報　告

工学システムに対する
社会安全目標の基本と各分野への適用

平成２９年（２０１７年）９月２０日

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

この報告は、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・リスク検討分科会が、安全目標の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・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

委員長	松岡　猛	（連携会員）	宇都宮大学基盤教育センター非常勤講師
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代表理事・研究所長、東京農工大学名誉教授
幹　事	須田　義大	（連携会員）	東京大学生産技術研究所教授
幹　事	水野　毅	（連携会員）	埼玉大学大学院理工学研究科教授
	遠藤　薫	（第一部会員）	学習院大学法学部教授
	大倉　典子	（第三部会員）	芝浦工業大学工学部教授・学長補佐
	柴山　悦哉	（第三部会員）	東京大学情報基盤センター教授
	桑野　園子	（連携会員）	大阪大学名誉教授
	高橋　幸雄	（連携会員）	東京工業大学名誉教授
	萩原　一郎	（連携会員）	明治大学　研究知財戦略機構・特任教授
	松尾亜紀子	（連携会員）	慶應義塾大学理工学部教授
	宮崎　恵子	（連携会員）	国立研究開発法人海上・港湾・航空技術研究所海上技術安全研究所運航・物流系運航解析技術研究グループ長
	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会長、東京大学名誉教授
	成合　英樹	（特任連携会員）	筑波大学名誉教授
	藤原　修三	（特任連携会員）	国立研究開発法人産業技術総合研究所安全科学研究部門名誉リサーチャー

安全目標の検討小委員会

委員長	成合　英樹	（特任連携会員）	筑波大学名誉教授
副委員長	野口　和彦		横浜国立大学リスク共生社会創造センター 大学院環境情報研究院教授
幹　事	中村　昌允		東京工業大学大学院環境・社会理工学院特任教授
	柴山　悦哉	（第三部会員）	東京大学情報基盤センター教授
	淺間　一	（連携会員）	東京大学大学院工学系研究科教授
	鈴木 真二	（連携会員）	東京大学大学院工学系研究科教授
	須田　義大	（連携会員）	東京大学生産技術研究所教授

坂井　修一	（連携会員）	東京大学大学院情報理工学系研究科教授
永井　正夫	（連携会員）	一般財団法人日本自動車研究所代表理事・研究所長、東京農工大学名誉教授
松岡　猛	（連携会員）	宇都宮大学基盤教育センター非常勤講師
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		横浜国立大学客員教授
山田　常圭		総務省消防庁消防大学校消防研究センター所長

本提言の作成にあたり、以下の方に御協力いただいた。

山田　陽滋　名古屋大学大学院工学研究科教授

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	石井　康彦	参事官（審議第二担当）（平成 29 年７月まで）
	粂川　泰一	参事官（審議第二担当）（平成 29 年７月から）
	松宮　志麻	参事官（審議第二担当）付参事官補佐（平成 29 年７月まで）
	髙橋　和也	参事官（審議第二担当）付参事官補佐（平成 29 年７月から）
	柳原　情子	参事官（審議第二担当）付審議専門職

要　　旨

日本学術会議は、2014年に「工学システムに対する社会の安全目標」（以下2014年報告と記す）を報告として取りまとめた。2014年報告は、工学システムの安全に関する現状を調査し、工学システムの社会安全目標の基本的考え方を整理し、具体的な目標として死亡に関する目標にALARP[1]の概念を採用し、その定量的基準値を提案した。本報告は、2014年報告の用語やALARPの適用範囲について見直しを行うと共に、2014年報告について安全工学シンポジュウム等において寄せられた規制と安全目標等の関係についても整理した。さらに、工学システムの各分野の特徴を踏まえ安全目標の適用について検討を行い、基本的な考え方の有効性と課題を明らかにして社会安全目標の実効性を高めるための検討内容について取りまとめた。

安全を考える際には経済的発展や国際競争力との兼ね合いで考えることが重要であり、本報告では最新のリスクの考え方であるポジティブとネガティブの影響を共に考えることの重要さを含めた総合評価の考え方を示すとともに、各分野での適用検討の結果を受け、基本的考え方の改定を行った。

2014 年報告からの改訂の概要は、以下の通りである。

１　安全目標の基本的考え方の改訂

本報告では、2014 年報告で検討を行った安全目標の基本的な考え方に関する見直しを行った。

まず、安全の定義の用語の変更を行った。本報告では、ISO/IEC ガイド 51 の定義を採用しているが ISO/IEC ガイド 51（1999 年）の「受け入れ不可能なリスクのないこと」から、2014 年改訂で「許容不可能なリスクのないこと」に変更されたので、本報告においても用語を変更した。

次に、安全目標と規制の関係を整理し、安全目標の必要性を明らかにした。

そして、本報告では、安全目標の基本的な考え方として、ALARP の考え方を人命に関する目標だけでなく一般的な分野に適用することとした。そして、ALARP の考え方に基づき、安全目標の基準として、達成出来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）の二つの基準を定め、その位置づけを以下の様に明確化した。

① Ａ基準は、事業者と社会との合意事項によるものとする。
② Ｂ基準は、その領域の関係者の意思・合意によって定められることが望ましい。
③ Ａ基準とＢ基準との間は ALARP 領域とし、便益、コスト、リスクの兼ね合いで目標を定め、設定した目標値については不断の改善努力を行う。

さらに、安全目標に関するリスク論の適用の意味を整理し、その具体的な適用において死亡リスクを目標に採用する場合の時間単位の検討を行い、「／年」を基本とし、「／生涯」

[1] ALARP は"as low as reasonably practicable"の略で ALARP の原則とはリスクは合理的に実行可能な限り出来るだけ低くしなければならないという考え方である

は慢性毒性のように一過性ではない影響に対してのみに使用することとした。

また、安全目標の一つとして多様なリスクのバランスを考えた評価方法の考え方を提案したが、その具体的な手法に関しては、今後の課題とした。

本報告では、安全目標に基づいた社会安全を推進していく際の行政、企業、有識者、市民の役割を整理し、ALARP の考え方を参照した際の許容する安全レベルを決定する判断の仕組みを提案した。

２　工学システムカテゴリー毎の特徴とプラント系システムの安全目標の提案

本報告では、安全目標の適用を実効性のあるものにするために、安全目標の設定方法を整理し、５つのタイプに分類した。

また、労働災害（労災）を各分野共通の一つとして、工学システムを７つのカテゴリーに分類し、それぞれの工学システムの特徴を整理した。

そして、2014 年報告で検討したそれぞれの規制等の現状の安全に対する考え方も踏まえ、工学システム毎に安全目標を検討する際の目標タイプの検討を行った。

さらに、プラント系の安全目標のあり方に関して、議論を行って提案を取り纏めた。他の工学システムに関しては、その特徴を整理して安全目標タイプを検討する段階に止まっており、具体的な安全目標の提案は、今後の検討課題としている。

本報告では、現状の安全の考え方も取り入れ、リスク論による目標と同時に確定論に基づく安全目標のあり方も付加している。また、分野によっては、現在の状況に加え、今後の技術進展を見込んだ安全の考え方を提案している。

３　工学システム安全に関する要求事項

工学システム安全を検討・評価する際の要求事項を以下のように取りまとめた。

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）と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、それまでに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。さらに、発生確率がゼロでない以上、事故は起こり得るので、起こった後の対策も考慮しておく必要がある。

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、ネガティブ双方の可能性）を勘案して決定することが望ましい。

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、算定したリスクの分析条件を提示し、リスク基準との比較における判断に必要な情報を付加することが求められる。

目　　次

１　はじめに

日本学術会議は、2014年に「工学システムに対する社会の安全目標」（以下2014年報告と記す）を報告として取りまとめた。本報告は、この2014年報告の考え方を工学システムの各分野へ適用し、各分野の特徴を踏まえた安全目標に関する適用の要点を取りまとめたものである。

安全は社会における重要な価値であり、事故や災害による大きな被害を無くすことを常に目標として掲げておく必要がある。しかし、社会には安全に影響を与えるリスクが複数存在し、しかもそれらのリスクが互いに関係を持っていることに留意すると、その安全活動は、理念的な安全の追求に止まらず実効性を如何に確保するかを考える必要がある。

社会の安全を実効的に向上させるためには、その時代において社会の安全に影響を与える様々なリスクに対し具体的な目標を設定して、対応していく必要がある。したがって、安全を考える際には経済的発展や国際競争力との兼ね合いで考えることが重要であり、本報告では、ポジティブとネガティブの影響を共に考えることの重要さを含めた多様な影響のバランスを考慮した評価の考え方を示すとともに、各分野における検討の結果を受け、基本的考え方の改定も行った。

２　2014 年報告の概要

(1)　作成の背景

工学システムは、その時々の社会が求める価値を実現するために最適な方法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り、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。

安全の目標を、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。2014 年報告では安全目標は時代ととも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

2014年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/IECGuide51：1999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、経済、物理的被害、社会的混乱等とした。

報告における基本的考え方は、以下のとおりとした。

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、経験したことの無い事故を未然に防止することも重視する。

３）　安全目標は、人命に加え、社会リスク[2]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である。

2　社会や生活の活動に影響を与えるリスクのことである

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) 2014 年報告の要点

① 安全目標の設定

安全目標の設定においては、人命を対象とした目標と社会リスクに対する目標に分けて検討を行った。

ア 人命を対象とした目標の考え方

安全目標としては、人命を対象とした目標では、達成出来ないことが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するという考え方を定めた（図１参照）

