8．鉄道の安全関連国際規格への対応と規格適合性認証について

鉄道認証室　　※田代 維史

1．はじめに

我が国の鉄道に関する技術標準としては、国の「鉄道に関する技術基準」、JIS（日本工業規格）、鉄道関連の各種団体規格などがあり、これらが国内における鉄道全体をカバーしてきた。各種鉄道製品のこれら標準への適合性に関しては、先ずメーカー自身が製品の技術文書中で規格準拠を宣言し、製品を受領する鉄道事業者自らが製品受入れの妥当性判断を行う仕組みとなっている。

一方、近年の海外市場ではこの仕組みが日本国内と異なっている。図１の例の様に海外では、工業規格が存在する製品の場合、規格適合性評価に基づく第三者認証が受入れ条件として重視され、特に鉄道運行の安全に直接関わる製品の場合、この条件は必須とされる。このように海外鉄道市場では安全関連規格に関する認証取得が重要性を増しており、欧州鉄道メーカーは欧州域内の認証機関から認証を取得し、世界市場への製品拡販を図っている。一方国内鉄道メーカーは、上述の仕組みから日本に鉄道製品の認証機関が存在しなかったため、海外市場における応札資格条件、あるいは納入後の稼働判断条件に規格適合性認証が求められた場合、海外の認証機関に認証を依頼してきた。

しかし海外の認証機関を利用すると、鉄道安全に関わる日欧の設計思想の違いの克服、外国語での対応、地理的制約等によって、膨大な手間とコストがかかると言われている。なおかつ、安全関連規格群は製品安全性の技術的仕様の妥当性と併せて、その仕様の達成プロセスの妥当性を求めるため、規格適合性説明文書の体系が我が国の上述の妥当性判断の仕組みに対応した技術文書の体系と大きく異なっており、国内メーカーは新たな技術文書体系を構築する必要に迫られている。

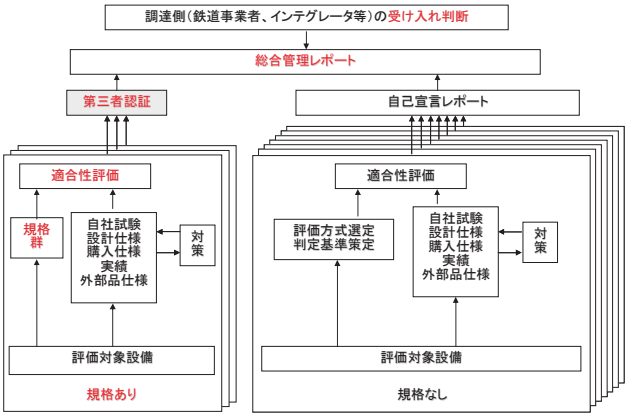

図１　海外鉄道プロジェクトの製品受入の仕組み例

このような背景のもと、交通安全環境研究所では認証機関を立ち上げ活動を開始した。

本稿では、安全関連規格の歴史、構造と特徴、説明文書の構成を述べ、交通安全環境研究所鉄道認証室の認証機関としての活動を述べる。

2．歴史的経緯

日本の鉄道は、ダイヤ乱れの少なさや鉄道設備の信頼性の高さにおいて世界最高水準にあるが、鉄道技術の国際標準化と規格適合性認証では欧米がリードしている。

欧州では、18 世紀から民間主体で認証事業が開始され、20 世紀後半の欧州統合に合わせて域内規格の統一が図られた。一方、米国では第二次世界大戦後、軍事・宇宙分野で信頼性マネジメント技術が進展し、アポロ計画などの成果が得られた。この技術と欧州で生まれた設計安全性の概念が融合した結果、鉄道分野では 1990 年代に、R : 信頼性、A : アベイラビリティ、M : 保守性、S : 安全性からなる RAMS 性能とその達成プロセスのマネジメントを要求する通称 RAMS 規格と呼ばれる欧州規格 EN 50126 が開発され、世界標準の IEC 62278 となった。

図２に安全マネジメント規格と、関係する機関群の構図を示す。安全マネジメント規格は、製品開発着手の冒頭で、目標とする SIL（Safety Integrity Level：安全性のレベル）を宣言させ、次に SIL を達成できたマネジメントの証拠（文書や立会い監査）を要求し、その証拠の妥当性の判断を中立・公平な第三者に委ねることを要求する。かつ、第三者性は SIL に応じて高くなる様に規定されている。この仕掛けにより、いわゆるフェイルセーフが要求される鉄道信号の様な設備の場合、外部の認証機関からの認証を取得せざるを得ない状況が作られている。安全マネジメント規格には、鉄道のような特定産業分野を対象とするものと、分野横断的なものがあるが、いずれのものもこれまで欧州の標準化団体 CEN（欧州標準化委員会）と CENELEC（欧州電気標準化委員会）が開発と管理を行ってきた。かつ、規格を適用される製品の計画・設計・製造等の各段階で関わるシステムインテグレータやコンサルタント、認証機関や試験機関もまた欧州勢が主導権を握っている。

