資料５－別添１１

（提案１２）

（案）

報　告

工学システムに対する社会の安全目標

平成２６年（２０１４年）　月　日

日　本　学　術　会　議

総合工学委員会

工学システムに関する安全・安心・リスク検討分科会

この報告は、日本学術会議総合工学委員会工学システムに関する安全・安心・リスク検討分科会が、安全目標のガイドライン検討小委員会の審議を反映して取りまとめ、公表するものである。

日本学術会議総合工学委員会
工学システムに関する安全･安心･リスク検討分科会

委員長	松岡　猛	（第三部会員）	宇都宮大学非常勤講師
副委員長	永井　正夫	（連携会員）	一般財団法人日本自動車研究所所長
幹　事	水野　毅	（連携会員）	埼玉大学大学院理工学研究科教授
幹　事	須田　義大	（連携会員）	東京大学生産技術研究所教授
	萩原　一郎	（第三部会員）	明治大学研究・知財戦略機構特任教授
	桑野　園子	（連携会員）	大阪大学名誉教授
	小林　敏雄	（連携会員）	東京大学名誉教授
	坂井　修一	（連携会員）	東京大学大学院情報理工学系研究科研究科長
	高橋　幸雄	（連携会員）	東京工業大学名誉教授
	長谷見　雄二	（連携会員）	早稲田大学理工学術院教授
	松尾　亜紀子	（連携会員）	慶應義塾大学理工学部教授
	向殿　政男	（連携会員）	明治大学名誉教授
	矢川　元基	（連携会員）	公益財団法人原子力安全研究協会理事長
	成合　英樹	（特任連携会員）	筑波大学名誉教授
	水野　光一	（特任連携会員）	独立行政法人産業技術総合研究所環境管理技術研究部門研究顧問

以下の方々にご協力をいただきました。

梅津準士		元食品安全委員会事務局長
河津　司		消費者庁企画調整担当審議官
笹倉　宏紀		慶應義塾大学大学院法務研究科准教授
高田　広章	（連携会員）	名古屋大学大学院情報科学研究科教授
中村　昌允		東京工業大学大学院イノベーションマネジメント研究科客員教授
野口　和彦		横浜国立大学環境情報研究院教授

安全目標のガイドライン検討小委員会

委員長	成合　英樹	（特任連携会員）	筑波大学名誉教授
幹事	長谷見　雄二	（連携会員）	早稲田大学理工学術院教授
	松岡　猛	（第三部会員）	宇都宮大学非常勤講師
	坂井　修一	（連携会員）	東京大学大学院情報理工学系研究科研究科長
	須田　義大	（連携会員）	東京大学生産技術研究所教授
	永井　正夫	（連携会員）	一般財団法人日本自動車研究所所長
	向殿　政男	（連携会員）	明治大学名誉教授
	梅崎　重夫		独立行政法人労働安全衛生総合研究所 機械システム安全研究グループ部長
	田村　兼吉		独立行政法人海上技術安全研究所研究統括主幹
	中村　昌允		東京工業大学大学院イノベーションマネジメント研究科客員教授
	野口　和彦		横浜国立大学環境情報研究院教授

以下の方にご協力をいただきました。

	梶本　光廣	原子力規制庁技術基盤グループ安全技術管理官

本件の作成に当たっては、以下の職員が事務を担当した。

事務	盛田　謙二	参事官（審議第二担当）
	齋田　豊	参事官（審議第二担当）付参事官補佐(平成 26 年 8 月まで)
	松宮　志麻	参事官（審議第二担当）付参事官補佐(平成 26 年 8 月から)
	沖山　清観	参事官（審議第二担当）付専門職（平成 26 年 6 月まで）
	菊地　隆一	参事官（審議第二担当）付専門職（平成 26 年 7 月まで）
	熊谷　鷹佑	参事官（審議第二担当）付専門職付（平成 26 年 7 月から）

要　　旨

１　作成の背景

工学システムは、その時々の社会が求める最適な価値を提供するものである。一方、工学システムは、高度化するにしたがい、その安全の確保が社会の重要な要求となってきて、安全に関する考え方やその目標のあり方を定める必要が出てきた。

安全の目標は、それぞれの立場ごとに設定したのでは、社会としての整合性が取れなくなる。本報告では安全目標は時代と共に変化するという認識に立ち、現代社会において実現すべき安全目標のあり方を取りまとめた。

２　安全目標の基本的な考え方

本報告における安全の定義は、「受容できないリスクがないこと」(ISO/IECGuide51の定義）を採用した。

安全目標の対象となる事項としては、生命、心身の健康、財産、環境、に加え、情報（喪失、漏洩)、経済、物理的被害、社会的混乱等とした。

本報告における、基本的考え方は、以下のとおりである。

①安全目標は、技術的かつ経済的に実現可能なものでなくてはならない。

②安全目標の設定においては、経験した事故の再発防止はもちろんのこととして、未然防止の考え方を重視する。

③安全目標は、人命に加え、社会リスクの観点も考慮に入れて対象のシステムの稼働・不稼働がもたらす人・社会・環境への多様なリスクを勘案して決定すべきものである。

④製造者、運用者と利用者の責任をバランスよく考える必要がある。

３　報告の内容

（１）安全目標の設定

安全目標としては、人命を対象とした目標では、達成できない場合は許容されない基準値（A）と更なる改善を必要としない基準値（B）を設定する。基準値（A）と基準値(B）の間は、リスクを総合的に判断して対応を定めることになる。

社会的リスクを安全目標の対象とする場合は、工学システムの事故の発生確率の低減と事故が発生した際の被害軽減対策により、最新状況で設定される安全目標より、対象とする工学システムの影響を小さくすることを求める。

（２）工学システム安全に対する要求事項

工学システムの安全を評価する際のリスク算定に対する要求や評価の役割分担等に関して取りまとめた。

目　　次

１　はじめに

日本学術会議では長年、工学システムに関する安全工学の立場からの検討、安全工学シンポジウムを主催しての学協会横断での情報交換、学術会議からの発信等と安全に関する活動を幅広く行ってきている。

第17 期の日本学術会議では､安全に関する特別委員会を設置し｢安全学の構築に向けて」を報告している[1]｡その後､第18 期 ヒューマン･セキュリティの構築特別委員会から｢安全で安心なヒューマン・ ライフへの道」を[２]、第19 期特別委員会から「安全で安心な世界と社会の構築に向けてー安全と安心をつなぐ」の報告が出されている[３]。また、人間と工学研究連絡委員会安全工学専門委員会では、第19 期において「安全・安心な社会構築への安全工学の果たすべき役割」[４]および｢事故調査体制の在り方に関する提言」[５]の公表を行った。

工学システムの安全･安心・リスク検討分科会が前々期の第20期より設置され､我々の生活の利便性向上のために取り入れている各種工学システムの安全とリスク、そしてそれが我々にとり安心できる状況であるか、という点を念頭に議論を進めた。その過程では安全目標に関しても関心が高く深い議論が持たれた。分科会の議論に基づいた総合的な報告が学術の動向平成21年９月号に特集として載せられている［６］。この報告は分科会での多様な議論が内容となっているが、その中の「安全目標ーリスクと安全・社会の安心ー」の記事には各分野での安全目標の考え方の概要が記されている。なお、第20期において分科会の下に「事故死傷者ゼロを目指すための科学的アプローチ検討小委員会」が設置され、道路交通の特殊性が議論され､提言｢交通事故ゼロの社会を目指して」の公表を行った[７]。

第22期において、安全目標をさらに深く検討するため、新たに分科会内に「安全目標のガイドライン検討小委員会」を設置し、広く工学システムの各分野を比較しつつ、安全目標の考え方を検討してきている。そこでは、安全目標について工学システム全体を通して考えた時、どのような考え方で整理すればよいかを中心に議論した。

本委員会では、工学システムに対する社会の安全目標を、対象とする安全の概念とその目標とするレベルと同時にその達成のための工学システムに対する要求事項としてまとめた。

今回、これらの安全目標達成のための基本的な考え方をガイドラインとしてまとめたので、その考えを広く社会に発信し関連各分野における安全目標決定の参考資料として活用されることを期待する。

２　安全目標設定の目的

企業等組織は、その組織目的の達成を目指しつつ、社会や生活の向上に貢献してきた。その活動の中で、多くの工学システムが開発・運用され、多くの成果を創出してきたし、その発達はこれからも必要不可欠なものである。

しかし、科学技術の発展は、工学システムの機能の向上をもたらすとともに、望ましくない大きな影響をもたらすリスクも増加させてきた。

この工学システムの持つ負の影響をもたらすリスクやリスクの顕在化を抑制するために、工学システムの安全に関わる多くの研究開発がなされてきた。また、社会的には、安全規制に関する検討も進み､工学システムの開発･運用に関する安全向上に寄与してきた。

しかし、工学システムが高度になるにつれ、安全の向上に関する検討は、再発防止という経験に基づく対応に加え、経験の無い事故をも防ぐ未然防止策を向上させることが重要となってきた。

これまで、工学システムの開発・運用における主たる検証対象であった規制は、社会・生産活動の多様性の中で必要条件として提示され、またその性格上被害の発生が明らかになったことに対して重点的に検討・作成されることが多かった。したがって、巨大な被害をもたらす事故を未然に防ぐためには、工学システムの開発・運用者は、規制を順守する一方、新たな科学技術社会の創造にふさわしい安全目標を掲げ、工学システムの安全性を高めていく必要がある。

さらに、現代社会においては、安全を考える際の対象は人的影響にとどまらず、社会的影響も考慮することが重要となってきた。

本安全目標は、工学システムが社会生活の豊かさに寄与するため、工学システムの開発者、運用者のそれぞれが、工学システムの持つリスクに対して、規制の範囲にとどまらずその安全性を追求していくことを支援するガイドラインとして作成したものである。

またこの安全目標の考え方は、日本社会に対する限定的なものではなく広く世界で共有できるものであり、今後の科学技術社会における安全の考え方として日本から発信を行いたい。

（１）　基本的な考え方

工学システムは、その時々の社会が求める価値を提供するものであることが望ましい。工学システムが担保すべき安全目標も、その社会が要求する安全を担保することが大前提である。そのため、工学システムも社会の要求を満足した上でどこまで安全であるべきかということは、他のリスクとの兼ね合いの中で決定されるものである。

工学システムは､その時代の科学技術水準の最善を尽くし種々の安全対策をとっても、それが社会に与える負の影響のリスクをゼロにすることはできない。あるリスク対策をとっても別のリスクを派生させるということもある。したがって、工学システムにおける安全目標は､「リスクをゼロにする」という理想を掲げるだけでは現実的な目標にな

りえず、科学的合理性に基づき決定することにより、具体的な安全の向上を図るべきである。

以上のことを鑑みると、安全目標としてリスクの考え方を採用することが有効であると考える。

本報告で提言する安全目標策定に関する前提は以下の通りである。

① 安全目標は時代と共に変化するという認識に立ち、理想的な社会状況を目指した理念的なものではなく、現代社会において実現が可能なものとする。なお、実現可能ということは、現状追認ではなく、今後の努力により技術的にも経済的にも達成可能なものという意味である。

② 安全目標の設定においては、経験した事故の再発防止はもちろんのこととして、未然防止の考え方を重視する。ここでいう未然防止とは、発生の防止のみならず事象が拡大して避けたい影響に及ぶことを防ぐ概念も含まれる。

③ 安全目標は、人命に加え、社会リスクの観点も考慮に入れて対象のシステムの稼働・不稼働がもたらす人・社会・環境への多様なリスクを勘案して決定すべきものである。ここでいう多様なリスクの勘案とは、多様な価値観が存在する状況下で許容できるリスクのバランスのあり方を考え、社会的合意を得るための概念である。以下ではこの概念を最適化という言葉で表すことがある。ただしここでいう最適化とは、特定の最適化方程式で解を一意的に定めるという意味ではなく、あくまで上で述べた多様なリスクの特徴を勘案し、そのバランスをとることをいう。

④ 本安全目標は、各工学システムの特徴を検証しつつ、工学システム全体を包括するものとする。

⑤ 製造者、運用者と利用者の責任をバランスよく考える必要がある。

（２） 用語の定義

ここでは、本報告における以降の説明が不確定・あいまいなものとならないようにするため、使用する用語を定義する。

・ハザード：人的あるいは物的損失を引き起こす事故の潜在力。安全分野においては、危険な事象を指すこともある。

・リスク：人間の生命や経済活動にとって望ましくない事象の不確実さの程度およびその結果の大きさの程度の組み合わせ（Guide51.の定義）[1]。リスクの事例としては、死亡リスク、傷害リスク、環境リスク、経済損失リスクがある。

・許容可能なリスク（tolerable risk）：社会における現時点での評価に基づいた状況下で受け入れられるリスク（JIS Z 8051 の定義）[1]。

・安全：本文中４．（１）で説明。

---

[1] ISO/IEC ガイド 51 によるリスクの定義「人間の生命や経済活動にとって望ましくない事象の不確実さの程度およびその結果の大きさの程度の組み合わせ」。ISO/IEC ガイド 51 に対する JIS である JIS Z 8051 の表現では許容可能なリスク（tolerable risk）は「社会における現時点での評価に基づいた状況下で受け入れられるリスク」となっている。

・危険：安全が損なわれそうな状態。
・安心：安全であり、かつ安全であることが信じられること。（または、規制や事業者が信頼できている状況。）
・便益：有用性の評価値。あるシステムを導入した場合のリスク減少量も便益に加えて考える。
・安全目標：現状のレベルと比較でき、その許容レベルを定めるもの。ステークホルダーを考慮に入れた実現可能な目標。
・工学システム：多数の要素が有機的に結合し、全体として特定の機能をもつもの。本報告では、プロセス、製品を含めて検討する。
・科学的合理性：わかっていることとわからないことを明確に示して考えること。
・社会的公平性：特定の地域・集団・個人だけが大きなリスクを負わないようにすること。ただし、リスクの影響を他の施策により代替することは、社会的に許容される。

３　各工学システムにおける安全検討の対象

工学システムは、その規模・種類等によって検討すべき安全の対象が異なる。工学システムの安全目標は、その工学システムの特徴を踏まえ検討することが望ましい。
主な工学システムと安全検討の対象を表１に示す。

表１　検討した工学システムと主な安全検討の対象

検討対象工学システム	主な安全検討の対象
原子力システム	環境影響　人的影響　エネルギーへの影響
(化学)プラントシステム	地域環境、人的影響　経済的影響
情報システム	社会的影響　産業的影響　企業被害　個人情報
交通システム（輸送体 OR システム）	利用者の安全　社会的影響　経済的影響
物流システム	環境影響　経済的影響
製品・製造物	人的影響　環境影響
産業機械	人的影響　機能喪失・誤作動
土木・建築物	人的影響　社会安全

また、本報告では、工学システムがもたらす安全問題として各分野に共通して重要な労働安全分野に関しても、検討を行っている。(AP９参照)

４　安全目標設定の検討

工学システムに関する社会の安全目標の構築を検討するに際して、各種工学システムの安全に関する実態を調査し整理を行った[AP２～10 参照]。安全目標値を提案しているところ、国の定めた規制値、基準値に従っているところ、明確な目標値を持たないところ等、分野による違いは大きいことが判明したが、それぞれの分野の特徴を捉えたものとなっており、この安全目標の構築には、有効な検討資料となっている。

（１）対象とする安全の概要

①安全の定義

本検討では安全の定義として、「受容できないリスクがないこと」（ISO/IECGuide51 の定義）[1]を念頭において議論を行った。この定義によれば、安全目標は受容できるリスクを明らかにすることではなく、基本的には受容できないリスクを明らかにすることとなる。さらに、この定義により安全か否かを議論するためには、受容する状況を社会として合意する必要がある。

②安全目標の対象となる事項

生命、心身の健康（短期、長期の健康被害・傷害・障害の視点も重要）、財産、環境、情報（喪失、漏洩）、経済、物理的被害、社会的混乱、等

③安全を検討する際の事故・災害のハザード[2]

自然現象、人的要因、機械的要因、化学的要因、システム的要因

④安全を向上するための施策[3]

未然防止、拡大防止、回復力の向上　等

（２）安全目標の要件

①目標は、達成可能なものでなくてはならない。

・目標は、特定の活動だけを利するものであってはならず、社会的公平性を前提とするものであること。

・目標は、達成可能なものでなくてはならないが、単なる現状追認であってはならない。

・目標は、何時までに実現するかを明確にすることにより具体性のある達成計画を作成し実行することがが望ましいため、マイルストーンを明確にして、達成時期を明示する。

②目標は、社会や技術の状況によって変わるものである。

・目標は、対象・被害形態・影響の大きさ、得られる便益の大小、経済的実現性、選択肢の有無等によって変わることを前提とする。

2　特定のハザードやイニシャルイベントに基づくリスクは、そのシステムのリスクの全てを表すものではない。

3　施策には、発生確率の低下と影響の低下の二つの事項に関する検討がある。

・目標と比較される各工学システムの安全の指標は、そのシステムの過去の実績にとどまらず、環境等の変化、潜在するリスクも考慮した将来の状況も含んだものである必要がある[4]。

③目標の作成プロセスは、透明性・合理性がなくてはならない。

・科学的根拠に立脚し、検証が可能であるものでなくてはならない。

・多くの人にとり、解釈が容易で明確であるものとする。

④目標は、各自の施策に反映できるものでなくてはならない。

・工学システムとしての製造から廃棄までの間を通じての安全目標が必要である。

・供給者・管理者として、施策に反映できるものであること。

・一市民の立場からの安全の判断にとっても、有意義でなくてはならない。

⑤目標は、人々に希望をもたらすものでなくてはならない。

・将来の制度改定、技術開発、意識改革につながるものであること。

（３）安全目標の概念

安全目標を検討した結果､「対象とする工学システムが如何に社会に対して有効な機能を有していても安全の確保のために最低限満足すべき要求」であるものと「満足すれば無条件で許容できると考えられるすなわち更なる改善を必要としない」ものの二種類があるとの結論に至った。前者が基準値（A）であり、後者が基準値（B）である。（AP１参照）

基準値（A）を満足できない工学システムは、如何に社会に有用な機能をもたらしても稼働ができないことになる基準であるため、現状社会から受けいれられている工学システムの存在も念頭に置いて決める必要がある。一方、基準値（B）は、他の条件を与えずに多くの人々がその受入れを合意すべき水準であるので、より高いレベルでの事故防止が科せられるものである。

この目標の達成に関しては、工学システムの事故を未然に防いだり、事故影響の拡大を防いだりすることに加えて、避難等の対策によって対象とする被害を目標以内に抑えることも含まれる。（AP２－１参照）

① 人命を対象とした目標

人命を対象とした目標といっても、全ての状況を同一基準で考えられるわけではない。

まず､その事故が､多くの人に関するものか､不特定な個人に関するものかによって、目標の考え方は異なる。さらに、１回の事故が影響を与える人数によっても、前述の指摘と同様に、安全目標の設定の仕方は異なる。

影響が不特定の個人に与える工学システムに関しては、個人の死亡リスクの観点から、無条件で許容できるもの（基準値（B））は、そのシステムの事故による個人の生涯死亡

4　統計的なリスクは、それまでのシステム状況を示している指標の一つで、システムの環境の変化まで取り込んだ、未来の指標としては十分とは言えない。

リスクを 10^{-5}／生涯～10^{-6}／生涯以下であるものを当面の目標とする。基準値（A）としては、少なくとも 10^{-3}／年～10^{-4}／年にすることが望ましい。（AP１参照）

基準値（B）を検討するにあたり、1986 年に出された米国政府の安全目標政策声明を参考にした。そこには、「原子力発電所近くの公衆の受ける原子炉事故による個人リスク及び公衆のリスクはいずれも原子力発電所以外の他の事故によるリスクの 0.1%を超えないこと」という数値的提案がある。私たちが通常さらされているリスクの 0.1%の増加はほぼ無条件に受け入れられるであろうという考えである。この数値基準は IAEA 等国際的にも踏襲されて現在でもそれをベースにした議論となっている。

基準値（A）もこの 0.1%の基準を考慮して検討したが、この基準レベルを採用している例として、船舶の安全に関してより合理的なルール制定方法としてリスク評価の考え方に基づいた FSA（Formal Safety Assessment）で定められている乗務員と乗客の ALARP（As Low as Reasonably Practicable：合理的に実行可能な限り低くするという原則）領域の上限基準である 10^{-3}／年と 10^{-4}／年がある。（表 AP７－２参照）

工学システムにおいて、対象となるシステムの使用を止めても、そのことによるリスクが発生しない場合は、ゼロリスクの達成が可能である。特定の工学システムのリスクをゼロとする場合として、ある工学システムの使用を止めることにより失われる便益が社会的に許容できるものであれば、社会は使用停止の判断をする場合もある。

代替システムを導入する場合は、当然ながら代替システム導入の場合のリスクとシステムを停止した場合のリスクを比較して判断することとなる。

さらに、ここでは死亡リスクをとりあげたが、障害の重度等に応じた目標も別に定める必要がある。

また、安全目標とリスクを比較する工学システムの単位は、対象とする工学システムや安全目標の対象とする事故によっても異なる。例えば、化学プラント等の施設を主体とした工学システムは、1 事業所単位で考えるものであるが、自動車の交通システムのように、社会において多くの輸送体がシステムとして機能しているものや情報システムのようにネットワークとして考慮すべきものは、そのシステムの特徴を踏まえて判断するものとする。

② 社会的リスクに対する目標

社会的な影響（人的な影響も含む）が大きくなる工学システムに関しては、工学システムの対象となる事故の発生確率と事故が発生した際の被害軽減対策により、被害を提案する安全目標より小さくすることを求める。

事故が発生した際の被害軽減対策の実効性が検証できない場合は、事故の発生自体を目標以内に抑えることを求める。（参照：AP３－２）なお、事故の発生の影響等の算定に際しては、５章の工学システム安全に対する要求事項を参照されたい。

ア　経済的影響が大きいリスクに対する安全目標の考え方

ここでは社会基盤への影響の大きなリスク（例：巨大施設の過酷事故や情報システムの大規模な社会的影響等）を対象として安全目標を考える。またこの目標の対象には、１回の事故の影響が限定的でも、その発生頻度が多大になることにより、社会に大きな影響をもたらす工学システムの事故等も含む。

(ア)事故が大きな影響をもたらす場合

１回の事故の影響が甚大な場合－－－リスクはなるべく取りたくないという考えからより厳しい発生確率を設定すべきである[5]。

事故発生の頻度が多い場合－－－利便性との関係で国民の合意を得ることが望ましい。

(イ)そのシステムや製品の存在をなくすことが社会的に大きな影響をもたらす場合

得られる環境の範囲でその工学システムが提供する機能の全体リスク最適化の視点で判断をする。

イ 環境的影響が大きいリスクに対する安全目標の考え方

（ア） 回復可能な場合の基準値(A)----------＞ 10^{-4}/（年・事業所＊）（表 AP２－１、AP３－１参照）

回復が可能であっても、環境に大きな影響を与える事故は、社会に大きな影響を及ぼすため、人命に関する基準値（A）と同等以上の厳しい要件が必要となる。またこの値は、原子力発電所の既存炉の炉心損傷頻度 CDF に関する目標値である 10^{-4}/年と同程度の値である。

（イ）回復不可能（次の世代に影響を残さない期間：例 30 年一世代では回復が不可能）な場合の基準値(A)-------＞10^{-6}/（年・事業所）

この基準値は、原子力発電所の新設炉の炉心損傷頻度 CDF に関する目標値である 10^{-6}/年の考え方も参考とした。この事象に関しては、発生確率の低下だけでなく、事故が発生した場合の人身への影響の緩和策も検討する必要がある[6]。

ウ 物理的被害の規模の大きいリスクに対する安全目標の考え方

(ア)原因となるハザードの除去が別の大きなリスクを含まない場合

ハザードの除去を目標とすべきである。別の大きなリスクとは、ハザードの除去や代替手段が、社会や生活に対して大きな影響をもたらすリスクである[7]。

---

5 リスクアバージョンの考えからより厳しい発生確率を設定すべきという考えは、IMO の提案の目標値に見られる。1 回で多数の死者が出る事故ほど許容し難くなるという観点を反映するものとして FN（Frequency - Number of Fatality）線図（人命損失数とある数以上の人命損失が発生する事故の発生頻度をグラフ化したもの）を用いて分析を行う方法を使用している。英国 HSE（Health and safety executive）も定量的リスク解析結果を FN 線図上で社会リスクの最大許容可能限界と比較して議論している。

6 時間的や空間的に環境的影響が大きいリスクに対する安全目標の考え方。発生確率の低下だけでなく、事故が発生した場合の人身への影響の緩和策の例としては自動車のエアバッグ等がある。

7 温暖化防止のためのフロン使用停止はオゾン層破壊を防ぐという観点から代替手段が講じられた。その時点では、社会や生活に対して大きな影響をもたらさないと考えられたので可能となった。一方、カードの不正使用、口座への不正アクセスを防止するため、カードシステムを停止することは社会的影響が大であるので現状では不可能とも考えられる。

(イ)技術的・経済的に事前の対応が可能な事象

被害の拡大を防ぐために必要な対策を実施する。この対策には、影響が敷地外に影響を及ぼさないことといった影響の限定化も含まれる[8]。(AP３－１参照)

ただし、影響の限定化に対しては、その実効性があることを検証する必要がある。

(ウ)ハザードや対象システム･物質･プロセス等の排除が、別の大きなリスクを伴う場合

対象システム等の排除が不可能であるため、対策により対応せざるを得ないので、可能性のあるリスクを総合的に評価し、社会・生活にとって最適な対策を講じることが望ましい。最適な対策とは、科学的合理性に基づき、社会の合意により決定されるものである。具体的には、対策の実施または実施しないことによる多様な視点からのリスクを明らかにして、判断を行うこととなる。リスクは、その影響の種類が異なるため、数値的に一意にその最適性が定まるものではなく、その時点での社会の価値観やニーズを反映して定めることになる[9]。

③ リスクの許容を判定する際に注意する観点

ア　対象の製品・プロセスから恩恵を受けないステークホルダーのリスクにも注意する

イ　リスクの低減対策は、技術の可能性、対策の費用対効果を勘案して行う

ウ　壊滅的な被害をもたらす影響を避けることは、経済的合理性に優先する

エ　リスクの算定結果が、評価に耐える品質レベルになければ、評価に使用してはいけない

オ　リスクの低減対策は、その対策効果を明らかにする必要がある

8　施設において火災報知器の設置を義務化する、スプリンクラーを備える。また、船舶において乗客全員が乗ることができる救命ボートを設置する　等はこの事例にあたる。

9 DDT は食物連鎖を通じて生物濃縮されることがわかり、環境への懸念から先進国を中心に多数の国で使用が禁止・制限されている。しかし、マラリア原虫を媒介するハマダラカ防除には DDT に取って代わる有効な薬剤がない。スリランカを例にとると、1964 年に DDT の使用禁止措置を行った結果、それまで年間 31 人にまで激減していた患者数が、年間 250 万人に逆戻りしてしまった。現在、WHO はマラリア防止に DDT 使用を推奨している。

５　工学システム安全に対する要求事項

（１）　工学システムの開発・運営者は、開発時においてその安全に関する検討範囲（影響の種類、原因の範囲等）、その目標とするレベル（安全目標）を明らかにして、運営時にはその安全レベルを最新の情報の下に検証した状況を公開する。

（２）　社会に大きな影響をもたらすリスクを持つ工学システムは、経験した事故の再発防止はもちろんのこととして、未然防止の考え方を重視すべきである。ここでいう未然防止とは、発生の防止のみならず事象が拡大して被害が甚大になることを防ぐ概念も含まれる。

（３）　安全目標は、対象システム等やリスクの特徴を反映したものであり、人命に加え、社会リスクの最適化の観点も考慮に入れて対象のシステムの稼働・不稼働がもたらす人・社会・環境に影響を与える多様なリスク（ポジティブ、ネガティブな双方の可能性）を勘案して決定することが望ましい。

・安全目標は、対象としたシステム等の安全をそのリスク(発生確率と影響の組み合わせ)により受容できるか否かを定めるリスク論的目標設定と防ぐべき事故を定めその受容要件として設定した外力や負荷に足して構造等の健全性を担保することや付属すべき機器等の具体的要件を定めた決定論的目標設定の双方があり得る。

