安全設計の考え方について

～安全学の視点から～

向　殿　政　男*

Masao Mukaidono

1．安全学への動機づけ

まず，なぜ，安全学なのかということから説明する．安全確保を技術的な側面から眺めると，安全技術は，これまで個別分野に特有の性質，特に物理的，化学的，数理的，社会的性質に基づいて開発され，発展してきた．安全技術は，基本的には現場に立脚した個別技術という性格を有している．従って，安全技術や安全工学は，縦割的，個別専門的な性格を有していて，統一的な視点を与えるのを難しくしていたのは事実である．しかし，安全技術には明らかに共通部分が存在する．ある分野で開発された安全技術には，その考え方の深層に，他の分野にも応用できる考え方が隠されているはずである．他の分野でも利用可能とするためには，その安全技術の本質を他の分野の人にも理解可能，応用可能なように一般化，原則化する必要がある．そうでなければ，各分野でそれぞれ血を流し，苦心して開発してきた安全技術や知恵が他の分野に応用できないので，もったいない話しであり，起らなくても済む悲劇を繰り返すことになる．このような発想から，各分野の安全に横ぐしを指し，各分野の安全技術に共通する考え方，手法等を領域横断的に体系的にまとめ，安全技術者の共通の常識にすべきであると考えたのが安全学を提案するに至った最初の理由である．

一方，安全の確保は，技術的な側面だけで実現できるわけではない．人間も関与するし，法律や組織等も関係する．すなわち，ものづくりに限っても，安全を守るためには多くの役割と立場がある．大きく分類すると，

(1)技術で守る役割(設備安全：安全設計技術)

(2)制度・組織で守る役割(安全管理：制度・ルール)

(3)人間で守る役割(運用安全：教育，訓練，伝承，ヒューマンファクター)

の三つがあると考えられる(**図1**)．技術の学問的背景には自然科学があり，制度・組織の学問的背景には社会科学があり，人間の学問的背景には人文科学がある．更に，これらの上位概念として，安全文化や安全思想等の理念的側面があるはずである．安全は，本来，自然科学，人文科学，社会科学を融合した全体性をもって対応しなけらばならない分野であって，その上に哲学がなければならない．安全に関する学問は，全体性をもって包括的に総合的に考察されなければならない．従って，安全工学でもなく，安全科学でもなく，安全学と名称を付けた理由はここにある．

もう一方，ものづくりにおける安全の時間的な流れを眺めてみよう．どの分野でも，安全確保に関する製品のライフサイクルから考えると共通の流れがある．一般的に，製品のライフサイクルと

1．技術で守る‥設備安全：安全設計技術、

2．制度・組織で守る‥安全管理：制度・ルール

3．人間で守る‥運用安全：教育、訓練、伝承、ヒューマンファクター

・この背景に安全文化がある

図1　安全確保に係る三つの立場

* 明治大学名誉教授

して，要求仕様⇒設計(ハードウエア，ソフトウエア)⇒製造⇒販売・設置⇒運用⇒保全(保守・点検・修理・交換)⇒使用終了または廃棄(リサイクル)となる．現実的には，運用中に事故やトラブルがあることを考慮すると，安全確保の段階を，ライフサイクルに従って，もう少し大きく分類すると，例えば，

(1)未然防止段階（予防安全：設計安全，寿命予測)

(2)運用段階(運用安全：保守・点検・修理)

(3)トラブル段階(事故安全：拡大防止，再稼働)

(4)再発防止段階(事後安全：事故調査，原因究明)

と4段階に分けられ，それぞれの段階で安全対策を施さなければならない(**図2**)．ここでの大事なことは，設計段階で，各段階での安全性を考慮して設計することである．安全は，上流で対応すればするほど，効率的，効果的，コスト減につながる．従って，安全確保のためには，安全設計の段階が最も基本的であり，重要である．事故が起きる前に手を打っておく未然防止が基本であり，再発防止の前にやるべきことである．この安全の流れと各段階は，ほとんどの分野で，かつほとんどの製品で同じであると考えられ，安全に係る人間にとって常識であろう．この各段階にもそれぞれ，技術的側面，人間的側面，組織的側面が関わっており，安全学として全体性をもって，総合的に考えなければならないと考えた次第である．

