】
  - 結局リスクアプローチになるのではないか。金額やメリットを踏まえて組合せで検討す

べき。【結城】

- セーフティを担保する部分のセキュリティ対策を検討すべきであり、体系的な役割分担を決定する必要がある。【山田】

３．事例紹介

各委員の資料３に基づく説明後、以下の議論があった。

事例①（畑委員）

「モデルライン」に基づき「想定制御ブロック」、「安全関連・非安全関連ライン制御構成」について、現在検討中の「IEC/TR CD 63074」に基づき機械安全におけるセキュリティの検討ポイントについてご説明があった。また、コマツの KOMTRAX を事例にセキュリティ確保策のご紹介があった。

- 「表１ SCS の基本的要求事項と考えられる影響の概要」においてレジリンエンシーの要素が抜けているのではないか。Timely response to event に復旧まで含むべき。【結城】
  - 機械メーカーとエンドユーザーの役割分担まで検討しきれなかったが、関係者の責任範囲を明確にしたいと考えている。本表を参照したいのはメーカーである。【神余】
  - インテグレーターは本表を参照して復旧まで適切に対応していくのか。【畑】

事例②（神余副主査）

E-Factory の事例として、生産量の計画・実績のリアルタイムデータの活用による「生産実績の見える化と設備稼働率向上」、RFID を用いた工程連携による「品質向上・ヒューマンエラーの撲滅」、センサーを活用したコンベアのコンディションベースのメンテナンスである「予兆メンテナンスシステム」のご紹介があった。

- 調べてみた事例を分類すると、ICT 応用の省エネ、品質向上、稼働性がメインとなる。リモートだと保全系がメインとなる。直接安全系に関わるものはなかった。まだクラウド活用で効果が出ているものはないと感じた【神余】
  - データの完全性が問題になる。要求される信頼度をどう定義、担保するかを制御に関わる場合は検討が必要。【結城】
  - データの捏造は、他社に対する妨害には効果がある。【神余】

事例③（石川委員）

「プラスチック射出成形機、周辺装置の集中管理システム」についてご紹介があった。また、現在、住友重機械殿の IoT/M2M における提供機器・サービスのポイントについてもご説明があった。

- 遠隔操作は可能だが、インターロック装置をつけてもバイパスをしてしまう利用者が多い。バイパスされるとフルカバーが開いている状態でもリモート操作によりフル稼働も可能となってしまい、人を傷つけるリスクがある。【杉原】
  - 標準装備のインターロックだけでなく、ロボット周辺の柵も利用者が勝手に変えてしまうことがある。【石川】

- ユーザー責任なのか、メーカー責任なのかを明確にする必要がある。【杉原】

- 利用者の不正は遠隔モニターできればいいが、だれの責任になるのか。【畑】
  - 海外は発電所でもログは必ず取っている。【森本】
  - ログはまだ法律的にも議論をしきれているとは言えない。また、製品仕様として示しておかなければ、マルウエアとなってしまう可能性もある。【神余】
  - ログの使い方と内容次第である。【結城】

事例④（木下委員）

「自動車エンジン・ミッション組立装置、周辺装置の管理システム」についてご紹介があった。また、IIJ 様との共同で検討している「Cognitive Factory」の進捗状況についてご共有があった。

- ロボットコントローラーの速度を PC によりログをとって、トレーサビリティを確立し、問題が発生した場合にリモートコントロールを行うという仕組み。【木下】
- AI による予兆検知に対するニーズとしては、検知だけでなく、パラメーターを変えることや、機械を修理するというものがある。アクティブ保全。外部からの悪意を持った攻撃と同様なバグをメーカーが自分で作り出してしまいかねない。【石川】
  - フィードフォワードを遠隔操作で行ったこともあるが、部品の脱着はロボットを入れないと難しい。【杉原】
  - エレベーターの大型なものは、既に監視技術の活用が進んでいるのでは。【向殿】
- エレベーターの例があったが、監視する経路があるのであれば進入経路もあるということなのでは。【首藤】
  - 数万円で作る IoT システムは基本的に双方向となっているため、進入経路もあるということである。【森本】
  - シャドウ IT が話題になっている。実際に現場でアセットマネジメントができなければ対策もできないことが問題になっている。【神余】

事例⑤（杉原委員）

工場内搬送を目的とした「遠隔操作による無人運転車」についてご紹介があった。また、その遠隔操作により無人運転車を路肩に停車する状況におけるリスクアセスメントについてもご説明があった。

- 自動運転を公道で実施するということの影響の大きさが正しく認識されていない。【杉原】
  - 現在は、国際法上、人がついて運転しなければならないと聞いている。【結城】

事例⑥（森本委員）

「生産工場内部の基幹ネットワークとライン制御の分離」について自動車部品メーカーを事例にご紹介があった。

- 工場の予算でソフトを業者に作成してもらったものを利用している事業所もあるが、作成した署名の無いソフトウエアは、ホワイトリスト制御の製品に登録が難しい。**署名がないソフトウェアは登録する際に「不明」と出るため、許可してよいかどうか、使う現場の人間が判断がつかず、結局登録できずに、機能をオフしてしまう。**【森本】

- 利用者にとってはソフトのアベイラビリティ（可用性）があり、使いやすいことが重要。【結城】

4．その他

次回の調査研究部会は、10 月 30 日に安川電機・入間事業所の生産ラインの視察後に同社会議室にて実施する予定とし、先方の都合に応じて別会場にて行うこととなった。

以上

平成30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
			三菱総合研究所
開催日時	2018年10月30日(火) 14:00~16:00	開催場所	ステーションコンファレンス東京・503B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(住友重機械工業㈱)、木下(平田機工㈱)、杉田(テュフラインランドジャパン㈱)、中村(㈱安川電機)、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)、引野(経済産業省)、山田(IPA)、穴田(テュフズードジャパン㈱・今回限り)	
	事務局	宮崎、野村、吉田((一社)日本機械工業連合会)、首藤、土屋、高橋(三菱総合研究所)	

