「労働安全衛生研究」, Vol. 3, No.1, pp.37-46, (2010)

総　説

リスクベースド・アプローチによる機械安全の現状と今後の課題†

松　本　俊　次*1

「機械の包括的な安全基準に関する指針」の公示，「機械類の安全性」に関するJIS B 9700などの刊行により，わが国の産業界においてもリスクアセスメントによる機械安全化が実施されるようになってきた．しかし大多数の事業所におけるその実態をみると，設計フェーズと運用フェーズに限定されたものとなっている．本稿では全ライフサイクルの各フェーズで今後取組むべきリスクベースド・アプローチによる機械類の安全化の課題，および今後活用すべき有用なリスクアセスメント手法について述べる．また，安全と品質は表裏一体の関係にある．そこで設計フェーズにおいてリスクベースド・アプローチで得られた機械類の安全設計品質の健全性を運用フェーズに至るまで維持しなければならない．このためOSHA／PSMの規定する機器類の健全性（mechanical integrity）の考え方を参考に，機械設備の安全性の確保に必要とする品質安全マネジメントのあり方についても言及する．

キーワード: 安全設計品質，RPN，JHA，健全性，ISO 9000s

1　はじめに

わが国の産業界において，リスクアセスメントによる機械安全化が実施されるようになったのは,「機械の包括的な安全基準に関する指針」の公示，JIS B 9700「機械類の安全性」およびJIS B 9702「機械の安全性－リスクアセスメントの原則」の刊行によるところが大きい．

機械類に潜在的に存在する危険源や危険事象を特定し，そのリスクを推定評価してリスクの低減を図るリスクベースド・アプローチによる機械安全化に関して，前記指針およびJIS が，機械類の全ライフサイクルにおける安全化の必要性を述べている．しかし，これらの指針およびJISに基づくリスクベースド・アプローチによる機械安全化は，機械製造者による設計上のリスク低減と残留リスクについての機械使用者への伝達，および機械使用者による新設機械類に対する更なる保護方策の実施について主眼を置いたものとなっている．このため産業界において実施されているリスクベースド・アプローチによる機械安全化は，設計フェーズ（段階）と運用フェーズに限定されたものとなっているのが現状の実態といえる．

一方，産業界で活用しているリスクアセスメント手法は，ハザード分析に関しては，チェックリスト法またはそれに類する手法が大多数を占めており，リスク評価法は，システム安全規格のMIL-STD-882が例示しているマトリクス法が大多数を占めている．このような実態から本稿では，全ライフサイクルの各フェーズで今後取組むべきリスクベースド・アプローチによる機械類の安全化の課題，および米国の産業界で活用している有用なリスクアセスメント手法について述べる．さらにリスクベースド・アプローチにより得られた機械類の安全設計品質の健全性維持に要する品質マネジメントのあり方についても言及する．

† 原稿受付　2009年11月30日

† 原稿受理　2010年02月10日

*1 松本技術士事務所

連絡先：〒259-1126 神奈川県伊勢原市沼目3-25-2

2　産業界におけるリスクベースド・アプローチによる機械安全化の現状

「機械の包括的な安全基準に関する指針」の公示および機械類の安全性に関するJISの刊行により，リスクアセスメントに基づく機械安全化の概念が，現在，産業界に定着しつつある．その結果，機械製造事業者および機械使用事業者が，機械設備が潜在的にもつハザードに起因するリスクの低減を図るリスクベースド・アプローチによるエンジニアリングとマネジメントの重要性を認識し，機械安全化に積極的に取組む姿勢が事業者にみえてきた．

しかし，前記指針およびJISは，リスクベースド・アプローチによる機械設備の安全化の主眼を，単体機械の設計フェーズと運用フェーズの保護方策においたものとなっているため，現状のリスクベースド・アプローチによる機械設備の安全化の進め方は，この範囲内に止まっているのが現状である．

また，リスクアセスメント実施のベースとなるハザード分析についてみると，ISO 14121「機械類の安全性―リスクアセスメントの原則」の中の付属書で採り上げている「危険源，危険状態および危険事象の例」を引用したチェックリスト法あるいはそれに類する手法が，活用されているのが現状である．

機械設備に関わるハザード（危険源）あるいはハザード事象（危険事象）は，機械自体のみならず原材料などのモノ，ユーティリティ，製造／工程，人／組織，作業手順，作業マネジメント，作業環境などにも存在する．このためリスクベースド・アプローチによる機械設備の安全化は，設計フェーズから運用保全フェーズに至る機械設備の全ライフサイクルの各フェーズにおいて実施してこそ真に実現する．したがって，設計フェーズにおけるチェックリスト法によるハザードの特定にのみに依存した手法では，他のフェーズにおいて活用されるべきリスクベースド・アプローチによる安全化の推進は限定されたものとなってしまう．例えば，ヒューマンエラーに起因するハザードであるヒューマンハザード，意図しな

いエネルギー放出によるハザード，設計・材料・操作などに関わる変更作業に起因するハザードなどに対しては，チェックリスト法以外の有用なハザード分析手法の活用が不可欠となる．

