提言

工学システムの社会安全目標の新体系

令和２年（２０２０年）８月２８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

この提言は、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・リスク検討分科会安全目標の検討小委員会での審議を踏まえ、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・リスク検討分科会におい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	須田　義大	（連携会員）	東京大学生産技術研究所教授
副委員長	野口　和彦	（連携会員）	横浜国立大学 IAS リスク共生社会創造センター客員教授
幹　事	水野　　毅	（連携会員）	埼玉大学大学院理工学研究科教授
幹　事	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 国際連携センター 副センター長
	遠藤　　薫	（第一部会員）	学習院大学法学部教授
	望月　眞弓	（第二部会員）	慶應義塾大学名誉教授・薬学部特任教授
	大倉　典子	（第三部会員）	芝浦工業大学名誉教授・SIT 総研特任教授
	柴山　悦哉	（第三部会員）	東京大学情報基盤センター教授
	桑野　園子	（連携会員）	大阪大学名誉教授
	柘植　綾夫	（連携会員）	公益社団法人日本工学会顧問・元会長
	辻　佳子	（連携会員）	東京大学教授
	永井　正夫	（連携会員）	一般財団法人日本自動車研究所顧問、東京農工大学名誉教授
	中川　聡子	（連携会員）	東京都市大学工学部電気電子工学科教授
	萩原　一郎	（連携会員）	明治大学研究知財戦略機構・特任教授
	平尾　雅彦	（連携会員）	東京大学大学院工学系研究科教授
	松尾亜紀子	（連携会員）	慶應義塾大学理工学部教授
	松岡　猛	（連携会員）	宇都宮大学地域創生推進機構 宇大アカデミー非常勤講師
	宮崎久美子	（連携会員）	東京工業大学名誉教授、立命館アジア太平洋大学国際経営学部 特別招聘教授
	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	（連携会員）	横浜国立大学 IAS リスク共生社会創造センター客員教授
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
	淺間　　一	（第三部会員））	東京大学大学院工学系研究科教授
	柴山　悦哉	（第三部会員）	東京大学情報基盤センター教授
	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顧問、東京農工大学名誉教授
	松岡　猛	（連携会員）	宇都宮大学地域創生推進機構 宇大アカデミー非常勤講師
	向殿　政男	（連携会員）	明治大学名誉教授
	田村　兼吉		運輸安全委員会委員
	山田　常圭		総務省消防庁消防大学校消防研究センター前所長

本提言の作成にあたり、以下の職員が事務を担当した。

事務	松室　寛治	参事官（審議第二担当）
	五十嵐　久留美	参事官（審議第二担当）付参事官補佐
	横田　真理江	参事官（審議第二担当）付審議専門職付

要　　旨

１．作成の背景

現代の先進国は人類史上で最も物質的に豊かな時代である。この物質的豊かさのために、多様な工学システムが果たした役割はきわめて大きい。しかし、この多様な工学システムは、環境や人の健康、生命への影響の他にも、経済への影響や社会混乱への影響等の様に様々な安全問題をも生み出している。我々は、物質的豊かさを追求するための活動と安全に関する活動を行ってきたが、現代社会は、物質的豊かさと同時に安全も含めた様々な価値の豊かさを求める社会であり、それぞれの活動はお互いに影響を及ぼしあっている。安全に関する活動は、物質的豊かさだけでなく、様々な豊かさを構築する重要で不可欠な要素であると同時に、必要なレベルを超えた安全の追求活動や安全への過度な要望が、便益を得る機会を失わせることや社会活力を奪う場合もあることも認識しておく必要がある。

２．現状及び問題点

安全に関しては、これまでその在り方に対して多くの検討がなされ、安全確保のための対策も実施されてきた。しかし、工学システムの複雑化、機能の高度化や活用範囲の拡大につれて、安全の対象も労働安全から社会安全へと拡大し、その影響も多様かつ大きなものになり、一度の事故で社会に大きな影響を与える可能性が高くなってきた。

これまで社会の安全は、主に行政の管轄分野に対する細やかな安全規制と事業者の真摯な努力により積み上げられてきたが、規制の改善は、大きな事故や災害を受けて行われることも多かった。このために、必ずしも規制を満足していれば事故を防ぐことができるわけではないことが、広く認識されるようになり、これまでの事故に学び規制により安全を確保するという仕組みも改善が必要であることが明らかになった。

３．提　言

本提言は、工学システムにおける安全目標を設定し社会の安全を確保するという新たな仕組みを提示し、その実現を目指すものである。

安全な社会を構築するためには、規制による安全に加えて、社会として共有できる具体的な目標を設定し、安全対応の進捗状況を確認して目標の達成を検証していく必要がある。

本提言では、まず安全の概念を整理し、社会としての目標の立て方とその評価の方法の検討を行った。

次に、これまでの工学システムの安全に関する活動を調査し、それぞれの考え方を整理した。そして、社会安全の対象とする工学システムを特徴に応じて５つに分類し、各々の特徴に対応した安全目標の在り方を検討した。

また、本提言では、多様な安全の課題に対して、安全目標の指標としてリスク指標を用いることを推奨している。このリスク指標の設定に関しては、社会の状況によってリスクの受容判断が異なることも勘案して、達成できないことが許容されない基準Ａと更なる改善を必要としない基準値Ｂを設定し、基準Ａと基準Ｂの間は、リスクを総合的に判断し

て対応することを求めている。

判断基準として二つの基準を定めるということは、社会の安全にはその社会においては、どのような便益があっても許容できないレベル（基準A）があるということと、社会状況によっては判断の可否が異なる状況がある（基準Aと基準Bの間で判断）ことを示している。

そして、その安全目標の構築と活用の仕組みとして、行政、学協会、事業者、市民の視点を取り入れた仕組みを検討し、安全目標を検討する組織により安全目標を設定するステップを整理した。

さらに、構築した安全目標の仕組みの活用に関する検討を行い、以下の６つの活用方法として整理を行った。

１）行政が社会自体の目標として我が国が目指す安全レベルを示す
２）行政が事業者に対して満足するべき安全に関する要件として示す
３）特定の工学システムの安全を検証するための指標として示す
４）技術開発目標としての指標として示す
５）長期的な社会の挑戦目標としての指標として示す
６）国際的な目標としての位置づけとして示す

本分科会では、工学システムの社会安全の在り方に関する検討結果を踏まえ、以下の５つの提言を行うものである。国は、以下の提言を実現する活動を推進するべきである。

提言１　工学システムの開発や運用に関わる行政や事業者は、活力があり豊かな社会を構築するために、社会安全の明確な目標を定めてその達成を目指す仕組みを構築するべきである。

提言２　学協会、事業者は、その業界・専門分野を超えて、経験した事故・災害の再発防止に加えて、経験していない事象に対してもリスク概念を用いて安全の向上を目指すべきである。

提言３　工学システムの開発や運用に関わる行政、事業者は、最新の情報・検討に基づいた安全目標を市民に提示し、市民はその安全目標に対いて積極的に責任のある意見を発信していくというそれぞれの役割を果たすことにより、市民も納得できる社会安全の仕組みを構築するべきである。

提言４　事業者や学協会は、工学システムの特徴に応じて安全目標を構築し、工学システムの開発や運用に関わる行政はその運用を行う仕組みを構築するべきである。

提言５　工学システムの開発や運用に関わる行政、学協会、事業者は、安全目標を社会の状況変化に応じて改定し、市民は社会状況に応じて安全目標が変化することを理解するべきである。

本提言では、工学システムの安全に関する行政・学協会・事業者に対し、安全目標を設定し、安全な社会構築に努められることを求める。

また、本提言では、工学システムのカテゴリー毎に、安全目標設定の参考となる事例を示しているので、具体的な安全目標を構築する際は、参考にされたい。

目　　次

1　はじめに

(1)　工学システムの社会安全目標の必要性

現代の先進国は人類史上で最も物質的に豊かな時代である。この物質的豊かさのために、多様な工学システムが果たした役割は極めて大きく、工学システムは、精神的豊かさや時間の豊かさ等の様々な豊かさにも影響を及ぼしている。しかし、この多様な工学システムは、様々な安全問題をも生み出しており、その結果、物質的豊かさだけでなく、様々な価値の豊かさにも影響をもたらしている。そのため、多様な豊かさを享受することを前提とすると一定のリスクは受け入れる必要がある。また、リスクの受け入れの検討に際しては、絶対安全はないことを認識する必要がある。