計20名

1．開会

事務局より挨拶を行った。

2．第2回研究部会の進め方

事務局の資料2に基づく説明後、安全設計のプロセスにおけるセキュリティの要件について以下の議論があった。

- 大前提として、生産システムにおける機械安全の観点からセキュリティの検討を行うこととする。日機連の研究部会により平成28年度まで検討された統合生産システムのモデルは、セキュリティの観点の考慮されていないため、今年度の検討の例題として活用する。IPA資料のセキュリティの観点をどう組み込むかが本日の議論の中心だと認識している。【向殿】
- 鍋蓋システムは、制御システムの安全に対する考え方と同様に、安全関連部分は完全分離を行う必要がある。ISO 13849の考え方にハードウェアでも取り組むことで、安全生産システムが構築できると考えている。【畑】
  - 安全系のエンジニアリング端末のサポートも考慮すると、危険な個所があることも言及しておきたい。【神余】
- 構成案の「セキュリティの脅威による被害」は、生産システムへのICT導入により想定される被害、リスクを意味していると理解した。機械安全の考え方をベースとしてシステムリスクも考慮していくことか。機械の設計側からセキュリティ要件を検討すると、より親和性が高いのではないか。【結城】
  - 一般的な制御系のセキュリティガイドラインは、モノづくりの手順を講書していないため、せっかくセキュリティガイドラインを作っても、生産工程に後から追加できないという苦情を耳にしてきた。やはり、機械の設計・生産、メンテナンスを含めたライフサイクルにおいて、どのようにセキュリティ対策をアドインしていくかということを検討したほうがよい。【結城】
  - 私の考えでは、被害は生産効率の観点もあるが、本議論では人が死なないようにすると

いうことを最優先として、その他の状況については、どのような順番でリスクを検討するか明確化しなければならない。【向殿】
  - この部会では、ガイドラインの想定使用者を明確化する必要がある。【結城】
- 開発プロセスの中で、リスク分析とバリデーションが要求されている。一方、IT と OT をつなぐようなケースではソフトウェアを組み上げてインストールして稼働したら終了となる。インテグレーションの段階でバリデーション等が必要だが、生産現場側では実際は行われていない。【森本】
  - 各社の開発規定にテーラリングする必要があるが、現在のところ、機能安全に関してはできているところが多く、セキュリティに関しては進んでいない。もともと、ISO/IEC 27000 に無理があった。【神余】
- リスク分析をプロセス上で説明するよりは、アクティビティとして定義し、それを年次計画として実施する方針を示したほうが、生産現場の業務関係の人には適しているのではないか。【森本】
- IPA のガイドラインでは、ソフト開発者とインテグレータがリスク分析者となっている。一方、実際には、工機部の人が開発の最終工程で確認することとなっているため、各社の工機部の責任者の人を本検討部会のガイドの想定使用者としたらどうか。【神余】
  - 設備のリスクアセスメントの中にセキュリティの観点を含むことができれば、機械の設計者は使えると思う。【畑】
- 機械安全の観点からは、ISO 12100 でセキュリティの考慮を追記することは可能だろう。しかし、分析の後段で、ハザードと安全の分析方法と脆弱性・脅威分析の方法が異なることに留意する必要がある。【神余】
- 機械設計担当者に IT 教育を行う必要があり、また、機械が止まった時の事業リスクの見積りに対する理解も望まれる。【杉田】
- 本ガイドラインは現場の動力につながるような 1 つの機械・設備という範囲に留めると理解した。【森本】
  - その通りである。【向殿】
  - セキュリティを検討するにあたり、目的、サービス、接続の仕方が定まらないと対策検討が難しいため、追加する ICT サービスを決定する必要がある。【神余】
  - ICT 利用の目的で、ロボットと人間の協働作業は考慮しないのか。【向殿】
  - 現状のモデルでは考慮されていない。しかし、本モデルのロボットのメンテナンスで、安全シーケンサ側に問題が発生すると暴走するので、危険な状態になる。安全シーケンサのソフトの条件を変えれば協働対応可能となる。【神余】
  - IEC61508 で認証されているような安全装置は改変できない。安全 PLC をどの程度乗っ取られるのかの想定を検討する必要がある。【杉田】
- セキュリティの場合、パスワードの使用方法に使用者側の文化（security environment）を考慮する必要があり、設備の持っている実力と運用の双方が重要である。あえて悪い状況の様々なシナリオを想定する必要がある。【神余】
- 普通の PLC と安全 PLC とで何が異なるために、普通の PLC より安全 PLC のほうが、セキュリティ強度が高いと考えているのか。RAM が書き換えられる可能性がある限りそのよう

な前提は成り立たないのではないか。【首藤】

- 基本的にどちらもPLCだから、エンジニアリング端末があり、プログラムをダウンロードして、動かすという意味では変わらない。ただ、企業文化の話では、例えば、ホンダのカナダの工場であれば、安全盤と制御盤は鍵を保有する責任者が異なり、安全盤を使うときは、安全の責任者によるコミッショニングを行う。日本も同様で、安全のプログラムを変更してダウンロードする時は、安全担当が立ち会う。ルールが守られていれば、簡単に安全PLCに侵入することは困難となる。【神余】
- 結局、人間系のルールに依存するのであれば必ずエラーが発生する。人間を介さない安全系を守る方策の例として、ROMの状態だけでCPUを動かすことができるならば、書き換えができないというものがある。最終的に安全に停止させるための最低限の機能のソフトウェアがROMに書き込まれており、それが起動して安全に停止することができる。そのため、最終の制御機能を動かすコンピュータの仕組みをどう考えるかが論点である。このような議論を通し、セキュリティバイデザインという考え方に本質的に近づく必要がある。【首藤】