・リスク論的目標設定においては、社会に重大な影響を与えるリスクに関しては、回復可能な場合の基準値(A)は、10^{-4}/（年・事業所）以下、回復不可能（一定期間：30年一世代では不可能）な場合の基準値(A)は、10^{-6}/（年・事業所）以下であることが望ましい。(AP２－２、AP３－１参照)

ただし、この基準値は、工学的視点だけからは定めることができず、その社会の現在の状況や目指す社会状況によっても変化するものである。

（４）　対象となる工学システムの現状リスクの算定に際しては、以下のことを踏まえることが望ましい。

①経験した災害・事故・トラブルに限定することなく、可能性を洗い出すように努めること。

②安全性評価にとどまらず、どこまでいけば危険かという危険性を評価し限界を見極めること。

③対象とする製品・システムに関しては、製造から廃棄までのリスクを総合的に評価すること

④設備・部材・製品の故障・経年劣化を反映すること

⑤ヒューマンファクタを考慮すること

⑥ソフトウェアリスクを考慮すること

⑦変更管理によるリスクを考慮すること
⑧不確定性の高いパラメータは、その設定の考え方について明らかにすること（原則として、希望的観測にもとづきリスクを小さく評価しないように注意すること）
⑨最新の知識や環境の変化を反映すること
⑩自然災害等との複合事象も想定すること
⑪非定常作業時のリスク評価も行うこと
⑫事故拡大防止対策の失敗確率を考慮すること
⑬影響の大きさに関しては、人身への影響、物理的被害の影響のほか、環境（生態系、動物）・社会・地域・生活・組織等への影響も評価すること
⑭使用する情報の公開性・検証性を確保すること
⑮リスク論的目標設定を行うのは、対象システム等の現状リスクが検証できる範囲に限るものとする。

（5） 工学システムに関する安全に関与した許認可に関しては、以下の役割分担が望ましい。

・対象システムの稼働・不稼働の決定は、社会的にその責任をとることができる主体が行う。

企業が主体となって判断を行う工学システムに関しては、国等は社会安全の視点から望ましいレベルをガイドラインとして示し、そのガイドラインを参考にして企業が判断をすることが望ましい。

一方、国が主体となるような社会的に大きな影響を持つ対象に対しては、行政は、対象とする工学システムの受容について、多様な視点からそのリスクを明らかにして、稼働・不稼働の根拠を明示することが必要である。

・社会に重要な影響を持つシステムに責任を持つ国（政治・行政）等は、先見性を持って国際的な動向と国民の価値観に配慮してガイドラインを作成し、稼動・不稼動を決定する。（国際的基準の例：船舶事例）
・事業者・専門家は、最新の知識・技術を用いて、現状リスクを把握・報告する責務を持つ。
・市民は、科学技術のシステム・製品を安全活用し豊かな社会生活を行うに際して、理解すべき科学技術のリスクに関して関心を持ち、その受容のあり方に関して常に考えておくことが求められる。

ただし、科学技術の多様さ複雑さを鑑みた場合、全ての工学システムに対して、市民の一人ひとりが理解を深くすることの困難さがあることも事実である。したがって、事業者・専門家・国等は、市民が判断するための情報をできる限り提供するとともに、市民からその判断が信頼される状況を作る必要がある。

６　本報告のまとめ

本報告では、安全目標の対象として従来の生命、心身の健康、財産、環境等に加え社会リスクの最適化の観点も考慮に入れて、対象のシステムの稼働・不稼働がもたらす人・社会・環境にもたらす多様なリスクを勘案して社会の安全目標を設定することにより、21世紀社会が目指す安全社会に幅広く適用できるように考えた。そのために、本報告において重要と考える安全目標の基本的考え方は、理念的なものではなく、技術的かつ経済的に実現可能なものとして、設定することとしている。

そして、今回設定した安全目標の特徴は、経験した事故の再発防止はもちろんのこととして、未然防止の考え方を重視したことにある。さらに、この社会の安全目標の実現に向けて、製造者、運用者と利用者が、それぞれの立場に応じてバランスよく責任をとることを求めている。

本報告の主要な内容は、具体的な安全目標の検討と、工学システムの評価に関する要求事項である。各検討事項の要点は、以下のとおりである。

（１）安全目標の設定

安全目標として、人命に対する目標と社会リスクに対する目標の二つを検討した。

人命を対象とした目標においては、その影響の範囲や規模によって一律に定められるわけではないということを明確にした上で、工学システムの事故等が一定の規模以内で、不特定の人に対する事故に対しては、そのシステムの事故による個人の生涯死亡リスクとして、達成できない場合は許容されない基準値（A）を少なくとも 10^{-3}／年～10^{-4}／年にすること、そして更なる改善を必要としない基準値（B）は、10^{-5}／生涯～10^{-6}／生涯以下であるものを当面の目標とすることを提案している。また、基準値(A)と基準値(B)の間は、リスクを総合的に判断して対応を定めることになる。

社会的に影響の大きなリスクをもたらす工学システムの安全目標としては、対象とする工学システムの社会に寄与する機能と与える被害の甚大さの組み合わせによって、異なる目標を提案している。そして、工学システムの対象となる事故の発生確率と事故が発生した際の被害軽減対策により、被害を本報告で提案する安全目標より小さくすることも求めている。

また、この安全目標は、リスクや対策の評価の信頼性が重要であるため、評価に際しての注意を要する点も明記している。

（２）工学システム安全に対する要求事項

工学システムの安全を評価する際のリスク算定に対する要求や評価の役割分担等に関して取りまとめた。

要求事項としては、先に記した安全目標の適用の考え方と共に、５.の４）に示したように工学システムの現状リスク算定の際にチェックすべき 15 の事項を提案している。さらに、工学システムの許認可時の主体となる行政等の役割に加え、企業、専門家さらには、市民の役割について記述している。

７　おわりに

私たち市民は日々の生活のなかで種々のリスクに曝されて生活している。これらのリスクを深く考えることなく受容している場合もあれば、不安を感じながらも決められている基準値に従っている場合もある。果たして、これらのリスクの大きさは整合性をもって合理的な水準に達成されているのであろうか。

本報告をまとめるにあたり、安全目標について工学システム全体を通して考えた時、どのような考え方で整理すればよいかを中心に検討を進めた。工学システムにおける安全は、科学的合理性に基づき決定すべきであり、安全目標としてリスクの考え方を採用することが有効であるとの前提での検討となっている。

工学システム（プロセス、製品も含む）に関する規制・研究開発・設計製造・運営を行う者が、実施すべき施策・活動を検討する際に、他の事業・システムの状況も参考にしつつ現状の事業・システムの状況とここで提案した安全目標を比較することによって、その乖離や課題を認識できるように、安全を考えるような基準の考え方を提案した。

なお、本検討において参考にした具体的な分野は、参考資料２のAP１から10に示した分野であるが、当然のことながら全ての分野を網羅しているわけではない。

本報告が、全ての工学システムに適用可能なものであることを検証するためには、さらに多様な分野における安全の考え方を精査する必要があるが、その検証のためにも、今回の基本的な考え方を、多様な分野で安全目標決定の参考資料として活用されることを期待する。さらには、社会活動や市民生活における安全の判断にも資することになれば幸いである。

なお、本報告は、各産業分野の安全のあり方を基に、工学システムの社会に対する安全のあり方について、基本的なあり方を検討するにとどまっており、この考え方を社会に実装するためには、産業分野毎にこの安全目標を適用し、その実効性・有効性を検証する必要がある。

＜参考文献＞

［１］日本学術会議、安全に関する緊急特別委員会、「安全学の構築に向けて」、2000 年２月 28 日
［２］日本学術会議、ヒューマン・セキュリティの構築特別委員会、「安全で安心なヒューマンライフへの道」、2003 年３月 17 日
［３］ 日本学術会議、安全・安心な世界と社会の構築特別委員会、「安全で安心な世界と社会の構築に向けてー安全と安心をつなぐー」、2005 年６月 23 日
［４］ 日本学術会議、人間と工学研究連絡委員会安全工学専門委員会、「安全･安心な社会構築への安全工学の果たすべき役割」、2005 年８月 31 日
［５］ 日本学術会議、人間と工学研究連絡委員会安全工学専門委員会、「事故調査体制の在り方に関する提言」、2005 年６月 23 日
［６］ 学術の動向、[特集１]工学システムに関する安全・安心・リスク、2009 年９月号、７頁～55 頁
［７］ 日本学術会議、総合工学委員会・機械工学委員会合同工学システムに関する安全・安心・リスク検討分科会、提言「交通事故ゼロの社会を目指して」、平成 20 年（2008 年） ６月 26 日

＜参考資料１＞審議経過

平成 24 年

４月 27 日　日本学術会議幹事会（第 150 回）
安全目標のガイドライン検討小委員会設置承認

５月 20 日　安全目標のガイドライン検討小委員会（第１回）
委員長、幹事の選出、今後の進め方について。梶本光廣氏「原子力施設の安全目標(案)」説明。

７月 12 日　安全目標のガイドライン検討小委員会（第２回）

８月 20 日　安全目標のガイドライン検討小委員会（第３回）
突如として顕在化する巨大被害、検討が十分でない複合被害等の検討

10 月２日　安全目標のガイドライン検討小委員会（第４回）

11 月 16 日　安全目標のガイドライン検討小委員会（第５回）

12 月 26 日　安全目標のガイドライン検討小委員会（第６回）

平成 25 年

１月 24 日　安全目標のガイドライン検討小委員会（第７回）

２月 27 日　安全目標のガイドライン検討小委員会（第８回）
田村兼吉氏が正式に委員として承認された。中間報告案の検討。

３月 25 日　安全目標のガイドライン検討小委員会（第９回）

５月２日　安全目標のガイドライン検討小委員会（第 10 回）

６月 10 日　安全目標のガイドライン検討小委員会（第 11 回）
中間報告書素案の審議。

７月 4 日　安全工学シンポジウム 2013
小委員会審議内容について OS を企画、報告。

７月８日　安全目標のガイドライン検討小委員会（第 12 回）
今後の方針、中間報告書案について議論。

９月 12 日　安全目標のガイドライン検討小委員会（第 13 回）
報告書案について最終的審議。

９月 18 日　工学システムに関する安全・安心・リスク検討分科会（第６回）
本報告書内容について報告。

10 月 25 日　安全目標のガイドライン検討小委員会（第 14 回）
報告書案について最終的審議。

11 月 20 日　安全目標のガイドライン検討小委員会（第 15 回）
報告書案について再度最終的審議。

12 月４日　工学システムに関する安全・安心・リスク検討分科会（第７回）
本報告書内容を説明、基本的に了承される。

平成 26 年

１月 14 日　安全目標のガイドライン検討小委員会（第 16 回）
報告書文言についての検討。

２月 10 日　安全目標のガイドライン検討小委員会（第 17 回）
報告書文言について詰めの検討。

３月３日　安全目標のガイドライン検討小委員会（第 18 回）
報告書文言を含めての最終的検討。

４月４日　工学システムに関する安全・安心・リスク検討分科会（第８回）
本報告書内容を最終的に確認。

４月 13 日　工学システムに関する安全・安心・リスク検討分科会
本報告書を承認（メール審議)。

４月 22 日　総合工学委員会により本報告書内容が承認される。

７月２日　安全目標のガイドライン検討小委員会（第 19 回）
報告書査読結果についての対応方法について検討。

７月 15 日　工学システムに関する安全・安心・リスク検討分科会（第９回）
査読意見に対応した修正案について審議、一部修正後承認を得る。

○月○日　日本学術会議幹事会（第○回）
工学システムに関する安全・安心・リスク検討分科会報告「工学システムに対する社会の安全目標」について承認

＜参考資料２＞

AP１．内容の補足説明　現状における各種基準、関連データに基づく考察

１　基準値（A）の推定

基準値（A）は以下の検討により推定できる。

（１）英国安全衛生庁（HSE）(*1)は 10^{-3}/年を労働災害における許容可能の上限値としての死亡確率と設定している。これは労働災害についての値なので年間 1800 時間の労働時間として生涯（70 年）にわたる確率を求めると、

→　10^{-3} x 70y x 1800／8760～1.4x10^{-2}/生涯となり、 一般人の 10^{-2}／生涯　の死亡確率リスクに相当することになる。

（２）１／生涯のリスクの 0.1%の増加は許容可能であろうとの前提（大多数の人々が受け入れるであろうと考える仮説）をもとに考えると、10^{-3}／生涯という死亡確率リスクの値が出てくる。

２　基準値（B）の推定

基準値（B）は以下の検討により推定できる。

（１）日常生活におけるリスクの 0.1％の増加は許容可能であるとの前提（大多数の人々が受け入れるであろうと考える仮説）に基づいて算出すると次の様になる。

人口動態統計における年齢別死亡率の最小値の 0.1%の値を目標とすると～5x10^{-6}／生涯となる。

平成 22 年度データ　10～14 歳女子の死亡率　7.1/10 万人＝7.1x10^{-5}/年＝5x10^{-3}/生涯

上記の 0.1%　＝　5x10^{-6}/生涯

（２）英国安全衛生庁（HSE）は broadly　acceptable　の上限を 10^{-6}/年と設定している。労働災害についての値なので基準値（A）での考察と同等に考えて、

→　10^{-6} x 70y x 1800／8760～1.4x10^{-5}/生涯の死亡確率リスクとなる。

（３）癌を誘導することが発見されている場合には添加物が人間の食品の安全とみなされることはないという米国連邦食品医薬品化粧品法（FFDCA）の考え（デラニー条項）があったが、ゼロリスク基準の矛盾が次々と出てきた結果、1996 年クリントン政権のとき、「食品品質保護法」成立にともなって、このデラニー条項は廃止され、代わって、生涯発がんリスクレベル 100 万分の１が目標値とされた。⇒10^{-6}／生涯

３　各種リスクに対する安全目標の考え方（人命リスクを対象として検討した例）

以下の議論では 基準値（A）--→10^{-2}／生涯～10^{-3}／生涯、

基準値（B）--→10^{-5}／生涯～10^{-6}／生涯 と考えての議論としている。

（１）避けることの可能なハザード

①化学物質｛例：ベンゼンの環境基準　0.01mg/l）、砒素 TDI（tolerable daily intake）(*2)=15μg/kg/week｝の環境基準値は例のように定められているが、これらに

は影響の現れる閾値があるため基準値以下であれば実際上リスクをゼロとすることができる。基準値を達成するということは、生涯死亡確率リスクは零を目標とすることとなる。(0／生涯)

②有用性がある場合は基準値（B）が達成されれば許容可とする。

③ハザードを制限・除去する場合にコストを要する場合は「不均衡因子」(FD：Disproportion Factor)で判断(*3)する（図 AP１－１参照)。NCAF(*4)、GCAF(*4)の考え方も参考とする。

過大なコストを要する場合は、FD=10 でも基準値（A）が達成できない場合使用をやめる。使用をやめられない場合は、基準値(A)が達成できるまでコストをかける努力をする。

④自動車、航空機、原子力プラント等は人工物であるので原理的には使用を停止してハザードを除去することが可能である。基準値（A）が達成されているかどうかを交通機関システムについて統計データより検討(*5)した結果が図 AP1-2 である。

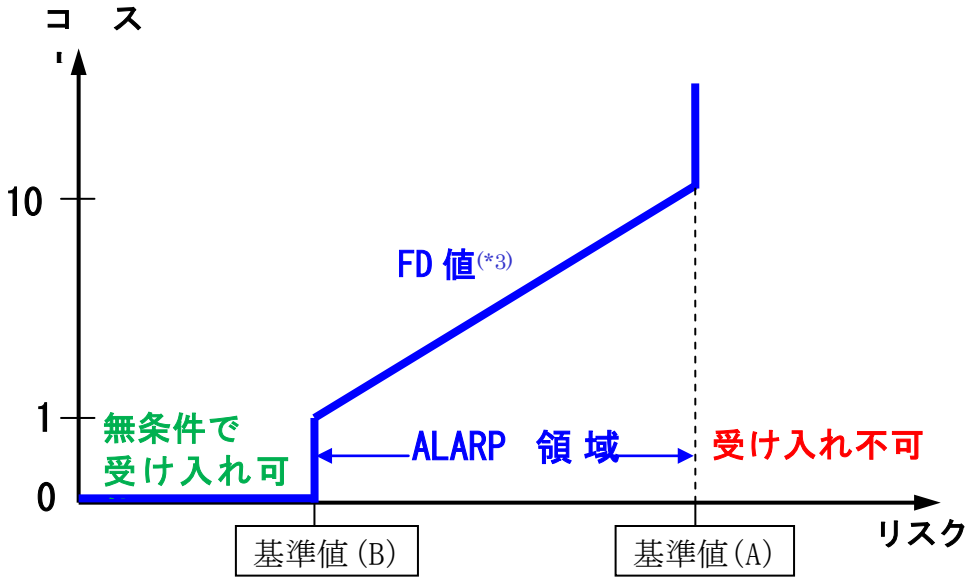


図 AP１－１　FD 値の考え方

(２)避けることの不可能なハザード

自然現象等でハザードが除去不可能でなおかつ閾値が存在しないものはリスクゼロにはできない。それゆえ以下の様な考え方をとる。

①有用性のない場合は基準値（B）の達成を基本原則とする。

②有用性のない場合で、ハザードを制限、除去する場合にコストを要する場合は不均衡因子（FD：Disproportion Factor)で判断(*3)する。上記条件が満たされない場合は基準値（A）が達成できるまでコストをかける努力をする。

③有用性がある場合も基準値（B）の達成を基本原則とする。

④有用性、リスク、コストのバランスを考慮する場合は、不均衡因子（FD)で判断(*2)す

る。NCAF、GCAF の考え方も参考とする。(*3)

⑤有用であるが本質的にリスクを減少できないもの（医薬品、放射線治療）あるいは代替手段がない場合は　有用性＞リスク　の場合に使用可とする。

＊1）Health and Safety Executive の略称で知られる英国の行政組織。日本では、安全衛生庁、健康安全局や保健安全執行部等の名称が使用されている。 約 4,000 人の職員を擁し､安全衛生関係法令に基づき安全衛生上のリスクを適正に規制することを仕事としている。多くのパンフレット、書籍も出版している。

＊2）TDI　動物実験等で求められた無毒性量(NOAEL)あるいは最小毒性量(LOAEL)を補正した値を不確実係数積(UFs)で割ってヒトへの無毒性量に変換したものである。

＊3）英国安全衛生庁（HSE）の提唱している考え方。FD を必要とされるコストとその費用により減少したリスクの比として、broadly acceptable　の上限（基準値（B））では FD=１，　ALARP（As Low as Reasonably Practicable：合理的に実行可能な限り低くするという原則）の上限（基準値（A）：unacceptable）では FD=10 を、intolerable 領域ではコストは際限なくかけるべきとの考え方。

＊4）　GCAF=⊿C/⊿R、NCAF＝（⊿C－⊿B）/⊿R　で定義され、それぞれコスト増加量（⊿C)、便益増加量（⊿B)、リスク減少量（⊿R）で構成される評価値。この値が費用対効果を表しており、これに基づいて安全対策実施するか否かの判断を行う。

＊5)各種交通機関システムを利用する際の個人の死亡リスクを統計データより算出すると概略以下の値が得られる。

商用航空機のリスク 10^{-6}死亡/flight　として評価すると、

一般人：国内外の旅行で年間 10 回使用するとして 50 年間旅行し続けると、

5×10^{-4}死亡／生涯

ビジネスマン：毎週飛行機を利用すると仮定すると、年 100flight～5×10^{-3}死亡／生涯

パイロット：年間 300flight　～　1.5×10^{-2}死亡／生涯

自動車移動のリスク　8×10^{-6}/1000km として一般人が年間 1 万キロ乗車すると仮定。

8×10^{-6}/1000km x 10000km x 70year = 5.6×10^{-3}死亡／生涯

船舶リスクの実績　　旅客船　1×10^{-6}/1000km、　漁船 10×10^{-6}/1000km、

漁業従事者：年間 4 万 km の操業があるとすると、

10×10^{-6}/1000km x 40000km x 70year =2.8×10^{-2}死亡／生涯

一般旅客：年に 4 回フェーリーで宮崎まで往復するとすると、

2000x4＝8000km/年＝5.6×10^{-4}死亡／生涯

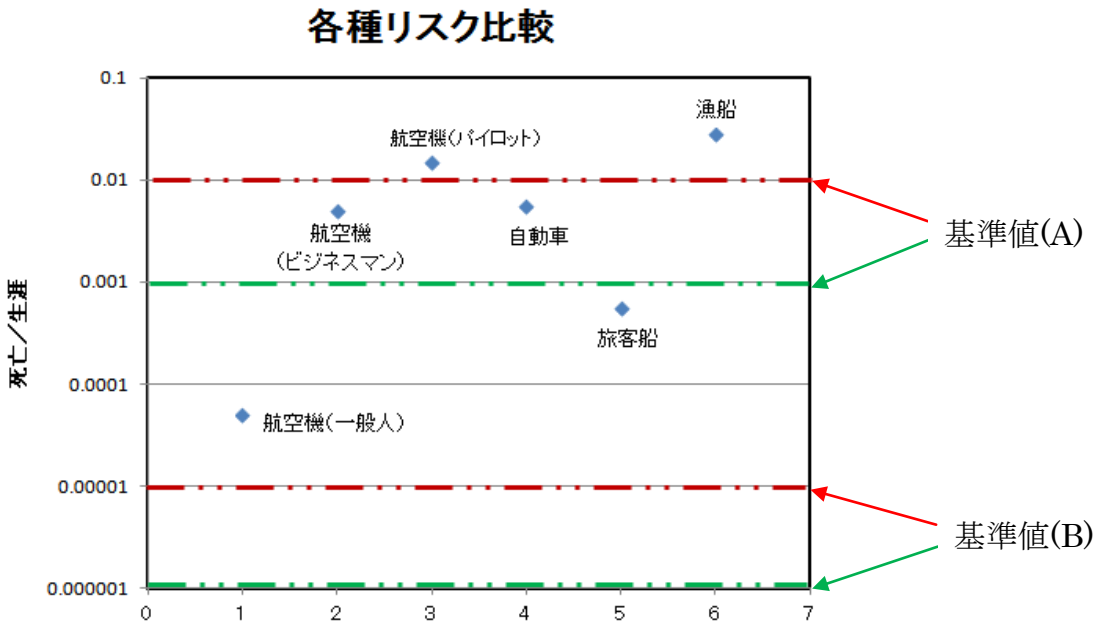


図 AP１－２　各種交通機関リスク比較

４　リスク、リスク減少のためのコスト及び便益を考慮した達成すべき目標値の考え方

リスクを減少させるために要するコストを横軸にとり、それに対するリスクの減少曲線が図 AP１－３中の右下がりの太い一点鎖線線で与えられている場合を検討する。通常、リスク減少は頭打ちとなり、リスクゼロにはならない状況となる。

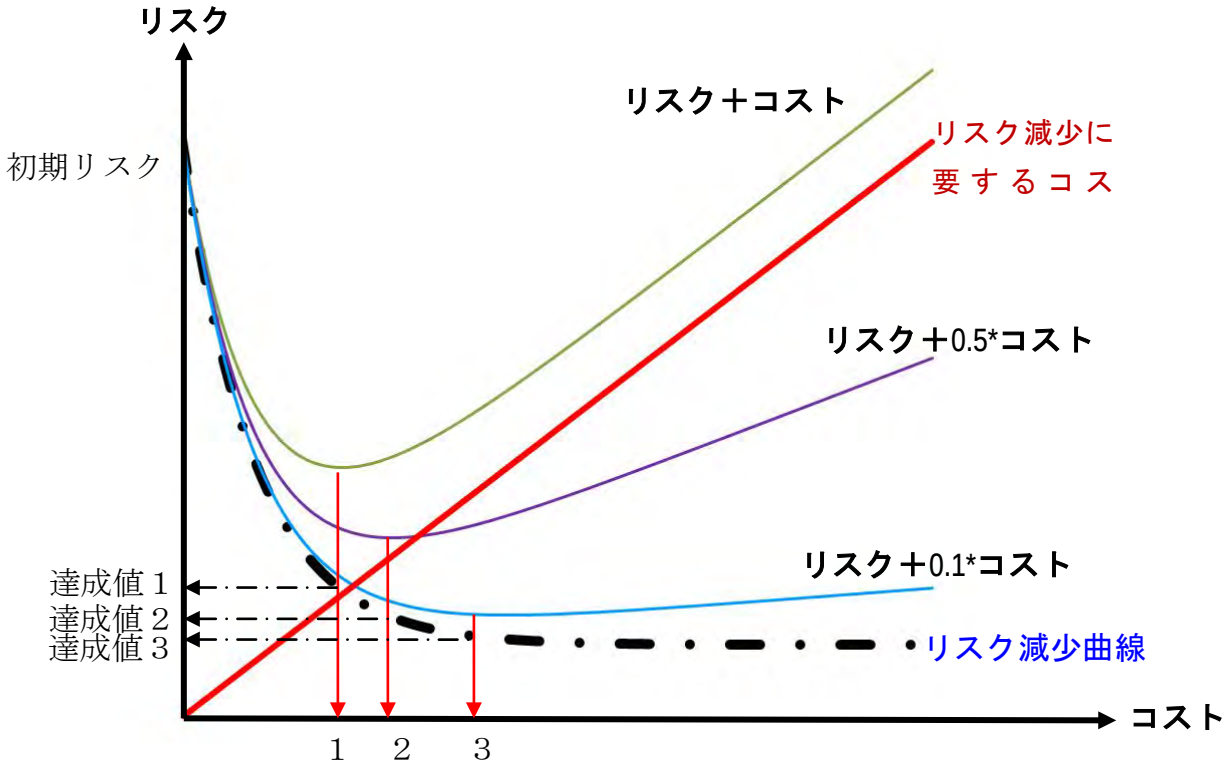


図 AP１－３　リスクと所要コストで決める目標値

コストとリスクの和が最小となる場合が最適な対応と考えた場合のコストは１のところで、その時達成されるリスクが達成値１と定まる。リスクに比較しコストを２倍かける場合は達成値２となる。10 倍のコストをかける場合は達成値３となる。もし、達成値３が図 AP１－１の基準値(A)より大の場合はさらにコストをかける必要がある。

便益（ベネフィット）を考慮した場合は図 AP１－４の様になる。便益（B）はリスクの大小によらず一定であるとしてリスクから便益を引いたものとコスト（C）の和が最小となる点によりリスクの達成値を決めるとする。便益の分だけ余分にリスクを受け入れることになり達成値としてのリスクは大きくなる。10 倍のコストをかける場合は、この図の場合リスクが便益以下となった時点でリスク減少のためのコスト投入を打ち切る。

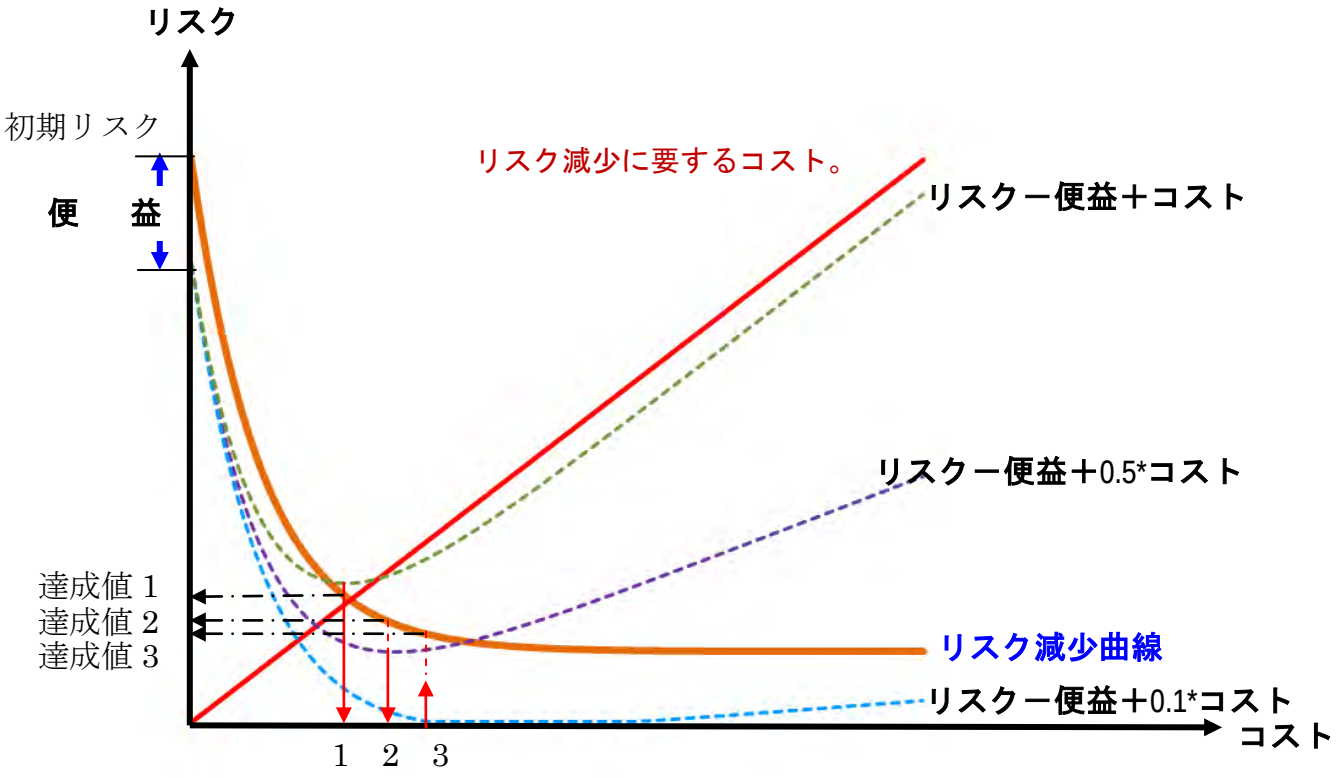


図 AP１－４　便益を考慮した場合の目標値

５　人命の損失と他のリスクとの換算例

リスク減少のためのコストとリスクを比較して賭けるべきコスト(達成すべきリスク値)を決めざるを得ない場合が出てくる。図 AP１－３、図 AP１－４はこの考え方を定量的に示し

