

社会の安全と安心のためのシステム安全管理の体系

Structure of Systematic Safety Management for Safety and Non-anxiety of Society

京都大学大学院 吉川 榮和 Hidekazu YOSHIKAWA 会員

Structure of system safety management is first discussed, and then several topics are introduced with respect to the scheme of system safety management. They are (i) creation of always generative safety culture in the organization, (ii) model of organizational accident and the philosophy of human error management for the maintenance activity, and (iii) the necessity of implementing technical risk communication activity. Lastly, the concept of offsite operation & maintenance support center, the introduction of proactive countermeasures for organizational accident and the evaluation of safety performance indices of all nuclear power plants by NUCIA are proposed for the future activities in the nuclear industries.

Keywords: safety culture, human error, risk communication, offsite operation & maintenance support center

連絡先: 吉川 榮和 〒606-8501 京都市左京区吉田本町 Tel/Fax:075-753-9217

1. はじめに

最近わが国では、企業不祥事（三菱自工、東電等）、工場・設備爆発（RDF工場、ブリジストン、出光等）、巨大システム（原子力、宇宙の事故等）、医療事故（多数の病院）などがメディアで報道され社会問題となっている。科学技術発展の一方で、それに関与する人間・組織の技術安全管理が行き届かず、社会の安心確保のためにシステム安全管理の体系の一層の向上が期待される。「安全」とは「様々な局面での危険を回避または出来るだけ小さくする営み」と定義して、事故や災害発生時の社会的影響の大きい科学技術システ

ムの「システム安全管理」の全体模式を検討し、図1のように纏めた。

図1の左右は、いわゆる事故の大きさを区別する「事故尺度」を示している。図の下から上方に事故のレベルが大きくなる。図1の左側には、原子力施設でのトラブルのレベルを示す国際原子力事象評価尺度（INES）を示した。

図1の中央部には、システム安全管理のための、「状態」対「対応行動」のマトリクスの体系を示した。縦方向は上述のような事故尺度の段階を示し、一方横方向は、プロセスの異常拡大過程→対応処置→対応の結果、と3つの時間経過を示している。全体として、最下部の正常な状態が、ヒュ

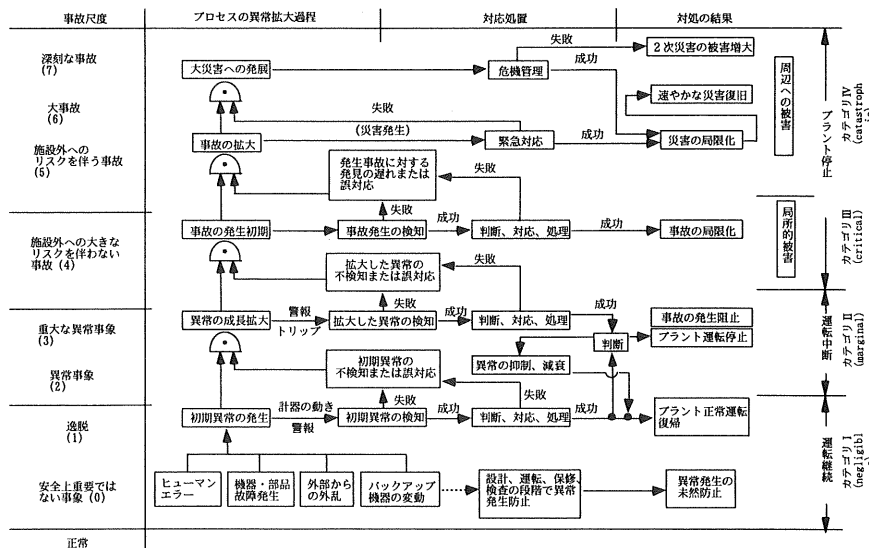


図-1 システム安全管理のマトリクスの体系

ーマンエラー、機械部品の故障、地震等の外部要因、バックアップ機器のトラブル等の要因で、初期異常が拡大して事故になり、対応を誤れば最終的には周辺に被害が及ぶと考え、プロセス異常の拡大過程を縦軸に、横軸にはそれを防止するための対応処置が段階毎に示されている。対応に失敗すれば縦方向の上方にいき、成功すればその段階で収束する。可能性としては緊急対応、さらには周辺に影響が及ぶ大災害の危機管理までをフォールト・ツリーで示している。

