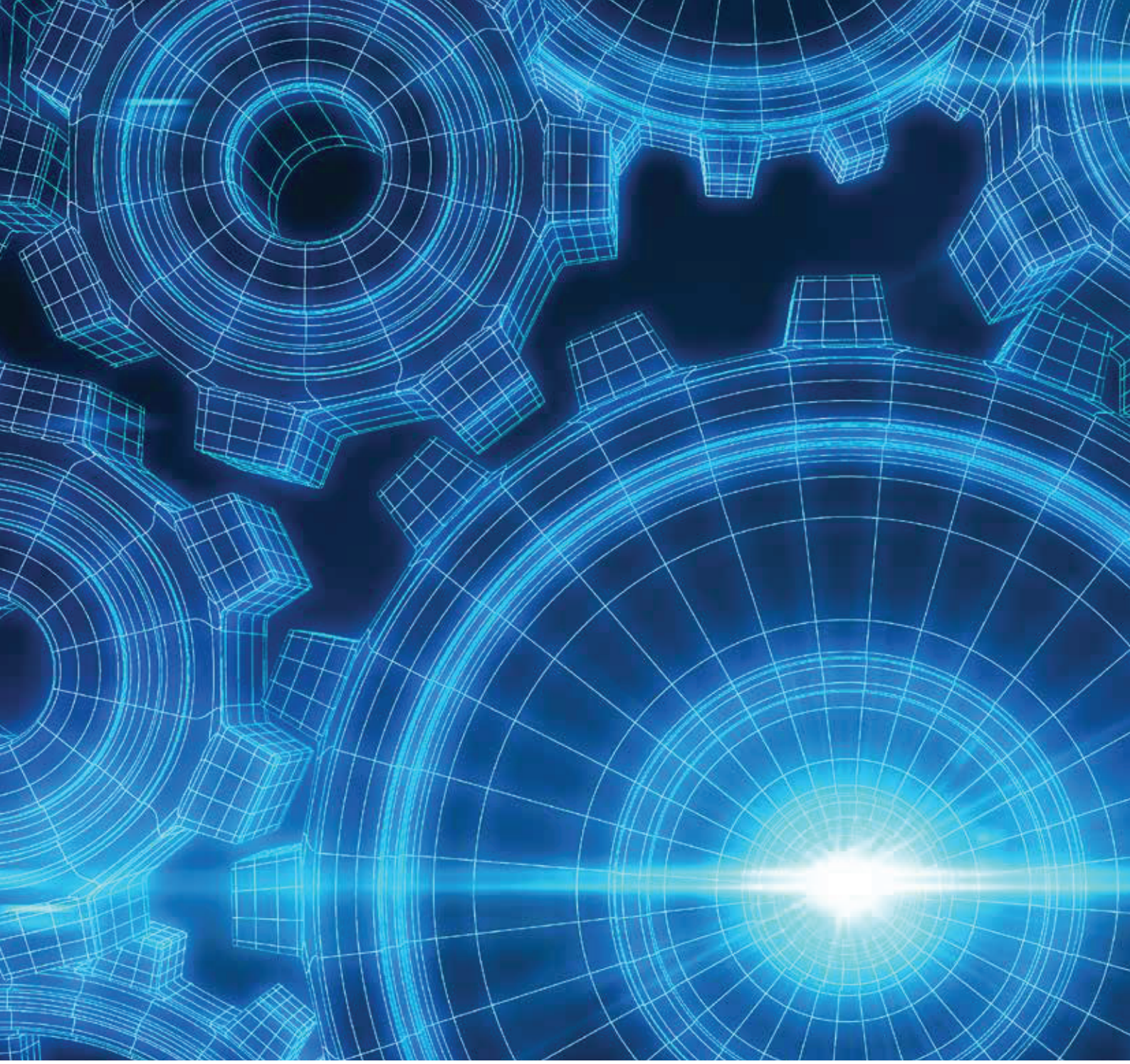


White Paper

白書

Safety in the future

将来の安全

Translations of this white paper has been authorized by IEC Japanese National Committee. The IEC and related organization do not warrant the accuracy, reliability, or timeliness of any information translated and shall not be liable for any losses caused by such reliance on the accuracy, reliability, or timeliness of such information. Any person or entity who relies on information translated does so at his or her own risk. If any questions arise concerning the accuracy of the information presented by the translated version, please refer to the English version of the white paper, which is the official version.

このホワイトペーパーの翻訳は、IEC日本国内委員会の承認下によって行われまた。IEC、及び関連団体は、翻訳された情報の正確性、信頼性、または適時性を保証せず、そのような情報の正確性、信頼性、または適時性への依存によって生じた損失について責任を負わないものとします。翻訳された情報に依存する個人または団体は、自己責任で行ってください。翻訳版の情報の正確性についてご不明な点がございましたら、公式版である英語版のホワイトペーパーをご参照ください。

※This booklet was created by the JAPAN CERTIFICATION CORPORATION on behalf of the Ministry of Economy, Trade and Industry in 2020.

※本冊子は、令和3年度経済産業省委託事業の予算で日本認証株式会社が翻訳しています。

概要

ますます多くの機械がファクトリーオートメーションとロジスティックオートメーション、モビリティとヘルスケアのプロセスに統合されるにつれて、それらと共に働く人々のための安全な手順を確保する必要性が増している。電気技術システムと人々の間の関わり方において、インターネット・オブ・シングス（IoT）、ビッグデータ、高度なロボット工学、特に人工知能（AI）はすべて変革し続けている。職場での効率をAIは劇的に改善でき、人のパフォーマンスの能力を引き上げることができる一方で、結果的として機械類が優秀な知能を備え、人がコントロールを失ってしまうのではないか、という疑問が生まれる。起こりうる追加的リスクを含めたこのようなシナリオの蓋然性は議論すべき議題として取り上げられがちだが、新技術が導入される際には人が予見できない重要な結果が常に表層化することがよくわかる。したがって、過去のどの時よりも、新たな人と機械の関係の中心に人の安全が確保されることが重要となる。

国際労働機関（ILO）の最近発表された推定によると、年間278万人の労働者が職場の事故や業務上の疾病で亡くなっている。何百万人を超える人が業務中、事故に遭っている。こういう要因が引き起こす経済コストとは別に、計り知れない人の苦しみを生み出す実体のない被害が存在する。過去1世紀にわたる調査と実践が繰り返し示しているように、関連する因果関係の大部分は回避可能であるため、これらは悲劇的で残念なことである。

人が労働災害において主要な役割を担っているため、設計や計画段階、そして業務の実施中に関わらず、人と機械の協業上の安全向上のいかなる取り組みも特に人・労働者の行動に重点を置かなければならない。また、未来は精巧に予見することが難しい一方、技術的、社会的、そして、法的メガトレンドは明らかに仕事や安全にインパクトを与えるであろう。

この白書では、実際の例を取り上げ、国連の持続可能な開発目標や、将来への革新的な安全解決策を開拓するプロジェクト、仕事、企業のさまざまな実生活例のような現在の社会の風潮とイニシアチブを参照することで、将来の安全について触れている。これらの解決策に共有することは、安全の考え方は人や機械、環境が協調する総合的なシステムにもたらされることを実現することが根底になっている。また、この白書では安全のための三者連携システムという協業フレームワークを紹介する。この概念は将来の安全のキーとなる要素を分析しながら体系的なアプローチを促進する。

三者連携システムと結びついて意欲的なビジョンを結実させるには、標準化、例えば機械と人の間での意思決定に関しもっとも圧力のかかる挑戦を緩和するというような視点から、安全に対する包括的なアプローチを拡大すること同様に、とてつもない努力が求められる。このように白書はこれらのニーズに対応するため、今後求められるであろう将来の安全のフレームワークを示す。

白書はIECとその委員会に特化して言及すると同様に、一般的な性格のものに対しても推奨事項を策定し締めくくる。
主な推奨事項として提案されたものは：

- 人と機械の分離に基づく安全から、人と機械が一体となって安全が達成される安全モデルへとシフトをしていくことで、安全性と効率性の両方を目指す社会的目標を確立する必要がある。

概要

- 人と機械が一体の新たな協調システムでは、人が最も優秀な構成要素ではなり得ない点を考慮すべきで、新しい安全のコンセプトが技術開発を通して創り上げられ、そのシステムにおいて人の位置づけを再構築すべきである。
- 安全性の結果を測定することは、事故発生統計に焦点をあてた長年の安全管理システムの重要な部分である。ただし、「先行」指標を導入することでより前向きで積極的なアプローチを予測に反映できる。
- 標準化機関は安全への包括的なアプローチを拡大し、深める必要があり、従来からの技術的な専門知識だけでなく、安全心理学、社会学、人間行動学の分野で収集された考察を統合することも求められる。言い換えると、将来の安全規格の開発において非技術的な要因にも焦点をあてることが推奨されるということである。

謝辞

この白書は、堤和彦博士（MSB委員長、三菱電機株式会社）が率いる将来の安全プロジェクトチームのIEC市場戦略評議会（MSB）がプロジェクトパートナーであるDr. Coen van Gulijk（TNO：オランダ）が中心のサポートによって作成された。

マネジメントチームは以下のとおり。
プロジェクトチームが次に続く。
（アルファベット順）：

Dr Kazuhiko Tsutsumi, Mitsubishi Electric Corporation, Project Director, IEC Vice President, MSB Convenor

Dr Coen van Gulijk, TNO, Lead Project Partner

Dr Atsushi Miyoshi, Mitsubishi Electric Corporation, Project Manager

Mr Dragi Trifunovich, Mitsubishi Electric Corporation, Project Manager

Mr Masao Dohi, IDEC, Project Manager

Mr Shawn Paulsen, CSA Group, IEC Vice President, CAB Chair

Dr Tommi Alanko, Finnish Institute of Occupational Health

Mr Tadashi Ezaki, Sony, SMB member

Dr Toshihiro Fujita, IGSAP

Mrs Jillian Hamilton, Manage Damage

Ms Rieko Hojo, JNIOSH

Mr Yun Chao Hu, Huawei

Mr Philippe Juhel, Schneider Electric, ACOS Chair

Dr Jens Jühling, BG ETEM

Mr Toshiyuki Kajiya, IGSAP, CAB Alternate

Mr Hiroo Kanamaru, Mitsubishi Electric

Dr Nobuyasu Kanekawa, Hitachi Ltd

Mr Pete Kines, National Research Centre for the Working Environment (NRCWE) (DEN)

Ms Tomoko Konya, NARO

Mr. Peter J Lanctot, IEC, MSB Secretary

Mr Vimal Mahendru, Legrand-India, SMB member

Mr Steve Margis, UL

Mr Hirokazu Nakano, METI

Mr Alan Sellers, Dyson Technology Ltd

Mr Shimizu Shoken, JNIOSH

Ms Thu Thủy Tran, NARO

Mr Bernd Treichel, ISSA

Mr Andy (Di) Wang, Huawei

Mr Joeri Willemsen, TNO

Mr Tsutomu Yamada, Hitachi Ltd

Dr Gerard Zwetsloot, TNO, Gerard Zwetsloot Research & Consultancy

目次

略語リスト

技術、及び科学用語

AGV	無人搬送車
AI	人口知能
API	アプリケーションプログラミングインターフェース
ATEX	爆発の可能性がある雰囲気内で使用を目的とした設備防護システム
BBS	行動科学セーフティマネジメント
BIS	建物情報システム
BSP	基本安全規格（国際電気標準会議）
CA	適合性評価
CAD	コンピュータ支援設計
CAM	コンピュータ支援製造
CCPA	カリフォルニア消費者プライバシー法
CDD	共有データ辞書（国際電気標準会議）
CSL	協調安全レベル
DC	直流
DL	ディープラーニング
EMI	電波障害
GDP	国内総生産
GDPR	一般データ保護規制
GPS	全地球測位システム
GSP	グループ安全規格（国際電気標準会議）
HPC	超高性能計算
HV	ハイブリッド車
IC	情報通信
ICS	工業制御システム
ICT	情報通信技術
IoE	全てのインターネット
IoH	ヒトのインターネット
IoT	モノのインターネット

ISMS	情報セキュリティマネジメントシステム
JTC	合同技術委員会
LGPD	一般保護規制(ポルトガル語では*Lei Geral de Proteção de Dados*)
LTE	ロング・ターム・エボリューション
LVDC	低電圧直流(給電)
OSH	労働安全衛生
PSS	製品安全規格（国際電気標準会議）
PV	太陽光発電
RAMS	ラムズ規格（信頼性、可用性、保守性、安全性）
RFID	無周波数識別
SBA	セーフティベーシックアセッサ（資格）
SC	小委員会（国際電気標準会議）
SCADA	スキャダ
SDG	持続可能な開発目標（国連）
SEG	標準化評価グループ（国際電気標準会議）
SELV	安全特別低電圧
TC	技術委員会（国際電気標準会議）
UAV	無人航空機
UWB	超広帯域無線システム

組織、機関、及び企業

ACOS	安全諮問委員会（国際電気標準会議）
CAB	適合性評価評議会（IEC,国際電気標準会議）
CASCO	適合性評価委員会(ISO,国際標準化機構)
EU-OSHA	欧州労働安全衛生機構
IGSAP	一般社団法人 セーフティグローバル推進機構
ILO	国際労働機関
IRGC	国際リスクガバナンスカウンシル
ISSA	国際社会保障協会
JISHA	日本労働安全衛生協会

MSB	市場戦略評議会（IEC,国際電気標準会議）
NARO	国立研究開発法人 農業・食品産業技術総合研究機構（日本）
NECA	日本電気制御機器工業会
SMB	標準管理評議会（国際電気標準会議）
WHO	世界保健機関

用語集

自立的な可動性
autonomous mobility
車載人工知能と連携するシステム（AI）
自動無人運転車の予測できない状況で判断を支援するリモートヒューマンサポート付き

基本的な安全に関する出版物
BSP
多くの電気技術に適用可能な問題、製品に関連する特定の安全関連に焦点を当てたIEC出版物

行動に基づく安全
BBS
継続的に自身と他の労働者と他の日々の行動において注視する経営陣と従業員間の安全パートナーシップを構築する過程

循環経済
circular economy
無駄をなくすこと、リソースの継続的な使用を目的とした経済システム

デジタルトランスフォーメーション
digital transformation
過去の非デジタル、あるいは、手動プロセスからデジタルプロセスへの変革による問題を解決のための、新しく、速く、頻繁に変化するデジタルテクノロジーの使用
注）デジタルトランスフォーメーションの例は、クラウドコンピューティング

デジタルツイン
digital twin
digital replica of a living or non-living physical entity
＜翻訳注:意訳しています＞リアル（物理）空間にある情報をIoTなどで集め、送信されたデータを元にサイバー（仮想）空間でリアル空間を再現する技術

量子もつれ
entanglement
ペア、または、グループの各量子の状況が他の量子の状況とは個別に述べられないような方法でペア、または、グループの量子が生成され、相互作用され、あるいは、空間的接近共有される時に起こる物質的現象

グループ安全出版物
GSP
2つ、またはそれ以上の範囲内の技術委員会内での特定の製品グループの安全面をカバーする出版物

国際労働機関
ILO
国際労働基準の設定を通じて、社会的、及び 経済的正当性を推進する国連のエージェント

モノのインターネット
IoT
物理世界と仮想世界からの情報に対応し、処理する相互接続された物、人々、システム、情報リソースやサービス

ISO / IECガイド51
ISO/IEC Guide 51
標準の安全局面の包含を目的とした規格の起草者への要件、推奨事項を規定するISO / IEC合同出版物
注）ISO / IECガイド51は、人、財産、環境、あるいは、これらの組み合わせ、あらゆる安全面に適用できる。

重ね合わせ

superposition

システムが同時にいくつかの別々の量子状態で存在する量子システムの特徴
注）重ね合わせは量子力学の基本原理

国連の持続可能な開発目標

SDGs

国連によって「すべての人にとってより良い、より持続可能な未来を達成するための青写真」として構築された17のグローバル目標の集合体
注）2015年に国連総会によって、国連決議70/1の一部を形成し、2030年までに達成されることを目的とし、作成された世界を変革する、持続可能な開発のためのアジェンダ2030

Wi-Fi 6

Wi-Fi 6

Wi-Fiテクノロジーの次世代標準
注）Wi-Fi6は、「AXWi-Fi」または「802.11axWi-Fi」とも呼ばれる。

第 1 節

将来の安全：課題、機会、標準化の役割

1.1 適用範囲

2030年までに、世界のほぼすべての電気技術システムにデジタルインテリジェンス（つまり、スマートオブジェクト、機械、及びデバイス）がある程度装備される。しかし、それに比べ、インテリジェントシステムが安全性、健康、及びウェルビーイングに影響を及ぼすかの理解がほとんどないように思える。職場の機械安全に関する要求はオートメーションの活用とともに急速に変化してきた。革新的な技術は保護装置を労働プロセスに統合することを可能にし、結果としてそのようなデバイスはオペレータに障害をもたらすことはもはやなくなり、その代わりに生産性をあげることに貢献してきている。

それにも関わらず、新しく複雑な安全性の要求がインテリジェントシステムの拡充化により表面化してきている。同時に、技術開発とデジタルの進歩は、これらの挑戦への革新的対応のためのツールを提供し続けている。

この白書では、電気技術システムの安全性に影響を与える開発に焦点をあてるだけでなく、そのような開発が行われるより広い社会経済環境を考慮に入れている。白書は職場にデジタルデバイスとロボットを導入するにあたってのチャレンジと、増加する人と機械の協業によって現れる特別なニーズを考慮している。しかしながらこれを超えて、この白書は社会的価値観に影響を与えるトレンド、文化の違い、職場の安全性の特性、規制の傾向を調べている。将来の労働者の安全、健康、ウェルビーイングに関する当該ゴールの具体的な実現に向けた標準化への寄与と同様に、国連の持続可能な開発目標(SDGs)　[1]の重要なフレームワークへの当該要因との幅広い関係性もまた考慮されている。

この白書の目的は、新たな技術環境で動作する公共の健康、安全促進にフォーカスされた人間中心の知的電気技術システムを設計するうえで、グローバルな規格開発組織の役割に前向きな影響を及ぼすことである。この安全性を確保することの責任は、政策立案者、規制者、産業パートナー、保険業者、学識経験者、及び調査機関、国連、及び非政府組織、多様なグローバル財団、開発当局などを含む多様なステークホルダーに課せられている。

トレンドについての議論の前置きとして、将来の安全に影響するイニチアチブと挑戦（Section2参照）、これらの挑戦を目指す際のキー要素とアプローチの確認（Section3参照）、そしてSection 4では考えられた三者連携フレームワークの適用領域の定義づけを行い、このセクションでは電気、社会経済要因や既存の安全性フレームワークに起因する現在の職場の事故事例を、人と機械の協業の安全機能を確保するための試みの中心に人への安全を置く必要性とともに検証する。本セクションはその試みにおけるIECの役割と、標準化の意味するところを概説して締めくくる。

1.2　職場での死傷者と電気

国際労働機関（ILO）の最近発表された推定によると、年間278万人の労働者が職場の事故や業務上の疾病で亡くなっている。[2]何百万人もの人が業務中、事故に遭っている。こういう要因が引き起こす経済コストとは別に、計り知れない人の苦しみを生み出す実体不明の被害が存在する。過去1世紀にわたる調査と実践が繰り返し示しているように、関連する傷害の大部分は回避可能であるため、これらの結果は悲劇的で残念なことである。さらに、モラルの欠落、アクシデントに続く仲間意識の希薄化や無気力感も経済活動に影響する。いかなる角度から測った、あるいはいかなる評価基準を利用した開発も、生命の喪失、生活の質の喪亡を正当化することはできない。

電力は本質的に不安全であると踏まえると、人が仕事で電力を利用する際に起こる犠牲は驚くことではない。しかしながら、グローバルにこのような事故の数を的確に決めることや、致命的な事故がどの位起こるのかを明確にするのは、死や傷害の原因特定と同様、容易な課題ではない。原則として、世界中の国において、義務的に職場の死傷者登録システムが維持されている。不幸にも、労働災害は世界中でさまざまな分野で違った記録のされ方をしている。

しかし、事故報告システムの煩雑さを考慮することがなくとも、我々は相対頻度を特定することによって電力関連事故の割合を推定することができる。この白書では、人と機械の傷害発生率や致死率を議論する際、二種類の報告様式について述べる

1）職場内と 2）職場外で報告された事故のカテゴリー：

- 消費者製品使用時のインシデント
- 製品設計欠陥による事故
- 製品欠陥に依らない、職場の製造時の不備と事故

電気系インシデント、あるいは事故の標準的な定義は直流による事故や傷害と関係している。電気技術の環境は変わってきている。今日ではコンピュータ関連、IOT接続、そして数えきれないほどの産業設備のアイテムが以前よりも随分多くパワー供給や、オペレーション、自動化において電気、及びサイバーに依存している。電気技術分野のインシデントや事故の正確な定義は考え直されるべきで、基準はこれらの出来事を計るために設計されるべきである。多くの先進国において電気システムによる事故での致死率幅は、1-4%（日本[3]）、及び3.5%（ニュージーランド[4]）;例えば、2.7%オーストラリア[5]とイギリス[6]　米国[7]では3.0%。

これらの割合は職場外のインシデント、死に至らない事故を含まず、経済的発展を遂げた国のみ対象で、発展途上国の事故による致死率は一般的により高くなると予想されることから、上記割合を指標としてだけ心に留めておくことが重要である。
しかしながら、少なくとも年間37万人の致命的な電気に関係する労働災害が継続的に存在する事実にも関わらず、これらの数値はそれでも比較的小さい。実際の死亡者数は相当数であるといえる。

1.3 概念、システムとしての安全性とパラダイム

概念としての安全は、障害（ハザード）の存在や、社会経済的なファクター、つまり規制、規格、業界でのベストプラクティスを含む安全のフレームワーク、個々のまたは特定の行動やその干渉、及び戦術等により修正され影響を受けたものが存在する中での人の行動が含まれる。このシステムは損失や、障害、死、ニアミスインシデントの頻度で測られる特定の成果を生む(図1-1参照)。

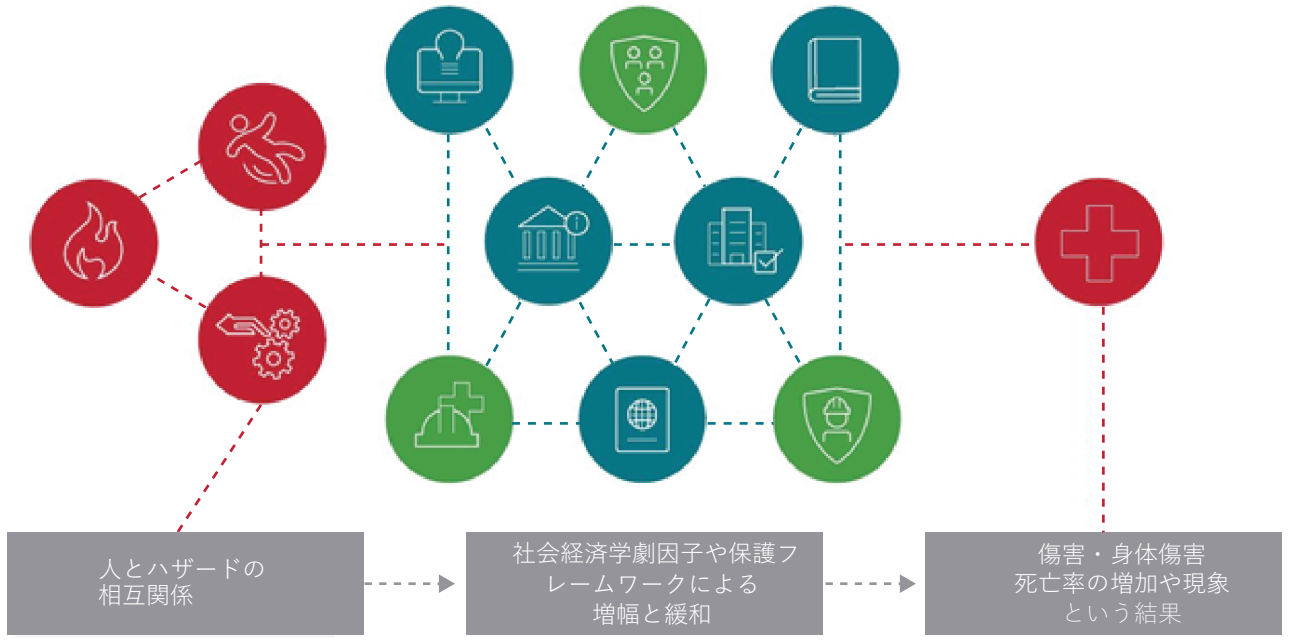


図1-1｜**安全システム**

ハザードに対する我々の理解も拡大し、健康やウェルビーイングに悪影響を及ぼしかねない心理的ストレスや低レベルの化学物質の被ばくのような慢性的なハザードを含めるようになっている。