た例である。リスクが人命損失確率の場合、コストと比較するため、人命の価値を金額で表示しなくてはならない。倫理上この種の換算は受け入れがたいとの主張もあるが各分野、特に保険の分野では導入されている。以下いくつかの例を見ていく。

（１） 英国安全衛生庁（HSE）の提案値（図 AP１－５.参照）

一人の死亡を金額で換算　＝1,336,800 ポンド=2 億 2700 万円（１ポンド＝170 円で換算）
回復不能な傷害　＝207,200 ポンド＝3522 万円
重度傷害　＝20,500 ポンド ＝348 万円
軽度傷害　＝300　ポンド＝5 万 1000 円

ここで、回復不能な傷害と死亡の価値の比が 0.155：１であるので、回復不能な障害の発生頻度は死亡に比較して 6.5 倍＝1/0.155 発生しても可と考えられる（被害と発生頻度の積が同一の場合同一リスクを表すとの考えに基づく）。それゆえ、$6.5x10^{-6}$～$6.5x10^{-3}$／生涯　の発生頻度が、基準値（B）から基準値（A）の範囲となる。

同様に重度傷害の発生頻度についての基準値（B）～基準値（A）の範囲は $6.7x10^{-5}$～$6.7x10^{-2}$／生涯となる。

軽度障害の発生頻度は　$4.5x10^{-3}$／生涯～4.5／生涯の範囲となり、生涯において軽度傷害が４、５回発生しても許容可能と考える。

（２） 船舶分野において OECD 諸国で妥当とされている値

一人の死亡＝300 万ドル＝3 億円

（３） 経済損失の許容発生確率

人命が価格に置き換え可能とし、換算に英国安全衛生庁（HSE）の提案を用いると、死亡リスクの許容発生確率を経済損失の許容発生確率に変換可能となる。

10^{-6}死亡/生涯（基準値（B））は 227 円／生涯の損失となりこの額は十分受容可能（無視し得る額）となる。

10^{-3}死亡/生涯（基準値（A））は 22 万 7,000 円／生涯の損失となりこの額以上の損失は回避すべき、つまり許容可能損失額の上限値となる。

（４）経済損失の許容発生確率、別の考え方

一般の人の生涯収入を 2 億 5 千万円と見積もると、それの 0.1%（10^{-3}）の損失は受容可能であろうとの前提（大多数の人々が受け入れるであろうと考える仮説で基準値(A)、(B) の検討におけると同等の仮説）により算出した額は 25 万円となる。

25 万円/生涯の損失は 10^{-3}/生涯の発生確率に対応すると言え基準値（A）に等しいので、許容可能損失額の上限値と言える。また、比例計算より、250 円/生涯の損失（$1x10^{-6}$/生涯）は無視し得る額と言える。

（５） 社会的損失の受容可能な発生頻度

上記(1)～(4)の議論は個人の経済的損失である。F-N カーブでは（損失人命数 x 発生頻度）の値を比較し、値が等しい時を同一リスクと捉える方法がある。これを社会全体としての経済損失・環境汚染を考える際に援用すると以下のような論議となる。

例えば一事故で 500 億円の損失が生じる事故の受容可能な発生頻度の上限を FUA と置くと、

500 億円 x FUA ＝ ２億 2700 万円 x 10^{-3}/生涯（70 年）

FUA= 4.54x10^{-6}/生涯＝6.5x10^{-8}/年 ；

対策不要の発生頻度 FBA は FBA=6.5x10^{-11}/年 となる。

さらに、単純にこの考えを拡張して、福島原発事故に適用し被害総額が 20 兆円に上るとして計算すると次の結果が得られる。受容可能な発生頻度の上限値 FUA=1.14x10^{-8}/生涯＝1.6x10^{-10}/年、対策不要の発生頻度は FBA=1.6x10^{-13}/年。FUA で示された値は、言い換えれば、約 63 億年（地球の年齢以上）に一度の発生確率でも受け入れられないということとなり、発生は絶対に認められないということとなる。

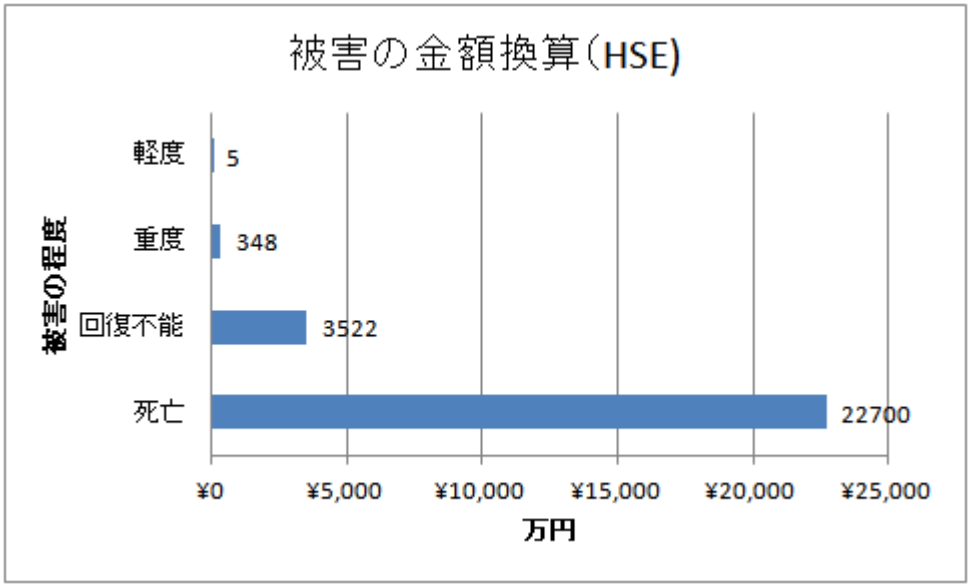


図 AP１－５ 被害の金額換算

AP２．原子力発電システムにおける安全

１　原子力発電における安全目標

原子力エネルギー利用、特に原子力発電における安全目標につき、その経緯と現状を記す。原子力発電は、開発当初から積極的な安全確保策をとりつつ進められたが、その過程で安全目標も検討された。安全目標を考える上での原子力発電の特徴として、少量の燃料で巨大なエネルギー(電力)を生産すること、反面、事故となると影響も大きいというリスクを伴っていること、半世紀あるいはそれ以上という長寿命のプラントであり、技術の進化や劣化、及び人的技術継承の重要性も考慮する必要があることである。

（１）原子力とリスク・便益・安全

原子力発電利用の最大の「リスク」は、核反応の制御失敗や発生する熱の制御失敗、そして機器装置の故障等に伴う多量の放射性物質の施設外への放出で、これにより施設周辺の一般公衆に「死亡」や「障害」を与え、「環境」へも大きな影響を与える。それに伴う「経済損失」も大きい。

一方原子力利用の「便益」は、核反応により発生するエネルギーの膨大さ故に、その「経済的利益や長期的資源としての価値、そして地球温暖化等の環境影響が少ないという価値」を有する。

「安全目標」は、「リスクと便益を考えて受容された状態」を目指す努力の方向を示すものである。特に原子力には、便益を受ける受益者とリスクにさらされる被害者が異なる場合があり、目標達成の具体的な進め方において受益者・被害者の公平性は別に考える必要もある。

（２）原子力発電の安全目標の特徴

原子力発電の特徴は、巨大なエネルギーをコントロールしながら利用するので、各国で多くの規制基準指針類が定められ、またそれを監視する規制機関が設けられると共に、国際的に検討する機関が設けられている。安全目標は、原子力施設の安全確保対策やこれら国や国際機関の基準や規制要件に深く関係する。

原子力発電は高度な科学技術をベースにした巨大システムであり、安全確保を検討する際の「事故・災害のハザード」は「人的」・「システム的」・「機械的」・「化学的」要因以外に「自然現象」も大きな要因となる。そのための安全対策は、「未然防止」・「拡大防止」・「回復力の向上」の視点から何重にもなされる必要があり、安全目標はその指標となる。

（３）安全目標の要件

原子力施設は開発当初より、放射性物質の放出による施設周辺住民への影響を最小限にすることを含めた安全設計がなされてきた。従って、「施設周辺住民でも、通常時はもとより、事故時においても放射線による被ばくの影響がないこと、例えそれを凌駕するような規模の事故が生じても、退避等により安全が確保されること」という目標がたてられており、これが「安全目標」といえる。「究極の目標」は退避の必要が無いこと

であるが、実際には退避を考えておく必要がある。

原子力施設は「高度な科学技術を利用する巨大総合技術による長期間利用施設」であるため、これを「維持し安全確保の水準の後退を防ぎ、さらに向上させる」ことが必須の要件であるので、これを目標に含むことも重要である。また、「技術や社会の状況変化」や「施策への反映」も考慮して目標を設定する必要がある。

（４）安全目標の基本的な考え方

原子力エネルギー利用における安全目標を考える上でのリスク対応とその評価は1950年代の開発当初から検討され､1970年代のラスムッセン報告以降は数量化も進み、安全確保策に取り入れられてきた。しかし、リスク概念を国民に理解してもらうことは各国とも多かれ少なかれ苦労している。だが福島第一原子力事故を経験した現在では、リスク情報を活用した安全確保策と安全目標設定をより積極的に行うことが必要であり、またその機会でもある。

原子力施設は、放射能・放射線の影響によって施設周辺、及びそれ以遠の住民の人命に関わる事故の発生を防止することが重要である。死亡という点では、「数ヶ月以内という急性死亡と、がんによる長期的死亡」リスクの両面がある。しかし、確率的リスク評価においても、事故による放射性物質の放出とそれによる人の死亡リスクを統計的に有意な値として出すことは数値が小さく極めて難しい。すなわち、死亡リスクが最も重要であるが、原子力ではこの直接的評価が難しく、「個人の生涯死亡リスクを 10^{-5}～10^{-6} 以下」にすることは、統計上の有意な値としては明記できず、不確定な点は保守的（厳しめ）に考えて死亡率として評価する場合もある。従って原子炉の安全目標策定のためのリスク評価では直接的な死亡リスクを用いず、炉心損傷や格納容器機能喪失の発生確率を指標とした「原子炉の性能目標」として表すことが行われる。IAEA 等国際的にも、「炉心損傷」､「格納容器機能喪失」､そして「放射性物質放出量」を指標値として安全目標を考えている。

社会的リスクとして重要なものは「経済的影響」であるが、原子力はその初期投資額が大きいこと、運転により得られる経済的メリットが極めて大きいこと、従って逆に事故が発生すればそのメリットが消えると共に初期投資額の負担が重くのしかかることが特徴である。「時間的や空間的に環境影響が大きいリスク」として、通常運転中の原子力発電における放射性物質の放散は、自然環境の中の放射性物質量と比較してそれほど問題は無い。大量の放射性物質を放散する大事故時における「土壌等の除染の必要性」等のリスクが問題である。

原子発電は、エネルギーをどうするか、という第二次世界大戦後の選択の中で方向が決められた。その後オイルショック等の何度も訪れたエネルギー危機への対処でも、日本の原子力利用の方向は変わらなかった。現在、エネルギー問題はグローバル化し、国際的な競争が激化している。自然エネルギー利用におけるリスク等も含めて、エネルギー問題を俯瞰的に検討することが必要で、その中から「グローバルに見たエネルギーリスクの最小化」とそこでの「原子力リスクの最適化」が浮かび上がってくる。

（５）安全目標設定において考慮する項目

日本ではこれまで安全目標設定への努力をしてきたが、「中長期的な目標」や「国際的動向」を考慮して「適宜見直しを行いつつ（期間毎)」設定する必要がある。産業界を含む原子力関連の機関が「設定する目標」の「指標」を国が主導して設定することが重要である。

原子力の安全確保とそのための安全目標設定には、多くの項目の考慮が必要である。例えば、「災害・事故・トラブルの可能性の洗い出し」、「故障・経年劣化の反映」、「ヒューマンファクタ」、「ソフトウェエアリスク」、「変更管理」、「不確定性の高いパラメータの根拠明示」、「最新知見・環境変化の反映」、「自然災害等の複合事象」等々である。これらの多くの項目は、原子力関連規格基準指針類で考慮されているが、安全目標としては重大事故への進展の未然防止と発生した場合の影響の最小化を目指す必要がある。特に、これまで十分考慮されてこなかった項目や、安全目標として目標設定するには知見がまだ十分でないものについては継続した研究が重要である。

２　原子力発電における安全目標設定の経緯と現状

（１）　軽水炉開発と安全確保の経緯

①世界の原子力開発と米国の軽水炉開発

第二次世界大戦後、戦勝国において軍用艦動力用として原子炉開発が始まり、これを発電用に用いる研究も引き続いて行われた。各国の進展も見て 1953 年 12 月にアイゼンハワー大統領の国連での「Atoms for Peace」宣言により世界的に発電用原子炉の開発と利用が開始され、1956 年には黒鉛減速炭酸ガス冷却のコールダーホール発電所が英国で営業運転を開始した。

濃縮ウランを用いる軽水炉は米国で開発されたが、広大な政府保有地での研究炉や試験炉段階では出力も小さく大きな問題はなかった。しかし、発電用炉としての出力増大と住民居住地への接近立地が原子炉の安全確保上の問題して連邦議会でも議論された。

ウラン燃料を被覆管の中に納めた燃料棒、燃料集合体を含む炉心の圧力容器内への装備、圧力容器を含む原子炉系の格納容器内への収納、そして非常用の炉心冷却系と格納容器冷却系の装備により、万一の時にも放射性物質の異常な放散を防ぐという設計により、 炉心損傷の防止と放射性物質の拡散防止という安全確保の基本が確立されて商業用発電所が認可された。

米国における最初の商業用発電炉は、航空母艦用に建造された炉を転用して 1957 年に運転を開始した電気出力 60MWe の加圧水型炉 PWR(Pressurized Water Reactor)の Shipping Port 発電所である。発電用として開発され 1961 年に営業運転を開始した Yankee Rowe がそれに次いだ。米国では加圧水型炉と共に発電用を目的とした沸騰水型炉 BWR(Boiling Water Reactor)の開発も行われた。当初は熱交換器を介して二次蒸気をタービンへ供給する強制循環二重サイクル炉 Dresden１号が 1960 年に、また自然

循環炉 Humbolt Bay が 1963 年に営業運転を開始したが、今日の BWR の基本型である直接サイクル炉は 1969 年営業運転開始の Oyster Creek が最初であった。これら商業用軽水炉の安全確保は、異常発生防止、異常が発生しても事故への拡大防止、事故へ発展しても放射性物質の異常な放出防止という 3 層からなる多重(深層) 防護の概念が基本となった。そして立地指針には、原子炉周囲の非居住地区とその周りの低人口地帯を設ける遠隔立地を基本とすると共に、いざという場合の退避等を念頭においている。

②日本の発電用原子炉の導入と安全対策

日本ではアイゼンハワー大統領の宣言直後の 1954 年度に原子力予算が組み込まれて原子力の平和利用が開始された。翌 1955 年には原子力基本法の制定や原子力委員会の設置、日本原子力研究所(原研)のスタート等があり、米国からの研究炉の導入等がなされた。1957 年には民間の電力会社により日本原子力発電(原電)が設立され、早速英国から 166 MWe の黒鉛減速炭酸ガス冷却コールダーホール型炉の導入を決定して東海発電所として国へ申請した。この炉は濃縮に大電力を必要とする濃縮ウランでなく天然ウランを用いており、また発電炉としては当時世界で出力が最大であり、その面からの経済性も考慮された。しかしこの炉には十分な耐震設計がなされておらず、また本格的な格納容器も無い炉であった。日本では耐震技術も進んでおり、それらをベースに燃料体の設計変更を行い、また格納容器の代替機能の整備を行うと共に、米国の安全確保の考え方を参考に原子炉緊急停止装置の多重化、緊急炭酸ガス冷却系等を追加するなどして、「コールダーホール改良型炉」として国へ申請され 1959 年に設置許可が出された。

さらに 1960 年頃には米国で開発が進んでいた軽水炉の導入が電力会社で検討された。そして 1963, 64 年には世界に先駆けて非常用炉心冷却系や格納容器冷却系等の工学的安全防護設備の有効性に関する国の大型プロジェクト研究(SAFE プロジェクト)が進められ世界的に高い評価を得る成果を得た。このように原子炉導入における安全対策には日本も当初から多くの努力を払った。1965 年から米国の BWR と PWR への発注がなされ、1970 年に敦賀 1 号(BWR)と美浜 1 号(PWR)が営業運転を開始した。

このように、原子炉の重要な安全対策は非常用炉心冷却系(ECCS)の強化による非常時の炉心損傷防止と格納容器の設置による放射性物質抑制であって、前者では大口径配管破断時の ECCS の能力と燃料棒の冷却特性が最大の想定事故としての課題とされ、また放射性物質の挙動も大きな課題としてその後多くの試験研究が原研を中心に行われた。

③TMI 事故とリスク評価及び安全目標

米国では原子力発電の安全と環境問題への対処として、ラスムッセンにより原子力発電所の確率論的リスク評価 PRA (Probabilistic Risk Assessment)がなされて 1975 年に最終報告が出された。これは原子力プラントのリスクを確率的に評価したもので、ルイス委員会でこれを再評価して 1978 年に報告が出された。この再評価報告では、ラスムッセンの確率論的評価手法の骨格の妥当性を認めた上で、絶対値は不確定性が多

いが、相対的評価には意義があるというものであった。その報告直後の 1979 年３月に TMI 事故が発生した。この事故の発端は単純な事象であったが、加圧器の安全弁が開いたまま固着したことに運転員が気がつかなかったため、小さな開口からの冷却水喪失事故と同じになって炉心上部が露出して燃料棒の破損溶融事故となった。ラスムッセン報告では、最大口径配管の破断より小口径配管破断の方が確率的に大きなリスクとなり得るというものも含まれており、小破断相当から始まった TMI 事故に相当するものであった。これにより PRA の有効性が確認され、日本でも PRA 手法によるリスク（安全)評価が盛んになり、機器の故障や人為ミス等の内的事象を中心にリスク評価技術が進展した。米国ではこのリスク評価結果を、安全評価のみでなく安全確保対策の充実・向上に活用することが行われており、さらに規制機関はリスク評価に基づく安全規制として活用している。

また米国では 1980 年に安全目標案を公表し、1986 年に安全目標の政策声明を発表した。その要旨は、発電所近くの公衆の受ける原子炉事故による個人リスク及び公衆のリスクはいずれも他の事故によるリスクの 0.1%を越えないこと、及び大量の放射性物質放出を伴う原子炉事故の発生確率が 10^{-6}/炉年より小さいことであり、これらはその後 IAEA 等での国際的な目標にもなった。また、リスク減少効果がごく小さいがお金のかかる安全対策は行う必要が無いことも含まれている。

④シビアアクシデント対応と深層防護

1986 年にチェルノブイリ事故の発生を受けて、日本も積極的にシビアアクシデント対応を行うことになり、1987 年に原子力安全委員会（原安委）は対応方針の検討を、また当時の通産省は原子力工学試験センターNUPEC(Nuclear Power Engineering Center）において研究を開始した。1992 年に原安委は「事業者はアクシデントマネジメント（AM)を自主的に整備して万一の時に的確に実施するよう強く奨励する」との方針を出した。これは規制要件ではないが実質上規制要件に近い形で行われており、その対応策は諸外国と比較して遜色は無かった。しかし、1995 年に OECD/NEA の原子力規制活動委員会においてシビアアクシデント対応に対する国際的な統一見解として、新設炉に対しては設計段階から対策を検討する等の合意がなされた。また IAEA でも安全原則や安全設計基準において、これまでの３層からなる多重(深層）防護に加えて、シビアクシデント対応(第 4 層）と発電所周辺の緊急事対応(第 5 層）を含む検討が行われた。日本では新設炉に対する対応策として 1999 年に民間自主基準が作られたが、事業者のAM整備の規制行政庁の最終的承認は2002年になってからであった。また1990年代後半からは、通産省によるシビアアクシデント研究予算も次第に減少して対応が進まず、シビアアクシデント対応を真剣に考える人材も弱体化した。

（２）原子力安全委員会と安全目標

①安全目標専門部会の設置と安全目標

このような状況であったが、原安委は、安全規制活動によって達成し得るリスクの

抑制水準として確率論的なリスクの考え方を用いて定める安全目標を活用することがさらに効果的であるとして2000年９月に安全目標専門部会を設置した。同専門部会は審議を行い2003年12月に「安全目標に関する調査審議状況の中間とりまとめ(以下中間とりまとめ)」を原安委に報告した。この中間とりまとめでは、施設が安全目標に適合しているかどうかの水準を性能目標として検討することが合理的であるとした。

そこで 2004 年７月に安全目標専門部会に性能目標検討分科会が設置されて審議を行い、2006年３月の会合において同専門部会は「発電用軽水型原子炉施設の性能目標について－安全目標案に対する性能目標について－(以下性能目標)」を取りまとめて原安委に報告した。

②中間とりまとめの要点

中間とりまとめでは、原子力災害発生時における公衆(個人又は集団) あるいは施設従事者に対する様々な健康影響や周辺への経済的な影響の発生が考えられる中で、それらのリスクの抑制水準を示すものが望ましいが、リスク評価技術の成熟度やリスクの抑制水準も異なることから、「国民の安全確保の視点から真っ先に留意し、かつリスク評価技術や抑制水準の議論が進んでいる公衆の個人に対する健康影響に関連したリスクを指標」とした安全目標案の検討を進めた。そして「定性的目標案」として公衆の日常生活に伴う健康リスクを有意には増加させない水準に抑制すること、「定量的目標案」として原子力施設の事故に起因する被ばくによって、施設の境界付近の公衆の個人の急性死亡リスクが年当り百万分の１程度を超えないよう抑制すること、また事故に起因する放射線被ばくによって生じ得る施設からある距離の範囲内の公衆のがんによる個人平均死亡リスクは年あたり百万分の１程度を超えないよう抑制すること、とした。さらに、原子炉施設や核燃料サイクル施設が安全目標に適合していることの判断の目安となる水準を性能目標として検討することが適切として、「原子炉施設では操業時に重大な炉心 損傷が発生する確率や大量の放射性物質がある時間内に放散される事象が発生する確 率」(核燃料サイクルも同様に放射線放射や放射性物質の放散が発生する確率) を検討することが合理的とした。

③性能目標の要点

性能目標は安全目標への適合性を判断するための補助的な目標と定義し、性能目標の指標として発電炉の特性に着目した指標を選定することとした。また内的事象と外的事象の両者を検討の対象としたが、産業破壊活動等の人為事象リスクは検討対象外とした。性能目標の指標としては、炉心損傷、格納容器機能喪失、大規模放射性物質放出に関わるものがあり、炉心損傷頻度 CDF (Core Damage Frequency)、格納容器機能喪失頻度 CFF (Containment Failure Frequency)、早期格納容器機能喪失頻度 ECFF (Early CFF)、 大規模放出頻度 LRF (Large Release Frequency)、早期大規模放出頻度 LERF (Large Early Release Frequency)等があるが、施設の性能をよく代表し適切に定量化できるものとして以下の２つの指標を併用することとした。

指標１　炉心損傷頻度 CDF (Core Damage Frequency)

指標２　格納容器機能喪失頻度 CFF (Containment Failure Frequency)

その定量的な指標値としては以下の値を示し、両方が同時に満足されることを発電炉に　関する性能目標の適用の条件とした。

指標値１　　CDF：10^{-4}/年程度

指標値２　　CFF　：10^{-5}/年程度

各原子炉施設におけるリスク評価とこの目標の比較にはリスク評価における不確かさを考慮した上で平均値を用いることとした。そして適用にあたり考慮すべき事項として、複数基立地における影響の適切な考慮、地震等の自然現象に伴う不確実さの考慮、外的事象の PRA 技術向上、等を挙げた。

④海外における動向

日本では原安委を中心に安全目標が検討されてきたが､米国等諸外国やIAEA､OECD/NEA等の国際機関もこれに関わる活動を行ってきた。2009 年の OECD/NEA の加盟国における取りまとめによると、表 AP２－１に見るように炉心損傷頻度 CDF の指標値は各国で大差はないが、新設炉と既設炉で使い分けている国もある。また表 AP２－２に見るように大規模放出では日本は格納容器機能喪失頻度 CFF として頻度を与えているが、大規模放出頻度 LRF と早期大規模放出頻度 LERF の頻度のみを与えている国､放出量も指標としている国(ヨーロッパ主体) がある。放出量を指標とする国では、Cs137 の放出量を 100 TBq 以下にする頻度をあげている国が多い。

（３）福島原子力事故と原子力規制委員会

東日本大震災により､福島第一原子力発電所１～４号炉で炉心溶融と水素爆発による原子炉建屋崩壊となるシビアアクシデントが発生した。この収束には時間がかかっており､かつ避難住民の帰還や土地の除染がなかなか進んでいない。想定できなかった大津波によるものとはいえ、この事故は日本の原子力の規制制度に大きな変化を与え，2012 年９月に新たに原子力規制委員会ができ、原安委と原子力安全・保安院の機能を引き継ぐこととなった。

同委員会は､新たに安全基準等を制定する作業を行うと共に､2013 年３月から安全目標について検討を行った。そこでは、大規模放出時の Cs^{137}の放出量が 100 TBq を越えるような事故の発生頻度は 100 万炉年に１回程度を超えないように抑制されるべきこと、を追加する方向で検討すると思われる。この放出量であれば、福島第一原子力発電所事故の場合の 100 分の１程度であって､原子力発電所の敷地範囲程度で影響が抑えられるもので、放出量を指標としている諸外国の数値ともほぼ同等である。

表 AP２－１　各国の炉心損傷頻度 CDF の目標値の一覧　（原子力規制委員会資料）

国	設定者	CDF 値(1/年)	備考
米国	規制機関(NRC)	10^{-4}	既設炉 新設炉
英国	規制機関	10^{-4}	限度(法的限度ではない)
		10^{-5}	目標
フランス	規制支援機関(IRSN)	10^{-5}	限度
スイス	規制機関	10^{-5}	
スウェーデン	事業者	10^{-5}	限度(法的限度ではない)
スロバキア	規制機関	10^{-4}	目標
オランダ	規制機関	10^{-4}	限度（既存炉）
		10^{-6}	限度(新設炉)
フィンランド	規制機関	10^{-5}	既存炉　新設炉
	事業者(FORTUM)	10^{-4}	
	事業者(TVO)	10^{-5}	目標
チェコ	事業者	10^{-4}	目標(既存炉)
		10^{-5}	目標(新設炉)
カナダ	規制機関	10^{-5}	
	事業者	10^{-4}	限度
		10^{-5}	目標
イタリア	規制機関	10^{-5} to 10^{-6}	目標
ハンガリー	規制機関	10^{-5}	目標
日本		10^{-4}	
ロシア		10^{-5}	
韓国	規制支援機関(KINS)	10^{-4}	既存炉
		10^{-5}	新設炉