更に，安全学の必要性を感じた理由に次のものがある．安全の関係者は，自分の分野に閉じこもり勝ちであり，自分の立場にこだわる傾向が強いと感じていた．安全関係者には真面目な方が多いのがこのような傾向を生むのかも知れない．しかし，安全こそ，他の分野に学ぶべきである．ところが，現実には，なかなか他の安全分野に学ぶのが難しいのである．その理由は，その安全分野独特の考え方や専門用語が歴史的に築き上げられていて，他の分野には容易に理解できないようになっているからである．時には，同じ用語が分野によって異なった意味に用いられていて，理解を困難にしているからである．そこで安全に共通する事項を統一的，体系的に安全学としてまとめ，安全に従事する人には共通した常識とすれば，その安全学の下で，各人の専門の安全分野や安全の役割を深掘りして頂ければ，安全学を通して，お互いに他の安全分野に学ぶことが容易になると考えた次第である．

以上のような考え方から，安全学の構造を図示したのが**図3**である．この図の意味していることは，一番下の第3層には，各分野の安全，例えば，自動車安全，機械安全，製品安全，食品安全等々無数にある各安全の分野を置き，各分野に共通する技術的側面，組織的側面，人間的側面を一般化，抽象化して中間の第2層に置き，それらを第1層の理念的側面のもとに全体性をもって，統一的に，総合的に考察する学問が，安全学であることを表わしている．各側面の具体的例を**表1**に示す．安全学のこれ以上の解説は，専門書に譲ることにして[1]，以下に，理念的，技術的な側面のいくつかの項目について簡単に紹介する．

2．安全の基本概念

安全の理念的な側面から安全の基本概念として

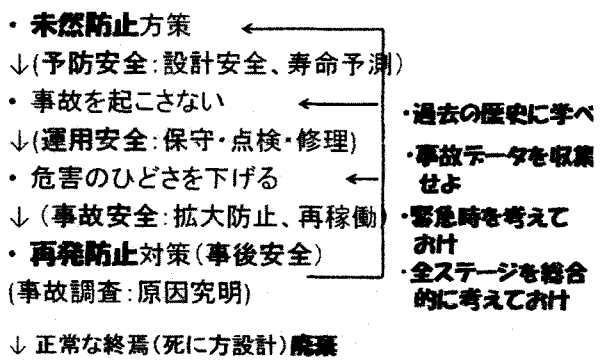


図2　安全確保のステージ

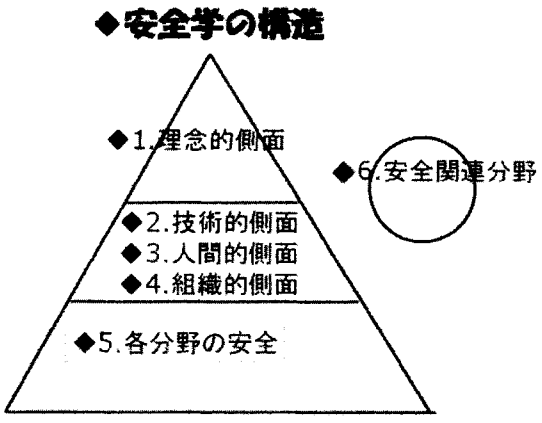


図3　安全学の構造

表1　各側面の例

分類	例
1. 理念的側面	安全哲学、安全思想、安全文化、安全の定義，安全目標，安全の構造，安全の責任、等
2．技術的側面	本質安全設計，フェールセーフ，信頼性，冗長性，機能安全、診断，保全，等
3．人間的側面	ヒューマンエラー，誤使用、HMインターフェース，人間工学，安全意識，認知、訓練・教育、技術者倫理、等
4．組織的側面	標準化，法律，規制，認証・認定，事故調査，マネージメントシステム，危機管理，等
5．各分野の安全	機械安全，鉄道安全，航空安全、情報安全，原子力安全，食品安全，製品安全，電気安全，医療安全，システム安全，労働安全，プロセス安全，ロボット安全，等
6．安全関連分野	防犯，保険，裁判，等