以上の結果、安全関連規格の開発、規格対応コンサルタントから規格適合性認証まで一貫して欧州勢が主導権を持つ構図が生まれた。

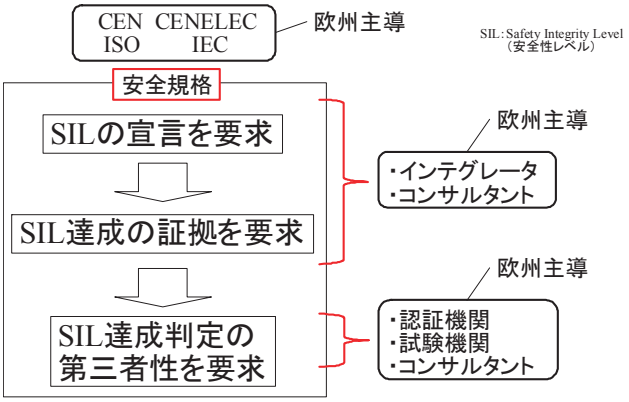

図２　安全関連規格と関連機関の構図

３．RAMS 規格の特徴

一般に規格には、特定製品の技術仕様を定め、その達成を要求するものと、目標達成業務のプロセスマネジメントを要求するものがある。RAMS 規格の特徴はこれらの要求を一体化したことと、鉄道製品の種別を限定しないことである。すなわちこの規格は、任意に選定された鉄道製品に関して、技術的 RAMS 仕様を定め達成することと、達成プロセスマネジメントの妥当性証明文書の作成を要求する（図３）。また達成プロセスは、図４に示すように製品の構想段階から、

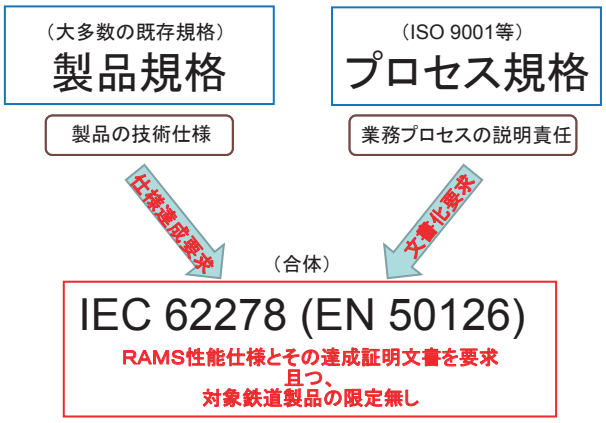

図３　RAMS 規格の要求

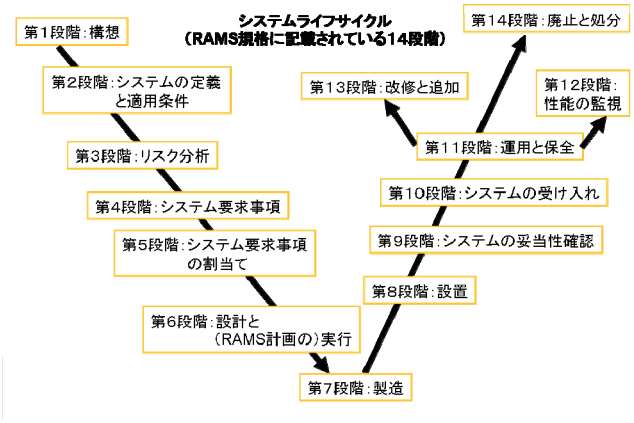

図４　システムライフサイクル

設計、製造、使用、廃棄までの全ライフサイクル段階をカバーしなければならず、メーカーは製品の RAMS 性能達成のための活動（RAMS Activity）を各段階において規定し、実行の証拠を文書で説明しなければならない。各段階における活動とは、先ずその段階において達成されるべき要求事項を規定し、前段階からのインプット（解析結果、試験検証の結果、参考情報等）が揃っていることを確認し、要求事項を実現する業務を実行し、その結果が妥当であることの「検証」を行い、次段階へのアウトプット（次の段階へのインプット）を行うことである。

ここでいう「検証」を一般通念としてみれば、次段階に対する問題の有無を確かめることであるが、RAMS 規格はさらに念入りな検証を求める。あたかもデータ通信プロトコルの階層構造と同じ様に、14 の RAMS ライフサイクル段階を上位層、中位層、下位層に分類する。通信プロトコルでいえば、例えばデータ通信を行う２台のコンピュータに組み込まれたプロトコルの各階層は、相手方の同位階層とは相互に