- 設計において全てソフトウェアでセキュリティ対策を構築すると非常にコストがかかるため、ハイブリッドのやり方を推奨する。ハードウェアで安全対応した方がコストの面で有利な場合が多くみられる。【結城】
- セーフティを万全にすれば、セキュリティ起因でロボットの予期せぬ動きが発生したとしても柵の中にあれば安全上問題ないということになっている。【杉田】
  - 安全設計をしていて、全てが確定的に動けば間違いない。しかし、セキュリティにおける想定外の事象を検討する必要がある。例えば、電子素子をROMからではなくフラッシュメモリから読んでいた同じ製品でも、バージョンアップによりネット側でフラッシュメモリが書き換えられるなど。【森本】
- コンポーネントのレベルでは、IEC 62443-4-1にコンポーネント、PLCとかSCADAとかのセキュリティ要件が規定されている。実際、横河電機の安全コントローラ系の2機種について、組み込みデバイスの認証を取得している。しかし、コンポーネントで認証を取っても、使用方法を守らなければ安全ではない。【神余】
  - PLC等の制御機器の利用条件を示すガイドは必要だと考えている。【神余】
- ガイドのターゲットさえ決定できれば分析に関する部分は書き進められる。対策に関しては、ハード側に寄った対策とIT側に寄った対策それぞれで例題を作れば良い。モデルは日機連のモデルを使用する。【神余】
- このガイドラインの範囲は、設計開発、実装、運用、廃棄までか。【結城】
  - 設計段階で、ライフサイクルを考えて設計するということである。【向殿】
- 機械安全の制御の安全機能に特化して、このガイドラインを作るべきである。普通の汎用PLCを使用している場合、安全PLCを使用している場合等、ケースバイケースで異なるため整理してガイドラインにすべきである。【畑】
  - 安全PLCそのものが安全ということではなく、あくまでも故障率の話として理解すべきである。イーサネットが接続されているのなら脆弱は増加する。【森本】

- 安全 PLC は信頼性が高いだけで、セキュリティに対する安全性はさほど高くない。【首藤】
- 安全 PLC の使用に対しメーカーが、安全マニュアルを発行している。安全 PLC をアイソレート（分離）した別電源で、アイソレートな接地等と示しており、安全 PLC の使用者は、マナーとして安全マニュアルに従って構築しなければならない。【森本】
- それも安全設計の基本としてガイドラインに記述必要があるのではないか。【首藤】

- 安全設計における最初のリスクアセスメントは、安全機能がないことを前提で実施する。同様に、セキュリティの場合もセキュリティ機能がない前提で検討し、攻撃された場合の被害を算出し、セキュリティレベルを決定するプロセスを踏む。【神余】
- 安全 PLC が対象として議論されているが、ここ数年、現場に導入されているのは、Windows DCS や Linux 系 DCS であり、いわゆるパソコンを利用したものもある。それらに適用される規格は信頼性の観点からはあまり考慮されていない IEC 60950 である。プラント等は、実際それで動いている場合がある。要は、安い機器を組み合わせてシステム構築することが一つの手段となっている現実を考慮する必要があるのではないか。安全 PLC をどう使うかが明確ではない。【結城】
  - 今回は、FA を対象としてはどうか。【森本】
  - 今年度は生産ラインを対象とする。そして、安全関連部とそれ以外を分離する概念も広がっていると考えて良いのではないか。【向殿】
  - 今回の対象はハザーダスエリアをゾーニングで分けられるような FA を対象とするということで理解した。【森本】
  - 事故が起きるのは、ハザーダスエリアを分離できない協調ロボットであるが、今回は対象外としたい。【神余】
- ガイドラインを作成するにあたり、対象モデルにおける制限はどうすべきか。【向殿】
  - 現実的には、例題のモデルの制御システムを明確にして、ネットワークに接続した場合を検討すればよいのではないか。【木下】
  - 弊社のシステムは、ロボットがロボットを組み立てたりするシステムで、メンテナンスを考慮し柵がない状態で、ERP とも接続されるシステム構成である。本部会で議論している例題とも非常に近く、例題の参考にする良い事例であると思う。【中村】
- 生産情報や故障メンテの情報を取り入れるためネットワークに接続することを前提において、リスクを検討して、対策案を考えれば良いのではないか。【神余】
  - 最終的に報告書を書く段階で今年度方針以外については、現状の問題について注意喚起をした上で、課題を整理して列挙しておく。来期に、整理した課題についての対策を取り組むというストーリーで進めたら良いのではないか。【首藤】
- この検討プロセスの流れがガイドラインになるのではと考えている。【神余】
- 今年は、安川さんのモデルプラントのレベルで検討して、来年度は未定であるが、下町ロケットの人達にも役に立つような内容を実施する方針で良いのではないか。【森本】
  - 機械安全に軸足をおいて、その上でセキュリティの課題を克服していく。【向殿】
  - 本部会の成果を読む人は、機械安全に関わる人であるため、その人達がわかるような内容であるべき。【神余】

- 進め方は、インターネットにつながるシステム構成と前提条件を想定した上で、何人かの有志で検討したい。【神余】
  - モデルのラインは、ロボットとかプレスは連携しているが、空間上は切れており、前工程では高等なものを使わずに、後工程で PLC を使っている。古典的なものと先進的なものがミックスしたラインである。【宮崎】
- PLC を使用した際のセキュリティ面で脆弱性が考えられる例と、リレーで構成した方が安全面でもセキュリティ的にも優れている場合もある、という、2 つのパターンを提示することを考えている。【神余】
  - 想定されるハザードが非常に大きい場合は、IT に基づく対策ではなく、システム構成によるセキュリティ対策とすべきと示す、という解釈で良いか。【宮崎】
  - 安全で言うと、IT 側に寄った安全シーケンサのセキュリティ対策版を使えという特化した話かもしれないし、あるいは、できるだけ CPU がないもので構成したほうがよいという話かもしれない。【神余】
- 今回のガイドの前提とは、安全と非安全部分がゾーニングされているということとなる。ゾーニングのうえ、安全側をリレーか安全 PLC で対策を立てるのかを検討する。今回は、人とロボットの協働が実現している未来の生産現場ではなくて、あくまでも安全設計が原則として適用できる代表的な工場を検討対象とすると理解した。【森本】
  - 対策を取った結果、安全かセキュリティに影響が出た場合に、どちらに落とし込むかというバリデーションも実施すべきである。【神余】
  - 今回は適切な使用方法がなされている安全設計による工程を対象とし、まずは安全 PLC をネットワークに接続するのか否かを検討する。一方で、生産系の工場システムからのデータ収集や、安全 PLC とのデータのやりとりも考慮すべきであり、最低限必要な障壁の説明やリスクを書き込んであれば良いのではないか。【森本】