安全は、社会の重要課題であり、これまでその在り方に対して多くの検討がなされ、安全確保のための対策も実施されてきた。その対応には、事故の原因を排除する本質安全[1]の活動や事故の影響をその事業所内に押さえ込み敷地外への影響を及ぼさないことを徹底する活動が追求されてきた。

しかし、工学システムの複雑化、機能の高度化や活用範囲の拡大につれて、安全の対象も労働安全から社会安全へと拡大し、さらにその影響も多様かつ大きなものになり、一度の事故で社会に深刻な影響を与える可能性も大きくなってきた。一方、一回の事故の影響が甚大ではなくても、その発生頻度が高いことが、社会に大きな影響をもたらす場合もある。

また、各工学システムは、厳格な規制等のもとで開発・使用されてきたが、技術の開発や社会の変化に従って、様々な問題が発生してきた。

一つ目は、工学システムの高度化と社会活動の工学システムへの依存度が増すにつれて、その事故の影響が直接的な被害に加えて、社会活動全般への間接的な影響も大きくなってきたことである。電力、ガス、通信等や自動車、鉄道、船舶、航空機等の輸送システムは、社会に必要不可欠なインフラシステムとなり、社会に大きな影響をもたらす重大事故を防ぐことは当然として、その活動信頼性を維持することが、社会安全のために重要な視点となってきており、安全に止めればよいとはいえない状況もでてきている。そのため、社会安全の活動の対象とする事故・トラブルの内容も広がり、目指すべき安全レベルも高くなってきている。

二つ目は、事故の多様性や影響の大きさの変化である。例えば、プラントが巨大で複雑になるにつれて、取り扱うエネルギー量が大きくなり、取り扱う物質や造り出される物質が多様化するにつれて、敷地の境界を越えて影響の種類も多様になると同時にその規模も大きくなり、事故への対応がより重要になってきた。そのために、発生確率が極めて小さくとも影響が大きな事象への対策の検討が必要となってきた。

三つ目は、環境変化や社会要求の高度化に伴い目指す安全レベルが高度化してきたことである。土木や建築における構造物の安全は、従来から高いレベルでの安全要求がな

[1] 以下の安全対応「(1) 危険源の除去、(2) 危害のひどさの低減、(3) 危害の発生確率の低減」の三つの方策の内、最初の二つの危険源の除去と危害のひどさの低減に対する方策が本質安全である。

されてきたが、自然災害の激甚化により、安全を考える前提が変化してきており、構造物に対する要求も高くなっている。また、生活への危険な影響を小さくするとともに利便性を確保することへの要求レベルも高くなり、社会安全にとって多くの課題が明らかになってきている。

四つ目は、技術開発速度の速い工学システムにおける安全対応の難しさである。例えば、自動車は自動化が進むにつれてこれまでの自動車の安全の仕組みでは検討できない事項も多くなってきた。ロボットもその活用が産業施設から一般社会や家庭に広がるにつれて、検討するべき安全項目も増大してきている。また、情報システムは、新製品の開発やバージョンアップの速度が従来の工学システムとは比較にならない速さで進んでおり、安全を構築する仕組み自体の改革が必須となってきている。

工学システムの社会安全に対する活動は、社会の重要課題であり持続可能な開発目標（Sustainable Development Goals ：以下 SDGs と記す）の 17 の目標においても直接的には「３．すべての人に健康と福祉を」、「９．産業と技術革新の基盤をつくろう」、「11．住み続けられるまちづくりを」、「12 つくる責任、つかう責任」に貢献するものであり、間接的には、全ての目標設定に貢献するものである。

これまで我が国の安全は行政の細やかな安全規制と事業者の真摯な努力により積み上げられてきた。しかし、規制の改善は、大きな事故や災害の事後対策として行われることも多く、必ずしも規制を満足していれば事故を防ぐことができるわけではないことが、広く認識されるようになった。

このため、これまでの事故に学び技術開発等や規制の改定により安全を確保するという仕組みも改善が必要となり、新たな社会の安全を構築する仕組みとして、安全目標を設定し社会の安全を確保するという仕組みを提言するものである。

(2)　これまでの検討経緯

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では、工学システムの社会安全目標について検討を行い、2 件の報告を発出してきた。［１］、［２］

小委員会の検討においては、まず安全目標の前提となる安全の概念を定義し、工学システムのこれまでの安全活動の調査を行った。（参考資料３参照）

次に、工学システムのこれまでの安全に関する規制や対応の考え方等を整理して、工学システムの特徴と安全目標の考え方を整理した。（参考資料 10 参照）

そして、安全目標の要件や規制との関係の整理も行い、安全目標にリスク概念を活用する際の考え方をまとめた。

これらの検討結果を基に、安全目標の基本構造と個別の工学システムへの具体的な適用について検討を行った結果、工学システムをその特徴に応じてカテゴリー分類を行い、そのカテゴリー毎に、具体的な安全目標を検討することとした。

工学システムのカテゴリーは、その特徴やこれまでの安全活動の経緯によって、５つに分類し、それぞれの工学システムの特徴と安全目標の設定方法を整理した。また安全

目標についても検討を行い、５つのタイプに分類した。（参考資料９参照）

これら２回の報告の内容に関して提言を活用する上で参考となる内容を抜粋して、本提言の参考資料としてとりまとめた。

⑶ 本提言の骨格

本提言は、これまでの２回の報告を受け、工学システムの社会安全目標について、社会で活用できる提言のあり方について議論を行い、以下の内容とすることとした。

① 安全の議論を実施するために、安全の定義、安全目標の概念、要件と規制との関係を明確にする

② 安全目標の標準的な構築のステップを提示する
工学システムをその特徴により５つのカテゴリーに分類して、望ましい安全目標の形式を示す。尚、具体的な安全目標の数値等は、各分野で設定できるように、参考資料に具体例を示す。

③ 安全目標の要件を示す

④ 安全目標の活用方法について示す

⑤ 安全目標の提言をその実行主体を明確にして示す

2　社会安全における安全目標活用の基本構造

(1)　安全へのアプローチと本提言の位置付け

安全に関する議論が錯綜する原因の一つに、議論の対象となっている安全の内容に関して共通の認識ができていないことがある。近年では、安全に加えて安心の問題も関心を集めているが、本提言は安全に関する提言に限定している。尚、安心に関しては日本学術会議では別途議論を進めている。

「安全」という用語は、特に対象を定めずに社会の安全を一般概念として議論する際に使用されたり、特定の事象に関する生命等を失う可能性の状況分類として使用されたりしてきた。「安全」という用語は、その使用される場合によってその時々に理解され使用されてきたと言える。しかし、安全目標を用いて安全を議論する際には、その検討対象である「安全」とさらには「目標」の考え方を明確にして、その安全目標の設定プロセスとその有効な活用に関して検討する必要がある。（参考資料３参照）

安全な社会の実現に向けて、それぞれの分野においてその特徴に応じた安全対策が進められてきた。安全設計の視点で検討が進められてきたものも、労働安全の視点で改善が進められたものもあった。工学システムは、技術の改革によって高度化していくが、新たな技術が想定する範囲内では、事故を起こさないようにするということが安全の基本である。しかし、その想定範囲が、検討する者によって異なっている状況では、社会からの賛同は得られない。したがって、安全に関して検討する際に、原因系や結果系の想定する範囲がどこまでかを社会的に共有しておく必要がある。

また、社会状況は、技術、社会価値等によって変化するために、求める安全のレベルも社会状況により変化するものであり、その時々の社会が求める要求を満足する必要がある。

安全の対象としては、事故を起こさないという視点に加えて、被害拡大防止・事故対応（救護、被害軽減、避難等）、さらには、早期復旧の在り方もその対象となる。従来の設計や運用の視点でも、そのチェック体制、設計ミスのチェック体制、メンテナンスも問われなくてはならない。

そして、工学システムの研究や開発の専門家も自らその在り方を考えることは必須であり、使用者である市民の受容性を担保することが必要である。その一方、使用者も、安全に使用する責任を持つ必要がある。

本提言は、前二期の活動を受け、安全目標の社会的目的とその位置づけを示し、安全目標設定の手順とその要点をまとめたものである。

本提言では、工学システムの安全に関係する行政・事業者と学協会に対し、安全目標を設定し安全な社会構築に努めることを、提言している。また、行政・事業者・学協会による安全目標を作る仕組みや活用方法を提言している。