通信が完全に出来なければならないが、これに類似してRAMS規格では、ライフサイクル第2段階（適用範囲の定義）と第10段階（受入れ）を上位階層の組と考え、第2段階で定義した仕様が満足されているか否かを第10段階で検証することを求める。中位層では第5段階（安全要求の配分）と第9段階（機能と安全性の検証）、下位層では第6段階（設計）と、第7段階（製造）のうちの出荷検査がそれぞれ検証すべき組となる。RAMS規格では次段階へのアウトプットの検証をVerification、同階層内の組同士の検証をValidationと呼んで区別し、かつ、両方の検証を合わせてV & V（Verification and Validation）という呼称を用いることで、検証漏れは許さないという姿勢を強調している。

4．RAMS文書

一般にマネジメント規格では、製品の機能・性能の規定、製品化過程の状況記録、修正管理、および要求事項との整合の検証を、技術的および管理上の各側面から文書化し管理することをConfiguration managementと呼ぶ。RAMS規格の運用においてConfiguration managementに対応する文書はRAMS文書と通称される。規格原文中のRAMS support documentationやSystem support documentationがこれに相当するが、どのような体系の文書を作成すればよいのかをRAMS規格自体は記述していない。RAMS規格には単に、適切なConfiguration managementが達成されるべき、という記載しかない。

そこで参考となるのはIEC 61508とEN 50129（IEC 62425の原案）である。前者は産業分野を問わずE/E/PES（Electric/Electronic/Programmable Electronic System；電気・電子・プログラマブル電子システム）製品の安全性マネジメント規格であり、後者は鉄道において保安レベル（いわゆるフェイルセーフ）の安全に関係する電子装置の安全性マネジメント規格である。これら2つの規格は共にRAMS性能のうちS＝安全性に重点をおいているが、RAMS規格対応の文書体系に関する実用的例を提供している。

前者はその参考付属文書に、安全性ライフサイクルの全体をカバーする文書構造と、E/E/PESおよびソフトウェアの安全性に関して記述することが望ましい情報の事例を詳細にリストアップしている。また文書の実体については、数種類の文書のセットであり、個々の文書のタイトルの具体例を掲げている。文書セットには、対象製品のライフサイクルの全ての局面をカバーする完全セットのほか、規格を運用するユーザの立場（設計、製造、検証、保守・保全、運用）に応じたセットがあり得ることや、文書の分類の仕方は対象製品のシステム規模の大小に応じて選択してよいことを記載している。後者はさらに踏み込んで、強制力のある規格本文中に、より具体的に文書の構成を提示している。

以上2つの規格はRAM性能に関する要求事項を明示的に掲げてはいないが、例えばS＝安全性を、マルコフ状態遷移図を用いた危険側故障率計算により数値的に評価する場合、R＝信頼性とM＝保守性の数値が、安全性と相関を持つことが示される。その際、A＝アベイラビリティも同時に算出される。この様にこれら2つの規格の対象である安全性は、もともとRAM性能とも密接に結びついている。そのため、RAMS文書の体系としてこれらの規格の例を参照することには合理性があるといえる。

図5にRAMS文書の構成例を示す。この例では、文書全体の名称をRAMS Reportとし、その下に7種類の文書を配列している。このうち主要な2つの文書、Quality Management ReportとTechnical RAMS Reportについて、それらの内部の文書の構成例を図示した。

RAMS文書の規格のユーザにとって最大の問題は各文書の内容の記載方が判りにくいことである。この主要な原因の一つは、ライフサイクルの段階毎に要求される様々なRAMS Activityと、図5の様な実体文書個々の内容を結びつける記述方に関するガイダンスが明示されていないことである。これに関しては、文書毎に全てのRAMSライフサイクル段階が含まれていると考えるべきである。すなわち図5に示す各文書は、個々のライフサイクル段階において、ユーザがその文書のタイトルに応じて行った活動（計画、設計、レビュー、製造、検査、品質マネジメント等）を記載するということである。

もう一つの主要な原因は、従来作成してきた技術文書（設計図書、検査報告等）とRAMS文書の構成が異なり、同一事項でも各文書に記載しなければならず、かつ、図5のRAMS Report中のTraceability reportの作成への対応を行わなければならないことである。RAMS規格が要求するTraceabilityの基本

