安全安心社会研究

［ 第１０号 ］

２０２３年３月

長岡技術科学大学
安全安心社会研究センター

巻 頭 言

長岡技術科学大学　システム安全系　教授
安全安心社会研究センター　副センター長　木 村　哲 也

イノベーションという単語を聞かない日はない。イノベーションは、資本主義社会の持続的発展の原動力として、20 世紀当初に経済学者のシュンペータにより「新結合」という表現で提唱された。現在の我が国でも「科学技術イノベーションは経済再生の原動力（内閣府）」として、各種イノベーション支援政策が実施されている。本学でも５年一貫性博士課程「技術科学イノベーション専攻」を設置し、イノベーションを主導できる人材育成に取り組んでいる。

自動運転、ドローン、AI 等イノベーションとして想定される技術のもたらす恩恵は計り知れない。では、イノベーションを安全安心に推進していく基本は何であろうか？　新規性の高いイノベーションでは、経験則に基づく安全や再発防止型の安全は、有効性が限定的と考えられる。安全安心なイノベーションの推進には、論理的に事故の未然防止を図るシステム安全に基づく安全が基盤と考える。

本学システム安全工学専攻は、我が国唯一のシステム安全を大学院レベルで教授する機関である。同専攻から多くの研究者が参加している本安全安心社会研究センターは、安全安心なイノベーション推進にも大きな寄与が期待されているのではないだろうか。この期待に本センターは応えているのか、本冊子の読者がどのような感想を持つであろうか、思いを巡らせながらの巻頭言とする。

内 容 目 次

巻頭言

長岡技術科学大学　システム安全系　教授　木村　哲也‥‥‥‥‥‥‥‥ i

【特集：これからのシステム安全】

システム安全を学んで感じたこと

長岡技術科学大学　特任教授　福田　隆文‥‥‥‥‥‥‥‥‥ 1

新しい時代の安全“協調安全”

日本認証株式会社　一般社団法人セーフティグローバル推進機構

松浦　裕士 ‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥ 8

AUTOSAR：モビリティの提供を「継続可能」とするためのプラットフォーム

イーソル株式会社　櫻井　剛 ‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥ １８

【工学教育賞受賞】

工学教育賞受賞

長岡技術科学大学 システム安全系　系長　門脇　敏‥‥‥ ４２

【客員研究員活動報告】

ドローンの事故調査について

五十嵐　広希 ‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥ ４４

機械安全を学ぶ方々の変化

今枝　幸博 ‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥ ４６

取り返しのつかない事故
岩岡　和幸 ····· ４８

ISO 12100 発行から 20 年
越前屋　睦 ····· ５０

「セーフティ」と「セキュリティ」
大賀　公二 ····· ５２

衛生設計と食品安全の統合
大村　宏之 ····· ５４

コロナ禍における食の安全
川瀬　健太郎 ····· ５６

安全の論理と必要条件と十分条件
杉本　旭　 ····· ５８

医療 DX と情報セキュリティ
野沢　義則 ····· ６０

製品安全競争力の見える化について
松田　利浩 ····· ６２

研究成果の社会実装
吉澤　厚文 ····· ６４

【センター活動】

令和３～４年度 安全安心社会研究センター主催の
講演会等の活動 ····· ６６

長岡技術科学大学における安全安心社会研究センターの
構築に向けた取り組み ····· ７１

システム安全を学んで感じたこと

長岡技術科学大学　システム安全系
福 田 隆 文

今回のご依頼では、指定された主題はなかったので、今までに感じてきたことを書こうと思います。論ではなく感じたことを記すことにします。あくまでも私見です。ですので、何回も「と思う」があります。

本稿で書きたいことは、「技術を知らなければリスク低減はできないが、倫理感がなければリスクを低減しない」という単純なことです。

1. ISO/IEC Guide 51 がいう安全

まずは安全の定義から考えてみたい。やはり ISO/IEC Guide 51:2014[1)]を見ておくべきだろう。このガイドは規格作成に当たって、安全側面（安全に関する事項）を取り込むためのガイドである。しかし、安全の定義やリスクアセスメントとリスク低減の反復プロセスなどは、規格作成に限らず、広く使われている。

同ガイドの初版（1990 年版）、二版（1999 年版）で文言の修正はあったが、大きな意味の違いはない。最新版[1)]では次のように定義されている。

3.14
safety
freedom from risk which is not tolerable

安全
許容不可能なリスクがないこと。
（翻訳は JIS Z 8051:2015[2)] による）

何となくは分かる。しかし、この定義を理解するためには、許容できるリスクか許容できないリスクのどちらかが分かる必要がある。そこで、同ガイドでも、次のように説明している。

3.15
許容可能なリスク（tolerable risk）
現在の社会の価値観に基づいて，与えられた状況下で，受け入れられるリスクのレベル

さらに、箇条 6.2 “許容可能なリスク”を立てて解説している。

許容可能なリスクは，次によって決定することができる。
－ 現在の社会の価値観
－ 絶対安全の理想と達成できることとの間の最適バランスの探求
－ 製品又はシステムに適合する要求内容
－ 目的及び費用対効果のための適合性の要因

この後で、「開発が技術面及び知識面において，製品又はシステムの使用に関して最小限のリスクにまで達成できる経済的に実現可能な改善できる場合は，リスクの許容可能なレベルを見直す必要がある」と記している。ここで見直す方向は許容可能なリスクを下げる（許容可能なレベルの判断を安全側に移動させる。）ことをいっている、と考えられる。しかし、上の 4 個のーを読んでも、具体的にはよくわからない。

ところで、同ガイドには次の細分箇条もある。（下線は筆者が記入した。）

6.2.3 規格作成者は，製品又はシステムの意図する使用及び合理

的に予見可能な誤使用のために，安全側面を考慮しなければならず，更に許容可能なリスクレベルを達成するためにリスクを低減する方策を規定しなければならない。

この部分から、規格に記された要求事項を全て満たせようにすれば、許容可能なリスクレベルになると理解できる。

これを整理したのが**図１**である。

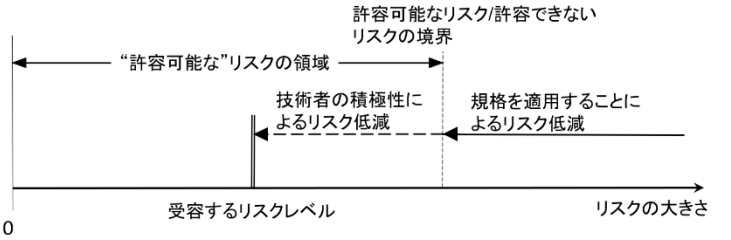

図1　リスクの大きさと許容リスクレベル・設計者の受容リスクレベル

ところで、受容可能なリスクレベルはどこだろうか。受容可能レベルは、受け手しか決められないと思う。だから図１内の縦の二重線の位置を決めるのは、例えばその商品を購入する人である。しかし、リスクを受容するのは、購入者だけではなく、設計者（あるいは製品を出荷するメーカ）もである。自社の製品の安全性を、規格に記されていることだけ行えばよいとするのか、もっとリスクを低減させて始めて出荷を可とするか、そのレベルはどこか・・・。出荷を可とするということは、メーカとして製品に残留するリスクを受容したということであると思う。残留リスクは０（ゼロ）にはできないから、どこまで低減さ

せるかの判断が要る。

国際規格は国際通商のためのもの[3]であるので、流通させるために求める安全のレベルを示す。従って、(流通させるという点で考えて)許容可能なレベルで記載されることになると考える。

ところで、規格は state of the art を反映して作成される。この語であるが、ISO/IEC Guide 2: 2004[4]で定義されている。

> state of the art
> developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience
> 到達技術状況
> ある時点での、科学、技術及び経験を結集した知見に基づいた、製品、プロセス及びサービスに関する技術力の到達段階。
> (翻訳は JIS Z 8002:2006[5] による)

ある時点は、製品の設計・製造段階で、その時点で達成している段階である。規格は、製品を流通するための基準であるから、作れることしか規定し得ない。しかし、科学、技術及び経験を結集した知見を基準としていることは意識しなければならないと思う。

2. 安全における技術者倫理の役割

図1に戻ってもう少し考えてみたい。今度は点線矢線の部分である。設計者が、もっとリスクを下げたい、と考えたとしても、技術力がなければできない。そのため、技術者は不断の研鑽が求められる。しかし、リスクをより低減しようと考えなければ、そもそも点線矢線のような低減は実行されない。規格を満足しているのだから、それでよいではないか、と考えたら、規格の求めるレベル、つまり流通を許容す

るレベルでの安全でしかない。ISO 規格、IEC 規格は全世界からエキスパートが集まって議論して決めるのであるから、それでよいという論理もあろうが、ISO 規格、IEC 規格は安全の教科書ではなく――繰り返しになるが――、流通を許可するための条件である。だから、設計者は、それでよしとしないで、その製品（機械、設備、玩具、家電品など）を使う人を思いやる気持ちを持つことが、安全な製品を生み出すために必須だと思う。会社の設計担当者なら、設計基準に従えばよし、だけではなく、設計基準を改善することも考えてみていただきたい。

ここまで書いていて、技術者倫理要綱を思い出した。公衆優先の原則は、法令や規格を遵守するだけでなく、加えて使用者の安全を最も大切な判断基準とすることを求めていると思うが、性能と安全性が相反するといった場合でなくても、意識しておきたい。

ちょっと話題を変えるが、IAEA（国際原子力機関）が、安全文化への取組の中で、国際原子力安全諮問グループが出した報告書 INSAG-4[6)]がある。その冒頭に、次の一節がある。（下線は筆者が記入した。）

> “神の仕業”といわれるようなことを除けば、原子力プラントで起きるどのような問題も、何らかの人間の誤りから生じる。
>
> それでも、人間の心は、潜在する問題を探知し除去するのに大変有効であり、安全に対して積極的で重要な影響がある。それゆえ、個人には重い責任がある。

INSAG-4 は、原子力の安全文化についての文書である。原子力のように設計だけでも、施工だけでも、運転だけでも多人数が関わる産業においても、個人、つまり参画している技術者一人一人の影響が大きいから、重い責任があるといっている。簡単にいえば、「危ないと思ったら、従前通りであっても、設計標準通りであっても、手順書通りであっても、先ずは指摘せよ、ということであろうと、私は考えている。

なお、ここで重い責任の原文は“heavy responsibility”である。つまり、職務上のことに応答するということで、事が起こってしまった後に責任をとって辞職するということではないように思う[脚注 1]。スペースシャトル・チャレンジャー号事故におけるボイジョリー氏などは、この責任を果たそうとした。

3. まとめ

今まで記したことを要約すると、次のようになる。

1．規格は通商のための基準を示した文書であって、安全の教科書ではない。よって、理想的な安全を提示しているわけではない。
2．規格を正しく理解して適用すること、それ以上の安全を目指すことには、技術が必要である。
3．しかし、技術は持っていてもリスク低減しようとする意思がなければ、規格に従って許容可能なリスクまでリスクを低減する以上のことはしない。だから、倫理観が問われる。
4．使う人に死亡あるいは重篤な傷害を負わせてはならないという技術者としてのプライドと倫理観を持ち続けたい。

ここまで私の感じたことを記しました。冒頭に「技術を知らなければリスク低減はできず、倫理感がなければリスクを低減しない」と記しましたが、要は、単なる歯車の一枚になってはいけないということです。どのような職務分担でも、製品の安全、作業の安全に関わる懸念は、発言するということです。

---

[1] 辞書によれば、responsibility には、（事故・過失などに対する）責任、という意味もある（小学館 プログレッシブ英和中辞典）。しかし、INSAG-4 冒頭の意味は応答する責任のことであろうと思う。

本稿が多少でも参考になれば幸いです。本冊子の読者の皆さまには、ご自身のお仕事について、安全とは何かを常に意識して頂き、安全を向上するように思考して頂きたいと願っています。

謝辞　INSAG-4 については、技術士の杉本　泰治　氏（T.スギモト技術士事務所）に多くを教えて頂いきました。INSAG-4 冒頭部分の翻訳も同氏によります。ご指導に謝意を表します。

参考文献

1) ISO/IEC Guide 51:2014, Safety aspects – Guidelines for their inclusion in standards
2) JIS Z 8051:2015, 安全側面－規格への導入指針
3) ISO (International Organization for Standardization): My ISO Job (2018), https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/my_iso_job.pdf (2022 年 12 月 23 日確認)
4) ISO/IEC Guide 2: 2004, Standardization and related activities – General vocabulary
5) JIS Z 8002: 2006, 標準化及び関連活動－一般的な用語
6) IAEA: Safety Culture, Safety Series No. 75-INSAG-4 (1991)

新しい時代の安全“協調安全”

日本認証株式会社
一般社団法人　セーフティグローバル推進機構
松 浦 裕 士

１．はじめに

第４次産業革命 Connected Industries 時代の到来とともに ICT(情報通信技術)の進歩により、IoT、AI、ビッグデータ、クラウドなどの技術が発展し、あらゆるものが互いにつながり始めている。この技術革新が生産現場に適用されると、生産性を上げ、柔軟な生産を可能となり、産業のあり方が大きく変わると言われている。

協調安全は、ICT 技術を安全機能に対して活用できないかという発想から生まれた新しい安全の考え方である。ものづくり現場では協働ロボットの普及に見られるように、機械と作業者との協働、協業作業のニーズが増加している。しかしながら、ものづくり現場に限らず、人と機械が同じ空間、時間で作業する現場においては、従来の安全の考え方である物理的な手段で、人と機械が隔離することは現実的ではない場合も多くある。

このような状況を鑑み、人と機械が同じ空間において作業する現場において、人と機械との隔離による安全対策のみに頼らずに、人と機械の協働や協調作業を可能にする新しい安全の考え方である“協調安全 (Collaborative safety)”を紹介する。協調安全は人と機械が対立するのではなく協調して新しい産業社会の実現を目指すものであり、人、モノ（機械)、環境など各構成要素が、ICT などを用いてリスクに

関係する情報（危険／安全情報）を共有することにより、自律的（自身）あるいは他律的（周囲の人やモノ）な制御により作業効率を維持・向上させながらリスクを低減するという新しい安全の考え方である。

２．安全の変遷

一般社団法人セーフティグローバル推進機構（以下 IGSAP）が提唱している安全対策の変遷である「Safety 0.0」、「Safety 1.0」、「Safety 2.0」について紹介する。