いくつかの項目を紹介しよう．まず，安全にはどの分野にも共通する概念がある．例えば，

(1)機械設備は劣化等でいつかは壊れるものである

(2)人間はいつかは間違えるものである(時には，認知症の人，意識を失う人，悪意の人もいる)

(3)組織やルールに完全なものはあり得ない．

という事実である．これらは，

(4)絶対安全は存在しない(リスクゼロはあり得ない)

ことを意味していて，すべての安全分野に共通の概念である．

次に，安全に関するいくつかの用語の定義を紹介しよう[2]．

1．安全とは…「許容不可能なリスクがないこと」
2．リスクとは…「危害の発生する確率および危害のひどさの組み合わせ」
3．許容可能なリスクとは…「現在の時代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」

上記の安全の定義は，安全といっても許容できるレベルのリスクは残っている状態をいうことを表わしている．このことは，利用者には，その残留するリスクを覚悟して安全を確保する責任と役割があることを表わしている．

安全設計で最も重要な概念と手順は，リスクアセスメントである．リスクアセスメントを文字通り解釈すれば，リスク(risk)，すなわち危険の可能性を，アセスメント(assessment)する，すなわち事前に評価することである．その目的は，事故の未然防止であり，その手順は，装置・設備を製造したり，運用や使用したりする前に，事前に，そこに存在するすべての危険の源泉(ハザード：危険源)に対して，そのリスクの大きさを評価して，その大きさに応じた適切なリスク低減策を施し，残ったリスク(残留リスク)が，作業者や利用者にとって，受け入れ可能，または許容可能なレベルになるまで下げておき，この過程を文書として残して置くことである．

リスクアセスメントの手順の概略を国際安全規格[2]に出てくる**図4**で振り返ってみよう．

まず，その機械・設備の目的，使用条件等を明確にする必要がある．これなしには，安全は語れない．この時，図にあるように，予見可能な誤使用の明確化を忘れてはならない．これは，意図した使い方，指定した正しい使い方でなくても普通の人間ならばやりそうな使用法(これを誤使用と呼ぶのがよいかどうか分からないが，一般的には合理的に予見可能な誤使用と呼ばれている)は，はじめから予見しておき，設計として事前に対応をしておかなければならないことを表わしている．次のステップが，危険源の同定(Identification)であるが，危険源(hazard)とは，リスクを発生させる潜在的な危険の源，危害を発生させる原因となる根本的なものをいう．危険源の同定とは，対象としているシステム・機械・設備・製品に存在する危険源をすべて見出せということである．次に，その見出された各危険源すべてについて，それぞ

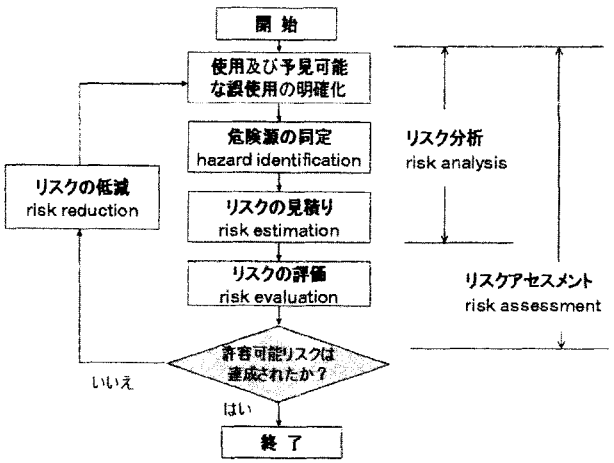


図4　リスクアセスメントの手順(ISO/IEC ガイド51[2]より)

