MOT 勉強会レポート第 10 回

「大規模工学的インフラ・システムのリスクマネジメント」

1. はじめに

「MOT 勉強会」2016 年の 10 回目は、12 月 15 日(木)夜 7 時より、中央区京橋区民館にて開催された。

事前に主催者から届いた案内では、「3.11 震災以降クローズアップされてきた、原子力発電所、水力発電所／ダム、宇宙航行システム等に代表される、大規模工学的インフラ・システムの事故リスクを中心としたリスク評価手法とリスクマネジメントの考え方を紹介し、今後日本に求められるリスクマネジメントの意味について考える。」とあり、一般人が普段なかなか目にすることのない大規模システムの内側に迫る内容をお聞きすることができた。

講師の多田浩之氏は、1984 年より 2016 年 8 月までみずほ情報総研株式会社(旧株式会社富士総合研究所)に勤務された後、現職の公益財団法人・未来工学研究所。
専門領域は、

- ・リスクアセスメント/リスクマネジメント(工学・社会工学)
- ・危機管理
- ・欧米の科学技術戦略

と多岐にわたる。

2. 講演概要

講演は、スクリーン上のパワーポイントに沿って行われた。パワーポイントの内容は、事前に配布されたレジュメとほぼ同じで、40 数ページに及ぶ膨大な内容であった。

レジメ目次は、以下のとおり。

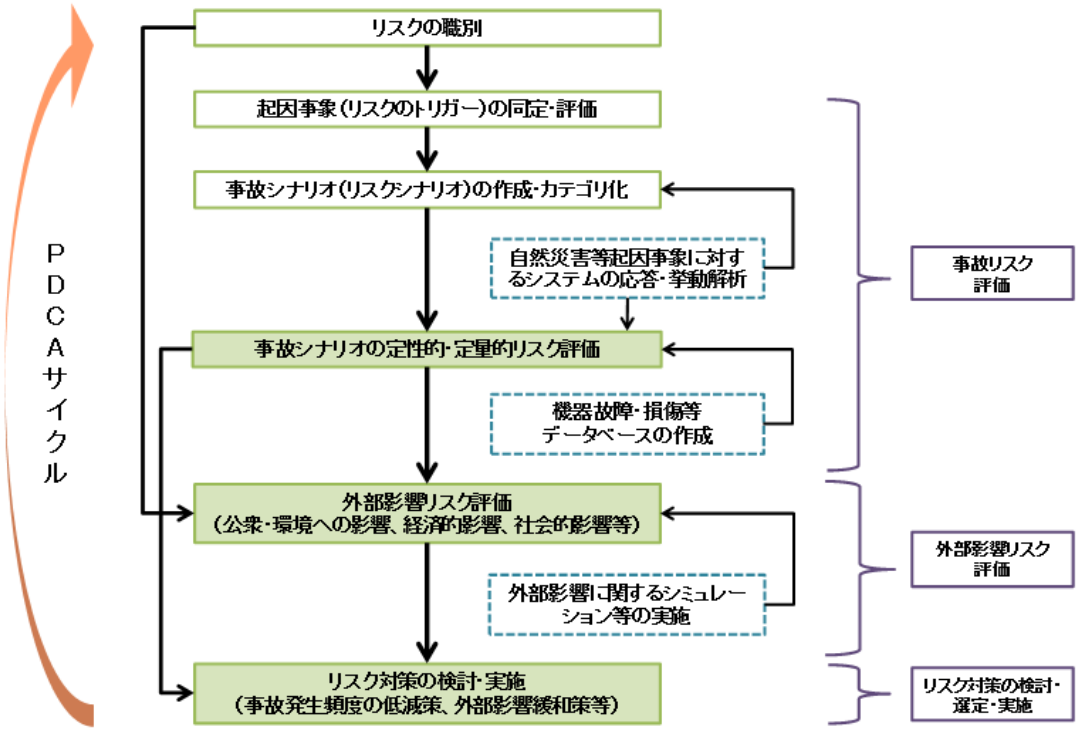
2-1 リスクとリスクマネジメントの定義

リスクマネジメントにおけるリスクおよびリスクマネジメントについては、ISO3100 で定義されている。
それによれば、リスクは「目的に対する不確かさの影響」と定義され、リスクマネジメントは「リスクについて、組織を指揮統制するための調整された活動」と定義される。
日本では、リスクマネジメントの定義を狭義にとらえる傾向にあり、かつリスクよりも安全性に重きを置く傾向にあったが、東日本大震災・311 以降は、リスクはリスクとして認めようとする姿勢に大きく変わった。

2-2 事故等リスクマネジメントの流れ

事故等リスクは、
(1) システム・組織に内在するリスク
(2) (1)が外部に影響を与えるリスク(影響リスク)
の二つに大別して検討する。
リスク対策については、(1)の発生頻度を削減し、(2)の被害等を緩和・低減する、という二つの観点から検討する。
これら検討の流れを、事故等リスクのフレームワークとして、フローチャートにすると次ページの図のようになる。