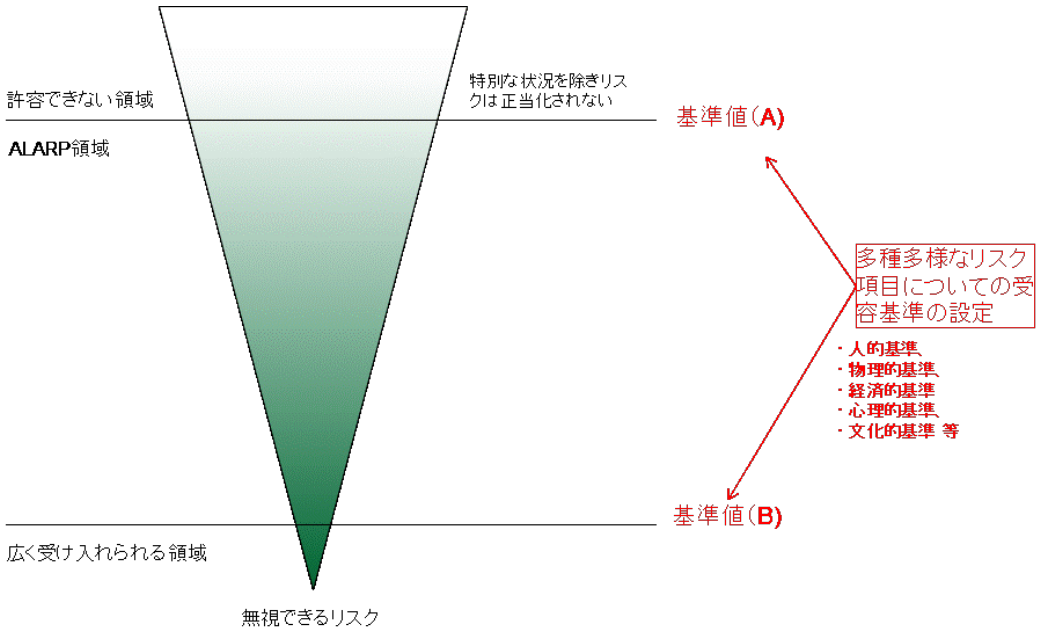

図１ 安全目標の基本概念

（出典）2014 年報告から修正して作成

不特定の個人に影響を与える工学システムに関しては、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とした。

さらに、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と考えられるとした。

イ 社会リスクを対象とした目標の考え方

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、対象となる事故の発生確率を低下させたり事故が発生した際の被害を軽減したりする対策を実施し、提案する安全目標を達成することを求めることとした。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、望ましくない事象の起こる頻度（発生確率）を小さくすることが求められるとした。この社会リスクの目標に

おいては、経済的影響が大きいリスク、環境的影響が大きいリスク、物理的被害の規模の大きいリスクにわけてその考え方を取りまとめることとした。（参考資料２ AP１　参照）

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。

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）とその目標とするレベル（安全目標）を明らかにし、運営時にはその安全レベルを最新の情報の下で検証した結果を公開することとした。

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、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、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や、最新の知識や環境の変化を反映することとした。

③　工学システムに関する安全に関与した許認可に関する役割分担

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こととした。

事業者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事業者が判断をすることが望ましい。事業者はそのガイドラインを最低基準として、自分の責任において安全目標を明確に示し、安全を向上する責任を持つとした。

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・報告する責務を持ち、市民は、科学技術のシステム・製品を安全に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とした。

ただし、科学技術の多様さ複雑さに鑑みた場合、全ての工学システムに対して、市民の一人ひとりが深く理解することは困難なので、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もに、その判断が市民から信頼される状況を作る必要があるとした。

３　安全目標の基本概念の再構築

(1)　安全目標の基本的な考え方

①　対象とする安全の概念について

ア　安全の定義

工学システムの安全目標を検討する際には、その目的である安全の考え方を明らかにすることが重要である。本報告では、安全を「許容不可能なリスクがないこと」（ISO/IECGuide51 の定義）[3]と定義する。（ISO/IECGuide51 の安全の定義が変更され

[3] これまでの「受容できないリスクがないこと」からの用語の変更である。これは英語表記が「acceptable risk」から

たので安全の定義やALARPの図の基準の名称も最新のものに変更した。）

このことにより、安全か否かの判断は、科学的分析結果を参考に社会状況等も踏まえ行うことになるが、その前提となる望ましい社会像を合意する必要がある。

イ　安全目標の対象となる事項

安全を検討する際の対象は、従来から検討の重要項目となっている生命、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、環境への影響に加え、情報、経済、物理的被害、社会的混乱、日常生活の不便等の多様な事項とする。

これらの影響は種類も大きさも様々であり、それぞれの工学システムにおいて対応すべき事象は異なる。本報告において社会の安全目標を定める対象は、各工学システムにおいて重大事故と定めるものとする。重大事故の考え方は、４．(2) で説明する。

また、工学システムの事故は、如何に安全対策を強化しても発生を0に抑えると事は難しいので、事故・災害発生後の対応も大変重要である。

安全目標は、それぞれの対象指標への影響とともに、社会への影響を総合的に評価することも必要となる。

ウ　安全を検討する際の事故・災害のハザード[4]

安全を検討する際のハザードは、自然現象、人的要因、機械的要因、化学的要因、システム的要因等の全ての要因を対象とする。

エ　安全を向上するための施策[5]

安全対策は、未然防止、再発防止、拡大防止、回復力の向上、迅速な復興等を含む。

②　安全目標と規制との関係

工学システムの安全に関して遵守すべき重要な事項は、規制によって定められている。しかし、規制の制定は、対象とする工学システムに関して多くの検討がなされた上で定められているが、工学システムに採用される技術の進展や機能の高度化・複雑化を常に規制に反映することは難しい。したがって、規制を遵守していれば事故が発生しないことが保証されているわけではなく、事故の発生が免責されるわけでもない。

社会や企業が新たな工学システムを高度化し、社会の豊かさや企業の発展を目指す限り、社会における必要条件である規制を遵守していることに満足するのではなく、活用する工学システムの特徴に応じ、その開発・運用者は、自ら安全目標を設定しその達成を目指すことが望ましい。

また、今後、工学システムの活用により豊かな社会構築のためにも、安全に関する規制と安全目標のあり方を行政・企業・市民で共有し、安全に関する新たな社会の仕組みを構築していくことが望ましい。

③　安全目標の要件

「tolerable risk」への変更に基づく表記の変更であり、示している内容に変更はない。

4　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。

5　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。

ア　目標は、達成可能なものであり社会的公平性を持たなくてはならない。

1）　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。

2）　目標は、技術的合理性、経済的合理性を含めて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。また、常に社会状況や技術の進化を反映したものである必要がある。

3）　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望ましい。

イ　目標は、社会や技術の状況によって定めるべきものである。

1）　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・技術的実現性、選択肢の有無等によって変わることを前提とする。

2）　目標と比較される各工学システムの現状を示すリスク指標は、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[6]。

ウ　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。

1）　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。

2）　多くの人にとり、解釈が容易で明確であるものとする。

エ　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。

1）　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。

2）　供給者・管理者として、施策に反映できるものでなければならない。

3）　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。

オ　目標は、人々に希望をもたらすものでなくてはならない。

1）　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。

(2)　安全目標の実用化に向けての提案概要

2014 年報告で提案した安全目標の基本的考え方に関する補足事項は、以下の通りである。

①　ALARP の考え方に基づく安全目標の基本概念を人命に関する目標への適用から一般的な安全目標の基本概念に拡大する（図１参照）

図１におけるＡ基準は、この基準を満足しないと社会から受け入れられない基準と位置づける。また、Ｂ基準は、大きな社会環境や技術に関する変化が無い限りこれ以上の安全レベルの高度化を求めなくても良い基準として位置づける。Ａ基準やＢ基準に採用するリスク指標は、対象となる工学システムにおいて、判断の際に特に重要となるリスク指標を採用する。工学システムによっては、Ａ、Ｂ基準共に、複数のリス

6　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。

ク指標を基準として採用する場合もあり得る。

また、A基準とB基準の差異は、その数値的な基準値の差異として示すとは限らず、基準と比較する工学システムの現状リスクの評価範囲の要求等の条件の厳密さの違いとして示すこともある。

なお、本報告におけるA基準、B基準と比較するリスクは、社会に重要な影響を与えるものを対象としており、影響の小さなトラブル事故は対象としていない。

② リスク指標を用いた安全目標について（3．(3) 参照）
リスクを考える時間単位について整理を行った。また、多様なリスクのバランスを考えた新たな評価方法について提案を行った。

③ 許容できる安全のレベルを判断するシステムのあり方について検討を行った（3．(4)参照）

④ 社会安全目標の工学システムの各カテゴリーの特徴と安全目標の適用（4章参照）

1） 安全目標の実用化に向けての安全目標タイプに関する体系化を行った。

2） 安全目標を設定する際の工学システムの特徴と安全目標設定の要点を整理し、そのカテゴリーに応じてリスク論と確定論による安全目標を併用する。

(3) リスク指標を用いた安全目標について

安全目標の基本的な構造としているALARPには、A基準、B基準の二つの基準を設定する必要がある。

2014年報告においては、一般的な基準値の考え方を示したが、各工学システムに具体的な目標として設定する場合は、2014 年報告および本報告の示す考え方を参考にして、各工学システムの特徴や社会における位置づけ等を考慮し、主体者が個別に設定することが望ましい。