機械設備における安全技術を振り返ってみると、機械がものづくりの現場で使用されると、機械の持つ高いエネルギーにより巻き込まれ、切断や押しつぶしなどの労働災害が発生した。機械による労働災害を防止する為に、作業者に危険源、危険事象を知らして注意を促す危険予知や指差し確認など作業者の注意による安全を「Safety0.0」と呼ぶ。次の段階は、欧州から始まった危険源である機械を、設計時に安全化技術を活用し安全化を実現する機械安全を「Safety1.0」と呼ぶ。機械安全の設計原則は、災害の多くは人の作業空間と機械の作業空間が重なり合った危険領域で発生するので、この発生メカニズムが設立しないように、「隔離の原則」、「停止の原則」に基づいて安全を確保するという考えである。「Safety1.0」段階における安全化技術も電気安全、制御安全、機能安全などの新しい技術が開発され、普及してきている。

更なる段階として、人、モノ、環境が ICT などにより情報を共有して、お互いに協調して安全を実現する新しい安全の考え方を、協調安全「Safety2.0」と呼ぶ。なお、協調安全という安全の考え方は提唱されてから間もないので、現在は国際的にコンセンサスを取っている段階であり、国際会議などでの議論を通じて用語や考え方などが明確化、具体化していくと考える。

図１　安全の変遷

３．協調安全の特徴

協調安全のリスク低減方策の特徴について説明する。

①人は、リスク低減に貢献出来るという考え方に基づき、人に適切なタイミングで具体的な危険情報を提供することによりリスク低減やリスク回避を実現する。

②危険源が停止させる前に、人の退避行動あるいは機械の回避動作により危険状態を避けて、出来るだけ機械を保護停止する前に危険状態を回避する。

③作業者の力量、経験などによって危害回避の可能性が変わるという考え方に基づき、作業者の力量、経験に基づいて機械の制御は２値制御（停止、稼働）から多値制御を実現する。

④リスクアセスメントでは、静的、動的要素を考慮するとともに、人

によるリスク低減、回避策を実施する場合は、人の行動分析による妥当性確認を実施する。
⑤リスク低減とは直接関係はないが、ICT などを活用した安全の見える化により、人の体調や作業場所、機械の状態を常時モニタリングが可能となる。

ここで上記 5 項目について少し補足説明する。
①機械安全では、「人は間違える」ということで人がリスク低減に貢献することに大きな期待はしていないですが、協調安全では人の能力をリスク低減に活用することを考えている。しかしながら、人の咄嗟あるいは反射的な危険回避動作は、人によって多様であり、反応時間もまちまちであるので、危険回避の最終段階では人の行動に委ねるべきではない。人によるリスク低減行動は、作業者が間違わないように適切なタイミングで的確な情報を提供して、危険につながる間違った行動をしないようにすることである。また人の能力を活用することは、人のやりがい、生きがいにもつながると考える。
②下記図 2 が危険源（ハザード）から危害（ハーム）に至るメカニズムを表している。通常危害が発生する場合は、いくつかの開始メカニズム(Initiating Mechanism)を経由して危害が発生すると考える。例えば危険源であるロボットが防護柵によって隔離されている現場では、作業者が防護柵のドアを開けて（IM1)、作業者がロボットアームの稼働範囲に侵入（IM2）して、そしてロボットアームが作業者と衝突するエリアで稼働し衝突時（IM3）に始めて危害が発生する。センサや ICT の活用によって、人の位置、機械の動作位置がリアルタイムに継続的に把握出来るようになれば、ロボットを保護停止する前にロボットアームが人と接触しないように回避あるいは一定の距離を保つ動作が可能となり、IM 1 や IM2 ではなく、IM3 で初めてロボットを停止させても、安全確保が出来ると考える。

図２．ハザードからハームまでのメカニズム

③昨今の新しい国際規格においては、作業者の力量、経験の違いによる、リスク回避の可能性について議論されている。協調安全では、この考え方に沿って機械の運転速度を、従来の「停止」「稼働」という２値制御から力量、経験の違いによって「停止」「低速」「中速」「高速」などの多値制御も可能になると考える。
④①、③で説明したリスク低減策を取り入れるならば、リスクアセスメントにおいて、それぞれリスク低減策の妥当性を確認する必要がある。とりわけ機械安全のリスクアセスメントは機械を中心とした考え方であり、人のリスク低減行動については十分な妥当性を確認していないので、人の行動分析による妥当性確認が必要と考える。
⑤人のバイタルデータなどを常時監視することにより、急な体調変化も確認できるやさしい現場になる。また機械の状態を連続監視することによって故障予知など機械設備の保全にも貢献できると考える。
　本章で協調安全のリスク低減策について紹介しているが、リスク低減策については、ISO12100 で要求されている３ステップメソッドの第１ステップである本質的安全設計方策を優先すべきであり、多くのアプリケーションにおいては、協調安全のリスク低減策は機械安全、機能安全や作業安全のリスク低減策とともに活用されると考える。

４．協調安全のアプリケーション紹介
　協調安全の対象市場としては、製造現場以外に建築、土木、農業、物流など幅広い市場で活用されると考えている。
とりわけ、人と機械の作業領域の分離がむつかしい建設、土木、農業

などの分野からの期待感は高い。
今回、協調安全の概念に基づいたリスク低減策の活用事例について２件を紹介する。

4－１　人と機械が協調する生産ライン

１）　生産ラインの説明と安全上の課題

人と機械を物理的に分離せず、人と機械がお互いに協力して、人手不足や作業品質のばらつきを解消し、変種変量生産にも対応する柔軟性と生産性を両立した生産ラインにおける、協調安全のリスク低減策を紹介する。

本生産ラインは、製造品の生産ラインでの工程位置を検知し、作業者に作業指示や異常発生を通知する。また、天井カメラによって作業者の位置情報も検知し、その位置情報と製造に関する様々な情報とを組み合わせて工程の進捗を可視化している。

図３　人と機械が協調する生産ライン

作業性を考慮した場合は、人と機械の作業空間を分離する物理的な防護柵が設置出来ないことから、人と機械の接触が発生しやすいことと本ラインへの部品の供給は、工程間を自律走行するマニピュレータ付きのモバイルロボットで行う為に、生産ラインの周囲を覆う物理的な周囲ガードを設置出来ないので、第三者の侵入をいかにして防ぐかという２つの課題がある。

２）　今回機械安全によるリスク低減策とともに採用した協調安全のリスク低減策について紹介する。

①作業者の力量、熟練度に合わせたロボットの速度制御リスクアセスメントを実施して、作業者の力量、経験（熟練者、非熟練者）に合わ

せた最適な速度でロボット稼働する（多値制御）。本制御を使用することにより、作業者の力量を考慮しない場合（誰もが回避可能な低速度でロボット）と比べて作業者の力量、経験に応じたロボットの速度設定により、作業時間の短縮効果がある。具体的な使用方法を説明すると図 4 のように、作業者は作業開始前に ID カードに登録されている力量、経験レベルを読み取らせて、表示器に表示されるロボットの動作速度レベルを作業者は確認する。協働ロボットは、作業者のレベル毎に設定された動作速度（安全制限速度機能で制御）で稼働するが、ロボットの稼働前に音声で力量、経験に応じたの速度レベル設定されていることを念のため、稼働前に作業者に知らせる。

図 4　作業者の力量確認

図 5　作業者の力量に応じた速度稼働

②危険領域侵入者への警告による自発的な退避行動

周囲ガードが無いために、作業中に生産ラインに従事しない第 3 者が何気なく稼働しているロボット周辺の危険領域に侵入した場合は、セーフティレーザセンサ(SLS)により第 3 者の侵入を検知しロボット含めて生産ラインは停止する。上記の安全対策で安全は確保できるが、ライン停止後の再稼働に時間がかかるという生産性への課題がある。今回天井カメラにより人と物とを区別して、侵入者が危険領域に接近した場合、第 3 者の侵入者に対して退避を促す警告（音声と表示）を発信して、SLS による保護停止前に、侵入者自らが気づき退避することにより、停止による生産性の低下を防止する。

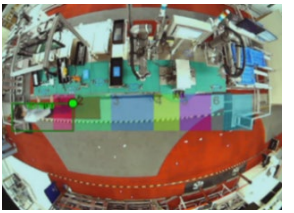

図６作業者の位置確認

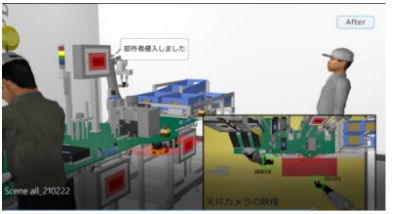

図７天井カメラによる侵入検知

4－２　人と自律移動ロボットの協調安全システム

自律移動ロボットの走行路は、作業領域とは分離してなく作業者との共存空間であるため、機械安全のリスク低減方策に加えて、協調安全の考え方に基づいたリスク低減方策も導入することにより、安全と生産性が両立する。自律移動ロボットと作業者の動線が複雑に交差するため、自律移動ロボットとピッキング作業を行う作業者が、接触、衝突するリスクが常に存在する。そのため作業者は、ロボットの動きに常に気を付けながら作業することになり、作業者の不安や作業効率の悪化が発生する。また自律移動ロボットが作業者接近時に安全確保のために設置されている SLS により停止する。本機能によって安全は確保されるが、自律移動ロボットが停止を繰り返すことによる走行時間が長くなるという課題を抱えている。今回、２つの協調安全の考え方に基づいたリスク低減策について紹介する。１つは自律移動ロボットが危険領域の手前で作業者を検知した際には、グラフィカルライトにより、作業者にロボットの接近と進行方向を知らせて、作業者自身の退避行動により、自律移動ロボットの SLS による停止を回避する。

もう１つは、自律移動ロボットに設置している LiDAR(Light Detection and Ranging)が作業者を検知した場合は、自律移動ロボットの衝突回避動作により、作業者との衝突を回避して自律移動ロボッ

トが停止しないようにする。なおLiDARの故障などにより回避動作が上手く動作しなかった場合は、SLSにより作業者との衝突前に自律移動ロボットが停止する。

図８　進行方向表示

図９　回避動作

５．我が国からの標準化活動

協調安全は、日本発の新しい安全の考え方で、現在、研究機関、機械メーカ、ユーザでテストトライアルあるいは運用が始まっており、リスクアセスメント、リスク低減方策などの検討、運用を開始している段階である。今後国際的に、協調安全の考え方、協調安全のリスク低減策が普及するためには国際標準化が必要と考え、2019年度から経済産業省の支援頂き標準化活動を開始している。

日本発の協調安全を国際的に認知頂くために、2018年10月にフランスで開催されたSIAS2018（International Conference on Safety of Industrial Automated Systems）において、IGSAP向殿会長から「Japanese approach for the realization of Future Safety Concept by implementing collaborative safety technologies」という題目で協調安全を紹介し、2020年11月にIEC(International Electrotechnical Commission:国際電気標準会議）からIEC白書「Safety in the Future」が発行され、将来の安全として協調安全を

取り上げられた。IEC 白書の発行を契機に IEC において、協調安全のガイドあるいは規格化の検討が始まっており、日本からも検討タスクフォースに参画している。今後、IEC はじめ国際標準化団体で、協調安全に関する様々な規格が制定されることにより、国際的に協調安全が普及することを望んでいる。

参考文献

１．日経 BP 社　Safety2.0 コンセプト編（2015）
２．向殿政男　　Safety2.0 とは何か？：中央災害防止協会（2019）
３．向殿政男　　一橋ビジネスレビュー2019 年　WIN　8－17（2019）東洋経済新報社
４．Clifton A. Ericson, Hazard Analysis Techniques for System Safety, Wiley,P14,P19 （2005）
５．令和 2 年度経済産業省受託事業報告書（2021）

AUTOSAR：モビリティの提供を「継続可能」とするためのプラットフォーム

イーソル株式会社
櫻 井　剛

※本稿は、2022-07-02 に開催された第 25 回 安全安心社会研究センター 特別講演会での筆者による講演「AUTOSAR：モビリティの提供を「継続可能」とするためのプラットフォーム」の要旨である。

1. はじめに

自動車 1 台当たりのソフトウェアの規模は指数関数的に増大し、ソースコード行数は今や 1 億行にもなろうとしている（図 1）。

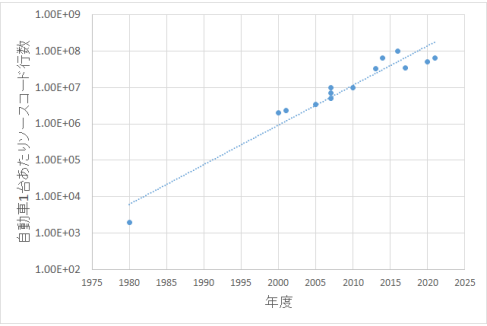

図 1：自動車 1 台当たりソースコード行数の推移
（文献（1）～（6）に基づき筆者作成）

自動運転の本格的な市場での普及を支える要素技術の 1 つである AI の導入に伴い、ソフトウェアの規模をソースコード行数だけで測ることはもはや適切ではないが、「規模・複雑さ」の増大傾向が続くことは明らかであり、また不可避である。この状況下でモビリティ提供を持続可能にするためには、各社個別での局所的な取り組みだけではなく、業界全体での横断的かつ継続的な改善が不可欠となる。

規模や複雑さとその増大への対処については、1990 年代には既に様々な試みが行われていた。ソフトウェア標準化に関しては、欧州の Herstellerinitiative Software (OEM Initiative Software) や OSEK/VDX (Offene Systeme und deren Schnittstellen für die Elektronik im Kraftfahrzeug / vehicle distributed executive) 等がその代表的なものであるが、個別機能要素レベルの取り組みにとどまっており (リアルタイム OS や通信、Network Management、Flash 書き換えなど)、ECU ソフトウェアやシステムアーキテクチャ全体を対象にしたものではなかった。また、自動車メーカーと ECU サプライヤの間では「標準化による再利用」に対するモチベーション面での温度差も存在していた。サプライヤ各社がプラットフォーム構築をすでに行っている中で、自動車メーカー主導で行われた標準化が、必ずしも win-win な関係をもたらすものではなかったことや、関心領域・価値を見出す領域の違いがその一因と考えられる。