「インフラ大規模工学システムを対象としたリスクマネジメントの概略の流れ」
(巻末資料 1　参照)



図から見てわかるように、事故等リスク評価の流れは、リスクの発見に始まって「システム・組織に内在するリスク評価」・「影響評価」・「リスク対策の評価」と三つの評価ステップに分かれている。

これらの評価ステップは、一回で終わるのではなく、PDCA サイクルを回しながら繰り返し行い、その評価結果を DB に蓄積し続けることが大切である。

2-3 事故等リスクの領域分類と領域別許容基準

事故等リスクマネジメントの手法は広範な分野で適用されるが、事故等リスクの内容から見ると、原子力発電・ダムなどのエネルギー産業インフラから、化学関係・食品関係などの企業単位など対象領域である程度層別できる。

事故等リスクの評価にあたっては、リスク毎の許容基準が必要になる。

許容基準は、リスク評価の対象となる領域によって異なるが、事故が多くの人命にかかわる原子力発電所事故やダム損傷・決壊事故などでは、その頻度は年に 10 のマイナス 4 乗以下に設定されていたりする。

2-4 システム・組織に内在するリスクの評価

(1)主なリスク評価手法（PRA）

システム・組織に内在する事故等リスクの評価を行うにあたって、その中心となる手法が確率論的リスク評価(Probabilistic Risk Analysis:PRA)である。また、その簡便法として FMEA(Failure Mode Effect Analysis)などがある。

PRA における主要な解析手法は、イベントツリー解析とフォールトツリー解析であり、それらを組み合わせて一連の評価が実施される。

イベントツリー解析では、ハザード発生からシステムの最終状態に至るイベントの流れを時間軸に沿って展開してリスクシナリオを作成する。
また、フォールトツリー解析では、特に機械・電気系設備が対象となるが、フォールトツリーを作成して、リスクシナリオを展開する。
こうやって展開したリスクシナリオは原子力発電施設のようなものでは、数万という膨大な数になるが、これらは、全てデータベースとして蓄積してリスクマネジメントの関係者が使用できるようにする。
できあがったリスクシナリオを解析して、リスク削減措置を検討する。
リスクシナリオの解析にあたっては、点推定解析、重要度解析、不確実さ解析、感度解析などの技法があり、それら解析の際の計算を手早く行える、アプリケーションが多数公開されている。(フォールトツリー・イベントツリー解析コード)

2-4 影響リスクの評価

影響リスクの定性的・定量的評価にあたっては、別途シミュレーション等により検討・評価する必要がある。
例えば、原子力発電所でのシビアアクシデント後の放射能漏れによる周辺住民への健康被害のシミュレーションなどがこれにあたる。

2-5 事故等リスク解析評価結果の整理のイメージ

主だった整理パターンは、以下の二つ。
・リスクシナリオを発生頻度の高いものから並べて、支配的リスクシナリオを抽出する。
・リスク要因を重要度の高いものから並べて、重要度の高いリスク要因を抽出する。

2-7 事故等リスクの定量化を簡略的に行う場合の手法 (FEMA)

PRA では、イベントツリー作成などを通じて得られた各シナリオは、事故等発生頻度や影響の大きさなどを統計データや工学データなどの分析から得られた数値をパラメータ入力することで定量的に評価されていた。
これに対して、FEMA などのように、パラメータ算定を簡略化して、専門家等の判断に基づいて、事故等発生頻度や影響の大きさをレベル区分した値で代用する、より簡便な方法もある。評価結果の表へのまとめ方として、リスクマトリクスなどがある

2-8 大規模工学的システムを対象とした事故等リスク評価事例

原子力発電所の PRA は、手法の開発は 1975 年に遡るが、実際の導入は 1979 年の TMI 事故などを契機に加速・定着していった。日本では、1986 年のチェルノブイリ事故以来注目が集まりはしたものの、評価システムとしての要件をしっかり満たした本格的な導入は先の大震災の 311 以降である。
日本における原子力発電所の設計は、三菱、日立、東芝の三社が行っているが、各社とも技術ノウハウが外に漏れることを嫌って、いずれも各社の系列や繋がりの深いシンクタンクなどが評価機関を担当している。

2-9 事故等リスクマネジメントの哲学

欧米と日本では、システムやヒューマンエラーに対する哲学が根本的に異なる。欧米は、人間は間違いを犯すものという性悪説に立ってシステムを設計する。
　日本では、大規模事故や人的ミス(過失)を許さない、あってはならないという哲学のもとにシステムを設計する。

　リスクマネジメントの考え方については、日本よりも欧米の方がより客観的・冷徹に考え抜いているという点で優れているように見える。例えば、我が国で原子力発電所事故の許容基準が設定されたのが、先の大震災の 311 以降であったというエピソードなどからもうかがえる。

　一方で、自主保全を例にあげると、欧米では設置者側での自主保全を義務付けているのに対し、日本ではそのような義務付けはなく規制側が関与することが多い。欧米では自主保全の要件を満たせば大規模事故が起きた時に免責を得やすいといった危うさもある。

3. 質疑応答

(1) リスク対策の効果はどのように測定するか?