社会経済上の条件、安全性のフレームワーク、及び特定の影響は安全の強化や低下にすべて作用している。最も広いレベルでは、社会、及び社会経済力はゆっくりと影響を及ぼし、安全性への影響を他のファクターから分離するのは難しいのかもしれない。しかしながら、そのような力は時間の経過とともに多大な効果を及ぼし得るため、無視することはできない。持続可能な開発目標を入念に練ることや、安全基準の有効性を高めることは、安全性向上のための前向きな条件づくりができるため、安全基準パラダイム全域において統合されるべきである。

1.3.1　社会経済的要因

ほとんどの社会は、人々に安全と不安のない環境を提供することを目指しているが、 その取組みの中でも資源の可能性には常に上限がある。その社会に対して利用可能な資源を評価する基準として、国の一人当たりの国民総生産（GDP）がある。単純に言えばGDPは、安全と他の社会的ニーズに対処するために割り当てられる財源の評価基準を提供する。

先進国では多量の「裁量ある」資源は、より安全なインフラや消費者保護、及びその他への政府支出を含め、特定の安全プログラムに割り当てるために潜在的に利用可能である。

財源が限られる発展途上国では、このような資源は基本的なサービスを提供するため、重要なインフラを構築するため、あるいは国全体の経済を形成、拡大するための取り組みに充てられる。これらの基本的な事象に対処することは、特に安全に関する事項を把握するのに配分される可能な資源としてはより少ない。しかしながら、良いニュースとしては、基本的なサービスとインフラストラクチャに対処することは安全性の向上と相互に関連する。

たいていの社会において最も影響力のある組織はその国の政府である。必要不可欠のサービスの提供者、規制や政策の起案者、及び経済資源の最も重要な基となるものの一つとして、政府は統制する人々の日々の生活に直接的に影響を与え、彼らの未来に大いに影響を及ぼし得る。政府の全体的な有用性を評価するいくつかの団体もまた、政府が安全のシステムを推進する役割であることにおいても評価している。政府の有用性がより高いレベルの社会では、より高い発展能力を示し、ポジティブに安全性に影響を及ぼすことができる政策を制定させている。政府の有効性が低い国々ではこの能力はしばしば著しくないがしろにされることや、正常に機能しないことがある。国連のSDGsは政府とすべてのステークホルダーに共に歩む動機付けを行い、開発に不可欠なキーエ

レメントを提供することを推し進めている。技術と機械が開発において不可欠なツールを構成しているので、SDGsの目的が技術を取り入れ生かそうとするのは当然のことである。このような開発は人類の安全に注視することが必須である。そういう観点から、人と機械のインターフェースで安全の技術的なフレームワークでSDGsを考えることは自然で不可欠な要求である。

IEC国際標準とIEC適合性評価システムは、SDGsの１７のゴール全てを満たす活動に貢献している。彼らは国や業界が持続可能な技術を採用し、構築し、ベストプラクティスを適用することを認め、質やリスクマネジメントと同じようにイノベーションの基礎を築いている。ほとんどすべてのSDGsはこの白書で取り上げられている安全面と安全に関する事柄を含んでいる。特に「SDG８：働きがいも経済成長も」、や「SDG３：すべての人に健康と福祉」が関連する。SDG８で構成されている目標の中で、機械やツールの安全、電子機器の安全、電磁波妨害（EMI）の保護と、全体的なリスクマネジメントは特に人と機械の協業環境での労働者のセキュリティと安全運転条件に影響する。この白書の後半で展開されるが、SDG３の中で医療機器技術に関してIEC技術委員会により触れられる点は、徐々に安全ソリューションの供えられた最先端の職場として統合されている。

同様に、教育を受ける権利は普遍的人権として広く知られる。これもはっきりと国連の枠組みの中でSDG４：質の高い教育をみんなに、として示されている。ただし、教育への関わりは世界中の個々の社会では大きく異なる。安全システムにおいて、研究者は安全性のレベルと基礎教育への広範なアクセスとの間に直接的な相関関係があることを示している。基礎教育は人々に、生活し、働き、人々やシステムに影響を与え得る重要な情報へのアクセス可能な環境をよりよく理解するための手段を提供する。さらに、教育システムの多くには安全に関する教育が含まれ、火災や溺死のような特定されたハザードについての詳細な情報も含まれている。

このように、良識的なアプローチは職場の安全や環境について考えられており、単なる電気の使用という枠組みを超えている。職場の安全衛生は持続可能な開発において、非常に重要になる可能性がある。労働安全衛生（OSH）の投資は国連のSDGsのアジェンダの重要な要素を達成することに貢献し得る。

技術はかつてないほど世界中で進歩している。コンピュータ関連、コニケーション、材料科学・工学におけるイノベーションは個々や共同の進歩に貢献している。大抵の部分において技術進歩は、よりよい製品やシステムを消費者に提供し、個人や環境リスクのレベルを下げるとともに生活水準を上げる。

さらに、テクノロジーは、ハザードを明らかにし、評価するのに活用され、より幅広く重要な安全情報の交換を促し、安全推進に重要な影響を与えながらより効果的な成果を得るためのプログラムと政策を調整する。

1.3.2　安全フレームワーク

安全フレームワークは、傷害防止に関連する特定のゴールを達成するにあたって、組織と資源を活用する方策とその実践である。安全の成果に直接インパクト与える政策領域としては、道路上の安全性、安全労働委衛生、消費者保護や法と標準などがある。

交通事故は傷害発生におけるもっとも最大の要因で2017年だけで世界で発生した死亡事故は推定120万人。急な都市化や多くの発展途上国の中流層の拡大により、道路上の安全は世界保健機構（WHO）、多くの市民社会団体においても過去10年で最も注視すべきものとなってきている。現在では多くの政府や団体は単に事故の運転手個人を責めることに留まらず、交通計画、道路インフラ、車両安全や歩行者を含めた道路規制の価値を認める安全システムのアプローチも含めるようになっている。

多くの成人が人生の約１/３を仕事に費やし、多くの職業において労働者は重要な安全衛生ハザードに直面している。労働に関連するリスクは、労働者をリスクから守ることを意図した規制や標準に見られるように、職業により大きく異なる。ILOは一連の国際的な規約やガイドラインを構築し、労働安全衛生の最低限のレベルのものを提供している。しかしながら、ILOの規約導入にあたっては任意であり各政府の裁量による。各国におけるILO OSHガイダンスによる評価は、世界の労働者の安全の相対的強度を測るものさしになり得る。

社会におけるすべての人は、物やサービスの消費者である。不安全な消費者製品の使用や露出は、結果的に火傷から中毒までさまざまな傷害を招く。不安全製品から人を守るのは企業、市民社会、政府の責任である。安全対策としては、安全設計、製造、輸入製品の検査と管理、市場からの不安全製品の撤去他、多くの安全対策も含む。これらの法律、規制や政策の相対的強度は、国内の安全システム全般において大きな影響を及ぼす。

行動規約や標準は、製造業者、敷設業者、建築家、建築業者、オペレーターに、製品やインフラに関する安全に言及するため、具体的要求、ガイダンス、ベストプラクティスを提供する手段である。多くの国では建築規約はビルの安全とセキュリティに対して最低限の要求を設定している。製品の安全基準は、製品やシステムがリスクを最小限にするように設計され、認められた基準で製造され、意図した使用者が安全に使用できるようにすることを確実にするために役立っている。このように規約や標準のしっかりとしたシステムは不安全製品や環境から人々を守っている。規格と適合性評価は、安全システム層の安全フレームワークの重要な部分を形成している。それらは両者共に規制（強制スキーム）から非公式規制（任意スキーム）へと循環している。

1.3.3　安全の結果

安全性の結果を測定することは安全管理システムの長年の重要なコンポーネントであった。まず最初にインシデント統計に着目すると、ごく最近、予防的アプローチの採用という観点からこのような指標が安全機能の「先行指標」として議論されるようになっている。包括的な安全性の姿を得るには、管理される特定のシステム要素と同様に、

安全エコシステムの各レベルが、さまざまな影響や外界に影響する環境を理解するために評価されるべきである。安全の共有システムの複雑さや多重さの評価には斬新なアプローチが求められている。システムの個々の評価の組み合わせで構成される複合的な指標は、ダイナミックで繊細で順応性があり、安全性に応用できる採用可能な評価法を構築するための1つの手法を構成する。

1.4 行動に基づく安全–人を中心に

さまざまな研究によると、設計や計画の段階あるいは作業を行う段階に関わらず、人は労働災害の原因と深く関わり続けている。全般的に、ヒューマンエラーの主な要因は76%から96%と推定されている[8]。通常、企業は安全に対する業務態度を教育と執行を併せることにより反映させようとしている。しかしながらこれまでのところ、安全に関する行動やアクシデント発生率の持続的な変更を生み出すようなこれらのアプローチの成功を確認する管理された研究はない。結果として、人と機械の協業における安全を改善する取り組みは、人の行動、管理者と労働者の行動を含んで特に注視されなければならない。これは行動分析が重要な価値をもたらしているということであり、特にそのアプローチは「行動科学セーフティ」(BBS)と呼ばれている。

行動分析は、1930年代に科学者によって実験室での実験をベースに制定された行動に関する自然法の一連であり、おおよそ1世紀前にさかのぼる。[9]その結果出された見解は、行動は、前例の影響、オペラント条件付け、及び環境要因の元、特定の行動のタイプを生み出す非人間的なシステムとしての行動として捉えられた。[10]

その見解は、前例をきっかけにすることで、あるいは、それを可能とすることで、より特定された結果を生み出す行動へと至り、行動のための場面設定をすることを示す。すなわち、すべての出来事が行動により決定されるということである。この結果、将来の行動にはね返ってくる学びの機会を生み出す。

BBSには、職場の安全のための行動分析的な関与の戦略の適用が含まれる[11]。最初に、BBS測定は、アクティブ、観察可能、測定可能で信頼できる方法で安全行動の観察を可能とする状況下で行われる。適切なステップが踏まれる状況では、労働者の行動に関する信頼のおけるデータが科学的に信頼のおける関与の基礎として使用される。このような関与の成功を決定する要因には以下が含まれる：

- フィードバックの受け取り手は、彼らの行動変更により達成できる安全目標の設定。
  目標設定は行動、目標達成は行動変容を増強する。
- 労働者に対する行動に特化したフィードバック。
  フィードバックを通じての行動のみ変更可能。
  フィードバックは個人的、かつ労働者個人の行動に関して、あるいは折れ線グラフ形式でグループに特化したもののいずれかを提供。
- 前向きな強化による行動変容
  行動を促進するためにさまざまな認証形式が活用される：
  賞賛、社会的認知、あるいは単に安全行動が評価されているという確認。

1.4.1 安全リスク管理：リスク分析と評価

BBSは、人の行動を管理するためのアプローチであるが、安全確保のリーダーシップとマネジメント戦略からは切り離して考慮することはできない。大きくは、安全リスクマネジメントには、事故予防、事故発生時の影響の最小化、柔軟かつ効率的な復旧を可能とすることによって、人の安全を遵守することを意図したビジネスプロセスの、

実用的、効率的かつ効果的な導入が含まれる。安全マネジメントには、安全を推進するための政策、適用、手順、実施の体系的な適用が含まれる。

従来、ルールや手順は専門家や執行者により影響を受けるタスクやリスク分析をベースとした静的な道具であり続けてきた。これらのルールはマニュアルやデータベースで文書化され、コンプライアンス遵守に署名を求められる従業員とともに、トレーニングという形で全従業員に利用可能となる。これはトップダウンやルールに対する合理的なアプローチを含み、そして、未熟練労働者や緊急対応に取り組む訓練者によって実施される日常業務を含んだ状況では最も効率的である。.

しかしながらルールは、ルールを実践する人の行動や活動による経験をベースとした行動パターンとして表面化する。文書化されたルールとは対照的に、これらの手順はある特定の活動や状況において局所的であり応用可能である。ルールに対するこのアプローチは、ボトムアップでダイナミック、そして決して完璧なものではなく、常に特定の状態や状況で適用を求められるため、手順指示に対する感度がベースとなっている。それは、外科医、パイロットや船員のように、広範囲に及ぶ経験と深い知識があってアドバイスをする程度で済むような人材の場合のように、バラエティに富んで不正確なものに対する柔軟さを含むダイナミックさ、複雑さ、相当の不明瞭さ・高リスクの業務に最適である。フィードバックをベースに行動規則を深化させ更新し、磨き上げるには専門知識を必要とする。両アプローチは将来の安全に必要な行動規則の側面を明確化するのに必要であり、それらを補完するものである。[12] [13].リスク分析は安全マネジメントにおける重要な部分を形成し、以下の活動を含む。

- リスク活動が行われる状況を明確にする
- リスクを評価する
- 必要な安全策を講じる
- リスク、及び採用した対策をモニタリングする
- 安全マネジメントシステムのすべての側面を評価する
- 差異を記録し、必要機関へ報告をする

安全マネジメントは安全エキスパートや管理者、そして労働者と協力し安全で有能な生産システムを得ることが求められる。それはマネジメントと意思決定のなくてはならない部分であり、戦略的、運用的かつ計画あるいは企画レベルにおいて適用される。

安全リスクアセスメントアプローチは、製品やシステムの設計、生産、流通、利用（メンテナンスを含む）、破壊や廃棄から生じる人に対してのリスク削減を目指している。製品やシステムの完全なライフサイクル（意図的な使用、及び合理的に予見可能な誤使用の両者を含む）は、製品やシステムが産業上のプロセス、職場、家庭内の環境、あるいはレジャー活動において使用されることを意図しているかどうかが考慮されなければならない。ゴールは人、財産、及び環境にとって許容可能なリスクのレベルに達することであり、悪影響を最小化することである。

安全リスクアセスメントの根本的な指針は、安全側面を考慮するかどうかに関わらず、また設計者、製造業者、サービス提供者、政策立案者や規制者のような他のステークホルダーに対し、有効な参考として活用され得る。一般的な安全関連のガイダンスとリスクアセスメントの側面に関してはISO / IECガイド51でカバーされている。低電圧機器の開発と関係する安全関連のリスクアセスメント、及びリスク低減に関する固有のガイダンス、及び関連規格はIECガイド116でカバーされる。

1.5 安全確保におけるIECの役割

電気システムの安全性はIECにとって常に重要な関心事である。人と機械の安全に言及する最初の技術委員会（TC）を1926年に立ち上げて（TC 16：人と機械のインターフェースに関わる基本安全原則、マーキング、及び識別[1]）以来、IECは何十もの新しいTCを、安全が標準化作業において中心となるべき人々のために立ち上げた。

しかしながら、IEC規格の多くがさまざまな安全面をカバーしているため、安全に関する事項はこれらの特定の技術員会に限定していない。IEC安全諮問委員会（ACOS）は、複数のTCが関与する困難な案件や各TC内での異なった意見を議論するフォーラムを提供することと同様に、IECのTC/SCに対し安全への疑問に応える包括的なガイダンスを提供する。IECは技術開発と並行し続けるため、基本安全とグループ安全の出版物は定期的に改正される。新規出版物が発行されると古いものからアップデートされる。このリストは安全機能タブの下にあるACOSのウェブページの安全機能タブ[2]で確認ができる。

IECはまた、製品、システム、サービスや認証スキームを含む規格グループの照合作業に向けた一定のアプローチを確立するための水平規格を発行してきている。IECガイド108は水平機能と水平出版物を扱うルールを取り決めている。それはまた、ISO/IEC指針や関係する特定のガイドと連動して使用される。IECガイド104は特に水平安全出版物の開発に関するルールを制定している。

IEC水平規格の構造は図1-2に示す。

図1-2｜IECガイド104に沿う安全の照合基準

IECガイド104は次の開発過程を含む：

- 基本安全出版物（BSP）は次のような水平安全原則を含む：
  - IEC 60529
    エンクロージャー（IPコード）による保護の程度
  - IEC 61508（すべての部品）、電気/電子/プログラム可能な電子安全関連システムの機能安全
  - IEC 61140、感電からの保護－設置と機器の一般的な側面

1 SMB決定143/18、SMBはTC 16の解散、及びTC16出版物所有権のTC3への譲渡を確認した。

2 www.iec.ch/acos

- 以下のような一般的な安全設備タイプを網羅するグループ安全出版物（GSP）：
  - IEC 60364-4-41、低電圧電気設備－パート4-41：安全のための保護－感電に対する保護
  - IEC 62477（すべての部品）、電子コンバータシステムと設備に対する安全要求
- 次のような特定の安全ガイド：
  - IECガイド110、家庭用制御システム－安全に関するガイドライン
  - IECガイド112、マルチメディア機器の安全に関するガイド
  - IECガイド117、電気技術設備－触れることができる高温の表面温度
- 次のような特定の製品の安全関連要件をカバーする製品安全規格PSS）：
  - IEC 62368-1、オーディオ/ビデオ、情報通信技術設備－パート1：安全要件

1.6 標準化の意味

コンピュータは、労働者が産業界で活動する手段を変化させながら業界全体が機能する手法を変革してきた。デジタル革命は、従来人類とのみ関連する側面を追加することにより電気工学の従来から達成できることを超えた機能性を創り上げてきた。知能である。他の分野のスペシャリストからの情報提供が求められているため、基本原則、調和、標準化に関する議論は、もはや電気技術者のみの範囲に限られない。1987年にIECは、情報技術に関する合同技術委員会1（ISO / IEC JTC 1）の創設を通じてISOとの協力により、順応をこの取組を実施してきている。この委員会には人工知能（SC42）、文書記述と処理言語（SC34）、ソフトウェアとシステムエンジニアリング（SC7）のような幅広いトピックに取り組む20以上ものの小委員会がある。

第 2 節

将来の安全に影響を与える動向、イニシアチブ、挑戦

2.1 はじめに

さまざまなタイプの社会的メガトレンドが、かつてない機会や将来の安全に関する展望を生み出している。しかしながら、それらの精力的な参入により、一連の新しい挑戦と脅威をもたらすことにもなる。ビジネスストラテジストのサトワント・シン氏はこのメガトレンドを「グローバルな持続性とビジネス、経済、社会、文化、及び個人生活に影響を与える発展のグローバルな持続性とマクロ経済力、それによる我々の未来の世界と変革の速度の上昇」[14]と定義している。

未来は正確に予見できない一方で、技術的・社会的メガトレンドは労働と安全の未来に明らかに影響を及ぼす。これは人口統計の進化、グローバル、及びローカルな経済傾向や政治転換、これらの激動と大変革に関しても当てはまる。現在起こっている劇的な変化は、グローバルレベルで不安定さと複雑さを増し、社会や職場において不安定さを引き起こし、不確実さとあいまいさを招いている。結果的に、従来のリスクマネジメント、安全、及び標準化に関するアプローチはもはや、十分でなく、再考が必要とされている。

白書のこのセクションでは、安全性の問題と未来の解決策に影響する技術的、社会的、法的な傾向を明確にする。この簡潔な調査の目的は次の2要素からなる：現在進行中の変革とこれから先の10年にわたるデジタルテクノロジーの基本的な理解を確実にすること、そして社会の発展においてこれらの進歩のために推定される影響、及びどのように社会が機能するかという点において結果として生じる変化を評価することである。

2.2 新たな安全を切り開く先進技術

インテリジェントな機械は社会のほとんどの局面に影響するデジタル革命の初期的なドライバーを形成している。この変革は世界では、ドイツでは「インダストリー4.0」、中国では「スマートマニュファクチャリング」「メイド・イン・チャイナ2025」、フランスでは「インダストリー・イン・ザ・フューチャー」、日本では「コネクテッドインダストリーズ」或いは「ソサエティ5.0」のようにさまざまな名称で呼ばれている。このデジタル革命はインターネット・オブ・シングス（IoT）、ビックデータ、人工知能（ＡＩ）、先進ロボット、クラウド/エッジシステムのような既存のテクノロジーがベースとなっている。これらのさまざまなシステムは、大量のデータ集積を運用し、未加工のデータから関連する情報を抽出し、情報を読み取みとり、特定の要因間の未解明の関係性を検出し、自動識別し、未来の傾向を予測する効果的な分析を可能にする大量のコンピューティング性能を提供する。これらのシステムはより正確な予測や人が成し得るよりも大量なデータを処理できるため、人知を模倣する（あるいは、むしろ超える）アプリケーションもいくつかある。

デジタルテクノロジー、及びその応用は、経済界の選ばれた産業や分野に限定されることなく広範囲に及んでおり、金融システム、モビリティ、ヘルスケア、教育、一般的なウェルビーイングなど、社会のあらゆるレベルに影響を与えている。工場、交通システム、パーソナルヘルスケア、ホームサービスの情報スペースは、しかし、ますますデジタル化され繋がっていくであろう日々の生活の局面でもある。

これらの変化は21世紀において、安全性を含めた社会的、政治的、文化的、経済的な発展をもたらす。

仕事や人生の多くの側面に破壊的な影響を及ぼしかねないキーテクノロジーとしては以下のようなものがある[3]：

- 人工知能
- バーチャルリアリティとデジタルツイン
- ホログラム
- スマートアシスタンスとロボット工学
- 自律移動と運転
- 6G、及びF6Gに基づく超高速ネットワーク
- 5Gワイヤレス、及びWi-Fi-6
- ブロックチェーンテクノロジー
- エッジコンピューティングとクラウドコンピューティング
- 量子コンピューティング

これらすべてのテクノロジーは現在まだ幼少期である。しかし今後10年間に日常生活に溶け込み、仕組みが形成される可能性が高まる。これらのテクノロジーの期待される能力と、潜在的な影響は次の通りである。

- **チップ上の人工知能**：
  AIチップセットは、ローカルな作業環境でAI加速を可能にする過程において、チップの中でのクラウドベース運用のAIアルゴリズムに対するソフトウェアの情報通信回路（IC）への移行を含む。このようなチップセットはAIアプリケーションに優れたアクセスを提供するだけでなく、実質AIの活用可能性を広げる。結果的に、情報通信（ICT）システム全体が最適化されるように変わる。機械搭載AIは、人と機械の相互関係の各局面で散在するようになるだろう。

- **超高速固定ネットワーク**：
  このようなネットワークはF6G（固定回線6G次世代）をベースにする。固定ネットワークの未来は完全に光通信化している。F6Gギガバイトネットワークは帯域幅、接続数、ネットワーク体験という3つのキーカテゴリーで大きな進歩を見せている。これらのF６Gにおける３つの注目点は、従来からの産業へのアクセスシナリオでユーザー体験を向上させ、そして光ファイバー網が従来からの産業バリアを克服するのを助け、これにより企業、交通機関、セキュリティやキャンパスなどの多様な分野へ迅速に浸透する。F6Gは産業が現在よりもより速いスピードで変革することも支援する。

- **超高速モバイルネットワーク**：
  6Gに基づいて、このようなネットワークは、同様の機能を提供する。6Gを組み込んだパイロットアーキテクチャは2030年頃を予定しており、商用6Gは2030年から2035年にかけて発売が予定されている。ワイヤレスセンシング、

  イメージング、ロケーション判別におけるさまざまな6G機能は、マルチテクノロジーの異機種環境ネットワークの支援を可能にする。よって、スマートマニュファクチャリング企業が異なったアクセスネットワークを配置すること、、及びオペレーション上の機能でAIを統合することを許容する。６Gネットワークは必要なコミュニケーション、コンピューティング、AI性能にアドレスする単一プラットフォームを提供する。これは知能を一元化させ、分配することを許容することである。（エッジで）

- **量子コンピュータとネットワーク**：
  量子コンピュータは、データの業務執行のための重ね合わせと絡み合いのような量子力学現象を直接的に利用する計算システムである。量子計算は２進数（ビット）代わりにクビット（量子ビット）を使用し、量子ネットワークは物理的に分離した量子プロセッサ間で量子ビットの伝達を促す。

3 https://future-summit.com/webinars/10-megatrends-and-future-technologies-2020-2030-business-new-part-1-2 を参照[ユーザーアクセスにパースワードが必要]