これらの流れを受け、2003 年に設立された開発パートナーシップが AUTOSAR (AUTomotive Open System ARchitecture) である。標準化されたソフトウェアフレームワークとオープンかつ「実際に利用される」ような電気・電子 (E/E) システムアーキテクチャを開発し確立することを目的とし、自動車業界やそれを取り巻く様々なプレイヤー (自

動車メーカーだけではなく ECU サプライヤやシステムインテグレータなどの各階層の企業・団体・教育研究機関）が全世界から参加しており、以下に示すような広い範囲の活動が行われている。

1) ソフトウェアアーキテクチャの標準化
2) ワークフローとデータ交換形式の標準化（Methodology）
3) 各種インタフェースの標準化（Protocol、Application Interface、Sensor Interface など）
4) コンフォーマンステストやアクセプタンステストの標準化（現在は活動休止）
5) コード実装による実証（後述の Adaptive Platform（AP）のみ）

普及状況に関しては、自動車メーカーの販売台数上位22社のうち、Tesla 社を除く 21 社が AUTOSAR に加入しており、また、2008 年頃からすでに市販車に広く導入されており、自動車以外の派生分野（例えば、船艇や発電機など）での利用も行われている（7)。

また、ASAM、CAIFS、COVESA（旧 GENIVI）などの他標準化団体との提携も進められている。国内の JASPAR との間でも、連携強化のための覚書が2022年に取り交わされ、地域固有の活動の AUTOSAR Regional Hub in Japan も立ち上げられた（8)。また、Software Defined Vehicle（SDV）や Mobility as a Service（MaaS）では車外の各種インフラ・サーバとの連携も必要であり、そこに登場する様々なインタフェース（Vehicle API）定義の議論も進められている（10)。

2. 車両電気電子 (E/E) システムおよびECUソフトウェアアーキテクチャ

自動車でのE/Eアーキテクチャは、サプライチェーンの成長過程や後方互換性面の制約の影響を多分に受けながらこれまで進化してきた。新車種だからといって、すべてが再度新規開発されるわけではなく、既存車種からの多くの「再利用」や車種間の「共通化」が行われることから、殆どの自動車はECUを単位としたモジュラー型開発が進み、1台あたり数十から百以上のECUが、車内ネットワークで相互接続されるような分散型E/Eアーキテクチャを採用している。しかし近年は、電動化などによるE/Eシステム構成の劇的な変化や、開発方式の転換もあり (SDVへの移行の背景には、強力なツール支援の下で、モジュラー型開発での「単位」を、従来のECUから、車内外を含めたソフトウェアに切り替えることが容易になったことなどもある)、ECU統合を含むアーキテクチャ・開発ワークフローの全面的な見直しが進められている (7)。Tesla社のように集中制御型E/Eアーキテクチャを採用する場合もある (9)。

さて、ECUのそれぞれの役割は大きく異なるが、表1に示すような各種観点で分けると、従来から用いられてきた制御系ECU、IVI (In-Vehicle Infotainment) 系ECU、そしてAD / ADASで新たに登場したECU (いわゆるVehicle Computerなど) の3種類に分けることができる。

表 1: ECU の 3 分類とそれぞれの性質

	従来型の制御系 ECU	ADAS / AD で新たに登場した ECU	Infotainment ECU
リアルタイム性の要求	高（us オーダー）	中～高（ms オーダー）	低（sec オーダー）
ECU の価格/利益率	低い利幅で固定化	それなりの価格/利幅?	低い利幅で固定化
		（但し押下げ圧力大?）	（車内の位置付けは?）
想定する安全面の要求	ASIL D まで	ASIL B～D	QM 以上 ?
演算能力の要求	低（~1k DMIPs）	高（>20k DMIPs）	中～高（~10k DMIPs）
動的な動作のサポート	不要（忌避）	“Planned Dynamics”	必要
起動時間の要求	短（ex. 数十～200ms 以内に送受信可能に）	短～中	長
			（数秒かかってしまう）
通信面の要求	比較的低速な	V2X などへの対応	各種
	シグナル指向のコネクションレス型通信	サービス指向通信が中心に	

OTS/OSS の利用	少ない	あり～多数	多数
一般に採用される PF	・スケジューラ ・OSEK/VDX OS ・AUTOSAR CP	・ AUTOSAR AP (POSIX PSE 51 プロファイル)	・POSIX の各種プロファイル ・AUTOSAR AP

AUTOSAR 登場当初は、相対的に ECU 数が多い制御系 ECU 向けに、ソフトウェアアーキテクチャ標準化が進められた（IVI 専用アーキテクチャについては､AUTOSAR 内での標準化ニーズが少なく対象から除外)。

その後、自動運転の実用化が視野に入ってきた 2010 年代中頃に、従来の制御系 ECU よりも高性能かつ動的な構成が求められる AD / ADAS ECU 向けのソフトウェアアーキテクチャやその開発の進め方(Methodology)、さらには標準化活動の進め方や範囲の見直しも含めた議論が行われ、2017 年に Adaptive Platform（AP）仕様の最初のバージョンがリリースされた。

AP 登場を機に、それまでの AUTOSAR の制御系 ECU 向けソフトウェアアーキテクチャは Classic Platform（CP）と呼ばれるようになり、また、CP / AP 共通の仕様群（たとえば通信プロトコル仕様など）は Foundation（FO）として切り出されている。

表 2: AUTOSAR CP / AP の基本機能ブロック

機能	BSWs in CP (主なもの)	FCs in AP (●: Foundation, ★: PF Service)
動作モードに基づく、各種処理の実行制御 (ライフサイクル管理) 及びメモリ空間分離	BswM EcuM, RTE Os	★**ara::sm** State Management ●**ara::exec** Execution Management ●**POSIX PSE51 / C++ STL** Operating System Interface
動作監視	WdgM, WdgIf, Wdg	●**ara::phm** Platform Health Management
通信、通信保護、および通信チャンネル毎の通信動作制御	ComM, <*Bus*>SM E2E, E2EXf, SecOC RTE, SomeIpXf, Com, Sd, PduR, SoAd, DoIp, TcpIp, <*Bus*>Tp, <*Bus*>If, <*Bus*>Trcv, <*Bus*> (Driver) 他 ※<*Bus*>: バス種別の略称。 Can (CAN), Lin (LIN), Fr (FlexRay), Eth (Ethernet), WEth (Wireless Ethernet), Ttcan (TTCAN)	●**ara::com** Communication Management (サービス指向通信, ECU間はSOME/IPおよびDDS on Ethernet only) ※AP では CAN / LIN / FlexRay への対応なし ●**ara::rest** REST (R21-11でobsolete)
Network Management	ComM, Nm, <*Bus*>Nm ※<*Bus*> 追加分: Udp (UDP)	★**ara::nm** Network Management
時刻同期	Os, StbM, <*Bus*>TSyn	●**ara::tsync** Time Synchronization
Log and Trace	Dlt	●**ara::log** Log and Trace
診断 (Diagnostics)	Dcm, Dem, FiM	●**ara::diag** Diagnostics
不揮発メモリアクセス	NvM, MemIf, Ea, Eep, Fee, Fls, BndM, MemAcc, Mem	●**ara::per** Persistency
インストール・更新管理	(該当なし)	★**ara::ucm** Update and Config Management
アクセス権限制御	(しいて言えばOs SC3/SC4)	●**ara::iam** Identity and Access Management
暗号サービス	Csm, CryIf, Crypto, KeyM	●**ara::crypto** Cryptography
侵入検知	IdsM	●**ara::idsm** Intrusion Detection System Manager
I/O制御	I/O Hardware Abstraction, Dio, Icu, Ocu, Adc, Pwm 他	(該当なし)

(C) 2022 Tsuyoshi Sakurai

CP / AP のそれぞれが提供する基本機能ブロック (前者は BSW: Basic Software、後者は FC: Functional Cluster) の概要を表 2 に示す。これらは、どの自動車メーカー向けか、どのサプライヤが作ったか、どの種類の ECU 向けかに関わらず一般的に使われるものであり、これらを用いて各種アプリケーションを実現している。

なお、制御ソフトウェアは高度な処理を可能にするが、直接には、ごく僅かな種類のマイコン入出力部（汎用 I/O，アナログ，パルスおよび通信）だけを制御して、マイコンの外とつながっている。それらにより様々なセンサーの情報を取り込み、アクチュエータを制御している。実際の制御対象のプラントなどはそれらのセンサー・アクチュエータを介して制御される。一般に制御ソフトウェアの開発では、高度な制御をいきなりマイコン入出力レベルで記述するのではなく、{マイコン入出力レベル，センサー・アクチュエータレベル，プラントレベル} などの階層モデルとその階層での制御を行うためのインタフェース定義（Vehicle API などの API）を用いて、段階的な抽象化・具象化を行うことが多い。プラットフォームという概念そのものがカバーする範囲やインタフェースを提供する範囲も多様であり、今後はより抽象度の高いレベルでの定義の標準化も進むものと考えられる。

3. Methodology

自動車に限らず大規模なシステムの開発においては、複数の異なる関係者による分担（分散開発）やツールによる支援は不可欠である。ワークフローの分担やツールチェインの切り替え点ではデータ交換が行われることから、ワークフローやデータ交換形式は分業やツール支援の基本的な枠組みを支配するものである。

AUTOSAR では Methodology and Templates として規定され、データ交換は XML をベースにした「AUTOSAR XML（ARXML）」が用いられている。

4. 各プラットフォームの概要

4.1. Classic Platform (CP)

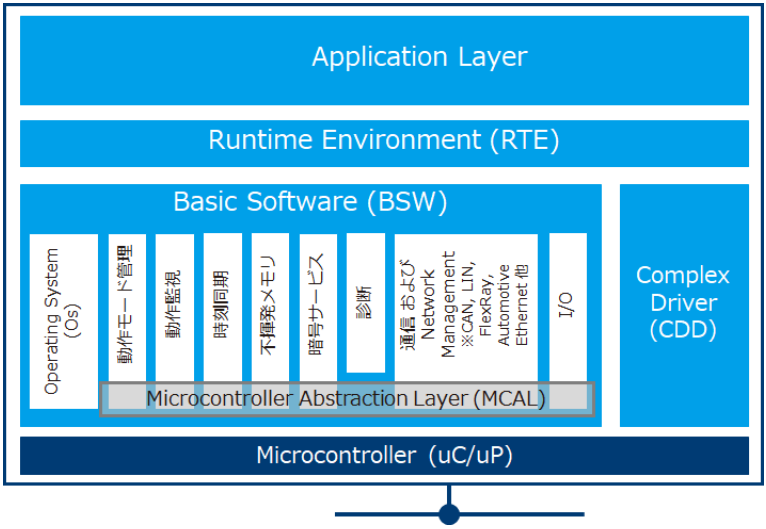

図 2: Classic Platform (CP) アーキテクチャ

CP では、いわゆる制御用マイコンの上に、Basic Software (BSW)、Runtime Environment (RTE)、Application Layer が順に載る構成としている。なお、これらの制御用マイコンでは一般に Memory Management Unit (MMU) を持たず、全アプリケーションが共通メモリ空間を使用する。メモリ空間分離が必要な場合には、Memory Protection Unit (MPU) が一般に利用される。また、64 ビット変数のアトミックアクセスができないような16ビットマイコンについては、

近年利用実績が殆どないことが AUTOSAR での標準化活動にて確認されており、2021 年発行の最新バージョン（R21-11 と呼ばれる）からは正式に対象から外された。

BSW は、どの自動車メーカー向けか、どのサプライヤが作ったか、どの種類の ECU 向けかに関わらず一般的に使われる基本機能ブロック（表 1）をハードウェアなどへの依存度合いに応じて階層化・分割した、約 100 個のモジュール群である。多種多様なユースケースに対応できるよう、その振る舞いやインタフェースなどを多数の設定パラメータにより切り替えることができる。上流設計情報（車両ネットワーク設計や診断機能定義、および、Software Component（SW-C）のインタフェースや振る舞いの定義）を用いた RTE / BSW パラメータの一部の自動設定も可能である。また、市場に存在するマイコンの CPU Core や周辺機能群は多様であることから、それらに対する依存性を、Operating System（Os）とドライバ部分（Microcontroller Abstraction Layer: MCAL）で吸収するようになっている。なお、当初は、BSW 製品をモジュール単位で異なるベンダーから調達することも想定していたため、モジュール分割での高度な細分化とそれぞれの間でのインタフェース定義、具体的な実装に踏み込んだ記述がなされてきた（このことで、標準化活動において変更の影響の見落としや、検討所要時間の増大などの問題も発生しやすくなっている）。しかし実際には、Os や MCAL を OS 専業ベンダーやマイコンベンダーから調達することはあっても、それ以外の BSW は、ひとまとめにしたパッケージとして調達することが圧倒的に多い。

RTE は、SW-C 間、SW-C / BSW 間の通信を実現し、また、SW-C や BSW 内の関数を実行するための環境（排他制御メカニズムなど）を提供する。

Application Layer は、BSW として標準化されない、システム・ECU

固有の振る舞いを実現するための Software Component (SW-C) の集合体である。個別の SW-C は通常 C プログラミング言語で記述され、ECU への配置や相互間の接続経路 (ECU 内、Memory Partition 間、CPU Core 間、ECU 間: 車載 Ethernet や CAN、LIN などの各種ネットワーク経由) の変更からの影響を受けずに再利用できるようになっており (経路の抽象化: RTE および適宜通信関連 BSW の組み合わせによる)、ECU 機能統合などを比較的容易に行うことができる。SW-C 群のつながり (SW 論理アーキテクチャ) は、車両 E/E システム (物理アーキテクチャ) とは独立して定義可能であり、後に論理と物理の対応付けを行うこともできる。これにより、従来よりも高度な SW-C の再利用管理を、自動車メーカー主導で行うことも可能となる。