工学システムがもたらす被害の中で死亡事故や環境に大きな被害をもたらす事故は、その発生を認めるという前提では稼働することはできない。したがって、工学システムの安全目標としてそのような事象が発生しないようにするということは、工学システムの社会安全目標の基本理念であり、欠かすことができない理念である。

しかし、このことから発生確率を0とするという目標を掲げると、ほとんどの工学システムが稼働できなくなることにも留意する必要がある。小さな質量やわずかなエネルギーも人の命を奪う可能性がある。また、環境等に影響を与える物質は、如何なる防護策を講じようとも環境への影響を理論的に0とすることはできない。

したがって、安全目標の達成を一定期間の事故発生の実績ではなく、リスク指標によって検証しようとすると、その発生確率を0とする目標をたてるということは、最初からその工学システムの稼働が認められないという結論になる可能性があることを認識しておく必要がある。

以下に、リスク指標を使用する事項に関して2014年報告からの改訂事項を記す。

① 死亡リスクを目標に採用する場合の検討

死亡リスクは、多くのシステムに目標指標として適用されているが、その適用対象

に関しては、以下の事項の考慮が必要である。

１） 死亡対策として、事故の発生防止、事故進展の拡大防止、市民の避難等の施策が存在する場合は、その全ての施策に関する実効性を踏まえた評価を行う。その際、施策の責任組織を考慮し責任組織毎の目標を設定する方式をとっても良い。

２） 工学システムの運営責任を持つ組織の安全目標としては、１回の事故で（広い範囲で）多くの死傷が発生する事故に対して、死亡リスクではなくその事故の発生確率を目標として設定しても良い。

３） 影響が一過性でない事象に関しては、障害の影響を生涯にわたって考えることが望ましい。

発生確率を考える際の単位時間は、環境や人体に対する慢性毒性等の様に蓄積性がある影響に関しては、/生涯（想定 100 年と考える）という単位を、単一事故影響が短期間に限定される場合は、/年で検討することが望ましい。

② Ａ基準、Ｂ基準の設定について

基本的には、Ａ基準は事業者と社会との合意事項であり、Ｂ基準はその工学システムの社会実装を行う関係者の意思によって定めることが望ましい。少なくともＡ基準、Ｂ基準は、その領域に適用されている法律、規制等との関係を明らかにしておくことが望ましい。

Ａ基準とＢ基準との間の判断は、ALARP 領域として、便益、コスト、リスク低減により得られるメリットと低減に要するコストとの兼ね合い、さらには他のリスク状況との兼ね合いで目標値を定めるべきである。

③ 多様なリスクのバランスを考えた評価による許容判断の考え方

この考え方は、Ａ基準とＢ基準の間のどこを許容レベルとするかという判断に、多様なリスクのバランスを考えた評価（以下総合評価と記す）の指標を採用する考え方であり、この考え方を採用する理由は二つある。

理由の一つは社会の求めるリスク基準が複数あり、一つの指標を満足したとしても他の指標を満足していないシステムは受容できないために、安全の判断に必要な指標を全て検証する必要があるからである。しかし、全ての指標を満足するという考え方だけであれば、すべての指標を一つ一つ検証すれば良いのであるが、総合評価を行うための指標（以下総合指標と記す）の必要性は社会に存在する多様なリスクは、独立ではなく、あるリスクを小さくすれば、別のあるリスクは大きくなるという関係がある。そのために最終的にはどのリスクをどのようなバランスで受け入れるかを選択する必要がある。この状況を考えると、社会や組織運営において、ある種のリスクと共生をする必要があるということが、総合指標の設定の基本的な考え方である。総合指標の使用フェーズは、新製品・システム開発時、行政の規制時、既存のシステムの変更時等の幾つかのフェーズがある。

理由のもう一つは、多様なリスクのバランスを考えた総合指標の設定の難しさで、評価対象とするリスクの種類が異なるため、単なる数値やランクの加算等で評価するというわけにはいかないことである。

総合指標の考え方は複数あり、対象とする工学システムや領域によって、より適した手法を活用することでよい。

総合指標の設定のために実施すべきことには、二つのステップがある。

第一は、対象とする工学システムが社会にもたらす全ての重大な影響に関する指標（リスク指標）を整理し、それぞれのリスクを検討することである。この検討すべき影響には、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）、プライバシー、利益、財産、環境への影響に加え、情報（喪失、漏洩）、経済影響、物理的被害、社会的混乱、日常生活の不便等が含まれるが、実際に検討を行う具体的なリスク指標に関しては、対象工学システムによって選択をしても構わない。

第二は、異なるリスクをその価値により重みを乗じて総合的に評価することである。その重みを企業で判断する場合は、経営者の価値観を反映することになり、社会としての判断の場合は、市民価値を含めた社会全体の影響・利益に鑑みてその社会の価値を反映することになる。重みの設定は、各リスクの価値観を階層分析法等で社会価値を定量化してリスクの重みとする方法や、リスクをその影響の共通なものを同じカテゴリーとして整理してリスクのランク評価を行い、カテゴリー間の重みを設定しリスクのランクにカテゴリーの重みを考慮して、そのリスクを評価する等の幾つかの手法がある。

複数のリスクを総合的に評価する指標を与えるモデルは、今後の課題である。

④　リスクの許容を判定する際に注意する観点

1）　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必要がある。

2）　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。

3）　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。

4）　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。評価に使用するリスク分析に求められる品質に関しては、４．(4) ④を参照されたい。

5）　リスクの低減対策は、その対策の効果を明らかにする必要がある。

(4)　許容できる安全のレベルを判断するシステム

安全目標を社会において活用するためには、安全目標の基本構造である ALARP の考え方を満足しているリスクに対して、そのリスクをどのレベルで許容するかという最終判断を誰がどのように行うかという仕組みを明らかにしておく必要がある。この判断には、安全、社会的混乱等の様に国等（自治体、国際標準化機構も含む）がガイドラインを示すことが望ましいものと、ある種の経済的影響の様に市場によって決められるものがある。

工学システムを許容する安全レベルの決定に関しては、以下の仕組みを提案する。

①　安全レベル決定の基本

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

体が行うことが基本である。

規制を満足した工学システムの稼働に関しては、事業者が主体となって実施するさらなる安全活動を前提とした判断を尊重することが望ましい。事業者の判断においては、国等が社会安全の視点から望ましいレベルを示す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システムに対しては、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。

② 決定の役割

安全目標の設定や安全目標を達成する為の活動は、国、事業者、専門家、消費者や利用者などである一般市民（以下市民と記す）に果たすべき役割が有り、その内容を以下に記す。

１） 国の役割

社会に重要な影響を持つシステムに責任を持つ国（立法・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安全、社会的混乱等に関して、その評価の考え方を明らかにしたうえで、稼動・不稼動を決定する。

２） 事業者の役割

国等が課した規制等を満足するとともに、安全に対する自社の考え方を経営方針、安全方針、安全目標等の形で社会に示すことが望ましい。また、事業者は自社が管理する工学システムの安全状況を、設定した安全目標との比較できる形式で最新の知見に基づき評価・提示することが望ましい。

３） 専門家（学識経験者）の役割

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。

４） 市民の役割

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に鑑みた場合、全ての工学システムに対して、市民の一人ひとりが深く理解することは困難なので、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もに、その判断が市民から信頼される状況を作る必要がある。

4 工学システム各カテゴリーの特徴と安全目標適用のための検討

(1) 安全目標の実用化に向けての安全目標タイプの展開

2014 年報告では、主としてリスク論を活用した安全目標の提案を行ったが、現在活用されている工学システムの中には、現時点では必ずしもリスク論によるアプローチが適当でない分野も存在する。社会安全目標を多様な工学システムに適用するには、安全

目標の考え方を現実に即したものに展開する必要がある。

本章では、対象となる工学システムの特徴を踏まえて、安全目標をＡ～Ｄのタイプ（考え方）に分類し、工学システムのカテゴリーによって、いずれかの目標タイプもしくはその組み合わせを選択するものとする。

＜Ａタイプ＞

このタイプは、安全と見なす環境として、制度・機器、保安距離等の要求事項を設定する考え方である。全ての工学システムにおいて、このタイプの規制・基準は存在するが、ここでＡタイプと分類するのは、このタイプの目標が大部分を占めるものをいう。

＜Ｂタイプ＞

このタイプは、毎年被害が複数発生する状況下において、被害の発生件数や減少数を目標として示し、安全を向上する考え方である。

＜Ｃ１タイプ＞

このタイプは、リスク指標を安全目標に採用するものであり、死亡被害の様に単一指標において、リスクの要素の内、発生確率を安全の指標とする考え方である。

＜Ｃ２タイプ＞

このタイプは、リスク指標を安全目標に採用するものであり、人的リスク（死亡、怪我等の被害の種類とその発生確率の組み合わせ)、物的リスク（被害の大きさと発生確率の組み合わせ）の様に、リスクを安全の指標とする考え方である。

＜Ｄタイプ＞

リスク指標を安全目標に採用するものであり、Ａ、Ｂ基準は、重要なリスク指標を採用するが、その間の許容レベルの判断は、複数のリスクから社会・組織の価値を考慮して総合的な指標を作成し、安全の指標として示す考え方。Ａ、Ｂ基準自体に総合的な指標を採用する場合もある。