(1)本質的安全設計によるリスクの低減
(2)安全防護対策(安全装置等)による
リスクの低減
(3)使用上の情報の提供による
リスクの低減

↑設計製造側の役割　　↓作業者の役割

＊訓練、個人防具、組織・体制・管
理によるリスクの低減

図5　スリーステップメソッド

その危険源が持つリスクを見積もる．すなわち，その危険源が原因で，危害が起きる頻度と危害の大きさを見積もる．次に，各危険源ごとに，危害の頻度とひどさからリスクの大きさを決める．最後が安全か否かの判定で，そのリスクの大きさが，十分に小さいか，許容可能か否かを判断する．もし，十分でない，許容できない時には，その危険源に対してリスク低減方策(保護方策)を施さなければならない．各危険源ごとにすべてのリスクが許容可能と判断されれば，これらのステップを文書化してリスクアセスメントは終わる．リスク低減方策には，実は施すべき順番があって，図5にその順番を示す．いわゆるスリーステップメソッドと呼ばれるもので，まず，本質的安全設計を行う．それでも残ったリスクに対しては，安全防護策(安全装置等)を施し，それでも残った残留リスクに関しては，安全に使うための使用上の情報を作業者や利用者に提供する．ここまでが機械・設備のハードウエア側の役割であり，その使用上の情報に基づき，作業者は保護具，訓練等で安全を確保する．ここでは，人間の注意の前に，機械・設備側の安全化を先に実行するという鉄則が示されている．

3．安全技術の基本概念

技術で安全を守る役割において共通する安全設計の基本的な考え方を以下にいくつか紹介する．

(1)　フォールトアボイダンス

システムの安全性を確保するためには，構成している部品やサブシステムが故障しないような信頼性の高いものでなければならない．まず，壊れにくい信頼度の高い部品を使用することが第一である．このアプローチは，最初から故障や欠陥は入り込まないという意味でフォールトアボイダンス(Fault Avoidance：故障回避)と呼ばれる．温度，湿度，振動，放射線，経年劣化等々に耐えなければならない．高信頼度の部品を作成するためには，物理的，化学的な究明と共に，品質管理の徹底が必須である．十分なテストも必要であり，一般的に超高信頼化部品は高価になる．そこで，それほど信頼度の高くない部品を用いてシステムとしての信頼度を上げるアプローチとして，次のフォールトトレランスがある．

(2)　フォールトトレランス

フォールトトレランス(Fault Tolerance)とは，システムを構成している一部に不具合(フォールト：Fault)が生じても，それに耐えて，またはそれを許してシステムとしては正常に機能するようにすることである．基本的には冗長技術を用いている．冗長技術には，空間冗長(二重系，三重系，多数決系，多重系，n out of m系等)，情報冗長(誤り訂正符号等)，時間冗長(正常になるま繰り返す)，等がある．冗長系や多重系はシステムの信頼度を上げることが目的である．原子力における多重防護の考え方は，基本的には多重系であるフォールトトレランスの一種と考えられる．この場合，多様性を伴った独立性の概念が重要である．すなわち，ハードでいえば，common mode failure(共通原因故障)がないように，機構的にも，配置的にも，材料的にも，エネルギー的にも，コンピュータのソフトウェア的にも多様性をもった独立性が要請される．なお，監視やチェック等における組織や人間にの独立性についても同様である．

(3)　フェールソフト

フェールソフト(Fail soft)とは，故障や障害の発生により，完全な機能は実現できなくても，大事な機能は最後まで維持して，徐々に縮小しながら機能を失っていくという考え方である．突然に故障してストップするのではなく，徐々に(ソフトに)壊れていくという考え方である．生きながらえることを優先するのである．故障がある場合

にそこを切り離して，システムを再構成することにより，システムの機能・性能を低下させて稼働させるシステム縮退もこの一種である．縮退運転ともいわれる．フォールバック(fall back)もこの一種である．分散冗長(機能を落としてでも稼働し続ける)もフェールソフトの一つと考えられる．分散冗長には，負荷分散，機能分散，危険分散，地域分散，等々がある．システムの一部が故障しても，故障箇所を切り離して残りの部分で機能を維持する例として，飛行機がある．一つのエンジンが壊れても墜落せずに残りのエンジンで飛び続けられる．人間は，フォールトトレラントになっており，かつフェールソフトにできている．例えば，腕，目，腎臓等は二つあって冗長系になっている．ただし，最後の重要な機能を保つ心臓は一つしかない．