さらに、本提言では、工学システムのカテゴリー毎に、安全目標設定の参考となる事例を示している。具体的な安全目標を構築する際は、工学システムの特徴を踏まえて実施されたい。（参考資料 10）

⑵　安全目標の対象とする工学システムの分類

安全目標を設定する際には、対象とする工学システムの安全目標を構成する安全の内容を明確にする必要がある。

本提言では、対象とする工学システムをその特徴やこれまでの安全への対応の在り方によって、表１のようにカテゴリー分類をおこなった。

インフラ系では、その性質やこれまでの規制との関係によって、土木構造物や建築物のように規制によってその安全性が詳細に定められているカテゴリー、電力・ガス・水道のように生活基盤となっているカテゴリーと、人や貨物を輸送する交通システムのカテゴリーの三種類にさらに分類した。

この分類は、今後の技術等の変化により、工学システムの性能や安全に関する主要事項に変化をもたらす場合があり、工学システムのカテゴリーは、その時々の工学システムの特徴を表わすものでなくてはならない。なお、自動車のように、自動化が進展中のシステムにおいては、その状況によって複数のカテゴリーに分類される場合もある。

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	オーナーカー、サービスカー（バス、タクシー、トラック等）
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	組み込みシステム・制御システム、社会インフラ（通信、クラウド、電子政府、金融等）

本安全目標では、①から⑤までの工学システムの安全とともに、生活製品を中心とした製品安全と①から⑤までの工学システムに共通して存在する労働安全とをその対象とする。（参考資料 11 参照）

工学システムのカテゴリーの特徴を、以下の事項に整理した。（参考資料 10 参照）

ア）　工学システムの特徴

対象カテゴリーの事故の特徴や社会との関係を整理した事項

イ）　安全目標の対象とする重大事故

安全目標は、その工学システムの重大事故に対して設定するものであるが、例えばプラント系に関しては、以下のように定めている。

・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
・多数者に健康の被害を与える事故
・広範囲に環境被害を与える事故
・原材料・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視点

カテゴリー毎に、安全目標を検討する際に必要な事項をまとめている。

例えばプラント系に関しては、事故が社会に及ぼす大きさを考慮することや設備設計や経年劣化対応等に留意することや、リスク評価を行う際の分析の前提条件を明示することに必要性等について記述している。

エ）　目標に採用する安全目標のタイプ

対象カテゴリーにふさわしい安全目標タイプ（参考資料 9 参照）を推奨している。

尚、モノのインターネット（Internet of Things：以下 IoT と記す）技術の進展によって、多くの工学システムまたは製品安全等において、情報システムの機能を併せ持つ場合が多くなってきている。IoT 技術の組み込み状況に応じて、安全目標に情報システムの特徴を踏まえた安全の考え方（参考資料 10⑤参照）を組み込むことが望ましい。

(3)　安全目標の基本要件

本提言は、社会における行政、事業者等の安全活動を、常にその問題点を検討し使用可能なリソースの中でその向上を目指す継続的な活動として位置づける。

安全目標を用いた安全向上の活動は、社会生活や産業活動を維持する中で推進される必要がある。

安全目標は、安全活動の拠り所となるものであり、その目標を達成したからといって安全活動が完了するわけではない。安全目標自体が、技術や社会的要求や価値観によって変化するものであり、安全目標の枠組みをどのようにするかということ自体も、その時点で目指す安全を検討する際に考える必要がある。

安全目標を活用して安全を検討するための要点は、以下の通りである。

①　安全目標の基本的考え方

安全目標は、絶対安全な状況は存在しないことを前提として設定されるものである。

安全目標の基本的考え方を以下に示す。

1）　安全目標は、その達成期間内に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。安全目標は、その適用分野における技術の進展の早さや安全に関する要求に応じて定める必要がある。

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、経験したことのない重大な事故も、その時々の知識により論理的に検討できる範囲でその可能性を分析し、現状の技術やリソースの範囲で事前に対応を行うことによって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・不稼働がもたらす生活・社会・環境への多様なリスクを勘案して決定する

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

べきである。

4） 製造者、運用者と使用者の責任をバランスよく考える必要がある。

5） 安全目標には、達成できないことが許容されない安全レベルが存在する。また、その状態を達成すればさらなる改善を求めないレベルも存在する。この二つのレベルの間でどこまでのレベルを要求するかは、社会状況において変化するものである。

② 安全目標を検討する際の要点

安全目標を検討する際の要点を以下に記す。

ア 各分野で安全検討の対象を共有する

安全を検討する際の対象は、工学システムの特徴によって事故事象として検討される場合やリスクとして検討される場合がある。安全の検討においては、その対象を事故やリスクまたはその影響を含めた組み合わせとして共有する必要がある。

例えば、巨大プラントの重大事故は、発生の可能性は小さくても、一旦事故が発生すると、その影響は人身の健康への被害のみならず、環境や社会生活への大きな影響を与える可能性がある。一方、家庭で使用するパーソナルロボットの事故は、使用者に危害を与える影響があるが、その影響は家庭内に限定される場合が多い。このように、検討すべき影響の内容も対象とする工学システムによって異なる。また、その検討の手法も、巨大プラントの場合は、対象とする重大事故の発生確率は小さくなる場合が多いために、検討対象をリスクとして捉え、その発生確率を算定すると共に、その多様な影響を分析する必要がある。一方、長年の使用実績があり、その対象において考慮すべき事象が台風等の様に豊富な経験があるような構造物においては、その対象物において考慮する負荷を設定し、その健全性を検証すれば良い場合もある。

対象候補の特徴を参考資料 10 に示す。

イ 安全目標の位置づけの明確化

安全目標には、その設定した状況を達成しているかを検討することによって社会の安全状況を検証していくためのものと、技術開発等の目安や実現するべき社会の状況を設定して活動をしていくためのものがある。

既に社会で多く運転をしている工学システムの中で、その重大事故が社会に大きな影響を与える可能性がある巨大プラントや鉄道等の社会インフラシステムは、現状の状況が安全であることを社会に示す必要がある。また、全自動運転の自動車のように先進的な技術開発を行っている工学システムや、現状の安全に関して社会のコンセンサスがとれているがさらなる向上を目指す工学システムでは、開発の技術目標として安全目標を設定し、開発を推進することもある。

また、どちらの場合も安全目標として、事故等の発生、被害の拡大防止、早期復

旧等の活動のどの範囲を目標とするかを明確にして、設定することが求められる。

ウ　安全目標の判断（評価）基準の設定

安全検討対象の事象に対して安全目標が達成されているか否かを判断する受容基準やリスク基準を、安全目標の判断（評価）基準（以下、安全基準と記す）として設定する。（参考資料４参照）

安全基準の例を参考資料８に示す。

エ　安全基準と比較するための評価を行う

評価に際しては、設定した安全基準に応じて、その実施主体を定めることになるが、安全に関する視点が多様化するにつれて、これまでの行政や事業者に加えて、学協会、特定非営利活動法人（Nonprofit Organization ：以下 NPO と記す）等の第三者機関を活用することもある。

これまでの安全規制は、人身や環境等への影響のように、工学システムがもたらす直接被害を対象とするものが多かった。しかし、社会が高度化すると、工学システムの影響が、生活、利便性や経済にもたらす影響も問題になる場合もでてくるので、多様なステークホルダの視点を加味する必要がある。また、情報システムのように、その利用が生活・産業に幅広く使用されるような工学システムは、供給者のみならず、その利用者の運用の仕方にもその安全性が影響を受ける場合もあり、社会としての安全に関する議論が必要になる場合も出てくる。

このために、評価に関与する団体・個人もその対象に応じた仕組みが必要になる。

③　安全目標を設定する仕組み

安全目標を設定する際は、まず安全目標を設定する枠組みを明確にする必要がある。

安全目標を設定する組織は、行政の場合も、業界や学協会、NPO等の第三者機関、市民の集まりである場合もある。

これらの組織が設定する安全目標は、行政、事業者から市民までの多様なステークホルダが活用するものであるため、設定される安全目標が多様な視点により構成されていることを示す必要がある。そのためには、設定した安全目標について多方面から意見を求めるだけでなく、その設定のプロセスの透明性を担保する必要がある。

目標を設定する組織が具体的な安全目標を設定する際は、「安全」の検討の対象を共有するとともに、設定する「目標」の内容及び活用の仕方を明確にする必要がある。

④　安全基準の基本要件

安全基準を設定する際はその基準を適用する前提・条件を明確にすることが必要である。安全基準は、仕様規定として定められる場合もあればリスク基準として設定される場合もある。また、安全基準は、事故等の結果としての被害が同じであっても、原因によって異なる場合がある。内部の機器故障によるものは、発生確率等で基準を