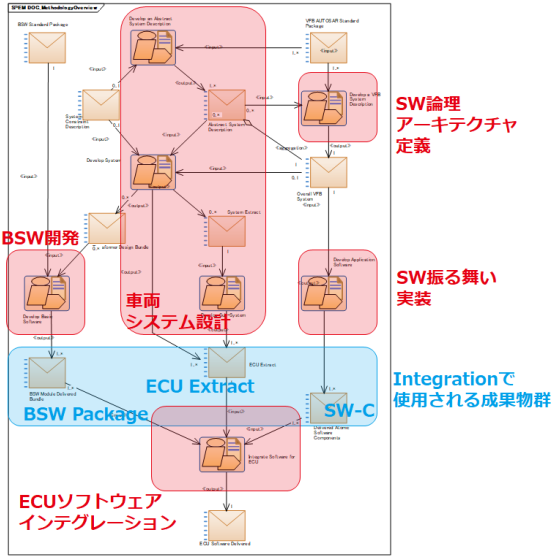

図 3: Classic Platform (CP) Methodology

おおよそのワークフローと主要なデータ交換を図3に示す。実際の開発の進め方は自動車メーカーやECU種別により差異があるが、以降、一般例を述べる。

BSW は予め開発済みのものを調達し利用する （業界全体での再利用）。

通信ネットワーク定義情報を含む車両 E/E システム （物理） の定義は自動車メーカーが行うが、SW-C 個別のインタフェース定義や SW 論理アーキテクチャ定義については、AUTOSAR 登場以前と同様に、要求仕様と通信ネットワーク定義情報に基づき ECU サプライヤなどが行うことも可能ではある （自動車メーカー主導の SW-C 再利用管理による効果を積極的に利用しない場合）。これら上流設計 （論理、物理とその対応付け） の情報は、全体情報から個別 ECU に必要な情報だけを抽出し、ECU Extract と呼ばれるデータとして提供される。

SW-C の振る舞い（コード実装など）は、機能要件と SW-C 個別のインタフェース定義があれば定義できる。SW-C に含まれる各関数 (Runnable Entity と呼ばれる） のトリガ条件などは、SW-C description と呼ばれるデータとして記述され、後の ECU ソフトウェアインテグレーション段階での RTE 自動設定などに利用される。

各データには、必要な機能や通信経路、物理配置など各所に登場するバリアント定義情報を含めることもできる。

ECU ソフトウェアインテグレーションは、BSW、ECU Extract および SW-C に基づき行われる。CP でのインテグレーションは、搭載される機能を考慮しての、起動やイベント応答での時間制約、安全・サイバーセキュリティ面で必要な方策の選定・実現なども必要となるため、スキル要求が極めて高く、さらには、上流工程からのインプットに対する検証や修正提案なども必要となり、作業量の面での負担も大きくなりがちである。インテグレータの了承なしに BSW 選定やスケジュー

ル合意を行うことはプロジェクトマネジメント面では極めて危険となる。

なお、基本機能ブロックやデータ交換形式などの各種仕様は標準化活動での合意の結果である。BSW やツールなどの製品実装に必要な情報のすべてを網羅的に記述しているわけではなく、現実に必要となる程度の相互運用性の確保に重点が置かれている。また、標準化以前から市場に存在する個別製品での様々な実装を許容するためにあえて詳細を規定しない場合もある。個別製品の実装にあたっては、当然ながら、追加での具体化が必要になる。

4.2. Adaptive Platform (AP)

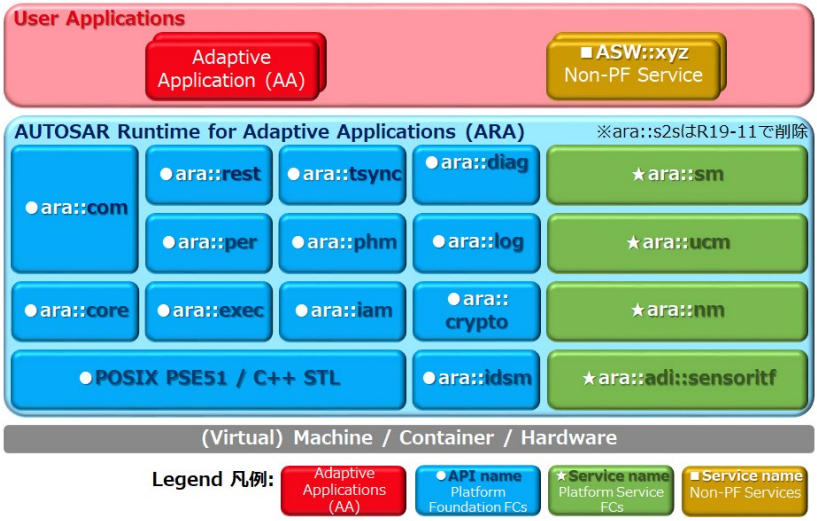

図 4: Adaptive Platform (AP) アーキテクチャ (R21-11)

AP では、MMU を搭載したプロセッサや System-on-a-Chip（SoC）の上に、POSIX OS（PSE51 profile）および Functional Cluster（FC）群から構成される AUTOSAR Runtime for Adaptive Applications（ARA）、User Application が順に載る構成となっている。いわゆる制御用マイコンとは異なり、プロセッサや SoC では MMU によりプロセスごとのメモリ空間が管理・分離され、また、相対的には制御用マイコンよりも演算性能が高くリソース規模が大きい。なお、ISO 26262 に基づく機能安全の対応では、現時点ではハードウェア入手性の問題から ASIL decomposition を用いることが多い。

FC については、基本機能ブロックとして提供する内容は CP とさほど違いがないが、比較的短期間で標準化を進める必要があった AP では、CP とは異なり基本機能ブロック標準化の粒度を大きくし、内部の実現手段に関する詳細を実装に任せている（R21-11 での FC 数は、今後廃止予定のものも含め 17 個）。

User Application は、FC として標準化されない、システム・ECU 固有の振る舞いを実現するための Adaptive Application（AA）の集合体であり、一般には C++プログラミング言語で記述される。なお、当初 C++の安全用途での利用に関しては懐疑的な見方もあり、MISRA C++（11）をもとに C++規格の改定版への対応も含めて安全関連 WG（WG-SAF）で議論が行われ、AUTOSAR C++コーディングガイドライン（12）が 2017 年に発行された。2019 年にはその検討作業の MISRA C++側への移管が決まり、2022 年 7 月現在、MISRA C++改訂版の発行に向けてレビューが行われている。また、Rust プログラミング言語対応の検討も行われている（7）。

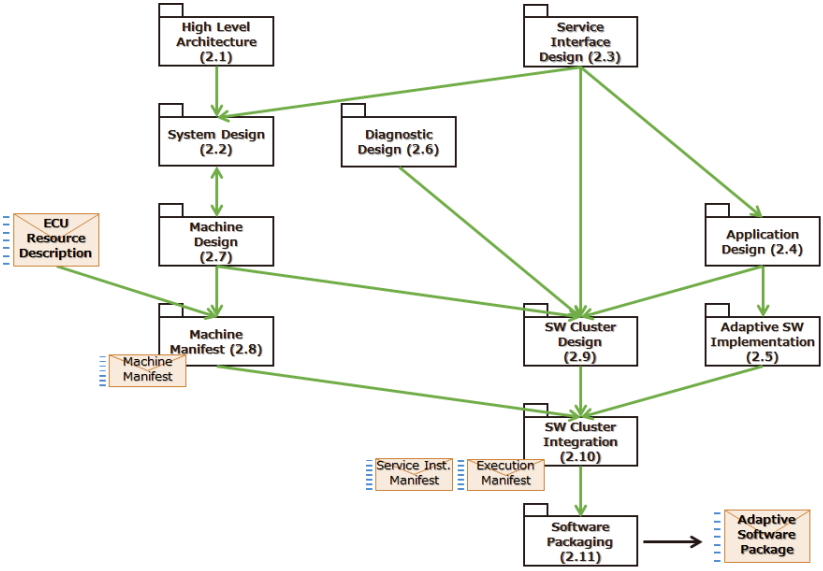

図 5: Adaptive Platform (AP) Methodology (R21-11)

おおよそのワークフローと主要なデータ交換を図 5 に示す。CP を用いた ECU を含む従来型の制御系 ECU の開発とは本質的な違いはない。しかし、CP でインテグレータに課されていた大きな負担の一部を、その前工程に振り分けるための各種試みが AP 標準化段階で取り入れられている。また、AP を用いた ECU では、自動車メーカーが開発主体になることが多いことも、CP を用いた場合との大きな違いである。

5. 運用

5.1. 人材育成および導入

組織側の AUTOSAR 導入の準備・組織整合の度合い（プロセスや、各種意思決定方法や評価判断基準を含むプロセスツールなど） が高い組織内での、SW-C のみの開発者ならば、必要な知識・スキルを絞り込むことは比較的容易である。

一方、特に CP のインテグレータは、前述のように必要知識やスキルが多岐にわたる。規模や複雑さの増大に伴い、「すべてを知り、経験する」ということは一層困難となる上、分業化が進むことにより、学びまた経験する機会は限定されている。計画的に機会を割り振ることをしたとしても、「こうすれば確実に育成できる」というシナリオが確立されているわけでもなく、また、組織整合の度合いにも大きく左右される。実際に AUTOSAR を初導入したプロジェクト関係者からは、技術面はもちろんのこと、組織整合できる環境の有無が大きく左右するとの声が聞かれる （導入推進者が本来持つ組織整合の能力がいくら高くとも、従来との違いを是とされなければ説得は困難）。ワークフロー全体にわたり各段階の活動内容と必要スキルを特定し、生じた様々な問題や困難に基づきそれらを見直しつつ、教育研修することが必要なのは当然のことだが、最初から「AUTOSAR プロジェクト関係者」と「それ以外」と単純に切り分けるだけでは、組織内対立が「システマチックなもの」として発生することを防げない。特に AUTOSAR に初めて対応する量産 ECU 開発プロジェクトにおいては、「新規の市販ソフトウェアモジュールの組み込み」という程度の認識でプロジェクトがスタートしてしまい、組織への AUTOSAR 導入準備の側面が見落とされることが多く、十分注意が必要である。

なお、国内では欧米に比べ RTOS 利用に対する抵抗が強く、Non-OS（あるいはスケジューラ型） と呼ばれる構造を現在も使っていることが少なくない。ISO 26262 自動車機能安全規格への対応をきっかけに、メモリ空間分離だけのために RTOS 利用は増えているとは言え、RTOS に関する知識を持たないベテランエンジニアが取り残されているケースも少なくない。一方、最初から RTOS をブラックボックスとして利用してきたエンジニアは、リスク分析の際に、RTOS 内部の動作把握や考慮 （スタックや汎用レジスタなどの実行コンテキストの退避と復帰などの、基本的な動作の詳細に対して） が困難な例も目にする。

組込みソフトウェア開発教育に関する議論は各所で行われているが、それ以前の「何をどのように分業していくか」が整理・明文化されていないケースもしばしば見受けられる。個別の差異がゼロではないからといって、前提条件と前提知識を定義しないままで行う教育の効果は当然低く、また、「教育に関する議論」では有効な結論を得ることが一層難しくなる。長らくソフトウェア開発のスタイルが変わらず、暗黙の常識に頼りがちな傾向がある現場では特に、「〇〇ができなければならない」のような要件特定・明文化や、他の要件との優先順位付けを、基準を定めて行うといった地道な活動に対して「非効率」のレッテルを貼ってしまいやすく、また、一足飛びに scrum などの「手段」に無目標・無思考で飛びつかせてしまうことも少なくないことに、注意が必要である。

5.2. 再利用と局所最適化との折り合い

再利用は、特段何をしなくともそれが可能になるわけではない。現実には、ISO 26262 が求める影響分析など何らかのコストがかかる。また、再利用すると言いながら局所最適化作業に多くの工数を割くこ

とが慣例化している場合には、「再利用するよりも、作り直した方が良い」という雰囲気が蔓延しやすくなり、再利用活動が形骸化しかねない。また、使用するマイコンの持つ機能や性能を限界まで利用し用途に合わせて細かく合わせこむような局所的最適化活動が、自社や自己の「強み」として肯定されてきた場合、標準化されたプラットフォームの利用や各種設計資産の再利用は、強みの発揮を阻害・制約するという否定的感情をも招く。再利用を促すためには、何らかの積極的な組織的施策が必要であり、その１つは、再利用と局所最適化に対する（できる限り、具体的な効果の測定に基づく）優先順位付けの明示だと考える。

5.3. 標準化、抽象化と、問題空間の分割、リスク・影響分析

複雑なソフトウェア構造を理解するには、抽象度の上げ下げ（段階的な抽象化・具象化とその行き来）が不可欠である。

構造化プログラミング（構造化定理）は、順序・選択・繰り返しの各制御構造を「ノード」に置き換えていったとき、最後に単一ノードが残るというものであるが、これもある意味では、複雑な構造を段階的に理解し、また関心領域だけに絞った議論を行うことができるようにするために、徐々に具象化していく手法であるとも考えることができる。処理内容と処理のトリガを分けるということも、スケジューリング問題や処理順序制約保証などを単独で議論できるようにするための方法である。詳細はここでは割愛するが、自動車分野では、2010年代後半からLogical Execution Time（LET）と呼ばれるスケジューリング手法に注目が集まっており、「マイコンやプロセッサの性能を限界まで引き出す」ことよりも「スケジューリングや情報の鮮度保証

を容易にする」ということの方がより重要視される傾向にあることをお伝えする。

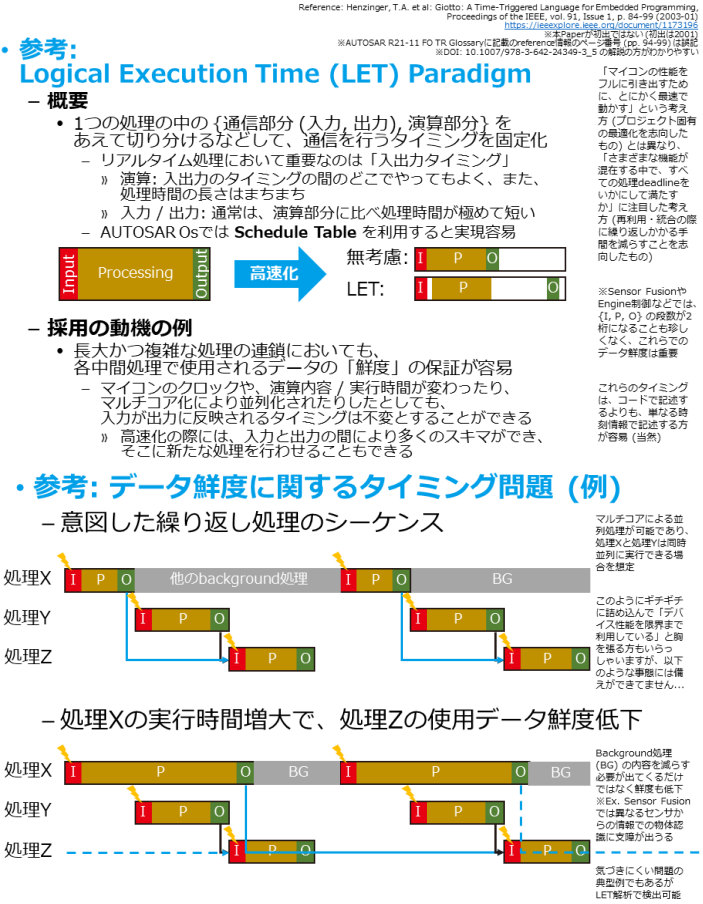

図 6: Logical Execution Time (LET)