そこで全ライフサイクルにおいて潜在的に存在する種々多様なハザードを見落とすことなく特定し，そのリスクを評価するためには，リスクベースド・アプローチによる機械安全化が先行している米国産業界で活用されている手法に目を向けるべきである．

3　リスクベースド・アプローチにおける機械の安全化の現状と課題

機械の安全化は，機械設備の全ライフサイクルの各フェーズにおけるリスクベースド・アプローチの実施により実現する（表 1 参照）．このため産業界で広く実施されている設計上の残留リスクに対する保護方策を主体とした安全化では不十分と云わざるを得ない．この現状を打破して更なるリスクベースド・アプローチによる機械の安全化を推し進めるには，下記に示すような事項にも取り組むことが必要となる．

①設計・運用フェーズ以外の調達，製造，施工，コミッショニング，運転，保全の各フェーズにおいてリスクベースド・アプローチによるリスクの低減を図る．

②多数の単体機械が統合されシステム化された機械設備においては，機械自体のみならず，機械と機械，機械と環境，機械とユーティリティなどの相互間のインターフェースに関わるハザードやハザード事象に対しても，リスクベースド・アプローチによるリスクの低減の実施が必要となる．

③全ライフサイクルに潜在的に存在するハザードやハザード事象に起因するリスクに対して，リスクベースド・アプローチによる安全化を図るためには，現在，産業界で広く普及しているアセスメント手法の他に，米国の産業界において活用されているリスクアセスメント手法を機械設備の安全化においても取り入れるべきである．

④安全と品質は，表裏一体の関係にある[1)]．設計フェーズにおけるリスクベースド・アプローチの結果で得られた安全上重要なサブシステムやコンポーネントの安全設計品質は，設計フェーズの後工程である調達，製造，施工，コミッショニングの各フェーズを経て運転保全フェーズに至るまで維持しなければならない．このため安全上重要なサブシステムやコンポーネントについては，設計フェーズにおいてリスクベースド・アプローチにより得られた安全設計品質の健全性を維持する品質マネジメントが必要不可欠となる．

⑤施工フェーズあるいは運転保全フェーズにおける次の課題に対しても，リスクベースド・アプローチによる機械の安全化が必要である．

・溶接，据付，閉鎖空間内などに関わる作業に伴うハザードに対する事故防止対策の立案と実施

・ユーティリティーの停止や主要設備故障のような緊急事態対応計画ならびに防火防災対策の立案

4　リスクベースド・アプローチによるフェーズ別の機械安全化の課題

産業界におけるリスクアセスメントの現状の実施状況からみて，今後取組むべきリスクベースド・アプローチによる機械安全化の課題は，機械設備の全ライフサイクルの各フェーズに存在する．設計フェーズで得られたリスクベースド・アプローチによる安全設計品質の健全性は，設計，調達，製造，施工，コミッショニング，運用，保全の各フェーズにおいて維持しなければならない．したがって各フェーズにおいてリスクベースド・アプローチによる機械安全化の課題がそこに存在することになる．

元来，リスクベースド・アプローチによる機械安全化の考え方は，米国の国防総省（DOD）および航空宇宙局（NASA）によるシステム安全規格に遡ることができる（表２参照）．安全と品質は，表裏一体の関係にあるので，システム安全規格は，DOD が調達先に対して，品質マネジメント規格と併せて遵守することを求めるためのものであった．DOD の調達用品質マネジメント規格の概念は，BS 5750 を経て ISO9000s シリーズの品質マネジメントシステム規格に引き継がれている．したがってリ

表１　リスクベースド・アプローチによる機械安全化に関する課題

	リスクを生み出す要因の例	リスクベースド・アプローチによる機械安全化のための課題の例
設　計 フェーズ	設計変更、資機材の変更	・機械設備を構成するサブシステム、ユニット、コンポーネントなどに対するリスク優先度指数（RPN)の算出 ・設計、コンポーネント、材料、ソフトウェアなどの変更に伴うハザードの特定とリスク評価 ・機械システム設備における機械間、機械・ユーティリティー間、 機械・環境条件間などのインターフェースに潜在的に存在するハザードの特定とリスク評価
調　達 フェーズ	調達先の品質マネジメントの不備	・調達品に潜在的に存在するリスク優先度指数（RPN）の算出 ・RPNに基づく調達先の選定 ・RPNに基づく試験検査レベルの決定
製　造 フェーズ	製造プロセスにおけるリスクマネジメントの不備	・製造工程に潜在的に存在する製造品質リスクの優先度指数（RPN)の算出 ・RPNに基づく作業工程および試験検査作業の改善
施　工 フェーズ	据付、組立、施工などの諸作業に対する労働安全マネジメントの不備	・重力、熱、放射線などのエネルギーに起因するハザードに対するリスク評価に基づく対応策の立案 ・作業手順、施工条件、ユーティリティー、建設機械器具などの変更に伴って生じ得るハザードの特定とリスク評価
コミッショニング フェーズ	作業点検調整の不備	・サブシステム、ユニット、コンポーネントなどに対するリスク評価と格付けに基づく作業手順、判定基準、不具合発生時への対応立案
運　用 フェーズ	作業手順の誤りや変更、点検の不備	・サブシステム、ユニット、コンポーネントなどに対するリスク評価と格付けに基づく点検保全計画の立案と実施 ・不具合／事故情報に対するリスク評価と対応策の実施