定めやすいが、テロ等のように、発見や被害拡大の防護機能の十分性を基準とする場合もある。

(4) 安全検討の対象

安全検討の対象を明らかにするためには、以下の事項に留意する必要がある。

① 安全検討の対象を検討するための仕組みの構築

安全検討の対象は、対象とする工学システムやステークホルダの視点によっても異なる。したがって、安全検討の対象は、行政や対象工学システムの専門家の視点に加えてその他のステークホルダの視点も合わせ検討する仕組みの構築が必要である。

② 安全検討の対象

検討する事故やリスクの整理に関しては、影響の内容・規模、またはその事象を発生させる原因等の安全に関する要素を検討する必要がある。この際に、定量評価が難しい、対策が明らかでない等の理由で、検討の対象から除外してはならない。

安全目標として確定できない事項が存在していることを明示することも、その安全目標を活用していくためには必要である。

(5) 安全目標と規制との関係

工学システムの安全に関して規制によって遵守するべき重要な事項が定められているものも多いが、安全目標を活用した安全確保を図る場合は、安全目標と規制の関係を明確にする必要がある。

対象システムの稼働・不稼働の決定は、安全目標を満足した上で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。その際、安全基準として規制を満足することは必須の要件であるが、規制を守ることで十分か否かは、その規制内容と工学システムの特徴によっても異なる。

工学システムが原因となる社会に対し好ましくない影響をもたらすシナリオの中には、その因果関係が複雑になり得るものがある。そのような状況に関しては、事業者、行政、第三者機関が、社会安全の視点でそのシナリオの発見に努め、その対応の責任範囲を議論する仕組みを構築する必要がある。

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・複雑化は、規制と安全との関係に変化をもたらしている。

社会や企業が新たな工学システムを高度化し、社会の物質的な豊かさを初めとした多様な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。

ただし、工学システムの技術の特徴や運営の実績が十分に認識され、規制下において

十分に安全であることが認知されているシステムに関しては、規制自体が安全目標と認定される場合もある。

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。

しかし、IoT、AI 等情報分野に特徴的にみられるように要素技術や設計・構築技術のみならず利用方法や利用環境等の変化が大きな工学システムに関しては、規制において技術の進展による新たな安全問題を完全に先取りすることは困難であり、規制に加えてそのシステムや製品の特徴を反映した安全基準を定める必要がある。

(6) 評価を行う際の要件

安全に関する評価は、安全目標で採用している安全基準と評価結果の比較によって行うものである。したがって、安全評価に採用する安全に関する分析は、安全基準と比較できる内容でなくてはならない。

また、リスクを用いて安全を評価する場合は、リスク分析を実施する際に、適切な判断が行えるように、分析に要求される条件を満足する必要がある。（参考資料７参照）さらに、リスク評価により低減対応を検討する際は、その費用対効果や低減効果等も検討する必要がある。（参考資料６参照）

また、評価に関しては、分析した前提を明確にして分析結果とともに、付加情報として提示する必要がある。

一般的に安全に重大な影響をもたらす可能性については、工学システムを社会に投入する前に評価する必要がある。一方、技術や環境の変化が非常に速いシステムに関しては、第三者による規制に類するような基準設定が難しい場合が出てくる。その場合は、対象となる工学システムを提供する事業者は、社会に投入する前に、その時点の知見で分析できる範囲で安全性に関して評価をすることが必要であり、第三者機関等により、対象システムの社会投入後速やかに必要な評価を行うことが求められる。

３　工学システムの安全目標の構築の仕組みと活用方法

本章では、安全目標設定の仕組みと安全な社会を構築するための安全目標の活用方法についてまとめた。

本章では、まず全ての工学システムに適用できる安全目標構築の基本ステップを示す。個別の工学システムの安全目標を構築する際の事例は、参考資料 10 を参照されたい。

また、安全目標の活用の仕方に関しても本章に記述している。工学システムの特徴に応じて、その活用方法も考えられたい。

(1)　安全目標構築のステップ

①　概要

安全目標を構築するステップを以下に示す。

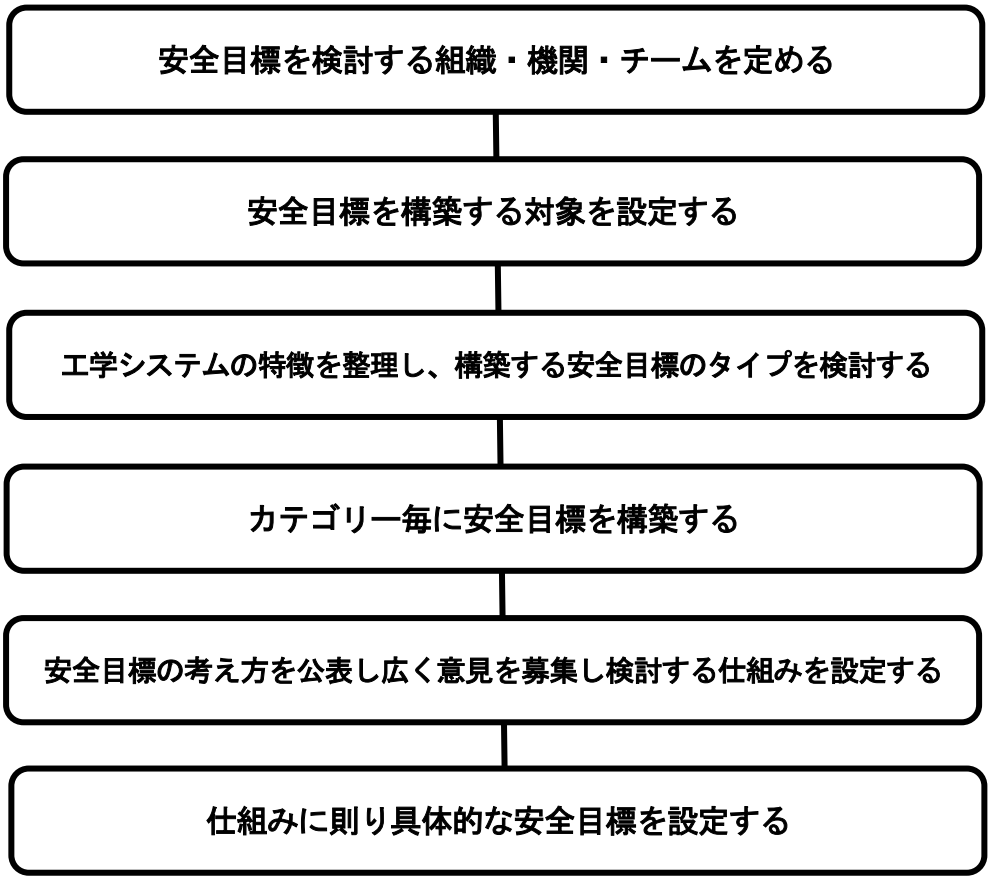

図１　安全目標構築のステップ

②　個別の安全目標構築のステップの内容

ア　安全目標を検討する組織・機関・チームを定める

安全目標案を検討する組織・機関・チームに対する要件は、以下の通りである。

（ア）　対象とする工学システムに関する専門知識があること

プラントシステムのように、構造力学、熱力学、反応化学、制御、ヒューマンファクタ、自然災害対応等、複数の専門知識が必要な工学システムでは、その全ての専門性を持つ者からなるチームによる検討が必要になる。

（イ）　社会的要求を分析する機能があること

プラントシステムでは、社会的要求には、事故自体を防ぐという要求の他に、事故が発生した際に避難等によって市民の安全が担保されることや、そのプラントが社会に提供している製品やサービスが速やかに継続されることも含まれる。

（ウ）　安全に関して体系的に分析する技術があること

工学システムに関する専門知識の他に、リスクを体系的に分析する技術

や、自然災害やテロといった工学的要因以外によって発生するリスクに関する分析技術も必要となる。

（エ） ステークホルダからの信頼が得られる組織・機関・チームであること
工学技術専門家が考える安全の事項に加えて、社会が要求する安全に関する諸要素について検討を行うことが必要である

（オ） ステークホルダ間のコミュニケーション機能を運営できること
コミュニケーションでは、専門家が実施した情報の開示以外にも、専門家が社会の要求を知ったり、新しい知識やデータを知ったりするためのコミュニケーションも必要となる

