新連載

あの事故はなぜ起きたのか!!

第1回

安全ライフサイクルの考え方

田辺 安雄

連載第1回，安全に関するマネジメント規格「IEC 61508」について説明する．漠然と「安全なものを作りたい」と考えるのではなく，安全な製品を作るための取り組み方について知っておけば，普段，顔を見ることのない部署の技術者とも連携して取り組めるようになるだろう．（編集部）

普段，利用している身近な場所での痛ましい事故に心を痛めることが多くありませんか．事故が起きると，管理会社はメーカの責任だといい，メーカは管理会社の責任だといい主張が食い違う場合があります．「責任のなすり合いをしている場合か」と，多くの方が感じていると思います．

筆者は，英国の安全の規制機関であるHSE（Health and Safety Executive；健康安全庁）の方と，このような問題について話したことがあります．「自分だけが良くて，ほかの人はどうでもよいという風土はイギリスにはない」と言われたことが印象的でした．

IEC 61508[1]は，製品そのものの安全規格であるような印象を持たれがちです．実際は英国における安全確保の考え方が基になった，安全に関するマネジメント規格です．安全の確保は，リスクに基づいて設計されたシステムや部品の性能だけに依存するものではありません．運用，保守にかかわるさまざまな立場の企業の取り組みにも関係します．従って，安全を確保するためには，これらを網羅する仕組みが必要です．IEC 61508では，**図1**に示す安全ライフサイクルという業務工程を定義し，マネジメントの枠組みを規定しています．全安全ライフサイクルは，安全装置の概念，設計，保守，改修，廃却に至る16フェーズからなります．つまり，ゆりかごから墓場まで，安全装置の面倒を，大切に見るという考え方です．

IEC 61508は，全安全ライフサイクルに沿って構成されているといっても過言ではありません．16のフェーズのそれぞれのフェーズについて解説することは，次回以降に譲ります．今回は，このような仕組みが作られた経緯を中心に，安全ライフサイクルについて解説します．