表 AP２－２　各国の大規模放出頻度 LRF と早期大規模放出頻度 LERF の目標値の一覧[１]

頻度のみを指標とするOECD/NEA加盟国					
国	設定者	指標	値 (1/年)	備考	
米国	規制機関(NRC)	LERF	10^{-5}	既設炉	
		LRF	10^{-6}	新設炉	
		CFF	10^{-1}	新設炉、条件付確率	
スロバキア	規制機関	LERF	10^{-5}	目標	
オランダ	規制機関	LRF/LERF	関数	限度、急性死亡者数と発生頻度	
チェコ	事業者	LRF/LERF	10^{-5}	目標(既存炉)	
			10^{-6}	目標(新設炉)	
台湾	事業者	LERF	10^{-6}	目標	
ロシア		LRF	10^{-7}	限度	
韓国	規制支援機関(KINS)	LERF	10^{-5}	既設炉	
			10^{-6}	新設炉	
日本	規制支援機関(JNES,JAEA)	CFF	10^{-5}		

放出量を指標にするOECD/NEA加盟国					
国	設定者	指標	値(1/年)	放出量	備考
英国	規制機関	LRF	10^{-5}	I-131:10^{4}T Bq	限度(法定限度でない)
			10^{-7}	Cs-137:200 T Bq	目標(線量/限度の段階的)
フランス	規制機関	LRF	10^{-6}	許容されない結果	目標
スウェーデン	事業者(Ringhals)	LRF	10^{-7}	Cs-134,137:炉心内蔵量の0.1%	限度(法定限度でない)
	事業者(OKG)	LRF	10^{-5} より かなり低	希ガスを除く炉心内蔵量の0.1%	
フィンランド	規制機関	LRF	5×10^{-7}	Cs-137:100 T Bq	新設炉/既設炉
	事業者(FORTUM)	LRF	10^{-5}	CDFの10%	
	事業者(TVO)	LRF	5×10^{-7}	Cs-137:100 T Bq	目標
カナダ	規制機関	LRF	10^{-6}	Cs-137:100 T Bq	
	事業者	LRF	10^{-5}	Cs-137:炉心内蔵量の0.1%	限度
			10^{-6}		目標

３．まとめ

以上のように、原子力発電は開発当初から安全確保のための努力がなされ、多くのプラント建設経験をベースに、リスク評価手法も進展した。しかしこのリスク評価には、詳細な機器類とその故障データ等々のデータが必要であるが、しっかりしたデータ等も限定されたものであり、現在のところ内的事象（機械類の故障や配管等の損傷、人為ミス等の要因による事象）への対応がなされている。これは相対的評価（故障等の場合の事故へ至るリスク上の重要性の比較評価）には有用なので、リスクの知見を活用する米国では規制判断に利用されている。一方、外的事象の扱いが課題であるが、いずれにしても日本ではこれらをベースにした新しい安全目標が原子力規制委員会で検討されると思われる。

原子力の安全確保のために到達すべき安全目標としては、「施設周辺住民でも、通常時はもとより、事故時においても放射線による被ばくの影響がないこと、たとえそれを凌駕するような規模の事故が発生しても、退避等により安全が確保されること」が目標であり、究極の目標は「退避の必要がないこと」であろう。それと並行して、「プラントの安全に常に目を配り、技術力や安全確保策の後退を防ぐこと」を惹起するものである必要がある。また、重要なことは「エネルギー技術の中の原子力」であり、グローバリゼーションが進んだ世界における今後のエネルギーの視点からの評価（エネルギーセキュリティー）である。

参考文献

[１]原子力規制委員会、第 31 回原子力規制委員会資料８－４、2013 年２月 27 日

AP３．化学プラントにおける安全

１．化学プラントの安全目標の考え方

化学プラントの労働災害発生件数は、“挟まれ”“巻き込まれ”等による事故が、一般の製造業と同様に圧倒的に多い。しかし、2011 年から起きた３件の爆発事故は、規模の大きさとともに、化学プラントの地域社会や環境に及ぼす影響、原料・素材供給メーカーとしての社会的役割が極めて大きいことを再認識させた。

各企業は“事故ゼロ”を目指して、日頃から①ルール遵守と変更管理の徹底、②リスクアセスメント及び危険予知の徹底、③関係者間での報・連・相の徹底等、安全管理の基本事項の遵守に努めているが､それでも事故が起きるのが現実である｡この実態を踏まえて、理念目標ではなく、現実に実行可能な目標のもとでの安全管理が求められる。

化学プラントの安全目標は､労働災害防止はもちろんのことであるが､“リスクベースの安全管理”のもとに、社会に大きな影響を及ぼす事故、特に爆発火災事故のような重大事故は起こさないことが求められる。

（1） 安全目標の考え方

最近の化学プラントの事故から得られた安全管理の考え方を表 AP３－１に示す。

表 AP３－１　事故から学ぶ安全管理のポイントと安全目標の考え方

項目	安全目標の考え方
１．爆発火災事故は社会に大きな影響を及ぼす	１．“危害の大きさ”は労働災害だけではなく、社会的影響を含めて評価する
２．全てのリスクに対応できない	１．重大事故は､たとえ､発生確率が低くても起こしてはいけない。 ２．リスクアセスメント（ＲＡ）に基づいて、リスクの大きさを評価し、優先順序をつけてリスクを低減する。 ３．残留リスク情報は、関係者で共有する。
３．事故が起きた場合の被害を最小化する	１．設計段階から本質安全化（危険物保有量の最小化）に取り組む。 ２．事故が起きたときの影響が及ぶ範囲を局所化し、自社の敷地外には影響を及ぼさない。

（2） 危害の大きさ

ほとんどの事業所は､｢休業災害：ゼロ、　不休業災害：前年度実績以下｣のように､｢労働災害ゼロ｣を目標に安全活動を行っているが、危害の大きさは、事故が社会にもたらす影響を含めて目標を設定することが必要である。

二つの事例を紹介する。

2013 年７月石油化学工業協会（石化協）は産業事故防止に関する行動計画 (1) をまとめ、表 AP３－２に示す「石化協の事故評価基準（CCPS 評価法）」に基づいて、事故の大きさを定量的に評価することを発表した。

CCPS 評価法は米国化学プロセス安全センター（CCPS）が、「プロセス事故・災害の防止」

を目的に提案している評価方法で、「人の健康」、「火災・爆発」、「漏洩の潜在的影響」、「社会環境への影響」の４項目を４段階で評価した総合ポイント数で評価している。

例えば、１名死亡を、経済的損失１～10 億円と同等に評価としている。死亡損失金額は、英国安全衛生庁（HSE）が、１名の死亡を（£１、336、800perfatality一＝約２億円）と評価している[2]ことと概ね合致している。

なお、CCPS 評価法は強度レベルを４段階で評価しているが、石化協は軽微な事故を加えた５段階で評価している。

表 AP３－２石化協事故評価基準（CCPS 評価法）[1]

強度レベル（ポイント）	人の健康	火災・爆発	漏洩の潜在的影響	環境への影響（環境対応費用）	社会への影響（参考データ）
1(27)	複数死亡	直接被害額10億円超	複数死亡の可能性のある放出	2．5億円超	(参考;レベル2)
2(9)	１名死亡	1億～10億円	構外で死亡の可能性のある放出	１億～2.5 億円	
3(3)	休業災害	1千万～1億円	敷地内放出	1億円未満	(参考;レベル3)
4(1)	応急手当	250 万～1千万円	放出が二次防護施設内でしきい値以上	短期的な改善対応	(参考;レベル4)
5(0.3)	レベル４未満	250万円未満	レベル４未満	レベル４未満	ー

＜参考＞英国安全衛生庁（HSE）が化学プラントにおける経済的損失の損益分析に用いる Monetary[2]

Fatality	1、336、800 £
Permanently Injury	207、200 £
Seriously Injury	20、500£
Slightly Injury	300£

野口和彦氏は、化学プラントの事故における損害額と年間発生確率との関係をまとめて、図 AP３－１に示すリスク管理基準[3]を提案している。

図中に示す網掛け領域は、現状における事故発生状況を示しており、リスク低減の目標ラインとして、この網掛け領域の最も低いラインを示している。損害額 10 億円・年間発生確率 10^{-5}を基点とし、損害額 10 億円以下の領域は、年間発生確率と損害額とのバランスにおいて許容ラインを設定し、損害額 10 億円以上の領域では、年間発生確率が１０$^{-5}$以下のラインをリスク低減の限界ラインとしている。

この提案には、二つのポイントがある。

一つ目は、災害に伴う危害の大きさを経済的数値で評価していることである。

二つ目は、リスクの大きさは、通常、「危害の大きさ」×「発生確率」として評価するが、年間発生確率１０$^{-5}$以下の確率は、数値としては算出できるが、発生確率の妥当性を現実

には評価することが難しいとしていることである。

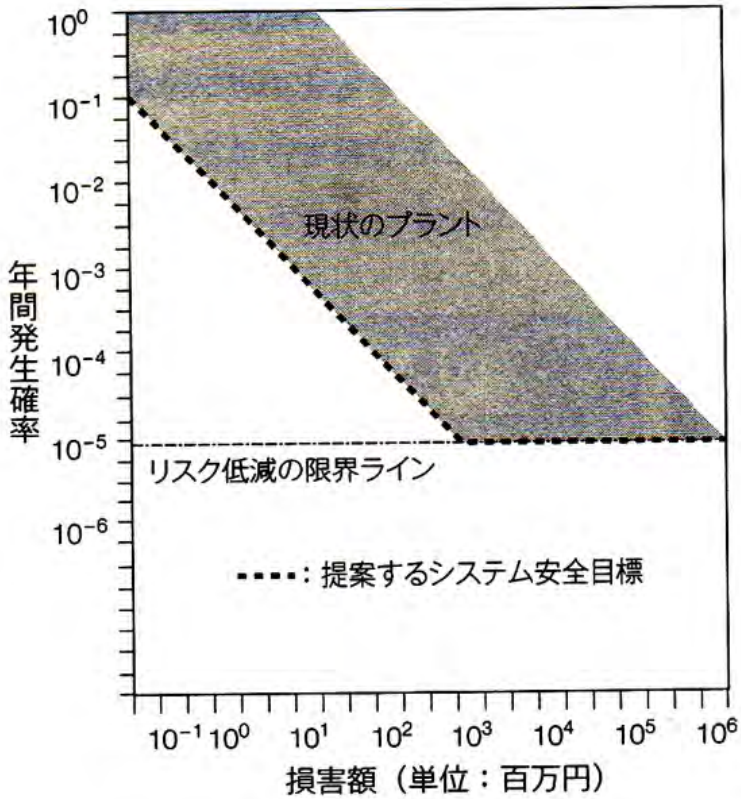


図 AP３－１　化学プラントの事故リスク状況とリスク基準[2]

（３） 重大事故に対する考え方

日本社会は「リスクがないこと」を安全と考え、「安全」か、あるいは「安全でない」の二つに区分して考える傾向が強い。一方、英国安全衛生庁（HSE：Health and Safety Executive）の考え方は、二つの点で相違がある。

一つ目は、安全を「受容できないリスクがないこと＝広く受け入れ可能なレベルにまでリスクが低減されていること」と定義している。

二つ目は、「広く受け入れ可能なリスク」と「許容できないリスク」との間には、リスクと便益との比較、並びに、リスク低減に要する費用と低減によって得られるメリットとの比較において、「ALARP（As Low as Reasonably Practicable：合理的に実行可能な限り低くするという原則)」の領域を考えている。

英国安全衛生庁（HSE）は、全てのリスクに対応して低減措置を講じることは、技術的にも経済的にも困難である。また、安全管理は、「人間は過ちを犯し、機械はいつかは壊れる」を前提としており、人間が過ちを犯すことなく、機械が壊れることがないならば、「リスクゼロ」があり得るかもしれないが、現実にはそんなことはあり得ないと考えている。

全てのリスクに対応できないとすれば、個々の事象のリスクの大きさを見積もり、その評価結果に基づいて、優先順序をつけてリスク低減措置を実施する。すなわち、重大事故の防止に重点を置いた安全管理を実施することになる。

英国安全衛生庁（HSE）は、1988 年に ALARP の原則を提案し、1999 年に「COMAH 規則：Control of Major Accident Hazard Regulation」を制定し、重大事故の防止を図っている。

この考え方は、1976 年 10 月にイタリアのセベソの農薬工場で爆発事故が起き、大量のダイオキシンが周辺地域の約 1800 ha に飛散したことに起因している。ＥＵは、1982 年セベソ指令、1996 年セベソⅡ指令、2012 年セベソⅢ指令を表 AP３-３に示すように発令し、ＥＵ各国に遵守することを要請した。

表 AP３-３　セベソ指令

1982年	セベソ指令	一定の産業活動に伴う重大事故の危険性に関する指令
1996年	セベソⅡ指令	危険物質による大規模災害の予防、発生した際の人間および環境への危害を最小限に食い止める ①安全管理計画書 ②緊急対策 ③近隣住民への情報提供 ④土地利用計画
2012年	セベソⅢ指令	大規模災害のリスク管理の強化 ①近隣住民への情報提供 ②指令対象施設に関する土地利用計画 ③産業施設の安全性を確保する検査基準

日本では、1976 年に「化学プラントにかかるセーフティ・アセスメントに関する指針」(4) が制定され、2000 年に改定された。

2000 年の改正ポイントは、新たな安全性評価手法が開発されてきたことに伴い、危険度を定量的に評価し、その評価に基づいてプロセス安全性評価手法を選定し、安全性を評価することである。

危険度評価は、物質、エレメントの容量、温度、圧力および操作条件の５項目により、災害の起こりやすさ及び災害が発生した場合の大きさを定量化し、それらの和によって危険度のランク付けを行い､危険度ランクに応じた安全性評価手法に基づいて評価している。(4)

2006 年労働安全衛生法が改正された。ポイントは、リスクアセスメント（ＲＡ）の実施を努力義務化したことである。

各企業に､努力とはいえ､ＲＡの実施を求めたことは､安全管理の大きな指針となった。ＲＡの考え方は、ＲＡを解説した「危険性または有害性等の調査等に関する指針　同解説（通称　リスクアセスメント指針)」(5) に記載されている。

重要なことは、日本においても、ALARP の原則の考え方が採用されていることである。

事故防止はリスク評価結果に基づいて実施し､「ランク４～５」の重大事故は、優先的にリスク低減措置を実施し､「ランク１」の場合は、必要に応じてリスク低減措置を実施する

ことが示されたことである。

この指針は化学プラントの安全目標に大きく関わってくる。該当部分を掲載する。

【指針】

10(２)(１)の検討に当たっては、リスク低減に要する負担がリスク低減による労働災害防止効果と比較して大幅に大きく、両者に著しい不均衡が発生する場合であって、措置を講ずることを求めることが著しく合理性を欠くと考えられるときを除き、可能な限り高い優先順位のリスク低減措置を実施する必要があるものとする。

【施行通達】

10　リスク低減措置の検討及び実施について

（２）　指針の 10(２)は、合理的に実現可能な限り、より高い優先順位のリスク低減措置を実施することにより、「合理的に実現可能な程度に低い」(ALARP) レベルにまで適切にリスクを低減するという考え方を規定したものであること。

なお、低減されるリスクの効果に比較して必要な費用等が大幅に大きいなど、両者に著しい不均衡を発生させる場合であっても、死亡や重篤な後遺障害をもたらす可能性が高い場合等、対策の実施に著しく合理性を欠くとはいえない場合には、措置を実施すべきものであること。

（３）　指針の 10(２)に従い、リスク低減のための対策を決定する際には、既存の行政指針、ガイドライン等に定められている対策と同等以上とすることが望ましいこと。また、高齢者、日本語が通じない労働者、経験の浅い労働者等、安全衛生対策上の弱者に対しても有効なレベルまでリスクが低減されるべきものであること。

【解説】

１　「合理的に実現可能な程度に低い：As Low as Reasonably Practicable (ALARP)」の考え方は、ISO・JIS や、英国安全衛生庁等において採用されている考え方である。

２　その内容は、英国等の運用では、指針の 10(２)に記載されているように、リスク低減に要する負担とリスク低減による労働災害防止効果を比較し、前者が後者と比較して著しく不均衡を欠くほど大きい場合には、それ以上の対策を要しないとする考え方である。ただし、「著しく不均衡」については解釈が示されていない。このため指針においては、指針の 10(１)にあるように、単に著しく不均衡が生じるのみならず、それによって措置を講じさせることが著しく合理性を欠く場合について、措置を講じなくてもよいという記載としている。

英国安全衛生庁（HSE）は、リスク低減に必要な費用が、低減されるリスク効果の 10 倍を超える場合は、
著しい不均衡とするガイドラインを示している。(2)

日本は、ALARP の原則に基づいてはいるが、【施行通達】にみられるように、両者に著しい不均衡を生じる場合であっても、死亡や重篤な後遺障害をもたらす可能性の高い場合は、リスク低減措置を実施すべきものと規定している。

「リスクアセスメント指針」は、致命的事故は、発生可能性の度合いがほとんどない場合においても、リスクランク『４』と評価し、直ちにリスク低減措置を講じるか、講ずるまでは使用しないことが望ましいとしている。(5)

例1：マトリクスを用いた方法

重篤度「②重大」、可能性の度合「②比較的高い」の場合の見積もり例

		負傷又は疾病の重篤度			
		致命的	重大	中程度	軽度
負傷又は疾病の発生可能性の度合	極めて高い	5	5	4	3
	比較的高い	5	4	3	2
	可能性あり	4	3	2	1
	ほとんどない	4	3	1	1

リスク	優先度	
4～5	高	直ちにリスク低減措置を講ずる必要がある。 措置を講ずるまで作業停止する必要がある。 十分な経営資源を投入する必要がある。
2～3	中	速やかにリスク低減措置を講ずる必要がある。 措置を講ずるまで使用しないことが望ましい。 優先的に経営資源を投入する必要がある。
1	低	必要に応じてリスク低減措置を実施する。

（４）化学物質の安全性（「リスクゼロ」に関する取り扱い）について

化学物質の安全性は、物質そのものではなく、その物質がどのような用い方をされるかによって決まる。

ほとんどの化学物質には、図 AP３－２に示すように、ある値の暴露量・摂取量に達するまでは体に影響を及ぼさないが、その値を超えると体に影響が出てくる。この境界点を「閾値」という。この関係を「用量―反応関係」といい、食品・医薬品や環境汚染物質等の安全性やリスクを評価する上で不可欠なデータである。

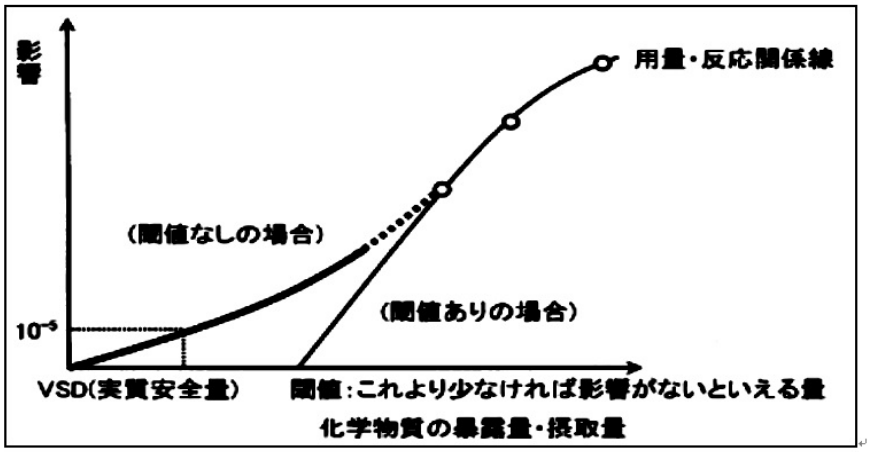


図 AP３－２化学物質の用量と反応の関係

一方、発がん性物質には、閾値のない場合が多いとされている。

「閾値なし」の場合は、少量の摂取であっても、体に何らかの影響がでることになるので、その物質を「使用しない」か、または「何らかの許容基準を設けて使用する」のいずれかを選択することになる。

アメリカは、1958 年「米国連邦食品医薬品化粧品法」の『デラニー条項』において、動物実験において発がん性が認められた物質を全面的に規制した。すなわちアメリカでも「ゼロリスク」という考え方を、かつては採用していた。

しかし、分析技術の進歩によって、かつては検出限界以下であった発がん性物質が検出できるようになった結果、多くの食品が規制対象になる不具合が生じた。そこで、1996 年食品保護法の制定とともに、『デラニー条項』が撤廃された。すなわち、図 AP３－２に示すＶＳＤ（実質安全量：Virtually Safety Dose）を定義し、ＶＳＤ以下ならば使用可能という考え方に転換した。

ＶＳＤは生涯 10^{-4}～10^{-6}の範囲で設定されるが、どの値にするかは、科学の問題ではなく、リスク管理ポリシーの問題といわれる。日本では中環審（1997 年)によって、ＶＳＤは生涯のがん発生確率 10^{-5}に相当する濃度とされている。(6)

低用量領域での評価において、0.1%の値を統計的に有意差有りと判断するには、数万匹のマウスを使った動物実験が必要になるので、0.1%以下の発生率の差を有意差識別することは事実上不可能とされている。

そこで化学物質の安全性は、高用量領域で測定した結果を、それ以下の低用量領域の値として外挿することになり、最終的にはリスク管理ポリシー問題として判断することになる。

（５） 社会的に許容されない事故

福島原発事故後、日本社会は「社会的に許容できない事故は発生確率が低くても起こしてはならない」という考えが強くなってきた。加藤尚武氏は、著書「災害論　安全性

工学への疑問」の中で、「確率論では、“低い確率で大きな損害＝高い確率で小さな損害”という等式を使ってきたが、この考え方では、異常な危険を事実上ゼロにはできない。損害が過度に大きい場合は、事実上ゼロにしなければならない」と提言している。(7)

化学産業において、1984 年 12 月 2 日深夜、インドの『ボパールの事故』が起きた。米のユニオン・カーバイド社の現地資本の殺虫剤工場から何千トンもの有毒ガスが流出し、インド中部のボパール町を一瞬のうちに汚染した。死者は、事故直後に 7000 人以上、その後 1 万 5000 人以上となった悲惨な事故である。

この事故は、化学産業の存続の是非が問われる社会問題になった。米国化学物質製造者協会（ＣＭＡ）は、1988 年化学産業の社会からの信頼を取り戻すために、レスポンシブル・ケア（ＲＣ）活動を開始した。ＲＣ活動は、化学産業が有益であることを訴え、有害性およびリスクに関する情報を市民に分かり易く説明する運動である。日本でも日本化学工業協会のもとで、ＲＣ活動が展開されている。

社会的に許容されない事故に関する米国とイギリスの考え方の例を紹介する。

事例１　米国労働安全衛生庁（OSHA：Occupational Safety & Health Administration）

OSHA は、緊急事態におけるアクションレベルを表 AP３-４のように示し、事故の影響の及ぶ範囲が、自社の敷地内、隣接地域、地域社会かによって、レベルを区分しており、災害が地域社会に及ばないようにしている。

表 AP３-４　OSHA の緊急事態のアクションレベル (8)

EAL	危機の大きさと影響範囲
レベル 1 警戒レベル(Alert)	限定された火災、爆発など災害で自社の組織で防災可能なレベル
レベル 2 自社内緊急事態 (Site emergency)	自社の隣接地域にも影響を与える火災、爆発、有害物の漏洩などの切迫した災害であるが、地域社会にまで及ぶことのないレベル。地域社会の消防、警察、医療機関などの支援が必要な危機レベル
レベル 3 緊急事態(General emergency)	最大の危機的事態の発生であり、災害が地域社会に及ぶ危機レベル

事例２　英国安全衛生庁（HSE）の土地利用計画

英国安全衛生庁（HSE）は、新設施設の土地利用計画が提出されると、当該施設から排出される有害物質の濃度によって、図AP３-３のように３つのゾーン(inner zone , middle zone , outer zone）を設け、そこにどのような施設（工場、住宅、小学校や老人ホーム、病院　など）があるかによって、有害物質が近隣の人々に対して及ぼすであろう危害とリスクを評価し、「その開発はやめた方がよいか否か」について助言している。(3)

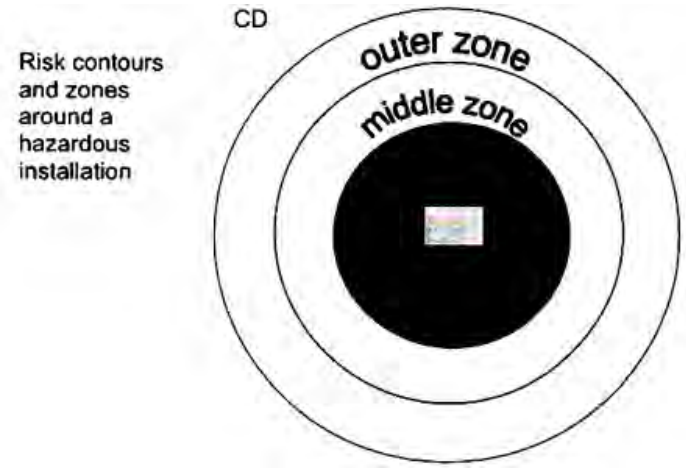


図 AP３－３　英国安全衛生庁（HSE）のリスク等高線［(3)］

二つの事例は、事故が起きた場合に、影響の及ぶ範囲が自社の敷地内に納まっているかどうかが、社会的に許容されるかどうかの基準になっていることを示している。

化学産業が存続していくには、このような考え方を取り入れて、自社の敷地外には危害を及ぼさないという考え方を徹底していくことが必要である。

２．事故が起きても、その影響を最小化すること

東日本大震災における原発事故は、リスクマネジメントの観点で考えると、いずれの原発も想定を超える津波に襲われたが、福島第一は津波によって全電源を喪失し致命的な事態となったが、福島第二、女川原発は、非常用電源設備が生き残ったために無事であったと捉えることができる。大前氏は、電源が一つでも生き残ったかどうかによってこの違いが生じたと述べている。［(9)］

これはリスクマネジメントの貴重な教訓である。リスク低減策を講じても、確率がゼロでない以上は、残存リスクが顕在化する可能性がある。津波が防波堤を超えることに対して対策が講じてあったかどうかの違いである。

化学プラントは、本来、危ない反応を取り扱っているので、リスク低減対策を講じても、リスクをゼロにすることはできない。福島原発事故を教訓に、種々の安全対策を講じるが、それでもなお、事故はあり得ると考えて、起きた場合の影響を極力小さくし、局所化する必要がある。

化学プラントは、これまで機能と経済性を重視して設計されてきたが、これからは設備の本質安全化を考えた設計が必要になる。

（１）　危険物保有量の最小化

化学プラントの事故は、反応暴走のような事態になると制御することができない。そこで、設計段階から、仮に、爆発事故が起きたとしても、その影響が小さくて済むように取り組むこと、すなわち、装置内に内在する危険物質の保有量を極力小さくすること

が求められる。

バッチ反応は、反応釜に反応開始時から終了時までの原料を保有するために、危険物保有量が大きくなるが、連続式反応方式を採用すれば、プラント内の危険物保有量を少なくできる。同様に、液相反応から気相反応に変更することによって、設備の本質安全化が図られる。

例えば、ニトログリセリンは、かつては、バッチ反応で製造していたために危険性が極めて高かった。そこで、インジェクター方式の反応器を採用して接触効率を良くした結果、装置内滞留時間を 120 分から２分に短縮できたので、生産が可能になった。[10]

（２） 影響の及ぶ範囲の局所化

化学プラントでは、装置内で異常な圧力が発生した場合に備えて、安全弁や破裂板を設けている。これは意図的に装置内に弱い箇所を作り、異常圧が発生すれば、安全弁や破裂板から内容液が外部に放出されるので、影響の及ぶ範囲を局所化することができる。

装置の全てを頑丈に作ることは、それに耐えられない圧力が生じて爆発すれば甚大な事故になる。リスクを完全に抑え込むと考えるのではなく、影響の小さなうちに、大事に至らぬようにする考え方が重要である。