イ　安全目標を構築する対象を設定する

大きな分類では、同じ工学システムと認定されても、異なる安全目標を設定した方が望ましいと考えられるシステムは、区別する。（表１参照）

工学システムは、その技術の進歩によって、その内容が大きく変化する場合がある。それにより、安全目標のタイプが変化する場合もある。（参考資料９参照）

ウ　工学システムの特徴を整理し、構築する安全目標のタイプを検討する

（参考資料９参照）

エ　タイプ毎に安全目標で使用する安全基準を検討する

（ア）安全基準の設定に際しては、その根拠、妥当性等を明確にする必要がある。

（イ）安全基準を理解するために必要な事項の説明を行う。

オ　安全目標の考え方を公表し広く意見を募集し検討する仕組みを構築する

（ア）安全目標の策定のプロセスを明示し、透明性を確保する。

（イ）安全目標の案を公表し、ステークホルダの意見を聴き、修正を行う。

（ウ）安全目標と規制との関係を整理しておく。

カ　仕組みに則り具体的な安全目標を構築する

２章に記述した安全目標の要件を守りつつ、対象工学システムの特徴を踏まえ安全目標を設定する。

⑵　安全目標設定の考え方

①　安全目標の基本要件

ア　目標は、達成可能なものであり社会的公平性を持ち、社会から受け入れられるものでなくてはならない。

（ア） 目標は、特定の活動だけを利して他に悪影響を及ぼすものであってはなら

ず、社会の多様な視点を考慮し、特定の視点に偏らないことが求められる。

（イ） 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。

（ウ） 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。

（ア）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。

（イ） 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、技術、環境や価値観等の変化も考慮した将来の状況も踏まえたものである必要がある[3]。

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。

（ア）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。

（イ）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。

（ア） 工学システムとしての設計から廃棄までの間を通じての安全目標が必要である。

（イ）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。

（ウ）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。

（ア）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　安全目標の判断基準として要求事項を採用する場合

工学システムの活用実績が十分にあり、対象システムの安全に対する社会の認識も定着している場合には、要求事項を明示した安全目標が成立しうる。

ただし、そのシステムが活用されている社会状況や環境または適用技術が変化する場合は、重大な事故が発生する前に、その要求事項を修正することが求められる。

③　安全目標としてリスク指標を採用する場合の考え方

ア　安全目標としてのリスク指標の設定

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ている。

（ア）人命等の重要リスクを対象とした目標の考え方

安全目標としては、達成できないことが許容されない基準Aと更なる改善を必

3　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場合もある。

要としない基準Ｂを設定する。基準Ａと基準Ｂの間は、リスクを総合的に判断して対応する（図２参照）[4]

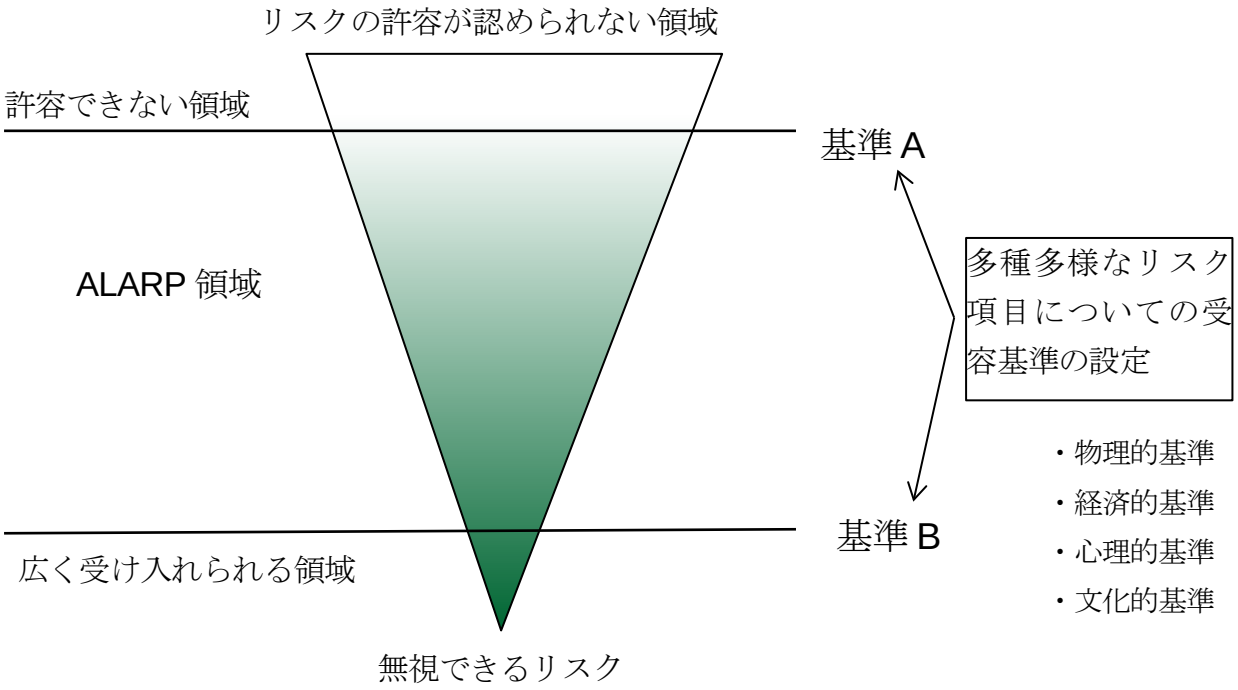

図２　安全目標の基本概念

（出典）「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 2017【2】から修正して作成

判断基準として二つの基準を定めるということは、安全にはその社会においてどのような便益があってもそのリスクが許容できないというレベル（基準Ａ）があるということと、社会状況によってはリスクの許容の可否が異なる状況がある（基準Ａと基準Ｂの間で判断）ことを示している。

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ることと、代替システムがある場合は代替することによる得失を総合的に評価し、トータルリスクミニマムが図れるのであれば、社会は使用停止の判断をすると考えられる。

（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が必要である。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、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必要である。この社会リスクの目標におい

[4] この考え方は、ALARP の考え方を採用している。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

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分けてその考え方を取りまとめる。

イ　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分析に対する要求や評価の役割分担等に関して取りまとめる。

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目標を最新の情報の下で検証した結果を公開することが必要である。

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必要がある。（参考資料７　参照）

ウ　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、基準Ａ、基準Ｂの二つの基準を設定する必要がある。

各工学システムに具体的な目標として設定する場合は、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。

安全目標にリスク指標を用いるということは、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が発生することを容認しているわけではない。工学システムはあくまでも、死亡事故や大きな環境事故を起こさないという前提で稼働する必要があるということは当然のことである。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かつ欠かすことができない理念である。

しかし、工学システムはその性質上、理論的に事故の発生確率を０にはできない。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。

エ　基準Ａ、基準Ｂの設定について

基本的には、基準Ａは事業者と社会との合意事項であり、基準Ｂは安全目標を構

築するステップの中で定めることが望ましい。少なくとも基準A、基準B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。

基準Aと基準Bとの間の判断は、ALARP 領域として、便益、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、さらには代替施策におけるリスクとの兼ね合いで目標値を定めるべきである。

④　工学システムの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べき主体が行うものとする。

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、事業者はそのガイドラインを守るべき最低基準として、自己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こととする。

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、理解するべき科学技術のリスクに関して関心を持ち、その受容の在り方に関して常に考えておく。

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公開し説明をおこなうことにより、その判断が市民から信頼される状況を作る必要がある。

⑶　安全目標の活用

安全目標は、工学システムの社会との関係によって、その活用の方法が異なる。また、その活用法の仕方によっても安全目標の内容が異なってくる場合がある。

安全目標の在り方は、その活用方法に応じて定める必要がある。

安全目標の活用方法を以下に整理する。

①　行政が社会自体の目標として我が国が目指す安全レベルを示す

国内外に対して、国として目指す安全の考え方を示す指標を安全目標として示す。社会の構成要員である行政、事業者、市民等が安全を検討し活動するために、その目標レベルを示す手段して活用する。

市民が議論する際の、共通指標として活用する。

②　行政が事業者に対して満足すべき安全に関する要件として示す

行政が事業者に対する安全のガイドラインとして活用する。

安全に対して必要な事項を仕様規定として具体的に法規で示す方法から、規格等を用いた規制への転換手段としての活用でもある。

③　特定の工学システムの安全を検証するための指標として示す

社会安全に重要な影響をもたらす可能性のある特定の工学システムに対して安全か否かを社会の視点から定めた指標として設定する。規制が示す指標と同一の場合もあるし、規制を守るべき最低基準と考えて規制よりも高いレベルを要求する場合もある。