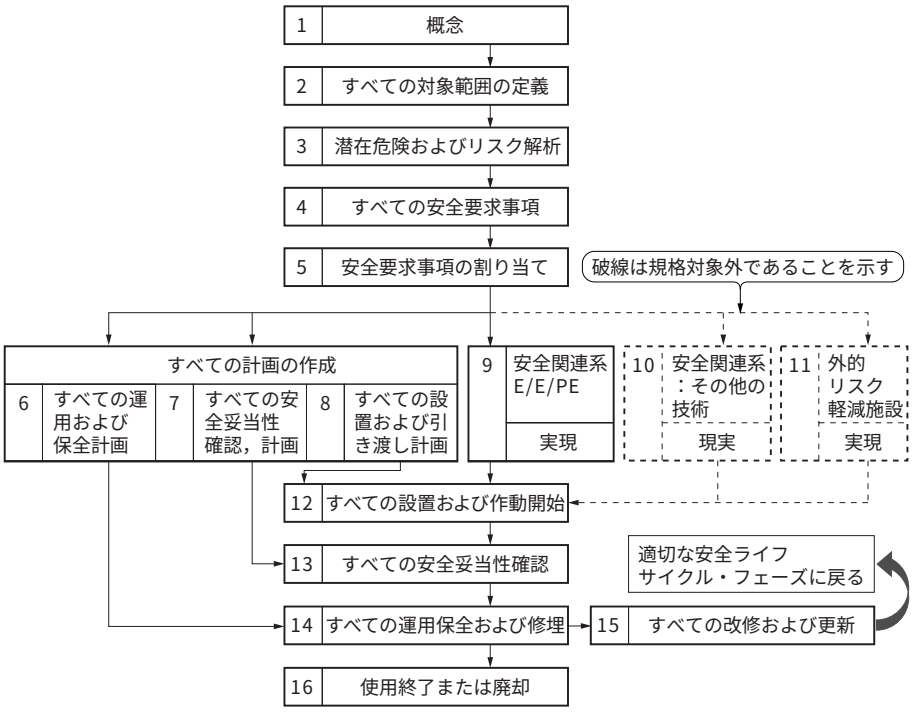
● 事故の分析から誕生

この安全ライフサイクルとは，どのような意図をもって導入されたものでしょうか．英国ではかつて，国内で発生した34の事故を，発生した活動のフェーズに着目して分析したことがありました．関心のある方は，HSEのOut of Control[2]を参照してください．しかし，分析された事故は，必ずしもIEC 61508の主要な対象である制御系や安全系の故障に起因したものではありませんでした．また，事故が発生した産業もさまざまでした．

事故の原因となった発生フェーズの分布を**図2**に示します．ここで，フェーズは，安全要求仕様，設計と実装，設置と引き渡し，運用と保守，引き渡し後の変更に関係するものとして分けています．また，**図2**は，どのフェーズが多いか少ないかを示したものではありません．なぜなら，調査した事故も34の事例しかなく，統計的な処理をするには不十分だからです．

しかし，この調査結果は，いくつかの重要な示唆を含んでいます．それを以下に示します．

Keyword HSE，IEC 61508，安全ライフサイクル，ソフトウェア・エラー，コンピュータ・エラー，フォールト・アボイダンス，フォールト・トレランス



フェーズ1；概念（の把握）
対象システムの環境と関連法規等を理解し，ハザード（潜在危険）や規制情報を把握します．

フェーズ2；すべての対象範囲の定義
対象システムと制御系の境界を定め，潜在危険分析およびリスク分析の範囲を定義します．

フェーズ3；潜在危険およびリスク分析
対象システムと制御系に対し，すべての運転モードで生じる潜在危険の分析およびリスク分析を行います．

フェーズ4；すべての安全要求事項
E/E/PE 安全関連系，他技術安全関連系，外的リスク軽減施設に対して，安全機能要求事項および安全度水準（SIL: Safety Integrity Level）要求値を，安全要求仕様書として作成します．

フェーズ5；安全要求事項の割り当て
安全機能要求事項および SIL 要求値を，E/E/PE 安全関連系，他技術安全関連系，外的リスク軽減施設に対して割り当てます．

フェーズ6；すべての運用および保全計画
E/E/PE 安全関連系の運用保全計画を作成します．

フェーズ7；すべての安全妥当性確認計画
E/E/PE 安全関連系のすべての安全妥当性確認を実施するための計画を作成します．

フェーズ8；すべての設置および引き渡し計画
E/E/PE 安全関連系の設置計画および引き渡し（作動開始）計画を作成します．

フェーズ9；E/P/PE 安全関連系実現
E/E/PE 安全関連系の安全機能要求事項と SIL 要求値に適合する E/E/PE 安全関連系を設計・製造します．なお，フェーズ9の実現フェーズは，E/E/PES 安全関連系のハードウェアに対する安全ライフサイクルと，ソフトウェアに対する安全ライフサイクルから構成されています．

フェーズ10；その他の技術安全関連系実現
本規格の対象外

フェーズ11；外的リスク軽減施設
本規格の対象外

フェーズ12；すべての設置および引き渡し
E/E/PE 安全関連系の設置および引き渡しを行います．

フェーズ13；すべての安全妥当性確認
E/E/PE 安全関連系が，すべての安全機能要求事項および SIL 要求値を定めた安全要求仕様に適合して妥当であることを確認します．

フェーズ14；すべての運用保全および修理
要求される安全機能を維持するように，E/E/PE 安全関連系を運用，保全および修理します．

フェーズ15；すべての部分改修および改造
E/E/PE 安全関連系の機能安全が，部分改修時や改造時，また，その後も維持されるようにします．

フェーズ16；使用終了または廃却
E/E/PE 安全関連系の安全機能が，対象システムの使用終了時や廃却中，また，その後の環境で適切であるようにします．

図1
IEC 61508 で定める全安全ライフサイクル
ゆりかごから墓場まで，安全装置の面倒を，大切に見るという考えに基づく．