３．化学プラントの安全目標

化学プラント安全目標（案）を下記に示す。

１．「事故ゼロ」は理念目標であるが、現実に実現可能な目標とする。
２．危害評価は、労働安全、経済的損失並に社会への影響を含めて評価する。
３．重大事故の防止を図る。
リスクアセスメントを実施し、評価に基づいて、優先順序をつけて対応する。
４．社会的に許容されない事故（致命的リスク）は、たとえ、発生確率が小さくとも避ける。その際に、地域社会に影響を及ぼさないようにする。
５．仮に事故が起きても、被害を最小化するように、設計段階から取り組む。
　① 危険物保有量の最小化
　② 影響の及ぶ範囲を局所化

最後に、事故の再発防止を図るには、当事者からの有用な証言を得ることがどうしても必要である。再発防止に有用な証言を得るためには、不幸にして、過失を犯すことになった事故の当事者を刑事罰として罰するのではなく、そこから得る情報を基に、事故の背景要因を糾していくことが必要である、そして、事故情報を社会共有の財産として活かしていくことが必要である。

（１）2013 年７月４日　石油化学工業協会　「産業保安に関する行動計画」
http://www. jpca. or. jp/pdf/20130722news. pdf
（２）Ｔ．Ｅ．Maddison：”The Control of Major Accidents in the Chemical Industry

-European Legislation and the Use of Appropriate Risk Assessment Techniques”
（３）野口和彦：「リスクマネジメント　目標達成を支援するマネジメント技術」、P117、日本規格協会(2009 年)
（４）平成 12 年３月 21 日　労働省労働基準局長「化学プラントにかかるセーフティ・アセスメントに関する指針」
（５）平成 18 年３月　「危険性又は有害性等の調査等に関する指針・同解説」厚生労働省安全衛生部安全課
（６）花井荘輔：「化学物質のリスクアセスメント」9－2、丸善株式会社（2003 年）
（７）加藤尚武：「災害論―安全性工学への疑問」世界思想社（2011 年）
（８）松本俊次；「リスクベースド・アプローチによる機械安全の現状の今後の課題」、労働安全衛生研究　Ｖｏ13、Ｎｏ１　ｐ41　（2010）
（９）大前研一：原発再稼働　最後の条件」小学館（2012 年）
(10) Ｔ．クレッツ、(訳)長谷川和俊:「化学プラントの本質安全設計―ユーザー優先の装置をつくるために一」、ｐ38～ｐ42、化学工業日報社（1995 年）

AP４．機械における安全

１．機械安全の経緯

機械類での安全性（機械安全）に関しては、開発当初から多くの事故を経験していた。例えば、機械式のプレスで指を切る事故はしばしば発生していた。特に、大きなプレス機械では、人命を損なうこともあった。また、例えば、蒸気や高圧のボイラーやタンクでは、圧力が上がり過ぎて爆発事故を頻繁に起こし、大きな災害を経験していた。これらの機械類で安全を確保するために、例えばプレス機械では、柵でプレスの入り口をふさぎ、柵が降りている時しか、従って人間の手が入らない時しか、プレスは稼働できないようにし、かつプレスが止まっている時にしか柵は上がらない、従って手は入らないという構造を作ることから、また、ボイラーでいえば、弱い部分を作っておいて、圧力が高くなると、本体は爆発する前に弱いところが噴いてしまうような安全弁を備える構造にすること等から、始まった。このように、一般的に機械安全は、構造的に安全を作る、従って満たすべき構造を仕様規格として決めるところから始まっている。これまでの事故の経験と安全技術の開発に基づき、現在では、機械安全の規格類に関して、統一した考え方の下に階層化されるに至っている。（図 AP４－１参照）。すなわち、数多くの個別機械の安全規格（C 規格）の上に、広範囲に使える安全装置等のグループ（B 規格）が置かれ、更に全ての規格に利用可能な基本安全規格（A 規格）を最上位にして、ISO/IEC ガイド 51（安全の規格作成のためのガイドライン）に従い、階層化されている。

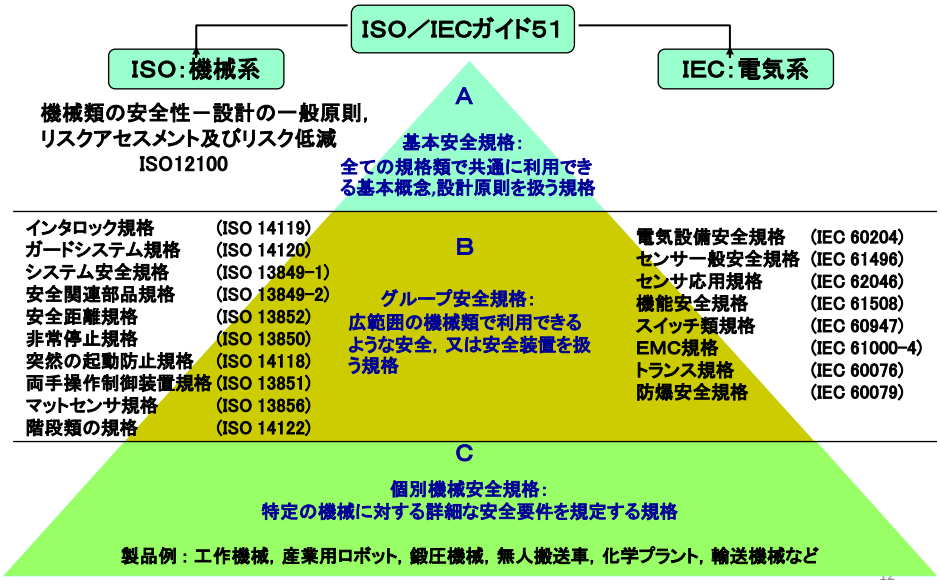


図 AP４－１　国際安全規格の階層化構成

一方、最近は、安全を確保するための制御装置や各種の安全装置にコンピュータ等の電

子機器を用いることで、安全が実現されるようになってきた。それら装置が正しく機能している間は、安全は確保されていると考えられるので、当初の構造で安全を実現するという発想から、信頼性に基づいて確率で安全を評価するという発想が重視されつつある。しかし、もちろん両者は無関係ではない。

２．構造安全と確率安全

故障しないように信頼性高く作るという概念(確率安全)と、構造で安全を実現し、故障したら安全側になるような構造に作るという概念(構造安全)は、根本的に異なった概念である。しかし、安全性を高める技術としては、両者とも必須である。なお、故障しないように信頼性高く作るためには、二つの考え方がある。一つは、コンポーネントそのものが故障しないように高信頼に作るフォールトアボイダンスという技術であり、品質管理や物理的な特性の向上によって実現される。もう一つが、冗長系（多重系）を用いて、全体として信頼性を上げるフォールトトレラントの考え方である。フォールトトレラントには、構造を工夫することで信頼性を上げるという、構造と確率の両方が考慮されている。

３．安全目標の表現方法の形式

安全目標といっても、その表現の方法によって、いくつかに分類できる。最も標準的な方法は、確率論に基づいて、数値的に安全目標を与えるものである。一方で、言葉で表現された定性的な安全目標もあり得る。更に、安全確保のために満たすべき構造等を規格や基準として決めるのも一種の安全目標である。これは、仕様基準的な安全目標と呼ぶことができよう。機械安全における安全目標は、前述のように、当初、満たすべき要件を示し、それを満足する構造を明記した仕様基準的な安全目標から始まった。その後、確率的な安全目標が提案され、最近では、両者を連携する試みが行われている。

４．カテゴリーという安全目標の考え方

機械にける安全目標の特徴は、危害のひどさの程度ごとに安全目標を構造として、又は確率として定めていることである。この状況を国際規格 ISO13849-１ 2006(JIS B 9705-１：機械類の安全性－制御システムの安全関連部―第１部設計の一般原則）で見てみる。この規格は、機械における制御システムの安全関連部についての規格である。すなわち、本来の機能を果たしている制御対象のシステムに対して、それを安全に制御する安全関連部、すなわち安全制御や安全装置等に対する規格であり、重要性に鑑みて(すなわち、それが正しく機能しなかった時の危害のひどさの程度を考慮して)、その構造の目標をカテゴリに分けて掲げている。カテゴリが大きいほど、機能しなかった時の危害のひどさの程度が大きいとしている。表 AP４-１は、この形での安全目標を表しているもので、要求事項要約ではあるべき構造が言葉として表されていて、その機能が失われて障害が発生した時のシステムの挙動を記してある。同表で、安全性達成のために使用される原則とは、主として安全が信頼度で達成されるのか、構造で達成されるのかについての注釈である(安全は、

基本的には構造かまたは信頼性で達成されるという事実に基づいている）。すなわち、カテゴリＢと１は、主としてコンポーネントの信頼性に基づいており、カテゴリ２以降は、構造に基づいて安全が確保されている。

表 AP４－１：カテゴリと要求事項（ISO 13849-1 2006）

カテゴリ	**要求事項要約**	**システム挙動**	**安全性達成のために使用される原則**
B	コンポーネントのみならず SRP/CS*及び／又は保護設備は，予想される影響に耐えるように，関連規格に従って設計，製造，選択，組立，組み合わされること。基本安全原則を用いること。 ＊制御システムの安全関連系：Safety-Related Part of a Control System	障害発生時，安全機能の喪失を招くことがある。	主としてコンポーネントの選択により特徴づけられる。
1	B の要求事項が適用されること。“十分吟味されたコンポーネント”及び“十分吟味された安全原則”を用いること。	障害発生時，安全機能の喪失を招くことがあるが，発生する確率はカテゴリ B より低い。	主としてコンポーネントの選択により特徴づけられる。
2	B の要求事項及び“十分吟味された安全原則”の使用が適用されること。安全機能は機械の制御システムにより適切な間隔でチェックされること。	チェックの間の障害の発生が安全機能の喪失を招くことがある。 安全機能の喪失はチェックによって検出される。	主として構造により特徴づけられる。
3	Bの要求事項及び“十分吟味された安全原則”の使用が適用されること。安全関連部は次のように設計されていること。 ―いずれの部分の単一障害も安全機能の喪失を招かない。かつ ―合理的に実施可能な場合は常に単一障害が検出される。	単一障害発生時，安全機能が常に機能する。 全てではないが障害のいくつかは検出される。 検出されない障害の蓄積で安全機能の喪失を招くことがあ	主として構造により特徴づけられる。

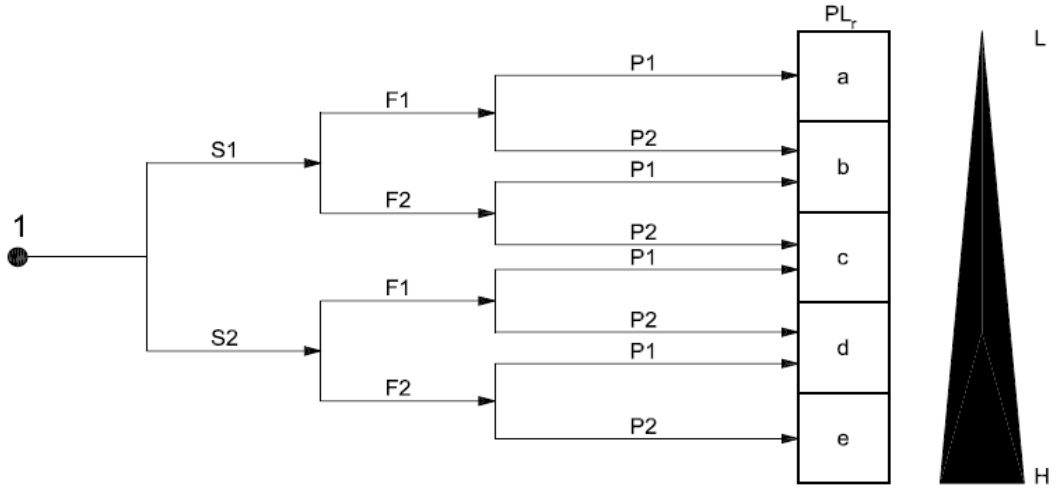
		る。	
4	Bの要求事項及び“十分吟味された安全原則”の使用が適用されること。 安全関連部は次のように設計されること。 ―いずれの部分の単一の障害も安全機能の喪失を招かない。かつ ―単一障害は，安全機能に対する次の動作要求のとき，又はそれ以前に検出される。それが不可能な場合，障害の蓄積が安全機能の喪失を招かないこと。	障害発生時，安全機能が常に機能する。 蓄積された障害の検出は，安全機能の喪失の可能性を減少する（高DC）。 障害は安全機能の喪失を防止するために適時検出される。	主として構造により特徴づけられる。

５．パフォーマンスレベルという安全目標の考え方

一方、安全関連部の満たすべき危険側故障の発生率の少なさがパフォーマンスレベル(PL)として示されている(表 AP４－２)。図 AP４－２に、PL の決定方法の例を示す。これは、リスクの大きさに従い、そのような危害が発生しないようにするために、安全関連部の信頼度の数値を決めているものである。この各 PL を実現するための構造のランクが表 AP４－１のカテゴリであるという関係にある。表 AP４－１のカテゴリーと表 AP４－２の PL の関係は、（ここでは、対応表は省略するが）色々な場面や条件を想定して検討されている。表 AP４－２によれば、死亡事故の可能性がある場合には最も大きなリスクであるので、それを防ぐための PL は e のレベルである必要があり、発生確率が 10^{-7}/時から 10^{-8}/時ということは、約 10^{-4}/年となる。

表 AP４－２ パフォーマンスレベル（PL）（ISO 13849-１ 2006）

PL	時間当たりの危険側故障発生の平均確率 (PDF) ［1/h］
a	$10^{-5} \leqq$ PDF $< 10^{-4}$
b	$3 \times 10^{-6} \leqq$ PDF $< 10^{-5}$
c	$10^{-6} \leqq$ PDF $< 3 \times 10^{-6}$
d	$10^{-7} \leqq$ PDF $< 10^{-6}$
e	$10^{-8} \leqq$ PDF $< 10^{-7}$
注記　時間当たりの危険側故障の平均発生確率に加えて，PL を達成するために，他の方策も必要とされる	



記号の説明

1　リスク低減に安全機能の寄与度を評価するための開始点

L　リスク低減への寄与度 “低”

H　リスク低減への寄与度 “高”

PLr　要求パフォーマンスレベル

S　傷害のひどさ

S１　軽症（通常，回復可能な傷害）

S２　重傷（通常，回復不可能又は死亡）

F　危険源への暴露頻度及び／又は時間

F１　まれから低頻度，及び／又はさらされる時間が短い

F２　高頻度から連続，及び／又はさらされる時間が長い

P　危険源回避又は危害の制限の可能性

P１　ある条件では可能

P２　ほとんど不可能

図 AP４－２ 安全機能に対する要求 PL_r決定のためのリスクグラフ （ISO 13849-１ 2006）

６．安全機能と機能安全

安全機能とは、システムが実現すべき本来の機能とは別に、安全を達成するための機能をいう。機械安全の規格である制御システムの安全関連部（ISO13849-1, JIS B 9705-1）では、「故障がリスクの増加に直ちにつながるような機械の機能」と定義されている。安全機能には、システム本体が実現している安全機能（本質的安全と言われる）と、安全防護柵や安全装置等の付加的に追加された安全方策が果たす安全機能とがある。機能安全とは、後者の安全機能、すなわち、本来の機能を果たしている制御対象を安全に制御する装置や安全装置が果たす安全機能をいう。機能安全は、主として、ソフトウエアとコンピュータを含む電子機器等が主要な安全機能を実行しているような大規模で複雑なシステムの安全性を対象としている。制御システムの安全も機能安全も、主として、本質的安全設計の次に施すべきとされる付加的安全方策が果たす安全機能を対象としていると考えることがで

きる。

７．機能安全における安全目標

機能安全の規格（IEC61508）では、安全関連部の役割を、低頻度作業要求モードと、高頻度作業要求又は連続モードに分類して､満たすべき機能失敗確率又は危険側故障確率を、安全インテグリティレベル（SIL)として定めている(表 AP４－３)。ここでは、最も高い SIL は４であり、高頻度作業要求又は連続モードとすると、発生確率が 10^{-8}/時から 10^{-9}/時となり、それは約 10^{-5}/年となる。PL と SIL の関係の例が表 AP４－４のように示されている。ここでは、SIL が４に対応する PL のレベルは存在しない。

表 AP４－３　SIL(安全インテグリティレベル)（IEC61508)

SIL	低頻度作動要求モード運用（注１）	高頻度作動要求又は 連続モード運用（注２）
4	10^{-5}以上10^{-4}未満	10^{-9}以上10^{-8}未満
3	10^{-4}以上10^{-3}未満	10^{-8}以上10^{-7}未満
2	10^{-3}以上10^{-2}未満	10^{-7}以上10^{-6}未満
1	10^{-2}以上10^{-1}未満	10^{-6}以上10^{-5}未満

注1　作動要求当たりの設計上の機能失敗平均確率
注2　単位時間当たりの危険側故障確率[1/時間]

33

表 AP４－４ パフォーマンスレベル（PL）と安全インテグリティレベル（SIL）との関係（ISO 13849-１ 2006)

PL	SIL 高／連続運転モード
a	―
b	1
c	1
d	2
e	3

８．あとがき

カテゴリを中心とした従来の機械安全は、構造安全の考え方が中心であり、最近注目を集めている機能安全は、確率安全の考え方が中心となっている。現実の安全性確保には、両者は密接にして不可分の関係にある。

AP５．自動車交通の安全

１．はじめに

警察庁交通局の 2012 年中の交通事故統計によると死傷者事故件数は 665,138 件と 2004 年度のピーク時（952,191 件）に比べ３割減少し、死者数は 4,411 人で 1970 年のピーク時（16 ,765 人）に比べ約７割減少している。これは近年の自動車の安全技術、救急医療、道路環境、行政、等々の改善効果のたまものではあるが、痛ましい事故は後を絶たず、更に超高齢化社会を迎えて新たな課題も取り上げられるようになり、交通事故防止対応は大きな課題として残されている。

今回、日本学術会議で議論している工学システムにおける安全目標の構築と課題について、自動車交通の立場から現状を紹介したい。特に、原子力発電事故などに比べて一回の事故の被害は少ないが、事故形態はパターン化できそれらを集約すると数多い犠牲者が同じパターンに数えられる。自動車交通の安全問題は工学システムの事故形態として、多様な学問分野（機械、電気、情報、土木、人間工学等）と多様な行政（内閣府、国土交通省、経済産業省、総務省、警察庁等）に関わるため、様々な角度・視点からの考察が欠かせない。

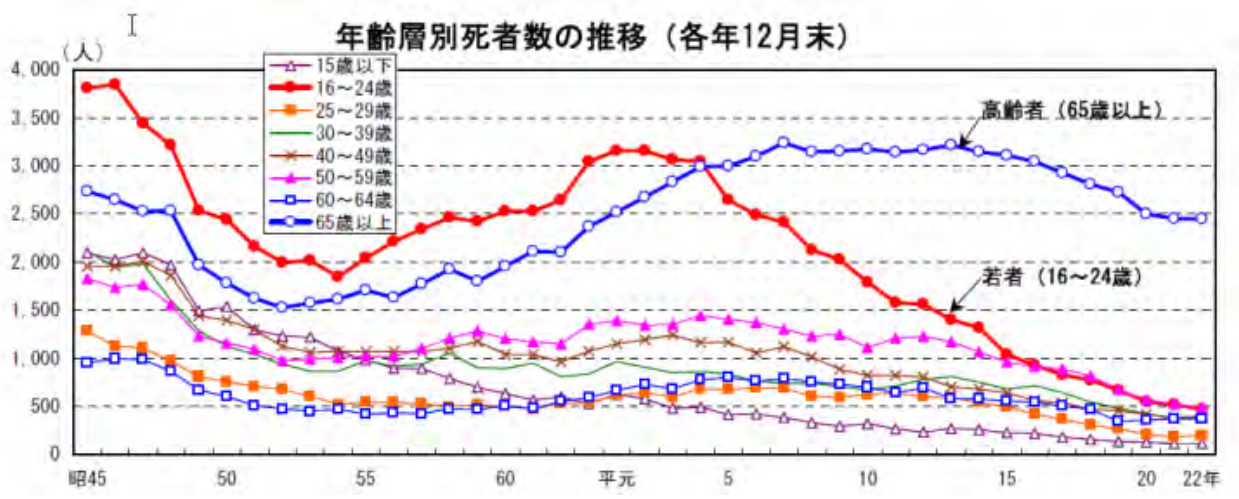


図 AP５－１　年齢別死者数の推移

２．自動車交通における事故の現状

最近の自動車事故において特筆すべき点は、高齢者事故死者、歩行中の事故死者、自転車乗車中の事故死者が多いという傾向がある。まず高齢者については、図 AP５－１に示すように 65 歳未満の年齢層の死者数が著しく減少しているのに対して、65 歳以上の高齢者の死者数がそれほど減少していない点である。これは高齢者人口が急激に増えていることと関連があるが、単純に年齢構成だけでは計り知れない要因を含んでいる。図 AP５－２は、自転車乗車中および歩行中の年齢層別死者数の割合であるが、62%、71%以上と高い割合

を示している。これは交通事故形態が変わってきていることを物語っている。図 AP５-３に示す交通事故類型別データによると、運転中の事故死者数が減少しているのに対して、歩行中死者数が相対的にそれほど減少していないために、数字的には逆転してしまっている。今後高齢者人口の割合が増々増えることを考えると、新しい観点からの安全対策が必要なことが分かる。

３．交通安全基本計画

内閣府の中央交通安全対策会議において、５年毎に交通安全基本計画が作成されている。第８次交通安全基本計画（H18～H22 年）としては、死者数 5500 人以下、死傷者数 100 万人以下の数値目標が立てられたが、平成 20 年事故統計において、死者数 5155 人、死傷者数約 96 万人ということで、数値目標が前倒しで達成されている。

国土交通省自動車局（安全政策課）では事業用自動車を対象として、平成 22 年に今後 10 年間で、事故死者数と死傷者数を半減、飲酒運転ゼロという事業用自動車総合安全プラン 2009 がたてられ､安全マネージメントを含めて､さまざまな安全対策が立てられている。

第９次交通安全基本計画（H23～H27 年）では、① 平成 27 年までに 24 時間死者数を 3,000 人以下（30 日以内死者数は約 3,500 人）、② 平成 27 年までに死傷者数 70 万人以下という数値目標が立てられている。この目標に対して、安全教育、安全技術、インフラ整備等の観点からの対策が必要であり、国土交通省としては ASV(Advanced Safety Vehicle)等の車両安全対策により死者数 4863 人（平成 22 年）から 1000 人削減（平成 32 年）を目標として掲げている。この数字が達成されれば、人口 10 万人当たりの死者数が 2.5 人程度となり、世界一安全な国に位置づけられることになる。

４．交通事故ゼロに向けた提言とその後

平成 20 年６月 26 日、日本学術会議「工学システムに関する安全・安心・リスク検討分科会」として、日本学術会議提言「交通事故ゼロの社会を目指して」を公表した。その骨子は、①ドライブレコーダの活用強化、②ヒューマンファクタ基礎研究の推進、③予防安全技術の研究開発と普及促進、④意識向上・交通安全教育の徹底化、であり、提言で示した考え方が学術活動としても定着しつつある。【提言要旨を参考されたい】

しかしながら、2012 年に７名の死者が発生した関越自動車道での高速ツアーバス居眠り運転事故や、2014 年に睡眠時無呼吸症候群（ＳＡＳ）の簡易検査で要経過観察と診断されていた夜行バスの運転手が、北陸道ＳＡでトラックに追突した事故、また歩行者列に突っ込む事故が後を絶たず、事業者の運行管理を含めて安全対策の重要性が認識させられている。

また安全技術面で言えば、提言で示したように、事故を未然に防ぐための予防安全技術の開発と普及が加速される必要があろう。事故原因の 90%程度以上の多くがヒューマンエラーに起因しているとされ、将来的には部分的な自動運転の出現が期待されるが、当面は予防安全技術、運転支援システムのできるだけ早い普及が望まれる。

安全運転のための運転支援・教材作成も進められており、安全運転診断ソフト作成、安全運転テキスト教材作成、危険予知トレーニングのためのヒヤリハットデータベース画像教材の作成、等が行われている。

５．ドラレコ活用・ヒヤリハットの法則

自動車技術会では2004年から3年間に渡り国土交通省の委託テーマ「ヒヤリハット分析によるASV等の効果把握・予測等の検討調査」でドライブレコーダを用いた研究を行ったが、そこで培ったヒヤリハットの収集・登録手法を基に、予防安全などの研究用としてのデータベース構築に努めた。2010年11月に、データの収集・登録・運営業務を自動車技術会から東京農工大学に新設したドライブレコーダデータセンターに移設した。データ数は2013年3月までに78,300件のヒヤリハットデータ（約400件の事故を含む）が登録されており、これは世界でも他に例を見ない大規模なデータベースとして、海外からも注目されている。

ヒヤリハットに関しては、従来から労働災害の経験則である「ハインリッヒの法則」がよく引き合いに出される。交通事故災害の場合はその関係がどうなっているのか、ドラレコで収集したヒヤリハットデータを基に検討した。（表 AP５－１参照）

表 AP５－１　人身事故・損害物数・ヒヤリハット数の比率（概数）
(H22 年統計)（死者数 4863 名(H22),4612(H23)）

	人身事故件数	事故損害物数	ヒヤリハット数
警察庁	73 万件/年		
損保協会		722 万件/年	
農工大 DB		618 件	17,700 件
比率	1	10	300

参考文献:永井、ドライブレコーダによるヒヤリハット分析と熟練ドライバモデルの開発、自動車技術、Vol.67 No.12、特集「自動車安全の医工連携」、2013.12

６．安全技術の評価基準

自動車の安全技術の向上が図られているが、開発に関しては衝突安全と予防安全とに分けることができる。衝突安全技術としてはエアバッグ・シートベルト・衝撃吸収ボディ等があるが、その性能評価の数値としては人体への衝撃値（衝撃加速度）があげられる。いっぽう、予防安全技術における数値目標は、事故をどの程度未然に防ぐことができるかの評価であるため衝撃値は意味が無く、現状では定まった評価基準は無いため早急な定量的評価法の確立が望まれる。特に一般ドライバにとっては、これまで実施されてきた衝突安全技術のアセスメントだけではなく、緊急自動ブレーキシステムなどの予防安全技術のアセスメントの結果が、安全な車に対する目安になると期待される。

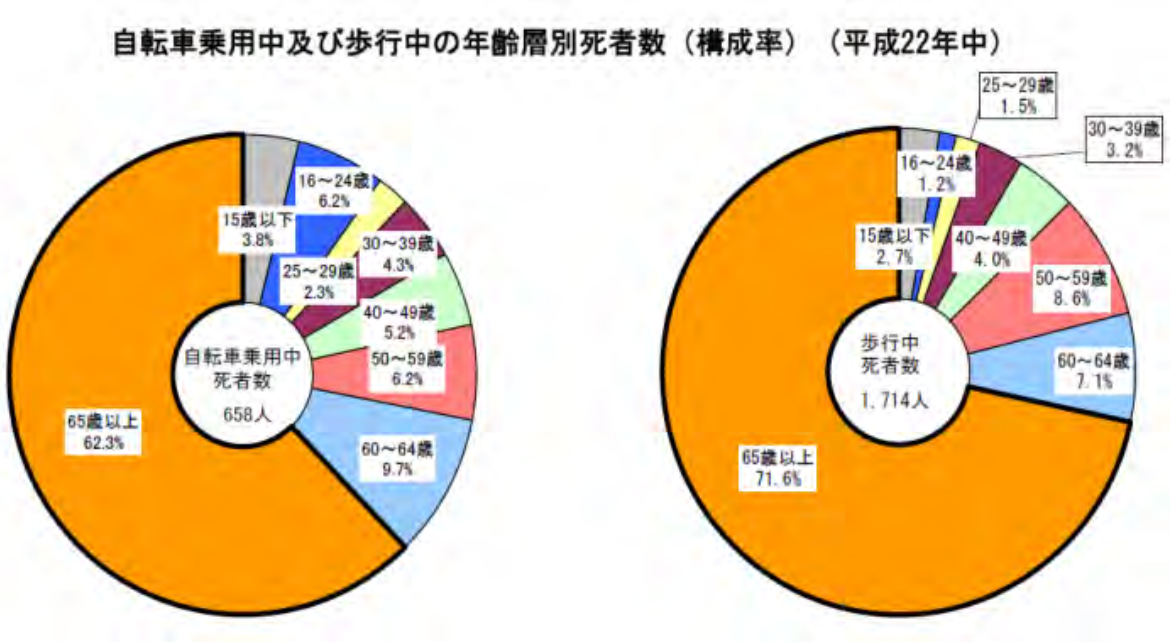


図 AP５－２　自転車乗車中・歩行中の高齢者死者割合

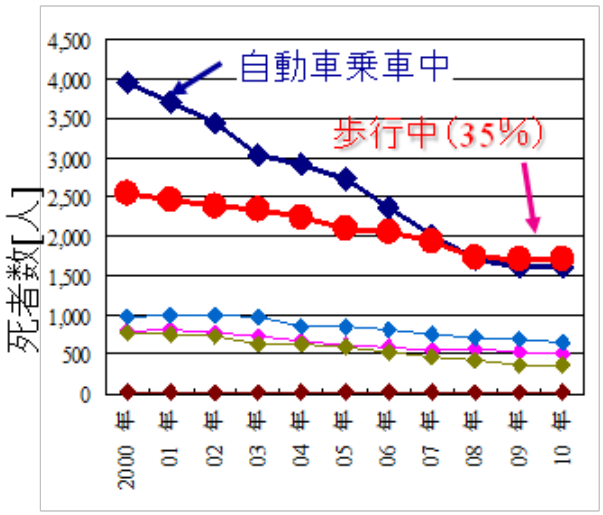


図 AP５－３　類型別交通事故死者数

【参考】提言「交通事故ゼロの社会を目指して」

日本学術会議・総合工学委員会・機械工学委員会合同
工学システムに関する安全・安心・リスク検討分科会
平成 20 年（2008 年） 6 月 26 日

要旨

１　作成の背景

交通事故による死者数は、1993 年以降減少傾向を維持し年間１万人台から 2007 年には 5,744 名と減少してきたが、自動車交通事故の経済損失は 6.7 兆円とも言われ、依然として大きな社会問題となっている。種々の施策等の対策の効果が得られているものの、究極目指すべきところである事故の無い社会には程遠い。このため、飛躍的な事故死傷者数の減少、究極にはゼロ化を目指すためには何をすべきか、等について検討した。