また、先に述べたように、一般に制御ソフトウェアの開発では、高度な制御をいきなりマイコン入出力レベルで記述するのではなく、{マイコン入出力レベル，センサー・アクチュエータレベル，プラントレベル} などの階層モデルとその階層での制御を行うためのインタフェース定義（Vehicle API などの API や、通信ネットワークでの上位通信プロトコル定義）を用いて、段階的な抽象化・具象化を行われる。低い抽象度レベルでの処理内容に変更があっても、高い抽象度レベルでのインタフェースに影響が表れないのであれば、それよりも高い抽象度レベルでのリスク分析（安全分析）の結果をそのまま再利用できるといえる（接続先がどう振る舞おうと、相方となるこちらは、「インタフェースに現れるもの」以外の形で影響を受けることはない）。

インタフェースがプロジェクトごとに変わってしまうのであれば、リスク分析結果の再利用の効果はさほど高くならないが、標準化活動で合意されたインタフェースを採用しているのであれば、変わってしまう可能性は相対的に低くなる。実現する機能が変わらないのにアーキテクチャやインタフェースだけを見直すことは、一般的には得るものがないとみなされてしまいがちだが、後のリスク分析結果の再利用性向上という観点を見落とすべきではない。

この観点は、標準化活動に参加する意義にもつながる。安全機構などのリスク対応の標準化は、標準化活動でのわかりやすい成果となりやすいが（例えば AUTOSAR では、鮮度情報と検証コードに基づく通信保護メカニズムとして、End-to-End Communication Protection（E2E）プロトコルや Secure On-board Communication（SecOC）プロトコルを提供）、唯一の正解がなく似たものが乱立してしまいやすい階層モデルやインタフェースにおいて、業界内での合意が進めば、ひいては後のリスク分析結果の再利用性向上という成果につながっていく。

5.4. 標準化とプラットフォーム安全保障

標準化活動は、アーキテクチャや安全、セキュリティなどの機能横断的 WG（ワーキンググループ）、および、通信や時刻同期などの個別機能の WG に分かれて行われており、また必要に応じて合同での議論も行われる（7)。提案を行うのは自動車メーカーに限られるわけではなく、また、シーズ・ニーズのどちらも議論の起点となりうる。参加し機能削除や変更、追加などの動向把握・提案を行うには、年会費負担に加え活動工数負担の義務が伴う上位会員資格（Premium Partner 資格や、スタートアップ企業向けの Development Partner 資格など）を得る必要がある。

一方、標準化活動の成果物（AUTOSAR 仕様およびソフトウェアコード実装）とそこに含まれる各種知財の商用利用ライセンスを受けるだけであれば、年会費負担のみの Associate Partner 資格でよいが、以下のリスクがある。

基本機能ブロック自体は元来「当たり前に使うもの」であり、それにより実現される機能のうち必要なものが変わらなければ、積極的に変える価値は殆どないように見える。しかし、それらの機能が、標準化活動を通じて予期せず変更・削除されたとしたら、その上に構築された設計資産やその運用プロセスに重大な影響を及ぼしかねない。ましてや、先に述べたように、AUTOSAR では Methodology としてワークフローやデータ交換形式を規定しており、分業やツール支援の基本的な枠組みにも影響が及ぶ。標準化活動への実質的な参加を行わないのでは（元来標準化活動に参加することのできない、Associate Partner 資格の下での規格の「ユーザ」としての参加のみ、あるいは、Premium Partner など標準化活動に参加できる資格を持っていても、

WG での議論に不参加の場合)、合意の結果を毎年秋のリリースとして知らされるだけである。経緯・背景の情報も殆ど含まれず、反論の機会・糸口をつかむことは困難となり、実質的には受け入れるしかなくなる。

「基本機能ブロックを組み込む」のような目標を AUTOSAR 導入の第一歩に据えるのは決して間違いではないが、それは「AUTOSAR の利活用」の長期目標として据えてよいものではない。仮にそうしてしまえば、次のリリース後も過去の実績が有効となる保証はなく、再利用や自動化による効果から自らを遠ざけることにもなる。

「開発のよりどころとなっているプラットフォームを、使えるようにし、使い続けられるようにし、また、使いやすくする」ことこそが最低限の目標であり、そのためには、標準化活動にただ名を連ねるだけではなく議論に入り込み、手段（measures）だけではなく、それが実現しようとする要件（requirements）やその背景にあるユースケース（use case）についても共通理解を築き、さらに「ユースケースの存在」そして「ユースケースの持ち主としての存在」の認知（acknowledgment）を得ることが、「プラットフォーム安全保障」の観点からは必要と考える。

なお、最初から議論に入り込むことは容易ではないかもしれないが、手段で合意できない場合には、その上の要件やユースケースに立ち返るという方法をとることで一定の認知を得ることが比較的容易だったという経験から、以下の順序（AURUM プロトコルと命名）をご紹介する。

・(1=最も抽象的)（Assure mutual）Acknowledgment / Awareness（A）

議論の場に受け入れ（られ）る
・(2) (Agree on) Use cases (U)
ユースケースを共有する
・(3) (Agree on) Requirements (R)
実現しようとするゴールや要件を共有する
・(4) (Accept limited / compromised / constrained) Use cases (U')
ゴール / 要件の実際のカバー範囲の限界により生じるユースケースの制約・妥協点を受け入れる
(Hint: 受け入れようとするからには、そこに目を向けてみる必要がある - ただ受け流すのではなく)
・(5) (Agree on) Measures (M)
実現手段を共有する

参考文献

(1) 標準化で開発効率向上 車載ソフト巨大化に立ち向かう, 日経 Automotive Technology, 2007年10月号, pp.82-97 (2007) ※日産での規模推移
(2) The Hansen Report on Automotive Electronics (2013-07/08) ※Mercedes Benz S-Class 2014MYでの規模
(3) 「第4次産業革命スキル習得講座認定制度(仮称)」に関する検討会(第2回) - 配布資料 資料6 IT利活用分野について(自動車分野), 経済産業省 製造産業局 自動車課 (20170517) https://www.meti.go.jp/committee/kenkyukai/shoujo/daiyoji_sangyo_skill/pdf/002_06_00.pdf
(4) Jeff Desjardins: How Many Millions of Lines of Code Does

It Take? Visual Capitalist (20170208),
https://www.visualcapitalist.com/millions-lines-of-code/
(5) JASPAR 活動報告会 開会挨拶資料 (2021-03-11)
(6) JASPAR 活動報告会 開会挨拶資料 (2021-09-16)
(7) AUTOSAR: 公式 website (How to Join, About - Introduction Part 1: Organisation and Framework 及び History, AUTOSAR Open Conference 2022 資料, R21-11 Specifications 他),
https://www.autosar.org/ (参照 2022.07.23)
(8) AUTOSAR: AUTOSAR and JASPAR announce collaboration in strengthening standardization in the field of Automotive and Future Intelligent Mobility, https://www.autosar.org/news-events/details/autosar-and-jaspar-announce-collaboration-in-strengthening-standardization-in-the-field-of-automotiv/ (2022.05.10)
(9) テスラが常識外の“集中 ECU” 部品が激減、ヒューズは消滅, 日経クロステック,
https://xtech.nikkei.com/atcl/nxt/column/18/01267/00013/ (2020-04-27)
(10) AUTOSAR: AUTOSAR Opening Strategy - Software Defined Vehicle Ecosystem, https://www.autosar.org/news-events/details/autosar-opening-strategy-software-defined-vehicle-ecosystem-2022-may-05/ (2022.05.05)
(11) MISRA C++:2008 Guidelines for the use of the C++ language in critical systems (2008)
(12) AUTOSAR: AP R21-11 Guidelines for the use of the C++14 language in critical and safety-related systems (2021)

工学教育賞（業績部門）受賞

長岡技術科学大学　システム安全系　系長
安全安心社会研究センター　センター長　**門 脇　敏**

長岡技術科学大学システム安全工学専攻が、第 26 回工学教育賞（業績部門）を受賞した。本賞は、公益社団法人日本工学教育協会が、我が国の工学教育並びに技術者教育等に対する先導的・革新的な試みによって、その発展に多大の影響と貢献を与えた業績を表彰するために制定しているものである。表彰式は令和 4 年 9 月 7 日開催の日本工学教育協会第 70 回年次大会において行われた。

【受賞の概要】

受賞の対象となった題目は、「安全工学におけるリカレント教育 ―システム安全の考え方に基づく実践的プログラム―」である。

長岡技術科学大学は、平成 18 年度に大学院技術経営研究科システム安全専攻を設置し、社会人を対象とした安全に係る教育を開始した。そして、国内外の安全規格・法規の上に立ち、システムの災害、リスク及び安全の解析プロセスを対象に、安全技術とマネジメントスキルを統合して応用できる能力を持つ安全に対応できる専門職を養成した。輩出した修了生は、安全技術者のリーダーとして社会で幅広く活躍している。そして、令和 3 年度からは大学院工学研究科システム安

全工学専攻として、安全工学に関するリカレント教育を行っている。

システム安全の考え方をベースとした実践的な大学院教育は、我が国において唯一であり、非常にユニークなプログラムとなっている。これまでに 200 人以上が修了しており、多くが安全分野においてオピニオンリーダーとして活躍している。また、国内外の安全規格の作成に携わっており、我が国の安全を力強く牽引している。この様に、リカレント教育を通して、安全安心社会の構築に貢献している。

システム安全工学専攻は、システム安全エンジニア等の安全に関連する資格制度を主導しており、厚生労働省の通達においても資格制度の有用性が明記されている。加えて、学術研究で得られた知見を基として、安全に関する啓蒙活動を展開し、社会への積極的な情報発信を図っている。例えば、国の関連機関（消費者庁等）と協働して、その官署の職員にシステム安全の考え方を理解していただき、業務に活用していただいている。本専攻は安全に係るリカレント教育と社会活動を通して、「安全」の重要性を社会に幅広く浸透させている。

受賞者は以下の日本工学教育協会 HP（第 26 回工学教育賞受賞者リスト）より閲覧可能となっている。

https://www.jsee.or.jp/jsee/wp-content/uploads/2022/03/2021kyouikusyo.pdf

工学教育賞

ドローンの事故調査について

安全安心社会研究センター　客員研究員　五 十 嵐 広 希

近年，ドローンと呼ばれる小型の「無人航空機」が，農業や，保守検査，撮影，自然環境調査，災害対応，社会科学など多様な分野で利用が広がっている．ドローンは 2010 年代から急速に普及し，普及に伴い多数の人身事故が国内外で報告されている．2017 年に日本の建設作業現場で制御不能になった小型ドローン（機体重量約 1.4[kg]）が作業用クレーンに接触し，バランスを崩した後に作業員の顔に接触，数針を縫う事故，2020 年には農薬散布用のドローン（機体重量 16.5[kg]）を屋内でのメンテナンス作業中に飛行させバランスを崩したドローンのプロペラで小指を切断する事故など，多く報告されている．

日本では，2015 年より国土交通省に事故報告をする制度が始まり，2021 年度までに 8 件の人身事故が報告されている．一方で，国土交通省に未掲載の事故の報道もあり，調査をした結果 12 件の人身事故を確認した．未報告の事故としては，死亡事故 1 件，眼球破裂 1 件，指の切断 1 件など，軽傷とは言えない事故が含まれていた．この理由は報告が「義務」ではなく，「お願い」であったことが大きな原因と推察される．一方で，2021 年に航空法が改正され，2022 年に施工された新たな制度により，報告が義務となった．これにより精度の高い事故報告が期待される．

上記を踏まえ、2015 年以前の国内の事故情報について，国内では統

計的な報告は確認が出来なかったため，過去の新聞記事や症例論文等での網羅的に検索などの情報収集からの調査を実施した[1]．調査の結果，国内では古くは 1970 年からラジコンなどで事故が確認され，農薬散布用のドローンなどで，2021 年までに合計 64 件の人身事故が確認された．内訳として死亡事故 11 件，重症 10 件などが確認された．潜在的にはさらにある可能性も高いと推察される．

現在，海外の事故情報も継続して調査しており，調査結果をもとに今後のリスクアセスメントの事例や，リスクマネジメントの検討の材料として，安全で安心な運用に寄与させたいと考えている．

［1］五十嵐広希，国内における無人航空機の重大事故事例報告，第 51 回信頼性・保全性・安全性シンポジウム，2022

機械安全を学ぶ方々の変化

安全安心社会研究センター　客員研究員　今 枝 幸 博

小職は機械安全に関する講習会講師を 13 年担当してきた。ところで、早くから機械安全に関して関心を持っていた人々はどれほどであっただろうか。一つの指標として日本機械工業連合会が開催してきた機械安全の講演会への参加者数を見てみると 2006 年には約 200 名で、その後は開催テーマへの関心度合いで上下するものの、コロナが蔓延する前の 2019 年では 312 名の参加があった。13 年で 5 割の増加となっている。

日本で JIS B 9702 が発行されたのが 2002 年、JIS B 9700-1/2 が 2004 年であり、2006 年の講演会に参加された 200 名はこれらの規格を発行当初から追い掛けられてきた方々と思われる。この中から長岡技術科学大学大学院社会人コースへ進まれた、あるいはセーフティアセッサの資格などを取得され社内外で活躍されていらっしゃるであろう。さて、現在は 2023 年で、日本機械工業連合会講演会の初回から 17 年が経過した。先達は既に現役を引退されてシニアアドバイザー、または独立されて個人での技術指導をされている方も少なくないと思われる。

凡そ 5 年を経て次の世代への指導者になられるとすると、現在小職が講師を務める講習会に参加されている方々はその第 4 世代から第 5 世代だろうか。最近特に気付くようになったことをここで幾つかご紹