このような全体枠組みの中で、各局面におけるトラブルを予見し防護するシステムを組み込んでいくことが、システム安全管理の使命である。

2. 常に学習する安全文化を創造する

JCO 事故調査報告書[1]で、調査委員会委員長の吉川弘之氏は、「安全性と効率性の二律背反」と題して次のような所感を述べている。

- ① 安全を向上させると効率が低下する。
- ② 規制を強化すると創意工夫がなくなる。
- ③ 監視を強化すると士気が低下する。
- ④ マニュアル化すると自主性を失う。
- ⑤ フールプルーフは技能低下を招く。
- ⑥ 責任をキーパーソンに集中すると集団がバラバラになる。
- ⑦ 責任を厳密にすると事故隠しが起こる。
- ⑧ 情報公開すると過度に保守的になる。

事故や災害発生時の社会的影響の大きい科学技術システムでは「安全性の確保」は最も重要である。しかし JCO では経営上の効率が優先されて安全性が軽視され、結果として作業者の人命が失われ周辺住民が退避する大事故を引き起こした。わが国の原子力界では、JCO 事故を契機に「社会の安心確保」の道として組織の「安全文化」の問題が真剣に論じられ取り組まれる一方、電力自由化を背景に「経済性向上」も課題とされている。そこでまず、「安全性と効率性の二律背反」を克服し、「社会の安心確保」を得る道として、まず組織の「安全文化」のあり方を考察する。

1986 年に旧ソ連で発生したチェルノビル事故は結果としてソ連崩壊の端緒ともなった。IAEA の INSAG 報告書は、「安全文化」という言葉で当時のソ連の原子力安全への組織要因上の数々の問題

点を指摘し、その重要性が世界的にクローズアップされた[2]。安全文化の定義やそれをどう測るかは多角的に議論されているが、安全文化には次のような二つの要素がある。

- ① 組織の成員が安全性の追求に対して持つ明示化されない信念、態度、価値観
- ② 安全性を達成するために組織が持つべき構造、実行、制御、政策

表-1 組織の安全文化の形態

組織の安全文化の形態	説明
Pathological (病的)	自分が関与しなければ関係ない。
Reactive (事後対応的)	安全は重要ですよ。事故がある度に沢山対策をしています。
Calculative (計算的)	あらゆるハザードを管理するシステムはございます。
Proactive (事前対応的)	我々はいつも見出す問題点に一生懸命取り組んでいます。
Generative (創造的)	安全が達成することは難しいことをよく認識しています。システムが失敗しうる新しいパスとそれへの対応策を考えるブレインストーミングをいつもしています。

P. Hudson は組織の安全文化には表 1 のような 5 段階があるとしている[3]。表中の Generative な組織が最も理想的で、システムの安全を脅かす問題の発生はすべてを予見することはできないと認識して、常にうまずたゆまず問題点の発見とその対応策を学習して、決して自己満足に陥らない。

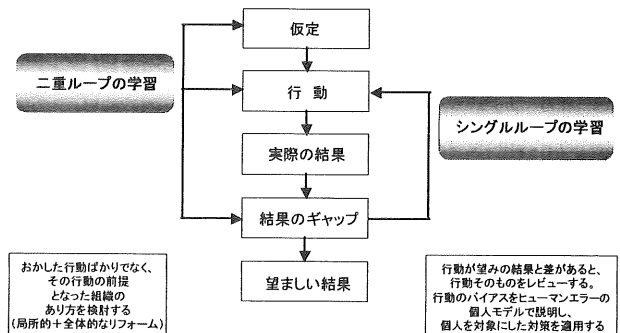


図-2 組織の学習の2つのタイプ—シングルループと二重ループ

P. Hudson はまた組織の学習を、図 2 のようにシングルループと二重ループの 2 つのタイプに分類している。シングルループの学習では行動が望みの結果と差があると、行動そのものをレビュー

する。そして行動のバイアスをヒューマンエラーの個人モデルで説明し、個人を対象にした対策の適用に留めるが、二重ループの学習では、個人が犯した行動への局所的対策ばかりでなく、その行動の前提となった組織のあり方を検討する。すなわち「常に学習する安全文化を創造する」には二重ループの学習が求められる。