以上

（資料２）

平成30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（案）			作　　成
			三菱総合研究所
開催日時	2018年12月17日(月) 14:00~16:00	開催場所	ステーションコンファレンス東京・503B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（住友重機械工業㈱）、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㈱）、森本（㈱制御システム研究所）	
	オブザーバ	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）、河合（IPA）	
	事務局	宮崎、野村、吉田（（一社）日本機械工業連合会）、土屋、高橋（三菱総合研究所）	

計16名

１．開会

事務局より挨拶を行った。

２．第４回研究部会の進め方

今年度成果となるリスクアセスメントの提示について以下の議論があった。また、三菱総研より資料４に基づいて、IoT技術事例の紹介を行った。

- 今年度は生産システムのセキュリティ脅威に対するリスクアセスメントの提示までという方向性で合意できたと認識しているが、読み手の共感を得られるようなICTサービスの定義や事例を提示できるかについて、議論しておく必要がある。（神余）
  - 日機連の「安全な生産システムの構築能力向上のための調査研究部会」で、作成された報告書をベースに、新たにセキュリティの観点から何を検討しなければならないかを追記する方針で作成してきた。手法としては、IEC 62443に則って分析を行う。セキュリティ攻撃によって、安全機能が失われる事象について、重点的に分析するという考え方である。セキュリティ対策については、今年度は代表的な1例に留めたい。（神余）
  - 日機連の部会で提示されたシステムに対するICT利用については、ロボットのリモート監視診断が適当と考える。診断として想定するケースとしては、まず、1日数回データ送信すれば良いと考えている。コマンドを送信してデータを取得するという、双方向の通信を考えている。（神余）
  - ロボットから定期的にデータを送信するということは、ロボットメーカーは、適宜、コマンドを送信してデータを取得できるということか？（向殿）
  - そうである。エッジコンピューティングは、今回のモデルから外している。（神余）
  - 誤ったコマンドを送信することによって、誤動作を起こさせる可能性も含んでいるということと理解した。（森本）
  - データの取得・コマンド送信のレベルによっては、様々なセキュリティ脅威が生まれると思うが、データを取得・蓄積を行い、要求があれば送信するという範囲の仮定をおい

て、その範囲でどのようなセキュリティ問題が生じるかを検討すれば良いのでないか。（向殿）

- CE マークを取得している機械装置であるならば、セキュリティアタックを受けて、機械が暴走してもインターロック内であるので、機械は壊れるかもしれないが、人は死ぬことはなく、本質的安全状態にある。これは、固定した機械の条件下でのことである。しかし、インダストリー4.0 のように、個々の機械が移動して再構成されるような場合は、個々の機械が、互いがぶつからないようなルールを設定して、統合管理するシステムが必要になるという、1 ランク上のレベルになる。（杉原）
  - 人が介入した時、SIL3 レベルにあればアタックを受けても、有効に機能する。しかし、インターロックを破った瞬間に電源カットでカテゴリ０の停止、つまりフリーで動作可能になる状態になり、調整ができないという問題が起こる。従って、従来の機能安全のみの考え方では不十分である。（杉原）
- 新しいアプリケーションを考えるのは、難しいので、あえて、既存のアプリケーションで考えることにしたい。（神余）
  - あえて、セキュリティのことを考えない構成にして、セキュリティ分析をしたら、それぞれの構成に対して、セキュリティ対策の要件が出てくるという形式にしている。（神余）
  - ポイントは、作成した資料で提示している利用サービスに関して、利用者が興味を持って読んでくれる内容になっているかということである。それに対して、セキュリティ分析をしたら、様々な問題が顕在化するというようなシナリオを想定している。そこで、委員にお願いしたいことは、魅力ある具体的な利用サービスを１つか２つ提示していただければ、より具体性のあるセキュリティ分析になると思う。（神余）
  - このようなモデルを提案して、どのようなセキュリティ問題があるかを洗い出し、そのためには、どのような対策をすれば良いかという論点と、もう一つは、セキュリティバイデザインという考え方で、設計の段階でどのような方策をとれば良いかを考えていくという論点の２つだと理解した。（向殿）
- 平田機工と IIJ と一緒に実施している管理システムの概要を説明する。既存の制御システムにアドオンするという考え方で、様々な情報を収集して、表示して見える化しようという取り組みである。セキュリティについては、考慮していないという状況ではあるが、どのように見える化するかという提案だと理解してほしい。外にデータを出すか出さないかは、お客様のニーズ次第であり、エアーシリンダー情報監視機能（シリンダーの保全管理を行う機能）、計測器モニター機能（光電管センサー、温度センサー、バーコードリーダー）、アプリケーション機能、ダッシュボード機能がある。（木下）
  - このシステムは、正常な範囲が決まっており、その範囲を超えたかどうかをチェックしているシステムか。各センサーの値は独立して判定しているのか、それとも、別のセンサーの値と関連させて判定を行うのか、どちらか。（向殿）
  - コンベアーに流れているワークに使用している光電管センサーの基本設定が変化したかどうかをアラームで出力して、実際に時系列に変化していないかどうかをロギングして、変化が何に起因して発生したかをトレースできるようにしている。（木下）
- システム構成については、どの領域を誰が責任を持って管理するかという問題がある。（神余）