量子コンピュータとネットワークは演算（ある種の演算において何千年もかかっていたものがほんの数分へと演算の回数が減っていく可能性を秘めている）とネットワーク形成（まさに光速データ伝送で行う）において、共にかつてないスピードを約束する。

センサー、カメラなどを含めた最新のICTの開発は、企業が、ある一定の安全リスクに関するリアルタイムに情報収集することを可能にし、これらは特に直接的あるいは間接的に人や機械の動きと結びついている。そのような情報、及び再度

ICTに基づき、そのようなリスクの動的制御を開発することが可能になりつつある。既にある例としては、いかに日本の鉄鋼エンジニアリング会社がフィールドエンジニアや現場作業員のための安全監視解決策を実践するかというものである。図２－１に示すように、プラットフォームは各現場作業員の状況やステイタスを登録する。体温、心拍数、姿勢といった労働者の情報に加え、取り巻く状況は、装着型のカメラを通じてデータに変換され、データプラットフォームのAIエンジンにより分析される。この方法で、管理者は前もって事故を防ぐために必要なアクションが知らされることができる。

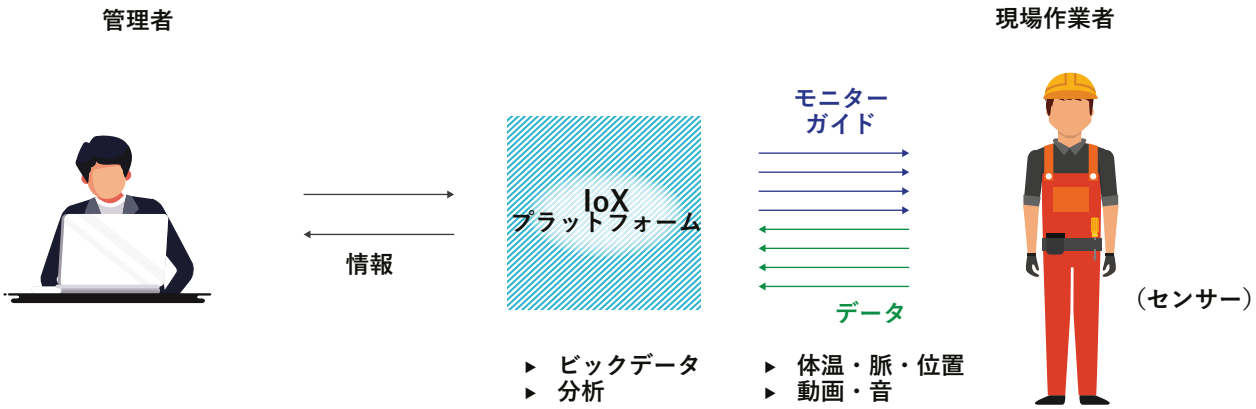


図2-1｜リアルタイムリスクアセスメントと管理

新しいテクノロジーの到来は、いくつかの手法で労働にインパクトを与える。職場の安全衛生に関する欧州当局（EU-OSHA［15］が2019年に、このようなテクノロジーの直接的影響下のデジタル環境において、職場での人間関係の変化にフォーカスした調査を実施した。結果として、次のような特徴を示した。

- 人と機械の協力の新しい形
- プラットフォーム（またはギグ）経済の出現
- 作業の個人化の増加
- 在宅勤務の拡大
- 画面を見ている時間の増加とデスクワークの増加

新しいテクノロジーの急激な広がりにより、AIの適用が人とうまく関わることを確実にする具体策の必要性が高まる。EU自体が、AIをツールとして許容しており、AIが使用にあたって信頼のおけるエコシステムを構築するために７つの原則に従う必要がある旨を述べた白書を発行している。［16］：

- 人為な作用と過失
- 技術的な頑健性と安全性
- プライバシーとデータガバナンス
- 透明性
- 多様性、無差別、及び公平性
- 社会的、及び環境的なウェルビーイング
- 説明責任

最後に、デジタル化の新たな時代もまた、たいていのテクノロジー応用のシームレスな機能が、ソフトウェア更新の利用可能性や優秀さを含むソフトウェアの質や（サイバー）安全に依存しつつある。

デジタル化におけるテクノロジーのメガトレンドの優位性は、他の技術領域におけるメガトレンドも、今後10年には人の営みへ影響を与え得るという事実を除外することはない、ということに留意すべきである。これらの中で最も優れたものは、ゲノム編集、免疫療法、アンチエイジングに関する調査、クローン技術のような生命科学における発展である。現在起こっていること、あるいは拡大が期待されるいずれかの一方が関連する他の技術の発展は、ナノテクノロジーや非化石燃料エネルギー技術（太陽光、水素融合、新型原子力）の分野における応用に早い段階で導入される。これらの分野での技術的なブレイクスルーは他のドメインで起こることは明確であるが、それらの応用はデジタル化に影響を受けるであろう。

2.3 社会的、及び法的な傾向

高度な技術のメガトレンド加えて、社会の動向は今後10年間のビジネス、仕事、生活に大きな影響を及ぼす。

この事例が循環型経済の考え方であり、その原則は、SDG12：持続可能な消費と生産パターンを確保する、に示される。循環型経済は、製品、部品、資源の持続的再利用が、それらの基本的な価値を下げることなく効果を発揮する経済オーダーの実現を目指す。循環供給物、資源回復、製品寿命の延長、プラットフォーム共有やサービスとしての製品は、循環型経済ループの重要な要素となる。このタイプの経済は「生産販売終了という概念を復元という概念に置換し、再生可能エネルギーの使用へと移行し、再利用の価値を下げる有害物質の使用を廃絶し、素材、製品、システム、及びビジネスモデルの優れた設計を通しのゴミの廃絶を目指す」（図2-2参照）。

最近のトレンドがデータとプライバシーにも影響を与えている。EU個人情報保護規則(GDPR)が2018年5月に発効されて以来、世界のデータプライバシーがその焦点をガイダンスからステップアップされて強化される方向へとシフトされてきている。法的には、カリフォルニア州消費者プライバシー法（CCPA）は2020年1月1日に発効し、ブラジルでは一般データ保護規則（LGPD：ポルトガル語）が2020年8月にスタートする予定である。

これらの重要な２つの法の制定はGDPR[18]によって（すなわち、規制化へのシフトを通して）推進力を増大させる。これらの法令は、データ収集と処理はプライバシー保護、データの質と完全性、データの保護を確実にしなければならないとの強い信念を育むことになる。データアクセスの透明性、ルール決め、及び不平等な先入観や偏見をなくす方法がかつてないほどに重要となっている。政府機関や産業に「必須のインフラ」を形成する

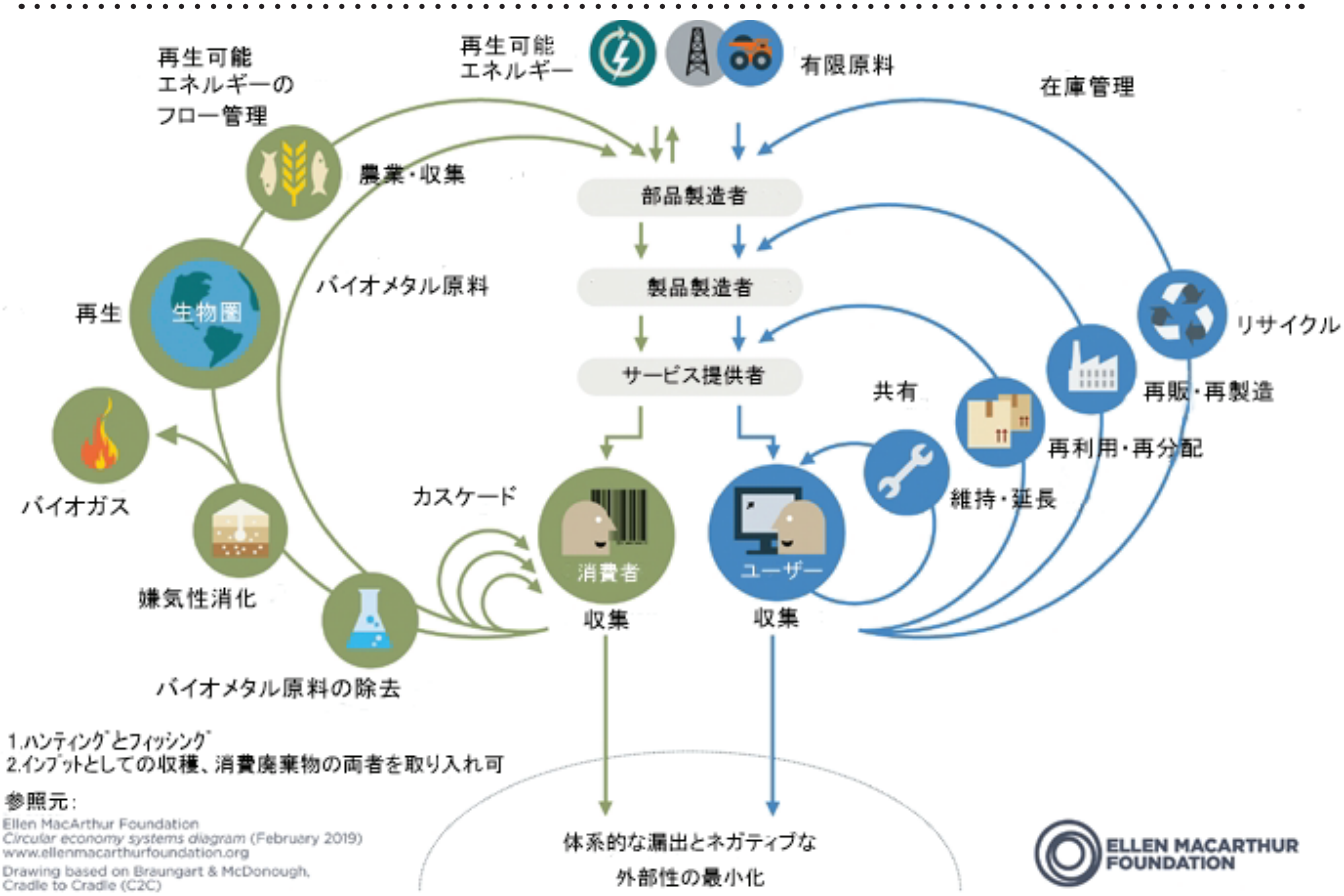


図2-2｜**循環経済におけるプロセス**[17]

部分とみなされる新しいテクノロジーの信憑性は、彼らの受容と採択にますます欠かせないものとなる。このようなインフラは守られ、物理的、及びサイバー的な攻撃、極端な気象条件や自然災害にも耐え得るものでなければならない。

2.4 追加動向、概念 、及びオプション

2.4.1 ゼロへの革新

もう一つの社会的概念として、「ゼロへのイノベーション」に向けての流れがある。シンによると、「・・技術的、経済的、人口統計的な発展よりももっと概念やコンセプトを…それは我々の社会の中で完璧を望む気持ちの表現である：ゼロ炭素排出量、ゼロアクシデント、カーボンニュートラルシティなどによって世界に貢献するビジョン」[14]。 したがってそれは、ゼロ欠陥、ゼロ故障にフォーカスした戦略を含む電気技術システムに適応可能でもある。ゼロへの革新はより良い世界ための長期的グローバル視野に緊密に関係し、例として、ゼロ貧困やすべての人々に働き甲斐のある人間らしい仕事があり、国連のSDGsで示されている。

ゼロへの革新はプログラムではなく、元来、運用戦略の採用にアプローチするものである。「ゼロへの革新における成功には、抜本的なゴールを前にしてそれを打開することを目指すアジェンダを必要とする。―ゴールとは、役にたたない外部性と欠陥のない、よりよい世界をつくることを意図している。」これは明らかに、企業の社会的責任や国連のSDGsと密接にリンクする倫理的な側面を含んでいる。それはまた、長期的な熱意、前向きなリーダーシップ、及び企業的、社会文化的支援を必要としている。

例えば、一般社団法人日本電気制御機器工業会（NECA）は2025年のビジョンとして「5ZERO マニュファクチャリング」を表明している。新的なテクノロジーを用い、欠陥ゼロ、生産ロスゼロ、納期延滞ゼロ、事故ゼロ、設備故障ゼロを目指し、努力することである。事故を完全に廃絶するという目標はまた、1973年に中央労働災害防止協会（JISHA：中災防）[4] により提唱された「ゼロ災害全員参加運動」の一環である。このキャンペーンは、安全の卓越性は、工場の卓越性や経済的成功に必要な要素とみなされるというビジョンに置き換えられる(図2-3)。

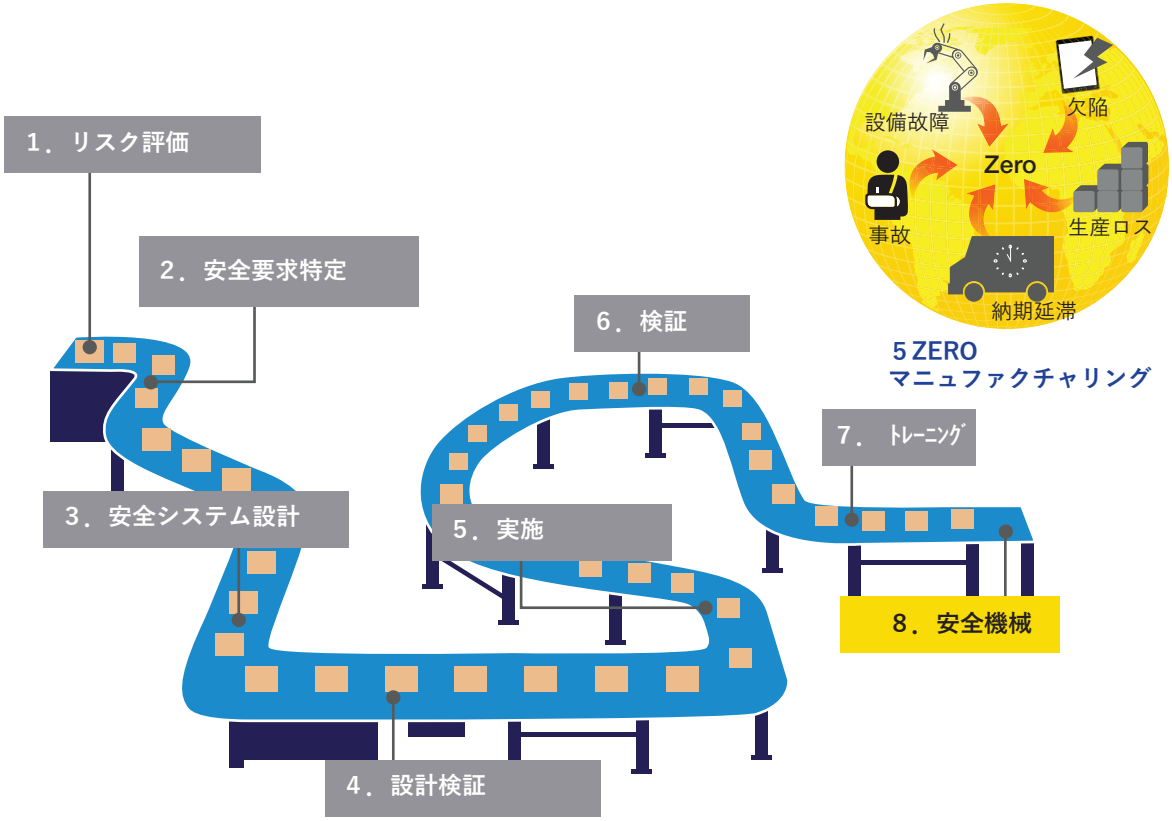


図2-3 | 5ゼロ製造[19]

安全プロモーションにおいて関連するイニシアチブは、安全性の領域を広げることを含み、健康、及びウェルビーイングも含めて既に労働安全衛生(OSH)の概念に既に組み込まれている戦略も含んでいる。職場の安全衛生とウェルビーイングは同じ人間・社会価値をベースにしているので、これらの分野での努力と目的の結びつきは３つのエリア間に相乗効果を生む。この融合は、国際社会保障協会(ISSA)により提唱された「ビジョンゼロ」と呼ばれる「ゼロへの革新」の概念に収斂される(図2-4)。

4　www.jisha.or.jp/english/index.html

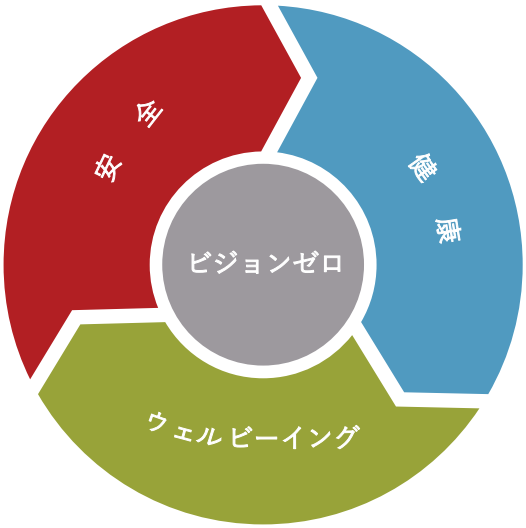


図2-4 |安全、健康とウェルビーイングの統合としてのビジョンゼロ [20]

ビジョンゼロは、「優れた安全、衛生とウェルビーイングを達成するために、安全で健康的な働き方[職場環境]を保証し、すべての事故、障害、労働災害を防ぐという展望とコミットメント」と述べられている。[21]これに関して、意図しない障害予防を超えて危険のないところに生じる情緒的安定や心理的安全のレベルまで含んで拡張すべきとの安全配慮の中心に人を置くことが重要である。[22]

ビジョンゼロでは6つの要素が強調される：

1) 安全、健康とウェルビーイングを促進するための戦略的取り組み

2) 安全なビジネスを構成する基礎としての、これらの要素の統合

3) この範囲で改善のための引き金となるイノベーション

4) 予防文化の開発

5) ビジネス倫理の基礎の構築と、企業の社会的責任、及び持続可能性のためのより幅広いプログラムへの貢献

6) ネットワーク構築、共創、共学習の要求

2.4.2 協調安全

リアルタイムのリスクアセスメントと制御の最初の経験は、協調的安全の概念の精緻化につながっている。このアプローチは、自らデジタルアプリケーションで構築された産業や経済を支援するために、デジタルテクノロジーと人と機械の関係性を活用している。このコンセプトは機械の安全性と、人と機械の相互作用の領域で開発されたが、他の多くの状況においても価値があり、応用できる。

ここに示す協調安全の概念は、いかに機械安全に対する取り組みが時間と共に発展してきたかのモデルである。（図2-5）この図のキーとなる点は、各進化の段階で人と機械が共存している状況において安全を確保する役割に注がれる特定の要素の識別である。最初に（セーフティ0.0 と呼ばれた時代）、安全は主に人の意識、能力、及び行動に頼っていた。人々は機械に存在する危険に注意を払わなければならなかった。

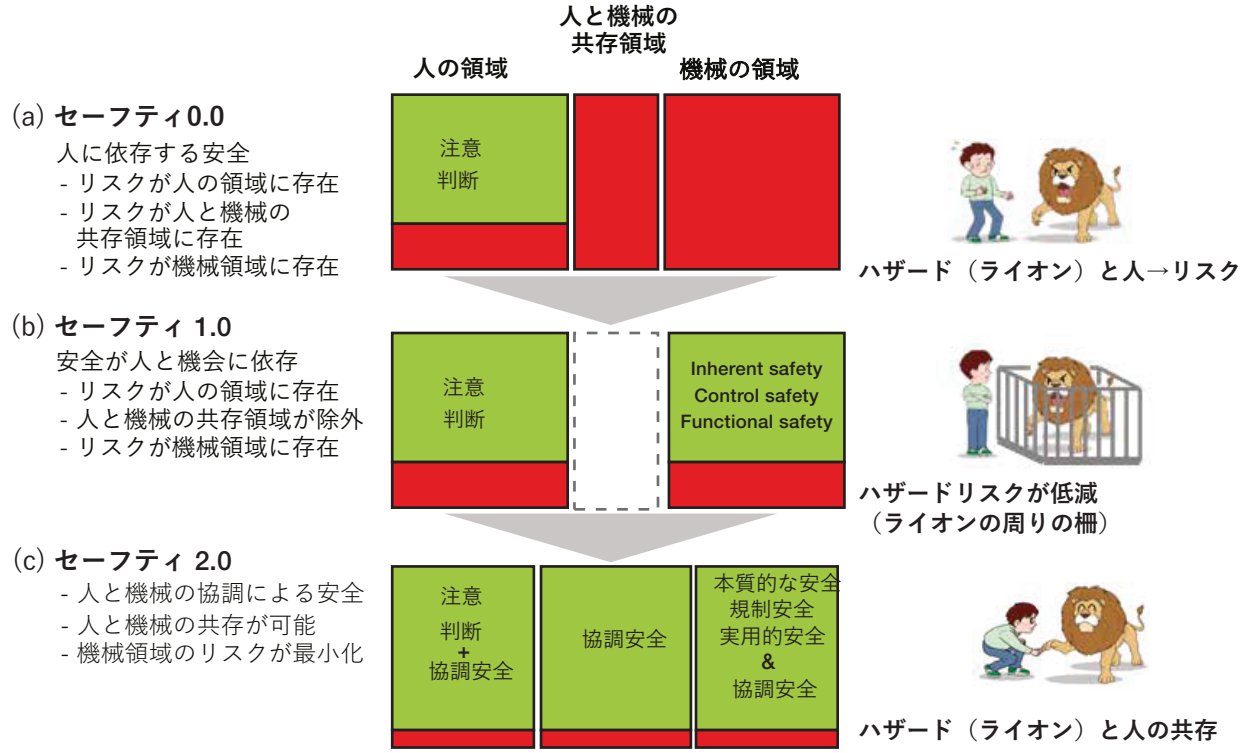


図2-5｜（機械）安全の発展における3つの段階

その次の段階では、機械がますます複雑なタスクを行うようになり、動く機械やシステムも危険な機械の動きからオペレーターを遮蔽するための安全対策が装備された。この段階での安全性モデル（セーフティ1.0）は、主に工学的ソリューション、つまり技術を介してのものであった。現在では機械の安全テクノロジーは主に3段階アプローチに基づくハードウェア志向の側面にフォーカスされている。即ちISO/IEC ガイド5.1に従い、１）本質安全設計、２）監視、及び保護装置、そして、３）使用上の情報。この段階で導入された基本原理は機械を人から分離することであり、機械と人が共存する際に、機械を人から離し、機械の動作を止めるということである。

IoT、AI、画像処理、ビックデータやその他のICTテクノロジーの進化は、以前では不可能であった安全機能を導入してきており、例えば経験の浅い作業員がいるところでの低速の動き、あるいは、危険時のオペレーションの一時停止といった柔軟なオペレーションを可能にする知能に投資されている。後半の状況では、例えば体調、経験または経歴、資格や能力など、いかなる作業員の存在にも関連するデータを機械に与える無線自動識別タグ（RFID）のような，人に装着可能なデバイスを介して機械へと送信されるデータに基づいて特定される。そのようなシステムが世界各地で発展し、セーフティ2.0と呼ばれる協調安全の新たな時代の幕開けとなった。

協調安全は人、機械、及びその動作環境がデジタル情報を互いに共有し、交信し、連携するときに実現する。その意味で環境には、物理的環境、組織、システム、データベース、標準、規制やルールが含まれる。

協調安全は、以前のアプローチとは異なり、人の能力に、テクノロジーや組織と同様、重要な同一レベルを置いている。スキル、能力、満足度、自己肯定感、健康、及びウェルビーイング感覚は公平に価値が置かれている。

協調安全の基本概念は次の要素で構成される：

- 機械の動き、人の行動、及びその労働環境に関するリアルタイムベースの情報をモニタリングするためのICTの最大限の使用と
- 通常動作や保守サービスの間の潜在リスク情報の検出と伝達による機械の動き、及び/または人の行動に対する安全制御
- ICTを使用した安全技術の採用が、機械の稼働率や作業者の効率を犠牲にしないことを確実にすること
- 安全技術の採用が、持続可能な形で安全対策が実行されるに際し、労働者やオペレーターの信頼性に貢献することを確実にすること