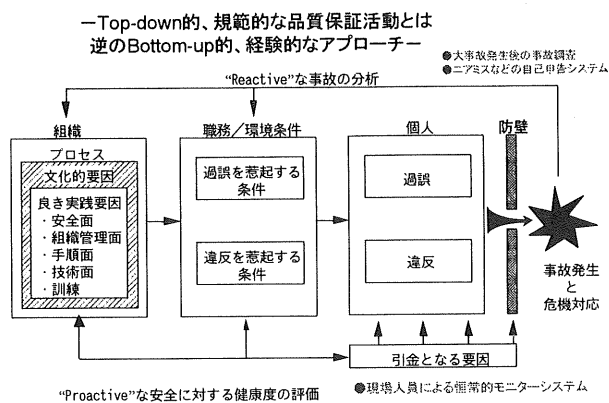


図-3 エラー管理への組織論的アプローチ

英国の労働安全の権威である J. Reason は、組織の安全文化の実践活動を工学化する方法論として、図3に示すようなエラー管理への組織論的アプローチを推奨している[4]。すなわち大事故発生後の事故調査やニアミスなどの申告システムを主体とする“Reactive”な事故の分析ばかりでなく、現場をよく知っている人達から安全上の問題の改善提案を求めるモニタリングシステムの導入など、Proactiveな安全に対する健康度の日常的な評価活動を行うエラー管理システムを提唱している。これはトップダウン的、規範的で文書化を重視する ISO9000 のような品質保証活動とは逆のボトムアップの経験的なアプローチである。安全情報を収集分析し、そこから得た教訓を組織に広く流布するために IT を活かした報告システムを導入すると“安全文化の工学化”が達成される。組織の集合知を活かし学習する文化、Generativeな安全文化を創出する最大の前提は、「公正な文化」と「報告する文化」を如何に組織に根付かせるかに掛かっており、これにはトップマネジメントの積極的関与が求められる。

3. 組織事故のモデルとメンテナンスのヒューマンエラー管理

3.1 組織事故の因果のパス

組織事故の因果は、図4のように組織から作業の場へとつながっていく。組織のプロセスには、(1)立案、予測、設計、管理、伝達、予算、監視、監査等の意思決定と、(2)これらの全体過程にまたがる組織の風土、文化、があり、これらが組織事故につながる負の要因を構成している。因果のパスの上流で創出された潜在条件は、部門的、組織的ルートを経て各々の作業場に伝達され、例えば高い作業負荷、時間圧力、不十分なスキルや経験、貧弱な装置、となってエラーと違反を助長する条件として表出される。作業の場の局所的な条件は、個々の技術者、技能工のレベルでの心理的エラーや違反の傾向と結びついて「不安全な行為」を創出する。不安全な行為は沢山犯される。しかし、沢山の防護壁のために悪い結果として表出することは稀である。しかし、防護システムとしての工学的安全設備、基準、規制、手順等は、組織のプロセスと防護と結びつける「潜在的な失敗の道筋」によって「システムの失敗」を活性化しうる。

組織的事故の要因をモデル化する

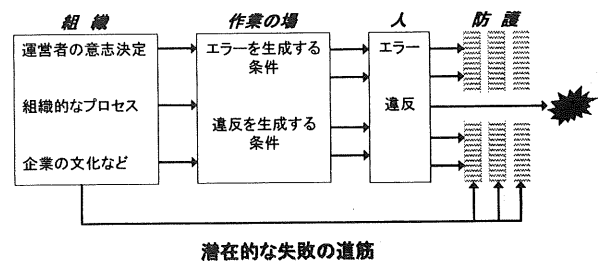


図-4 組織的事故のモデル化

3.2 Sharp End (人間とシステムのインタフェース)の人々への見方を変える

Sharp End の人は「事故を先導する人」ではない。むしろ、システム的要因によって作業の場で「待ち受ける事故」を「引き受ける人」である。彼等の作業する職場環境のシステム上の問題によって、Sharp End の人々は、無意識にわなにかげられる。

3.3 多重防護への見方を変える

人ないし技術システムの単一故障には、多重防護のシステムは有効である。しかし、問題は単一故障以外の複合故障である。複合故障で様々なコ

ントロール、防護、安全措置の多重防護システムをくぐり抜ける唯一の事故タイプは組織的事故である。これはシステムの多くの異なったレベルでの複数個の要因間の考えられないような組合せが関係している。