２　現状及び問題点

交通事故は、物損も含めれば年間約 800 万件にものぼり、日常茶飯事になっているが、国民の意識としては他人事であり、遭遇すれば運が悪いと感じる傾向がある。自動車の利便性と引き換えに、事故のリスクはやむを得ないという受け止め方もある。しかしながら、年間 5,000 名以上の尊い命が失われており、当事者およびその家族に与えるダメージは計り知れない。

一方、自動車技術は年々進歩してきており、予防安全技術の事故予防効果が認識され、一部市販化されているものの普及はなかなか進んでいない。また近年、事故やインシデントの客観データを記録できるドライブレコーダ等の機器が急速に普及する情勢になってきており、安全技術や安全教育への取り組みに対する期待が高まっている。

このような背景のもとで、事故の発生を定量的に捉えることによって科学的アプローチにより防止策を考え、人間心理に踏みこんだ検討なども行いつつ、究極には死傷者ゼロを目指すための、総合的アプローチをオールジャパン体制で構築していくことが重要である。歩行者や自転車も含めた自動車交通の特殊性や国民の意識等を考慮に入れ、科学的アプローチによる予防安全技術と教育啓発等の両面で対処していくための諸課題の抽出とロードマップについて議論を行いまとめてきた。

３　提言の内容

（1）ドライブレコーダの活用強化

事故の瞬間の映像を収録できるドライブレコーダ等の車載記録装置により事故原因が的確に分析できるようになれば、道路交通における「ひと、みち、くるま」の安全対策にも的確に反映させることが可能となる。事故に陥りやすい道路環境、ヒューマンエラーを起こしやすい走行条件、運転者の運転特性、を分析することにより、人間特性の基礎研究、安全運転教育、安全技術開発、道路環境の改善、に幅広く活かすべきである。

（2） ヒューマンファクタ基礎研究の推進

事故を未然に防ぐことを目的とした予防安全研究に際して、人間工学、心理学、医学、脳科学を融合した人間研究の展開が望まれる。人間行動学に関するヒューマンエラーモデル構築、異常に至る兆候をいち早くセンシングする新しい手法の導入、ストレス、居眠り、認知・判断のメカニズムの解明などの基礎研究を推進すべきである。また事故原因の大きな割合を占めてくる、高齢者、歩行者および自転車に関する取り組みを今後強化すべきである。

ヒューマンファクタ研究が大規模に展開できるように、学際的な研究組織の立ち上げと、そこで使えるようなドライブレコーダ等によるフィールドデータの収集・分析を集中的に行える体制の構築が望まれる。事故やヒヤリハットデータを多数集め、研究に使えるようにする仕組みづくりを進めるため、オールジャパン体制の研究組織を構築すべきである。

（3）予防安全技術の研究開発と普及の促進

人間はミスをするものであるという前提で、認知支援、判断支援、操作支援等々のドライバ支援技術を確立して行く必要がある。高度な運転支援技術に関しては、人間操作と機械支援との協調関係および社会的受容性の評価が重要となる。更に、将来的にはロボット技術の導入による新しい運転支援、限定的な自動運転の導入も検討すべきである。

交通事故の多くは、不適切な速度での走行が事故発生や被害度増大につながっている。被害軽減ブレーキは追突事故による死傷者を10分の1程度に削減できると期待されているが、そもそも速度規制を着実に実行すれば、事故防止や衝突速度低減につながる。ISA（インテリジェント・スピード・アダプテーション）を始めとする安全機器開発、導入の効果評価、社会的受容性評価のための社会実験を実施すべきである。

（4）道路交通構成員全体の意識向上・教育の徹底化

ドライブレコーダにより取得したフィールドデータや運転シミュレータを活用した教育プログラムあるいは運転診断ソフトが開発され、免許取得時や更新時に、十分実感を伴うような形で教育が実践される体制の構築を検討すべきである。また、子供から高齢者まで、自動車や二輪車等による交通とどのように向き合っていくかをきちんと教育していく必要がある。特に無秩序な自転車に関して、将来的には車両の登録制や運転者の免許制などの制度改革も含めマナーとスキルの向上を考えていくべきである。

以上の提言をもとに、交通事故の無い社会を目指していくためには、自動車交通の特殊性を考え、事故はやむを得ないとか事故に遭ったら運が悪いと言ったこれまでの考えを改め、あらゆる努力をしようという国民的なコンセンサスが最も重要である。

AP６．鉄道における安全

１．鉄道における安全

鉄道における安全性の問題は、輸送事業における最優先課題として鉄道事業者を始め、鉄道車両、施設などの関係事業者の努力により、我が国においては、きわめて高い水準にある。鉄道システムは、線路などのインフラ設備、車両の運行管理、車両の維持管理、信号制御、乗務員や駅業務など、鉄道輸送にかかわる基本的な業務が一元管理されていることが、高い安全性を保っている一つの理由と考えられる。

明治５年に鉄道が海外技術を導入して開業以来、国産技術の育成を進め、我が国独自の技術により大成された新幹線は、乗客の死亡者がゼロという極めて安全性の高いシステムを構築してきた。

新幹線の高い安全性は、過去に経験した重大事故に学ぶことと、総合的な取り組みによると思われる。現在でも、在来線における重大事故を教訓に、安全性のより一層の向上に取り組んでいる。

２．安全性向上の経緯

新幹線の高い安全性は、時間的にも空間的に専用の交通路を独占的に確保していることが挙げられる。踏切を排除し、高架軌道による外的要因を極力排除し、他の交通システムとは完全に切り離されている。定期的な車両や施設の保守点検も徹底されており、経験と技術的な取り組みにより、メンテナンスの基準が定められ、体系化されてきている。夜間に線路の保守作業を行っているが、時間的な占有を保つために、営業列車が走行する前には、確認車とよばれる専用車両を走らせ、異常がないことを確認したうえで、営業列車が走行する。

信号システムもコンピュータ制御によりフェイルセーフ機能を考慮した極めて安全性の高いシステムが導入され、デジタル技術の進化とともに、アップグレードされている。ヒューマンエラーによる事故防止のためには、例えば信号の見落としを防ぐための車内信号方式の採用や、ATC による自動制御システ、列車集中管理システムが導入されている。

このような高度な安全システムは、在来線における多くの痛ましい重大事故の経験をもとに、進化してきている。いくつかの例を以下にあげる。

（１）桜木町列車火災事故

1951 年４月に発生した「桜木町列車火災事故（死者 106 人）」は、直流 1500V の架線にパンタグラフが異常に接触したことから、大電流が車両に流れ、火災を引き起こしたものである。車体からの脱出過程にも問題があり、多くの乗客が焼死する痛ましい事故となった。この教訓から、車両の不燃化対策が進むともに、車両からの避難に対する検討も進み、隣の車両への移動が可能な貫通路の設置や窓やドアの扱いなどが工夫されるに至った。

（２） 三河島列車衝突事故

1962 年５月に発生した「三河島列車衝突事故(死者 160 人)」は、貨物列車と２本の通勤列車の３重衝突事故であり、安全対策が進んだという観点からは、重要な事故である。発端は、貨物列車が赤信号にかかわらず盲進し、合流する本線を支障して、並走する通勤電車に衝突してしまった。この側線には予防安全の仕組みがあり、信号無視が生じても本線を支障しないような工夫があったものの、防ぎきれず、さらに、衝突後に対抗列車に対する列車防護の不備から、３重衝突を許してしまった。すなわち、(１)貨物列車の信号無視（機関士）、(２)並走旅客電車に衝突、(３)列車防護の不備（車掌、駅員、信号手）、(４)対向列車の衝突・転覆、(５)避難した乗客の被害と連鎖的に事故の被害が拡大した。この事故を教訓に、自動列車停止装置(ATS)の開発・導入が図られ、ヒューマンファクタが重要であることが認識され、鉄道労働科学研究所が国鉄内に設置され、安全研究の進展が進むことになった。

（３） 鶴見列車衝突事故

1963 年 11 月に発生した「鶴見列車衝突事故（死者 161 人)は、貨物列車の脱線により並走する横須賀線の列車2本が衝突するという３重衝突事故であり、貨車の脱線対策と、車両そのものの走行安全性の向上につながった。

新幹線においては、標準ゲージを採用し、曲線半径を大きくすることにより、高速走行の安定性・安全性を優先した方式となっている。

新幹線開業後においても、在来線における重大事故とその対策は、以下のようなものが挙げられる。

・北陸トンネル列車火災(1972 年 11 月６日；トンネル内火災での緊急停止の禁止)
・信楽高原鉄道正面衝突（1991 年５月 14 日；事故調査検討会の発足）
・日比谷線脱線衝突（2000 年３月８日；航空・鉄道事故調査委員会（運輸安全委員会）設立、低速脱線対策、輪重管理）
・京福電鉄正面衝突（2000 年 12 月 17 日；ブレーキ多重化）
・上越新幹線中越地震脱線（2004 年 10 月 23 日；脱線防止ガード、被害軽減のための逸脱装置）
・福知山線脱線転覆衝突（2005 年４月 25 日；運行記録計の義務付け、安全管理）
・羽越線強風転覆（2005 年 12 月 25 日；風速規制強化）。

このような悲惨な事故を防止するということから、鉄道においては、「事故ゼロ」が目標であり、その対策は、事故後の被害軽減ではなく、「予防安全」に主眼が置かれてきた。そのため、かつては事故後の被害軽減の検討は、事故を前提とする考え方として排除されてきたともいえる。福知山線の事故を契機に被害軽減の重要性が再認識され、これらの対策も進むことになった。

３．近年の鉄道安全性向上の主な対象

鉄道事故では、ハードウエア（軌道、車両、施設）の不備によるもの、ソフトウエアとして運転や信号にかかわるもの、外的要因として自然災害や踏切事故などの鉄道の責任外の事故とがあり、鉄道においては、ハードウエアとソフトウエアの改善に重点的に取り組んできている。いずれにおいても、設計や保守作業における人的ミスや、運転などの操作によるミス、管理ミスなどヒューマンファクタにかかわる要因が大きいため、これらを極力考慮し、排除する手法がとられている。

鉄道事業者による安全性向上の取り組みは、鉄道事業者の責任によって生じる事故を防止するということに主眼をおかれてきたため、自然災害への取り組みや、鉄道事業者のみでは安全が確保できない踏切やホーム事故への取り組みが近年の安全性向上の対象となっている。

現在では、鉄道事故の大半は、踏切とホーム上における人身事故(酔客、自殺)であり、後者の対策として、ホームドア、ホーム柵の設置などが推進され、新たな技術開発も積極的に行われている。

ホームドアについては、当初は　バリアフリー対策が主眼であったが、新大久保事故(2001 年１月 26 日)を契機に安全対策として義務付けの方向性の検討が開始されたが、技術的制約・コストの制約が大きく、現在では、新線・大規模改良での義務づけと、１日の利用者 10 万人以上の駅に設置が望ましいとするガイドラインが国土交通省より示され、近年では、自殺・酔客以外においても、携帯電話・スマートフォンによる事故も増加傾向にあり、総力による取り組みがなされている。

４．安全目標の考え方

鉄道においては、事故ゼロが目標であり、現状では安全目標の合理的・論理的な議論の場が求められていない。事故後の対策が主体であること、安全対策投資が基本的に民間事業にゆだねられているという状況もある。

安全目標として、乗客の遭う被害として取られるのか、乗務員をどう捉えるのかという問題もある。また、鉄道では、事故の発生頻度は、時間当たりではなく、輸送人員と列車走行距離の積あたりの事故率が重要であり、旅客を輸送しない貨物鉄道についての評価の観点も議論が必要である。我が国の高い安全性を持つ鉄道を海外に展開することが、現在求められているが、その折には、海外の事情にあった、安全目標での議論は大変有益と考えられる。

AP７．船舶・海洋における安全

１　船舶における安全

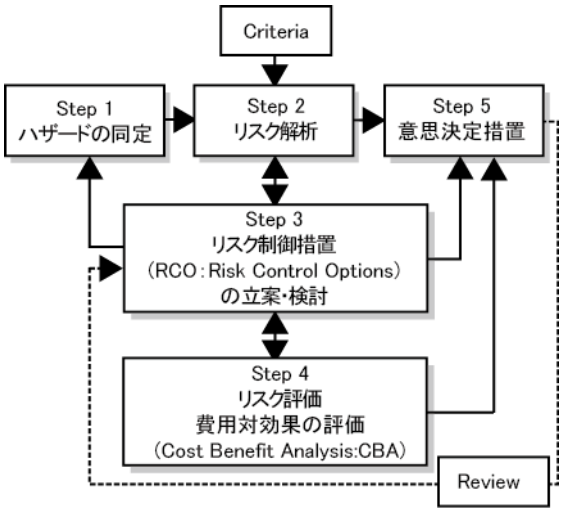
（１） FSA (Formal Safety Assessment)

国際航路を航行する船舶の安全管理の基本的枠組みは、国際海事機関 IMO (International Maritime Organization)で決定され、これが各国規則や船級協会規則に反映されるため、世界共通のものとなる。IMO は国際連合が 1948 年に設置した常設の海事専門機関で、本部は英国ロンドンにあり、現在の加盟国は 165 カ国（準加盟国 3 カ国）である。設立の目的は、「国際貿易に従事する海運に影響のある全ての種類の技術的事項に関する政府の規則及び慣行について、政府間の協力のための機構となり、政府による差別的措置及び不必要な制限の除去を奨励し、海上の安全、能率的な船舶の運航、海洋汚染の防止に関し最も有効な措置の勧告等を行う」とされている。

船舶の国際的安全基準は、1912 年に起きたタイタニック号の事故をきっかけに、それまで各国が独自に定めていた安全基準を国際的に統一しようということから合意した SOLAS 条約 (Safety Of Life At Sea)が最初である。SOLAS 条約は、現在も IMO が改正しながら維持し続ける、最も重要な条約の１つとなっている。しかし、大事故が発生したことを受けて改正が行われることから、事故直後の状況から不必要に過剰なものとなりがちであり、自国を有利にしようという多分に政治的な提案も横行したことから、より合理的なルール制定方法としてリスク評価の考え方に基づいた FSA (Formal Safety Assessment)が導入された。

FSAは、1993年のIMO/MSC62(第62回海上安全委員会)において英国が提案したもので、その後の議論および試験的な適用の積み重ねに基づき、暫定ガイドラインが修正され、最終的なFSAガイドラインが承認された。FSAは構造化され、客観性とトレーサビリティを有する、包括的で合理的な安全性評価手法である。IMOにおける規則制定における意思決定のツールであり、規則をより合理的なものとするために、特殊な提案や施行を少なくし、著しく政治的な議論を抑えることを目的としている。IMOでは、全ての提案がFSAを用いることを義務づけられているわけではないが、最近は多くの安全基準の改正がFSAを用いて提案され審議されている。

ここで、FSAガイドライン[1] [2]に基づき、その概要を説明する。図AP７－１に示す様に、FSAの手続きはStep１～Step ５の５段階に分かれている。



図AP７－１　FSAの手続き

①　Step１：ハザードの同定

Step １では、最初に事故に至る種々のハザード（危険性）を同定する。同定には、種々の分野の専門家の意見を組織的に汲み上げるHAZID会議を主体とした創造的な手法と、海難データ等の分析を主体とする分析的な方法が組み合わされて用いられる。さらに、表AP７－１のようなリスクマトリクスにより被害程度と発生頻度の数値化を行い、ハザード発生時の粗い影響評価を実施し、リスクの大きいハザードを絞り込む。FSAではリスク＝被害程度×発生頻度という定義を使用しており、リスクマトリクスではRI（Risk Index）＝SI（Severity Index）×FI（Frequency Index）となる。さらに粗い事故シナリオを作成し、RIに基づいた事故シナリオの優先順位付けを行う。

表AP７－１　FSAのリスクマトリクス

リスクインデックス(RI)					
発生頻度指数(FI)	頻度	影響度指数(SI)			
		1	2	3	4
		軽微	重大	深刻	壊滅的
7	しばしば	8	9	10	11
6		7	8	9	10
5	合理的に起こりそうな	6	7	8	9
4		5	6	7	8
3	稀	4	5	6	7
2		3	4	5	6
1	極めて稀	2	3	4	5

②　Step２：リスク解析

Step ２では、事故シナリオの詳細なリスク解析を行い、事故確率、事故後の災害拡大が生じる確率とその重大性を求めることにより、対象船舶の全体リスクを個々の事故シナリオのリスクの総和として求める。

この場合のリスクとは安全の指標であり、先に述べたようにFSAでは事故の発生頻度と被害程度との積によってリスクを定義しており、想定する被害は、人命損失、環境影響、財産の喪失である。リスク評価指標には、個人リスク及び社会リスクがあり、個人リスクとは、個人が交通機関を利用している期間中のその個人の死傷頻度を示す指標、社会リスクとは、交通機関を利用している集団の、考慮対象期間中の死傷頻度を示す指標である。集団の社会リスクはその集団に属する個人リスクに集団の大きさをかけたものである。社会リスクの指標としてPLL (Potential Loss of Lives)があり、船舶の場合は1隻1年当りの死者数となる。PLL の値が同じであっても、１回で多数の死者が出た事故ほど許容し難くなるという観点を反映するものとしてFN (Frequency - Number of Fatality)線図（人命損失数とある数以上の人命損失が発生する事故の発生頻度をグラフ化したもの）を用いて分析を行う方法があるが、FSA でもFN線図が使用されている。

FSAでは表AP７-２に示す様に、リスク許容基準としてALARP (As Low As Reasonably Practicable:合理的に実行可能な限り低くするという原則)領域の上下限を定めている。リスクがALARP領域の上限を超えていれば、許容不可能領域（Intolerable）として、緊急にリスクの低減が必要となる。また、ALARP領域にある場合は合理的に実行可能な範囲でリスクの低減が必要とされる。一方、リスクがALARP領域の下限以下であれば、無視可能領域（Negligible）としてリスク低減は不要である。つまり、IntolerableまたはALARPの場合のみ次のStepに進むこととなる。ここで、ALARP領域の上限値に対しては、乗客や公衆に対して乗員を１桁下げていること、また新船に対しても下げていることに注意されたい。なお、このリスク許容基準については暫定的なものであり、反対意見も多いことから、見直しが検討されている。

表AP７-２　FSAのリスク許容基準

決定パラメータ		許容基準	
		ALARP 領域の下限	ALARP 領域の上限
個人リスク	乗組員	10^{-6}	10^{-3}
	乗　客	10^{-6}	10^{-4}
	海浜にいる公衆	10^{-6}	10^{-4}
	新船に対する目標値	10^{-6}	上記数値から一桁下げた値
社会リスク	上記のグループ	経済指標より得られる	

③ Step ３：リスク制御措置の立案

Step ３では、リスクがALARP領域にある場合に高リスクをもたらすハザードそのものや、あるいは事故シナリオの発生を抑制するための安全対策であるリスク制御措置RCO (Risk Control Options)を検討し、それらを導入した場合のリスクの減少を推定する。FSA では個別の対策のことをリスク制御手段RCM (Risk Control Measure)、RCM

の集合をRCOとよぶ。RCOには事象の発生頻度を減らす予防措置と、結果の重大度を減らす緩和措置がある。

④ Step ４ ：費用対効果の評価

Step４では、Step３で考案された種々のRCO を実現するためのコストを評価し、費用対効果の評価を行い、RCO の優先順位付けする。FSA にはその指標値としてGross Cost of Averting a Fatality (GCAF)とNet Cost of Averting a Fatality (NCAF)の2つががあり、以下の式で表される。

GCAF = ΔC/ΔR

NCAF = (ΔC-ΔB)/ΔR

ここで、

ΔC：RCO の導入による追加コスト (US$：RCO の価格、訓練費用、逸失利益等を含む)

ΔR：RCO の導入により削減されるリスク

ΔB：RCO の導入による経済的利益

である。

GCAFは、１単位のリスクを削減する場合に必要とされるコストを意味する。一方、NCAFは、RCO 導入により利益が得られる場合の正味のコストを意味し、利益としてRCOの導入により防止される被害の金銭的な価値が含まれる。

GCAFまたはNCAFの値が評価基準の閾値より小さければ、費用対効果の観点から有効なRCOとなり、そのRCO の導入が測られる。現在のFSAガイドラインでの評価基準の閾値は、OECD 加盟国のGCAF の現状より、死亡および障害の場合300万米ドルを使用している。しかし、この値をもっと高くすべきとの意見も多く、現在、見直しの動きがある。

⑤ Step ５：意思決定のための推薦

Step５では、Step ４の結果を判断し、導入すべきRCO を提案する。

手順や検証の複雑さがあるもの、FSAを用いたIMO提案は年々増加しており、バルクキャリアの安全性向上、電子海図表示システム(ECDIS)の強制化、タンカーのイナートガスシステム(IGS) の強制化等がFSAを用いて規則化されており、現在では旅客船等の船体損傷時の復原性用件の向上が議論の対象となっている。

(2) 環境 FSA

安全に関する FSA が成果を上げてきたことから、海洋環境保全に関する新基準導入に際しても FSA の考え方を活用するために、EREC (Environmental Risk Evaluation Criteria)を FSA ガイドラインに盛り込むことが検討された。EU の共同研究プロジェクト SAFEDOR は、油流出を対象として、CATS (Cost of Averting a Tonne of Oil Spilt)

つまり、１トンの油流出を防ぐために実施するRCOとして拠出する金額、という概念を導入し、以下のような評価基準を提案した。

$\Delta C/\Delta R = CATS < CATS_{thr}$

ここで、

ΔC： RCOに導入による追加コスト（US$）

ΔR：RCOによる油濁リスク減少効果

$CATS_{thr}$：任意のRCOの費用対効果を判定するための閾値

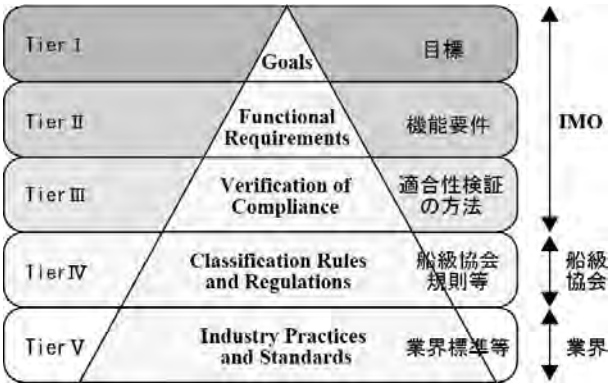
である。

当初、SAFEDORでは閾値$CATS_{thr}$として6万米ドル/トンの一定値を提案したが、日本等が国際油濁賠償基金（IOPCF）の1970～2005年までの油濁事故データに基づき、油濁量(W)と油濁損害金(C)に関する回帰分析を実施し、C/Wは一定値ではなく、Wの関数であり、Wが大きくなるとC/Wが小さくなることを示し、回帰分析に基づく関数型$CATS_{thr}$を提案し、IMOで採用された。海洋環境保全にFSAを導入しようとする動きは、今のところ油流出のみにとどまっているが、影響が大きいだけに今後の動きが注目される。

（３） GBS(Goal-Based Standards)

1997年のナホトカ号の事故では、重油約6,200トンが日本海に流出し、沿岸域に大きな被害をもたらした。これ以後も、老朽化したタンカーの大事故が相次ぎ、1999年のエリカ号事故ではフランス沖に重油約10,000トン以上が流出、2002年のプレスティージ号事故ではスペイン沖に積荷油約77,000トンが流出した。

これらの事故は、直接的にはシングルハルタンカーのフェーズアウト促進（2010年まで)、シングルハルタンカーによる重質油の輸送禁止、特別敏感海域（PSSA）の設定等の施策につながったが、間接的には、被害国である欧州委員会（EU諸国）の主張が強くなり、これまでの規則を策定してきたIMOや老朽船を承認していた船級協会とその団体であるIACS（International Association of Classification Society)への信頼性が揺らぐこととなった。このためIMO/IACSは信頼と主体性を回復するために、事故後の対応から事前リスク回避に力点を移し、IMOは規則の目的・安全レベル・機能要件の明示として目標指向型基準GBS（Goal-Based Standards）体系を導入し、IACSは合理的で透明性のある船舶構造の統一規則としてCSR（Common Structural Rules)の導入を図った。



図AP７－２　GBSの構成

この内、GBS は図 AP 7－2に示す様な Tier Ⅰ～Tier Ⅴのピラミッド型をしており、許容できるリスクレベルを目標として先に定めるという点で、FSA とは異なる安全評価体型となっている。

2 海洋開発における安全

（1） 海洋開発におけるリスクベース安全性評価

船舶と異なり、海洋構造物については国際的な統一規格は存在せず、生産国自らが安全管理の体系及び規則を定めることになっている。こうした各国の安全管理機関の実例としては、ノルウェー石油監督局 NPD (Norwegian Petroleum Directorate)、英国安全衛生庁 (HSE : Health and Safety Executive)等が広く知られている。

海洋開発においては多くの重大事故が発生しており、特に、海洋石油・ガス関連の海洋構造物では、事故発生時の人命、自然環境への被害が甚大である。このため、リスク評価に基づく合理的な安全管理の重要性が広く認識され、原子力分野で研究されていた QRA (Quantified Risk Assessment)を海洋構造物へと適用するプロジェクトは 1970 年代と比較的早くから開始された。これには、とりわけ Alexander L. Kielland 号と Piper Alpha 号の事故が大きな影響を与えた。

1980 年に北海油田の掘削リグ Alexander L. Kielland 号が疲労破壊によって全損沈没するという大事故[3]では、1981 年に NPD[4]が全ての新設海洋構造物に、ALS (Accidental damage Limit State)の照査を義務づけ、1984 年には ALS による定量的評価基準を導入した。また、1988 年の北海油田のリグ Piper Alpha 号の爆発炎上事故では、連絡不備や組織上の問題点が事故原因とされ、オペレータによる自律的安全管理体制と客観的安全性評価の必要性を認識させた。この結果、英国安全衛生庁 (HSE) は Safety Case Approach[5]を導入することとなった。ここでは、ALS と Safety Case Approach の概要を解説する。[6]

（2） ALS (Accidental damage Limit State)

一般に構造物の限界状態設計(Limit State Design)では、構造物または部材が満足すべき設計条件として、以下の3種類の限界状態を考慮する。

①使用限界状態 (Serviceability Limit State : SLS)

②終局限界状態 (Ultimate Limit State : ULS)

③疲労限界状態 (Fatigue Limit State : FLS)