協調安全において必要不可欠な目的は、機械、人とそれらの動作環境間のマルチトラフィックの情報循環を通じて相互支援のパートナーシップを構築することである。人は機械によって行動を制限するよう規制され、機械は人の介入で動くスピードを落とすあるいは停止することを規制される。協調安全における最新のICTテクノロジーの最大限の活用のおかげで、使用上の安全を確実にする労働者/オペレーターの責任は、機械や情報技術に大幅にとって代わっている。結果的に、オペレーターはより少ない特定研修、専門知識と経験が求められることで業務プレッシャーが軽減される。

2.4.3 規範的な法律と標準化/適合性評価オプション

従来の法で規制された安全衛生保護は、少なくとも建前上は政府の検査を通じて強制的に実施されてきた。検査官の人数の限界はさておき、このモデルがなぜ大きな課題とされているか基本的な理由がある。前述の社会、テクノロジー、及び労働におけるメガトレンドは世界の急速な変化をもたらしている。技術革新は、特に情報技術に関する分野は、産業の関係と同様に、生産過程、労働の特性と条件に影響を与えている。これに関して、規範的な法律制定は、現実よりも遅れをとっており、一方でイノベーションを同時に妨げる、ということはほぼ明確である。

多くの所管で、この問題に関する4種の具体的な対応があり、それらは次の通り：

1) 製品よりもプロセスに注視することによって、法律制定をより柔軟にする。例えば、いかにプロセスを構築し実践するかという点で、安全管理プロセスの質へのフォーカスが産業に高い自由度を与える。

2) 安全衛生を手段ではなく目標で規定することによって管理の圧力を減らす。これは、産業が、いかに必須の目標を達成したいと望むかを選択するうえで、より大きな自由度を許容する。

3) 安全衛生の義務を満たすためのトリガーとして経済的なインセンティブを活用する。これにより産業に内在する市場メカニズムを利用する。

4) 国、あるいは、地域レベル（例えばヨーロッパなど）での自主的な合意（例えば、政府と社会パートナー間あるいは政府と産業部門間）により強制的な要求事項を補完する。

結果として、標準化と適合性評価は単に民間主導以上のものになってきており、法的安全規制を補

う不可欠なものとして、より評価されるようになり既に実際に機能している。このことは産業界に、規格開発するための新たなタイプの圧力ももたらす。

安全管理システムの標準化と適合性評価（例えばISO４５００１、及び請負業者の安全管理に関する国または地域のシステムなど）は管理業務にフォーカスした、法制を自然に補うものである。適合性評価は法実施とは異なる私的規制をもたらすが、政府の検査やこのような規制を緩和することを補完する重要なファクターとして政府に徐々に認識されている。加えて標準化は、このような経済的インセンティブが、ある特定の標準をベースにする一方で、経済的インセンティブを創るのに一つの役割を果たす。

このように、自主的な合意は通常はさまざまな監視活動（何が影響しているのか？）や安全規格の実施程度の監視を必要とし、適合性評価はしばしばその合意に組み込まれた重要な要素である。さらに国際安全規格は、適正な安全法制が実施されていない国の安全にも大きな影響を与える。

2.4.4　メガトレンドと労働への影響

この章で述べられた技術や社会におけるメガトレンドの多くは労働の世界に直接影響を及ぼしているし、将来も及ぼす。結果的に、労働の特性と構造は変化しているし、徐々に将来の安全衛生とウェルビーイングに関する新たな挑戦と関わってきている。最も際立つトレンドと労働への影響は表２-１にまとめられている。

表2-1｜メガトレンドと仕事への影響

メガトレンド	仕事への影響
デジタル化	▪ 在宅勤務の増加 ▪ 新しいプラットフォーム（またはギグ）経済 ▪ 作業の個別化の増加 ▪ 新しい形の人と機械の協力 ▪ 利用時間の増加と座りがちな仕事と行動の増加 ▪ ストレスとメンタルヘルスの問題の増加
経済的、及び政治的開発	▪ リモート本社への依存度の増加 ▪ サービス産業の増加 ▪ 自営業の台頭 ▪ 仕事と雇用の柔軟性の向上 ▪ 「フレキシキュリティ」の台頭 ▪ 仕事と社会の二分法
グローバリゼーションと新規事業モデル	▪ （グローバル）サプライチェーンとOSHの関連性の向上 ▪ 仕事のアウトソーシングとオフショアリング ▪ 下請け業者の管理 ▪ 組織の頻繁な再構築と作業の再編成

人口統計	▪ 高齢化する労働力 ▪ 年金の定年が高い（労働寿命が長い） ▪ 職場での慢性疾患の増加 ▪ 労働力の多様性（年齢、文化、必要な能力と利用可能な能力の不一致（知識、スキル、態度）言語、宗教など） ▪ 必要な能力と利用可能な能力の不一致（知識、スキル、態度）
持続可能性	▪ ライフサイクル終了時の作業の増加

2.5 リスク管理、リスクガバナンスと標準化の課題

メガトレンドは、安全に影響を及ぼすさまざまなリスクを管理する必要性を表している。物理的な職場の安全側面はもはや、サイバーセキュリティや環境破壊、倫理的な挑戦などの他のタイプのリスクによって独立して管理されるものではない。しかしながら、「リスク」の考え方は、標準化対応の意味合いとして現れる 2 つの対照的な理解をもって、既存のISOとIEC規格で定義されている。

- ISO/IEC ガイド 5 1 に示される安全規格の幅広い定義：
  「危害の発生確率と危害の深刻さの組み合わせ」
- ISO31000シリーズとISOガイド73からのマネジメント定義：
  「目的[の達成]に関する不確実性の効果」（図 2-6を参照）

ISOの定義は、ネガティブまたはポジティブとなり得る不確実性による効果（マイナス、またはプラスのリスクを含む）を意味する。この解釈は通常、ビジネスにおけるリスクのことを言う。リスクのポジティブ面は、「セーフティ - II」アプローチと呼ばれる。セーフティ - II は、「成功事例の数が可能な限り高い状況」と定義され、さまざまな状況において成功をもたらす能力である。セーフティ - II は、物事が誤った方向へ向かうことを予防するよりも、正しく進むことを確実にするよう努めることで達成される[23]。IECにおいては、しかしながら、ネガティブな結果に言及する従来からの解釈が一般的である。

リスク管理の目的は、人と価値を創造し、保護することであったし、そうあり続けている。リスクマネジメントは、人とテクノロジーの相互関係を改善すること、異常や事故を避けること、イノベーションを推進すること、目標達成を支援すること（ビジネスの継続性を含めて）により、対象システムの不利な成果に言及し、パフォーマンスをコントロールする。これは、対象システムを所有する組織によって確立され維持される必要がある。データシステムの急激なデジタル化とセンサー経由のいたるところにある通信ネットワークが、安全目標をよりいっそう直接的な方法でサポートすることを可能にしている。

しかしながら、リスクマネジメントの報告は直接的ではない。センサー、カメラ、ICTシステムは膨大な量のデータを照合しているが、評価をするうえで最も簡単なことは、必ずしもリスクを統制して安全を達成するための最も関連する要因ではない、ということである。人の行動、文化的価値、企業文化、リーダーのコミットメントや個人間のコミュニケーションなどの要因は、データシステムにおいてそう簡単に捕えられない。

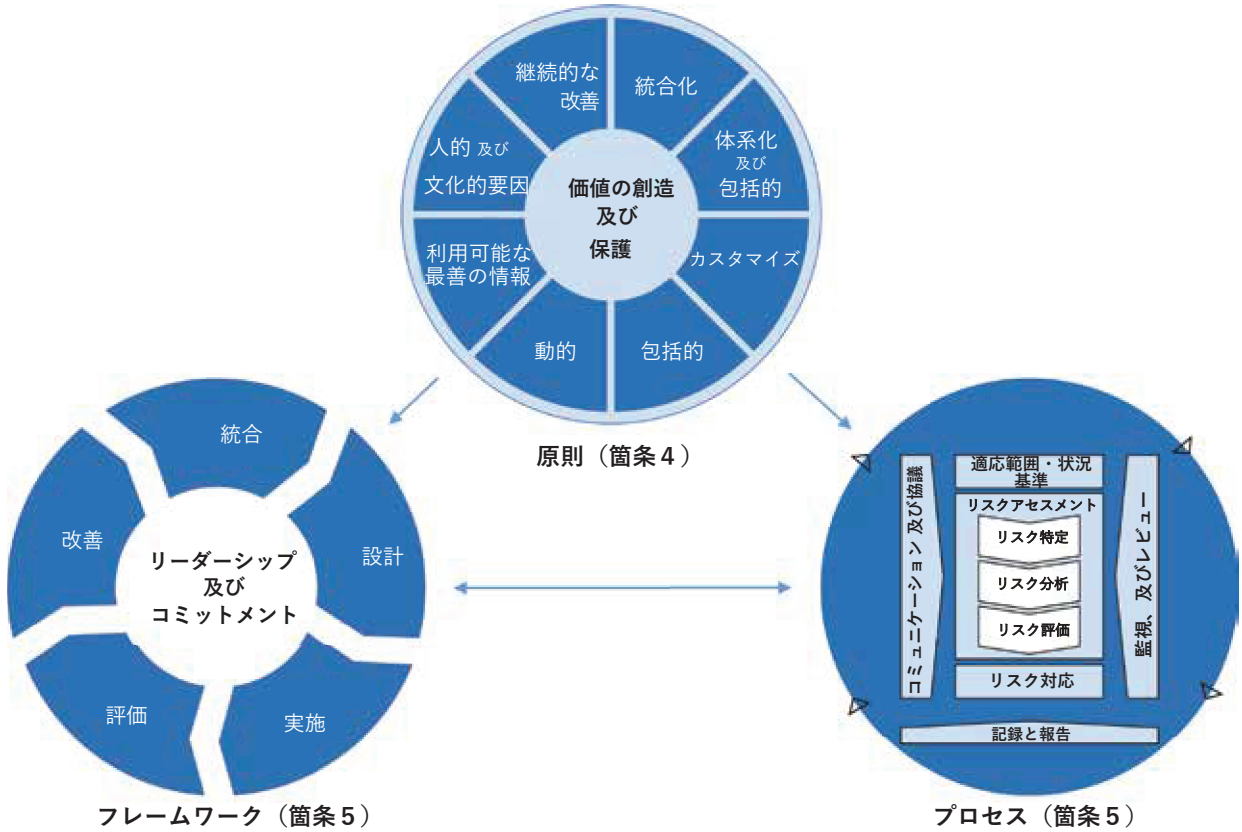


図2-6 | リスクマネジメントフレームワーク（ISO 31000）

この分野で研究は始まっているがゆっくりと進んでおり、ビッグデータの世界ではそのような要素が無視される危険性がある。

結果的に、政策決定者や産業界は、新技術やイノベーションによる機会やリスクに関して新たなタイプの不確実さを扱い、さまざまなステークホルダーを含めた議論をしなければならない。これらのプロセスをガイドするのに関与するアプローチは、リスクガバナンスがあり、公的、私的な組織や企業間の協調がベースとなっている。

リスクガバナンスのための協調アプローチは、以下の５のステップで構成される反復プロセスで構築される：

1) 事前評価、認知、構想

2) リスクの技術的かつ認知された原因や結果の評価を含む査定

3) 特性化と評価：リスクとそれを管理する必要性についての判断

4) 管理：リスク管理オプションからの選別と実施

5) 分野横断的なさまざまな局面：
コミュニケーション、ステークホルダーとの関わり、文脈理解[24]

このリスクガバナンスのプロセスは、不確定、複雑、不明瞭なリスクのマネジメントにおいて

ステークホルダーを積極的に巻き込む。透明性とオープンコミュニケーションは、すべての重要なステークホルダーを招待し、支援し、巻き込むため、また共同評価や意思決定のベースとして相互信頼関係を構築するためには不可欠である。革新的な技術を備えた複雑なシステムのリスクガバナンスにおけるステークホルダーとの協業は、「協調安全」という用語に対する別の側面を示している。

リスクガバナンスのプロセスの目的は、どのように（部分的な）未知のリスクに対応するかという判断と一緒に到達する。関係する戦略は、新たなテクノロジー開発とイノベーションに影響を与えることによってそのようなリスクをコントロールすることであり、リスクの発生を妨げることによってではない。リスクの特性は戦略に影響し、ステークホルダーの関与については、表2-2に規定される。

表 2-2｜リスク特性、戦略、及びステークホルダーの関与[5]

リスクの分類	特徴	戦略	ステークホルダー関与
単純なリスク	リスクは既知 科学的知識は利用可能	ルーティンベース戦略の適応	有益な談話
複雑なリスク	原因と結果に関する限定された知識 定期的に限定され、新たに出現する財産につながるシステム内の多 くの相互関係	コンセンサス探求 有効な証拠の識別と特性評価 センスの明確化 構造安定性の向上	認識論的談話
不確実なリスク	リスクに関する知識は限界があることの認知 リスクアセスメントは（部分的に）危険であること	リスクの徴付けのためのプロキシの使用 意外なこと、復元力を強化する能力向上 予防手段の考慮	反射的な談話

5　出典：2017年国際リスクガバナンス評議会（IRGC）

不明瞭なリスク	何が受け入れられるリスクであるか、及び/または、信頼がおけるのは誰かについての異なる意見や信条をもたらす異なった価値観、原理、あるいは主張	関連の価値感と主張を含む、関係する全情報解析 対立解決法を適応 自信と信頼を築く	一般的に公共を頻繁に含む、対話と参加型談話
未知の未知	前例のない、及び未知のリスク	未知のようであるが、除外されないリスクを減らす、既知のリスク情報の体系的評価	

リスク戦略とステークホルダーの関与のリサーチは、技術や社会で起こる急激な開発をモニターしているが、どうしようもなく遅れをとっている。結果的に、新たなリスクの管理のための科学的ベースは限定されたままである。さまざまなステークホルダーが、新しいテクノロジーを評価し装備するプロジェクトに関与しており、関係する機会とリスクの認識と同様に、結果に多様な主張を持っている一連の賛同者と共に関与している。結果、科学者やエンジニアの権限はもはや無批判に、或いは特別には受け入れられない。現在、一般的に受け入れられるリスクガバナンスプロセスを網羅する標準は存在せず、このようなプロセスが幅広く実践されることを阻止しているような欠落状態である。サイバーセキュリティの関係するエリアでは、不確実で、複雑で、曖昧かつ未知のリスクが、安全性の複雑な問題を創り出すために結合されるであろう。結果的に将来の安全規格はもはや単に電気技術者によって定義付けられるものではなく、政府機関や社会を含む、幅広いステークホルダーからの情報提供が反映されるであろう。

今や、そして将来は、新たなテクノロジーの出現や破壊的革新に関連するリスクが、より大きな社会的議論あるいは論争の枠内でますます考慮されるようになるであろう。

2.6 標準の挑戦

特定の種類の機械あるいは製品を包括する既存のISO、及びIEC安全規格の多くは、まだ包括的な安全面を含めることができていない（関連する安全技術だけでなく、通信テクノロジー、反応時間、運用管理、コア人材の能力、など）。標準化コミュニティは安全確保のためにその役割を再考する必要がある。技術的構成要素だけに着目した安全規格は、規範的規制として同類の制限がある。それはイノベーションを阻害するかもしれないし、頻度を増やしてアップデートをしなければならず、国際標準化プロセスに対する課題をもたらす。協調安全の原則は、さまざまな産業分野（例えば、製造、土木、建築、農業、ヘルスケア、交通機関など）に共通的に適用されるため、規格開発は幅広いステークホルダーを巻き込んで異なったアプローチを採用する必要がある。一つのオプションは、協調安全においては、意図する目標やこの協調アプローチのパフォーマンスのターゲットを規定しながら、それに対応する

目標達成のプロセスに対する最低限の要求を規定するという、より「パーフォーマンスベースの」（「仕様ベース」と異なる）規格を開発することである。

政府が規制緩和によって安全管理を緩めること、企業が民主主導で安全のための社会的責任を担うことで規制緩和を補填することで、安全に関し産業に支援された新たなタイプの規格開発に機会が開かれていく。このような方法により産業分野の規格は、より制限が緩和され、開発された規格を維持管理していくことは重荷とならず、技術進化により対応しやすいものとなり得る。

第 3 節

安全のための三者連携ステム

このセクションでは、技術進化とその職場安全への導入効果の影響下にある避けて通れない安全の概念の進化に焦点をあてる。その中心において安全は、人と機械の相互作用における基本的なシフトによる影響を受け、その中で人と機械は手動によりかつ精神的な部分により両方のタスクをシェアすることになる。結果としてデジタル機能は、人と機械が共存する職場で、あるいは実際に人と機械との協業を可能にするような他の空間で、シームレスに動く職場づくりの一助と成り得る。安全のコンセプトを描きそのフレームワークで安全を伝えるにあたり、我々は、人、機械、環境が将来を確かなものにするために連携する三者連携システムとして新たな職場パラダイムが機能することを簡素化する。この安全モデルの三者連携システムは、システマチックアプローチを将来の安全の重要な要素の議論へと促進する。

情報の流れ、システムの境界、及び繋がり、種々のレベルの高度化を含む三者連携システムの記述に引き続き、このセクションでは、現在の、及び未達のテクノロジーが関係しながら展開されることを検証し、サイバーセキュリティの技術的な必要性を標準化や適合性評価に導入とともに考慮する。

3.1　人、機械、作業環境

2030年には安全の概念は、人、機械、環境が協調する総合的なシステムで提供される。そのような協調は、情報の流れが、労働者、(半)自立機械、そしてそれらが機能するIT環境などの、システムの異なった構成要素間を行ったり来たりすることで可能となる。この協調のフレームワークを安全に関する三者連携システムと呼ぶ(図3-1)[25]。

図に示されるように、人は、個人や複数個人の業務タスクをあらわす。機械とは、機械、電子機器性能や人口知能、或いは精巧なコントロールシステムを搭載したロボット或いはツールを示す。環境は、コンピュータや進行する業務の支援をするために導入された支援システムを示す。これらは、職場の電子モニタリングシステムやエッジノードであり、工場では監視制御やデータ収集システム（SCADA）、あるいは、与えられたオペレーションをサポートするために付与されたクラウドベースのサポートを行うものである。活動によって、またその活動が農業、ロボット化された生産、化学処理やロジスティクスを含むかどうかによって、人のタスク、及び関与する技術は幅広く変わるが、これらの３つの主な要素はどのような形であれ常に存在する。

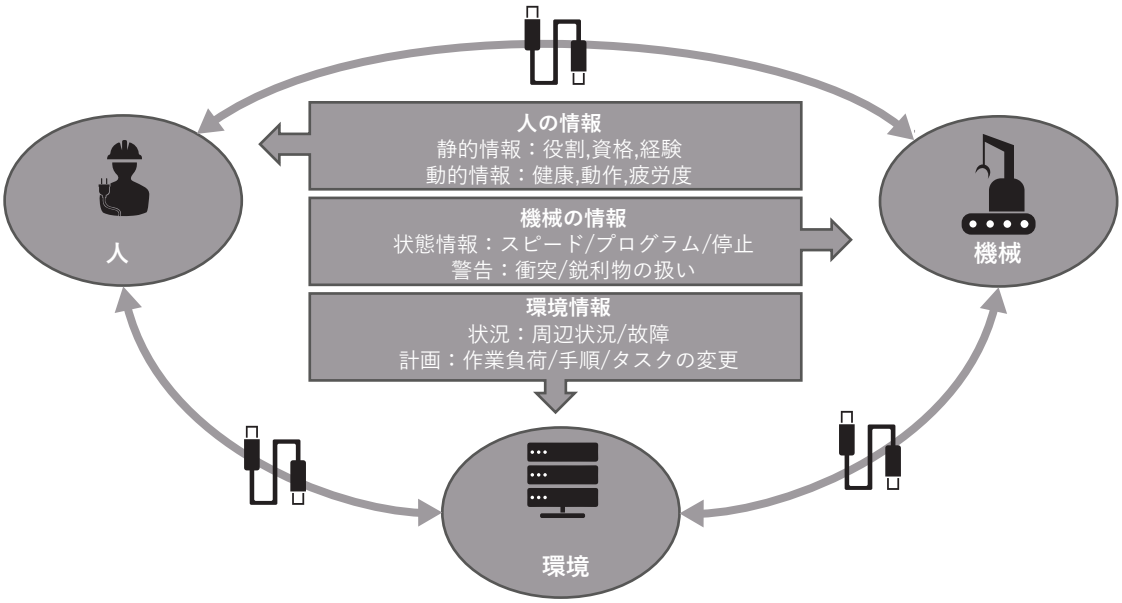


図 3-1｜将来の安全のための三者連携システム

3.2 三者連携システムにおける情報の流れ

三者連携システムの構成要素間では、３種類の情報が行き交う(図3-1)。**人の情報**は、人あるいは人が絡むオペレーションに適応することを許す機械に関連する情報である。これは静的あるいは動的情報の一方になり得るが、常に人の状態にフォーカスされている。静的情報は長い時間をかけてほんの少ししか変わらない、例えば、労働者の資格、キャリアパス、職務経歴に関する情報である。動的情報は、日々あるいはリアルタイムで変わるもので、作業者の疲労レベル或いは着手した特別なアクション、例えば、小さなミスを修正したり、臨時の休憩をとったりする情報である。機械はおそらく周辺の環境システムに助けられ、安全な製造を確実にするために、これらの変化にオペレーションを適応させることが必要である。人の状態は、脈や体温を含めた生物学的データや身体動作、作業者の行動やポジションを登録するデバイスを通じてモニターされる。

機械の情報は、稼働している機械の状況を含む：機械が稼働中か待機中か、安全重要部品が正しく機能しているかどうか、ロボットハンドに関する情報、プログラム動作か協調動作かなどのオペレーション状況などの情報である。この情報は、安全行動を促すために人に伝達される必要がある。機械は、機械の故障や、今にも故障しそうな状況を直ちに警報で知らせる。このような情報は、人と機械が共存する環境で働くためのキーとなる。

今日現在、機械は作業工程において次の段階への伝達が可能であるが、同時に、機械は一連の作業中に態勢の変更を示唆することも可能である。（例えば、立つように人に知らせたり、休憩をとるように示唆したり）同時に何人かで作業をする際、協調の環境では、機械は、各作業者の安全衛生を向上するために、作業の配置交換を示唆することも可能である。

労働環境は、人と機械のコンタクトを容易にする**環境情報**や、より幅広い企業のシステムとのリンクを同時に形成する三者連携システムの欠かせな

い構成要素である。人にとって環境の役割は、人間工学、空間、周辺条件、及び社会交流の観点から、安全な労働条件を整えることである。例えば、作業者にとっては、どの機械がアップデートにより、オペレーションが変わるのかを知ることは、とても有益なことである。同様にその環境は、どの作業者が特定の日に作業工程にいるのか、どのような特定の安全が、作業者個人毎に関係するのかを知らせることによって機械をサポートする技術的なICTシステムのネットワークを提供する。同時に現場の作業環境は、安全手順あるいは安全方針の変更についての情報を提供する、会社のより幅広い事業環境とのつながりを維持している。

3.3 三者連携システムにおけるシステムの境界と連携

三者連携システムアプローチは、システムの境界内のプロセスや、ステークホルダー、目標、不慮の事故、ルールのような外的な力や要素との連携についての明確な説明を必要とする。

進歩した人と機械の協調は技術的に複雑で、連携するネットワークもまた複雑である。このシステム説明の例が図3-2に示される。それは対象システムの安全は孤立していず、むしろ他の機関やグローバル社会にも接点のある会社の内部のシステムのエコシステムに依存するということである。

これらの連携は、対象システムのオプションと限界を示しており、以下が含まれる：

- 漠然としたビジネス目標を満たす（例：生産目標）
- 他の目的へのコンプライアンス、及び確立すべき優先順位の階層に従うシステムの内部目的の最適化
- 職場の安全衛生基準に適合（例：規則）
- 安全な人と機械の協調に関わる基準を満たすこと
- ICTシステムとインターネットが引き起こすセキュリティリスクへの対処