3.4 ヒューマンエラーへの多重防護

ヒューマンエラーへの多重防護には次の2つの機能がある。

① エラーの検知

予見されなかったエラーを明るみに出すために設計された手順的防護策としての機能のチェックと独立監査がある。しかし、双方とも誤まりやすい人の実行に依存するから、手順はいつも脆弱である。

② エラーの影響へのシステムの耐力を増す。

検知されなかったエラーの影響を contain するよう防護策である。

3.5 メンテナンス組織のエラー管理対策

メンテナンスは主として集団作業で行われ、関与する組織が多い。そこで用いられるエラー管理対策には、要員の選抜、訓練／再訓練職務計画、ジョブカード、タグとリマインダー、シフト交代制、職務許可システム、人材管理、免許と認証、チェックとサインオフ、技術および品質監査、手順、マニュアル、ルール、規制、規律・規範、トータル品質管理、と多岐にわたる。エラー管理の原則で最も大事なところは、この20年余に進んだヒューマンエラーの理論を活用するところにあるが、そのエラー管理には次の13の基本原則を銘記すべきである。

- ① エラーは本質的に悪いものでない
- ② 人の条件は変えられないが、人の働く条件は変えられる。
- ③ 最も優れた人が最悪の誤りをおかす。
- ④ 人は犯そうとっていないエラーをそう簡単に避けることができない。
- ⑤ エラーは結果で原因でない。
- ⑥ ヒューマンエラーは普遍的で不可避である。
- ⑦ 同じパターンのエラーが再発する。
- ⑧ 安全上重要なエラーはシステムのあらゆるレベルで生じる。
- ⑨ エラーの管理は「管理できることを管理する」がポイント。
- ⑩ エラーの管理は「よい人を優れた人に変える」。

- ⑪ 唯一の最善の道というものはない。
- ⑫ 効果的なエラー管理はその場その時限りの手当てで終るものでなく、耐えざる改善を目指す。
- ⑬ 「エラー管理を管理する」ことはエラー管理の過程の最も挑戦的で困難な部分である。

4. 2つのリスクコミュニケーション

リスクコミュニケーションは、「個人、機関、集団間での情報や意見のやり取りの相互作用的過程」[5]、「(あるリスク問題に関して) 関係者の参加・参画を進展させながら、リスクの理解とそれへの対処の行動について双方向の交流を進めること」[6]と定義される。このようなリスクコミュニケーションは一般には図5のように描くことができる。

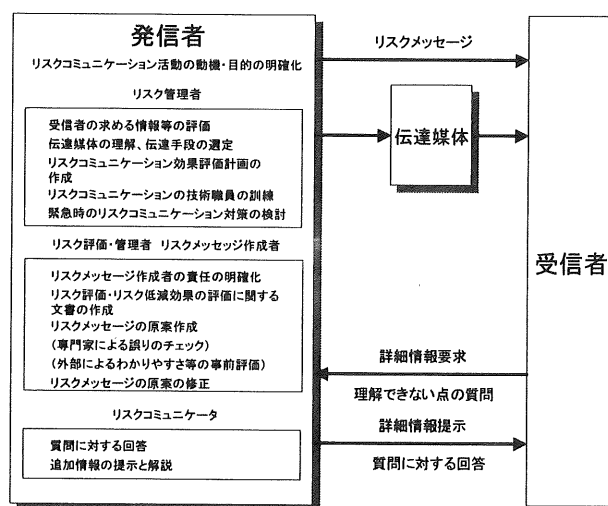


図-5 リスクコミュニケーションの一般的構図

社会的に影響が大きい産業システムのリスクコミュニケーションでは、図6に示すように、産業システムの組織内部での技術的リスクコミュニケーションと、組織外部への公衆リスクコミュニケーションの二つがある。技術的リスクコミュニケーションの目的は、リスク発生の防止またはリスク低減にあり、公衆リスクコミュニケーションではリスクの受容である。公衆リスクコミュニケーションは、社会心理学の分野で研究が進んできた。例えば木下富雄氏は、リスク情報の発信者から受け手へ技術のよい点ばかりを宣伝する従来の説得型コミュニケーションより、リスク情報の送り手は技術のよい点も悪い点も公正に受