なお、本報告におけるＡ基準、Ｂ基準に比較するリスクは、重大事故を対象としており、本安全目標の提案では影響の小さなトラブル事故までを対象としていない。

Ａ～Ｃまでの考え方は、これまで各分野において既に採用されている事例もあるが、各工学システムへの適用において、検討すべき事項も存在する。また、Ｄタイプに関しては、学術会議の 2014 年報告以外にはこれまで具体的な提案がなされておらず、より詳細な検討が必要となる。

⑵　各工学システムカテゴリーの特徴と安全目標設定の要点と検討課題

工学システムの安全に関する規制等の動向、安全への取り組みに関しては、2014 年報告に取りまとめている。本報告では、その検討も参考にして、安全目標を検討する際に考慮すべき工学システムの特徴を検討し、分類した。

工学システムへの安全目標の適用を検討する際には、その特徴を考慮した安全目標を設定する必要がある。本項では、2014 年報告で検討した工学システムの規制等の安全への考え方と、工学システムの特徴を考慮して、安全目標の具体案を検討する際の安全目標のタイプの検討を行った。安全目標を制定する際の工学システムのカテゴリ

一分類案を表１に示し、各カテゴリーの特徴および安全目標の検討時に考慮すべき視点を以下の通り整理を行った。

表１　工学システムのカテゴリー

カテゴリー	カテゴリーに含まれる工学システムの小分類と説明
① プラント系	原子力プラント、化学プラント　等
② インフラ系	（ア）土木・建築
	（イ）電力・ガス・水道ネットワーク
	（ウ）鉄道・船舶・航空
③ 自動車	
④ ロボット	産業用ロボット、生活支援ロボット　等
⑤ 情報システム	
⑥ 製品安全	工学システムが生み出す製品の安全として目標対象とする
⑦ 労働災害	全工学システムに共通の労働者の安全として目標対象とする

①　プラント系

ア　工学システムの特徴

一度の事故で一般市民の生命健康、社会経済や環境に大きな影響をもたらす可能性のあるシステムのカテゴリーである。

イ　安全目標の対象とする重大事故

プラント系の工学システムが安全目標とする重大事故は、以下の通りとする。

１）　オフサイト１名またはオンサイト複数名以上の死亡者が発生する事故

２）　多数者に健康の被害を与える事故

３）　広範囲に環境被害を与える事故

４）　製品・サービスの供給停止も含めて、経済・社会活動に関して大きな影響をもたらす事故

ウ　考慮すべき安全目標の検討の視点

この項はプラント特有の事故を対象としており、プラントで発生する労災は、⑦労災での考え方を参照されたい。このことは、以下の他のカテゴリーについても同様である。

このカテゴリーの安全目標においては、安全目標が対象とする重大事故を明示して安全目標の達成を目指す必要がある。特に社会に大きな影響を及ぼす巨大事故に対しては基本的に事故を発生させない努力を行うものとする考え方を社会と共有する必要がある。評価の対象とする事故は、規制において求められる事故を考える際の条件に限定せずその時点で想定しうる災害規模をリスク評価の対象とすることが望ましい。

このカテゴリーの重大事故に関しては、設備設計においてその対応を考慮し、大きな事故に至らないシステムを構築することが求められる。プラント系の事故は小さな事故の発生頻度を減らすという考え方も必要であるが、重大事故は設計

に起因して発生する事例も多く、設計段階において重大事故のシナリオを予測し、リスク低減対策を優先的に実施することが重要である。

一方、近年、化学プラントでは設備の経年劣化や老朽化による事故やトラブルが増加しており、維持管理対策が重要になる。安全の状況は常に見直さなければ安全レベルが低下する。リスクアセスメントは人や設備の変化も含めて、一定期間ごとに繰り返さなければならない。また、変更管理（変更に伴う新たなリスクを想定して対策を講じること）の不備に起因する事故が増えており、専門技術者の関与が望ましい。

事業者は、現状リスクと安全目標を比較する場合には、そのリスク分析のモデルに対する情報や対象としている要因、使用データ等の評価情報を付加して、評価しているリスクの内容を明確にする必要がある。また、リスク論には、目標と比較する現状のリスクに関して、検討している事象のシナリオ（原因・トラブル拡大の考え方）の十分性を如何に担保するかという課題が存在することも認識する必要がある。

安全目標の対象とする事象や活動の範囲をどう設定するかによって、目標の立て方が変わってくることにも留意する必要がある。

安全目標指標として一般市民の人的被害指標を設定すると、その対応には工学システムの安全対応に加えて住民避難と消防等の行政による防災対応も検討対象となる。

（ア） 対象を事業者とした場合：自治体の避難活動の成果を期待せずに、大規模な事故の発生確率や影響の及ぶ範囲を制限する目標を設定することになる。

（イ） 対象を自治体や市民にまで広げた場合：人的リスクや放射性物質、化学有害物質の漏えいなど環境影響を目標とする。

エ　目標に採用する安全目標のタイプ

アからウまでの工学システムの特徴と現在の規制等の状況を踏まえると、安全目標としては、Ｄタイプの適用が望ましい。

②　インフラ系

ア　工学システムの特徴

日常生活の基盤となっているシステムであり、その運営は組織的に行われている。

イ　安全目標の対象とする重大事故

安全目標が対象とする重大事故は、それぞれのシステムにおいて社会に重要な影響を与えるものとして別途定めるが、ユーザー・供給者・運用者等の死亡事故に止まらず、サービスの停止により社会生活に大きな影響を及ぼす事象も対象とするべきである。また、サービス停止後の復旧・再開までの時間も安全目標として設定することが望ましい。

ウ　考慮すべき安全目標の検討の視点

社会活動や一般市民の生活に多大な影響をもたらす可能性のあるシステムであ

り、広範囲に影響を及ぼす事故の防止と同時に災害時の復旧指標の目標設定も重要である。

（ア）　土木・建築

想定される地震、風水害などの自然外力および火災等の災害に対して、個々の建造物の社会的役割に応じた安全目標レベルを設定するとともに、それを達成するための(社会的合意の得られた)設計要件と施工要件を明示することが重要である。

一般に数十年以上の長期にわたって使用に供されるインフラ系の建造物は、経年劣化に加えて用途変更や社会変化等に伴う使途変更などにより安全性能が変化することから、その維持・管理を含めた安全目標を設定することが望ましい。

安全目標が対象とする重大事故は、その事故で一度に多数の人に傷害が生じたり社会活動に大きな支障を及ぼす事故とする。

リスク評価を用いたメンテナンスも重要な安全目標の一つである。

以上の対象システムの特徴と現在の規制等の状況を踏まえると、本システムの安全目標は、ＡまたはＣ１タイプの適用が望ましい。

（イ）　電力・ガス・水道ネットワーク

通常時の安全目標と同時に、自然災害遭遇時の復旧目標を安全目標として設定することが必要である。また、社会生活インフラは、電力の様に他のインフラの復旧状況に大きく関わったり、上水や下水の様に相互の関係が密接なものがあったりするため、社会生活インフラとしての総合目標を検討することが必要である。

重要インフラ施設に関しては、安全目標の一環として緊急事態における BCP(事業継続計画)を明確に示すことが求められる。

維持管理においては、システムの重要度を勘案し、老朽化対策等の計画を構築することが重要である。

電力は短期間の停電でも影響が大きい場合がある。

水道、ガスは、供給停止が一定の時間を超えると大きな影響をもたらす場合が多い。

重要な社会インフラにおいては、バックアップ体制や迅速な復旧目標を作っておく必要がある。

以上の対象システムの特徴と現在の規制等の状況を踏まえると、本システムの安全目標は、ＤまたはＢタイプの適用が望ましい。

（ウ）　鉄道・船舶・航空

社会活動や特定の利用者の生命や輸送物に大きな影響を与える可能性のあるシステムであり、利用の利便性と人的被害等への対応のバランスを検討することが望ましい。

a　鉄道

鉄道分野では、脱線、転覆、転落等の各キャリア（貨物車、客車等）の特

徴的な事故への目標を優先としつつも、不通、時間遅れ等の事象の影響を含めて安定輸送に配慮しつつ目標を設定することが望ましい。また、乗客に原因があるホームからの転落のように利用者に責任があるような事象を、利用者の安全に対する役割・安全意識の向上のあり方も含めて、どのように位置づけるかも検討事項となる。特に、踏切問題に対する検討や異常時に如何に被害を減らすかも重要である。

貨物・物流の安全目標は別途定義する。

以上の対象システムの特徴と現在の規制等の状況を踏まえると、本システムの安全目標は、Ｃ２またはDタイプの適用が望ましい。

b　船舶

船舶分野では、国際海事機関の規則策定等にリスク評価が利用されるなど、リスク指標との親和性は高い。これは、海洋開発分野でリスク評価の概念が原子力分野と並んで早期から導入されたことに起因する。ただし、他の交通インフラと異なる船舶固有の特徴も多く、特に、下記の点を考慮する必要がある。

1）　フェリー等の一部の旅客船を除いて、船舶は人の輸送ではなく、物の輸送や漁業等が主要な使用目的であること。

2）　大型船は一隻ごとに異なり、同一の船舶は存在しないこと。

3）　危険物等、積み荷そのものによるリスクが存在すること。

4）　プレジャーボートから巨大タンカーまで、大きさ、操縦性、航行支援機器等のレベルも船舶によって大きく異なること。

5）　日本近海であっても、操船者には外国人も多く、言語による相互コミュニケーションが難しい場合があること。

6）　船舶は原則としてどの海域でも自由に航行できること。

7）　自然環境の影響を大きく受けること。このため、こうした多様性を整理するとともに、国際規則との整合性が求められることにも注意を要する。省エネ化・リスク対応等を総合的に評価する目標が必要である。