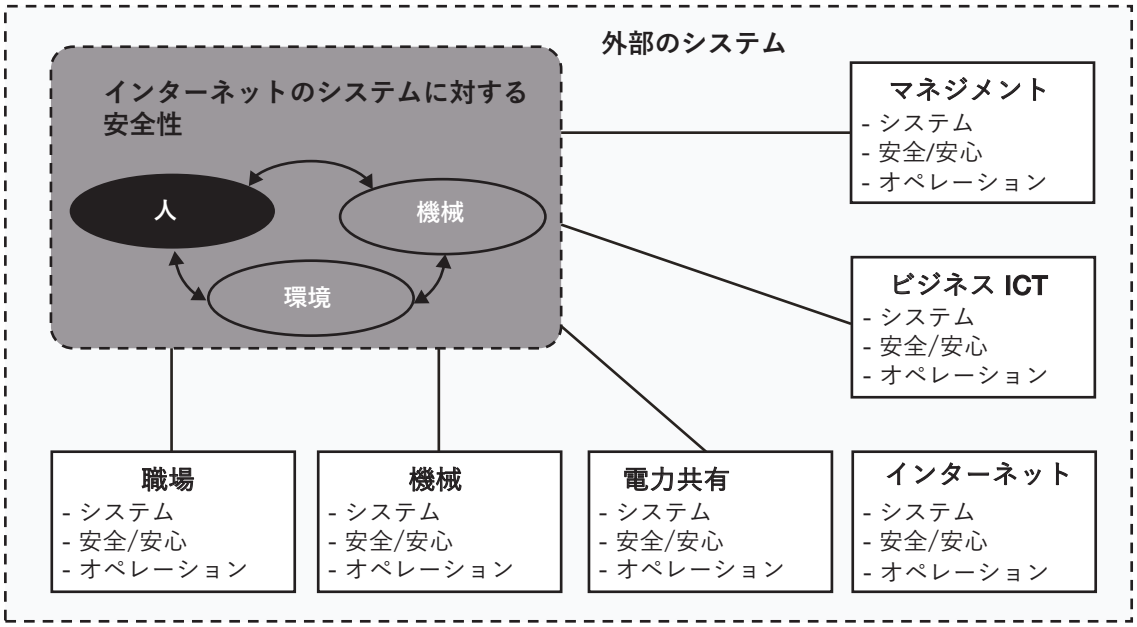


図 3-2 | 安全における三者連携の抽象的なシステム定義

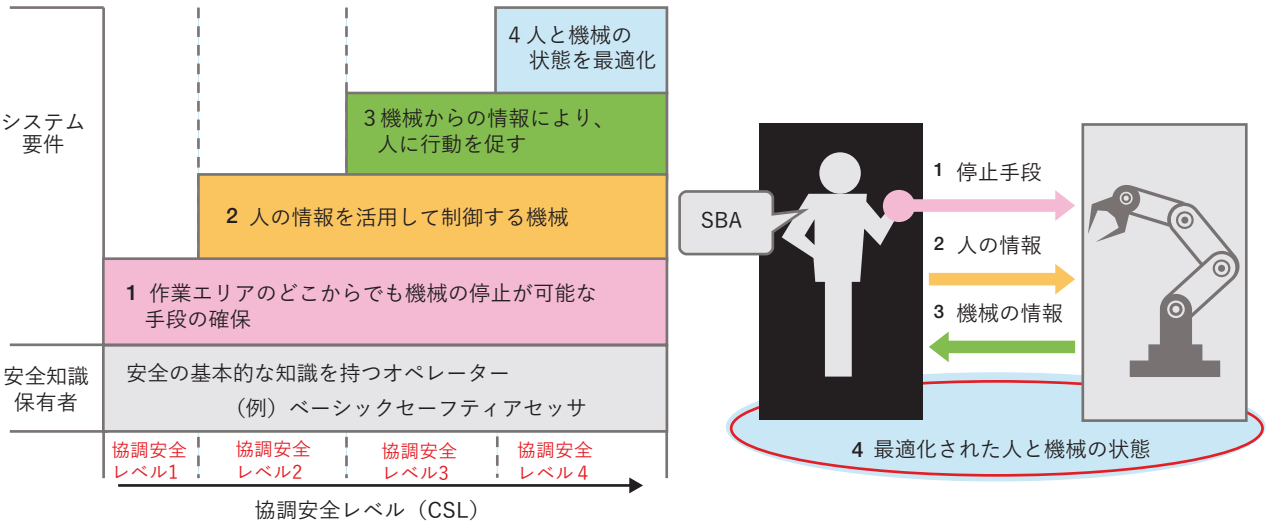


図3-3｜協調安全レベル

安全性の問題は通常、対象システム内外での通常運転からの逸脱が原因で発生する。逸脱はシステムの設計や目標の変更が通常原因になり得るが、外部での変更によっても起こり得る。この白書の目的のためには、人、インテリジェントな機械、、及びICTシステム間の複雑な相互関係に依存する安全保護システムに注目することである。

3.4　三者連携システムの洗練度

すべての作業プロセスが同じように構築されているわけではなく、安全性と信頼性はシステムごとに大幅に異なるであろう。したがって、洗練度の違いは将来の安全システムであると想定される。協調安全レベル（CSL）の概念は、図3-3において透明性のあるフレームワークのベースを提供している。[26].

CSLモデルは、基本安全レベルに4つの洗練度を加える。これらは次のように協調安全の特定のパフォーマンス基準を説明している：

- SBA–セーフティベーシックアセッサの資格は基本的な知識とスキルの一定レベルを示し、すべての労働者に要求される安全関連のスキルである。このレベルは、現在存在する労働安全に対する法的要件を示している。アプローチは国または地方の資格制度に基づくであろう。

- CSL-1–現在、ほとんどの固定された職場や製造機械には緊急停止機能が備わっている（車両などの一部機械ははそうではないが）。このレベルにおいては、協調安全環境では、職場のどのエリアからでも動作停止を可能とすることが想定される。
- CSL-2–このレベルでは、機械が人の情報を活用するための、処理能力のある機械を導入する。このレベルでは、機械が安全制御に関するパーフォーマンスを可能にするよう、労働者の情報が機械に知らされる。
- CSL-3–このレベルでは、双方向の伝達が確立されている。CSL-2の機能に加え、機械には、労働者に安全情報を送るための人間工学に基づいたヒューマンインターフェイスが供えられる。

- CSL-4–最高レベル
  システムが、システム全体の安全衛生を改善するために最適化が図られる。このケースでは、環境内のデータネットワークが製造プロセスの最適安全と効率的機能を補助する。

3.5 三者連携システム実現のキーとなる技術

現在利用可能でありかつ予測されるテクノロジーは、三者連携システムの洗練された相互機能に必要となる概念的フレームワークと基本的な相互接続性を提供している。3.5.1から3.5.3では、テクノロジーがこのようなシステムの能動コンポーネント間に流れる情報を確実にする複雑な挑戦に取り組むための３つの重要な点が述べられる。

3.5.1 IoE

三者連携システムは統合された機械と知的アルゴリズムに依存しているため、ワイヤレスネットワークやインターネットを通じての接続性は核となる手段である。概念としてインターネット・オブ・シングス（IoT）は中心になる。IoTは、人と人、 あるいは人とコンピュータの交信の必要のないネットワーク上で転送される相互のコンピュータデバイス、機械的、及びデジタル機械を指名する。作業スペースでIoTは、感知、識別、処理、通信、作動、、及びネットワーク構築能力を備えたさまざまな機械のシームレスな統合化を促進する。安全目的で同じアプローチが使用されるとき、その概念はインターネット・オブ・ヒューマン（IoH）として再分類される。

結局のところ、人（IoH）のモニターに応用されるシステムと、機械（Io T）をモニターするのに採用されるシステムは非常に類似なものである。いずれも監視目的の検出機能を備え、データをシステム内で交流させるために広域のネットワークの通信機能を使用し、データをデータセンターで照合し、集中型クラウドあるいはローカライズされたエッジ、時にはセンサー自体に分析を頼っている。簡単に言えば、基本的なインフラは同じで、２つを合わせてインターネット・オブ・エブリシングス（IoE）システムとすることは意味のあることである。職場でのIoEシステムで、図3-4に示すプロセスは加速し、製品需要は直ちに満たされ、製造のリアルタイムの最適化が達成される。

図 3-4 | インターネット・オブ・エブリシングス

日本のICTソリューションプロバイダーから提案されたIoHシステムでは、労働者は、GPS、カメラ、アクセラレータ、ジャイロセンサーを備えたスマートフォホン、体調測定の機能を備え温度や湿度センサーの搭載されたスマートウォッチを装備する。これらは、個人レベルで人をモニターする基本的な感知デバイスとして扱われる。

デバイスはオンサイト通信システムを通じて、クラウドあるいは構内でデータシステムと接続される。通常の労働環境下で、収集された情報は労働者の物理的ポジションや体調（心拍数、ストレスレベル、動きの速度、標高、動力学、水分量）を評価するのに用いられ、各人が歩いているのか走っているのか、苦痛などにさらされているのかどうかを自動的に検出する。情報は労働者のスマートフォンに集められるのでこのデータを他の労働者の状況と結合すること、労働者が危険物やガス雲に接近しているかどうかや高所で作業しているのかどうかを識別することが可能である。作業が室内であれば、ビーコンやウルトラUWB（UWB，超広帯域無線）のような屋内測位技術が必要とされる。これにより、仮に誰かがATEX[6] 爆破性区域などの危険地域に足を踏み入れた際、管理者が警告できる。

スマートフォンのセンサーは静止、つっかえ、落下などの異常な動きを容易に検出できる。
そのようなケースでは、アラートは即、監視員のディスプレイに転送され、緊急警報が関連する労働者のスマートフォンに送信可能である。付近に同僚がいたら、同僚は状況を直接評価でき、可能であればいつでも助けに向かえる。スマートフォンに搭載のカメラは画像を取り込むのに用いられ、即、IoHプラットフォームに転送され、保存される。

監視員がこれらの静止画像をチェックし、直接対応あるいは次の段階の対応が可能となる。画像に加えて、ニアミスの報告、状況報告、及び他のさまざまなタイプの運用上のやり取りは遅れることなくシステムに転送される。電話は、電話をかけることができることを忘れるべきではない。

スマートウォッチに搭載されている感知装置は、低体温症、熱中症や体調不良の兆候を感知できる。

スマートウォッチからの脈拍数のデータをもとにして、温度と湿度データやエネルギー排出量を結合させる複雑な計算が可能となる。結果として、スマートウォッチが休憩をとる必要性を知らせる。

労働日の最後に、深層学習をもとに認識アルゴリズムの型を使って危険の兆候を察知するため、蓄積データが集中して分析される。結果は特定の作業処理を改善するのに、あるいは、個人単位で必要になる研修に適用できる。

それらのテクノロジーの能力を備える以外に、このようなシステムが、関係する労働者のプライバシーを保証し、データ処理、データ保護や使用したアルゴリズムの監視において労働者の代表を巻き込むことは不可欠なことである。

3.5.2 オントロジーとセマンティック相互運用性

情報交換は三者連携システムを機能させ、成功を確実にするキーである。ICTシステムは独自に、及びそれに関わる人とも通信が可能であるべきである。三者連携システムの複雑さは、それがAI性能を提供する複数のICTシステムを搭載したインターフェースが関わる際、急激に増す。この複雑さの例として、最近のIEC白書「Semantic interoperability（意味論的相互運用性）」に記述がある[27]。

6 爆発の可能性がある雰囲気内で使用する設備（ATEX）

協働ロボットのモーターがオーバーヒートしているという情報を労働者が必要としている状況を仮定してみよう。最初に問題の検出を行うために、モーターの温度を検温し、それからその情報を分かりやすいようにデジタル化する必要がある。その温度の数値に加えて、時間、計測単位（例えば、°Fや °C）、センサーと測定される箇所を識別する測定器、及びおそらく追加要素の情報がデータに含まれるべきである。データはその後、IoTシステムに転送され、この（そして、おそらく、同時に他の多くのシステムの）コンポーネントの温度が過度かどうか、労働者が増えたリスク情報を必要とするかどうか、アルゴリズムが評価する。よって、IoTアプリケーションは該当データと関連する決定を「理解する」必要があり、労働者はその内容とメッセージ転送の理解が必要であり、ICTシステムを取り巻く環境はそのメッセージが理解されたことを「理解する」必要がある。

このように特別な情報システムの最初の条件は、個々の部分がオーバーヒーティングについての理解が共有されること、そしてどういう手段でこの要因が関係しているかを知ることである。個々に訓練され得る人は倫理的思考と知能を持ち合わせていて、そのチェーン内でリンクがある。しかし、すべての機械はプログラミングされる必要性がある。すなわち、特に、もしそれらが知的で満ち溢れる状態であれば、抽象的な知識に基づくルールに従って稼働する必要がある。

この理解は情報が交換されるうえで知識表現スキーマにおいて定義されるべきである。これは通常設計者やプログラマーが、関連する知識を知識モデルやオントロジー[7] へ落とし込む作業である。辞書上や意味論的な取り決めで構築されたオントロジーは、質量、長さ、時間のような基本的な特性から、機械の使用を通じて問題を解決するレベルまで、あるいは機械を使用するうえでの倫理感の考慮までをも含み、いかなる抽象レベルにおいても知識を説明し得る。このように示される知識とは、実世界からのデータを説明する情報モデルをベースにしている。この目的を達成するために、実世界の潜在的な知識を明確な知識構造を有する人が要約することにより、機械に使用され得るフォームへと変換する試みが行われる。実世界の出来事をデジタル化するプロセスは、これらの抽象的なレベルに及ぶ。

オントロジーデータモデルは、システムの各小さな部分（労働者、体温計、アルゴリズム）向けに作られたものであるが、それらはより高いレベルのオントロジー、つまり相互システムの全局面をとらえるオントロジーか、わずかに抽象度の高い概念を寄せ集めるオントロジーによって繋がり得る。表3-1は広く知られている安全モデルのボウタイ方式に由来する基本的なオントロジー（存在論）的定義を示す。

表3-1｜安全性のオントロジー定義[28]

概念	オントロジー定義
ハザード	危害を引き起こす可能性のある物や活動。 トップイベントの一部であり、脅威によってリリースされる。
脅威	ハザードが発生するトップイベントを生成すると考えられる原因。 バリアは特定の原因に関連付けられている。

7 この意味でのオントロジーは、「プロパティと関係性の間に見られるサブジェクトエリアまたはドメイン内の一連の概念とカテゴリー」”, www.lexico.com/en/definition/ontology

バリア	トップイベントを防止する、または変更する手段。 被害を軽減するための重大なイベント。それは他のバリアをある時点で防止し、特定の脅威に関連付けられている。
重大なイベント	ある時点で脅威によって作成されたシナリオまたは望ましくない状態。 それは障壁とリリースの結果によって防止されるイベント。
結果	トップイベントによってリリースされる可能性のあるイベントで直接生成される。このイベントは、バリアによって変更される。

セマンティック相互運用性、あるいは「明確かつ意味を共有するデータを交換するコンピュータシステムの性能」[8] は、3つの構成要素が途切れなく互いに通信しなければならないため、安全に関する三者連携システムにおける技術的要求のキーと考えられ得る。しかしセマンティック相互運用性は、今日の高度に断片化され不均衡な範囲に及ぶ技術、インターフェース、プロセス、及びデータモIEC　CDD内でデルからの処理により、オープンで、理解可能で、統一的ソリューションを備えた、将来のIoTエコシステムを構築するする産業プロジェクト全体の成功における決定的要素となる。

三者連携安全システムのような異なったIoTシステム内の通信において、セマンティックレベルは相互運用性を実現するために必須である。そのために、情報交換の両面（すなわち、対象とする異なるIoTシステム）は、共通的に合意された参照モデルを参照にしなければならない。オントロジーにより決定される相互運用性の解決策の複雑なシステムは、この取り組みに対処するために開発されてきた。

IECは既に、製品記述が構造化された安全関連特性を含むIEC共通データ辞書（IEC CDD）内のオントロジーを開発途上である。なぜなら、セマンティック相互運用性は三者連携安全システムに不可欠であるため、より特別な安全関連の概念が標準データベースフォームにて開発すべきであり、IEC CDDに迎えられるべきである。

3.5.3　保証アルゴリズム

AIは、人知が到底太刀打ちできないほどの複雑な問題の解決を確約する。しかしながら、この開発は固有の問題と共にある。解決策の説明として、見つかった解決策が安全という意味である必要はない。AIエンジンは、学習段階と論理化段階における不適切なデータにより、危険な事象を生み出すかもしれない。それ故、安全性は強制される必要があり、AIシステム自体は、独立して動く安全検証アルゴリズムが装備される必要がある。その概念は図3-5に示される[29]。

保証アルゴリズムはディープラーニング（DL）ネットワークのベースで運用される。ディープラーニングは2つ以上のレベルから成る中間層を構成するニューラルネットワークを利用した機械学習法である(図3-6)。

DLは3つのタイプの学習がある：監視、悲監視、強化学習。

8　en.wikipedia.org/wiki/Semantic_interoperability

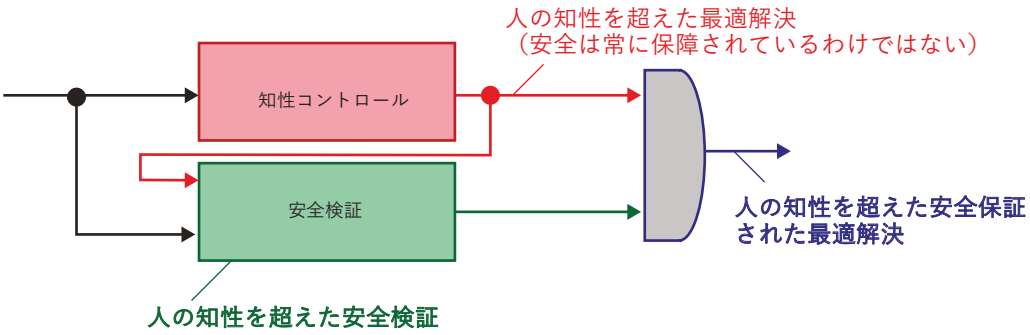


図3-5｜安全検証を搭載したAI機器

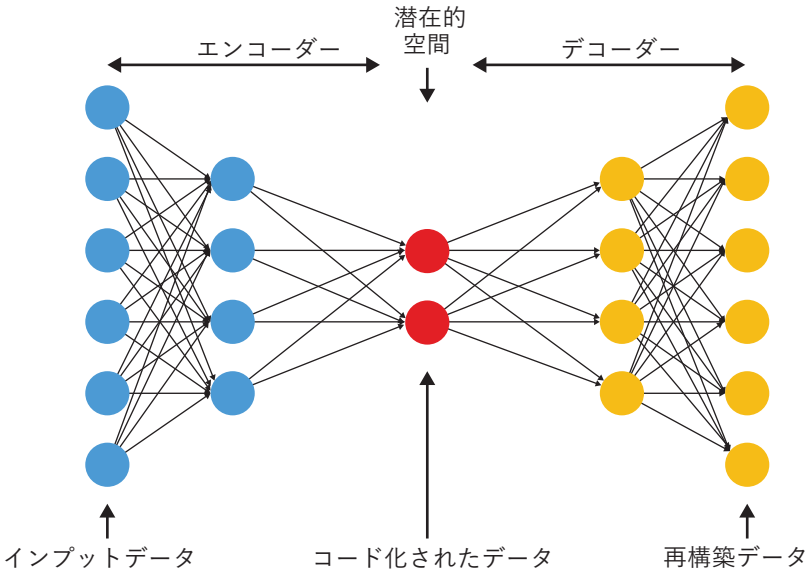


図3-6｜ディープラーニング・ニュートラル・ネットワーク

監視学習では、特定のデータインプットとこれに対応するデータのアウトプットが生成される。主なメリットとして監視学習は、データ圧縮にあるということ。この手法は効果的であるが、新しいトレンドを見出すようには設計されていない。安全性の監視学習は提供されたデータに依存する。特に不完全なデータや不完全な演算の効果（学習に使用しないデータの処理ができない）に影響を受けやすい。もし、この学習タイプが安全保証のために利用されるなら、AIエンジンが正しいデータで鍛錬され、AI処理の学習や推論の両段階において、十分にテストされることを確実にするため、人の監視のために標準化されたプロトコル（おそらくアルゴリズムにより強化）を供給する必要がある。

強化学習は報酬機能として予想されるアウトプットを使用する。これは、（知られている）重要なトピックの導入に依存することを継続するが、フレキシブルな報酬機能により差異や新たなトピックを許容する。強化学習のメリットは、ある程度の目的管理に関与する自動的な最適化とい

うことである。強化学習の安全性は、演算の完全性と同様、提供されるインプットデータ、アウトプットベースの（評価基準を含む）報酬機能に依存する。安全の検証については、推論のフェーズでAIエンジンを不安全ソリューションから遠ざけるため、検証機能（ソリューションの境界をモニターする一種の安全関連機能）を追加する必要がある。

非監視学習はインプットデータのみをベースとして機能する。対応するアウトプットデータは生成されない。悲監視学習の長所としてはそのデータマイニングのような機能にある。言い換えると、潜在的に可変を取り出すことはこの種の学習で可能であるが、この手法は、人が通常行うやり方でアウトプットをラベリングするには比較的弱い。これは安全目標の達成に相反し問題になり得る。事実、悲監視学習はどんなものであれ、安全の保証はできないことを示す。安全機能が追加された場合には、それは悲監視学習アルゴリズムのコントロールの一部として動作する完全自動安全検証機能を含むことを必要とし、逆説的に、非監視学習それ自体に含むことになるであろう。

3.6 三者連携システムのための新技術

現在適用中の他のものと同様に前述のキーテクノロジーに加えて、新しく開発された技術的なアプローチが、人、機械、ICTシステムの相互関係が安全の三者連携システムの基礎を形成するデジタル環境に革命をもたらすことを確約する。

3.6.1 デジタルツイン

運用領域の考えられる反応の範囲内でIoT業界は、確立したテクノロジーをベースにした既製のソリューションを整理し、デジタルツイン構築と呼ばれるデジタル環境ワークスペースのシミュレーションを可能にする。最もシンプルな表現としては、デジタルツインは、サイバーと物質的な世界の橋渡しをすることに関与する。より広義な意味では、デジタルツインは、分野が反映される、予測される、あるいは他で探すうちのいずれかで変化が影響することにより物質的な世界からサイバースペースへ模倣あるいはマッピングすることである。安全性という点において、デジタルツインは安全状態をサポートするのに使われる包括的なデジタルモデルである。

このようなマッピングの例は、大がかりな建築プロジェクトがコンピュータシステム上で完全にモデル化することを通じた[30]建築業界のビルディングインフォメーションシステム(BIS)、そしてコンピュータを使った設計システムや製造（CAD/CAM）システムが構成要素や部品や機械の設計において活用される製造業界において関連する[31]。安全に関してこのテクノロジーは、労働安全を強化することを可能にし、差し迫った、予期せぬ安全関連案件に寄与する。

デジタルツインは特定の安全慣行をテストするため、火災や爆発を視覚でシミュレーションするため、及びシミュレーションにおいてウォータースプリンクラー・消火器システムのようなテストされ実証されたものを提供するための最適なフレームワークを提供する。

しかし、デジタルツインの可能性はそこで終わらない。デジタルツインが実際の労働環境を模倣するとき、労働スペース実践への動的なアプローチをもたらす。それは過去では厳密な静的アプローチであり物理的な世界にもっぱら限られたものであった。図3-7に製造環境におけるデジタルツインの事例を示す。「デジタルツイン」という用語は、労働者の安全に適用される状況下で「協調安全におけるデジタルツイン」あるいは、「人と機械の労働空間のためのデジタルツイン」がよりふさわしい呼称なのかもしれない。