④　技術開発目標としての指標として示す

指標は、技術開発の目標として設定する安全レベルである。関係する技術者が工学システムの目標としての安全レベルを共有し、工学システム全体の開発計画やそれぞれの分野で開発するべき技術を検討するため設定する。

⑤　長期的な社会の挑戦目標としての指標として示す

社会の長期目標としての安全レベルを示すために活用する。今後の制度検討や、開発投資の目安にも活用できる。

⑥　国際的な目標としての位置づけとして示す

国際基準との調和を考慮した国際的な安全の目標設定として活用する。

４　提言

２章、３章に示した検討結果をもとに、以下の５つの提言として取り纏めた。

本提言は、工学システムの安全目標を設定し社会の安全を確保するという社会の安全を構築するための新たな仕組みを提示して、その実現を目指すものである。国は、以下の提言を実現する活動を推進するべきである。

提言１　工学システムの開発や運用に関わる行政や事業者は、活力があり豊かな社会を構築するために、社会安全の明確な目標を定めてその達成を目指す仕組みを構築するべきである。

社会安全は社会運営の基盤であり、その在り方は社会の多くの活動に影響を与えるものである。これまで我が国の安全は、高度な規制を遵守する方式に従って守られることを基本としてきた。そのため、安全に関して事業者が目指す安全目標を設定して活動を行ったり、市民の要求を安全の制度に組み込んだりする活動等が難しい側面があった。

しかし、技術変化の激しい工学システムにおいて、常に規制により安全を担保するという仕組みには限界がある。これからは、新たな安全目標を用いた安全推進の仕組みの構築が必要であり、例えば、化学プラント等では、米国科学プロセス安全センターや日本の石油化学工業協会は、それぞれ事故評価基準を発表しているが、業界の評価指標にとどまっており、社会の産業安全指標として社会全体の視点で広く認識されているわけでは無い。このような社会に大きな影響をもたらす事故の可能性に対する安全の考え方は広く社会で共有し、その推進を図るべきである。

そのため、工学システムの開発や運用に関わる行政（内閣府、総務省、文部科学省、経済産業省、国土交通省、厚生労働省、農林水産省、環境省、防衛省等）や事業者は、社会安全の構築のために、目指す目標を明確に定め、その達成のために必要な仕組みの構築、技術開発、教育・訓練等を実施するべきである。

（P.３　2.（1）、　P.７　2.（5）参照）

提言２　学協会、事業者は、その業界・専門分野を超えて、経験した事故・災害の再発防止に加えて、経験していない事象に対してもリスク概念を用いて安全の向上を目指すべきである。

社会は技術開発や環境の変化により急激に変化しており、対応するべき事故・災害の種類・規模も変化している。このような変化に対して社会安全を確保するには、安全対応活動も経験した事故の再発防止活動にとどまらず、経験していない事故・災害に対してもリスクの概念を用いて、対応を考慮するべきである。

これまで実施されてきた経験した事故の再発防止を徹底するという手法では、新たな巨大事故の発生を無くす事は難しく、社会はいずれ大きな被害を経験する事になる。しかし、リスクという可能性を考慮した安全の構築には、リスクという概念の正しい理解、リスクの概念を用いた安全活動の有効性や高度なリスクマネジメント技術を社会で共有する事が必要になる。

学協会、事業者は、その業界・専門分野を超えて、社会の安全に影響を及ぼすリスクに関する分析・活用研究を行い、リスクの定量評価の精度の追求だけでなく、広くその活用の仕組みを構築するべきである。

リスク概念を用いた安全目標の仕組みでは、達成できないことが許容されない基準値と更なる改善を必要としない基準値を設定して、安全目標を設定する方法を推奨する。

(P.3　2.（1)、　P.11　3.（2）③　参照)

提言３　工学システムの開発や運用に関わる行政、事業者は、最新の情報・検討に基づいた安全目標を市民に提示し、市民はその安全目標に対いて積極的に責任のある意見を発信していくというそれぞれの役割を果たすことにより、市民も納得できる社会安全の仕組みを構築するべきである。

社会安全をどのように考え対応をするのかということは、社会を構築する多くの視点によって議論し判断をしていかなくてはならない。

例えば、原子力システムに関しては、原子力規制委員会によって厳しい安全基準が定められているが、その安全のあり方に関して必ずしも社会全体から賛同を得られているとは言え無い状況である。安全目標を具体的に検討し、設計する役割は、主に工学システムの開発や運用に関わる**行政や事業者が担うことになるが、市民は安全目標やその検討時に示される情報に関心を持ち、市民としての意見を示すことが重要である。**

このことは、これまでのように、行政が定めた規制を市民が追認するという状況では無く、社会から広く支持される安全構築の仕組みに対する市民参加が不可欠だということである。

この仕組みを適切に運用するためには、工学システムの開発や運用に関わる行政・事業者・市民のそれぞれが他の視点も理解し、その意見を反映し、社会として実行できる合理的な対応を検討する制度を三者がそれぞれの役割を果たし構築するべきである。

(P.4　3.（3)、　P.9　3（1）　参照)

提言４　事業者や学協会は、工学システムの特徴に応じて安全目標を構築し、工学システムの開発や運用に関わる行政はその運用を行う仕組みを構築するべきである。

社会安全を達成するための安全目標は、対象とする工学システムが多様であり、その社会における実績や技術の変化の状況等も大きく異なるので、安全目標は、その工学システムの特徴と社会からの要求を勘案して、本提言に記した基本的考え方を踏まえつつ、実効性のある安全目標の設定とその実現を目指す活動を行うべきである。

巨大プラントのように、規制に加えてリスク分析の結果を併せて安全の仕組みを構築しようとしている分野もあれば、長い実績があるシステムにおいては規制遵守を安全の必要十分条件としているものもある。また、変化の激しい情報システムの分野や新たな実装分野を抱えるロボット分野においては、その規制要件から議論が始まっているものもある。

事業者や学協会は、その対象システムの特徴を反映した評価法を開発し、工学システムの開発や運用に関わる行政は、その組み込みを工学システムの進化に遅れることなく行い、適切な評価を行う仕組みを構築する必要がある。

(P.4　3. (2)、(3)　参照)

提言５　工学システムの開発や運用に関わる行政、学協会、事業者は、安全目標を社会の状況変化に応じて改定し、市民は社会状況に応じて安全目標が変化することを理解するべきである。

社会安全の在り方は、社会の要求に応えるものでなくてはならず、社会状況や技術開発の状況に応じて変化するものである。安全目標を活用して、社会安全の構築を目指すには、安全目標が常に社会からの要求を満足しているようにするべきである。

また、安全の構築には、技術、資金、人財等のリソースのあり方は大きな影響を及ぼすために、社会で大事な安全という価値も、社会の他の価値との共存の中で考えていくものであり、高度化された社会では安全を工学システムの技術要件だけで考えて行くわけにはいかなくなってきている。安全な社会を構築する仕組みは、社会理念として高い状況を目指すという目標を掲げれば良いわけでは無く、その目標を実現できるための実効性が重要である。

工学システムの開発や運用に関わる行政、学協会、事業者は、社会状況や技術状況の変化に応じて、社会安全目標を改定し、改定の必要性と有効性を市民に示すことが望ましい。

市民は、安全目標の改定の必要性やその有効性についての理解を深め、必要に応じて、自分たちの意見を安全目標に反映するための意見を表明することが望ましい。

工学システムの開発や運用に関わる行政、学協会、事業者、市民は、社会状況に応じて、社会安全の在り方を定めていく仕組みに対して、それぞれの役割において参加することを求める。

(P.9　3 (1)、P10　3 (2)　参照)

５　おわりに

工学システムは社会の様々な機能を高度化し、現代社会を豊かで利便性の高いものに改善してきた。社会における工学システムの重要性が高まるにつれて、その安全の確保の重要性も増してきている。しかし、工学システムの技術開発は絶え間なく実施されることにより大規模化や複雑化が進み、その事故が社会に与える影響も多様化したことにより、安全を担保する仕組みも、改革が必要となってきた。

本提言は、社会の要求に応えられる工学システムの安全の確保のために、安全目標を活用した新たな仕組みを提言するものである。

本提言では、社会の安全の実現を目指す仕組みを、供給者である事業者やその規制を行う行政の役割だけではなく、学協会や市民の役割も含めてその仕組みの構築を提案する。

豊かで活力があり安全な社会の構築のために、本提言に基づき安全の仕組みが構築されることを期待する。

＜参考文献＞

［１］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、報告「工学システムに対する社会の安全目標」、2014年９月17日.