以上の対象システムの特徴と現在の規制等の状況を踏まえると、本システムの安全目標は、Ｃ２またはDタイプの適用が望ましい。

c　航空

航空分野では、航空機の安全と飛行場等の安全・信頼性を合わせトータルシ　ステムとして考えることが望ましい。このことは、鉄道、船舶でも同様である。なお、この分野に関しては、検討が開始された状況であるため、望ましい安全目標のタイプに関しては、記述しない。

③　自動車

ア　工学システムの特徴

事故の原因が、製造事業者（クルマ)、道路管理者（ミチ)、利用者（ヒト）等の複数の関係者が関与する工学システムである。また、近年、自動運転等の採用の様にシステムが大きく変化しようとしている分野である。

イ　安全目標の対象とする重大事故

自動車事故における「重大事故」については、国土交通省令（平成 27 年改訂）に明記されている。自動車事故は、年間約４千人もの死者（24 時間以内）が生じている工学システムであり、予防安全技術が実用化され、多くの人命を救える事が認知されるようになると、交通事故は大幅に削減されなければならないという「社会的受容性」そのものが厳しいレベルになってきている。また他の工学システムとは異なり、高齢者に起因する重大事故の増加が無視できなくなっている。

ウ　考慮すべき安全目標の検討の視点

自動車分野の現在の安全目標は、事故による死傷者数を如何に減少するかということが主となっており、リスク論の適用が難しい状況にある。

また、システムの特徴でも記述したように、安全の責任主体はヒト・ミチ・クルマの３者に分けられる。安全目標の設定に関しては、自動車交通システムとしての総合目標を設定するとともに、それぞれの責任組織や利用者の役割を明確にして、それぞれの目標を検討することが望ましい。

さらに、自動運転等のシステムが大きく変化しようとしている状況での安全目標の設定の仕方に関しては、道路交通安全の３要素である自動車の安全技術（クルマ)、道路インフラの整備（ミチ)、道路交通規制・取り締まり（ヒト）が、それぞれ独立には実現しないため、他の領域の安全目標の考え方を取り入れ、安全目標の考え方が、技術の進展に遅れないようにすることが重要である。

安全の指標には、渋滞による社会的・経済的損失も考慮する必要がある。

なお、交通工学の観点から、渋滞による社会的・経済的損失、環境悪化を議論することができる。渋滞の原因には、①事故に起因して発生する渋滞、②インフラ整備の遅れによる渋滞があるが、前者は交通安全に直接関連し、後者はそうではないが、社会的損失という意味では同じで、自動運転により解決が期待されるので、安全目標の設定にも配慮が求められる。

エ　目標に採用する安全目標のタイプ

アからウまでの工学システムの特徴と現在の規制等の状況を踏まえると、安全目標としては、Ｂタイプの適用が望ましい。

④　ロボット

ア　工学システムの特徴

今後、多様な産業や生活の場面に投入される工学システムであり、利用が今後広がる可能性が大きく安全を考える状況設定が難しい分野でもある。

従来の産業用ロボットのように製造機械の一部として位置づけられるものが依然大半を占めるが、今後は多様な産業や生活に投入されることが期待され、歩道走行車両、義肢装具、玩具、軽航空機等他の機械システムと境界を共有し、著しい進展を遂げている情報通信技術を取り込みながら発展して行くことが予想される。その多くが、人間に対して直接サービスを提供することを目的とすることから、機械安全の中で最も人間と直接接触することによるリスクが多様に見積もられるべき

工学システムである。

イ　考慮すべき安全目標の検討の視点

安全目標を設定する上では、製造業を中心としてこれまでロボット産業の進展を支えてきた産業用ロボットと、今後急激な市場拡大が予想されるサービスロボットにカテゴリーを分けて考えることができる。前者は固定形のマニピュレータが中心で、直接のロボットの使用者を対象として使用環境におけるリスクアセスメントの徹底が図りやすく、彼らに対する安全教育も前提にすることが概ね可能である。この観点に立てば、４.⑵⑦労災の考え方が役に立つ。ところが同じ産業用途のロボットでも非製造業である第１次産業用途の場合は、たとえば自動走行農作業トラクター等のように、使用者の教育や彼らにとって安全な作業環境を必ずしも整えられない状況に置かれるため、リスクアセスメントの設計原則に基づく安全技術導入の徹底が求められる。にわかに社会の注目を浴びるようになった、医療・介護施設等で障がい者を対象とする介護ロボットの場合も、使用者は介護者であるが、作業対象である被介護者に重篤度のより高いリスクがあることから、被害形態に応じてリスクの形態をしっかりと定めて安全方策に取り組む必要がある。

これに対し、公共・一般施設や公道で案内、清掃や広告等の作業を行うサイネージ・ロボットや、空撮、物流用途の産業用ドローンのように、使用者のほかに一般の人がリスクに晒される場合では、いまだ産業が黎明期にあり好発要因の分析に足るデータが収集されていない現状に鑑みると、Ａタイプの安全目標も合わせて検討する必要があると考えられる。

ウ　目標に採用する安全目標のタイプ

アからイまでの工学システムの特徴と現在の規制等の状況を踏まえると、安全目標としては、Ｃ２タイプの適用が望ましい。

⑤　情報システム

ア　工学システムの特徴

インフラ系を含む多くの工学システム、さらには金融や電子政府などのインフラにも組み込まれており、これらの制御を司っている。また、ネットワーク化と自動化が進んでいるため、遠隔攻撃の難易度が他の工学システムに比べ低く、被害が広範囲に波及しやすい傾向がある。そのため、事故や攻撃により社会活動に甚大な影響をもたらす可能性がある。

イ　安全目標の対象とする重大事故

情報システムの事故や情報システムに対する攻撃が原因となり、他の工学システムに安全目標の対象とする重大事故が発生した場合にも、情報システムの安全目標としての重大事故と見なすべきである。

また、情報システムのサービスが停止した場合、被害時間と被害を受けた利用者数がある程度多いと「重大」となる。電気通信事業法施行規則（昭和 60 年４月１日郵政省令第 25 号）では、緊急通報を取り扱う音声伝送で、１時間以上の停止または品質低下を３万人以上の利用者が被ると「重大」と定義する。時間と利用

者数の閾値は通信の重要度に応じて異なり、音声伝送を除く無償インターネット接続サービスの場合、24 時間以上かつ 10 万以上、あるいは 12 時間以上かつ 100 万以上のとき「重大」となる。

ウ　考慮すべき安全目標の検討の視点

制御系の情報システムに関しては、その誤作動の影響を受けるシステムの安全目標に照らして、情報システム自体の安全目標を設定することが必要である。

トラブルの防止と同時に、情報システムの可用性（利用すべき人が利用できること）の問題も同時に検討することが必要である。そのためには、重要な情報システムの多重化、早期復旧のための事業継続計画の策定などが重要である。

安全目標としては、システムの要求分析、設計、実装、テスト、運用、廃棄などのライフサイクルの各段階の作業において、リスクに及ぼす影響を総合的に検討することが望ましい。

情報システムをとりまく社会環境の変化は激しく、また攻撃者の能力は時間とともに急激に増大する可能性がある。この影響を受ける情報システムでは、リスク評価を事前に行うだけでなく、運用中にも継続的にリスク評価を行うとともに、ソフトウェア更新等の対応も必要に応じて行うことが重要である。

安全に関わるステークホルダーのうち、システム利用者や情報システム部署の他に、情報システムを社会や企業のどの部分にまで適用するかを判断する政策立案者や経営者の役割も考慮する必要がある。

また、制御系の情報システムへの安全目標と情報自体の漏えい、改竄等のリスクに対する対応目標の双方を設定する必要がある。

エ　目標に採用する安全目標のタイプ

アからウまでの工学システムの特徴と現在の規制等の状況を踏まえると、安全目標としては、Ｄタイプの適用が望ましい。

⑥　製品安全

ア　安全目標対象の特徴

一回の事故による被害は個人または少数に限定されるが、その影響は多数に関与する可能性があるものであり、安全レベルの設定が産業や社会生活に大きな影響を与える。この分野の安全は、製造事業者と製品利用者との相互理解とコミュニケーションを前提に成り立っており、提供される情報への信頼が重要である。

イ　安全目標の対象とする重大事故

（ア）一般消費者の生命又は身体に対する危害が発生した事故のうち、危害が重大であるもの。

１）死亡事故

２）重傷病事故（治療に要する期間が 30 日以上の負傷・疾病）

３）後遺障害事故

（イ）消費生活用製品が滅失し、又はき損した事故であって、一般消費者の生命又は身体、環境、財産、情報に対する重大な危害が生ずるおそれのあるもの。

ウ　考慮すべき安全目標の検討の視点

製品の設計・製造という事業者の責任範囲での目標と同時に、想定されない使用方法によりリスクレベルが大きく増加することが考えられるので、使用者教育を含め市民の使用に関する範囲を含む目標を設定すべきである。

事業者が示した使用方法を外れて使用された場合でも、予見可能な誤使用は事業者の責任範囲であるが、社会通念を超えた使用方法は、使用者自身の自己責任の範囲になる。安全に関する要求水準を高めることは、事業者の技術力向上のインセンティブになる。一方では、過度な要望はそのコストを利用者が負担すべき場合も生じてくる。