(4) フールプルーフ

人間は，誤りや間違いをするもの．フールプルーフ(Fool proof)とは，人間が間違えても危険な誤りを起こせないような構造的な設計をいう．危険側の誤りが発生しないような設計である．誤りを起こしたら次へ進めないように安全側に固定する設計も含まれる．「ポカよけ」と呼ばれることもある．基本的には，間違えても大丈夫なようにする，間違えられない構造とする，少しぐらいの間違えならば許す構造などをいう．

(5) フェールセーフ

故障しても(失敗しても)安全であるという考え方．故障は認めるが，安全側の故障のみとすること．故障すると，正しい機能を果たすか，または，ある決まった状態に固定されるように構造的に構成する．重力等を利用する場合が多い．止まれば安全などの無条件安全の状態の存在が条件となる．フェールセーフは，安全性を目的としている．

(6) 危険検出型と安全確認型(図6)

センサー等に基づく安全システムの作り方には，次の二つの考え方がある．

1．安全確認型(透過型センサー)－安全であることを確認して，安全情報を受けているときだけ作業を続行する．安全情報がない時は止める．

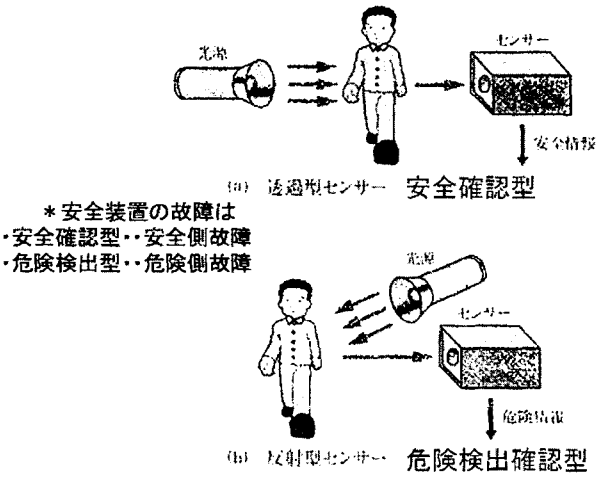


図6 安全確認型と危険検出型

2．危険検出型(反射型センサー)－危険であることを検出して，この危険情報により作業を止める/回避する．危険情報がない時は続行する．

光源やセンサーが故障すると，危険検出型では人間が検出されず，危険信号が伝達されないので危険な状態が発生する．すなわち，危険側故障となる．安全確認型では，安全信号が伝達されないので，危険状態は発せしない．すなわち，安全側故障となる．センサー等の故障を考えると，システムをフェールセーフに構築するには安全確認型でないと構成できないことが分る．

4．まとめ

なぜ，安全学なる新しい学問体系を考えるようになったかの経緯と共に，安全と安全設計に関する基本概念について紹介した．安全の基本概念は，安全に関係する多くの分野に共通する考え方である．また，安全設計の基本概念は，ものづくり安全の世界では，どの分野のどの製品でも通用する安全技術における共通概念である．このように分野を超え，立場を超えた安全や安全技術の共通概念は，安全に関する総合的な学問である安全学の重要な一部を構成している．ここで紹介した内容は，安全以外の分野にも参考になるアイデアが多く含まれているのではないかと考えられる．