重要度指標などの計算式をよく使う。

※参考: 重要度指標の例と計算式。

・Fussell Vesely(ファッセル・ベズレイ)重要度
・Criticality 重要度
・Risk Achievement Worth (RAW) ～リスク増加価値
・Risk Reduction Worth (RRW) ～ リスク低減価値
など

(2) 過去のデータが無い場合のリスク評価はどのようにするか?

ジェネリックデータ(民生品などの一般的なデータ)から類推する方法と、新しく作られた機能部品・製品から得たデータを反映させる方法などがある。

(3) リスク(特に原子力発電所)は、場所や気象で異なるか?

異なる。例えば自然災害でも地震が評価に入るのと入らないのでは大きく違ってくる。

(4) 戦争などカントリーリスクは、同じ手法で評価できるか?

わからない。

(5) シナリオ作成はどのようにして着想を得るのか? 想像力によるものか、それとも科学的に詰めて行って作成できものなのか?

・対象となるシステムの性能や機能に熟知している必要がある。
・ハザードの設定が最も難しい。
・地震など実験施設もあるが金がかかる。
・ヒューマンエラーや、特に空間的インターフェースを介して起きる事故など想像しづらいものもある。

(6) 火星探査など未知の領域に挑むとき、NASA はリスクマネジメントをどのように考えていたのか?

・火星探査のことは判らないが、宇宙ステーションなど宇宙開発では「人が乗っている」ということが重要である。

「人の命を預かっている」のだから、全くわからないことでも想定しておく。そして想定したことを全部ドキュメントとしてシナリオに残しておく。新たに判ったことがあればそれをシナリオに織り込むという PDCA を繰り返すことが大切である。
日本は、この PDCA の繰り返しをやらない。一回ぽっきりであることが多い。

(7)「品質管理」では、確率の低いものについては起こりえないと判断してしまうが、こういった考え方が日本のリスクマネジメントに悪影響を及ぼしていないか?

・「人の命」にかかわるところは、(事故が起きることを前提に)最後の手段を残すべきである。

・日本では、失敗が許されないという考えが強すぎて、完成度を追い求めすぎる。

・宇宙開発では、「うまくいかない時の訓練」や「リカバリーバックアップ」といった視点が大切である。
日本人には「有人宇宙船」は打ち上げられないと感ずる所以である。

(8)「考えられないものも残す」ことがやはり大切か?

米国では、ブレーンストーミング(で出てきた想定シナリオ)を全て残しておき、それが DB になっている。
原子力発電など、日本にはそのような DB がない。アメリカのものを使っている。

4. 所感

(1) 理科系的なアプローチと文科系的なアプローチの違いを実感

BCM など企業リスクマネジメントについては知っているという方も多いかと思うが、それらが講師の言われるように、文科系的アプローチのリスクマネジメントであるとすると、今回のテーマである「大規模工学的インフラ・システムのリスクマネジメント」が、定性的・定量的のいずれの評価手法においても、極めて工学的知見を駆使した理科系的な手法であるということを実感できた。

(2) リスクマネジメントに向き合う欧米と日本との違い

違いの由来を、人間の犯すミスに対する「性悪説」と「性善説」でかたづけられない問題であると感じた。

確率論的リスク評価(Probabilistic Risk Analysis：PRA)の ‘Risk’を’Safe’と読み替えたり、「失敗」や「不良」といった語をネガティブ表現と受け取って極端に嫌う日本人の体質に根差すもので、日本人がこれからも世界と伍してイノベーションの分野でリードしていくためには、克服すべき課題であると、改めて感じ入った。

(3)「未知なるもの」「無知の領域」に向き合う楽しさ、新たな発見の鍵?

講演を聞く前は、「リスクマネジメント」というだけで、後ろ向きの議論のように感じていたが、それは筆者の思い込みであったと反省した。

聞き終わってみると、「未知なるもの」「無知の領域」に対処する新たな技術イノベーションを生み出すきっかけを作ってくれる、エキサイティングな仕組みになるのではと感じた。

参考文献

資料 1. 「エネルギー・環境インフラ・システムのリスクマネジメントと危機管理の哲学」

2016 年 1 月 28 日 環境エネルギー第 1 部　多田 浩之

https://www.mizuho-ir.co.jp/publication/column/2016/kankyo0128.html

(監修 加藤美治、執筆 石垣純)