また、製品によって与える影響の種類と規模が大きく異なり、今の基準値（A)、(B）という考え方で整理できるかも検討する必要があり、特にこれまでの製品では許容されていた安全レベルが、新製品では適用されない等の問題に対する明確な方針を明らかにする必要がある。安全目標の考え方の普及により、使用者がより合理的な許容範囲の判断を下せるようにすることも重要である。

エ　目標に採用する安全目標のタイプ

アからウまでの工学システムの特徴と現在の規制等の状況を踏まえると、安全目標としては、Ｃ１タイプの適用が望ましい。

⑦　労災

ア　安全目標対象の特徴

事故の原因が被害者の行動に起因する場合がある安全領域であり、実施すべきことがわかっているが、その実行が難しい領域でもある。

イ　考慮すべき安全目標の検討の視点

近年は子供の頃から危ない経験をしていない若年層や経験年数の少ない層、60歳を超えた高齢者層の事故が増えており、災害発生率も高い等、従来なら考えられなかった事故も発生している。労働環境も正規社員と非正規社員との関係、元方事業者と関係会社との関係など、社会状況が変化している。一方では海外での事業化も進展しており、グローバルな安全に関する考え方も考慮する必要がある。これらの状況を踏まえた安全目標が求められる。

安全目標の設定において、結果目標としての安全目標の設定だけでなく、達成に至るまでの手段に関しても目標設定を行うことが望ましい。

理想的な目標として死亡災害０を目標としているが、基準値Ｂは「どこまでの災害ならば許容するか」について関係者間の合意が必要になる。実現に必要なコストや可能性を考えると、事故ゼロを求めることは、必ずしも合理的な目標とはいえない。2006年労働安全衛生法が改正され、リスクアセスメント指針が制定された。そこでは“合理的に実現可能な限り、より高い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）レベルにリスクを低減するという考え方が規定されている。ただしリスクが低減される効果に比較して必要な費用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場合等は、著しい不均衡とはいえず、対策を実施すべきである。”とされている。

軽微な事故に関しては事業目標等の関係において合理的な目標を定めることが必要である。重大事故の目標設定は度数率より強度率を採用することが望ましい。

ウ　目標に採用する安全目標のタイプ

アからイまでの工学システムの特徴と現在の規制等の状況を踏まえると、安全目標としては、AおよびBタイプの適用が望ましい。

(3)　プラント系工学システムの安全目標の提案

ここでは、他の工学システムに先立って検討した、プラント系工学システムに関する安全目標について記す。

プラント系の安全目標は、Dタイプの目標設定が望ましいと考えるが、総合指標の具体的内容は、今後に実施するため、本報告では、まず、A基準とB基準の提案を行う。安全目標の値の検討に際しては、現状の安全規制等の結果を参考として、設定した。(AP２,AP３参照)

① プラント系の工学システムのA基準は、以下の事項を満足するものとする。

ア　設計そのものに起因する事故や機器の故障、破断、腐食、操作・作業ミス等の事象を原因とする重大事故の発生確率は、10^{-6}／年以下[7]を満足すること。なお、この評価においては、システム操作のミスも含めヒューマンファクタの考慮も必要である。また、影響の大きさや発生確率の不確かさが大きな場合は、その不確かさを検討した際の情報等を含め、判断に有効な情報を示すことが必要である。

イ　地震等の自然災害に関しては、想定される原因事象に対して致命的な事故を発生させない為の設備や体制をとり、災害が発生した際に対応できる体制を整備すること。

ウ　テロに関しては、監視システム等による対応をおこなうこと。

② プラント系の工学システムのB基準は、以下の事項を満足するものとする。

ア　設計起因や機器故障、テロ、自然災害等のあらゆる原因事象に関して、その時点で事故発生の可能性がシナリオとして明らかな重大事故の発生確率を10^{-6}／年以下を満足すること。

イ　テロ等を起因とするリスクの発生確率が10^{-6}／年より大きくても、A基準ではテロ等起因の事故確率に関しては言及していないので、上記①を満足している場合は、A基準を満足していることに変わりは無い。テロ等のように発生確率の分散が大きな事象の評価は今後の検討課題である。

---

[7] この値は、化学プラントや原子力プラントに関するリスク指標の中で、化学プラントでは致命的な事故に対して要求される数値であり、原子力では新設炉に要求されている炉心損傷頻度の値の中で厳しい数値を採用したものである。AP２，３参照。

(4)　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。さらに、発生確率がゼロでない以上、事故は起こり得るので、いったん起こった後の対策も考慮しておく必要がある。

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、ネガティブ双方の可能性）を勘案して決定することが望ましい。

ア　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加え構造等の健全性を担保することや付属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。

イ　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（ここでいう回復不可能とは、30年で回復不可能：一世代では回復不可能な一定期間）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。

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、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、算定したリスクの分析条件を提示し、リスク基準との比較における判断に必要な情報を付加することが求められる。

⑤現状リスク算定に関する要求事項は、AP７を参照されたい（2014年報告に記載）

５　おわりに

本報告では、2014年報告の考え方を、工学システムの特徴を踏まえて適用を試みた。

プラント系の工学システムに関しては適用する安全目標の具体的提案を行っているが、他のカテゴリーに関しては、対象となる工学システムの特徴を整理するに留まっている。

今後、他の工学システムに関しても具体的な安全目標の提案を行った上で、その結果を踏まえて工学システムの社会安全目標全体の見直しを行い、提案したい。

多くの方がこの工学システムの社会安全目標に関して関心を持ち、本安全目標の考え方をそれぞれの分野において適用を検討していただければ幸いである。

〈参考文献〉

１．　「報告」工学システムに対する社会の安全目標　平成26年９月　日本学術会議.

２．　ISO/IEC　Guide51　：2014　Safety aspects ― Guidelines for their inclusion in standards.

＜参考資料１＞

１．これまでの報告

平成 26 年（2014 年） 9 月 17 日

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　安全目標の検討小委員会

「工学システムに対する社会の安全目標」

www.scj.go.jp/ja/info/kohyo/pdf/kohyo-22-h140917-２.pdf

２．参考とした文献

小委員会における議論において、以下の文献を参考にした。

① 向殿 政男：「安全の理念と安全目標」、『学術の動向』、第21巻、第３号，PP.８－13（2016）.

② 野口 和彦：「工学システムに対する社会安全目標」、『学術の動向』、第21巻、第３号，PP.14－19（2016）.

③ 永井 正夫 、小野 古志郎：「道路交通における安全目標の現状」、『学術の動向』、第21巻、第３号，PP.20－26（2016）.

④ 田村 兼吉：「海事分野における安全目標の国際的取り決め」、『学術の動向』、第21巻、第３号，PP.27－31（2016）.

⑤ 中村 昌允：「化学プラントの安全目標」、『学術の動向』、第21巻、第３号，PP.32－38（2016）.

⑥ 成合 英樹：「原子力発電プラントの安全目標」、『学術の動向』、第21巻、第３号，PP.39－43（2016）.

⑦ 柴山 悦哉：「情報システムの安全目標」、『学術の動向』、第21巻、第３号，PP.56－60（2016）.

⑧ 山田陽滋：″生活支援ロボット分野の安全研究″、自動化推進、Vol.45、 No.４、p.12　2016.

３．今期の活動報告

（1）工学システムに関する安全・安心・リスク検討分科会　審議経過

平成 27 年

第１回	２月 16 日	・役員の選出（委員長、副委員長、幹事） ・今期の活動方針 ・小委員会の設置等について（安全目標の検討小委員会の設置）
第２回	５月 11 日	・小委員会活動報告、シンポジウムの状況について、 ・話題提供（化学物質分野における安全目標について）
第３回	９月 18 日	・小委員会活動報告、シンポジウム報告、「学術の動向」特集企画案 ・話題提供（合意形成の条件―社会学の立場から）
第４回	12 月 18 日	・小委員会活動報告、「学術の動向」特集企画案、シンポジウム企画

・話題提供（医療事故防止のための医薬品の包装に対するユーザビリティ工学からのアプローチ）

平 28 年

第５回　４月 21 日　・小委員会活動報告、安全工学シンポジウム 2016 企画案）
・話題提供（車の自動運転に関する安全の考え方）

第６回　９月 21 日　・小委員会活動報告、提言・報告等のまとめ方について
・話題提供（食品安全分野のリスクアナリシスとコミュニケーション）

第７回　12 月 21 日　・小委員会活動報告、小委員会からの提言のまとめ方について

平 29 年

第８回　３月 14 日～27 日　・報告「工学システムに対する社会安全目標の基本と各分野への適用」のメール審議を実施し、承認した。

第９回　４月 27 日　・小委員会活動報告、今期および来期活動について
・話題提供（車の自動運転の様々な課題とその解決の展望について）

８月 17 日　・第 23 期第 250 回幹事会にて本報告が承認される。

（２）安全目標の検討小委員会の活動報告

平成 27 年

第１回　５月 11 日　・役員の選出（委員長、副委員長、幹事）
・今期の活動方針
・安全工学シンポジウム

第２回　６月 24 日　・今期活動方針に関する審議
・安全工学シンポジウムパネルディスカッションの進め方
・リスク研究学会「社会安全目標とリスク・アプローチの役割
・原子力総合シンポジウム

第３回　８月３日　・安全目標の構造、内容、目標設定の要素の関する審議
・学術の動向（2016 年３月号）特集に関する審議

第４回　９月８日　・学術の動向（2016 年３月号）特集の記載内容に関する審議
・今期取りまとめの概略スケジュール
・「フェリー火災事故」、船舶分野の安全に関する話題提供
・各分野の安全基準：原子力、情報