け手に伝えて、送り手と受け手と一緒に考える双方向の共考型リスクコミュニケーションの方が社会の信頼を得やすい。しかし、肝心の産業システムが事故ばかり起こしているようでは幾ら共考型リスクコミュニケーションでも効果はないとも述べている[7]。

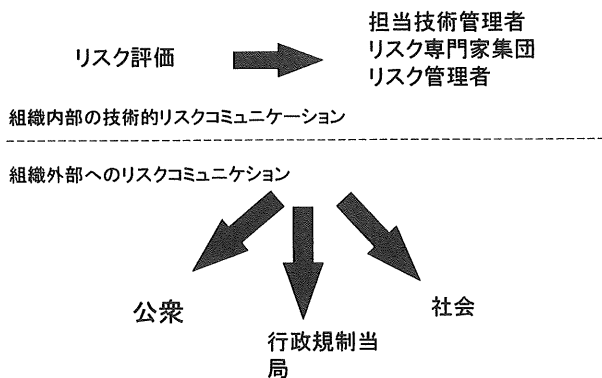


図-6 産業システムの2つのリスクコミュニケーション

技術的リスクコミュニケーションは、管理従事者、設計、製作、保守、運転等の技術者に対するコミュニケーションに焦点を当てるものだが、公衆に対するリスクコミュニケーションほど取り組まれてこなかった。しかし過去のもんじゅ事故といい、JCO事故といい、いずれも設計技術者、現場作業者に技術的なリスク情報が伝達されていなかったことが根本にあった。このことから組織内部の技術的リスクコミュニケーションの方が先決である。このような技術的リスクコミュニケーションの目標は次のようなリスク認知、リスク理解、リスク制御活動の促進である。

(1) リスク認知

リスク認知とは、産業システムのリスク環境を知ること、産業システムのリスク制御の必要性を知ることである。具体的には、リスクに関する動機付け（リスクにかかわる賞罰、リスク削減報奨金等）、リスクに関する連絡（リスクに関する所内ニュース、コンピュータ情報の発信、リスクに関するポスター、リスク小冊子の発行など）、リスクに対する親密度向上（リスク訓練、リスク講義、リスクブリーフィング、リスク管理ツールの活用など）、重要リスクの警告（リスク警告の張り出し、リスクのラベル化とタグ化）などへの取り組みである。

(2) リスク理解

リスク理解とは、産業システムの工学的なリスク情報を理解することである。具体的には、リスク概要の理解（リスク評価結果の階層化、層的リスクサマリー）、リスク状況の理解（リスクコンフィギュレーションマトリクス、リスクモニタ、手順ガイダンス）、リスク内容の理解（リスクテキストブック、階層的リスク情報パッケージ）などへの取り組みである。

(3) リスク制御活動

リスク発生に関わる仕事の効率化によりリスクを制御することである。具体的には、リスク作業ガイド（リスク管理ガイドライン、リスク管理手順書）、リスク作業モニタ（リスクに基づく保安上の規程、リスクの優先順位づけ、リスクワークダウン）への取り組みである。

組織内部の技術的リスクコミュニケーションで提供される多様なリスク情報を図7に示した。要するに、ここで述べた技術的リスクコミュニケーションは、2.に述べた「常に学習する安全文化」を創造する取り組みの一つの具体的なイメージを与えるものである。

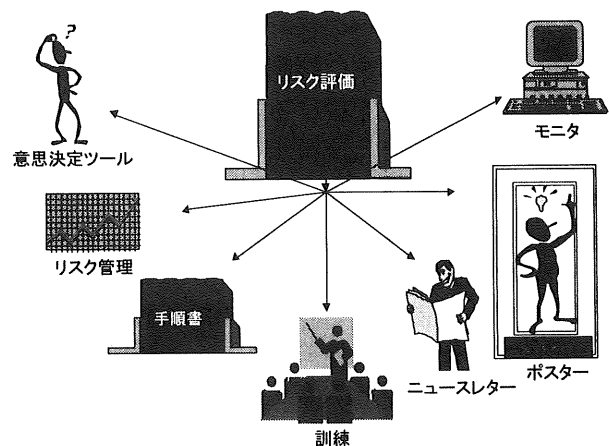


図-7 リスク情報の様々な使用形態

5. わが国の原子力発電への提言

5.1 事業構造について

わが国の電力会では社の原子力発電の保修体制としてメーカ、電力双方の協力会社による重層構造化した作業体制、地元対策を兼ねた人海戦略による過剰な保守作業を特徴としているようだが、日本原子力産業会議によれば、今後の社会趨