- データのオーナーシップも考慮したほうが良い。（結城）
- アセットマネージメントは、もともとエマーソンがバルブのパッキンの最適な交換時期を知るために、すべての工場からのデータを分析して、ちょうど良いヒステリシスカーブを見つけて、最適な交換時期を決定した。（神余）
- ユーザー側は、適切なメンテナンス時期を教えてもらえるというメリットのために、自分のデータを提供するという契約になっている。GE などはそのような契約をしている。（森本）
- 現在のところ、データの所有権について、FA に関してはお客さんにあるということになっている。自動車はメーカーのものとなっている。（神余）
- データの所有権と利用権の話については、整理しておいた方が良い。（結城、神余、向殿）
- データの所有権については、現在のところ我々のユーザーは、メーカーにデータを渡そうとはしない。予防保全のために、データ提供していただければ、適切な時期を教えることができると言っても承諾しない。現場レベルの担当者は希望するが、情報セキュリティ委員会が関与してくると、外部に情報を出すのはダメという判断になる。工場の稼働データは、ノウハウになるということで、最終的には渡さないという判断になる。（石川）

• 既存設備に追加可能になるというのが、この場の議論のポイントとなると考えている。安全関連部が ICT の部分と分離することによって独立しているということで、安全は脅かされないという見方ができるのでは。（石川）
  - 現在のところ、SIL とセキュリティレベルは別なので、分けて対応するということにしているが、結果的に干渉することもあり得るというのが、現時点の世界の認識である。（神余）
  - 利用者（システム導入者）が、キチンと安全のことを考えている場合、問題なくインテグレーションできるが、利用者のシステムが、安全について明確になってない場合、安全性の担保は利用者の責任なのか、機能追加した側の責任なのかが曖昧になる。今回の神余さんのモデルの場合は、安全系を適切に組み込んであるという前提で行うが、このあたりは、事前確認を要することになる。（森本）
  - ロボットコントローラの中身が、安全関連部と機械部のエッジにデータを渡すところが、CPU が別になっているというような構造になっていないと危険である。（石川）
  - 現実には、安全通信が SIL3 レベルであれば、CPU2 つで実施することが一般的であり、その保証の下で、安全通信も安全制御も分離したネットワークで実施するということであれば、安全という解釈になるのでは。（神余）
  - 始めからネットワークの安全系を使う場合は分離しているが、IoT システム業者が制御システムの保守用のイーサネットポートから常時データを取る仕組みに流用してしまった時に、アープのストームが起こることで制御系に影響が出てしまう場合もある。後付けの場合には留意すべきケースがある。（森本）
  -
  - 始めからネットワークの安全系を使う場合は分離しているが、IoT システム業者が保守用の回線から兼用してしまった時に、アープのストームが起こることで繋がってしまう

場合もある。後付けの場合には留意すべきケースがある。（森本）

- 選択肢として、経営レベルの決断の問題であると思う。我々は、ボトムアップで安全問題とセキュリティ問題にトライしている。（向殿）
  - 日機連的には、機械メーカーに対して通信は双方向であるというメッセージを訴えるべきである。（森本）
  - 危険状態のことを考えて、書き換えできない領域と書き換えできる領域を分けて、一切侵入できない状態を確保するということを示すべきだと思う。（杉原）
  - 最終的には、そのような考え方になると思う。（向殿）
- 扱うものによって、可用性重視か、安全性重視かにパターン化できないものか。（結城）
  - リスクアセスメントの時に考慮するのか、対策の時に考慮するのかが曖昧である。（神余）
  - 安全重視なのか可用性重視なのかセキュリティ重視なのかによって、それぞれ別々に発展してきた。しかし、繋がることで境界が曖昧になったため、どのように切り分けて、どこに重点を置くかということ考える必要もある。（向殿）
  - IEC 62443 のリスクアセスメント的にいうと、松竹梅のやり方がある。そのような具体的なイメージを持って議論したい。（神余）
- 止まらないことを優先する考え方もあって良いのではないかという議論があるが、その前提は、システムが非常に小さいエネルギーの場合であり、想定される被害の程度に依る。切り分けをどのように考えれば良いのか。（首藤）
  - 可用性が重視といっても、まず安全が大前提となる。状態監視保全によって、可用性を高めるというのもあって良いのではないかということである。（結城）
  - 人が立ち入らない範囲を前提に置き、柵に囲われている機械においては止まらないということである。（木下）
  - 定常に稼働している場合と違って、メンテナンスモードやティーチングモードで人が柵の中に入って作業する場合、この運用フェーズでアタックを受けた場合はどうなるのか。（首藤）
  - あくまでも安全系が正しく動作しているという前提に立っている。（木下）
- 日機連のスタンスとしては、機能安全および安全系が正しく設計されている前提のもとに、下手なことをやると安全系が無効化する可能性に対するアセスメントを実施するということと理解した。（森本）
  - トップダウンというよりは、ボトムアップ的にやっていこうということである。（向殿）

３．今後の進め方

今後の進め方について以下の通り、合意が図られた。また、次回の検討部会は委員日程調整の後、決定することとなった。（候補日：２月４日(月)午後、２月５日(火)）

（資料２）

1　実施事項：現状認識を含めた ICT 利用のための提言の作成

(1) 神余副査

・1 月第 2 週までに、H29 年度に作成した次をもとに現状認識を含めた ICT 利用のための提言案を作成　→　委員及び／又は事務局へ送付

> 1.セキュリティの脅威は機械安全におけるハザードを生じる新たな因子
> 2.セキュリティの脅威から生じるハザードは、確実に発生するものと考える
> 3.セキュリティの脅威への最終的な対策は「停止」

(2) 委員

・1 月末までに、受け取った神余副主査・提言案に対するコメント/加筆・修正

注：最終案については、2 月末までに固める。

2　実施事項：ICT サービスを利用したシステムにおけるセキュリティ RA 事例の作成

(1) 木下委員

・12 月中に平田機工様のプレゼン資料のうちの機器構成例を全員に展開

(2) 神余副査

・1 月第 2 週までに、制御機器の接続例+平田機工様の事例を統合したユースケース案を作成（RA 除く）　→　委員及び事務局へ送付

(3) 委員

・1 月末までに、ユースケース案に対するコメント/加筆・修正

(4) 神余副査＋委員

・2 月末までに、ユースケースの RA を実施

3　報告書案（3 月末）

上の 1 及び 2+アルファを統合し、報告書作成。

以上

平成30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(案)			作　　成
			三菱総合研究所
開催日時	2019年2月4日(月) 13:00~17:00	開催場所	安川電機 入間事業所 会議室
出席者 (敬称略)	委員	神余(三菱電機(株))、石川(住友重機械工業(株))、木下(平田機工(株))、杉田(テュフラインランドジャパン(株))、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(株))、中村((株)安川電機)、畑(機械安全実践技術促進会)、森本((株)制御システム研究所)	
	オブザーバ	結城、河野(内閣官房 内閣サイバーセキュリティセンター)、古閑(平田機工(株))、中富((一社)日本機械工業連合会)	
	事務局	宮崎、吉田((一社)日本機械工業連合会)、高橋(三菱総合研究所)	