表 2　DOD および NASA のシステム安全と品質マネジメント規格

	DOD（国防総省）の システム安全に関わる規格	NASA（米国航空宇宙局）の システム安全に関わる規格
システム安全の 要求事項を規定した規格	MIL-STD-882： System Safety Programs for Systems and Associated Subsystems and Equipment Requirements 1969	NHB 1700-1(v3)： NASA Safety Manual, System Safety 1970
品質マネジメントの 要求事項を規定した規格	MIL-Q-9858： Quality Program Requirements、1954	NHB 5300.4 (1B) Quality Program Provisions for Aeronautical and Space System Contractors、1969

スクベースド・アプローチによる機械安全化への取組むべき課題の多くは，ISO 9000s シリーズの中に示唆されている．ただし，わが国の産業界においては ISO9001 による品質マネジメントシステムの認証取得にのみに関心が向けられ，ISO 9000s シリーズに織り込まれているリスクベースド・アプローチによる安全設計品質の維持に関する規定については注目されず現在に至っている．

1)　設計フェーズで取組むべき課題

a）機械の構成要素に対するリスク評価

機械設備を構成する多種多様なコンポーネント（サブシステム，ユニット類を含む）に潜在的に存在するリスクレベルは，すべて同一ではない．コンポーネントによっては起こり得る不具合や故障が，上位のサブシステムあるいはシステム全体に大きなリスクをもたらす．不具合や故障が上位のシステムに致命的影響を及ぼすものほど設計基準，耐久性，検査基準などの要求仕様を厳しくし，リスクレベルの低減を図らねばならない．

大きなリスクをもたらす可能性のあるコンポーネントの品質や信頼性に問題が生じれば，機械設備システムに重大な影響をもたらす．自動車業界においては，コンポーネントの不具合が自動車の安全性に大きな影響を及ぼすものを従来から経験的に「重要（保安）部品」，不具合が安全性に及ぼす影響の少ないものを「汎用部品」として区分してきた．しかし，1993 年，自動車の構成要素に対するリスク評価法としてリスクベースド・アプローチによる実務的で簡便な手法が，米国自動車業界の SAE（Society of Automotive Engineers）により，SAE J-1739 Potential Failure Mode and Effects Analysis として刊行された．

この SAE J-1739 に提示されている設計用 FMEA により，コンポーネントのもつリスク評価が，客観的相対値であるリスク優先度指数（RPN：Risk Priority Number）として算出できるようになった．SAE によるコンポーネントのリスク評価法の考え方を導入している自動車生産用の ISO 9001 対応の ISO/TS 16949 品質マネジメントシステム[2)] では，製品設計フェーズにおいて SAE 方式の設計用 FMEA[3)] および製造用 FMEA[4)] の実施を次のように規定している．

> 7.5.1.1 コントロールプラン
> 組織は次の事項を行うこと。供給製品のシステム、サブシステム、構成部品、及び/又は材料の各レベルで、設計用 FMEA 及び製造用 FMEA の結果を考慮した量産試作段階および量産段階のコントロールプランを有すること。

b)　設計変更に伴うリスク評価

設計フェーズにおいて設計，コンポーネント，材料，ソフトウェアなどに関する作業を実施する中で，様々な変更を迫られる状況がしばしば発生する．このような変更は，機械設備に望ましくないリスクをもたらすこともある．このため変更に際しては，変更作業に起因して起こり得るハザードあるいはハザード事象の特定と，そのリスク評価が必要となる．

品質マネジメントシステム規格の ISO 9004 では，設計開発フェーズにおける変更について次のように述べている．

> 変更の結果が望まれた通りのものとなっていることを確実にするために、いかなる場合も関連する変更の後で、妥当性の確認を実施すべきである。(中略)
> リスク評価のツールの例には、次のようなものがある。
> — FMEA
> — FTA　（以下略）　ISO 9004 ：7.1.3.3

DOD 規格ではリスクベースド・アプローチにより評価された変更に起因するリスクの大きさを表 3 に示すように区分し，適切な対応措置を講じることを要求している．

表 3　設計変更の影響度クラス（DOD-STD-480A）

クラスⅠ変更（Class Ⅰ Change）	システムの性能、信頼性、安全性、コスト、または要求仕様に影響を及ぼすような設計変更
クラスⅡ変更（Class Ⅱ Change	システムの要求仕様に影響を及ぼさない比較的僅かな設計変更

なお，表 3 で引用した DOD - STD-480A は「変更管理（Configuration Control）」に関する規格であるが，この変更管理の考え方は ISO 9000s シリーズの「ISO 10007 1997, Quality management systems - Guidelines for Configuration management に引き継がれている．

c)　インターフェースに関わるリスク評価

多数の機械設備から構成される機械システム設備においては，機械間，機械・ユーティリティー間，人間・機械間，機械・環境条件間のインターフェースに関わるハザードが潜在的に存在する．したがって，特に機械シス