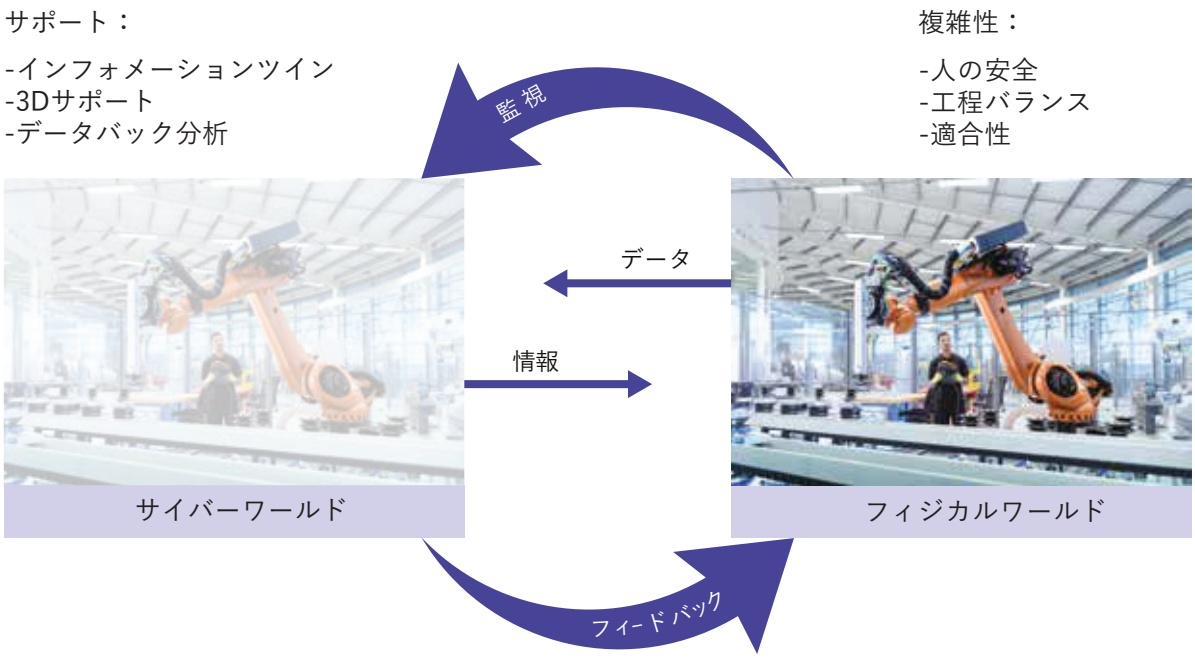


図 3-7｜フィジカルワールドと並行するデジタルツインオペレーション

3.6.2　リアルタイムの衝突回避

リアルタイムプロセッサ（機能は口語的に「高性能コンピューティング（HPC）」と呼ばれる）は、ビジョン、動き、他のセンサーを備え、ものが静的あるいは動的な障害を示すかどうかに関わらず、人や他の物が衝突するのを回避することができる動くロボットを含んだ労働環境をつくりだすことができる。

衝突防止は、遠隔操作車両を含む自動運転車両システム、海洋船舶、乗用車を含む、自動走行車システムで広く用いられる概念である。しかしながら、そのコンセプトは同時にロボットを急速に普及させてきた。輸送業務に関して衝突防止システムは、シールド、停止や接近アラームなしで人と機械が協調する職場を設計するために重大かつパラダイムチェンジのアプローチを示す。

この白書では、未来の人と機械の相互関係が、人の反射神経よりも効率がいいリアルタイム動作検知、処理、反応をベースにすることを想定している。関係するスピードは、ダイナミック、リアルタイム動作計画のためのリアルタイムプロセサを特徴づける次世代ロボット工学を必要とする。このような計画は、ロボットの動作領域に入ったであろう静的または動的障害物の回避を可能にする一方で、設定された特定の開始地点から目標とする動作終了地点までのロボットの演算と履行を可能にする。図3-8ではリアルタイム動作検出がどのようなものかを示す。

ロボットの通過経路に障害物が置いてあるとき、例えば、人が作業台の上に箱を置くという作業過程に入っている間、その障害物と人はバーチャルあるいは他の検出機器を経由してロボットに識別され、システムが新しい動作計画を演算する。ものの動作スピードによって、いくつかの反応が可能である：

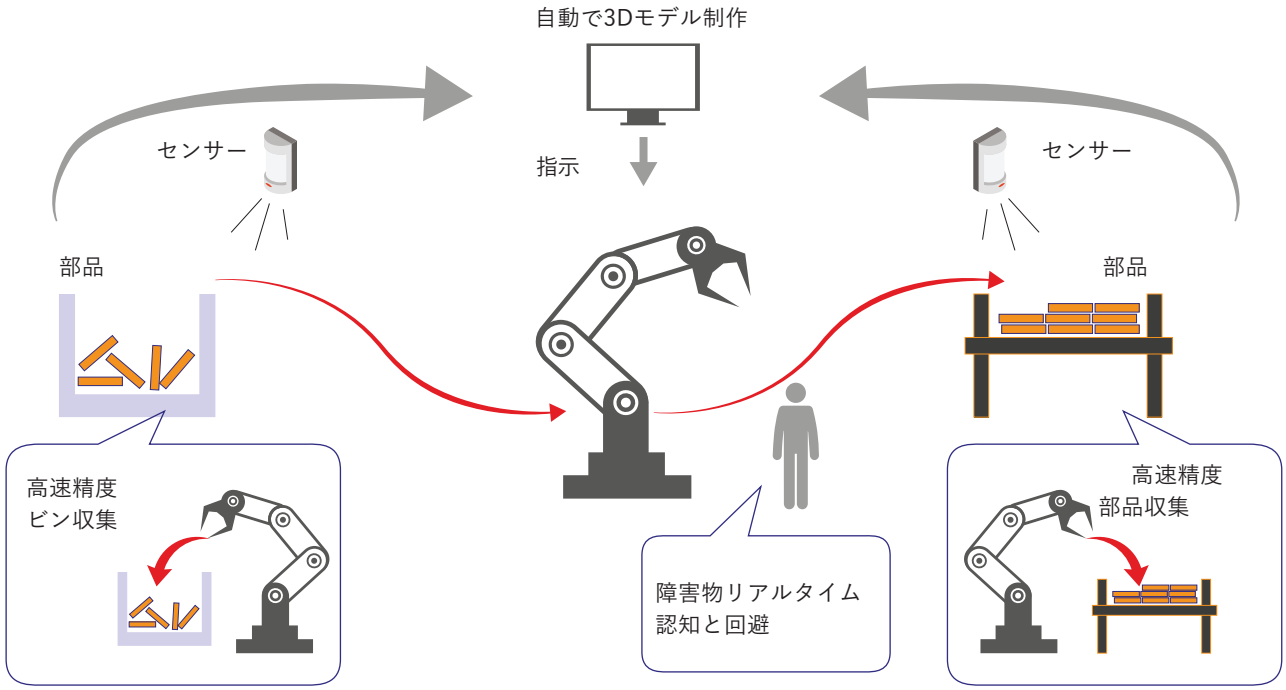


図 3-8｜リアルタイム動作のキー要素：探知・検算・実施

- 経路上で動かない物体や動きがゆっくりの物体の場合、あるいは人の通常作業中、システムは機械がもとの経路に沿って作業を続けることを防止する
- 早い動作の物体の場合システムは、障害物との衝突を防ぐためロボットの動作を時間内に停止し、新しい動作経路を構築するためにその目的地を再度見直しする
- もしメカニカルアームの反応に対してとても速く侵入する場合、損傷を最小限に食い止めるためにシステムがその動作を停止する

3.6.3 AI支援による行動分析

高度なエッジAIは、クラウドからの事前の「ティーチングデータ」を必要とすることなく、通常とは異なる人の動きの検知が可能になる。AIを用いれば、このように職場での人の動作や行動を分析することができるようになる。機械そのものに備わった十分なコンピュータの性能、あるいは、環境から得られたコンピュータの性能により、機械はオペレーション中に労働者に不安全な動きやや不健康な姿勢を知らせるよう仕組まれる。このような情報は労働プロセスや労働環境の継続的な改善を支持してきた従来のデミングサイクルモデルで用いられる。デミング改善サイクル（計画－実行－評価－改善）はこのように、AIと人が全体的な職場環境の安全を改善するための役割を共有するさらなる活動領域となる(図3-9)。実際には、正しい指示のもとで、AIは労働者の安全のための一定のタスクを実行できる。

最も基本的な設計において、このようなシステムは機械学習なしでさえも、労働者やその周りの人によって見逃されるような人の動きのわずかな差異を検出するセンサーやシグナル処理技術をもたらす。

より速い処理時間を持つエッジAIで、通常の人では見抜けない労働者の一部の動作中の異常や必要のない動作の検出が可能となる。いくつかの技術により、数ある中でも次のような異常を検出することが可能である：

- 運動要素の境界予測：
  作業プロセスの観察を繰り返した後、アルゴリズムが通常の労働場所とその場所を超える空間までの距離を識別する
- 標準オペレーションパターン：
  アルゴリズムが、通常繰り返しのタスクがどの位時間がかかるのか、そのパターンからのどのくらいずれがあるのかを認識するアルゴリズム。これは疲れ、意図しない傷害、あるいは、他の安全衛生に関する問題を防ぐのに役立つであろう
- 非標準的な動作の検出、あるいは体勢：
  アルゴリズムは、立っている、または座っている、あるいは疲れや倦怠感を引き起こす極端な体の動き（例えば、サークルの中でのストレッチ、あるいは、ウォーキングのような）の間の人間工学的でないポジショニングを検出する

そのような異常が検出されるとAIアルゴリズムは、背筋を伸ばす、あるいは少しゆっくり歩く、のような人の行動にちょっとした変更を指示することができる。同様にシステムは休憩を指示し、個人との協業における労働プロセスに適応することができる。

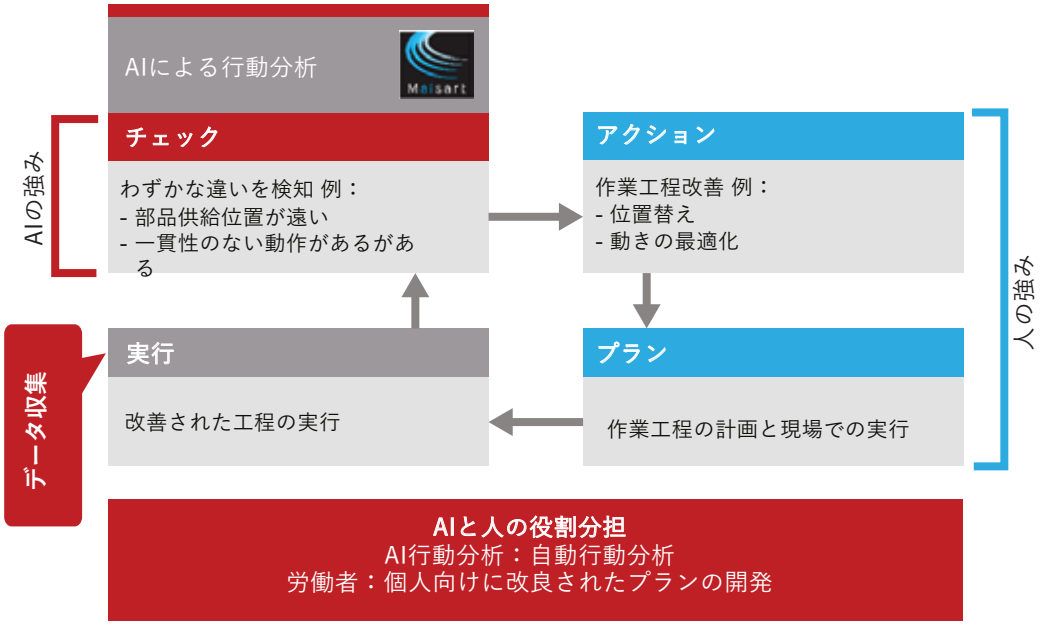


図3-9｜AI行動分析

3.7 技術的必要性：サイバーセキュリティ

情報技術の使用の増加で、サイバーセキュリティが安全管理システムの増大する複雑さを管理するための取り組みのコーナーストーンを形成する。特にこれはスマートマニュファクチャリングや協調安全メカニズムに関係するからである。しかし、このようなシステムの複雑さはそれらの微弱性を増し、確実に安全機能の損失を招く。

ISO/IEC２７０００ではセキュリティマネジメントシステム（ISMS）の概要が紹介されている。それはIECガイド１２０「セキュリティ側面―出版物に含むべきガイドライン」に沿うすべての分野特有の規格の参照用として用いられるセキュリティ標準の基礎を構築する。ISMSのフレームワークは、繊細な情報の守秘義務、全体性と可用性を保護するために用いられる。情報セキュリティマネジメントシステムは、情報セキュリティの３本柱：人、プロセス、技術に対応する施策を含むリスク管理のためのシステマチックアプローチを提供している。

しかしながら、産業用制御システム（ICS）は実質的な汎用情報システムとは大幅に異なる。動的、及び変わりやすい脅威からの保護は両者にとって重要である一方で、安全はICSにおける最も重要な要素となる。もし、ICSが攻撃により壊れた場合、安全機能により提供されるリスク軽減は機能しなくなる。システムは不安全となり、雇用者がリスクにさらされる。安全目標はセキュリティを必要とする。産業用制御システムの新たな情報セキュリティマネジメントシステムのゴールは、全体性、有用性、機密性、安全性を連携させることである。いくつかのISMS導入の施策は有用性係数において安全面を含む。しかし、これは産業にとっては不十分である。ハッキング、自然災害、コントロールシステムにおける内部的な問題のような脅威や、脆弱性による社会へのインパクトは、深刻な経済的、社会的な崩壊をもらす大きなダメージに成り得る。

そのため安全は、全体性、有用性、機密性と同じようにISMSにおける不可欠な価値と認識されるべきである。リスクマネジメントのシステムアプローチはこの目的に欠かせない。安全機能や接続性を支えるすべてのシステム、及び製品規格はISO/IEC２７０００あるいはその他のセクター固有のセキュリティ規格をベースにサイバーセキュリティ要求を包括すべきである。

3.8 三者連携モデルの標準化、及び適合性評価の意味

三者連携モデルにおける人と機械の安全をモニターする規制当局は、次を含む、さまざまな要因を考慮する必要がある。

- 製品など、個々の構成要素の適合性評価
- すべての製品の総計とそれらの相互運用システムタイプ認証
- 人の力量やこれらの環境で働く要員の認証

個人がロボットの並ぶ生産ラインで働いているのか、あるいは建築現場なのかどうか、製品安全、システム安全、個人の力量が安全な労働環境において全て重要である。

三者連携の安全アプローチは、システムの異なる部分にフォーカスするための個々の標準化活動を全体として分離し易くする。技術的に、比較的高い抽象レベルで三者連携システムの各構成要素に対する標準化、及び/またはガイダンスが求められている：それは人がインテリジェントな機械と協調する安全な労働環境を確実にし、特に知能を搭載した機械の達成可能な安全目標を定義し、そして（セマンティックな）相互作用、コンピューティングパワーや倫理、セキュリティ標準に焦点を置く職場周辺のシステムをインターフェースフレームワークに提供することである。

機械の標準は、技術仕様を含む既存の標準とは少し異なる。このような仕様は、人が共に働く物理的システムにつながる比較的直接的な標準から、電気の、機械の、ロボットシステムの安全標準に、及び得る。機械が協業環境で作用する場所は、今までにない高いレベルの標準がインテリジェントな機械に安全目標を与えるために開発されるべきであり、おそらくそのような要素は、リアクションタイム、動作速度、及び/または、人体への最大インパクトのような要素も含まれる。同様のことが環境内のシステムにも当てはまる。

ISO/IEC JTC 1は、端末エッジ機器やクラウド上の装置に対する要求について協議するためのフレームワークを提供している。AI（SC42）に関する小委員会もまた、協議のための関連フォーラムのようであるが、安全面は分けて扱われるべき、あるいは安全に対する水平規格グループと連携すべきである。

職場における人に関しては、人が、知的な人と機械の協調を意図した機械と働き、維持し、プログラムあるいは設計をするために所有する必要のある知識や力量レベルを明確にする認証システムを導入することは繊細なことにみえる。

3つの構成要素が一緒である三者連携システムに対し、認証フレームワークが部品よりも統合システムに焦点を当て開発を急ぐべきである。鉄道安全のケース（IEC６２２７８　　鉄道への適用―信頼性、可用性、保全性、安全性（RAMS）の仕様書と表明）のような複雑なリスク分析を含み得るが、個々のシステムコンポーネントの適合性を表明するよりシンプルなシステムで十分であろう。

これらのどのケースも適合性評価が関連するようである。ISO/IEC　　１７０００で定義されるように、適合性評価は特定の要求が満たされることの実証である。その要求は規制、規格、あるいは技術仕様書を含め得る。適合性評価は、試験、検査、妥当性確認、検証、認証などの多くの異なる活動をカバーし、個人あるいはコンビネーションのいずれかに適用される。3つの機能は、選択、決定、レビューであり、規定要求事項に適合していることの表明に使用される(図3-10)。

適合性評価活動は認定目的でISO CASCOで開発された種々のISO/IEC 規格が活用される。これらは試験・校正試験所の適格性に対する一般要求をカバーするISO/IEC１７０２５、製品認証機関の認定基準であるISO/IEC１７０６５、及び要員認証機関のオペレーション基準を規定するISO/IEC１７０２４（また人の認証機関としても知られる）を含む。

例えば、AI、人と機械の相互関係、労働者の機能的安全、適合性評価機関や法律制定者のような三者連携モデルに適用される革新的なテクノロジーを考慮するうえで、革新速度を落とさないデジタルトランスフォーメーション時代の要求を満たすために、異なるスキルの組み合わせ、力量、適応技術が必要とされる。新たな意味合いとして、製品はもはや単に機械的、電気的デバイスではなく、労働環境周辺の人、機械、知的ソフトウェアが全て機械学習機能を経由し互いに関係し合う三者連携システムに組み込まれている。適合性評価機関、標準化組織や法制定者は、製品が進化し、人の役割と、その環境における人間的、社会的価値に細心の注意を払うような技術環境を包含なければならない。

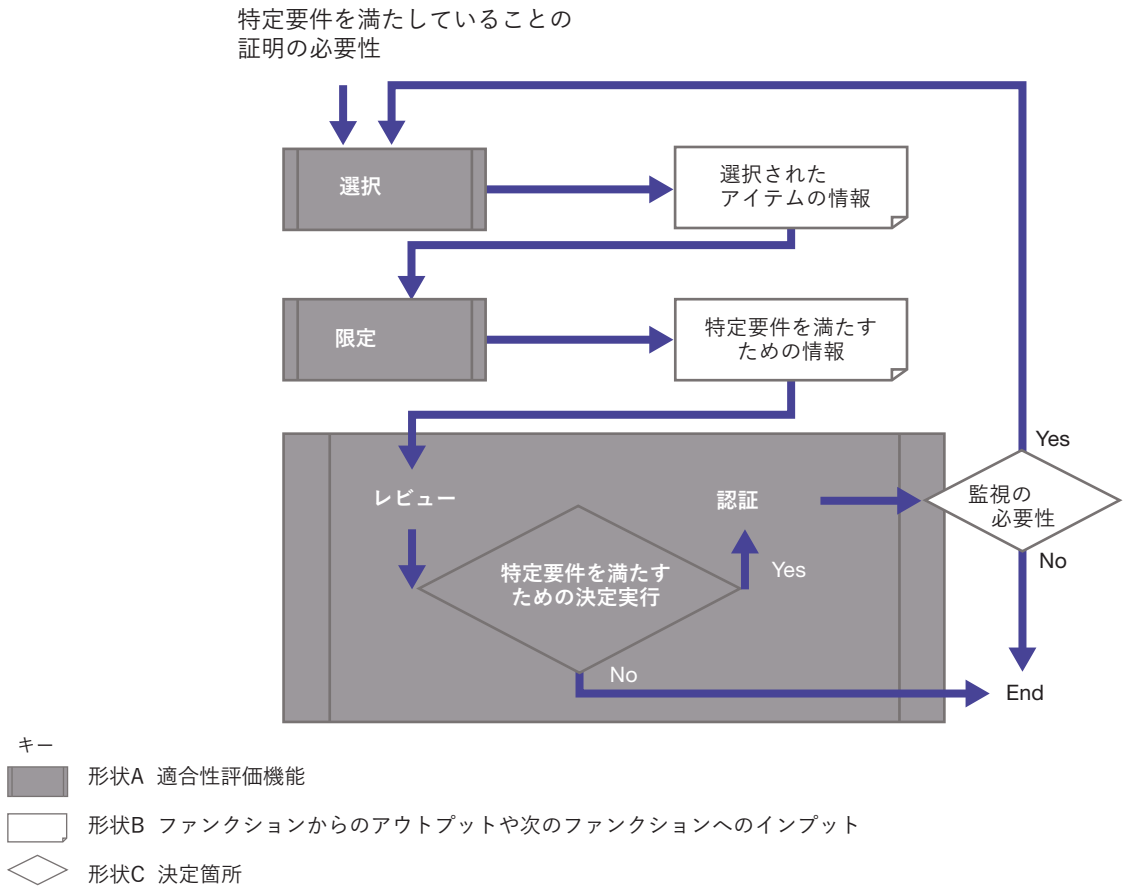


図3-10｜適合性評価への機能的アプローチ（ISO / IEC 17000）

第 4 節

三者連携システムの応用分野

このセクションでは、電子機器と知的機械を含めた革新的な安全解決のパイオニアとなるプロジェクト、業務、及び会社のいくつかの例を紹介する。該当する応用は論理的な連携の必要性はなく、安全の三者連携システムで使用されるパターンが認識されるであろう。開発されたソリューションのいくつかは、ヘルスケア―あるいは製造業のような安全関連環境においてAIにより提供される生来のコンピュータの力の有効な利用にフォーカスされている。一方で、安全の骨格としてのネットワーク、つまりロボットを導入している製造業の現場で実施されるリモートセンサーによるメンテナンスや工業化された農業、ターゲットとする人と機械の安全な相互関係に焦点をあてる。すべての事例は、作業現場とそれらの環境の間の明確なインターフェースの必要性を強調し、将来必要となる革新的な安全ソリューションを開発するのに必要な力を整理することができる。

4.1　製造業における人と機械の協調

人と機械の相互関係が存在する職場において、協業ロボットの使用で多くの例があるが、安全柵は存在しない。従来の産業ロボットは一般的に柵で人と離されている一方で、協調ロボットは、労働者と機械が協力する環境における人との直接の相互関係を可能にすることで柵の必要性を取り除いた。このような状況下で、ロボットは主に、繰り返しの肉体的な骨折り業務（３K: 危険、汚い、きついと呼ばれる※英語では3D:Dangerous,Dirty, Demandeing ）に対し、手先の器用さを必要とする作業[32]に集中できる人とともに責任を負う。図4-1は当該状況を示す。この種の配置の詳細例は次の通り。

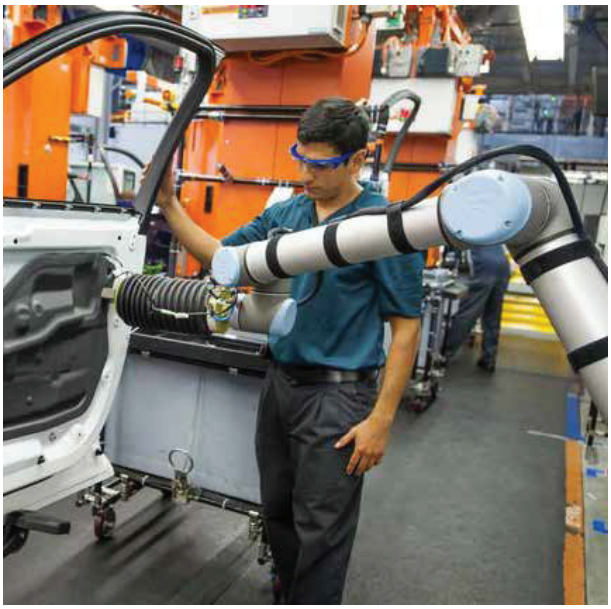


図4-1 |労働者とロボットが協業する労働環境の例
（出典：www.acro.com）

ハイブリッド車（HV）インバーターの製造プロセスにおける空間と柔軟性を最大限にするために、日本の主な自動車会社[9] は組み立てや検査を容易にするための協業ロボットを採用してきた。

9　トヨタ自動車株式会社 https://global.toyota/en

例えばロボットが、労働者の身長により、HVインバーターの配置と動く方向を決定する。協業ロボットはまた、ペアでジグ機能を実行できる：1つは単純なねじ締めのため、もう一つは、労働者が関わるために相応しい角度で作業部品を置くためである。労働者の重荷となる業務手順を最大60%まで軽減することに加え、製造業においての協業ロボットの使用は、物理的かつ心理的なストレスに対して効果的な軽減策を示している [33]。

ロボット[10] の主要な製造業では協働ロボットは、ボールねじを組み立てるのに使用されており、重い作動装置を運ぶロボットと、ベアリングの設置のような手先の器用さを求められる業務を行う労働者と共に使用されている。