第５回　10 月 23 日　・学術の動向（2016 年３月号）特集の記載内容に関する審議
・各分野の安全基準：化学プラント
・安全分野のカテゴリー分類

第６回　12 月 24 日　・各分野の安全基準:建築
・安全分野のカテゴリー分類の確認

プラント系、インフラ系、情報システム、製品、労働安全

平 28 年

第７回　２月 10 日　・産業現場での労働安全に関する話題提供
歴史的災害、ILO 条約、フィラデルフィア宣言と人権宣言
・安全の理念と安全目標に関する審議、ALARP 原則、基準値Ａ、Ｂ
・工学システムの安全目標取りまとめの全体スケジュール

第８回　４月 21 日　・安全工学シンポジウムの概要
・工学システムのとりまとめスケジュール
基本的な目標の考え方、各カテゴリー分野、
個別の安全目標:原子力、化学プラント

第９回　６月１日　・安全工学シンポジウムの発表内容に関する審議（８件）
・安全目標の基本的なガイドライン

第 10 回　７月 28 日　・安全目標タイプに関する審議：Ａ、Ｂ、Ｃ１、Ｃ２、Ｄ
・基準値Ａ、基準値Ｂと規制値との関係
・ロボット分野の安全目標

第 11 回　９月 16 日　・「報告」骨格に関する審議

第 12 回　10 月 25 日　・「報告」本文内容に関する審議
安全定義、ISO/IEC ガイド 51（2014 年版）の採用
目標「　/年」と「　/生涯」、慢性毒性の考え方
総合目標の考え方
許容判断基準と国、事業者、市民の役割　等

第 13 回　11 月 24 日　・「報告」本文内容に関する審議
Ａ基準とＢ基準、環境的影響の大きいリスク、
各カテゴリー毎の安全目標の審議　　等

第 14 回　12 月 22 日　・「報告」本文内容に関する審議
総合指標の考え方、プラント系記載内容に関する審議　等

平成 29 年

第 15 回　１月 23 日　・「報告」本文内容に関する審議
工学システムの許認可に対する役割分担、
各分野ごとの重大目標の考え方　　等

第 16 回　２月 20 日　・「報告」本文内容に関する審議ならびに了解
・参考資料に対する確認

第 17 回　４月 19 日　・報告に関する分科会査読結果等に対する対応
・安全工学シンポジウムパネルディスカッションへの取り組み

第 18 回　６月６日　・今期の総括と次期活動方針

＜参考資料２＞

AP１.社会リスクに対する目標の基本的考え方

AP２.化学プラント系の安全目標

AP３.原子力施設の安全目標

AP４.サイバー攻撃を対象にした深刻度のレベルの定義

AP５. 電力の停電による影響

AP６. 電気通信事業法施行規則（昭和60年４月１日郵政省令第25号）抜粋

AP７. 工学システムの現状リスクを算定する際の要求事項

AP１　社会リスクに対する目標の基本的考え方　（2014 年報告再掲）

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が社会に与える大きな影響等）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－－－過酷な事故に繋がる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[8]。

事故発生の頻度が高い場合－－－受容の判断に際しては、社会の多様なニーズとの関係で社会との合意を得ることが望ましい。検討に際しては、対象となる工学システムの不稼働がもたらす社会への影響、代替方法採用の可能性ならびに採用することとの得失比較等を考慮することが望ましい。

（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

想定される状況下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。総合指標の判断に関しては、４）に後述する。

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

環境に大きな影響をもたらす事故は、発生確率を安全目標として設定する。

ここでいう大きな環境影響とは、生活や社会活動に大きな影響を及ぼしたり、生態系に大きな影響を与えたりするものをいう。

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

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。（AP３参照）

（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。（この考え方の基本情報は AP３）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[9]。

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

8　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。

9　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。

(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[10]。

(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[11]。(2014 年報告 AP３参照)

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[12]。

---

10 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。

11 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。

12 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。

AP２　化学プラント系の安全目標

１．化学プラントの最大規模事故の想定。

化学プラントは、セベソ事故、ボパール事故などの過去の災害の反省から、セベソ指令、OSHA 基準のように、事故が起きても、被害の及ぶ範囲を、自社の敷地内（コンビナートエリア内を含む）に収めることがプラント設計の基本にある。最近の重大事故といわれる東ソー、三井化学、日本触媒の重大事故は、いずれも、この枠内に収まっている。

したがって、事故防止の考え方は、事故が起きると仮定して、その最大影響範囲が自社内に収まるように設計する。(事故の影響範囲がエリア外に及ぶ場合は、その企業は社会の大きな批判にさらされ、その事業から撤退せざるを得ない事態になる)

２．化学プラントの事故評価指標

2011 年より、石油化学工業協会(石化協)は、下記の事故評価指標に基づいて評価している。

表 AP２－１　石化協の事故評価基準

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	－

この指標は、米国科学プロセス安全センター（CCPS）の評価指標を参考にしている。

（１）人の健康、火災・爆発による経済的影響、漏洩の潜在的影響、環境への影響（環境対応費用）の総合評価で評価

（２）重大事故

それぞれの項目の強度レベル１　および各項目の和が 27 ポイント以上

人の健康：　複数死亡　　オフサイト　１名、オンサイト　複数名

火災・爆発：　経済金額　1000 万ドル以上（10 億円以上）

化学品の漏洩：オンサイトまたはオフサイトでかなりの負傷者や死者の出る化学品の放出

地域／環境への影響：

数日間の全国メディア報道、250 万ドルを超す環境改善、地域への重大な影響

参考文献

２０１６年６月７日　石油化学工業協会「２０１６年度産業保安に関する行動計画」

２．米国国防総省の規格における事故への対応

米国国防総省の規格（MIL-STD-882D）の考え方を、以下に示す。表 AP２－２－１（松本俊次：「プラントのプロセス安全」p84-87、(2004 年）日本プラントメンテナンス協会より引用：以下表 AP２－２－２～４も同様）はハザードの分類、表 AP２－２－２は発生確率の分類、表 AP２－２－３はリスクアセスメント・マトリックス、表 AP２－２－４はリスクインデックスの評価基準である。

リスクマトリックス（AP２－２－３）において、致命的事故では発生確率 10^{-6}／年以下とすることが必要とされている。

表 AP２－２－１　ハザードの分類（MIL-STD-882D）(1)

種別	カテゴリー	環境、安全、健康上の影響基準
致命的 (Catastrophic)	Ⅰ	死亡、不治の全身的障害、100 万ドルを超す損失、または法規違反の回復不可能な重大環境破壊をもたらす
危機的 (Critical)	Ⅱ	不治の一部身体障害、3 名以上の入院となるおそれのある労災疾病、20 万ドル以上～100 万ドルの損害、または法規違反の回復可能な環境破壊をもたらす
限界的 (Marginal)	Ⅲ	1 日以上就労できない傷害・疾病、1 万ドル～20 万ドルの損害、または環境再生を施せば法規に反しない軽度の環境破壊
ネグリジブル (Negligible)	Ⅳ	就労できる傷害または疾病、2000 ドル～1 万ドルの損害、または法規に反しない些少の環境破壊

表 AP２－２－２　発生確率の分類（MIL-STD-882D）(1)

発生確率レベル	ハザードの発生確率	
	特定の個々の品目について	全体について
A:頻発する $X>10^{-1}$	頻繁に起こり得る	絶えず経験する
B:起こり得る $10^{-1}>X>10^{-2}$	耐用期間中に数回起こる	頻繁に起こる
C:随時に $10^{-2}>X>10^{-3}$	耐用期間中にときには起こり得る	数回起こる
D:起こりそうにない $10^{-3}>X>10^{-6}$	耐用期間中にありそうもないが起こり得る	ありそうもないが、合理的に見て起こり得る
E:起こり得ない $10^{-6}>X$	まずあり得ないので起こることはない	ありそうもないが、可能性はある

表 AP２−２−３　リスクアセスメント・マトリックス（MIL-STD-882D）(1)

ハザードの大きさ / 発生確率レベル	Ⅰ 致命的	Ⅱ 危機的	Ⅲ 限界的	Ⅳ ネグリジブル
A:頻発する	1	3	7	13
B:起こり得る	2	5	9	16
C:随時に	4	6	11	18
D:起こりそうにない	8	10	14	19
E:起こり得ない	12	15	17	20

表 AP２−２−４　リスクインデックスの評価基準（MIL-STD-882D）(1)

リスクインデックス（RI）	とるべき処置
1～５	許容できない
６～10	望ましくない（設計上で軽減できない場合、警告文のシグナルワード：「危険（DANGER）」
11～17	許容できる（設計上で軽減できない場合、警告文のシグナルワード：「注意（CAUTION）」
18～20	許容できる：検討不要