介したいと思う。

コロナ渦により対面からリモートでの講習形式になり、講習の修了後にメールにて何度か質問を頂くようになった。その質問であるが、

① 規格の記述を実務へどのように解釈すべきなのかイメージできない。

② 実際のコンポーネントをよく分かっていない。

③ スライドの説明に添えてある小さなイメージ写真に注目している。

といった共通点が見られる。①については、今まで以上に平易な説明や実例を示すことで、理解が進むと考えられる。②では受講者は実際のコンポーネントをある程度知っていると思っていたが、そうでも無いとして改めようと思う。対面では実際の製品を持ち込むことも考えられるが、リモートではそうは行かない。できる限りイメージ映像を入れて説明することも今後は必要だろう。③は前述の改善二項目にも関連する。質問を頂き驚いたことであるが、説明スライドに実物のイメージとして小さく入れてある写真で、それが説明内容と違わないかとの質問であった。よく見ればご指摘通りであった。リモート環境で手元の画面において拡大されているのであろうか。

企業の規模で様々であろうが、それでも分業化が進んでいて設計者とはいえ、リストや図面と現物が一致しなくなっているのであろう。また、機械安全の普及につれ技術系ではなく、労働安全や環境系出身の方々の参加も増えてくるであろう。

リモート講習会では、移動のための時間や費用面等で参加しやすいという受講者のメリットもあり、コロナが収束してもこの形態のニーズは一定程度続くと思われる。今回の気付きを含めて、今後のコンテンツ改良を継続し、より理解の進む講習会にしたいと考えている。

ISO 12100 発行から 20 年

安全安心社会研究センター　客員研究員　越 前 屋　睦

ISO 12100 が発行され 20 年が経過したことを機に、この 20 年の成果や課題を見直してみた。

ISO 12100 が 2003 年に発行され、残念ながら休業災害件数は増えているが死亡者数は約半数まで改善された。（表１）

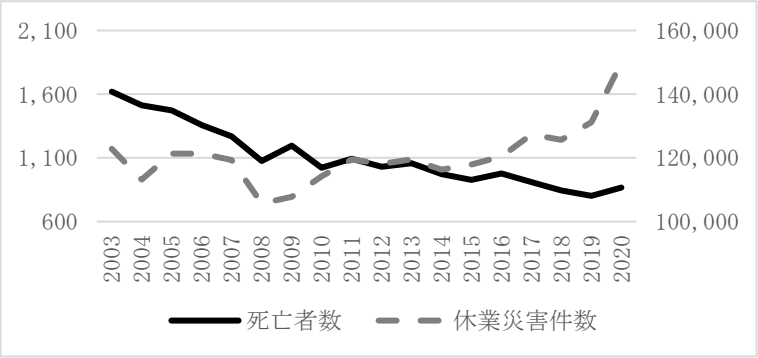

表１：労働災害統計

これらの成果はリスクアセスメントのみでは成し遂げられなかったとは想像できるが、災害が起きてからの「対策」ではなく、災害が起きる前に行う「方策」として他にできることが無いか考察してみた。

リスクアセスメントは、化学物質が義務化されているため安全衛生では周知されたように推測するが、機械設備ではまだ課題が残っている。課題は会社ごとに背景があると思うので技術的要因に限定して考える。災害が発生する要因の一つとして、危険源や危険事象の見逃しがあると考える。DC(Diagnostic Coverage)：診断範囲の図を拝借してリスクの見逃し図（図 1）とするが、検出可能な安全側故障(λsd)を「予測可能な許容可能リスク」と考え、検出不可能な安全側故障(λsu)を「予測不可能な許容可能リスク」、検出可能な危険側故障(λdd)を「予測可能な許容不可能リスク」、検出不可能な危険側故障(λdu)を「予測不可能な許容不可能リスク」と仮定した際に「予測不可能な許容不可能リスク」をいかに発見するかが災害件数の低減につながると考える。

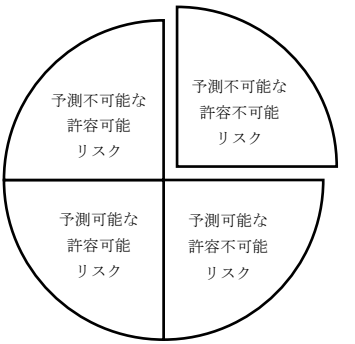

図 1：リスクの見逃し図

この予測不可能な許容不可能リスクを発見する方法は、各要素技術の基礎や応用、実際に現場で起きている不具合やチョコ停を知り、作業者や保全担当者の行動心理などを発見することと考えるため、今後も災害が 1 件でも減るよう研究を継続したい。

「セーフティ」と「セキュリティ」

安全安心社会研究センター　客員研究員　大賀公二

セーフティとセキュリティとは、日本語訳では、両者とも「安全」となるが、異なる意味であり、基準や規格も異なることを認識する必要がある。

「セーフティ(safety)」は、「受け入れ不可能なリスクが存在しない状態」、「人命への危害やシステムの損害のリスクが許容可能な水準以下に抑えられている状態」と定義され、安全を脅かすリスクを可能な限り排除するという考えである。

一方、「セキュリティ(security)」は、「攻撃から守ることによって得られる安全」であり、「攻撃」は、Web の改ざんやシステムへの不正侵入などのような悪意ある行為となる。

従来、筆者の担当分野である宇宙機システム、飛行機、自動車等の分野においては、セキュリティよりもセーフティが重視され、人への危害を中心に、リスクを低減し安全確保を図ってきた。

「セーフティ」と「セキュリティ」は異なる視点から「安全」を捉えているが、モノと IT の融合が進む時代には、両者を分離して考えることできなくなってきている。例えば、自動車に搭載されているネットワークに外部から不正侵入し、自動車の制御を乗っ取られることになれば人命を危険にさらされることになる。不正侵入は「セキュリティ」による対策が必要ですが、不正侵入できない設計や構造にしてお

くことも大切であり、こちらは「セーフティ」による対策が必要となり、両者の違いを正しく意識した対策が必要である。
現在、セーフティクリティカルな分野では、セキュリティ対応についても強く求められており、その両立が必須であるが、下記に示す多くの課題があるものと考える。

- セーフティとセキュリティ両者に精通したエンジニアは少ない
- 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たらよいのかわからない。
- 機密漏洩やシステムに対する改ざん・攻撃が、健康や安全性、環境に重大な影響を及ぼすといったシステム特有の被害イメージをつかみにくい。
- 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
- セーフティエンジニアの多くは、セキュリティリスクへの認識は十分といえない

「セーフティ」「セキュリティ」の一方のアプローチのみで、他方をカバーすることは困難である。現状では、両者のそれぞれの規格があり、システム開発においては、それぞれ異なったアプローチにより、両者の規格に適合させる必要がある。
現在、筆者のチームでは、宇宙機システムの安全かつ確実なミッション達成のための S&MA(Safety and Mission Assurance)活動を、さらに進化させ、セキュリティ対応を付加した統合活動を定義し、S2&MA活動の構築を進めている。
「セーフティ」「セキュリティ」両者への対応活動を、確実かつ効率的に遂行すべく、要求・基準の整備、ガイドライン整備、解析・評価、設計、教育研修に至るトータルサービスを提供すべく活動を実施しており、あらためて、本コミュニティでの議論をさせて頂きたい。

衛生設計と食品安全の統合

安全安心社会研究センター　客員研究員　大 村 宏 之

HACCP(Hazard Analysis and Critical Control Point)システムは安全な食品を製造するための世界標準の衛生管理システムである。

この HACCP システムは、2020 年に日本でようやく施行された。

このシステムを適切に機能させるためには、複数の前提条件が必要であり、その一つに衛生設計(HD：Hygienic Design)がある。日本ではほとんど知られていないが、HD は ISO 12100 が定める機械類の安全性に含まれる安全特性の一つである。

日本を含む多くの国は、EU のように ISO 12100 を考慮した機械類の安全性を衛生関連法令とリンクさせておらず、参照情報としての提示もしない。そのため、食品産業界では規格に基づく HD の考慮がほとんど行われておらず、前提条件としての HD は、担当者個人又は企業独自による考え、又は文書に基づいてきた。

だが、食品の国際流通量拡大を踏まえ、食品安全(FS：Food Safety)に関連する国際組織“GFSI”は、FS のマネジメント規格のベンチマークとして、前提条件である HD に対する取り組みを“スコープ J1”として定め、2020 年にリリースした。

このスコープ J1 は、『HACCP システムを構築する製造ラインの機械類は、国際安全規格に基づいた HD を採用しなければならない』ことを食品産業界に示した、日本で初めての国際的な文書となった。

スコープ J1 が定める HD マネジメントの主な事項に、「衛生面のリスクアセスメントの実施」「規格に基づく衛生リスク低減」「洗浄性の評価試験は認定ラボで行う」こと等がある。

食品機械の HD を定めるタイプ C 規格は、ISO にはまだない。だが筆者が所属する工業会では、ISO/IEC ガイド 51 に整合する JIS 開発だけでなく、スコープ J1 への包括的な備えにも取り組んできた。

その一つが「洗浄性評価ラボの設置(写真 1)」である。スコープ J1 は、第三者による試験について「認定された施設、又は国際的ガイドラインに従う施設で実施する」と定める。

筆者らは、(一財)日本食品分析センターと協力し「洗浄性評価ラボ(TL：Testing Laboratory)」の承認及び公認を得るための取り組みを 10 年前から行っており、ついに今年、実を結んだ。

2022 年 2 月､TL は ISO/IEC 17025 の認証を NITE から得た(写真 2)。次いで 10 月に国際的なガイドラインを開発する EHEDG の審査を受け 11 月上旬に公認された。これによって、2023 年の夏頃より日本で初となる、国際標準の洗浄性評価試験の実施が可能になる。

今後も引き続き国際的な動向を注視し、我が国の食品産業を支える一助となる活動に取り組んでいきたい。

写真 1 TL に設置した洗浄性評価プラント

写真 2 認定証

コロナ禍における食の安全

安全安心社会研究センター　客員研究員　川 瀬 健 太 郎

筆者の専門分野である食品安全科学分野は、生活に不可欠な「食」がテーマである。社会情勢の変化や食品に関わる法規制などの整備が食の安全にどのような影響を及ぼすのか、の視点を意識して研究調査を進めている。食品リスクには様々あるが、そのひとつが食中毒である。広域で同時に多発すると深刻な健康被害をもたらすリスクがある社会的な脅威である。2020 年 1 月の国内初の新型コロナウイルス感染者発生の報道から 3 年が経過した。同年 4 月の緊急事態宣言を端緒に、行動自粛要請、飲食店に対する営業時間の短縮要請が断続的に行われた。折しも 2021 年 6 月から原則すべての食品事業者に対し、改正食品衛生法に基づく HACCP（国際的な食品安全管理手法）の導入が完全制度化された時期である。食品事業者はその導入準備と管理運用を進めつつ、デリバリーやテイクアウトなど新しい販路を開拓するなど、食の提供形態に大きな変化が見られた。社会的には三密回避、マスク着用、アルコール洗浄が習慣化し衛生意識が高まった。

では、このコロナ禍における食中毒の発生状況はどうか。厚生労働省が例年食中毒統計を公表しており、直近 5 年でみると事件数は 2018 年が 1,330 件であったが、2020 年は 887 件、特に 2021 年は 717 件と過去 20 年で最も発生が少なかった。食中毒患者数は 2018 年の 17,282 人から 2020 年 14,613 人、2021 年 11,080 人と顕著に減少がみられた。

表 1　2020-2021 年に発生した大規模食中毒事案

発生年	年間患者数	発生月	発生施設（所在地）	原因食品	患者数	原因物質
2020年	14,613	6月	学校給食施設（埼玉県）	海藻サラダ	2,958	病原大腸菌O7:H4
		8月	飲食店（東京都）	仕出弁当	2,548	毒素原性大腸菌O25
2021年	11,080	4月	弁当製造施設（岡山県）	仕出弁当	2,545	ノロウイルスGII
		6月	乳処理施設（富山県）	学校給食牛乳	1,896	病原大腸菌OUT（OgGp9）:H18

表 1 はコロナ禍での大規模な食中毒発生事例である。特筆すべきは 2,000 人超のノロウイルス感染事例が 2012 年の広島県での事例以来 10 年ぶりに発生したことである。上記岡山県の事例は従業員から食品へのノロウイルス汚染などが発生原因であった。他 3 事例は学校給食衛生管理基準に基づく当日調理及び加熱調理の不徹底（埼玉県）、非加熱野菜の洗浄消毒の不備（東京都）、食品加工機械の保守管理不良による微生物汚染（富山県）など複数の項目において指摘がなされた。食品事故のみならず、食品の異臭、異物混入、変質変色や食品表示ミスなどの食品苦情も例年発生し同様類似の事例も後が絶たない。対応とその対処を誤ると深刻な有症事故を引き起こす引き金となる可能性があることから、食品苦情を決して軽視、看過してはならない。

筆者は過去 40 年間の食品異臭苦情事例を収集、分類し実態と傾向を調査し原著論文として発表した。考察として、HACCP 視点に基づいて事例のハザード分析とフローダイアグラム分析を実施することが異臭原因の工程特定につながることを数値化して明らかにした。これら知見を食の安全の高度化支援に活用していきたいと考える。

＜論文掲載＞

川瀬健太郎、日佐和夫、濱田（佐藤）奈保子：食品異臭苦情の分類と HACCP 視点での原因工程特定、安全工学会誌、NO.61、pp.340-347、vol.5（2022）

安全の論理と必要条件と十分条件

安全安心社会研究センター　客員研究員　杉 本　旭

安全の論理学に関わる以前のこと、安全の論理的理解の重要性を明快に示してくれたのは、新幹線関連の高名な安全技術者であった。彼の主張は、「新幹線は必要条件でなく十分条件で運転すること」、そして(当時の)私の安全では、新幹線を運転できないということであった。必要条件/十分条件は、論理学の専門用語でもあるが、論理学リテラシー貧困をズバリ指摘されて、私の博論のテーマは「人間機械安全作業システムの論理的研究」となった。

言うまでもなく、ヒトは、正しさ(無矛盾)をもって応えるべき約束(責任)の存在を承知する。そして、この約束(責任)を前提にするのが私たちのテーマの「安全」である。もしシステムの説明(言葉)に矛盾があれば、取り返しのつかない結果になりかねない。