多国籍の工作機械の製造業者[11] は無人搬送車（AGV）ロボット、つまりＡＧＶ、協業ロボット、ビジョンセンサー、電動ハンド、及びレーザースキャナーで構成されるロボットを開発している。 AGVロボットは例えば、作業部品の設置と撤去、空気の吹き出し、バリ取りなどに使用し得る。それは周辺の障害物を避けながら、指示された方向に自動で移動する能力がある。これは職場の床の磁気テープを導入する必要性をなくし、こうして工場のレイアウト変更を容易にする。TGVロボットはまた、工場内で工場内の物品を配分する際にも使われ得る。従来の自動システムとは異なり、この技術は工場のフリーレイアウト設計を可能にし、ロジスティクス管理を可能にする。AGVロボットの姿は、ロボットに足があること示す。それは、閉ざされた空間や制限されたエリアの自動システムを構成するよりも、AGVロボットが人と同じエリアや人と同じレベルで稼働し、それによりロボットと人の共存を促進する。

上記の例では、三者連携システムにおいて人と機械の協調をハイライトしている。システムは、人を回避するのに十分な適性と速度が与えられれば、人を相手に安全に相互作用するようにできる、ということを示している[34]。現在このようなシステムは、迅速な適応装置を構成し、特定の運用課題にカスタムメイドで対応する。このことは、１つの職場から他の職場まで安全に対する教訓を置換することはいうまでもなく、同じ工場内で幅広い職場に対応するために、これらのシステムをスケールアップすることを難しくしている。これらの労働環境は三者連携システムから、部分的かつ全体的の両者を考慮することをベースに、人と機械の間の相互作用を識別し明確化することにより、そして安全機能を最適化することにより、恩恵を受ける。安全機能を設計する際に環境システムを考慮に入れることがもう一つの利点である。

4.2 建設業における インテリジェントマシン

西日本では、安全性向上のため、最先端のセンサー、照明やAI技術が試験的に導入されている阿蘇の国道57号の滝室坂トンネルの建設工事が進行中である[35]。機械と環境の情報と同様、人の情報を利用するスマートセーフティシステムの複雑なネットワークが構築されている（図4-2）

作業環境にはいくつかのスマートセーフティシステムが設置されている。そもそもトンネルにはビーコンと検出センサーが工事領域、労働者のヘルメット、及び重機に多くの場所に設置されている。これで追跡される機械と労働者の位置を確認でき、タブレット端末で表示することができる。事故を防ぐために、ホイールローダーには右、左、後ろにAIカメラが搭載され、各AIカメラには警告ライトとブザーが取り付けられている。

10 ファナック株式会社 www.fanuc.com

11 DMG森精機株式会社 www.dmgmori.co.jp/en

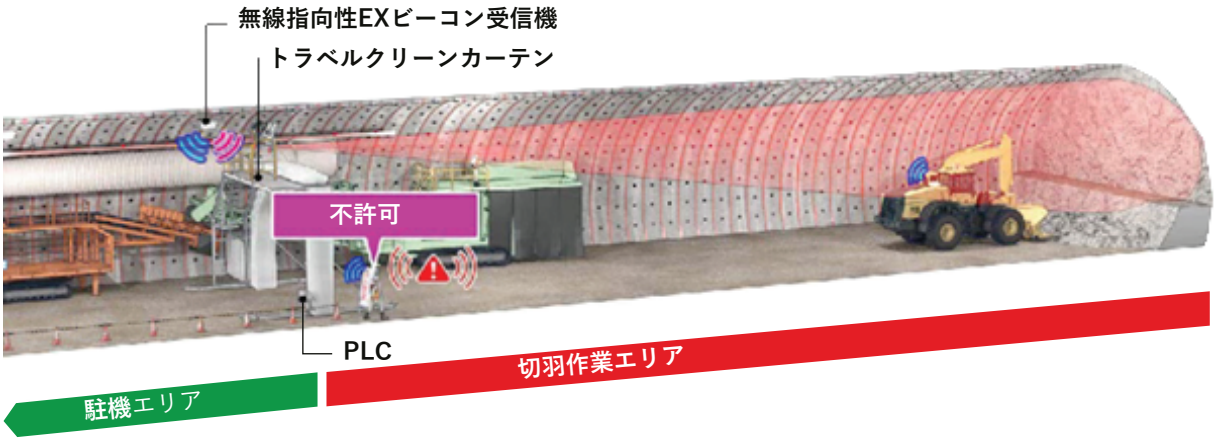


図4-2｜ICTを介して労働者、機械、環境をつなぐトンネル保護システム

AIカメラはホイールローダーの近くの労働者を検出し、ホイールローダーの動きに対してアラームを鳴らす。照明システムさえも安全に役立つ。最初に、次のような状況では、現場では、通常より高い光強度で作業をする：このトンネル保護システムの標準は通常の100ルクス標準よりも強い、200ルクスである。それだけで、良好な視界が労働条件を容易にし、異常な状態を検出する機能を容易にするので、平均的なトンネルと比較して安全性が向上される。第二に、労働者が危険の潜む制限地区に入るとき、照明の色は白から赤に変わり、トリガーとして警告アラームが鳴る。発掘現場は特に騒がしく、照明の色の変更は非常に効果的である。この綿密な安全へのアプローチによりそのプロジェクトは2020年3月に一般社団法人セーフティグローバル推進機構（IGSAP）からSafety2.0適合マークを取得した。適合性マーキングは、システムが協調安全の要求事項を満たしているという証明となる。

三者連携システムに関しては、次のようなインテリジェント機械の強力なショーケースを構成する：カメラや、人を検知し適切な時間にそれを知らせるAIを搭載したロールローダー。システムの集まり、車両搭載のインテリジェントカメラ、照明、及び労働者追跡システムすべてが、職場を安全のためにAIシステムに特化したフロントランナーにしている。それは労働者と、AI機能と環境システム（照明システム）を備えた機械を統合する。労働者と機械の位置情報は、機械の安全制御や労働者の安全行動を支援するために共有されるので、このシステムの協調安全レベルは、 規格の明確なガイドラインでは、CSL－３に近いと考えらえる。CSLレベルはより具体的かつ正式に決定され、改善点が規定され得る。三者連携アプローチは、システム全体の安全証明と同様、個々のシステムに対する要求を標準化することによって、安全な労働環境を設計するために構築するシステムをより容易にする。

4.3 農業の安全を促進する環境でのインテリジェントネットワーク

デジタル農業は、農産業において主なトレンドとして広がってきている。デジタル農業では、生産を拡大する活動と同様、 安全を促進するのに、労

働者、機械と環境はICTにより繋がっている。　例えば、対応したネットワークは、一部はGPSシステムによってサポートされるセンサーを経由して、農業で使用される化学物質のより良い管理実現する。（図4-3)。固定センサーに加え、機械や無人高所作業車（UAVs）に装備されたモバイルセンサーが、AIテクノロジーを使ったデータマネジメントシステムで全て分析される湿度、土壌圧縮度肥沃度、葉温、微気候、昆虫、病気や雑草侵入に関するマップと総合するのを助ける。したがって、ICTシステムは、どの種類の、どれくらいの量の化学物質が土に必要で、どこに必要なのかを正確に知るという点で農家をサポートする。この正確さによって、穀物生産に使用される化学物質を最小限にし、それにより、化学物質の排出や農場付近に住む人々の化学物質に関係する病気のリスクを軽減する。

図4-3 ｜農場全体での健康と安全のためのネットワーク
（出典：The National Agriculture and Food Research Organization 国立研究開発法人 農業・食品産業技術総合研究機構：NARO）

しかしながら、そのネットワークはまた、いかに人と機械、及びデジタル処理された環境が 総合的なパフォーマンスを最大限にするために共に取り組むことができるかのショーケースでもある。機械は反復作業や過酷な作業をすることが得意で、人は目的、決定、及び創造性を再構築するのに長けている。　したがって、人と機械の協調コンセプトは、農業において製造改善や安全管理の観点で適切な戦略である。

阿蘇のトンネルプロジェクトの例のように、センサー、安全デバイスやドローンが製造に関連したリスクを地図に精密に示すことができる。

安全情報は、データ処理が行われるシステムの周辺に伝えられる。危険な状況が起こりそうなら、システムは監督者に対し、及び該当する機械に対し、適切なアクションを取るための警告を発報することが可能になる。　そのようなシステムは将来、農場管理者に事故防止のために障害物を取り除く可能性を提供する。

上記の例は、人と機械の間の業務を統合した開発済みデジタルネットワークがいかに安全を促進しているかに着目している。

ICTネットワークやシステムの拡張端末は、労働者を安全に留まらせることや、農場管理者と健康情報を共有するのを手助けする。もし気象条件が変更し、労働者が装着可能な検知器を備えているならばシステムは警報を発することができ、体調をモニターすることができる。もし周辺でのコンピューティング力が強力であれば、AIは事故の分析、予測、予防をサポートすることが可能である。

4.4 自動化された安全側面を備えた配電システム

電力配電システムの安全はこれまで懸念事項の中心であった。なぜなら、多くのエネルギーの輸送は本質的に不安全なであったからである。しかしながら、エネルギーの状況は特に、配分された、及び/または再生可能エネルギーの出現、送電網の安定性が保障された主要な発電所の漸進的な閉鎖、電力の消費者というよりも「電力自給自足者」に成り得るいかなる送電網のユーザーも含めたユーザーレベルの一歩進んだエネルギー効率プログラムの導入、などにより、さまざまな劇的な変化に直面している。ローカル生産や自動消費のトレンドには、送電網を利用しない小規模発電網があり、必要に応じて、電力消費や送電網への直接サービスの提供の集合型を導入することなどがある。

この新しい変成作用エネルギーの状況は明らかに電力インフラの安全が取り組むべき方法に関して課題をもたらす。しかしながら、多くの革新的な戦略が、新しいリスクに直面する電力インフラの同レベルのレジリエンスを確実にするために配置されていることをここで再度述べる。これらの戦略の第一は、以下を認めるデジタル手法の強化である：

- エンドユーザー（スマートメーターを通じての）の一部分において同様、インフラ自体の増強されるモニタリングやコントロール機能性；このテクノロジーは増加の一途をたどるICT機能に電力分配コントロールセンター機能を追加する
- 共通モード故障の検知と削減例として、（わずかな）管理されてない分配エネルギー資源の増大によるもの
- 侵害の予測と対応
- スマートグリッドメーターをベースにしたエネルギー予測能力の増加
- エンドユーザーのスマートグリッドの使用を通じ、また、ネットワーク自体からのデータ抽出を通じた資産の条件付きをベースとするメンテナンスへのシフト

デジタル手段の使用強化の欠陥では、産業はサイバーセキュリティの脅威に悩まされてきた。さまざまな方法においてサイバーセキュリティは主な関心事であり安全リスクの元凶となってきていて、結果としてグリッドの回復力に影響を与え得るものである。たとえグリッドマネジメントシステムが労働者と正常に直接相互作用しなくても、多くの労働者は機能するためにそれらに依存している。この産業によって直面する問題は、デジタル的に可能ないかなる安全システムにおいてもサイバーセキュリティの必要性をハイライトする。ローカルな三者連携安全システムは、グリッドコード、スマートモニタリングや信頼性の観点からシステムインターフェースを明確に記述すべきであるという事実を示している。

4.5 配電ネットワークのスマートモニタリングのメンテナンス

高圧送電線はさまざまな地理的環境に及ぶ。これは、洪水、地震、地滑りのような自然災害によってもたらされたものに加え、しばしば検査担当者に重大な安全リスクをもたらす。AIに基づくインテリジェントな検査アプローチは、さらなる効率的でタイムリーなライン検査を可能にし、これにより担当者が直面するセキュリティリスクを大幅に減じる。関連するインテリジェントな検査材料は、調査されるシステムの関連部分、及び主要な

リスクシナリオとのリンクを自律的に識別する推理能力を持つローカルAIモデルを装備する。

送電線検査は、さまざまなタイプのリスクシナリオを特定する必要がある。それは物体の欠陥（絶縁体の欠陥、ボルトの緩み、金属の変形など）、通路上のリスク（危険な構造物によるもの、超高層の建物群など）、あるいは、外部の無縁なもの（鳥の巣やその他の侵入物）を含む。これには高解像度画像や動画を迅速に処理可能なインテリジェントな検査装置が必要である。識別された危険警報はリアルタイムで現場の検査員へ送信され、タイムリーな処理ができるようワイヤレスネットワークを通じて中央の監視局へ送られる。同時に、リスクと特定されて分類されたイメージはまた、モデルトレーニングと最適化のためにクラウドで要約される。

関係する環境と障害が大きく変化するので、モデル自体は最適化され、継続的に更新される必要がある。したがって、インテリジェントな検査システムがクラウドエッジでコラボレーションするのを可能にすることはとても重要である。クラウドの中では、強力なAIアクセラレータ機能が、モデルの生成と最適化に使用され、情報は更新と同期するネットワークを通じてインテリジェントな検査機器に転送される。

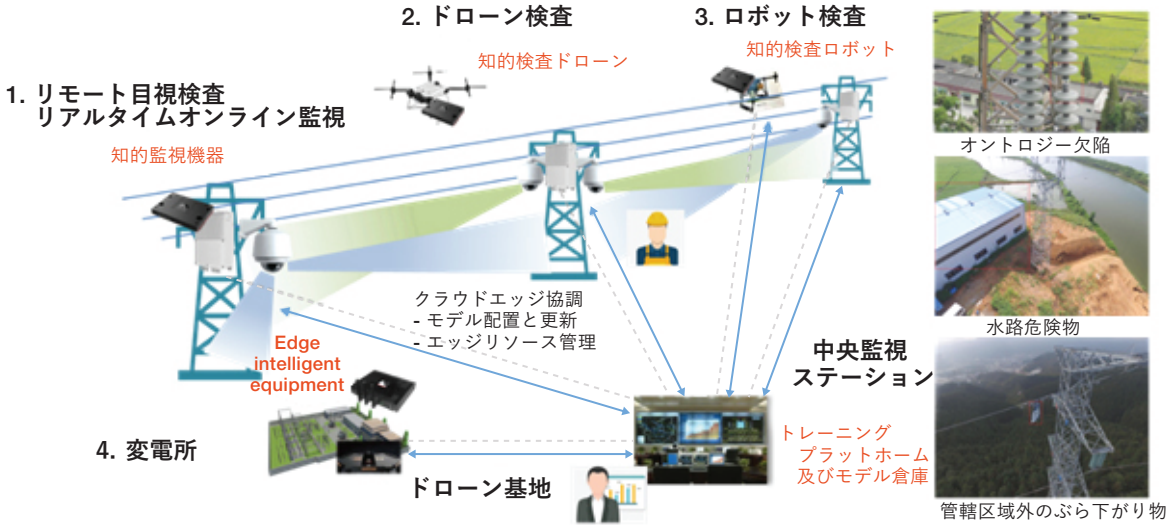


図4-4｜電力線のスマート監視システム

図4-4の例は、センシングシステムが人をサポートするときにどうやってメンテナンス作業がより安全な状態でできるかということを示している。検査担当者は、危険なほどの高度での測量の必要がなく、より迅速に危険因子を特定し、そのようなシステムが電力ネットワークと共に使用される時には、リモートで問題解決ができる。

4.6 都市の治安

多くの都市、特に安全な都市技術に多額の投資を行って来たような都市は将来、犯罪率の減少を経験する一方で、従来犯罪（強盗、恐喝、誘拐、暴行、公序良俗違反、深刻な交通犯罪）は、特に失業率の高く富の分配の不平等な都市においては、依然、存在するだろう。

犯罪者は、安全な都市技術の効果に対抗するため、例えば監視カメラを避けたり、電子デバイスを身に付けなかったり、あるいは、安全技術メカニズムが少ない町へ移動するなど、彼らの行動を変えると予想される。組織犯罪グループ、特に国際犯罪に絡むようなグループは、デジタルプラットフォームの使用を通じて活動の幅を広げる。そしてテロリストと犯罪組織の間にリンクが出来上がる可能性があり、彼らは主に密輸、麻薬密売、合成ドラッグや天然資源の違法取引などで違法な収入を得る。

犯罪の領域を超えて、グローバル化された健康の脅威は引き続き公共の安全に影響を与える。公衆衛生問題の発生がより複雑で挑戦的であり続ける世界保健機関や世界経済フォーラムと同じくらい多様な団体の意見により、現在のコロナ禍は世界が直面する最後の深刻なパンデミックではないことは明らかである。さらに、生態学的劣化や地球温暖化の影響下で、都市はますます密集し、不十分な住宅供給、及び水、下水道、電気、廃棄物管理のような基本的なサービス不足で表されるスラム街が増加する。

このような状況では、犯罪と同様、公衆の混乱により伝染病が発生する可能性がある。公共安全に対するそのような進化する脅威への対応として、多くの国家当局ではデジタル安全システムに取り組んでいる。これらのシステムのほとんどが独立して運営されているが、プライバシー規制が許す場合、データベースは、犯罪、テロ、伝染病、及び自然災害などを検知する機会を増やすため、互いに繋がるであろう。このような協力体制は、協調的な公共安全を構成し、将来ますます導入されることになるであろう。多くの公共安全機関は、次の主要な構成要素を含む何らかの形のC4ISR、あるいは、協調的なC-C4ISR[12] ソリューションを取り入れるだろう。

- 協調的なコマンド＆コントロール（C2）：
  自動通話分析、フィルタリングやディストリビューションによる、及び及びリアルタイムビデオ監視やソーシャルメディア統合といったマッピング以上の可視化による単一の緊急電話番号を通じて複数の機関の協業を可能にする集中的，可視化されたコマンドセンター化
- 協調的コミュニケーション（C）：
  一つのデバイスで音声、ビデオ、そしてモバイルアプリを実装する、そしてレガシーシステムと同様に他の類似のものとの相互動作が可能な、事業用LTEベースのブロードバンドのクリティカルコミュニケーション追跡システム。システムはカバレッジのないエリアで素早い展開のための迅速なバージョンを提供しなければならない。
- 協調クラウド（C）：
  コンピュータ資源を最大化させ、情報交換を支援し、ユーザー中心のアプリを許容し、需要が急上昇した際にダイナミックな資源を提供し、新たなサービスの迅速な展開を促進する、オープンスタックベースの策定可能かつ弾力性のあるプラットフォーム
- 協調インテリジェンス（I）：
  未知のものを発見し、点と点をつなぐための大規模な並列処理データベースと分析アルゴリズムを含むビッグデータ技術の使用
- 協調監視（S）：
  効果的な分析と効率的な達成のための2層の知的なビデオ監視クラウド、これはエッジノードでの仮想化された処理、及びエッジノードと中央ノードの間の高解像度ビデオの超高速移動による。
- 協調偵察（R）：
  多量の並列処理をサポートする、さまざまなサプライヤーからのセンサーに対して統一されたAPIインターフェースを装備したセキュアなIoTクラウドプラットフォーム

12 C4ISRとC-C4ISRは、ファーウェイによって開発された共同の公安ソリューションネットワーク
www.huawei.com/en/news/2017/4/C-C4ISR-Public-Safety-Solutions

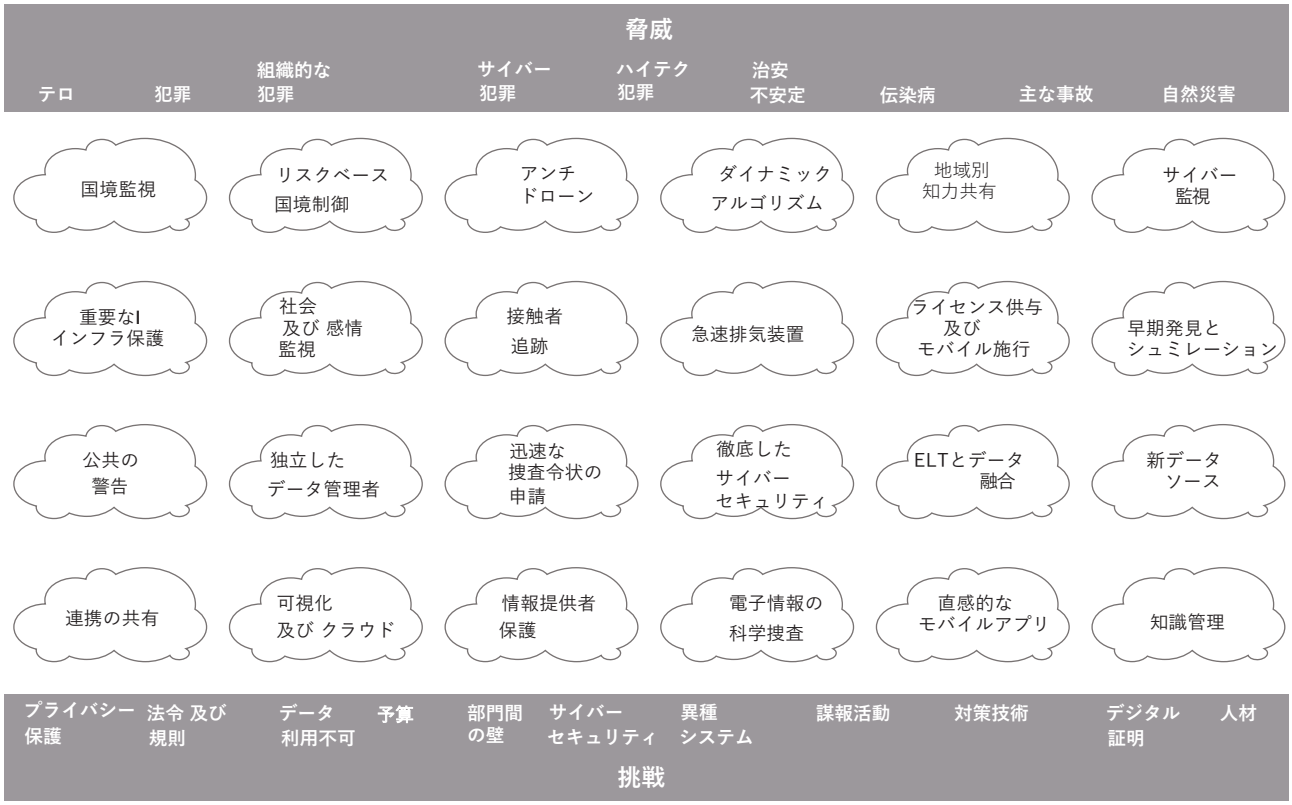


図4-5｜協調的な公安のための脅威と課題

三者連携システムに関して協調的な公共の安全戦略は、市または全国規模のICTシステムが最終的にさまざまな企業システム（図4-5）の骨格となるように開発され、それは職場の「環境」が、データ統合やAIのデータをベースにスマートな決定を生み出すためにさまざまな形式の情報が集合する大規模な企業アーキテクチャシステムに繋がり得ることを示す。たとえ国際的な企業が多様な目標を持っているとしても、それらの企業システムは、幅広い実体との協業を可能にする類似のスケールや複雑さであることを期待されるかもしれない。（例えば、何千もの井戸や異なるつくりやブランドの精製装置やパイプラインを監視している石油会社のように）。公共安全フレームワークと企業の両者の場合、異なる組織間におけるデータ交換を統制する法令や規制が必要である。

このような共有はケースバイケース、バッチ、またはリアルタイムベースのいずれかで発生する可能性がある。データが異なるソースからくるので、含まれるデータ標準の欠如によりもたらされる挑戦もまた解決されるべきである。

4.7　電気へのアクセス

今日、世界でおよそ11億人に正規の電気アクセスがない。SDG 7：手頃でクリーンなエネルギー、は、2030年までに手の届く価格で、安全で、信頼性があり、クリーンなエネルギーへのアクセスを確実にすることにフォーカスしている。しかし、電力供給は言うほど簡単なものではない。世界中の居住施設や住居に安定した電気送電網に接続することは、高価で、時間がかかり、規制で拘束され、荒く遠隔地への挑戦でひどいものである。結果として、複雑な送電線のネットワークや変電所を通じて遠隔地に繋がった広範囲にわたる発電所