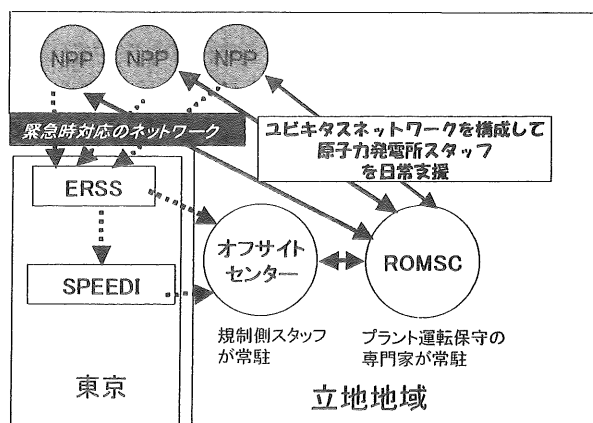
勢からとくに保修関係で以下の問題が指摘されている[8]。

- ① 技術技能の伝承の仕組みづくりとレベル維持
- ② 人数の確保
- ③ 工事方法の合理化・省力化
- ④ 人材の共通活用
- ⑤ 地元活性化への貢献

そして以下の具体的方策を提言している。

- ① 原子力保修技術者の民間資格制度の確立・・・保修技能者の数とレベルの確保、安定的確保のために民間資格制度を設立する。資格化する技能の種類、必要とするレベル、認定方法、資格の有効範囲などを検討する場を設ける。
- ② 多層構造の緩和・・・現場問題の発掘、技術力向上、管理スタッフ削減のため、直営率の増大を図る。直営部門の業務量の年間平準化、経済性維持のため、社内あるいは事業者間のアライアンスを検討する。
- ③ 年間工事量の削減と平準化・・・アライアンスの実施、状態監視保全、リスクベースメンテナンスの導入、停止中の検査工事の運転中への移行により年間工事量の削減を行う。また規制の高度化について技術的検討の場を設ける。
- ④ 管理手続き、運営ルールの見直し、統一化・・・各サイトで異なる管理手続き、運営ルールの統一、簡素化による実質作業時間の合理化、アライアンスの容易化を志向して各社間での検討の場を設ける。
- ⑤ プロセスの改善・・・保修等の発電所の維持管理上の様々な作業プロセスの各社の実績評価、比較、差の分析、成果の共用のために米国 NEI のプロセス管理などを参考に検討する。
- ⑥ エンジニアリングセンター構想・・・以上の(1)から(5)の提言を実効ならしめる方法としてエンジニアリングセンタの設置を検討する。アライアンス実施の中核として、保修技術者、技能者の配置運用管理、作業ルール、マニュアル、放射線管理等の統一化、民間資格の技能者等の登録、サイト間活用を行う。

上記の原子力産業会議基盤強化委員会のエンジニアリングセンターの構想は、筆者が日本保全学会誌に寄稿したオフサイト運転保守支援センターの構想[9]とも合致する。原子力防災と保全管理の強化という現今の社会の要請する、原子力安全への安心に応える道としての、オフサイト運転保守支援センターの構想を図8に示す。原子力災害時に防災活動に関与する機関は、事故発生した原子力発電所の立地地域におけるオフサイトセンターと、東京に設けられる原子力災害対策本部であり、事故発生した原子力発電所からはプラントの事故パラメタが緊急時対応のネットワークを経由して災害対策本部に伝送され、ここではERSSと称する緊急時対応支援システムを用いてリアルタイムで事故状況を理解し、把握するとともに将来の事故進展予測を行って、プラント周辺に放射能放出が予測された場合にはその発生前に放出量予測値をSPEEDIと称する環境被曝予測システムにインプットして発電所周辺の被曝程度を予測する。これらのシステムの予測結果は災害対策本部および現地のオフサイトセンターに伝送されて、住民退避を含めた防災活動の立案に用いられる。



SPEEDI: 環境被曝予測システム
 ERSS: 緊急時対応支援システム
 ROMSC: オフサイト運転保守支援センター
 NPP: 原子力発電所

図-8 オフサイト運転保守支援センターの構想

オフサイトセンターは万一の原子力災害に備えるものであり、社会的安心のための代償とも言える高価な保険料である。また、このような事態の発生はそもそもあってはならない。そこで、オフサイトセンターは整備されている現実を踏