［２］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、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」、2017年９月20日.

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

［４］日本学術会議、安全に関する緊急特別委員会報告、「安全学の構築に向けて」、2000年２月28日

［５］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報告、「安全で安心なヒューマンライフへの道」、2003年３月17日

［６］ 日本学術会議、安全・安心な世界と社会の構築特別委員会報告、「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

［７］ 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報告、「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

［８］ 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報告、「事故調査体制の在り方に関する提言」、2005年６月23日

［９］ 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

[10] 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」、2008年６月26日

[11]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

[12]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)

[13]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

[14] 特集「社会における安全目標その多様な展開」、学術の動向 2016 年 3 月号 pp.8-60

[15] 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.

[16]松岡猛、「工学システムに対する社会の安全目標と原子力発電」、日本原子力学会誌 時論　Vol.57, No.7 pp.434-435(2015)

＜参考資料１＞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 29 年

第１回	12 月 25 日	・役員の選出（委員長、副委員長、幹事） ・今期の活動方針 ・ 小委員会の提案（継続・新規） 安全目標の検討小委員会の設置と委員が承認された。

平成 30 年

第２回	４月 19 日	・小委員会活動報告、安全工学シンポジウムの状況について、 ・話題提供（安全安心のフレームについて）
第３回	９月 12 日	・小委員会活動報告、安全工学シンポジウム報告、
第４回	メール審議	・「報告（案）老朽・遺棄化学兵器廃棄の安全と環境の保全に向けて」について承認する件

令和元年

第５回	５月 27 日	・小委員会活動報告、安全工学シンポジウム 2019 企画案） ・話題提供（新興技術に関するイノベーションシステム）
第６回	メール審議	・「公開シンポジウム「安心感等検討シンポジウム」の開催」について承認する件
第７回	10 月 18 日	・安全目標に関する議論 安全目標の検討小委員会がまとめている提言案の説明と表出に向けてのスケジュールの説明があった。内容について審議し、今後、今次会議の意見に基づき小委員会で修正案を作成し、スケジュールに従い審議を進めていくこととなった。

令和２年

第８回	メール審議	安全目標の検討小委員会の提言に関する審議を行い、提言案を承認した
第９回	１月 21 日	安全目標の検討小委員会の提言に関して、英語版の作成や、国際展開について意見交換がなされた。

（2）安全目標の検討小委員会の活動報告

平成 30 年

第１回　　４月 27 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 14 日　・今期活動方針に関する審議
・個別分野の安全目標
航空分野の安全目標
化学プラントの安全目標　（含む米国CCPS安全基準）
・ 安全工学シンポジウム

第３回　　７月 25 日　・個別分野の安全目標
プラント安全目標（化学プラントの安全目標 ）
・工学システムの社会安全目標の検討課題
・安全工学シンポジウム2018開催結果報告

第４回　　８月 30 日　・「工学システムの社会安全目標」活動について
(1) 輸送システムの事故の発生確率の考え方
(2) 工学システムにおける労働災害の考え方
(3) 情報システムにおける安全目標の考え方
(4) 自動運転における安全目標
(5) 本質安全の考え方
(6) 全体目標と個別分野目標

第５回　　10 月 11 日　・個別分野の状況
(1) 情報分野
(2) 事故が起きた後の対応について
(3) メンテナンス

平成 31 年

第６回　　１月８日　・個別分野の安全目標
「機械安全における安全目標とSafety 2.0」
・「今期提言のまとめ方と課題」

第７回　　３月 22 日　・個別分野の状況
ロボット分野における安全の考え方
・今期「提言」のとりまとめ方
・安全工学シンポジウム

令和元年

第８回　　６月 17 日　・今期のとりまとめ方針に関する審議
安全目標の新体系
プラントの安全目標
情報の安全の考え方

製品安全における安全目標
自動運転における安全目標
・安全工学シンポジウムについて

第９回　８月７日　・今期「提言」とりまとめについて
「安全目標の新体系」提言骨子に関する審議
・安全工学シンポジウム2019の開催結果と総括
・「自動車の自動運転の推進と社会的課題に ついて
―移動の本能と新しい社会のデザイン―」

第 10 回　10 月４日　・提言「工学システムの社会安全目標の新体系」の取りまとめ
に関する審議

第 11 回　12 月３日　・「提言」本文内容に関する審議

令和２年

第 12 回　１月 10 日　・「提言」本文内容に関する審議と了解
・分科会査読結果等に対する対応
・安全工学シンポジウム

（３）日本学術会議幹事会

令和２年

第 293 回　６月 25 日　・提言「工学システムの社会安全目標の新体系」について
承認

＜参考資料２＞用語の定義

本提言における説明が不確定・あいまいなものとならないように、使用する用語を定義する。

・ハザード：潜在的危険要因（ISO/IECGuide51.の定義）。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：危害の発生確率及びその危害の度合いの組み合わせ（ISO/IECGuide51.の定義）。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、経済損失リスク等がある。
・許容可能なリスク（tolerable risk）：現在の社会の価値観に基づいて、与えられた状況下で受け入れられるリスクのレベル（JIS Z 8051 の定義）。
・安全：参考資料３で説明。
・危険：安全が損なわれそうな状態。
・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広義の便益に加えて考える場合もある。
・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。一つまたは複数の判断基準を含んだものであり、ステークホルダ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持つもの。本提言では、プロセス、製品を含める。
・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。

＜参考資料３＞安全の概念　（参考文献[１]より抜粋）

工学システムの安全目標を検討する際には、その達成目的である「安全」自体を社会として共有できるように、その定義や考え方を明らかにすることが重要である。

ア　安全の定義

本提言では、安全を「許容不可能なリスクがないこと」（ISO/IEC Guide51 の定義）と定義する。

ここでいうリスクは、安全の定義を採用した ISO/IEC Guide51 のリスクの定義である「危害の発生確率及び危害の程度の組み合わせ」のことをいう。

このことにより、安全か否かの判断は、科学的分析結果と社会状況等も踏まえ行うことになる。この判断を社会的に合意するためには、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。

これまでの工学システムに関する安全に関しては、工学システムが存在することによって生じる影響を対象としてきたが、存在している工学システムを停止、排除することによっても社会には影響が生じる。社会安全を考慮する際には、この二つの影響を考慮する必要がある。

これらの影響は種類も大きさもその発生確率も様々であり、それぞれの工学システムにおいて対応するべき事象は異なる。本提言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。

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確率を０に抑えることは難しいので、事故・災害発生後の対応も含めて安全の目標を設定することが必要な場合もある。

安全目標は、それぞれの目標設定の対象とする指標（例：生命、健康、経済指標等）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によって作成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[5]

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[6]

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。

これまでの安全対応では、未然防止、再発防止等の事故等の発生防止に注力してきた。事故が頻繁に起きる分野では被害発生回数と被害の軽減がまず重要であり、社会の成熟度とともに事故リスクを軽減する予防安全施策の重要度が増す。

さらに、事故発生防止の重要性は当然であるが、事故等が発生した際の被害の拡大防止や早期の復旧等も社会安全には、重要である。

個々の工学システムの安全目標の対象は、その適用範囲や影響の大きさによって異なってくる。

＜参考資料４＞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

（**参考文献**[2]より抜粋）

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

5　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。

6　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。

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よいのであるが、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、別のリスクが大きくなるという関係もある。そのために最終的に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るべきことには、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。この検討するべき影響には、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。その重みを事業者で判断する場合は、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。

＜参考資料５＞リスクマネジメントの構造

ここでは、安全を検討する際に活用するリスクマネジメントの用語について、その関係を示す。

リスクマネジメントの用語の使い方は、いくつかの方式があるが、本提言では、ISO31000：2018（JISQ31000：2019）の考え方に基づき使用している。

1）リスクマネジメント（risk management）
リスクマネジメントのプロセスには、リスクアセスメントとリスク対応が含まれる。
・リスクアセスメント
・リスク対応