計16名

1．開会

事務局より挨拶を行い、神余副主査より本会議の論点について説明があった。

- 年度末までのスケジュールを確認したい。前回の会議であった提言の内容であり、昨年度を踏まえたものにしたいため本日議論を行う。また、ICT システムを想定したリスクアセスメントを実施するため、脅威分析に基づく事故想定までは今年度達成したい。例題をどうするか、分析方法は IPA の制御システムの分析（IEC 63074)、森本委員作成のフォームに基づく分析の二つがある。本日は大きな方針を定めたい。【神余】

2．提言に関して

資料５に基づき、神余副主査より説明があり、その後以下の議論があった。

- 本提言案のように明確に言い切っているセキュリティ脅威に対する考え方は世の中にない。また、ここまで機械に特化した焦点でのレポートはない。当たり前の話であり、昨年度成果とも矛盾はない。ご意見がほしい。【神余】
- リスクの影響の与える対象を明確にしないと読者は理解が難しい。研究部会のタイトルともリンクさせるべきである。財産なのか人なのか等、広く理解されてしまうため。【畑】
  - できる限り、機械安全の論点に寄せて構築している。どの程度提言に前提を書き込むかも検討すべきだと認識している。【神余】
  - 読者に適した報告書としてほしい。【畑】
- 安全制御系はハードウェアで制限すべきだということは確かにそうだと理解できる。【安川電機】
  - そこを強調するように表現している。協働ロボットのような話もあるため、どこまでそういった話を書くかも検討が必要。【神余】
- 共通要因故障としてのネットワークを見ているのか、IoT として接続してよいと考える安全系の独立とはどのレベルか。【畑】
  - 個人的には CPU があるものは全て信用できないという。【神余】

- 安全系といっても完全な　共通要因故障とならないよう制御系と安全系が多様性を持つということと理解した。【畑】
- しかしプラントや鉄道システムだとこの 3 つ目は突然停止することが安全だとは限らないため、適用は難しいが機械安全のスコープでは適用可能だと考えている。そのため日機連の読み手に違和感のない対象に制限している。【神余】
- 結局どのような ICT サービスを想定するのかがポイントにもなる。【神余】

- 2 番目の提言は機械を扱うサービス事業者にとって脅威の実現する難易度の見積もりは難しい。どこまで具体的な話まで落とすのかがポイントである。松竹梅レベルか、一般的な技術論から検討するものか、具体事例に基づくかのどちらか。【森本】
  - IPA の制御システムのガイドラインに記載の内容を想定していた。リスクアセスメントの表が松竹梅、技術的な難易度、悪意の強さ等の表があるが、それを簡単に使いやすいものにしなければならない。日機連として機械観点から簡単なものにしたい。【神余】
  - 誤解を招いてはいけない。【森本】
- サイバー攻撃による自動設備の本質的安全設計と読み替えてはどうか。サイバー攻撃によるハザードは確定的である、サイバー攻撃の対策は。【杉原】
  - サイバー攻撃は多種多様であるため、因果の果で考えたほうが良い。サイバー攻撃と公表されている事象のほとんどが自損事故だが、メーカーは原因を明確に公表したがらない。サイバー攻撃と限定してしまうと視野が狭くなってしまう。CPU を入れることによる新たなリスクだと理解すべき。【結城】
  - 実際は物理セキュリティ対策の方がサイバーセキュリティ対策よりも効果がある。そのためサイバーセキュリティ対策といわずにあえてサイバーを抜いた。【神余】
  - 複雑になればなるほど止めても安全ではない。【結城】
  - 確かに、複雑系になればなるほど止めるのが困難になる。本検討部会では、機械安全を対象とするため、可能だと考えている。【神余】
- 安川電機の工場のネットワークは工場に閉じた構築が行われているのか。【石川】
  - 外とは繋がっていないが本社と繋がっている。インターネットと繋がる回線とは別に、工場は専用回線を利用している。【安川電機】
  - 外側の情報を取りに行くときは仮想 PC を立ててそこから繋げている。一部その仮想 PC を経由して外部へ情報を出している。データは専用回線で本社部門に直結でいっている。【安川電機】
  - 管理されており、閲覧できる人も一部ということか。【石川】
  - そうである。【安川電機】
- 提言についてはコメントを頂いたうえで１か月検討したい。【神余】