テム設備においては，このようなインターフェース間に存在し得るハザードの特定とリスク評価が必要不可欠となる．この点についてISO 9001対応のISO/TS 16949では，次のように規定している．

> 7.3.1.1　境界領域的アプローチ
> 製品を具現化するために境界領域的アプローチをすること。これには次の事項を含めること。
> ―　潜在的リスクを低減する処置を含むFMEAの実施およびレビュー

2)　調達フェーズで取組むべき課題

調達品のもつ潜在的リスクの大きさに比例したベンダーの選定が必要不可欠となる．このため設計フェーズで算定したコンポーネントのRPNにより，調達品のもつリスクの大きさに基づき下記事項を実施する必要がある．なお，ISO 9004ではこの点に関して次のように規定している．

> 購買プロセスには、次のような活動を考慮したマネジメントを確保すべきである。
> ―　当該購入品に関連するリスクの特定と低減
> （以下、略）
> ISO9004：7.4.1

a)　RPNに基づく調達先の選定

一定水準の品質を有する調達品を購入するためには，調達先であるベンダーの格付け（Rating）に基づき，調達品のもつ潜在的リスクの大きさに比例したベンダーの選定が必要不可欠となる．調達品のもつ潜在的リスクの大きさを推定評価する手法としては，前述したSAE J-1739の規定する設計用FMEAの活用が望ましい．

b)　RPNに基づく製品仕様と試験検査の決定

RPNが一定値以上の調達品については，ベンダーに対する製品発注書において，安全基準，定常状態と過渡状態時の設計上の要求仕様，耐久性・信頼性・保全性を含む構造上の要求事項，試験検査要求事項，品質保証および関連ドキュメントの提出などに関する要求仕様を重視した発注条件が重要となる．

3)　製造フェーズで取組むべき課題

機械類の製造ラインの各工程において，生産設備や作業に起因して不具合事象が発生する可能性がある．不具合の発生は，製造品質に影響を及ぼす．影響の度合は，製造ラインの工程により異なる．

各工程で潜在的に起こり得る製造設備や作業条件の逸脱に起因する不具合事象の製造品質への影響度，その発生頻度，およびこれらの不具合事象の検出度から，各工程の製品品質に及ぼすリスクを評価し，リスクに比例した生産管理によることが望ましい．

このためのリスクベースド・アプローチによる分析手法として最適なものがSAE J-1739の規定する製造用FMEAである．各工程のリスク優先度指数（RPN）に基づき意図する製造品質を得るために重点的に工程管理すると共に，RPNの値に応じて当該工程の試験検査作業の改善を図る．この考え方は，食品製造工程について危険分析を実施して重要管理点（Critical Control Point）を設定し，危害の発生原因とその防止策を立案実施する食品安全管理基準であるISO22000の規定する概念に類似するものである．

4)　施工フェーズで取組むべき課題

a)　施工作業の変更に伴うリスク評価

作業手順，施工法，ユーティリティー，建設機械，作業者などを変更せざるを得ない場合，その変更により生じ得るハザードあるいはハザード事象に起因するリスクを最小限に抑えなければならない．このためリスクベースド・アプローチによるリスクの低減策が必要不可欠となる．

米国のコンストラクション OSHA §1926 [5] は，工事業者に対して，次のような工事安全プログラムの策定と実施を要求している．

> 工事安全プログラムは、次の事項から構成すること：
> ―　現場のハザードの特定と管理に関する手順の確立手段／方法
> ―　プラン、作業ルール、標準作業手順／方法
> （以下、略）　OSHA §1926

b)　事故防止のためのリスク評価

建機による重量物の吊上げ，溶接工事，非破壊検査などの諸作業は，重力，熱，電気，放射線などのエネルギーを伴う作業であるから，適確な施工管理が実施されていなければ労災事故や災害発生の要因となる．したがって，作業に伴う意図しないエネルギーの放出や漏洩，拡散などに起因するハザードを特定しリスクを評価するリスクベースド･アプローチによる事故防止が必要となる．

米国のOSHAは，このようなエネルギーの放出，拡散などに起因して労災事故が多発するクレーンなどの建機作業，溶接作業，あるいは視覚による安全確認ができない閉鎖空間内の作業などは，責任者の許諾を要する作業（Permit Works）として位置付け，工事安全プログラムの策定と運用上の規制をしている．

5)　コミッショニング・フェーズで取組むべき課題

プレコミッショニング作業およびコミッショニング作業において，設計フェーズで得られたリスクベースド・アプローチによるコンポーネントの安全設計品質が維持されていることを確認し，あるいは維持されるように試験調整を実施しなければならない．このためサブシステムやユニットを含むコンポーネントに対するリスク評価

と格付けに基づき，作業手順，判定基準，不具合発生時への対応策などを立案する必要がある．

OSHA／PSM [6] は，高リスクの新設設備のコミッショニングに対しては，OSHA の査察官が現地に立ち入り，設計フェーズから施工フェーズに至るまでリスクベースド・アプローチによる安全設計品質の健全性を維持するためのエンジニアリングおよびマネジメントが実施されたことを示す証の提示を求める規定を設けている．