参考文献

（１）松本俊次：「プラントのプロセス安全」p84-87、（2004 年）日本プラントメンテナンス協会　より小委員会で作成したもの

AP３　原子力施設の安全目標

(1)安全目標決定の経緯

2014 年報告に記したように、原子力施設は大量の放射性物質を内蔵していることから安全確保には多くの努力が払われてきた。しかし 1978 年の米国 TMI 事故と 1986 年のソ連チェルノブイリ事故という炉心溶融と放射性物質の放散を伴う事故の発生があり、米国において TMI 事故以降検討が進められていた安全目標政策声明が 1986 年に発表された。これは「発電所近くの公衆の受ける原子炉事故による個人の急性死亡リスクは、他の全ての事故による急性死亡リスクの 0.1%を超えないこと、すなわち他の事故等による年間の全死亡者数の 0.1%以内であること」、「原子力発電所サイト境界から 10 マイル以内の公衆の原子力プラント運転によるガン死亡リスクは、他の全ての原因によるガン死亡リスクの合計の 0.1%を超えないこと」、および「大量の放射性物質放出を伴う原子炉事故の発生確率は 10^{-6}/炉年より小さいこと」とした。これはその後国際的な目標になった。

日本では原子力安全委員会が 2000 年から安全目標の検討を開始し、米国等の例を基に 2003 年に中間とりまとめを行った。すなわち「定性的目標案：公衆の健康リスクを有意には増加させないこと」、「定量的目標案：原子炉事故による被ばくにより施設境界の公衆の個人死亡リスクが 10^{-6}/年程度を超えないよう抑制すること」、「事故による放射線被ばくによりある範囲内の公衆のガンによる個人平均死亡リスクが 10^{-6}/年程度を超えないこと」を定めた。さらに安全目標に適合しているかの判断の目安の水準を施設の「性能目標」として炉心損傷発生確率や大量の放射性物質放散事象の発生確率を 2006 年に定めた。指標として、炉心損傷頻度 CDF：10^{-4}/年程度、格納容器機能喪失頻度 CFF：10^{-5}/年程度、とした。ここでは内的事象と外的事象を検討の対象としたがテロ等の人為事象リスクは対象外とした。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」「地震等自然現象に伴う不確かさの考慮」「外的事象の PRA 技術向上」等をあげた。

諸外国でもこれに関わる活動を行ってきており、2014 年報告で記したように、OECD/NEA 加盟国により取りまとめが 2009 年になされた。その表を表 AP３－１と表 AP３－２として再掲する。CDF の指標値は各国で違いはないが、新設炉と既設炉で分けている国がある。また大規模放出事象は日本では CFF として頻度を与えているが、大規模放出頻度と早期大規模放出頻度を与えている国、放出量も指標として与えている国がある。放出量を指標とする国ではセシウム Cs137 の放出量を 100TBq 以下にすることをあげている国が多い。日本では福島第一事故後にスタートした原子力規制委員会が 100TBq を超える事故の発生頻度を 10^{-6}/年を超えないように抑制することを定めた。100TBq は原子力発電所の敷地範囲内で影響がほぼ抑えられる値である。

表 AP３－１　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 AP３－２　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（2）

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

(2) 安全目標と確率論的リスク評価 PRA

安全目標におけるリスクの決定にはレベル１PRA(炉心損傷確率)、レベル２PRA(放射性物質大量放出確率、すなわち格納容器破損有無)、レベル３PRA(環境への放射性物質放出量と住民の健康影響評価)というフルスコープの確率論的リスク評価(PRA)が必要である。米国では 1986 年以降、２つの原子力発電所についてこの PRA を実施した。当初はこれによる評価ができると考えられていたが、しかしこれは大変な作業が必要ということも分かった。NRC も安全目標政策声明の改定に関わる PRA の規制への取入れ等に関するスタッフの提案を 2001 年に否決した。

(3) 米国における軽水炉の代用安全目標：(参考文献参照)

リスクとして、大量放射性物質放出（格納容器機能喪失）に伴う急性死亡リスクと、炉心損傷に伴う放射性物質放出に伴う近隣公衆のガン死亡リスクを考える。

大量の早期放射性物質放出に伴う急性死亡では、米国における全事故による急性死亡リスクが５×10^{-4}/年なので、その 0.1%の安全目標基準は５×10^{-7}/年。サリー原子力発電所の PRA 計算では内的事象による１マイル以内の早期死亡最大条件付確率は３×10^{-2}。したがって、早期放射性物質放出（格納容器機能喪失）頻度が１×10^{-5}/年以下であれば安全目標を満足する。

３×10^{-2}×10^{-5}/年　＝　３×10^{-7}/年　＜　５×10^{-7}/年

サイトから 10 マイル以内の公衆の原子力プラント運転の結果として受けるガン死亡リスクは、米国の全ガン死亡リスクが年 500 人に１人(２×10^{-3}/年)なので、その 0.1%の安全目標基準は２×10^{-6}/年。サリー原子力発電所の PRA 計算では内的事象による 10 マイル以内の潜在的死亡最大条件付確率は４×10^{-3}。したがって原子炉炉心損傷頻度 CDF が 10^{-4}/年かそれ以下であれば安全目標を満足する。

４×10^{-3}×10^{-4}/年　＝　４×10^{-7}/年　＜　２×10^{-6}/年

これらのことから格納容器機能喪失頻度１×10^{-5}/年、炉心損傷頻度 10^{-4}/年が出てきており、日本の安全目標設定の議論でも利用されている。

(4) 2017 年報告で提案する安全目標　プラント系の安全目標は、一度の事故で生命・健康、社会経済、環境に大きな影響をもたらす可能性があるので、安全目標の対象とする重大な事故を明示し、巨大事故に対しては事故発生防止の努力を行う。そのための安全基準として、Ａ基準とＢ基準を提案する。

Ａ基準：プラントの設計起因・機器故障・破損・腐食・作業操作人的ミス等の内的事象による重大事故の発生確率を 10^{-6}/年以下。地震等の自然災害に関しては、致命的な事故を発生させないための設備や体制をとり、テロに対しては近隣住民の避難時間を確保する。

Ｂ基準:プラントの設計起因・機器故障・テロ・自然災害等あらゆる原因事象に関して、事故発生シナリオとして明らかな重大事故の発生確率を 10^{-6}/年以下。

重大事故には、生命・健康ばかりでなく、社会・経済・環境等へのリスクを含める。社会・経済・環境リスクの評価が今後の課題である。

参考文献

(1) NUREG-1860、Feasibility Study for a Risk-Informed and Performance-Based

Regulatory Structure for Future Plant Licensing, Volumes 1 and 2, U.S.NRC (2007年)

（2）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

AP４　サイバー攻撃を対象にした深刻度のレベルの定義

サイバー攻撃を対象にした深刻度のレベルの定義として、米国では、2016年７月にCyber Incident Severity Schema (https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf)を定めたが、この概要は以下の通りである。

・Level ４までで想定している被害は次のもの。
- public health or safety
- national security
- economic security
- foreign relations
- civil liberties
- public confidence

・Level １から ４ までの差は、多分、被害の種類ではなく、規模や確率。
・Level ５になると、想定被害は次のもの。
- wide-scale critical infrastructure services
- national gov't stability
- the lives of U.S. persons

AP５　電力の停電による影響

電力の停電による例としては、情報機器の停止に伴う情報の喪失、病院設備の停止、信号機停止、エレベータ停止等が考えられる。さらには0.07秒の瞬断でも操業停止に追い込まれた例もある。停電の原因としては、天災、人為的原因、機器故障、燃料不足の他に需給のアンバランスに起因する電力特有の問題もある。

資源エネルギー庁のデータによると各国の需要家１軒当たりの年間停電時間（停電が発生してから復旧するまでの時間）は日本22分/年、ドイツ38分/年、米国85分/年、英100分/年であり、１軒当たりの停電回数は日本0.2回/年、ドイツ0.45回/年、米国1.0回/年、英0.9回/年となっている。統計データからは各国とも安定的に電力供給が行われていることが見てとれるが、鉄道への電力供給復旧まで３日を要した例（JR東日本高崎線、2016年３月15日発生）や配電設備の火災で都内35万軒が停電し完全復旧まで約１時間、火災の鎮火まで４時間要した例がある（埼玉県新座市東京電力施設、2016年10月12日午後３時30分頃発生）。社会生活への影響が重大な事例が散見されるので安全目標として考慮すべき事項を詰めていく必要がある。

AP６　電気通信事業法施行規則（昭和60年４月１日郵政省令第25号）抜粋

第五十八条　法第二十八条の総務省令で定める重大な事故は、次のとおりとする。

一　次の表の上欄に掲げる電気通信役務の区分に応じ、それぞれ同表の中欄に掲げる時間以上電気通信設備の故障により電気通信役務の全部又は一部（付加的な機能の提供に係るものを除く。）の提供を停止又は品質を低下させた事故（他の電気通信事業者の電気通信設備の故障によるものを含む。）であつて、当該電気通信役務の提供の停止又は品質の低下を受けた利用者の数（総務大臣が当該利用者の数の把握が困難であると認めるものにあっては、総務大臣が別に告示する基準に該当するもの）がそれぞれ同表の下欄に掲げる数以上のもの

電気通信役務の区分	時間	利用者の数
緊急通報を取り扱う音声伝送役務	一時間	三万
緊急通報を取り扱わない音声伝送役務	二時間	三万
	一時間	十万
利用者から電気通信役務の提供の対価としての料金の支払を受けないインターネット関連サービス（音声伝送役務を除く。）	二十四時間	十万
	十二時間	百万
一の項から三の項までに掲げる電気通信役務以外の電気通信役務	二時間	三万
	一時間	百万

二　電気通信事業者が設置した衛星、海底ケーブルその他これに準ずる重要な電気通信設備の故障により、当該電気通信設備を利用する全ての通信の疎通が二時間以上不能となる事故

AP７　工学システムの現状リスクを算定する際の要求事項　(2014 年報告再掲)

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。