３．「安全な生産システムの ICT 対応（案）」について

資料４に基づき、神余副主査より説明があり、その後以下の議論があった。

- IEC TR 63074[1]はリスクの考え方がセキュリティとセーフティで異なる。その考え方の違いを記載したほうが分かりやすくなるのではないか。【畑】
  - 脅威分析と機会分析を両方する必要はある。【神余】
  - する、しないは別として考え方を記載する必要はある。【畑】
  - 脅威分析のいくつかのパターンを作ることで、何が起こるのかを示したほうがよいとは考えている。同じ事象をとっても人によって対策は異なるため、一元化は困難と考えて今年度は行わない。【神余】
  - 今年度は、森本委員に提供してもらったフォーマットベースで分析を進めていこうと考えている。【神余】
- IEC TR 63074 を JIS 化する議論を現在行っている。トップの規格は IEC 62443 である。EU の政策会議で組み込みシステムの基本的考え方とすることが示されたため、IEC 62443 を完成として、ベースとして検討されている。【神余】
- 安全にフォーカスをするのか、資産にフォーカスするのかの被害の記載がない。今回は安全を中心とした議論とするのか、設備機器が壊れるところまで対象とするのか。資料３を見ると、どこまでを分析の対象範囲かを検討したい。【森本】
  - 守るべきはエンジニアリングである。機械だとその部分が表に出てこないため、守るべきデータを含めた言葉として、資産という表現とした。最も優先すべきは安全ということで変わりはない。【神余】
  - 経路としての解釈だと理解した。【森本】
- データ改ざん等までこのフォーマットのみを見て検討できるのか。日機連として資料３を埋めたサンプルを出すのか、フォーマットだけを報告書に載せるのか。【森本】
  - サンプルを出さないと分からない。定常作業、立ち上げ作業、製造作業と分割して示してもいいのではないか。【神余】
  - マニュアルやポリシーがないとただシートの穴埋めとなってしまい意味がない。【結城】
  - 例を載せて公開したほうが良いだろう。【神余】
  - ISO 31000 の議論からスタートしたほうがいいのでは。リスクアセスメントの目的は何であるのかという部分等が抜けており、現場から積み上げた話になってしまっている。また、会社・組織によって何を守りたいか考え方が異なる。【結城】
  - ユーザーにとっては難しいのではないか。【森本】
  - リスクマネジメントの理解は難しいのではないか。一方で、安全のリスクアセスメントはトレーニングをすれば対応できると考えている。機能安全が流行っており、確率論が主流となっているが、現場としたら確定論としてみて対策を検討する必要がある。【神余】
- セキュリティのリスクとは、ということを具体的な事例を挙げて解説したほうがいいのでは。【畑】
  - あえて機械安全においてはセキュリティのリスクをハザード分析に乗せて実施してはどうかということを示している。【神余】

[1] IEC TR 63074 ED1 Security aspects related to functional safety of safety-related control systems

- 機能安全は機械の安全の最終手段である。【畑】
- 安全の体系を確立した後にシステムとしての脆弱性がどこにあるのか、という検討の流れでよいか。【森本】
- 工場のファイアウォールをどうするか等の議論を始めるときりがない。【神余】
- 安全系が確立された工場で IoT を導入するためにどういった検討が必要かという議論だと理解した。【森本】
- セーフティの分析の中にセキュリティの観点を入れるという方針で実施したい。【神余】
- 機械屋さんに分かってもらうために、最低必要な分析を示したい。そのため、資料３を示し、構造は同一だとしても作業によって被害が変わることを示す。そのため、資料３の前にリスクアセスメントをするために、作業分析が必要だと考えている。【神余】
- 作業分析で出てきた作業ごとに資料３に書き込んでいくというイメージである。【森本】

- ライフサイクル全体を扱わなくてよいのか。【結城】
  - 廃棄・リサイクルは含まない。機械の運用・作業という観点で検討してもらいたい。【神余】
  - データの廃棄を考慮する必要がある。【結城】
  - オペレーションに焦点を当てたいと考えている。【神余】
- セキュリティの脅威の洗い出し方を理解できる事例を併せて示してほしい。【畑】
  - 機械安全リスクアセスメントができる人であれば手が届くレベルにしたい。【神余】
  - 現状の提言よりもっと機械安全に寄せてもよいかもしれない。【神余】
  - 読者はだれか。【結城】
  - 日機連の機械安全ができる人。【神余】
  - 設計する側、使う側の双方が含まれる。【畑】
- 事例があまりないため、現状は原則論に伴って検討を進めているが、このようにケーススタディーを作っていかなければならないと考えている。メーカーとユーザーと機械ベンダーで考えていくためにも、まずは日機連の読者に伝わるような形で作成していきたい。【神余】

4. 今後の作業について

- 作業内容：２つのターゲットに対する分析を、森本委員のシートをベースに作業のフェーズを４パターン程度作り、パターンごとにシートを埋める。
- 日程は今後調整する。

以上

平成30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
			三菱総合研究所
開催日時	2019年3月11(月) 10:00~12:00	開催場所	ステーションカンファレス 東京605A会議室
出席者 (敬称略)	委員	向殿(明治大学)、神余(三菱電機(株))、木下(平田機工(株))、杉田(テュフラインランドジャパン(株))、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(株))、森本((株)制御システム研究所)、澁谷(テュフズードジャパン(株))、笹川((一社)日本工作機械工業会)	
	オブザーバ	引野(経済産業省)	
	事務局	宮崎、野村、吉田((一社)日本機械工業連合会)、土屋、高橋((株)三菱総合研究所)	

計15名

1．はじめに

事務局より挨拶を行い、神余副主査より本提言のポイントについて説明があった後に以下の議論があった。

- 守るべきはエンジニアリングであることは前提でよいのではないか。エンジニアリングとはどういう意味か。【首藤】
  - 狭い意味では、PLC、安全系を指す。これらの部分を早く復旧させることが重要となる。エンジニアリングステーションのバックアップをしておくことが重要だがかつて言及されていたことはない。オペレーターがまずは気づかないとならない。【神余】
  - システム、ハード、ソフトを全て含んでいるという考えだと理解した。【向殿】
  - 広い意味だとオペレーターがいかに早く気付くかという観点も重要であり、人間も含まれる。議論が必要である。【神余】
- セーフティ、セキュリティの観点に事業継続性を含むと議論が複雑になるため、現状のフォーマットで議論したい。IPAやNISCの文書を参考としたい。産業保安観点の資料を活用できればと考えている。【神余】
- 対策をどうするかはケースバイケースである。機械安全のひとが見て分かるようなリスクアセスメントを目指したい。そのためライフサイクル全体は難しい。これまで日機連が作成したガイドラインと合わせて、オペレーションに着眼したい。【神余】

2．３０年度の報告について

森本委員より資料２、神余副主査より資料３について説明があった後に以下の議論があった。

- ITセキュリティの対策は可能性を下げることができても被害の大きさを下げることはできない。だからこそセキュリティとセーフティ双方の対策が必要。【神余】
  - ➢ 被害の大きさに関して、セーフティを重視しているという観点から、工場が止まらなかったら「小」・止まったら「中」・人や機械に被害が出たら「高」という理解をしてほしい。
  - ➢ 可能性に関しては、実行の難易度で小・中・高を判断した。生産中の機械に対するアタ