①の使用限界状態は、構造物や部材が過度な変形や変位等により、正常に使用できなくなる状態であり、通常の供用または耐久性に関する限界状態である。②の終局限界状態は、構造物や部材が破壊したり、大変形、大変位を起こしたりして機能や安定を失う状態であり、最大耐力に対応する限界状態である。③の疲労限界状態は、構造物や部材が繰り返し荷重により疲労損傷し、機能を失う状態である。

しかし、多くの重大事故では、設計・建造・運用段階における何らかの人為ミスや欠陥、あるいは衝突、爆発などの事故による損傷を発端として、それらが次第に拡大していき、破局的状態に至っていることがわかった。したがって、重大事故を未然に防ぐためには、万一何らかの原因で損傷が起きた場合も、それが直ちに全損、沈没などの重大な事態につながることがないよう、システムが適切なレベルの冗長性(Redundancy)を持つことが必要である。

このような概念に基づいてNPDは、上述の3種類の限界状態に加えて

④事故崩壊限界状態 (Accidental Collapse Limit State, ALS)

の評価を行うことを規定した。ALSでは、事故や異常荷重により構造物に損傷が生じた場合に、それが複数部材に逐次的に拡大して全体崩壊に至ることがないかどうかを調査することにより、全体構造としての冗長度を確認する。したがって、ALS は逐次崩壊限界状態 (Progressive Collapse Limit State, PLS)とも呼ばれている。主な事故事象としては、火災、爆発、船舶の衝突、重量物の落下、バラスト調整の失敗等であり、異常事象としては、ULSで想定する以上の波条件を考える。

ALSでは、事故荷重、異常荷重については、いずれも「年超過確率 10^{-4} レベル」、また損傷後の逐次崩壊挙動チェックのための荷重条件は「年超過確率 10^{-2} レベル」と規定している。また、事故確率を統計データから求めることは困難である衝突や火災等については、リスク解析を行うことに より、検討対象とする事故シナリオと事故荷重を決定するとしている。

（3） Safety Case

Piper Alpha の爆発炎上事故報告書(Cullen Report)は、オペレータによる自律的安全管理体制と客観的安全性評価の必要性を指摘した。この勧告に応え、英国政府は石油ガス生産を行うオペレータに対し、Safety Caseと呼ばれる文書の作成、提出を義務付けることとなった。その後、主要な各国政府はこれに倣い、自国領海内で操業するオペレータに対してSafety Caseの提出を要求しているため、事実上、海洋開発安全管理規定のデファクトスタンダードとなっている。

Safety Caseとは、労働者に対するリスクを企業が如何に効率的に制御するか、特に重大事故によるリスクをどの様に減らし、最小化できる管理システムを構築しているかを立証するために記述する文書のことをいう。Offshore Safety Case Regulation では、個々の海洋施設について、火災、爆発、構造損傷、ヘリコプターや潜水に絡む事故など、全ての可能性のある事故について検討が求められる。安全確保のアプローチは、従来の規則遵守型(prescriptive type)ではなく、自らが安全目標を定め、それが満たされることを証明するといった、いわゆる目標設定型(goal-setting type)である。その目標安全レベルの設定に対しては、ALARP概念が適用され、費用対効果を考慮して実現可能なレベルで可能な限りリスクを低減させる必要がある。

Safety Case は大きく次の３段階から構成される。

①FD(Facility Description) (*1)

②FSA(Formal Safety Assessment)

③SMS(Safety Management System)

①のFDは、システムの記述である。②のFSAは。システムに関するリスク評価とリスク低減策をまとめたものである。Safety Caseでは、設計、建造段階のリスク低減策を検討するだけでなく、それらを供用期間にわたって適切に管理する人的・組織的体制やPDCAサイクルを含む Safety Management System が構築されていることを示さねばならない。構造設計に関する規定が中心であるNPDの規定よりもさらに総合的な安全管理システムの構築が求められている。

英国の水域内で操業する全ての海洋構造物は、Safety Case を英国安全衛生庁 (HSE) のOSD(Offshore Safety Division)に提出し、承認を得なければならない。有効期間は３年であり、３年ごとにRevised Caseを提出しなければならない。また、安全性に重大な影響を持つ構造または装置の変更を生じたとき、事故やニアミスを生じたとき、既存設備に比べて大幅な技術的進歩があったとき、OperatorやOwnerが代わったときには大幅な改訂が必要となる。

なお、Safety Case と IMO/FSA は用いるリスク評価法やフローはほぼ同一であるが、前者が特定の施設/システムを対象にするのに対し、後者は条約や規則の対象となる一般化された船舶を対象にする点が異なっている。

＊1)ここで用いている略語 FD は 17 ページで用いた略語 FD とは別の語に対する略語である。

参考文献

[１] IMO Secretariat: Consolidated text of the Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process (MSC/Circ. 1023-MEPC/Circ.392), MSC 83/INF.２(2007).

[２] 金湖冨士夫、有馬俊朗: 船舶海洋分野におけるリスク評価の事例としてのFSA、海上技術安全研究所報告第8巻第4号(2009).

[３] 後藤政志:海洋構造物の事故と安全性,日本金属学会誌, 第66巻,第12号(2002).

[４] NPD: Regulations for load-carrying structures for extraction or exploitation of petroleum, The Norwegian Petroleum Directorate, Stavanger (1984).

[５] HSE: Safety Case Regulations Health and Safety Executive, HMSO, London (1992).

[６] (社)日本船舶海洋工学会:大規模海上浮体施設の構造信頼性および設計基準研究委員会最終報告書(2010).

AP８．情報システム（ICT）の安全

１　はじめに

社会において、情報システムは日々に重要度を増してきている。メールやソーシャルメディアによる情報交換が人間活動の中心を占めるようになっているし、医療・国防・交通制御・発電プラントなどでは、情報系はライフラインの役割を果たすようになっている。情報インフラの経済規模も、かつて想像もできないほど巨大なものになった。

情報システムは、従来の工学システムと異なり、「物」ではなく、「数」（で表現される「情報」）を対象とする。「数」は、読み取り、コピー、書き込み、遠距離での交換がだれでも簡単にできるものであり、保護するのがむずかしい。

「データ」だけでなく、「操作」も情報であり、「数」で表現される。「操作」を並べて問題を解くアルゴリズムを表現したものが「プログラム」である。世の中にはさまざまなプログラムがあるが、これらを総称してソフトウェアという。ソフトウェアは、挙動が統計になじみにくく、初期不良が見つけにくく、バグや脆弱性がきわめて短時間に無数に複製されるという特徴がある。反面、通常の工学システムに見られる経年劣化は、ソフトウェアには起こらない。

情報システムでは、人は匿名のまま、いつでも、どこからでも、データやプログラムに対して遠隔操作を施すことができる。これを悪用すると、広範で破壊的な攻撃を行うことができるようになる。悪意あるユーザは世界中どこにもいるのであり、愉快犯から国家間のサイバー戦争まで、さまざまなレベルの攻撃が仕掛けられている。

また、いわゆる「うっかりミス」などヒューマンファクタが瞬時に大きな影響を及ぼすのも情報システムの特徴であろう。東証ジェイコム株誤発注事件では、「１株 61 万円の売り」を「61 万株１円の売り」と誤入力したために、400 億円以上の損害を出すことになった。インテル社の初期の 32 ビットプロセッサでは、除算器の設計ミスが発見され、全数リコールによって 4.75 億ドルの損害が出た。

昨今のソフトウェアはたいへん複雑なものとなった。１億行を超えるプログラムも出現している。その反面で、ユーザ数は爆発的に増加し、システムそのものがブラックボックス化している。すなわち、ソフトウェアは日を追って検証困難で、脆弱性が混入しやすいものとなっている。

さらに、現在の情報システムは、多くの場合、ベストエフォートという考え方によって構築されている。ベストエフォートとは、サービスにあたって、ベストは尽くすが保証しないという意味であり、基本ソフトウェアの信頼性・安全性、インターネットの接続性やスループットなど、どれも保証なく販売・利用されている。ベストエフォートには、技術の発展速度をあげ、新技術の社会への普及を促す効果があるが、いっぽうでバグや脆弱性を残したまま運用することとなり、システムダウンやサイバーアタックの危険が常にある状態でシステムを使い続けることになりかねない。

以上、情報システムの阻害要因はユーザから基本ソフトウェア、さらにハードウェアと多階層にわたり、原因から結果が予測困難になっている。その上、ベストエフォートの考

え方で運用されているものが多い。様々な要因による故障／アタックに対処し、故障／アタックの伝搬を止め、正常動作状態を維持することが必須となっている。

２　ディペンダビリティとセキュリティ

情報システムの安全・安心は、可用性・信頼性・安全性・完全性・機密性・保全性から成り立っていると考えられる。「セキュリティ」は、このうちで、可用性・完全性・機密性が守られている状態を言う。また、「ディペンダビリティ」は、可用性・信頼性・安全性・完全性・保全性が守られている状態を言う。

サイバーアタックによって攻撃を受けても、設計ミスや放射線などがあっても、それがそのままシステムの障害につながるわけではない。侵入(intrusion)や故障（fault)、異常(error)という順を経て、最後に、障害(failure)が発生してシステムが異常動作することとなる（図 AP８－１)。大きなシステムの場合は、小さなシステムの障害が、上位システムの故障につながり、これが異常、障害につながる、という階層型の伝播が起こることになる。

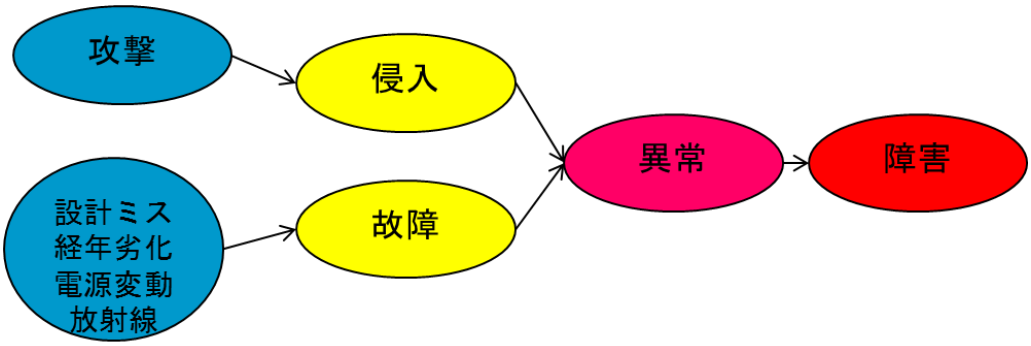


図 AP８－１情報システムに障害が起こるまで

セキュリティが損なわれると、個人情報の流出やネット詐欺によるプライバシーの破壊や財産喪失が起こり、サイバーテロによって私企業や国家が莫大な損害を被ることになる。ディペンダビリティが損なわれると、行政サービスや銀行勘定系、証券システムなどが停止し、交通機関やプラントが止まったり暴走したりし、ひどい場合には、人命に関わる事故が起こることになる。その他、別の種類の事故・事件として、出会い系サイトの悪用による殺人事件なども現実に起こっている。

侵入や故障を防ぐ手段として、回避、耐性向上、除去などがある。一般に要因を完全に除去することは、回避することよりもコストがかかる。必要なセキュリティとディペンダビリティを現実的なコストで実現することが、情報システムの安全目標となる。

３　大規模攻撃・高度な攻撃

情報セキュリティを阻害するものとしてサイバー攻撃があるが、近年これは大規模化・高度化が進んでいる。多数のパソコンが知らないうちにウィルスに感染し、クラッカの指

示のもとでいっせいに特定サーバを攻撃するボットネット攻撃は、その典型である。2007年から頻発しているエストニアや米国・日本・韓国への大規模な攻撃は、国家の関与が疑われている。

さらに高度な攻撃として、標的型攻撃、ゼロデー攻撃、遠隔操作型ウィルスなどが出現した。中でも最も大規模で衝撃的だったのは、イラン各施設に対するStuxnet攻撃である。Stuxnet 攻撃では、４種類のゼロデーウィルス（それまで発見されていなかったコンピュータウィルス）を使い、ディジタル署名によるマルウェア性を隠蔽するなど、それまでなかった高度で入念な攻撃法を用いており、イランでウラン濃縮用の遠心分離機8400台を停止させた。これには、米国とイスラエルの国家的関与が疑われている。

今後は、原子力発電所を暴走させて臨界状態にするなど、さらに破壊的な攻撃も考えられる。

４　安全目標

ハードウェア情報機器については、経年劣化の見積もり、ソフトエラー率の算出など、従来の物理インフラ同様に確率論的に安全目標を論じることができる。目標とするハードウェアのエラー率がソフトエラー率を下回る場合は、多重化などによってこれを補えばよいのである。

ソフトウェア（CADによる回路設計を含む）については、信頼性を数字で表すことが困難である。バグや脆弱性は、ポアソン的な現象ではなく、仕様記述の丁寧さ、プログラム言語の性質、アプリケーションの性質、プログラマの性格や経験、ソフトウェアの管理体制、開発期間などに強く依存する不規則・非線型の現象だからである。一般に、ソフトウェア工学と呼ばれる技術体系のさまざまな手法が有効と言われている。ただし、信頼性・安全性を高めるための新しい手法やアルゴリズムが、その導入時にはプログラマが慣れていないことによって、かえってこれらの障害になることもある。

機能安全規格IEC 61508においては、ソフトウェアの安全性を向上させるための開発技法が数多く挙げられており、安全度水準に応じて必ず使用すべきものを規定している。安全度水準は数値目標で定義されているため、この規格は、どのような開発技法を用いて開発されたソフトウェアはどの程度の安全性を持つかを、過去の経験に基づいて定量化していると言える。

行政・学協会の役割としては、情報セキュリティ・ディペンダビリティを管理する中央機関を設けること、法制度を整備すること、情報に関する安全委員会（事故調査委員会）を設けること、情報教育（倫理教育を含む）を初等教育から徹底すること、資格認定制度を作ることなどがある。

日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会では、この観点から、平成20年６月26日に提言「安全・安心を実現する情報社会基盤の普及に向けて」（http://www.scj.go.jp/ja /info/kohyo/pdf/kohyo-20-t58-4.pdf）をまとめている。

AP９．労働安全

１　労働安全分野における安全目標

労働安全の分野では、英国安全衛生庁（HSE）が示したリスク管理目標を労働災害防止の目標値として使用することがある。例えば、HSE 発行の“Reducing risks、 protecting people、HSE’s decision making process”[1]では、その第 130 項の冒頭で労働者一人あたりの死亡労働災害の発生確率を 10^{-6}回/年に設定している。

この目標は、100 万人の労働者が１年間働いたときに、死亡を伴う危害の発生件数の推定値を１件未満とする水準である。また、厚生労働省では第 12 次労働災害防止計画（平成 25～29 年度）の５年間で死亡者数及び死傷者数を各々15%以上減少させることを目標としているが、これも広い意味の安全目標と考えられる。

現在、労働安全分野の担当者はこれらのいずれかの数値を目標値として使用することが多いようである。しかし、このような数値の利用を含めて労働安全分野における安全目標をどのように設定するかは、今一度考察が必要と考えられる。そこで、労働安全衛生総合研究所の特別研究報告[2]を基に、主に機械システムを対象とした労働安全分野における安全目標について記す。

２　機械災害防止への取り組み

日本では、現場の優秀な作業者や管理・監督者の技能と注意力に依存して労働災害を防止するという手法が一般的であった。しかし、人の技能と注意力に依存した対策には明らかに限界がある。

これに対し、機械安全の先進国と言われる欧州では“人は誤った行動を行い、機械は故障やトラブルを起こす”ことを前提に安全技術を作り上げてきた。現在、この技術は ISO 12100 などの機械安全国際規格として標準化されている。そして、この規格が日本で広く知られるにしたがって、当該規格に基づく安全方策を日本でも実施すべきとの意見が機械安全の専門家から強く主張された。

また、労働安全衛生総合研究所が首都圏で発生した機械による死亡労働災害（“挟まれ・巻き込まれ”及び“激突され”災害に限る）129 件の死亡労働災害を分析したところ[3]、設備対策の不具合に起因する事例は 102 件（79%）と 8 割近くを占めていた（表 AP９－１参照）。以上の結果からも、ISO12100 などの機械安全国際規格に定められているガードや安全装置を設置していれば死亡労働災害の 8 割近くを防止できた可能性が推察された。

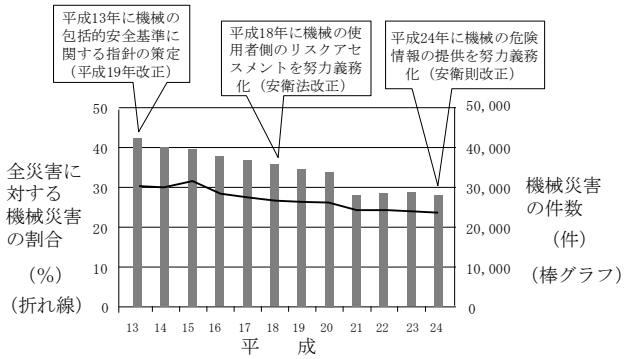
このため、労働安全衛生総合研究所では、この主張及び上記データを根拠として、厚生労働省と連携して労働安全衛生法の改正（危険性または有害性等の調査等に関する第 28 条の 2 の追加）と機械安全国際規格 ISO12100 と実質同一の機械の包括的な安全基準に関する指針の制定などを進めてきた。これにより、約 10 年前に全労働災害の 30%近くを占めていた機械による労働災害は、全労働災害の 25%近くまで減少した（図 AP９－１参照）。

この点は、労働災害の発生件数が長期的に下げ止まりにある中で画期的であったと考えられる。ただし、図 AP９－１では経済等の影響も考えられるので、その妥当性について今

表AP９－１　設備対策の不具合に起因する災害

	設備の種類	件数
①	固定式ガード	45（34.9%）
②	インタロック式ガード	67（51.9%）
③	①+②（ガード）	87（67.4%）
④	保護装置	31（24.0%）
⑤	制御システムの安全関連部	30（23.3%）
	総　計	102（79.1%）

注）①～⑤には重複あり。挟まれ・巻き込まれ災害１２５件、激突され災害４件。ただし、車両系荷役運搬機械と建設機械は分析の対象から除外。



図AP９－１　機械災害の推移（休業４日以上の死傷災害）
（出典）　労働者死傷病報告書（厚生労働省調べ）

後十分に検証する必要がある。

一方で、日本では、東日本大震災の惨禍を経験した中で、過去に繰り返し発生する災害（図 AP９-２の“タイプＡ災害”）だけでなく、発生確率は低いが重篤度は著しく高いために社会的影響の大きい災害（図 AP９-２の“タイプＢ災害”）に対する対策の重要性を強く意識せざるを得ないと考えられる[4]。このためには、件数重視から重篤度重視への戦略転換が不可欠と考えられる。また、東日本大震災で問題となった“想定外”に対する対策も併せて重要である。実は、これらの問題と真剣に向き合おうとすると、どうしても現在の ISO/IEC ガイド 51 で示された“安全”の定義を見直さざるを得ない。

さらに、現段階でどうしても触れておかなければならない問題点として、長期的に減少していた日本の労働災害の発生件数が、ここ数年、逆に増加の傾向となっているという問題がある。これが経済の活性化による一時的な現象なのか、あるいは日本の安全管理のあり方に抜本的転換を迫る重大な問題が起きているためなのか、正直なところ分からない。しかし、この機会に日本の安全管理のあり方を抜本的に改善しようとするならば、大胆な発想を持ってこの問題に正面から取り組む必要がある。

このため、以上のような問題意識を基に、根拠に基づく安全理論（EBS：Evidence-Based Safety）という新たな体系が構築されつつあるので、特に重要と考えられる要点を以下に概説する。

危害のひどさ	危害の発生確率	分類
大	大	災害多発機械
小	大	
大	小	重篤災害
小	小	許容

⇨ タイプＡの災害
過去に繰り返し発生している災害をいう。

⇨ タイプＢの災害
発生確率は低いが重篤度が著しく高いために社会的影響の大きい災害をいう。

図AP９－２　タイプＡ災害とタイプＢ災害

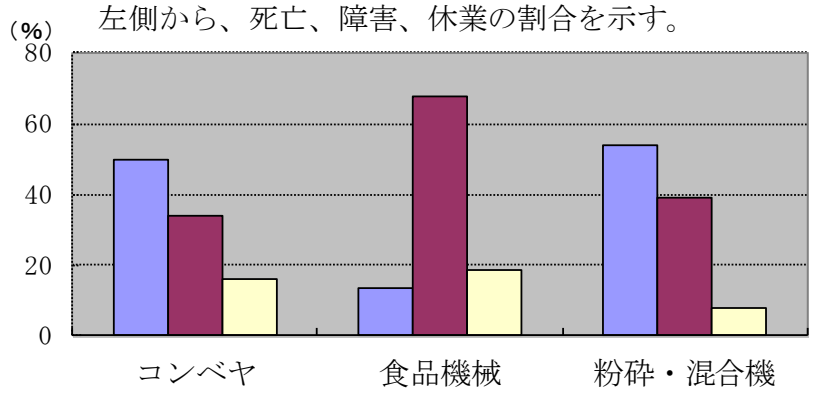
３　件数重視から重篤度重視へ

労働災害の中には、過去に繰り返し発生しているタイプＡ災害と、発生確率は低いが重篤度は著しく高いために社会的影響の大きいタイプＢ災害がある[5]。現在、日本で実施されている労働災害防止対策の多くはタイプＡ災害を対象とする。この災害に対しては、“労働災害は本来あってはならない”という基本理念の下に、災害の発生件数を減少させる対策が講じられる。そして、軽微な不休災害も含めた災害の発生件数の大小を評価指標とし、件数が減少したことを理由として安全成績が向上したと主張する（この延長線上に無災害表彰制度がある）。

しかし、実際には、労働災害の発生件数が大きく減少した職場で、ある日突然、死亡災害や一度に３人以上が死傷する重大災害、あるいは企業経営に甚大な影響を与える爆発・火災などの重篤な労働災害が発生することがある。この原因の一つとして、過去に繰り返し発生しているタイプＡ災害に対する対策が、発生確率は低いが重篤度は著しく高いために社会的影響の大きいタイプＢ災害に対して必ずしも有効でないためと推察される。

以上の点からも、今後の労働災害防止対策では、過去に繰り返し発生しているタイプＡ災害だけでなく、重篤度が高く社会的影響が大きいタイプＢ災害に対する対策のあり方も明確化していく必要がある。

同様に、タイプＡ災害でも重篤度を重視した対策が必要である。この点を明らかにするために、典型的なタイプＡ災害である食品機械、コンベヤー、粉砕・混合機に起因する災害を対象に労働損失日数の内訳の調査がなされた[6]~[8]。その結果、休業災害に相当する労働損失日数はいずれの機械でも 10～20％程度であったのに対し、死亡や障害に相当する労働損失日数は 80～90％程度と圧倒的に高かった（図 AP９－３参照）。この結果だけを考慮しても、件数重視から重篤度重視への戦略転換の重要性が推察される。



図AP９－３　災害多発機械の労働損失日数の比較

４　想定外に対する対策

（１）基本的戦略

次に、想定外に対する対策の明確化を試みる[9]。安全管理では、労働災害を事前に予測して回避するプロセスが不可欠である。このため、実際の職場では、発生する可能性がある災害をあらかじめ想定して、それを回避する対策が実施される。このような対応は、単

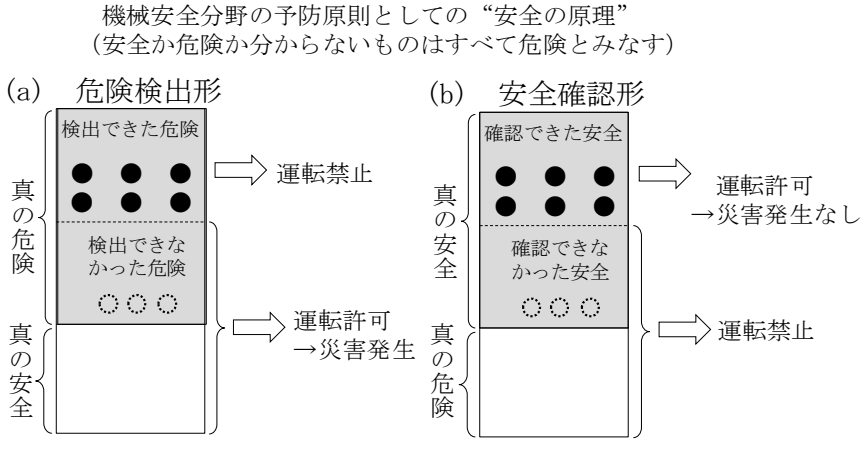
純な機械などを対象とした場合、適切な対策と考えられる。しかし、少しでも複雑な対象になると“想定外”という問題が表れる[9]。

図 AP９−４は、この問題を図式化したものである。図で、(a)は前述した考え方に基づいて対策を実施した場合である。この場合、確かに労働災害を想定した人が回避すべきとした問題（図の●印）は確実に取り除かれている。しかし、この人が想定しなかった問題（図の点線の丸印）は残念ながら取り除かれずに潜在している。そして、何かの拍子にこの問題が顕在化したときに労働災害が発生する可能性がある。

このような説明に対しては、“想定者はプロだからそんな見落としはしない”との反論があるかもしれない。しかし、実際の労働災害は、想定者がうっかり見落としたときだけでなく、問題の所在は確認していたが“まさかそのようなことは起きないだろう”（確率が低いと判断）、“十分な対策をしたから大丈夫だろう”（過信）などと思っていたときにも発生する。特に後の２つは、想定者が許容可能なリスクや残留リスクと判断していたものが重篤な災害の原因になったということで、ここにリスク評価の難しさがある。

では、このようなときの対策の妙案はあるのか。この問題に対して普遍的な解答を示すのはたいへん難しい。しかし、少なくとも一旦発生したら社会的に影響の大きい災害に対しては、どんなに発生確率が低いと判断しても確実な対策を施すことが重要と考える。このとき、発生確率や件数が少ないことを持ってリスクが低いと判断してはならない点に特に留意する必要がある。

従来、日本では労働災害の発生件数を減らすことを重視してきた。しかし、前述したように、本当に減らさなければならないのは重篤度が高い災害である。ちなみに、日本では、丸のこ盤に対する対策を実施する場合、発生件数の多い指の切傷災害を重視する。これに対し、機械安全の先進国である欧州では、一旦発生したら死亡に至る可能性が高い木材の反発による災害を重視するといわれている（もちろん、指の切傷の中には切断などの障害を伴うものもあり、この対策は重要である）。また、最近、企業経営でコンプライアンスが重視されているが、安全に関しては比較的軽微な出来ごとが強調される一方で重大な問題が見逃されているように感じる。



図AP９－４　危険検出形と安全確認形

いずれにしても、発生確率や発生件数の大小に惑わされないで、“重篤度の高いものに対しては確実に手を打っておく”ことが重要である。このとき、“残留リスクや許容可能なリスクなどという言葉に惑わされずに、残されたリスクの確定と適切な対策の採用によって最後まで面倒をみるという安全側の割り切り”も併せて考慮すべきと考える。

（2）安全確認形による対策

次に、想定外を考慮した対策の一つとして、安全確認形[10]という考え方を示す。これは、図 AP 9－4 (b)に示すように、安全が確認できる条件の下でのみ機械の運転を許可する方法である。このようにすれば、そもそも安全が確認できない条件（この中には危険な条件や想定外の条件を含む）の下で機械を運転することはないから、想定外の問題が発生する可能性は理論的には根絶できる（ちなみに、図 AP 9－4 (a)のように危険を検出したときだけ機械の運転を停止させるのを危険検出形と呼んでいる)。この方法は、想定者が危険をうっかり見落としたときなどに特に効果を発揮する。

ただし、この方法では、安全が確認できなくなったときに、迅速かつ確実に機械を停止させる必要がある。したがって、この方法は、停止によって安全を確保できる鉄道や産業機械などに対しては適用できるが、停止によって安全を確保するのが困難な航空機などには適用が困難である。

なお、安全確認形では“安全か危険か判断がつかない不確定なものは、必ず危険とみなす”という考え方が重要である。これを杉本と蓬原は“安全の原理”と呼んでいる[11]。同様の考え方として、環境分野における予防原則がある。これは“科学的に因果関係が十分証明されない状況でも、疑わしいものは規制する”という考え方である。また、品質の分野でも“良品か不良品か分からないものは不良品とみなす”という考え方が成り立つ。これらは、品質・安全・環境などの各分野を横断する普遍的な考え方であり、想定外を考慮した対策でも重要と考えられる。