まえ、これを原子力の安全と安心を日常的に支える機関と位置づけて、図8中のROMSCとしてオフサイト運転保守支援センターの導入を構想した。

オフサイト運転保守支援センターの構想の主要な特徴は、以下のとおりである。

- ① 高度な運転保守技術の研究開発、運転保守に関わる民間基準策定、シビアアクシデント対策、運転経験の分析、ヒューマンファクター分析、安全文化醸成活動等の中核センターとする。
- ② マンマシンシステム専門家、ヒューマンファクター専門家を含めた高度な技術者を集中させて、緊急時対応とプラント保守に関わるリスク管理技術能力の維持向上をはかる。
- ③ 規制側のオフサイトセンターと隣接設置して、防災専門家、運転管理官、地方自治体スタッフ等と日常的に連携を深める。
- ④ 電力会社、原子力メーカによる合弁会社か、政府、自治体の支援を得たPFI方式の事業形態で運営する。

このようなオフサイト運転保守支援センターの事業には、上述のエンジニアリングセンターの機能以外に、表2に示すような研究開発が挙げられる。

表-2 オフサイト運転保守支援センターの業務

領域	業務
運転領域	中央制御室運転員への多様な日常的運転モードへのOJT支援 (起動停止、出力上昇、計画停止時の原子炉監視など)
	シビアアクシデント時のオフサイトセンターへのスイッチ以前の収束操作支援(オフサイトセンターとの協同作業による)
保守領域	日常のISI(供用時点検)への状態監視保全技術のR&D
	原子炉コンポーネントの欠陥検査技術のR&D
運転・保守共通	高放射線領域の日常点検・定期保守作業用ロボット技術の開発
	人的要因・組織要因の向上に関わる運営管理法の工場

5.2 組織事故への事後対策と事前対策について

Reasonによれば、組織事故のエラー事象の生じる3つの要因(原因となる要因、それらが相互作用を生じるタイミング、その結果)の偶発的発生は根絶できないが、その原因となる要因を見出して除去すること、その結果を軽減する防護を改善するための組織的な対策は可能とし、エラー発

生に耐性のある組織にするには、事前対策、事後対策の2つの段階で「安全情報システム」の導入が有効としている。そして、「事後の結果への対策」(Reactive)と「事前のプロセスへの対策」(Proactive)は表3に示すように相互に補足しあって作業場と組織のエラーを引起す要因の同定と防護(バリアと保障措置)のギャップの発見に効果的に役立つとしている。

表-3 事後対策と事前対策の双方の協働

	事後の結果への対策 (Reactive)	事前のプロセスへの対策 (Proactive)
作業場所と組織的要因	多くの事象の解析から単一の事象では見分けられない原因と結果のパタンの再発が明白になる	システムの”バイタルサイン“の定期的サンプリングによって最も修正を要する事項が明らかになり、システムの適合性、耐性向上につながる
防護、障壁、安全措置	各々の事象はメンテナンスシステムの多くの防護層の部分的でないし完全な貫通を示している	定常的なチェックはどこに防護上の弱点が現在あるのか将来どこで出現する恐れがあるのか明らかにする

事前対策では、実際の現場で働くさまざまな組織、職種の作業員から幾人かある程度の長期間にわたってモニターに任命し、MESH(工学的安全性の健康度管理システム)と称する情報システムに、作業場の状況、手順、用具、仕事の管理など問題点気がつくたびに自由に入力してもらうというもので、その収録データを統計分析して重要な問題点の事前抽出に役立てるというものである。また、事後対策は、いわゆるヒヤリハット事故データのルートコースを分析するもので、MEDA(メンテナンスエラー検出ガイド)という情報システムがある。

また、Reasonはそもそも安全文化の最も高度に進んだ組織は、信頼性 ということばで規定される性質を備えているだけでは不十分で、将来どんな不測の事態が生じてもそれに柔軟に適應して乗り切ることが求められるとして、これを 組織の耐性 ということばで代表させている。そして組織の耐性を高めるには、次の3つのCが必要と述べている。