2）リスクアセスメント
リスクアセスメントとは，リスク特定，リスク分析及びリスク評価を網羅するプロセス全体を指す
・リスク特定
リスク特定とは、リスクマネジメントの対象とするリスクを特定すること
・リスク分析
リスク分析には、リスクの不確かさ，リスク源，結果，起こりやすさ，事象，シナリオ，管理策及び管理策の有効性の詳細な検討が含まれる。リスクの定量的分析をリスク算定と呼ぶこともある。
・リスク評価
リスク評価は，リスク対応を決定するために、リスク分析の結果と確立されたリスク基準との比較を行うなどの評価を行うものである。

3）リスク対応
リスクに対処するための選択肢を選定し，実施することである。

＜参考資料６＞リスクの許容判定及び低減対策を実施する際に注意する観点

（**参考文献**[2]より抜粋）

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のリスクにも注意する必要がある。
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。リスク分析は、その結果が判断に使用できるレベルまで、検討を行うべきである。また、その算定の条件が明らかであれば、その前提の範囲で判断に活用できる場合もあるので、リスク分析は、その結果に加えて算定モデルに対する付加情報を添付することが必要である。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、【参考資料７】を参照されたい。
オ　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。

＜参考資料７＞リスク分析の要件　　（参考文献[1]より抜粋）

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、希望的観測に基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他、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。

＜参考資料８＞死亡リスクを目標の判断基準として設定する場合の考え方

（参考文献[1]より抜粋）

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、社会的に受け入れられた安全目標を満足する範囲内で、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よい。

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よい。

3） 影響が一過性でなく回復ができない影響が発生する事象に関しては、障害の影響を障害を受ける者の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よう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。

＜参考資料９＞安全目標のタイプ　　（参考文献[2]より抜粋）

①A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。

②B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。

③C１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、死亡被害のよう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。

④C２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）のように、リスクを安全の指標とする考え方である。

⑤Dタイプ

リスク指標を安全目標に採用するものであり、基準としては、その基準を満足しなければ社会から受け入れられないレベルの基準と、その基準を満足するとそれ以上の安全レベルの向上を要求しない二つの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。この二つの基準自体に総合的な指標を採用する場合もある。

＜参考資料 10＞工学システムの各カテゴリーの特徴　　（参考文献[2]より抜粋）

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） 原材料・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　考慮する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、参考資料 11 の労働安全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の共有認識とする必要がある。評価の対象とする事故は、規制が求めている基準を、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、重大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ことによって重大事故の芽を摘む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、化学プラント等では設備の経年劣化や老朽化による事故が増加しており、設備維持管理対策が重要になってきている。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、事業所トップが実施責任を担い、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（MOC: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、MOC は、製造現場がやってよいことに対する事業所としてのガイドラインを定めるとともに、専門技術者や経験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（根本原因・トラブル拡大、防御階層の考え方）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など、リスクコミュニケーションも検討対象となる。

（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、有害な化学物質等の漏えい防止など環境に及ぼす影響の抑制を目標とする。

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 考慮する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及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したりする事故とする。

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、電力のように他のインフラの復旧状況に大きく関わったり、上水や下水のよう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、衝突等の各キャリア（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・安全意識の向上の在り方も含めて、どのように位置づけるかも検討事項となる。特に、外部要因による踏切事故の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。そのためには、鉄道の内部での検討にとどまらず、幅広い視点での検討が望ましい。また、事故の原因として、運行時の体制に起因するもの以外にも、近年では、設計及びその承認プロセス、車両・施設等の保守・点検体制による事故や重大インシデントが発生しており、これらの検討も重要である。自然災害からの安全性の確保の視点から、計画運休が実施されるようになったが、安定輸送の視点から利用者への周知の在り方や社会受容性も検討することが望ましい。

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ALARPの概念を用いた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、海洋開発分野で原子力分野と並んで早期からリスク評価の概念が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）　主に人の輸送より物流や漁業等に職業として利用されていること。

2）　内航船と外航船に分かれており、内航船はその国独自の規則、外航船は世界統一規則で造られていること。

3）　プレジャーボートから巨大タンカーまで大きさは2桁も異なり、それに伴って操縦性、航行支援機器等のレベルも大きく異なること。

4）大型船は一隻ごとの注文生産であり、同一の船舶は存在しないこと。

5）　危険物の輸送等、積み荷そのものにリスクが存在する場合があること。

6）　日本周辺海域であっても、操船者に外国人も多く、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。

7）　原則として世界中どの海域でも自由に航行でき、気象・海象等、自然環境の影響を大きく受けること。

このため、安全目標設定には、こうした船舶固有の特徴を理解するとともに、国際規則との整合性や環境適合性等を総合的に評価することが必要である。

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。現在、Safety risk severity table（ICAO Doc9859）では、Ｃ２タイプの目標を採用しており、Ｃ２またはDタイプの適用が望ましい。

③　自動車

ア　工学システムの特徴

自動車は、オーナーカーとサービスカーに大別されるが、両者に共通するのは事故の原因が、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ことである。特に自動車の運転は人と車システムが一体となって初めて機能するものであり、ヒューマンエラーが死亡事故要因の95%を占めている分野である。このような現状に対して近年、自動運転・運転支援システムの採用のように革新的イノベーションが起きつつある分野であり、安全に対する考えが根本から変わりつつある。

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こと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　考慮する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。特に地方での移動支援サービス（MaaS：Mobility as a Service）の開発には、地方自治体との合意形成が重要となる。

さらに、自動運転・運転支援システム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)、運転者（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・経済的損失などの社会的インパクトも考慮する必要がある。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　考慮する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、生活支援ロボット等の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、参考資料 11 の労働安全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、使用者の他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

組み込みシステムあるいは制御システム（以下、「制御系の情報システム」という）は、多くの工学システムに組み込まれており、その制御を担っている。さらに、通信やクラウドサービスはもちろん、金融や電子政府などの社会インフラの制御も多くの部分を情報システム（以下、「社会インフラ系の情報システム」）が司っている。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と比べて低く、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

制御系の情報システムの事故や同システムに対する攻撃が原因となり、制御対象となる他の工学システムに安全目標上の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、社会インフラ系の情報システムにおいては、サービス停止の範囲と時間がある程度大きいと「重大」となる。たとえば、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　考慮する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、特に社会インフラ系の情報システムにおいては、可用性（利用する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。

安全目標の検討では、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における作業のリスクを、総合的に反映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、情報システムの安全目標とともに情報そのものの漏えい、改竄、消失等のリスクに対する対応目標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。

＜参考資料11＞工学システムの安全に関係のある製品安全と労働安全の特徴

（**参考文献**[2]より抜粋）

本提言では、工学システムを５つのカテゴリーに分類し、それぞれの特徴と安全目標の考え方を整理したが、安全を考える上で重要な製品安全と労働安全も検討を行い、以下のように整理した。

⑥　製品安全（工学システムによって製造された製品の安全）

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、その影響は多数に及ぶ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）一般消費者の生命また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、又は毀損した事故であって、一般消費者の生命または身体、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　考慮する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、事業者が想定してい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るべきである。

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が、一方では、過度な要望はそのコストを最終的には利用者が負担する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、既に設定している基準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、特にこれまでの既存製品では許容されていた安全レベルが、新製品では許容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。

「これは安全」と安全確認できる使用と、「これは危険だ」と確認できる非常識や無謀な使用との間に、使用方法いかんで安全か危険かわからない状態がある。事故が起きた製品がこのようなケースに当てはまるとき、これを単純に「消費者の誤使用」と決め付けてしまえば、安全か危険かわからない状態に対する事業者の認識が曖昧となり、対策をとらず放置する結果を招きかねない。

一方、ある製品において、ある程度のリスクが存在し、その時代の技術では是正することができないような場合、消費者はそのリスクを受け入れて、それを承知の上で安全に使いこなすといった、「かしこくリスクと付き合っていく」ことも必要である。

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　労働安全（工学システムの製造・運転において生じる安全問題）

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、実施する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　考慮する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、元方事業者と関係請負人との関係など、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、対策を実施するべきである。”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。

リスクが大きい場合は、直ちに安全対策を講じるべきであるが、設備点検やメンテナンス作業、建設工事等においては、これ以上の工学的対策が困難な場合がある。その場合は「特別管理作業」等として指定し、作業に携わる労働者の資格を認定するなど継続的な管理対策が必要である。また、予算的な理由等により、直ちに改善措置を講じるのが困難な場合は、暫定措置を直ちに実施した上で、継続的な管理的対策を実施しつつ、本格的なリスク低減措置を講じる必要がある。

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、Ａ及びＢタイプの適用が望ましい。