6) 運用フェーズで取組むべき課題

a）保全計画の立案

機械設備を構成する多種多様なコンポーネントがもつ潜在的なリスクの大きさは，コンポーネントにより異なる．このため保全計画の立案に際しては，リスクベースド・アプローチによる手法が役立つ．機器類の損傷メカニズムに焦点を当てたリスクベースド・アプローチによる機械設備の保全計画の策定手法としては，ASME（米国機械学会）が提示している RBI（Risk Based Inspection）／RBM（Risk Based maintenance）がある．

また，リスクベースド・アプローチに基づく検査計画を策定することにより，安全プログラムを改善することもできる．このような RBI 手法としては，API RP 580 Risk-based Inspection による RBI 手法がある．なお，OSHA/PSM は，高リスク設備に対してプロセスの安全確保の上で重要な機器類に関して，安全設計品質のメカニカルな健全性（Mechanical integrity）を保持するための RBI スタディーを要求している．

b） 危機管理アクションプランの策定

可燃性化学物質を扱う化学プロセスプラントのような事業所でなくても，機械設備が主体をなす造船所，タイヤ製造工場などにおいても，溶接作業などに起因して大きな火災事故が過去に発生している．多数の機械設備から構成される機械システム設備の新設計画あるいは運用に際しては，その生産基盤を脅かす重大事故や火災などの緊急事態の発生に対して，危機管理アクションプランの策定が必要となる．この点について ISO/TS 16949 は，次のような規定を設けている．

> ユーティリティーの停止、労働力不足、主要設備故障および市場回収のような緊急事態対応計画を立案すること。　　ISO/TS 16949、6.3.2

緊急事態に備えた危機管理アクションプランを立案するには，ハザードを特定しリスクを推定評価するリスクベースド･アプローチに基づくものでなければならない．推定評価したリスクの大きさから，組織内で定めた緊急事態アクションレベル（EAL：Emergency Action Level）により，必要なアクションプランを策定する（表４参照）．

米国では，事業所における危機管理アクションプランの策定に関して OSHA がアクションプランの構成項目を規定し[7]，NSC（National Safety Council）がリスクアセスメントに基づく計画立案についてのガイダンスを公示している[8]．

表４　　緊急事態アクションレベル（EAL）の設定例

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

5 活用すべきリスクアセスメント手法

リスクベースド・アプローチによる機械設備の安全化作業に関わるハザードの特定およびリスク評価に関わる手法として，今後，わが国の産業界が積極的に活用すべきものとして，米国の産業界が活用している主な分析評価手法を取り上げる．

1) ハザード分析手法

a） JHA（Job Hazard Analysis）

JHA は，特定の作業を成し遂げるための作業動作を見落とすことなく時系列的にリストアップし，その作業環境下にある機器，装置，工具，原材料，物品，作業工程，エネルギーなどに潜在的に存在するハザードを特定すると共に，作業に伴うヒューマンハザードを特定するための分析手法である．JSA（Job Safety Analysis）とも称されている．

JHA は，個々の作業動作をステップ毎に，一つの動作を一つ操作指示文として，時系列的に列記していく．個々の作業動作ステップ毎にリスクを生み出すハザードが存在するか否かの確認は，表５に示すようなガイドワードからチェックしていく．

表５　JHA 分析用のガイドワードと使用例

Who	誰が行うのか：　熟練者、有資格者、新人など
Why	何故行うのか：　確認、安全確保など
How	どのように行うのか：　保護手袋を着用、工具を使用、腕を伸ばして　など
Condition	どのような条件下で行うのか：　屋外、閉鎖空間内、高所など
Trigger	ハザードを誘引する事象は：　繰返し作業、作業面で滑る、つまずく　など

JHA によるハザード分析の優れている点は，ヒューマンハザードの特定のみならず，機械設備ユーザーに対する操作指示と警告の伝達が，次の理由により適確に実施できることにもある．すなわち，運転保全マニュアルの作成にあたり，JHA 分析作業用ワークシート通りに操作指示文とハザードに対する警告文を記載していくと，操作指示文の記載漏れがなくなり，必要な警告文を関連す

る操作指示文と併せて記載することができる．したがって，製造物責任法理に適った運転保全マニュアルが出来上がることになる．なお，OSHA は，ヒューマンエラーに関わるハザード分析には JHA が最善であるとしている[9]．

b) CA（Change Analysis）

ウラン加工施設で発生した臨界事故にみられるように，作業変更が大きな災害をもたらすこともある．変更作業に起因して発生する可能性のあるリスクを低減するには，起こり得るハザードあるいはハザード事象を見落とすことなく特定し，そのリスクを評価することが，変更リスクマネジメント上から重要な課題となる．

変更リスクマネジメントは，限られた時間内で業務遂行に支障をきたすことなく実施しなければならないから，簡便でかつ見落としのないハザード分析法の実施が望ましい．変更リスクマネジメントに活用できるハザード分析のためのガイドワードとその使い方の例を表６に示す．