- ① Commitment: ビジネス圧力の増大に直面し、トップマネジメントは効果的にエラー管理と安全管理を実行する意志がある。
- ② Cognizance: マネージャは“安全戦争”の

性質、とくに人間と組織的要因について理解している。

- ③ Competence : 安全とエラー管理のツールが理解され、その目的に十分であり、適切に利用されている。

そして、3つのCに基く組織の耐性の評価法として次のようなチェックリスト法の導入を例示している。

- ① HPAC (Human Performance Awareness checklist) 3つのCについてそれぞれ10個ずつ、合計30の質問の各問に自分の組織が該当するかどうかを Yes (+1)、No (-1)、don't know (0) で答えるものである。
- ② CAIR (Checklist for Assessing Institutional Resilience) 組織にどの程度エラー耐性があるかをマネージメントの4つのP (Philosophy, Politics, Procedure, Practice) で明らかとする。

旧 NUPEC ヒューマンファクタセンターでは、SCEST と称する安全文化評価支援ツールを開発している[10]。これは組織の安全文化の程度を、安全確保のための仕組み(体制、手段、活動)、

要員の安全態度・安全行動、および 組織の安全態度・安全行動の共有性、の3点からチェックリスト方式で評価するものである。とくに は規制当局(具体的には保安検査官)の使用を想定している。保安検査に安全文化の外部監査システムが導入される可能性を指摘しておきたい。

5.3 韓国における原子力発電の安全性能指標について

表-4 韓国における原子力発電所の安全性能指標

安全性能評価領域	分類	指標
原子炉安全性	運転安全性	計画外炉停止率 計画外出力低下率
	多重防護	燃料信頼性 原子炉冷却材漏洩 格納容器信頼性 緊急対応準備度
	安全システム	安全注入系利用可能性 非常用ディーゼル利用可能性 補助給水系利用可能性
放射線被曝安全性	敷地内	従業員集団被曝線量
	敷地外	公衆/環境被曝線量

最近、韓国では科学技術省および原子力安全研究院が、表4のような各種の原子力発電所の安全

性能指標をWEBで公開している[11]。最近、電事連で取り込まれている原子力発電安全情報公開ライブラリ「ニューシア」ではこのような日本版安全性能指標を公開することも期待される。

6. 結びと将来展望

公共性が大きく、事故や災害発生時の社会的影響の大きい科学技術システムの安全と安心を高めるには、科学技術システムの運営、管理、実務、作業に携わる人々が一体となって安全を支え、不断に「安全文化」を醸成する活動が重要である。本稿ではその具体的な取り組みの工学的方法論の一端を紹介したが、その定量的な評価、指標化にリスク概念の導入によるリスクベースのシステム安全管理への発展を期待したい。また組織の安全文化醸成活動の取り組みを社会に発信し、社会の反応を効果的に組織内部の安全文化醸成にフィードバックする仕組みが「社会の安心の確保」に繋がると期待している。

参考文献

- [1] 原子力安全委員会ウラン加工工場臨界事故調査委員会：「ウラン加工工場臨界事故調査委員会報告」、1999年12月24日。
- [2] International Nuclear Safety Advisory Group (INSAG) 1991: Safety Culture (Safety Series No.75-INSAG-4), International Atomic Energy Agency(IAEA).
- [3] P. Hudson: Aviation Safety Culture, (Leiden: Centre for Safety Science, Leiden University, 2002).
- [4] J. Reason: Managing the Risk of Organizational Accidents, (Aldershot: Ashgate, 1997).
- [5] National Research Council, Improving Risk Communication (1989).
- [6] 日本リスク研究学会：リスク学事典，(2000)。
- [7] 木下富雄：リスクコミュニケーション：思想と技術、エネルギーレビュー、24-2, pp.6-10, 2004.
- [8] 日本原子力産業会議：基盤強化委員会 人材問題小委員会 報告書 平成15年6月。
- [9] 吉川 榮和、大井 忠：オフサイト運転保守支援センター—その構想と課題—、保全学、Vol.3, No.1, pp.70-74, 2004.
- [10] 原子力発電技術機構：安全文化の理解と評価のための手引き(改訂版) 2004年4月。
- [11] Young S. Eun: Development of Nuclear Power and Safety Regulation in Korea, Korea Institute of Nuclear Safety, 原子力学会関西支部講演会(エネルギー・環境—海外事情) 平成16年3月5日。