参考文献

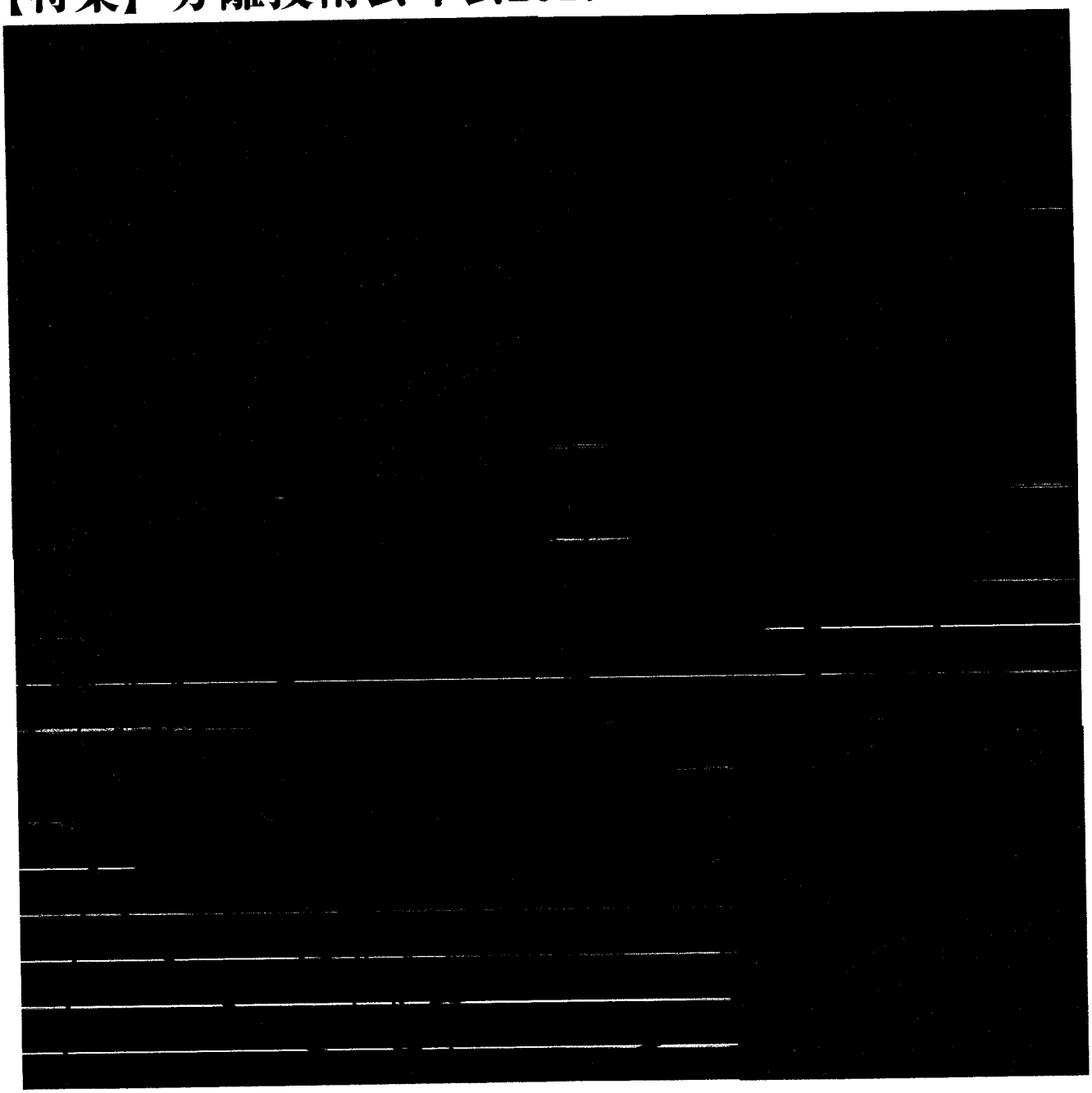
1) 向殿政男：入門テキスト安全学，東洋経済新報社，2016-3
2) ISO/IECガイド51，1.999（JIS Z 8051, 2004） 安全側面－規格への導入指針

ISSN 1343-7860

分離技術

NO. 5
2017 vol.47

【特集】分離技術会年会2017



URL : http://www.sspej.gr.jp
SSPEJ 分離技術会
The Society of Separation Process Engineers, Japan