表６　変更リスク分析用のガイドワードと使用例

ガイドワード	ガイドワードの使い方の例
What	何を変更するのか：設計、エネルギー、材質、形状、配置、ソフトウェア、作業手順、防護デバイス、機器類など
Who	誰が代わるのか：オペレータ、ワーカー、サブコン、有資格者など
When	いつ変更するのか：即時、適時、随時、常時、不具合発生時など
Why	変更の理由は：耐久性の向上、コストダウン、納期遅延など
How	どのように変更するのか：　電子式検知から機械式検知へ、スタンバイ予備機の設置による信頼性の向上　など
Where	どこで変更するのか：サブコン工場、製造ライン、据付現地など
Condition	どのような状況下で変更するのか：屋内作業下、雨天下、夜間など
Trigger	ハザードを誘引する事象は：落雷、停電地震、電磁ノイズなど

c) HAZOP（Hazard Operability Study）

HAZOP は，プロセスプラントに潜在的に存在するハザードとプラントの操作性を分析する目的で開発された手法である．したがってその分析対象は，流体プロセスに限定されていた．しかし近時，HAZOP は，流体プロセスの圧力，流量，温度などのパラメータに適用する"more"，"less"，"higher"などのガイドワードを用いて，マネジメント分野においても活用されるようになってきた．

表 7　　緊急事態対応計画用のガイドワードとその使用例

ガイドワード	ガイドワードのもつ意味	使用例
no 又は not	意図するものが得られなければ	受電電力がダウンしたら
more	量的に増大したら	火災による被害が拡大したら
failure	故障したら	バックアップ電源が故障したら
part of	意図することが限定されてしまったら	警報システムによる通報が一部に限定されたら
reverse	意図することが逆になったら	責任者がなすべき緊急停止命令を出さなかったら
other than	意図どおりにすべて達成せず、異なることが発生したら	緊急避難通路が塞がれたら

この拡張型の HAZOP を米国の産業界では"Intelligent HAZOP"とも称している．"Intelligent"という語が意味する通り，問題解決のための判断，あるいは意思決定を下すための手法として活用するものである．表７に緊急事態対応計画などに適用する場合のガイドワードとその使用例を示す．

d) ETBA（Energy Trace Barrier Analysis）

火災や重大労働災害の発生は，溶接作業やクレーン作業に起因する事故例にみられるように，流れてはならない流路に熱エネルギーや位置のエネルギーが伝わり，その流路に位置している人やモノあるいは環境にエネルギーが及ぶことにより発生する．

ETBA[10] は，熱エネルギー，電気エネルギー，位置のエネルギー，放射線エネルギーなどの意図しない各種エネルギーの伝導，拡散，放出などに起因して起こる事故や災害の予知活動に有用な手法である．意図しないエネルギーが意図しない地点や空間に流れても，その流路上にあるターゲット（人，モノ，環境）に及ぼすエネルギー流動を抑止する下記のようなバリアーがあれば事故や災害を抑止できる．

バリアーの例

壁面、金属閉鎖空間、配管、電線管、緩衝材、地絡継電器、過電流遮断器、避雷器、フィルター、エアスペース（空隙）、吸音材

ETBA によるリスク分析評価作業は，図１に示す手順で実施する．

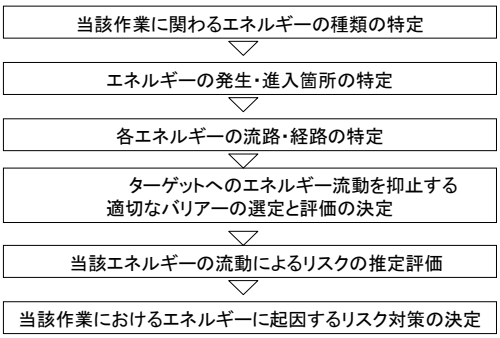

図１　ETBA による分析評価作業手順

2)　リスク評価手法

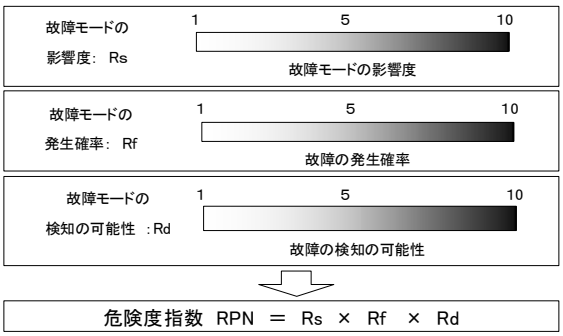

図２　設計用 FMEA

a)　設計用 FMEA（Design Failure Modes and Effects Analysis）

コンポーネントの変形，磨耗，炭化，緩みなどの故障モードの発生により，上位のシステムあるいは最終製品に及ぼす「故障モードの影響度（Rs)」と「故障モードの発生頻度（Rf)」および「故障モードの検出の可能性（Rd)」を図２に示すようにそれぞれ等級化し，各々の指数を１～10 とした相乗積である Rs×Rf×Rd の値を「リスク優先度指数（RPN:Risk Priority Number)」として算出する．評価算出した RPN は，最も影響度の大きい値が 1000（＝10×10×10）で，最も影響度の少ない値が１（＝１×1×１）となる．