5　安全の定義と安全目標

次に、以上の検討を踏まえたうえで安全の定義に対する考察を試みる[12]。ここでは、“安全目標＝確率論的なリスク管理目標”と単純に捉えてよいかという問題提起を行う中で、安全の定義に対する考察を試みたい。

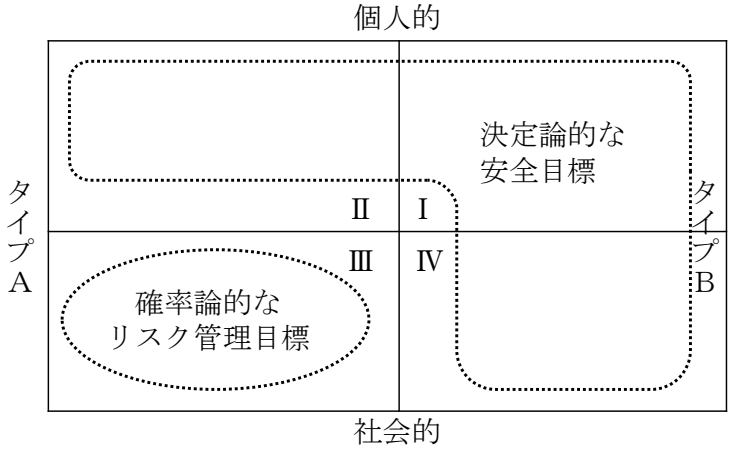
安全規格を作成する際の国際的なガイドラインである ISO/IEC ガイド 51 では、安全を“受け入れ不可能なリスクがないこと”と定義している。この定義に従えば、安全目標として確率論的なリスク管理目標を採用するのも理解できる。しかし、全ての災害に対して安全目標として確率論的なリスク管理目標を採用するのが適切かは文献[２]で問題としている。

例えば、過去に繰り返し発生しているタイプＡ災害に対しては、行政的な目標値として確率論的なリスク管理目標（例えば、英国の HSE が示した労働者一人あたりの死亡労働災害の発生確率を 10^{-6}回/年未満とするという目標）の設定が必要かもしれない。これに対しタイプＢ災害では、いかに発生確率が低いと言っても、万一災害が発生した場合には、社会的に取り返しのつかない事態に至る可能性が高い。このとき、“事故や災害は確率的に

発生するのだからやむを得ない”という考えは、実際上、受け入れ難い。

同様に、労働者個人にとっても、軽微な労働災害（例えば、ナイフで軽い切り傷を負うなど）であれば、“災害は確率的に発生するからやむを得ない”として、怪我をした反省も含めて、そのリスクを受け入れることが可能かもしれない。これに対し、発生した労働災害が過去に繰り返し発生しているタイプＡ災害であったとしても、死亡や身体障害を伴う重篤な災害である場合は、被災者個人にとって到底受け入れは不可能である。

図 AP９−５は、以上の点を考慮して安全目標のあり方をまとめたものである。図からも明らかなように、確率論的なリスク管理目標が採用可能なのは、タイプＡ災害の社会的安全目標（領域Ⅲ）に限られる。これに対し他の領域では、確率論的なリスク管理目標の採用は困難で決定論的な安全目標を必要とする。



図AP９－５　社会的安全目標と個人的安全目標

ここで決定論とは、事故や災害は起こり得ることを前提に“確実に”（決定論的に）予防策を講じることを目的とした技術をいう。この技術では、事故や災害の発生確率を“ゼロ”とすることを目標に安全方策が実施される。しかし、絶対安全は困難であり、決定論的方策を採用したからと言って事故や災害の発生確率を“ゼロ”にできるとは限らない。では、決定論的方策によって事故や災害はどの程度まで減少できるのか。この質問に対しては“分からない”というのが正しい答えであろう。

むしろ危険な機械に対する決定論的方策では、比較的危険性の低い機械に対して確率論的なリスク評価を実施したときよりも事故や災害の発生確率は高くなることもあり得る（一般に、危険な機械の方が事故や災害の発生確率が高くなるのは当然である）。そして“分からない”からこそ、事故や災害の発生を防止するための未然防止策だけでなく、万一事故や災害が発生したときの被害拡大防止策を確実に実施しておく必要がある。現在、未然防止策は通常時の安全管理、被害拡大防止策は異常時の危機管理に対応させられているが、これを技術的方策として一体化を図るとともに、被害拡大防止策においても決定論の考え方を採用することが、この分野における重要な課題になると考える。

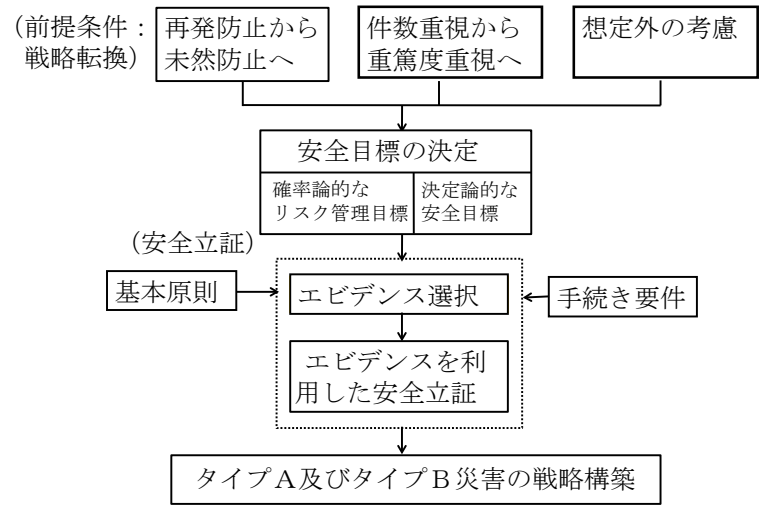
図 AP９−５は、安全をリスクの問題として捉えられる部分が全領域の一部（領域Ⅲ）に過ぎないことを示唆している。このことは、安全をリスクに依存しない新たな概念として

再構築する必要があることを意味する。このため、文献[９]では安全を“未然防止のための仕組みと戦略の構築”と定義した。このとき、安全目標は“未然防止の観点に立った活動か”、“災害防止のための手段とその仕組みは妥当か”、“戦略は適切で普遍的か”という観点からの設定が可能となると考えられる。

６　根拠に基づく安全理論の提案

次に、以上の結果を踏まえた上で、根拠に基づく安全理論（EBS）の体系の提案を記する。図 AP９－６に、EBS 体系の概略図を示す[2]、[5]。

この体系では、前提条件となる安全管理上の留意点として、再発防止から未然防止、及び件数重視から重篤度重視への戦略転換が不可欠である。また、想定外に対する対策が不可欠である。



図AP９－６　根拠に基づく安全理論（ＥＢＳ）の体系図

実際の EBS 体系では、安全目標を達成したか否かを立証する際の“根拠”を必要とする。これをエビデンス（Evidence）と呼ぶ。一般にエビデンスというと実験データを想定する。しかし、未知の要因や想定外事象などの不確定要因、あるいは設計段階での安全要求事項の見落としなどが影響する安全分野では、長い歴史と経験に裏付けられた“実績”や自然法則などの“理論”も、エビデンスとして重要と考えられる。

このように、EBS の体系では表 AP９－２に示す情報（データを含む）、実績、および理論というエビデンスを総合的かつ相互補完的に活用しながら科学的根拠を示していく点に特徴がある。しかし、単にエビデンスを示しただけでは科学的根拠としては十分でなく、エビデンスの活用にあたって適切な基本原則および標準化された手続きに従うことが、EBS 体系を構築する際の必要十分条件と考えられる。このため、これらの基本原則と手続き上の要件も併せて検討された。このうち、基本原則には機械安全分野の予防原則である“安全の原理”を始めとして表 AP９－３に示すようなものが考えられる。また、手続き上の要件としては、表 AP９－４に示す公平性、公開性、透明性、倫理性、専門性などが考えられる。

表AP９－２　根拠に基づく安全理論（EBS）で利用できるエビデンスの区分

区分	説明及び具体例
情報	情報として提供される事例やデータなど。例えば ・災害情報　・典型災害事例　・災害統計 ・機器の信頼性・安全性データ ・FMEA、FTA、ETAによる信頼性解析結果
実績	歴史や経験に裏付けられた技術・戦略・制度など。例えば ・ISO12100に定めたリスク低減戦略 ・モジュール方式による適合性評価制度 ・第三者認証に基づくCEマーキング制度
理論	自然法則や論理などの理工学に裏付けられたシステム構築理論、安全性立証法など。例えば ・物理や化学などの自然法則 ・フェールセーフシステムの構築理論 ・安全確認形のシステム構成理論

表AP９－３　根拠に基づく安全理論（EBS）で利用できる基本原則

区分	説明
可謬性	人は誤り、機械は故障することを前提に保護方策を実施
予見可能な誤使用への配慮	通常の使用だけでなく、予見可能な誤使用も考慮
ライフサイクルへの配慮	通常の運転時だけでなく、段取り、トラブル処理、保守・点検、修理、清掃、改造、廃棄などの作業も考慮
根本原因重視	ヒューマンエラーの背後にある根本原因を重視
予防原則としての安全の原理	安全か危険か分からないものはすべて危険とみなす
絶対安全の困難性への配慮	絶対安全は困難で、リスクは必ず残留することへの配慮

表AP９－４　根拠に基づく安全理論（EBS）で利用できる手続き上の要件

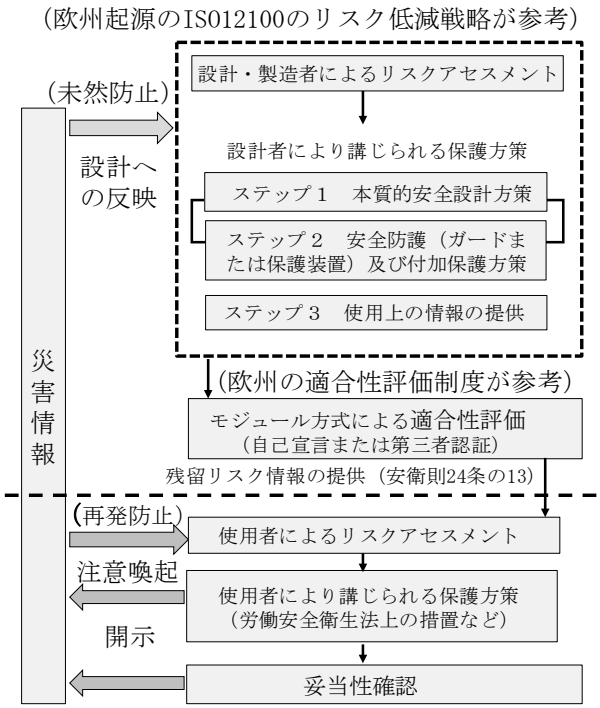
区分	説明
公平性	特定の個人や集団が過大なリスクを負わない
公開性	安全やリスクに関する情報は、何人にも公開されており、容易にアクセス可能である
透明性	安全立証、適合性評価、リスクの評価などに関する手続きは、所定の透明かつ明確なプロセスにしたがう
倫理性	専門家は、所定の技術者倫理を備えている
専門性	専門家は、State of the art に基づく専門性を備えている
公正・中立性	専門家は、利害関係者から独立した公正・中立性を備えている

７　タイプＡ及びタイプＢの労働災害防止戦略

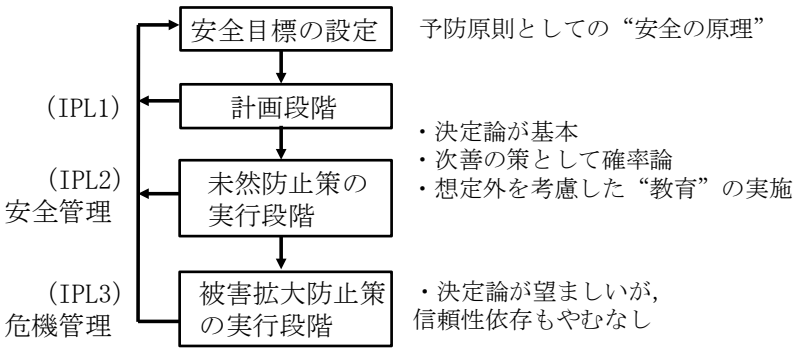
次に、タイプＡ及びタイプＢの労働災害防止戦略の提案の要点のみを概説する。

図 AP９-７に、タイプＡ災害の労働災害防止戦略の要点を示す[2]。この戦略では、①ISO12100 に定めるリスク低減戦略、②モジュール方式による適合性評価、③機械の使用者による妥当性確認、④機械の設計・製造段階での災害情報の活用が中心となる。このうち、①と②は主に機械の設計・製造段階で実施するもので、製品の自由な流通を目的とする欧州の機械安全制度の活用を図っている。これに対し、③及び④は、労働安全を確保するために特に重要と考えて提案されている制度である。

また、図 AP９-８はタイプＢ災害の労働災害防止戦略の要点を示したものである。この戦略では、通常時の安全管理に対応する未然防止策だけでなく異常時の危機管理に対応する被害拡大防止策を独立防護層（IPL:Independent Protection Layers）として構築して行くことが重要と考える。



図AP９－７　タイプＡの災害防止戦略



IPL：独立防護層（Independent Protection Layers ）

図AP９－８　タイプＢの災害防止戦略

特に、一般に被害拡大防止策は人の注意力や設備の信頼性に依存せざるを得ない確率的な対策との思い込みがある。しかし、実は被害拡大防止策に決定論的な考え方を導入することによって、タイプＢ災害に伴って生じる被害を著しく低減することも可能と考えられる（この具体例に、杉本らが提唱しているクリティカル・インタロックがある）[13]。したがって、今後は決定論的観点からの被害拡大防止策について引き続き検討を進める必要がある。なお、タイプＢの労働災害防止戦略は十分なものでないので、引き続き検討して高度化を図っていく必要がある。

８　おわりに

労働安全の分野では、英国安全衛生庁（HSE）が示したリスク管理目標（労働者一人あたりの死亡労働災害の発生確率を 10^{-6} 回/年未満とする）や厚生労働省が第 12 次労働災害防止計画（平成 25～29 年度）で示した死亡者数及び死傷者数の減少に関する目標値を安全目標として使用することがある。

しかし、このような数値の利用を含めて労働安全分野における安全目標をどのように設定するかは、今一度考察が必要と考えられる。そこで、労働安全衛生総合研究所の特別研究報告である文献[２]を基に、主に機械システムを対象とした労働安全分野における安全目標の検討結果を示した[2]。

参考文献

[１] HSE Books、Reducing risks、protecting people、HSE’s decision making process”、R2p2、（2001）

[２]梅崎重夫・濱島京子、 第三次産業の労働災害防止対策に関する技術基準等の検討、労働安全衛生総合研究所特別研究報告、JNIOSH-SRR-NO。43（2013）pp.101-108

[３] 梅崎重夫・清水尚憲、産業機械の労働災害分析、産業安全研究所特別研究報告、NIIS-SRR-NO.33（2005）pp.53-67

[４] 梅崎重夫・板垣晴彦・齋藤剛・伊藤和也・山際謙太・崔光石・高橋弘樹・濱島京子・清水尚憲・大幢勝利、よくわかる！管理・監督者のための職場における安全工学、日科技連出版社（2013）

[５] 梅崎重夫・濱島京子・清水尚憲、根拠に基づく安全を考慮した安全目標と安全性評価指標の提案、安全工学シンポジウム 2013（2013）pp.334-337

[６] 梅崎重夫・濱島京子・池田博康、食品機械を対象とした労働災害分析、労働安全衛生総合研究所安全資料、JNIOSH-SD-NO.27（2010）

[７] 梅崎重夫・濱島京子・清水尚憲・板垣晴彦、コンベヤーを対象とした労働災害分析－労働損失日数の活用によるリスクの定量的評価－、労働安全衛生研究、Vol.5、 No.1（2012）pp.33-44

[８] 濱島京子・梅崎重夫・板垣晴彦、粉砕機及び混合機を対象とした労働災害分析－労働損失日数の活用によるリスクの定量的評価と比較－、労働安全衛生研究、Vol.5、 No.2（2012）pp.87-97

[９] 梅崎重夫・清水尚憲・濱島京子・平沼栄浩・高木元也・島田行泰・三平律雄、よくわかる！管理・監督者のための安全管理技術－管理と技術のココ SF がポイント-（基礎編）、日科技連出版社（2011）

[10]杉本旭・粂川壮一・深谷潔・清水尚憲・梅崎重夫・池田博康・芳司俊郎・蓬原弘一、安全確認形安全の基本構造、日本機械学会論文集 C 編、Vol.54、No.505（1988）pp.2284-2292

[11]杉本旭・蓬原弘一、安全の原理、日本機械学会論文集 C 編、Vol.55、No.530（1990）pp.2601-2609

[12]梅崎重夫、最近の制御技術(6) -安全制御システムの運用で要望される管理技術 -、クレーン、Vol.51、No.9 (2013)
[13]本間慶太・杉本旭、原子力プラントの深層防護とクリティカル・インタロックの概念、安全工学シンポジウム 2013 (2013) pp.338-341

AP10.　製品における安全について

１．はじめに

ガス機器や電気製品などの消費生活用製品の安全性については、製品が数が多く世界的な規模で社会に出ていること、一般消費者に対して教育や訓練をすることが難しいこと、各家庭に存在する製品の保守点検の実施が困難なこと等により、特定な製品に関しては、消費生活用製品安全法で安全基準が決められており、この基準を満たすものしか製造・販売は認められていない。しかし、特定製品以外は、市場に出てからの事故情報に基づき、企業によるリコールや国による回収命令等が行われる。消費生活用製品安全法では、その中の電気用品安全法に関しては 2013 年から性能規定化が始まっているものの、基本的には、仕様基準として、安全目標が決められている。市場からのリコールや回収の基準は、その時代の社会の消費者期待基準で決められると解釈されるが、近年は、リスクアセスメントの考え方に基づき、許容可能なリスクレベルとしての数値的な安全目標が用いられるようになって来ている。

２．リスクアセスメントに基づく許容可能なリスクのレベルの考え方

最近の製品安全における安全の考え方は、機械やシステムの安全性に関する規格類全体を規定している ISO/IEC ガイド 51（JIS Z 8051 2004：安全側面－規格への導入指針）と、ISO12100(JIS B 9700：機械類の安全性－設計の一般原則　リスクアセスメント及びリスク低減)の考え方に従い、絶対安全は存在せず、リスクアセスメント（図 AP10-１参照）に従い、許容可能なレベル、または、適切に低減されたレベルのリスクをもって安全とするというリスクベースに従って、安全目標が決められつつある。

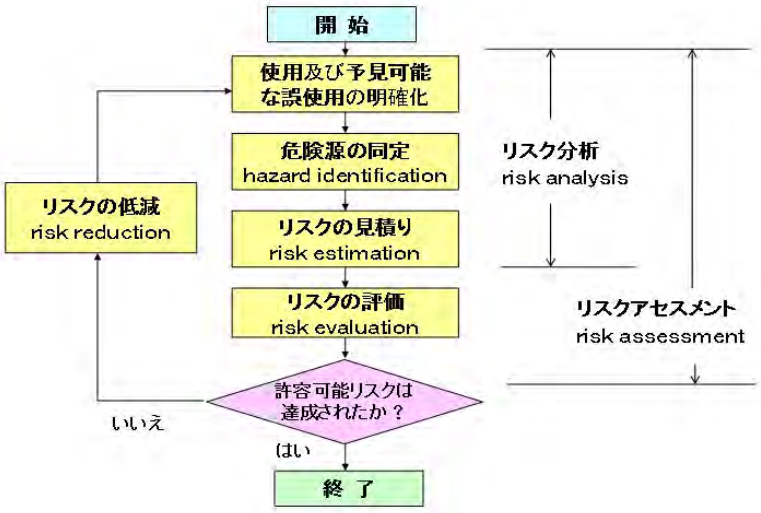


図 AP10-１ リスクアセスメントの手順（ISO/IEC ガイド 51 より）

その決め方の一つの例であるリスクマトリックス法を以下に紹介する。ここでは、リスクの定義、すなわち、“リスクとは、危害のひどさ（の程度）と危害の頻度の組合せ”に従

い、危害のひどさと頻度とをいくつかのレベルに分け、その組合せでリスクのレベルを決めるものである。表 AP10-１が、ひどさ（A)を４レベル、頻度（B）を６レベル、リスクを４レベルにした例であり、その組合せとしてリスクのレベルを割り当てた例が表 AP10-２である。これらのレベルは、定性的な言葉で表現されていて、その具体的な内容や数値は、製品により、条件により、また、時代によって異なる、としている。それは、ISO/IEC ガイド 51 に述べられている定義、“許容可能なリスクとは、その時代の社会の価値観に基づく所与の 状況下で，受け入れられるリスク ”に対応している。

表 AP10-１　リスク、危害、頻度のレベルの例

A　危害のひどさ
１：無視可能な
２：軽微な
３：重大な
４：破局的な

B　頻度
１：信じられない
２：起りそうにない
３：あまり起らない
４：ときどき起る
５：かなり起る
６：しばしば

C　リスクの大きさ
１：無視可能なリスク
２：許容可能なリスク
３：受け入れられないリスク
４：まったく受け入れられないリスク

表 AP10-２　リスクマトリックスの例

B ＼ A	1	2	3	4
1	1	1	1	1
2	1	1	2	2
3	1	2	2	3
4	2	2	3	4
5	2	3	4	4
6	3	4	4	4

実際にどのレベルの大きさのリスクならば許容可能とするかに関しては、現実には、ALARP（As Low as Reasonably Practicable：合理的に実現可能な程度に低い）原則が用いられている。すなわち、無視可能なリスクや広く受け入れられるリスクに関しては、それ以上のリスク低減は求めず、許容できないリスク以上に関しては、特別な状況を除き正当化されないとする。この両者の間の大きさのリスクに関しては、合理的な理由がない限り、できるだけリスクを低減する努力をすべきである、という原理である。実際には、この許容可能な領域（許容領域）を ALARP 領域と称して、いくつかのリスクレベルに分けて、リスクを下げる目標、すなわち、危害のひどさを下げるか、または頻度を下げるかの指標とする場合が多い。以下に、その例として、我が国で開発され、用いられている R-Map の考え方を以下に紹介する。

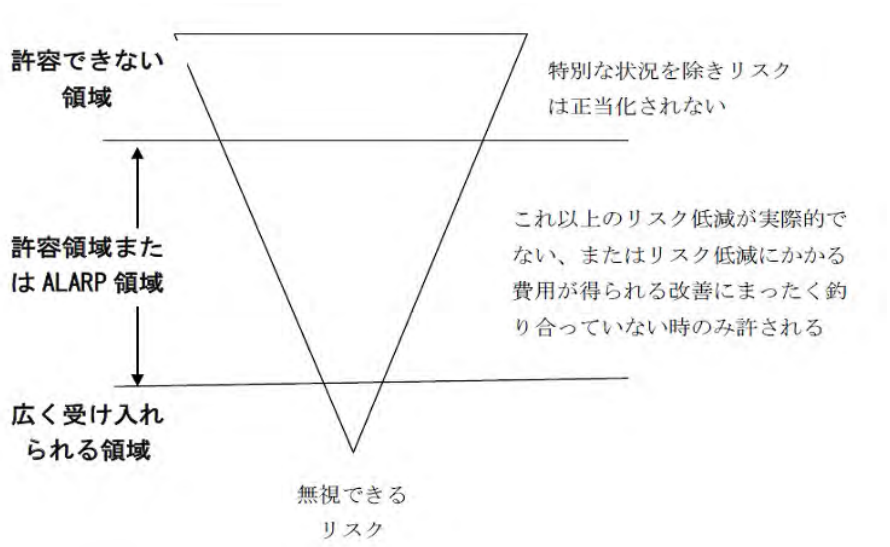


図 AP10-２　ALARP (As Low As Reasonably Practicable)の原理

３．R-Map による許容可能なリスクとリコールの判定

R-Map(Risk Map)は、松本浩二氏を中心にして、日本科学技術連盟の「R-Map 実践研究会」で開発され、現在、各企業で安全目標として盛んに活用されているだけでなく、経済産業省及び NITE ではこの値を採用してリコール判断の参考にしている。以下この項の資料は全て、松本浩二氏の資料に基づくものである。

表 AP10-３が、R-Map の基本構造であり、マトリクス法に基づいている。危害の発生頻度を０レベルを入れて６レベル、危害のひどさを０レベルを入れて５レベル、リスクは、大きく分けて、A 領域（許容できない領域)、B 領域（許容可能な領域)、C 領域（無視、又は無傷の領域）の３領域とし、更に、A 領域を A1,A2,A3 の３レベル、B 領域を B1,B2,B3 の３レベル、C 領域は１レベル、従って、リスクは、７レベルに分けられていることになる。ここで、C 領域は、まったく安全と考えられる領域としている。表 AP10-３では、頻度も程度も定性的な言葉で表されているが、その具体的な例が、表 AP10-４と表 AP10-５に示されている。

表 AP10-６に、消費生活用製品に使用する具体的な数値と程度を記入した R-Map を示す。この表では、発生頻度のゼロレベルを 10^{-8}/(台、年)としている。すなわち、死亡事故の発生する場合、安全と見なせる領域としての安全目標は、頻度（確率）として、10^{-8}/(台、年)としていることが分かる。

R-Map は、発売した製品が市場で事故を起こし、事故率を見た場合、もし A 領域にあるなばら販売禁止とし、B 領域になるならば、リコールすべきであると判断される、というような使用の仕方をする。更に、それらを安全な領域に持って行くためには、設計で対応するとすれば、事故の頻度をどの位下げ、危害のひどさをどのレベルになるように設計すれば良いかといった判断にも用いられる。

表 AP10-３　R-Map

発生頻度							
5	頻発する	C	B3	A1	A2	A3	A領域
4	しばしば発生する	C	B2	B3	A1	A2	
3	時々発生する	C	B1	B2	B3	A1	
2	起りそうに無い	C	C	B1	B2	B3	B領域
1	まず起り得ない	C	C	C	B1	B2	
0	考えられない	C	C	C	C	C	C領域
		無傷	軽微	中程度	重大	致命的	
		0	Ⅰ	Ⅱ	Ⅲ	Ⅳ	
		危害の程度					

表 AP10-４　危害の程度

	定性的な表現		人に対する危害	火災
Ⅳ	致命的	Catastrophic	死亡	火災、建物焼損
Ⅲ	重大	Critical:	重傷、入院治療を要す	火災
Ⅱ	中程度	Marginal:	通院加療	製品発火、製品焼損
Ⅰ	軽微	Negligible	軽傷	製品発煙
0	無傷	None	なし	なし

IEC規格等

医療機器の法規制
欧州RAPEX法規制

家電製品協会

⇒経済産業省リスクアセスメント基準

表 AP10-５　発生頻度

レベル	定性的な表現		定量的表現（件/台・年）		
5	頻発する	Frequent	10-2超	10-3 超	10-4 超
4	しばしば発生する	Probable	10-2以下 ～10-3超	10-3 以下 ～10-4超	10-4 以下 ～10-5超
3	時々発生する	Occasional	10-3 以下 ～10-4超	10-4 以下 ～10-5超	10-5 以下 ～10-6超
2	起りそうに無い	Remote	10-4以下 ～10-5超	10-5以下 ～10-6超	10-6以下 ～10-7超
1	まず起り得ない	Improbable	10-5以下 ～10-6超	10-6以下 ～10-7超	10-7以下 ～10-8超
0	考えられない	Incredible	10-6以下	10-7以下	10-8 以下

IEC規格等

R-Map; 0レベルは製品による

表 AP10-６　消費生活用製品に使用する R-Map

発生頻度							
5	(件/台・年) 10-4 超	頻発する	C	B3	A1	A2	A3
4	10-4 以下 ～10-5超	しばしば 発生する	C	B2	B3	A1	A2
3	10-5 以下 ～10-6超	時々 発生する	C	B1	B2	B3	A1
2	10-6以下 ～10-7超	起りそうに ない	C	C	B1	B2	B3
1	10-7以下 ～10-8超	まず 起り得ない	C	C	C	B1	B2
0	10-8 以下	考えられ ない	C	C	C	C	C
			無傷	軽微	中程度	重大	致命的
			なし	軽傷	通院加療	重傷 入院治療	死亡
			なし	製品発煙	製品発火 製品焼損	火災	火災 (建物焼損)
			0	Ⅰ	Ⅱ	Ⅲ	Ⅳ
			危害の程度				