を含む従来型のグリッドモデルは、進化し技術開発によって生まれる新たな可能性に適応するためにプレッシャーがかかっている。

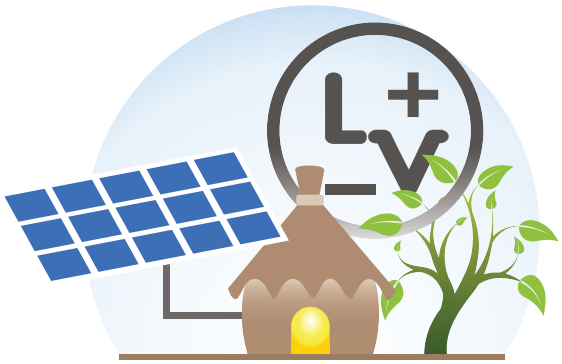


図4-6｜低電圧直流供給電（LVDC）：現代生活に欠かせない資源としての電力

ひとつの解決策は、照明、ラジオ、あるいは多分医療器具などの基本的な電気器具に電力を供給する太陽光パネル、制限のある電力変換器や電池のような、既存のローカル電力技術に適応することである。しかし安全性はこれらの単純に見えるネットワークにおいても取り組みが残っている。電気ショックから保護することを確実にするために、電気設備の電圧はDC電力を使用した安全超低電圧(SELV)に制限される。これは農村地域に、本質的に安全で手ごろでもある直流低電圧（LVDC）の受電設備を構築することを可能にする。これはエネルギーのアクセスを確保し、不均衡を減らすことに好影響を与えてきている(図4-6)。IECが創設したシステム委員会SyC は、この目的達成のためLVDC[13] の標準化に関するガイダンスを提供している。さらに、熱的影響や火災の危険からの保護を確立するために、負荷や電気機器の総合的な値（ワットで計算する）にはまた限界がある。そのため、バッテリーの容量や配電ケーブル経由の電力供給は両者とも制限され、電気機器と電池間の絶縁距離が規定されている。逆説的に、そのような基本的な電力システムは

13 go.iec.ch/syclvdc

スマートフォンを充電するのに使用されるであろう。ソーシャルメディアが電話に装備される時、新規の電力ユーザーは常に、役に立つであろうがなかろうがAIにさらされる。

しかしながら、ネットワークはまた、LVDCシステムをいかにより安全にするかにおいて、ユーザーを誘導する装備やアプリを備えるであろう。そして多分、そんなシステムを他のアプリ経由でモニターするであろう。それに関してこの技術は、ハイテク労働環境に焦点をあてがちな三者連携システムより得られる利益はないように見えるが、真実から遠ざかることはない。ネットワークシステムの使用を通じ、新規の電力ユーザーは、これまで未知のベンダーあるいはクライアントと、及び可能性としてギグエコノミーともインターフェースを築くであろう。この例は、三者連携システムにおけるインターフェースの重要性、及びある程度、それらを機能させる人と機械の必要性をハイライトする。

4.8 標準化の意味するところ

このセクションでは、人が安全保護の取り組みが中心であることを示してきた。知的であるなしに関わらず、機械は製造、食品生産、配電と情報交換を促進するが、それは安全な方式で行わなければならない。ここで述べられる労働は、電気設備が使用可能などのような環境においても、AIに支援された安全機能を装備することが実現可能であることを示している。これにより、JTC 1 との協業において、デジタル安全システムにおけるAIの役割に関係するガイダンス開発ワーキンググループ、及び/または標準化活動を発足することに価値があるとするIECの見解を強化する。

このセクションでのもう一方の注目点として、電力に依存する各産業において多種の三者連携システムが存在するということである。技術標準はこれらすべての産業における発展を促進するために

当然開発されるべきものである。例えば、前述で示したように、LVDCテクノロジーの標準化が包括的なアプローチを求めることに応じ、IECがその課題に関するシステム委員会を構築してきている。SyC LVDCは 低圧直流の標準化におけるガイダンスを提供し、太陽光（PV）エネルギーシステム(TC 82)、電気設備の安全(TC 64)や、電気付属品(TC 23)を含むさまざまなIEC技術委員会からのインプットを盛り込んでいる。公共事業や電気システムのために、安全のためのAIシステム導入を導く新たな標準を設計するベースを潜在的に供給する既に利用可能な設計がたくさんある。同じことがネットワークされたシステムに当てはまる（特にワイヤレス）。一方農産業は、特にその必要性に関わる標準開発について考える必要があるだろう。

第 5 節

結論

5.1 人より賢い機械との労働

この白書は、社会のメガトレンド、技術革新、及び産業界の開発状況が我々の安全に対する理解を変えさせていることを明示している。この点で特に関連があるのは、ICTシステムが機械と職場にAIを導入していることである。今後10年にわたり投入されるそのような技術（量子コンピュータ、超高速ネットワーク、及びチップ化されたAI）の更なる改善により、人はもはやシステムの中で最も賢いコンポーネントではなくなるということを想定する必要があるかもしれない。このことは本白書が将来の安全に言及する背景とは相容れないことである。

5.2 人を最優先に

将来の標準は、人とシームレスに働き、かつ安全の定義が危険からの解放という心理的感覚を包含する技術システムを設計するため、単なる意図しない障害（致死に至るまで）を超えて進展することが推奨される。このことは、IEC、及びその他の標準化機関は、異なる技術委員会の専門家間のより明確な相互対応を要求する、及び/または社会的責任を代表し言及してくれる安全心理学者や社会学者の知見を求める等により、安全に関する水平連携を拡大し深化しなければならないであろうことを意味する。

同時に標準化機関は本来任務を果たす必要がある－将来の安全を確実にするため、機械の開発者、供給者、システムインテグレータに対する技術規格にフォーカスすることである。この意味で、もし人が連携したシステムにおいて最優先となるならば、設計による安全は最も賢明なアプローチを構成することになる。働く者の代表が安全に関わる標準開発に関与すべきであり、その標準は電気技術製品或いはシステムのライフサイクルの全てのステージを考慮したものであるべきである。

5.3 将来の安全確保のための挑戦は何であろう？

5.3.1 社会責任への信頼の柱

IECの源は明らかに、製造された電気技術システム、及びその安全性をカバーする技術規格開発にある。しかし知能が注入された機械の出現により関与する社会的責任の側面を無視することができなくなっている。同時に政府は、制限的な技術法規を目標志向の法規に置き換えることにより、安全保護規則（及び、その他の社会領域における規制戦略）への縛りを緩和している。この規制緩和されたフレームワークのもと、企業は安全に関する社会的責任を負うことによって規制緩和を補うことが期待されている。しかし標準化機関もまた、実践的な規格、及び適合性評価プロセスを通じて社会的責任を果たすための重要な役割を果たしている。標準化機関は、既に安全やセキュリティのような社会目的の達成に貢献するため社会の利害関係者と関係づけられており、産業界のドライバと政府規制当局の間のギャップの橋渡しを行うユニークな立場と位置付けられている。
SDGsのような野心的な社会目標の達成に貢献するため標準化努力への特別なフォーカスを超えて取り組むことは、IEC義務の範疇外とはいえない。

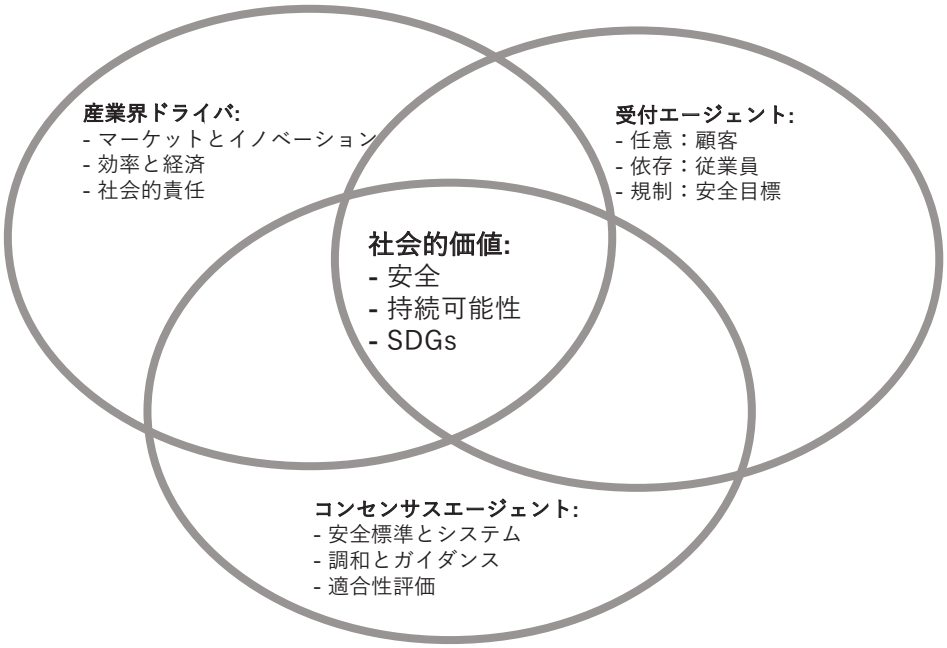


図5-1｜**社会の進歩を可能にするものとしての標準化団体**

図5-1は、変化のドライバと規制当局との間で信頼を形成する3番目の柱としてIECがそのポジションを位置づけるスキームを提案するものである。このフレームワークのもと、IEC、及びその他の標準化当局は、すでに実施している業務の重要性を減ずることなく社会的目標を達成するための国際合意ブローカーとして各々の立場を強固にする。安全は踏み台になる可能性があるものの、安全という次元はSDGsにおいて深く根付いているため、社会進歩を可能にするものとして幅広い役割を担う機会がある。

5.3.2　インテリジェントシステムのエコシステムに向けた標準化

安全に関わる三者連携モデルは将来の安全へのシステマチックなアプローチであり、この白書で種々の事例とともに提示されたコンセプトである。三者連携のアプローチは、職場、及びその他の領域における人、機械、及びインテリジェントなICTシステムの連携のもとでキーとなる関心事を明確にするのを可能にする。

システムの各種コンポーネント間の情報の流れは、安全かつ効率的な製造のキーを構成する。農業、ロボット化された製造工場、化学処理やロジスティックかどうかに関わらず、人のタスクやこれに伴う技術に係る固有の設計は変わりうるが、三者連携フレームワークのカギとなるエレメントはひとつまたはその他の様式で常に存在する。

三者連携システムは人とその労働環境を第一に据えているが、個々のフレームワークは高度なつながりを持つ世界に存在する。三者連携のエコシステムは、近接する職場同士やビジネス環境に相互接続性を供給するのみならず、財務や銀行システム、政府機関や法的フレームワーク、社会ネットワークや組合などにも拡大している。この複雑な相互接続性のウェブはシステムのエコシステムを創り上げる。これらエコシステム（AIに関するEU白書ではこの点を「信頼のエコシステム」と言及）に対する法的フレームワークは政府内、及びグローバルな組織内によく配備されている一方、そのような連携形態の技術上、及び運用上の詳細は、IEC、及びその他の標準化機関、

また安全方策を標準化する努力、連携したシステム、技術的な詳細、革新のフレームワーク、及び機密性の範囲内でより適切に含まれている。三者連携システムはこのような標準化に対する優れた出発点を提供するが、個々の標準もシステムのエコシステムにも同様に言及しなければならないであろう。

しかしICTシステムの印象深く時として圧倒的なインパクトにもかかわらず、現状、及び将来の安全確保に関わる人の質（例．価値、組織文化、リーダーシップ、委託事項、及び対人コミュニケーション）は容易にはデータシステムでは捉えられない。そのような要因は無視されるかもしれないという危険が存在する。したがって、安全に関する将来の規格開発は、社会的、及び組織的環境における非技術的要因に明確な注意を払うことが推奨される。ここで再び、性能規定化（仕様規定化とは逆の意味で）された規格が、特に標準化プロセスの出発点として最低限の安全要求を言及するにあたっては大いに役立つであろう。

5.4 インテリジェントな手段を用いた適合性評価

政府、企業、雇員、及び消費者は、レビューされる製品、プロセス、システム、設置、データ、設計、或いは要員の安全要素を確定するため、適合性評価の種々の側面に依存している。知的ICTシステムの導入は、新たなタイプの規格開発を必要とするようになってきており、これは一方で適合性評価における革新的な開発を呼び起こす。

第一に、知的システム、及びICTに対する規格導入とともに、適合性評価文書（例えば手順規則や運用文書）は、動きの速い技術的な環境下でのより迅速なオペレーションに言及する必要がある。

第二に、三者連携システムでカバーされる仕組みは、より早い、より効率的な決定プロセスによる迅速性をサポートし現状より格段に多い情報量を扱う組織へと進化している。更には、人はもはや適合性評価を行うことのできる唯一の知的な遂行者ではないかもしれない。機械読み取りのできる文書は、製品やシステムの進化とともに変更をリアルタイムで効力を発揮させるため、適合性評価がより迅速な評価の社会をサポートすることを可能にする。同様に試験方法は、多分デジタル化の可能な試験環境をコントロールするダウンロード可能な機械読み取り手順の様式による適合性評価の文書化とともに進化する必要がある。

デジタルツインは適合性評価をサポートする汎用性のある解決策に貢献する。それは既存の、及び/または将来の製品またはシステムの評価に対し、現実的なアプローチを提供する。その結果としてそれはまた、システムが構築され、運用され、変更され、廃棄される時のモニタリングのための原動力としての役割を果たす。デジタルツインは、システムが構築される前にシステムをシミュレートできるため、安全設計原則に従うことが推奨される。このことは、安全、及びその他の側面に対する適合性評価が事前に利害関係者と議論し検証しておくべきことを認めている。

ＡＩに基づく安全検証アルゴリズムを独立して運用する仕組みの導入とともに、人はもはや安全確保を担当するシステムにおいて唯一の知的な遂行者ではない。そたとえそのようなシステムが現状では幼少期であるとしても、適合性評価に与える最終的なインパクトを考慮しておく価値はある。この方向の開発は適合性評価目的の基礎的なシフト、及び新たな信頼性の様式を導入することになる。適合性評価に関する機械読み取り可能な文書は道途上であるが、ＩＥＣ、及びその利害関係者は、将来の安全を準備するにあたってそのようなシステムの予見可能性、意欲及び運用に関する調査を行う必要がある。

5.5 グローバルな安全優位性の達成に向けて

システム、規格、及び実践に関わる持続的改善に関するメカニズムを組み込むという観点から、さらに重要な要因が存在する。安全の結果の測定は、長年にわたり事故統計にフォーカスされて安全マネジメントシステムのキーとなる部分を形成していた。しかし、その計算に「先行」指標を導入することによって、より先を見据えた主導的なアプローチが採用できる。安全に関わるより完成された展望を得るため、管理される特定のシステムと同様に、安全エコシステムの各層が環境上の外部特性によって作用する影響を理解するために測定されるべきである。安全のシステムが有する複雑かつ多層的な性格は、その測定に対し新たなアプローチを求めている。複合的な指標、構成されたシステムの個々の対策の組み合わせを含めるということは、安全に適用され得るダイナミックな、繊細かつ採用しやすい測定手段を構成することである。

グローバルな安全優位性を達成するためには、グローバルな多様性が認められなければならない。多くの社会が人々のために安全でセキュアな環境を提供しようと努める一方、活用できる資源はいつもその努力に対して制限的な要素となる。国の一人あたりの国民総生産（ＧＤＰ）がその社会における利用可能な資源の一つの尺度となる。先進経済圏では、より「裁量権」のある資源が、特定の安全プログラム、例えばより安全なインフラづくり、消費者保護、及び類似の対策への割当てに潜在的に利用される。発展途上国では、財政的資源はあまり豊富でなく、政府支出は基本サービス、重要インフラ構築あるいは経済を形作る努力に対して割当てられがちである。ここれらの案件に言及することは、安全関連に特化して利用可能となる資源を少ないままにしておくが、基本的なサービスやインフラを強化することは、通常は安全に対する改善と相関性のあることである。

グローバルな安全優位性に向けて世界を操ることは大規模で、複雑で、多面的なチャレンジである一方、IECは、安全、エンジニアリング、システム構築、及びICT分野の専門家の調整役として長年にわたって培われた歴史とともに、利害関係者を一同に集めてコンセンサスを導く特別な存在となっている。最終的にはそれは、将来の安全を確保する努力によって成功を可能にするポリシーメーカー、規制当局、産業界、保険業界、学識経験者、及びプライベートな研究組織の間で確立したパートナーシップであろう。

第 6 節

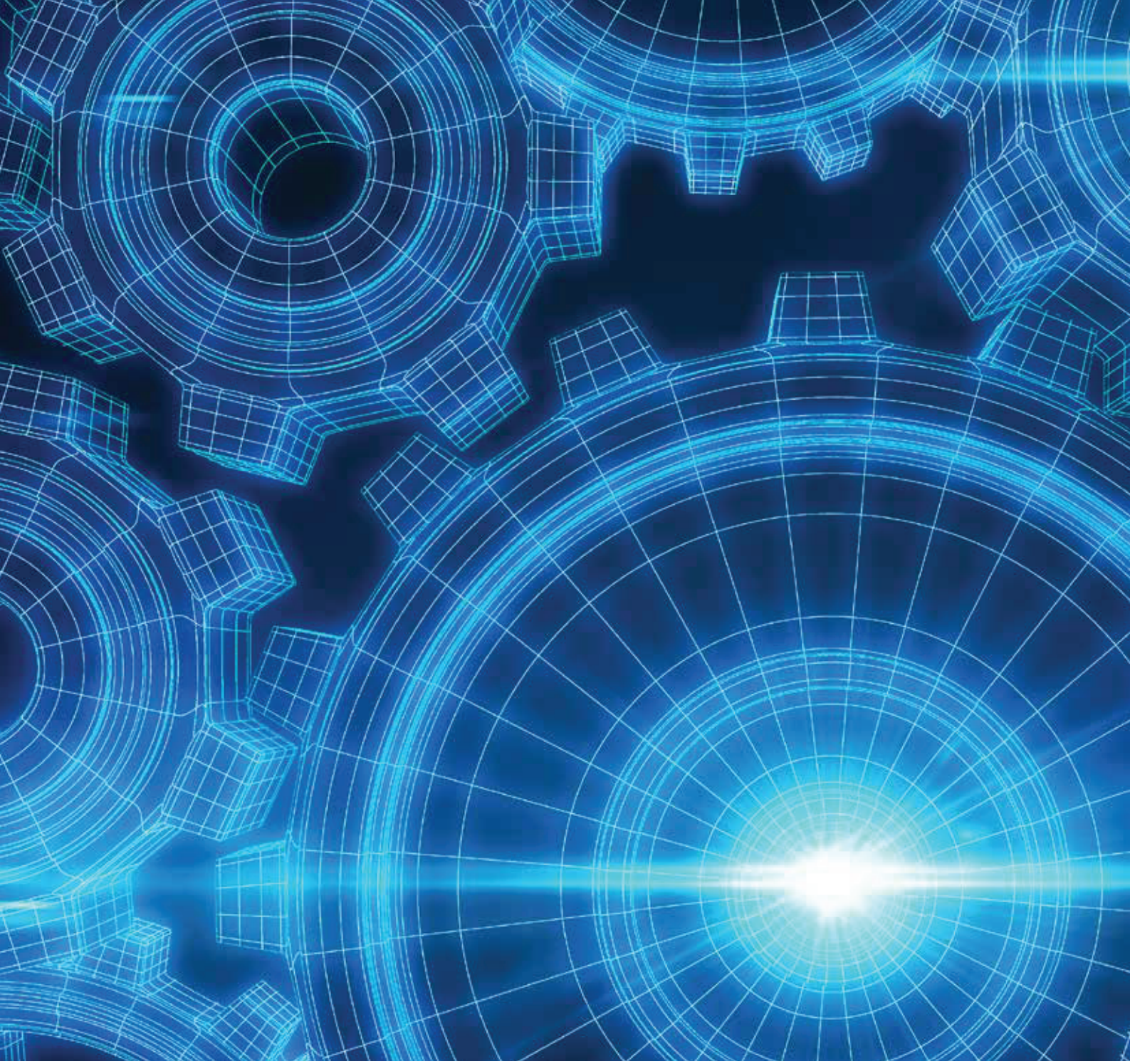
勧告

6.1 政府規制当局、産業界のドライバ、及び標準化機関への勧告

- **規制当局**
  - 政府、及び規制当局は、制限的な安全法令から目標志向の法令への必要なシフトに関し、議論を活性化すべきである。
  - 人と機械の分離に基づく安全モデルから、安全が人と機械の協調を通じて実現できるモデルへとシフトすることによって、安全と効率化の両方が実現できることを目指す社会的ゴールを確立すべきである。
- **産業界ドライバ**
  - 産業界のプロモータは、人とシステム間のコミュニケーションが将来の全てのシステムにおいて不可欠な成分であると認識すべきであり、安全、及びセキュリティを確実にする技術開発を促進すべきである。
  - 新たな人と機械の協調システムにおいて人はもはやもっとも知的なコンポーネントではなくなるという可能性に配慮が必要である。安全の新たな概念は、技術開発、及びシステムにおける人の位置の再構成を通じて考慮されるべきである。
- **標準化機関**
  - 標準化機関は、安全に関する彼らの包括的アプローチを拡大し、深化させる必要がある。このことは過去からの技術的な知見のみならず、安全心理学、社会学、及び人間行動の分野で収集された見識も盛り込むことを求めている。言い換えれば、将来の安全規格開発にあたっては、非技術的なファクターにも明確な注意が払われるべきことが推奨される。
  - 同時に、機械開発者、供給者、及びシステムインテグレータが将来セキュリティ努力を支えることを確実にするため、技術規格の推敲にフォーカスすることは標準化機関の義務である。この努力に対する前提条件は、もし人が協調システムの中で最優先と考えられるならば、設計による安全確保は最も賢明なアプローチであるとの理解である。規格は製品やシステムのライフサイクルにおけるすべてのステージが考慮されるべきである。
  - 標準化機関は、実践的な規格、及び適合性評価プロセスにおいて社会的責任を促進するという重要な役割を果たしている。標準化機関は既に、安全やセキュリティといった社会目標の実現に貢献するという点において社会の利害関係者と関わりを持っており、産業界のプロモータとその受容者の間のギャップの橋渡しとしてユニークな位置づけとなっている。

6.2 IECコミュニティへの勧告

- **標準管理委員会(SMB)**
  - IECにおいて、標準化評価グループ（SEG）の機能のひとつが、機能改善のためのTC/SC構造に対しその定義づけと強化策を実施するとともにシステムアプローチを求める新たな市場や技術を予測することである。SMBは、ガイドラインのレビュー、新たな規格審議組織の発足、、及び人－機械の協調安全を達成するために必要な既存規格の修正、及び維持管理等につき議論を開始するため、「将来の安全」に関するSEGを発足することが推奨される。この議論については、SEGメンバーはIECコミュニティの内外から選別されるため、安全諮問委員会（ACOS）にリードされることが望ましいであろう。効率的な規格開発に向けた第一段階としてこの委員会に寄与してもらうため、その他の標準化機関からのリエゾンを招聘することが推奨される。
  - ACOSは（ISOと連携して）、協調安全を達成する周辺技術開発が予測していたより早く加速するかもしれないため、現在審議中の安全に関するガイドライン（ISO/IEC Guide 51）のレビューを加速するべきである。
  - この白書で参照される将来の安全に関する規格開発は、既存の技術委員会に頼るよりもむしろ新たな技術委員会の設立が求められるかもしれない。新たな技術委員会の設立というオプションを避けることなくとも、SMBは既存の技術委員会との役割分担に関し、十分かつ迅速な議論を実施すべきである。
- **適合性評価評議会（CAB）**
  - CAB、及びその傘下のCAシステム（IECEE、IECEx、IECQ、IECRE）は、SMBのもとで包括的アプローチに従って開発された規格に基づく三者連携安全システムに関し、新たな適合性評価・ービスを開発することが推奨される。三者連携安全システムの適合性は下記を含むが、これらに限るものではない：
    - 既存の安全規格に従う製品/機械安全
    - ICTの相互動作性能を含む、統合されたシステムレベルとしての協調安全
    - セーフティアセッサ、監督者、及びそのマネジントスタッフの要員力量
  - CABは国家当局や規制組織に、IECに登録された機関によって実施されたIEC適合性評価結果のグローバルな受入れを実現する動機づけを与えるため、ILO/ISSAとのコミュニケーションチャンネルを確立することが推奨される。
- **市場戦略評議会（MSB）**
  - MSBは社会、市場、及び技術トレンドを継続して調査すべきであり、安全に直接関係すると思われるいかなる顕著な変化に関しても、SMB、及びCABにインプットすべきである。必要に応じ、この白書がレビューされるべきである。
  - MSBはまた、安全事項に関する知見をシステマチックにシェアできるう、SMB、及びCABとの直接的な連携を行う恒常的なスキームを確立すべきである。



ISBN 978-2-8322-8870-2

CHF 50.-

International Electrotechnical Commission

国際電気標準会議

3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
info@iec.ch
www.iec.ch

IEC WP Safety in the future:2020-10(en)