論理学は、矛盾（“偽”）を見分けて、無矛盾（“真”）を求めるのを助ける。基本的には必要条件と十分条件を立てて、必要条件（“偽”とされる理由/原因）と十分条件（結果を“真”とする条件）との関係で、課題（命題）の正しさ（“真”）を証明する。

言うまでもなく、システムの説明は言葉による。つまり、言葉の論理が関わるということである、しかし、言葉はあいまいであり、(形而上学的）曖昧さや誤りが含まれるが、これはやむを得ない。システムの条件は、基本的には目的に関わることであり、よって安全の必要条

件は副次的、要するに「注意して運転する必要がある」の命題に集約されると言っていい。必要条件による安全が不十分(“偽”)とされるのは必要条件の有する限界、すなわちリスクはゼロにならないからである。現状の安全方策は基本的には安全の必要条件であって、程度の差こそあれ、真なる安全を提供するものではない。論理学の示すところ、安全の不十分を補完すべく、十分条件によって真の安全を確保すべきとされる。

リスク低減は必要条件によるところ、論理学は、到達した許容リスクでさえも真の安全と認めない。それにも拘らず現実にはどうか。許容リスクが勝手に安全(“真”)と定義されているではないか。許容リスクが真の安全でないことを十分承知の上でのこと。これは本来許されないフェイクである。

さて、先の必要条件に言葉の論理を適用すれば、現実には、必要条件(:注意≧運転≧残留リスク≧事故)となる。つまり、注意して運転してもその限界で残るリスクによって事故の可能性があるということになる。そしてその解決を、人間特有の“対偶”という論理的機能(能力)に委ねる。「注意して運転する」(:注意≧運転)だけに注目すると、その対偶は「注意できないので運転を止める」(:¬運転≧¬注意)になる(ただし、“対偶”は予測の関係になることに注意)。これが、十分条件の基本的な表現である。詳しくは、紙面の都合でできないが、単純な例とは言え、リスクに基づく安全上の問題(必要条件)を対偶によって解決する(十分条件)という基本は変わらない。ちなみに、必要条件では事故を発生確率として扱うが、十分条件では、例えば、インタロックが、センサによる 10 秒後の事故を 5 秒で止めて防ぐというように、事故はセンサによる予測時間となる。最後に、安全の論理を思い切ってまとめれば、安全の必要条件は“リスク低減”であり、安全の十分条件は“事故の前の停止”だと考えていいだろう。

医療 DX と情報セキュリティ

安全安心社会研究センター　客員研究員　**野 沢 義 則**

新型コロナウイルスの蔓延をきっかけにして医療分野のデジタル化が追い風となった。当初は、未知のウイルスに対する不安を最小化させる目的でサーモグラフィや映像関連機器の導入が中心であった。その後、新型コロナ感染症患者の情報把握や、2040 年頃に直面するマンパワー不足に向けて更なる IT 化が提案されている。政府は、医療分野の DX(デジタルトランスフォーメーション)を推進するため、医療 DX 推進本部を設置した。マイナンバーカードの健康保険証利用に加え、電子処方箋や各種手当の判断資料に活用するなど利用者の利便性向上が期待されている。現在、各医療機関が個別に導入している電子カルテシステムにおいても、医療機関同士でのデーター交換ができるように HL7 等のデーター交換規格により電子カルテの標準化が進められている。

一方、医療機関をターゲットにしたサイバー攻撃がメディアから報じられ、医療 DX の期待とは裏腹に医療機関では脅威と不安に駆られている。これまでは、コンピューターウイルスに感染したパソコンのウイルス駆除に時間を要したという経験はあるものの、電子カルテシステムの全面停止という事態の深刻さには恐怖である。電子カルテシステム導入黎明期には、システムトラブルを当初から想定し、伝票運用に切り替えるなど代替え手段を準備して通常業務を行っていた。し

かし、ここまで電子カルテシステムが普及し安定した稼働を続ける今となっては、電子カルテシステムの停止は診療や治療に大きな影響や多大な損害を与える事は容易に想像できる。また、電子カルテシステムは、医事会計システムや各種医療機器、検査や放射線部門の部門システムと密接に連携し稼働している巨大なシステムでもある。このようにシステム依存度が高まった状況の中、2022 年 10 月に関西の医療機関で発生したサイバー攻撃事件は、数か月間にわたり診療に影響を及ぼした。

これまで医療機関の情報セキュリティ対策は、職員の不正(個人情報紛失等)が中心であった。今回のランサムウェアによるデーターの暗号化や金銭要求など悪意のある攻撃には、十分な対策ができていない。2022 年に医療機関を狙ったサイバー攻撃が少なくとも 13 件あったと報道されている。しかし、医療機関には情報セキュリティに詳しい人材は、一部の医療機関を除いて雇用されていないのが現状である。そのため、IT ベンダー任せっきりの場合もあり、責任の明確化も含め組織として体制の整備が急務である。

これまで医療安全(患者安全)を中心に活動してきたが、BCP(事業継続計画)や情報セキュリティに関しても知識が求められる。安全安心研究センターの人材ネットワークを活用し、他の産業事例も参考にしながら客員研究員として社会に役立つ活動を行いたい。

製品安全競争力の見える化について

安全安心社会研究センター　客員研究員　松 田 利 浩

私は、2020 年 6 月まで約 30 年間製品安全関係の認証機関で勤務してきた。この間、様々な方と標題「安全は競争力になり得るか」について議論を交わす機会を得てきたが、未だその明確な答えは持ち合わせていない。今回は、肩ひじを張らずにエッセー的な読み物として持論を述べたい。

多くの方に「安全は競争力になりますか？あなたの会社のモノでは如何でしょう」と尋ねると、「はい、なります」と「いいえ、なりません」と答えが二分する。安全のポジティブインセンティブの考え方によれば、「安全は価値があるもの」と認識することの重要性を説いている。

例えば自動車のエアバック。運転席用フロントエアバックは、1980 年初頭普及し始めた安全装備である。当初は、オプション装備でありこれらが装着した自動車は消費者から交通事故安全の有力な装備として認識され価値があると多くのユーザーに認識されていた。しかし、こんにち運転席用フロントエアバックが装備された自動車を価値があるものとして消費者が積極的に選択し競争力があるかと言われれば「いいえ」だろう。では、衝突被害軽減ブレーキはどうか？半数以上の方は「はい」と答えると思う。運転席用フロントエアバックと同じようにいざ衝突事故が起きた際に傷害の程度を減少させるもので

あり、交通事故時の傷害リスクを低減させることが期待である安全装備なのにだ。この二例における答えの違いは、おそらくその安全装備の普及具合によるものだろう。つまり、安全装備の価値は「積極的に選択」から普及拡大と共に「あって当たり前」に変化し、ほぼ全ての自動車に装備されると存在自体が「無関心」になり価値を失う。

では、同じく自動車のペダル踏み間違い時加速抑制装置（誤発進抑制制御装置）はどうだろうか？現在装着率は約７割、これから本格普及が始まる段階なので、前例に倣えば「はい」となるはずだが、実際には回答者の年齢や健康状態、住んでいる地域、家族構成などによって答えはまちまちになると思う。つまり、この例では回答者の必要度が影響している。運転者自身や家族が運転能力の不安を抱えている場合には「はい」、抱えていない場合には「いいえ」という具合だ。もしかしたら、自動車のペダル踏み間違い事故の報道など社会に与えるインパクトも安全装備の価値を動かす要因になりうるかも知れない。

以上のように安全装備の価値、すなわち「安全が競争力になり得るのか」の答えは一様ではなく、様々な条件やパラメータが組み合わさって導かれるものではないかと考える。長年製品安全に携わってきた身としては、「安全競争力指数」のような数値化（見える化）が可能なのか、可能な場合にはどのような関数式で言い表すことができるのか、単純だけど興味の尽きない話題だと思っている。

参考文献

1)　向殿 政男、安全と CSR, 金融 CSR 総覧、経済法令研究所、pp.280-28520、06－12
2)　国土交通省、命を守る安全装置、自動車総合安全情報
https://www.mlit.go.jp/jidosha/anzen/02safetydevice/index.html

研究成果の社会実装

安全安心社会研究センター　客員研究員　吉 澤 厚 文

大学の研究は「これまでできなかったこと」を「できる」ようにするところにその醍醐味がある。一方、研究成果は社会に役立って初めてその役割を果たすという「技学」の精神からすると、これをどう社会実装するかという課題が残る。大学の研究成果を社会実装するには、その成果を商品化し、ビジネスとして社会に広めていくプロセスを設計することが現実的、かつ重要である。

ここでは、現在実施されている長岡技術科学大学と東京電力ホールディングス㈱との防災・減災に関する包括連携協定に基づく共同研究に関し、成果の社会実装プロセスについて述べたい。具体例として、災害時に避難所に水を供給するシステム「ウォーターチェンジャー®」の開発プロセスを振り返り、ビジネス化への要諦をまとめる。

2020 年度より開始した共同研究により、バイオの力を利用してエネルギー消費を極力抑えた可搬型中水供給装置が開発された。これは、小さな太陽光パネルのエネルギーを使い、雨水や川の水がバイオ反応層中を自然落下する間に浄化され、中水を供給できるものである。しかし、これを実際に商品として使用できるようにするためには、装置としてできることとできないことの境界をはっきりさせ、安全・品質、耐久性や使い勝手といった要求されるスペックを満たしてゆく必要がある。さらに、コストや意匠性といった要素も重要である。具体的

に商品として使用が始まると、商品の保証やクレームなどに対応できる体制整備も求められる。

これらの要件を大学側で対応することは困難であり、研究開発された装置を商品化できるパートナーを見つけなければならない。本研究では、新潟県のご支援をいただき、災害技術の様々な展示会に本技術を展示することで、パートナー探しを行った。その際に重要となるのが、自分たちの技術の特徴をどのように相手にアピールするか、といったデモンストレーション技術である。この事例では、開発技術の特徴を容易に理解できるようにするために、装置のシースルーモデルを作成し、展示・説明を行った。これは大きな成功要因となった。

展示会への出展の結果、複数の会社が商品化に意欲を示していただき、新潟市のユニトライク社により商品開発、販売が行われることとなった。商品第１号は新潟市の工事現場に設置されたが、基礎研究フェーズは終了していたものの、共同研究開始後２年半というスピードで商品化し社会実装できている。

また、商品第２号は、長岡市のご理解をいただき、３年ぶりに開催された長岡まつり大花火大会の会場に、手洗い水を供給する目的で設置いただいている。

このウォーターチェンジャー®は、防災用として開発をしてきたが、社会のニーズは多種多様であり、今回は避難所ならぬ工事現場やイベント会場での活用という形で実装された。そのニーズの掘り起こしや開拓にはやはりビジネスに明るいパートナーの存在が欠かせない。また、パートナーとの契約を行う際に、研究開発された知財の所在を明確にしておくことが求められる。本装置では、２件の特許申請並びに２件の商標登録を実施している。

本事例が、読者の研究の社会実装に向け、何らかの参考となれば幸いである。

令和３～４年度
安全安心社会研究センター主催の講演等の活動

新型コロナウイルス感染拡大予防対策として、令和３年１２月の特別講演より入場制限を設け、オンラインで同時配信しております。

第２４回 特別講演会

日　時：令和３年１２月１８日(土)　１３：００～１７：００
場　所：田町グランパークカンファレンス　４０１ホール
主　題：「安全の基本を考える」

昨今の技術の発展は素晴らしく、工業設備、身の回りの製品に活用されています。ところで、社会に技術を提供するときに技術者が考えておくべきことは何でしょうか。 安全をリスクで考える上で基本は何でしょう。安全に関する情報もインターネット上などに多く存在していますが、本質的な情報を見いだし、活用できているでしょうか。 逆に考えると、どのような形で情報をまとめ、提供するとよいでしょうか。

このように考えると、安全の基本を再確認して、それを基に議論することが必要と考え、そのきっかけとして企画しました。

【プログラム】

・12:40～13:00　受付
・13:00～13:10　開会の挨拶
　本日の趣旨説明（門脇　敏 センター長）
・13:15～14:25　講演１
　「安全の論理～安全を基本から見直す」
　長岡技術科学大学名誉教授　杉本　旭　氏

・14:40～15:50　講演２「安全の制度設計：日本の課題は
どこまで解決したのか？」
開志専門職大学副学長　三上　喜貴　氏
・16:00～16:30　講演３「最近の機械安全規格から見る
安全の動向と考察」
長岡技術科学大学システム安全工学専攻
教授　福田　隆文　氏
・16:30～16:50　総合討論（司会：福田　隆文　教授）
・16:50～17:00　閉会挨拶（塩野谷　明　副センター長）

第２５回 特別講演会

日　時：令和４年７月２日(土)　１３：００～１７：００
会　場：田町グランパークカンファレス　４０１ホール
主　題：「情報技術・IoT・コンピュータ技術を活用した安全
― 何ができるか、予め考えるべき点は何か ― 」

コンピュータとその利用技術の発展はめざましく、IT、AI等の言葉もよく使われています。実際、私たちの生活、産業界の活動、社会インフラなどで活用されています。

安全に目を向けると、小型デバイスを用いた人の識別や画像認識による人の識別、AI による判断等広範な技術が広範に使われるようになることは間違いありません。今は本格導入の初期にいると考えられます。

そこで、この技術を安全へ適用する可能性・事例を知り、同時に考えなければならない課題を考えます。また、これらの活用に不可欠なソフトウェアの発展の状況と課題について考えてみます。

【プログラム】
・12:40～13:00　受　付
・13:00～13:05　開会の挨拶
安全安心社会研究センター センター長　　門脇　敏

・13:05～13:55　第一講　「新しい時代の安全
“協調安全”の概念、実例及び課題について」
一般社団法人セーフティグローバル推進機構
松浦　裕士　氏
・13:55～14:05　質　疑
・14:15～15:05　第二講「人工知能(AI)と自律制御の安全」
国立研究開発法人　産業技術総合研究所
藤原　清司　氏
・15:05～15:15　質　疑
・15:25～16:15　第三講「AUTOSAR: モビリティの提供を
『継続可能』とするためのプラットフォーム」
イーソル株式会社　　櫻井　剛　氏
・16:35～17:00　総合討論
・17:00～17:05　閉会挨拶
安全安心社会研究センター　副センター長　木村　哲也

第２６回 特別講演会

日　時：令和４年１２月１７日(土)　１３：００～１７：０５
会　場：グランパークカンファレンス田町　４０１ホール
主　題：「イノベーションとそれに対応した新しい規格」