ックは難しいため小が多く、遠隔操作になると高を設定している。

- リスクアセスメントを行うということが本事業の目的。【神余】
- 可能性は確定論的な観点で検討する必要があり、やりがいのある対象が選定される。セキュリティの攻撃対象はやったほうが儲かるか否かという視点もあっても良いのではないか。【向殿】
  - 「命が惜しければ金を出せ」というサイバーアタックを受ける場合もある。バイパスというイレギュラーをするということで、インターロックをはずして動かすことも可能になる。安全装置を機能安全に特化したコントローラー、ソフトセンサを使用している場合、人に対する被害はおよばない。ハードで対策をするということはアタックを受けても影響しない。ソフトウエアスイッチはもはや効果はない。【杉原】
  - インターロックは切らないといった物理的な対策が結論になる可能性はある。【向殿】
  - ここまでの議論であれば、日機連の読者は理解できるだろう。【神余】
- ウイルスアタックがあった場合に何が起こるのかを資料２、３に示されていると理解した。本質的に制御情報システムが持っている脆弱性について、資料２、３を通してあぶり出すことができ、それに対する技術的な対策を検討できる。脆弱性にどういう対策が必要なのかを切り分けて理解できるような資料が作成できれば本会議の成果として成功だろう。【首藤】
  - このレベルの生産ラインだと、守るべきものが 100～200 程度出てくる。IPA 等の資料では守るべきものをリストアップせよ、から始まるがそれは今回困難である。【神余】
  - インテグレーターにどこまで何を要求しなければならないのか、という切り分けが可能になる。今の問題は、現在持っているシステムがどの程度脆弱なのかが理解できていないことである。【首藤】
  - セキュリティアタックは進歩する。現在の議論がいつまで通じるのかは定かではない。【向殿】
  - 時代によってルールは変わるだろう。【神余】
  - 生産ライン全体といっても個別にどんなシステム、どの事業者（誰）が組んだシステムなのかで脆弱性レベルは全く異なる。製品として販売されているものを使用するのであれば安全性は高いが、事業者が独断で構築したシステムは、脆弱性が高いというレベル差が存在する。【杉原】
  - 我々は機械安全の観点から議論していることを忘れてはならない。家電 IoT と生産システムの場合ではなにを守るべきかが異なる。守るべきものと対応した脆弱性の検討等、区分けをしたうえで議論を進めないとならない。【向殿】
  - スマートホームの議論でも、テーブルタップのようななにが刺さるか分からない製品は、リスクを想定することは難しいため除外して法律を検討した。【杉原】
  - IT 屋さんはデータを守る話に寄るが、日機連の議論としては、性能や生産能力等のパフォーマンスを守るという観点になるのでは。【神余】
  - ISO 31000 という観点を重視させるためには人命をお金に換算する必要もあるのでは。価値観を決めないとマネジメントには響かない。例えば、セキュリティアタックを受けたことを検知しても生産ラインは動くといった状況で、工場長はどのような判断をすべきなのか。その判断の指標となるようなガイドを作ってはどうか。【杉田】

- マネジメントになるとコスト換算が必要であるが、日機連としては最も重要なことは人命を守るということである、ということを前提としたほうがよい。【向殿】

- セキュリティは安全制御にコンピューターが入ってくるため信頼性の話になる。大事なのは、信頼性・セーフティ・セキュリティ・レジリエンスである。セキュリティバイデザイン、セーフティーバイデザインという観点を入れていきたいが、概念に順番つけて検討を進めていきたい。【向殿】
  - 生産能力と生産品質と重要な観点の順序を付ける必要がある。【神余】
- リスクが中と高である場合は対策を検討しなければならないという明示や、IT セキュリティ対策を重視したもの、物理セキュリティを重視したもの等、ガイドを付けたうえで、どのような対象に影響があるのか明確に示しておいたほうがよい。【神余】
  - 生産システムを念頭に置いて、人命が最重要であるという考え方でいいのでは。【向殿】
  - メーカーとユーザーのリスクアセスメントの整合性が問題になる。リスクを受け入れるのは機械ユーザーになる。そのため、労働安全の４段階に合わせてもいいのではないか。【杉田】
  - それでは極高という出てこないランクをつけてはどうか。【森本】
  - 原発のメルトダウンレベルは極高に当てはまるが、工場レベルでは発生しないという前提で設定すればいいのではないか。想定はしているということだけを示す。【神余】
- 当工業会では、このような検討はしていないが方向性に納得している。今後コメントがあれば共有していきたい。【笹川】
- 厚労省がインテグレーターに対して機能安全の教育を始めた。労働安全の教育においても機能安全の教育をする。その次はセキュリティの教育の導入が考えられているようである。【向殿】
  - システムインテグレーションに関しての教育を現場の安全担当者に教育することは難しいのではないか。【森本】
  - スイッチをハードでつけておくことが安全なのに気づいていないメーカーが多いのではないか。【杉田】
  - IoT 家電についても温度センサーをつけてヒューズできるという物理的対策を検討している。【向殿】
  - 高所作業の命綱がないレベルが、ソフト対策だけで安全対策を行うレベルと一緒ではないかと感じる。【森本】
- 資料３に記載の「ファーウェイ」を修正する必要がある。【神余】
  - スパイチップという表現で、ソフトウエアではないものであることを示す。【森本】
- 現場エンジニアリングをどう変えるか。設定変更・調整にすることを検討する。【森本】

２．来年度事業の方向性について

- 対策の検討を行うことに主眼を置く。そのうえで、トレーニングカリキュラム等への展開も検討する。

以上

平成 30 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

発　行　2019 年 2 月
発行者　株式会社三菱総合研究所
〒100-8141
東京都千代田区永田町二丁目 10 番 3 号
電話 ： 03-6851-2581