RPN の値が一定水準の大きいコンポーネントから順次優先的に改善してリスク低減策をとる．リスク評価対象の多数のコンポーネントの RPN 値を低レベル，中レベル，高レベルと区分した場合には，図３および表８に示すような判断と対応策が必要となる．

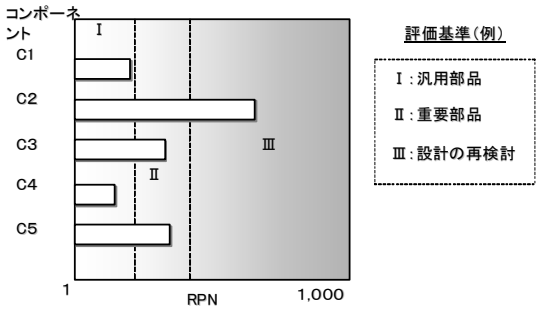

図３　設計 FMEA：危険度指数の評価例

表８　RPN によるリスク判定基準例

RPNの範囲	評価判定基準
Ⅰ	・許容できる。現状のままでよい。
Ⅱ	・リスク軽減対策を図る。 ・調達条件を再検討する。
Ⅲ	・許容できない。 ・設計の再検討が必要となる。

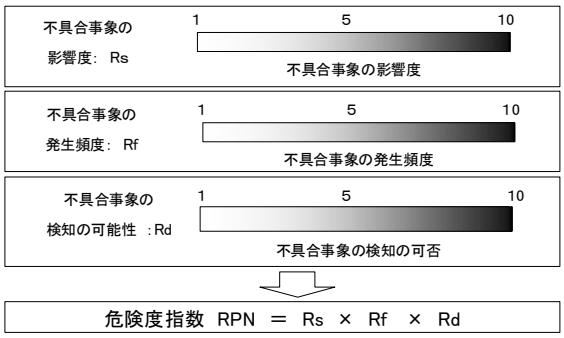

図４　製造用 FMEA

b)　製造用 FMEA（Process Failure Modes and Effects Analysis）

製造設備や作業条件の逸脱に起因する製造工程の不適切な嵌め合い，切削不良，組立てなど不具合事象による各工程の製品品質に及ぼす「不具合事象の影響度（Rs)」，「不具合事象の発生頻度（Rf)」および「不具合事象の検知の可能性（Rd)」を図４に示すように各々を等級化し，その指数を１～10 とした相乗積である Rs×Rf×Rd の値をリスク優先度指数（RPN: Risk Priority Number)」として算出する．評価算出した RPN は，最も影響度の大きい値が 1000（＝10×10×10）で，最も影響度の小さい値が１（＝１×1×１）となる．RPN の値が一定水準の大きい工程から順次優先的に改善し，製造工程に起因するリスク低減策を採る．

c)　RBI/RBM（Risk Based Inspection/Risk Based Maintenance）

一般に RBI/RBM は，設備システムを構成する多様なコンポーネントの中でシステムダウンをもたらすリスクの大きい機器類を選定し，その部位の機械的破損による被害の大きさと破損の起こり易さから，保全計画の策定に用いる手法として知られている．これに対して API RP 580 による RBI は，米国の OSHA/PSM，欧州の Seveso Ⅱ指令 [11] などの法的安全要求規定や PHA（Process Hazard Analysis），RCM（Reliability Centered Maintenance）などのハザード分析手法を補完する統合マネジメントツールとして，他のリスクマネジメントでは扱えなかった領域を扱うリスクアセスメントでありマネジメントである [12]．

このため API RP 580 による RBI は，高リスク設備を対象としたものであるが，機械システム設備に対しても事故の未然防止を図るツールとして活用することができる．

図 5 は API RP580 が提示する「機械的破損による被害の大きさ」と「破損の起こり易さ」のファクターから，コンポーネントのリスク評価を行うリスクマトリクスの例である．

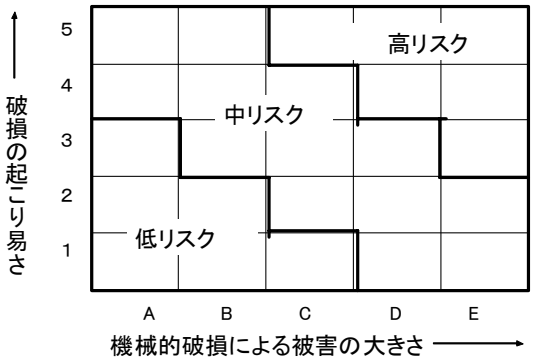

図５　リスクマトリクスの例

6　おわりに

機械設備の設計フェーズにおけるリスクベースドアプローチで得られた安全設計品質は，後工程の調達フェーズから製造，施工，コミッショニングなどの各フェーズを経て運用フェーズに至るまで，その健全性を保持しない限り，機械設備の安全性は真に達成できるとは云い難い．