は、ライフサイクルの第 1 段階から第 5 段階の間に発生した要求事項が後のライフサイクル段階での検証事項と完全にリンクされていることを記述することである。上述の様に RAMS 文書体系では、同じ事項を複数の文書に記載することが生じるため、一つの事項に関してトレースすべきリンクが複数必要となる。さらに RAMS 規格は、ライフサイクルのある段階で RAMS 性能達成上の不具合が発覚した場合、その原因を最初に作り込んだ段階に戻って対策すること（フィードバック）、およびその顛末をすべて記録することを要求する。一般的に、ライフサイクル第 7 段階（製造）において仕様項目数が最大に達し、その後の段階では検証事項としてまとめられるため、リンク数が減じてゆく。複雑なシステム製品の場合、このリンクを管理する Traceability report 文書は巨大なものとなる。さらに、ライフサイクルの n+1 番目の段階へ後段からのフィードバックすなわち不具合対策のための仕様変更が求められたとする。この変更が複数の文書において新たな事項を生じ、あるいは既存の事項への変更も生じ、ライフサイクルの後段へも波及してゆく。そのため、特に複数チームが開発に参加する規模の製品の場合、トレーサビリティの管理は困難を極める。従ってトレーサビリティに関しては、有効で、かつ、管理可能な記録方法の工夫が必要である。

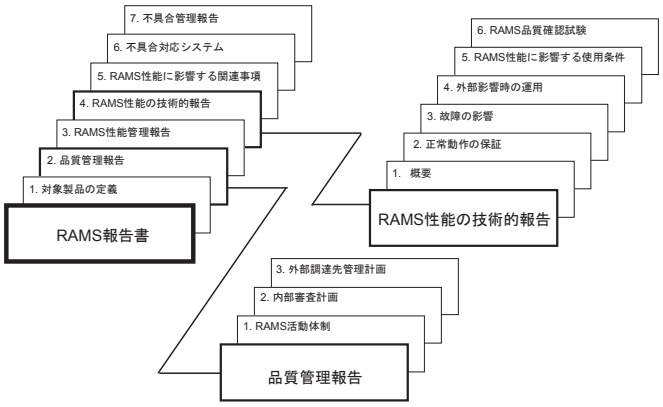

図 5　RAMS 文書体系例

5．交通安全環境研究所における規格適合性認証活動

このように海外市場向けの、安全関連規格への適合性説明文書の作成にはかなりの労力を必要とし、かつ、第 1 章に述べた様に、認証取得のための困難な条件があるため、これらの解決が強く望まれていた。

そのため、平成 20 年 6 月 19 日の交通政策審議会陸上交通分科会鉄道部会の提言を受け、国土交通省鉄道局、鉄道総合技術研究所を事務局とする鉄道技術標準化調査検討会において平成 22 年 3 月、「鉄道認証機関設立検討ワーキンググループ」が設置され、交通安全環境研究所を予定認証機関として対応の検討が行われた。その結果に基づき平成 23 年 4 月、交通安全環境研究所鉄道認証室が開設された。認証対象規格は上記「ワーキンググループ」によって選定された、海外でニーズの高い 5 規格（表 1）である。これらのうち、信号用安全関連電子装置に関する IEC 62425（通称、セーフティケース規格）に関して平成 24 年 9 月 6 日、交通安全環境研究所鉄道認証室は独立行政法人製品評価技術基盤機構（NITE）認定センターより鉄道分野の製品認証機関として認定を取得した。認定後これまでに、この規格を適用した信号関連製品に対し 5 件の認証書を交付している。

表 1　認証対象規格と認定取得規格

No.	IEC規格番号（原案の欧州規格）	規格の概要	
1	IEC 62278（EN 50126）	対象製品種別を限定せず、対象鉄道製品のR（信頼性）、A（アベイラビリティ）、M（保守性）、S（安全）に関する目標の設定、目標達成の証拠と達成プロセスの証拠の提示をライフサイクルの各段階毎に要求	
2	IEC 62425（EN50129）	IEC 62278の考え方をベースに、安全に関係する鉄道用の装置、システムの安全性証明手続きを詳細に規定	← 2012年9月認定取得
3	IEC 62279（EN 50128）	安全に関係する鉄道用のソフトウェアの、要求される保安度に応じて開発条件を規定	
4	IEC 62280-1, 2（EN50159-1, 2）	安全に関係する鉄道用のデータ伝送に関するシステム構成、手順を規定。IEC 62280-1は閉鎖通信系、IEC 62280-2は開放通信系が対象	
5	IEC 62236-1～5（EN 50121-1～5 ）	鉄道向けEMC（電磁両立性）規格	

今後は他の 4 規格についての認定取得を目指すと共に、交通安全環境研究所鉄道認証室の開設時に適用した、認証機関が準拠すべき規準である ISO/IEC Guide65 が昨年、ISO/IEC 17065 として国際規格となり、併せてその内容が改訂されているため、これに適合する認証業務体系への移行を進める予定である。

6．まとめ

安全関連規格の歴史、構造と特徴、説明文書の構成を述べ、交通研鉄道認証室の認証機関活動について紹介した。

交通安全環境研究所では、公正・中立の立場から国際規格適合性認証を実施することを通じて、日本の鉄道システムの海外展開や鉄道技術の維持・発展に貢献していきたいと考えており、当研究所の認証システムをご活用頂ければ幸いである。引き続き関係各位の御指導、ご支援をお願いしたい。