昨今の技術は、従来の延長上ではないイノベーティブ（革新的）な発展の途上にある。 それに対応して、従来の安全とは異なって機械と人が接触する場合の安全確保の検討、あるいは、新たなセンシング技術の活用の検討が規格化の段階まで進んでいる。 また、インベーションに付随する新たなリスクに対して、事前に検討を行うことが実用化への関門である。今回は，この点を議論したく、規格の面から２講演、国家プロジェクトである次世代空モビリティの社会実装に向けた実現プロジェクト（NEDO）に関しての講演の後に、講

師、会場・遠隔の聴講者で意見交換を行う。

【プログラム】

・12:30～13:00　受　付

司会進行：長岡技術科学大学　特任教授　福田　隆文

・13:00～13:05　開会の挨拶

安全安心社会研究センター　センター長　門脇　敏

＜第Ⅰ部＞　新しい規格の動向

・13:05～14:05　第１講「機械の可動部分と人の接触時に生成される力学的な安全データの標準化」

豊田工業高等専門学校　校長　山田陽滋 氏

・14:05～14:15　休　憩

・14:15～15:15　第２講「IEC 61496“機械類の安全性―電気的検知保護設備”における新しい検出技術（画像、ミリ波）を使った安全センサ規格の開発動向」

オプテックス株式会社　村田記一 氏

オムロン株式会社　竹島昌俊 氏

・15:15～15:25　休　憩

＜第Ⅱ部＞　イノベーションーにおける課題と解決

・15:25～16:25　第３講「ドローンイノベーションと標準化」

東京大学大学院 工学系研究科

航空宇宙工学専攻　五十嵐 広希　氏

・16:25～16:30　休　憩

＜第Ⅲ部＞　総合討論

・16:30～17:00

・17:00～17:05　閉会挨拶

安全安心社会研究センター　副センター長　木村　哲也

第２７回 特別講演会

日　時：令和５年１月２１日(土)　１４：３０～
会　場：田町グランパークカンファレンス 302＋303 会議室
主　題：航空安全とドローン安全
【プログラム】
・14:15　受付
司会：安全安心社会研究センター 副センター長　木村 哲也
・14:30　開会の挨拶
安全安心社会研究センター センター長　門脇 敏
・14:35　講演１　題目：航空安全（耐空性維持）
講師：公益社団法人 日本航空技術協会　稲垣 充　様
・15:45　講演２　題目：ドローン安全
講師：長岡技術科学大学 教授　木村哲也

・16:30　パネルディスカッション
（ファシリテーター：木村）
テーマ：航空安全とドローン安全の融合
パネラー：稲垣様，センター客員研究員若干名

長岡技術科学大学における安全安心社会の構築に向けた取り組み

年	本学の動き	社会全体の動き
2001 (H13)	機械安全工学寄附講座 設置	3月　平成13～17年度科学技術基本計画の理念として「安心・安全で質の高い生活のできる国」 5月　厚生労働省より「機械の包括的な安全基準に関する指針」
2002 (H14)	4月　大学院機械創造工学専攻に「機械安全コース」創設	9月　初の日朝首脳会談 10月　拉致被害者5人帰国
2003 (H15)		5月　専門職大学院設置基準 機械安全の基本国際規格 ISO12100（機械類の安全性－設計のための基本概念、一般原則）発行 食品安全基本法公布（7月施行）
2004 (H16)	3月　「機械安全コース」第一期生修了	4月　文科省 安全・安心な社会の構築に資する科学技術政策に関する懇談会報告書 7月　新潟・福島豪雨 新潟県中越地震 ISO12100に基づき JIS B 9700 制定
2005 (H17)		安衛法が改正、リスク評価努力義務化（翌4月施行） 4月　個人情報保護法施行
2006 (H18)	1月　中越地震調査報告会 4月　専門職大学院「システム安全専攻」創設	技術経営関係専門職大学院10校により MOT 協議会発足 消費生活用製品安全法改正　危険性有害性調査の努力義務化 3月　厚生労働大臣がリスクアセスメントの実施による自主的な安全衛生活動の促進を図るための指針を公表
2007 (H19)	10月　新潟中越沖地震震災復興シンポジウム	5月　重大事故報告制度運用開始 7月　厚生労働省が「機械の包括的な安全基準に関する指針」を改正 新潟県中越沖地震
2008 (H20)	3月　システム安全専攻第一期生修了 **4月　安全安心社会研究センター発足** 博士後期課程情報・制御専攻に「安全工学コース」 7月　新潟中越沖地震一周年震災復興シンポジウム	5月　中国四川省で M8.0 の大地震 6月　岩手・宮城内陸地震 秋葉原無差別殺傷事件 9月　リーマン・ブラザースが経営破綻 10月　大阪市の個室ビデオ店火災

年	本学の動き	社会全体の動き
2009 (H21)	9月　本センターに客員研究員制度 創設	9月　消費者被害を防ぐため、食品や製品の事故、クレームなどの情報を一元化した消費者庁発足
2010 (H22)	3月　システム安全エンジニア認定委員会（向殿政男委員長）との協力による「システム安全エンジニア資格制度」を創設、第一回試験を実施	1月　ハイチ地震、25 万人死亡 6月　「はやぶさ」地球へ帰還 10月　チリ鉱山、69 日ぶり作業員 33 人奇跡の生還
2011 (H23)	**3月　「安全安心社会研究」創刊** 4月　大学院博士課程に「安全パラダイム指向コース」	3月　東日本太平洋沖地震 東京電力福島第一原発事故発生 7月　欧州改正 RoHS 指令施行 新潟・福島豪雨 8月　放射性物質汚染対処特措法
2012 (H24)	3月　「安全安心社会研究」第2号発行 小千谷市と原子力安全対策支援パートナー協定締結 4月　大学院修士課程に「原子力システム安全工学専攻」	4月　厚生労働省が、機械譲渡者等が行う機械に関する危険性等の通知の促進に関する指針を公表 9月　原子力規制委員会発足 12月　中央自動車道トンネル天井崩落事故
2013 (H25)	3月　「安全安心社会研究」第3号発行 8月　高専生・教員を本学に招き「安全基礎工学」の講義を実施	2月　PM2.5 対策で国が暫定指針 4月　第 12 次労働災害防止計画 (2013 年度～2017 年度) スタート 7月　原発の安全対策の新規制基準が施行 8月　京都花火大会で露店爆発事故
2014 (H26)	3月　「安全安心社会研究」第4号発行 10月　生活空間の高度リスクマネジメントのためのエビデンス情報基盤構築」プロジェクト始動 （JST ／ RISTEX）	4月　厚労省が安全技術者への教育プログラムを提示。その中で、システム安全エンジニア有資格者は全てを修得しているとみなされた 6月　労働安全衛生法改正 消費者安全法、景品表示法の改正法が成立・公布 8月　広島土砂災害 9月　御嶽山噴火 11月　サイバーセキュリティ基本法が成立

年	本学の動き	社会全体の動き
2015 (H27)	３月　「安全安心社会研究」第５号発行 システム安全専攻修了生が 100 名を超える 10月　システム安全アソシエイト第一回試験を実施	１月　内閣に「サイバーセキュリティ戦略本部」、内閣官房に「内閣サイバーセキュリティセンター（NISC）」が設置される ４月　子ども・子育て支援新制度スタート ５月　列島各地で火山活動活発化 ８月　川内原発１号機が再稼働、原発ゼロ解消 ９月　国連で持続可能な開発目標（SDGs）が採択 10月　マンション傾斜、基礎工事のデータ改ざん発覚
2016 (H28)	３月　「安全安心社会研究」第６号発行 ８月　高専フォーラムにてシステム安全のワークショップを開催 ９月　SSE 資格制度：システム安全サブエンジニア第一回試験を実施	１月　個人情報の保護に関する法律に基づき、個人情報保護委員会が内閣府の外局として設置される ４月　熊本地震　大分県中部地震 ６月　改正労働安全衛生法施行 10月　マイナンバー制度スタート 11月　福岡・博多駅前の道路陥没
2012 (H29)	８月　高専フォーラムにてシステム安全のワークショップを開催 「高専教員・学生向け出張講演システム安全の基礎」を実施	１月　改正育児・介護休業法施行 ３月　安全保障関連法が施行 ７月　九州北部豪雨
2018 (H30)	８月　高専フォーラムにてシステム安全のワークショップを開催 「高専教員・学生向け出張講演システム安全の基礎」を実施	８月　私大医学部で不正入試発覚相次ぐ ４月　第 13 次労働災害防止計画(2018 年度～2022 年度）スタート ７月　大阪北部地震 ９月　北海道胆振東部地震 12月　改正出入国管理法が成立
2019 (R１)	３月　「安全安心社会研究」第７号発行 ８月　高専フォーラムにてシステム安全のワークショップを開催 「高専教員・学生向け出張講演システム安全の基礎」を実施	３月　厚生労働省 機能安全教育の通達 ４月　働き方改革関連法が順次施行 ６月　改正児童虐待防止法成立（翌年４月施行） ８月　九州北部豪雨
2020 (R２)	３月　「安全安心社会研究」第８号発行 「高専教員・学生向け出張講演システム安全の基礎」を実施	１月～新型コロナウイルス感染症（COVID-19）が世界的大流行 ３月　新型コロナウイルス対策の特別措置法が成立 東京オリンピック・パラリンピック１年延期決定

年	本学の動き	社会全体の動き
2020 (R２)		４月　改正民法、労働基準法改正（働き方改革関連)、改正健康増進法、改正意匠法（知的財産権等）などが施行 ４～５月 緊急事態宣言(１回目)が発令 ６月　「改正道路交通法」施行、「あおり運転罪」創設 ７月　レジ袋有料化スタート 11月　中災防が労働災害防止団体や安全衛生関係団体と連携し、働く人の安全・健康を守るための安全衛生教育を支援
2021 (R３)	３月　システム安全専攻修了生が 200 名を超える ４月　システム安全工学専攻に改組 ９月　「安全安心社会研究」第９号発行 12月　KOSEN フォーラム参加	２月　新型コロナウイルス感染症の医療者ワクチン接種始まる ７月　熱海で大規模な土石流 東京オリンピック・パラリンピック開幕 12月　大阪ビル(放火)火災
2022 (R４)	９月　システム安全工学専攻が工学教育賞を受賞	２月　北京五輪冬季最多メダル ロシア軍、ウクライナ侵攻 ４月　知床半島沖で観光船沈没 ７月　安倍晋三元首相銃撃され死亡 11月　サッカーW 杯開催
2023 (R５)	３月　「安全安心社会研究」第 10 号発行	１月　新型コロナ５月から「５類」に引き下げ決定

▽ 編集後記

長岡技術科学大学　安全安心社会研究センター事務局　小林まゆみ

安全安心社会研究１０号発行にあたり執筆者の皆さまにおかれましては、ご多様にもかかわらず期限内の提出に感謝申し上げます。原稿依頼から締め切りまでの期間が短く、ご苦労をおかけし申し訳ございませんでした。

「安全安心社会研究」は２０１１年３月に創刊号を発行以来、今号で第１０号を迎えます。その間、震災、豪雨、豪雪、猛暑の自然災害、新型コロナウイルス感染拡大など様々な出来事があり、特集も掲載されました。

今後も機械、労働、食品、医療など各分野の安全について取り上げ、本誌が安全安心社会構築の一翼を担うことを期待します。

※今号より PDF ファイルをホームページへの掲載のみで、冊子の発行はいたしません。

令和４年度　安全安心社会研究センター組織

センター長

長岡技術科学大学	システム安全系　教授	門脇　　敏

副センター長

長岡技術科学大学	システム安全系　教授	木村　哲也

教員

長岡技術科学大学	情報・経営システム系　教授	塩野谷　明
長岡技術科学大学	機械系　教授	上村　靖司
長岡技術科学大学	電気電子情報系　教授	岩橋　政宏
長岡技術科学大学	環境社会基盤系　教授	細山田得三
長岡技術科学大学	システム安全系　教授	阿部雅二朗
長岡技術科学大学	システム安全系　教授	三好　孝典
長岡技術科学大学	システム安全系　教授	山形　浩史
長岡技術科学大学	システム安全系　准教授	大塚　雄市
長岡技術科学大学	システム安全系　准教授	張　　坤
長岡技術科学大学	システム安全系　准教授	北條理恵子
長岡技術科学大学	システム安全系　実務家教授	坂井　正善
長岡技術科学大学	システム安全系　実務家教授	津田　積善
長岡技術科学大学	システム安全系　実務家准教授	宮地由芽子
長岡技術科学大学	システム安全系　講師	佐藤　大輔
長岡技術科学大学	システム安全系　助教	高橋　憲吾

事務局

長岡技術科学大学	技術支援センター	山田　修一
長岡技術科学大学	安全安心社会研究センター	小林まゆみ

令和４年度　安全安心社会研究センター客員研究員 ＜五十音順＞

五十嵐広希（東京大学 大学院 工学系研究科航空宇宙工学専攻）
今枝　幸博（村田機械株式会社）
岩岡　和幸（旭化成株式会社　延岡支社　環境安全部）
越前屋　睦（吉川鐵工株式会社）
大賀　公二（有人宇宙システム株式会社　安全開発・ミッション保証部　部長）
大村　宏之（社団法人日本食品機械工業会　事業部）
奥田　真司（奥田労働安全コンサルタント事務所　代表）
川瀬健太郎（日清オイリオグループ株式会社　人事・総務部付）
櫻井　　剛（イーソル株式会社 ソフトウェア事業部及びガバナンス室(兼務)シニアエキスパート）
杉本　　旭（長岡技術科学大学　名誉教授）
野沢　義則（八戸市立市民病院　医療技術局　局長）
松浦　裕士（日本認証株式会社　事業企画推進部）
松田　利浩（Office Co. Think　代表）
吉澤　厚文（東京電力ホールディングス株式会社　フェロー）

安全安心社会研究［第１０号］

令和５年３月　発行

長岡技術科学大学　安全安心社会研究センター

〒940-2188　新潟県長岡市上富岡町 1603-1

電話 0258-47-9856

発行責任者：門脇 敏

E-mail：info_safety@vos.nagaokaut.ac.jp

ホームページ：https://whs.nagaokaut.ac.jp/safety/

国立大学法人
長岡技術科学大学
Nagaoka University of Technology