米国の OSHA/PSM の規定では，化学プロセスプラントのような高リスク設備に対して，設計フェーズにおいてリスクベースドアプローチで得られた安全設計品質の健全性をコミッショニング・フェーズに至るまで維持するためのエンジニアリングとマネジメントの実施を設備設計事業者に求めている．この OSHA/PSM で要求している安全設計品質の持続的維持は，プロセスの安全性を維持する上で重要な機器類に対して，メカニカルな健全性（mechanical integrity）の保持を要求するものである．

この考え方は，電気/電子/プログラマブル式安全関連システムの機能安全性の国際規格である IEC 61508 において，制御系システムの安全機能の健全性レベル（SIL: Safety Integrity Level）を被制御系の装置・機器類（EUC : Equipment Under Control）が潜在的にもつリスクの大きさに応じたものとする，という考え方と一致する．

OSHA／PSM では，設計フェーズで得られた機器類の安全設計品質をコミッショニング・フェーズまで維持するため，製造フェーズからコミッショニング・フェーズまでの一貫したポリシーに基づく品質マネジメントの実施とその証の提示を求めている．

安全と品質は表裏一体の関係にあるので，品質マネジメントの観点から機械設備の安全化には，いかなるエンジニアリングおよびマネジメントが必要であるかということは，前述したような背景から ISO 9000 s シリーズ，とりわけ ISO 9004「品質マネジメントシステム ― パーフォーマンス改善の指針」の中に示唆されている．

米国では OSHA/PSM と ISO 9000s を融合した安全マネジメントシステムの概念を「総合品質安全マネジメントシステム（Total Quality Safety Management System）」[13] とも称している．わが国の ISO 品質マネジメントシステム規格は，従来，認証取得のための規格としての認識に限定されてきた．しかし，ISO 9000s 品質マネジメントシステム規格は，MIL-STD-882 システム安全に必要とする品質マネジメントについて規定する規格の流れを受け継いでいるのであるから，リスクベースド・アプローチによる機械安全化が求められる時代においては，機械設備の全ライフサイクルにおける安全設計品質の健全性の保持に要する品質マネジメントのあり方を示唆するものである，という認識に立たねばならない．そうすれば必然的にリスクベースド・アプローチによる機械安全化に関わる今後の課題が明白になってくる．

文　　献

1) HSE, Successful Health & Safety Management - Health and Safety series booklet HS(G)65, 1991; 12
2) ISO/TS 16949 Quality management systems - Particular requirements for the application of ISO 9001-2000 for automotive production and relevant service part organizations
3) Design Failure Mode and Effects Analysis
4) Process Failure Mode and Effects Analysis
5) OSHA §1926 Safety and Health Regulations for Construction
6) OSHA §1910.119, Process safety management of highly hazardous chemicals
7) OSHA §1910.38, Employee emergency plans and fire prevention plans
8) NSC, Accident Prevention manual for Business & industry - Engineering & Technology, 12th, Ch.11, 2001
9) http//www.osha.gov/SLTC/etools/safetyhealth/mod4 factsheets.worksite.html
10) Richard A. Stephans, System Safety for the 21st Century; WILEY, 2004, 149-159
11) Council Directive 96/082/EC of Dec. 1996 on the control of major-accident hazards involving dangerous substances
12) API RP 580 Risk-based Inspection, 2002,:2-3,
13) Michael B. Weinstain, Total Quality Safety Management and Auditing, Lewis Publishers, 1997
14) 須加他，プロジェクトエンジニアリング　ハンドブック，日刊工業新聞社, 1979: 483-499
15) 松本俊次，プラントのプロセス安全，日本プラントメンテナンス協会, 2004

「補足１」

変更管理に関する DOD-STD-480A Configuration Control あるいは ISO10007 Quality management-guidelines for configuration management において使用されている「コンフィギュレーション（configuration）」という用語の原義は，「配置」という意味をもつ．しかし，第二次世界大戦中，米国航空機業界において航空機を大量生産する過程で，コックピットの

計器類などの「配置」の変更を効率的かつ適時に実施するための変更マネジメントが生まれた．このような経緯から変更管理を「コンフィギュレーション・マネジメント(Configuration management)」と称するようになった．

「補足２」

コミッショニング（commissioning）という用語は，試運転作業中における契約当事者間の業務範囲と責任を明確化するため，発注者が実施するコミッショニングとコミッショニングに先立って受注者が実施するプレコミッショニング（precommissioning）に区分される．

Current Situation and Risk-Based Approach to Safety of Machinery

by

Toshitsugu MATSUMOTO [*1]

"Guideline for the comprehensive safety standards of machinery" and JIS B 9700 " safety of machinery" are producing remarkable results in a risk-based approach to safety of machinery in industry. However, the risk-based approach to safety at machine manufacturers and machine users is mostly limited to the design and operating phases. This paper addresses topics for future study in a risk-based approach to safety of machine and risk analysis methods to be utilized over the entire lifecycle of a machine. The level of machine safety obtained from risk-based approach in the design phase must be maintained over the entire lifecycle of the machine. As safety and quality are two sides of the same coin, this paper also describes the quality management needed to ensure safety of machine referring to the mechanical integrity of safety design stipulated in OSHA/PSM.

Key Words: safety design quality, RPN, JHA, integrity, ISO 9000s

*1 Matsumoto Registered Consulting Engineer Office