鉄道のセキュリティと安全性

―無線を活用した列車制御におけるセキュリティと安全―

森　崇　矢田部 俊介（西日本旅客鉄道（株）鉄道本部技術開発部）

背景

近年，列車の安全に対する要求は，今までの「列車を衝突追突させない」，「列車を脱線させない」というだけではなく，気象状況や踏切の状況により列車を安全に保つことや，保守作業を安全に行うこと，また踏切をより安全にすること（保安度の向上）や踏切の警報が鳴る時間を適正にし，鳴り過ぎないようにすること（警報時分の適正化）が求められている．西日本旅客鉄道（以下，JR 西日本）の中期経営計画においても，「鉄道オペレーションのシステムチェンジ」が述べられ，より高い安全性を目指すことが明らかにされている．

列車の安全を常に保つということは，列車運行中，いついかなる時でも列車速度を制御する機能が必要条件である．この事項を実現するため，先行列車の位置や設定された進路，進路中の障害事象を集約し，その情報をもとに個別列車が制御を行うことが考えられる．

これは 1960 年代から ATC（Automatic Train Control）として実現されているが，レールに制限速度を指示する信号を流し，それを列車が受信し，指示された速度を超えるとブレーキをかけるというシステムであった（**図 -1**）．しかしこのシステムには問題点があった．まず，機器室からケーブルを通しレールまでの配線が必要で，地上システムが複雑になる．次に，速度制限信号が固定であり，ブレーキ性能の一番悪い列車に合わせて信号を設定するため，列車の減速が必要以上に早期に行われる例が多かった．そのため早期に強いブレーキがかかり，運転間隔が広がった．また，早すぎるブレーキにより乗り心地も悪くなった．

この事象を解決するため，階段状ではなく，連続的に速度を制御する「パターン式」の ATC が 1990 年代から実用化されたが，レールを用いた伝送という点は，同一であった（**図 -2**）．

近年，無線技術の進展により，レールによる伝送ではなく，無線による双方向伝送を情報伝送の手段として活用する事例が増えてきた．これによると，レール伝送から無線伝送となるため，レールに装置を取り付けるのではなく，レールから離れたところから伝送できるようになり，その結果工事の容易化と保守の安全性が図られる．また，レール伝送による ATC と比べ，出力が弱く，機器室におけるシステムの小型化も図ることができる（**図 -3**）．

このように無線による ATC は，世界的に見ても増加傾向にあるが，無線特有の課題である，電波伝搬の安

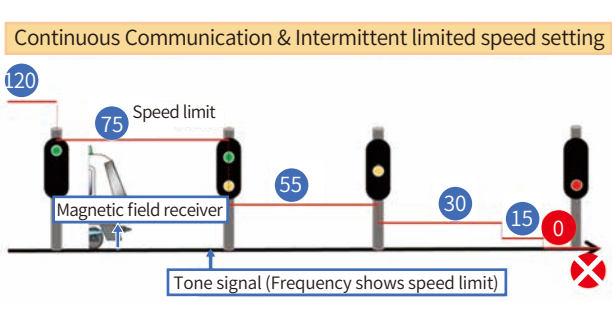

図 -1　レールに速度信号を送信した ATC の例

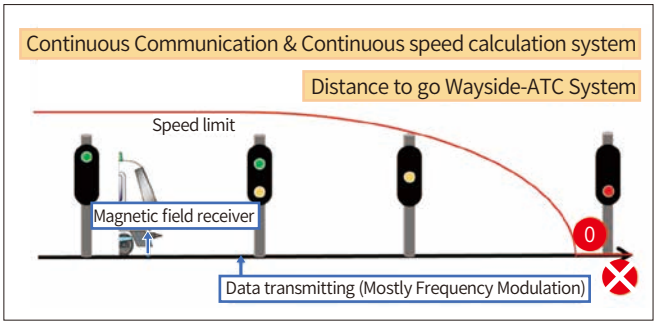

図 -2　パターン式 ATC の例

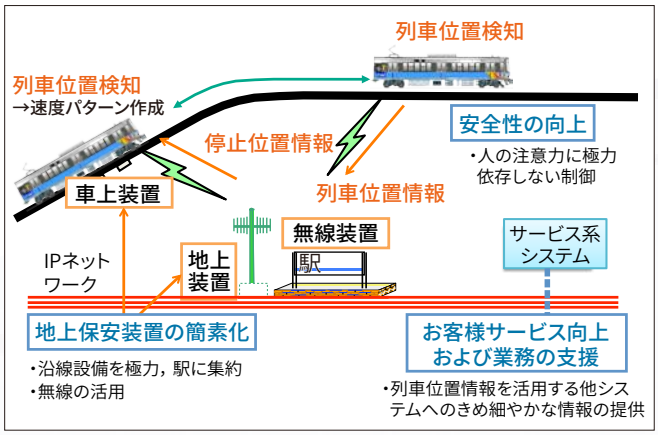

図 -3　JR 西日本における無線を活用した列車制御の目指す事項

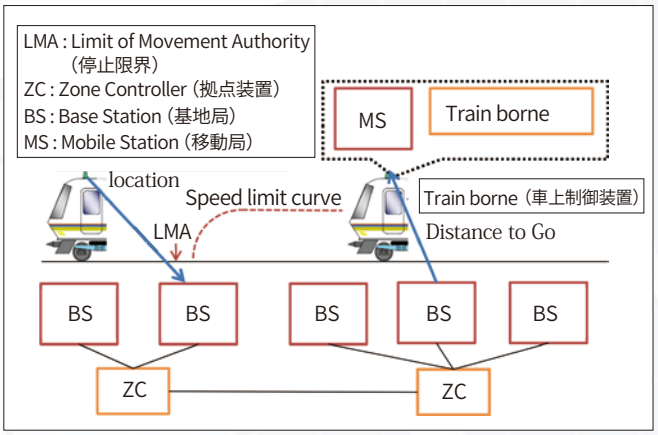

図 -4　無線を活用した列車制御システムの概念図

定性の課題や，セキュリティの課題についてしっかりと取り組む必要がある．また，ATC としての信頼性・稼働率・保守性・安全性（Reliability, Availability, Maintainability and Safety, 以後「RAMS 性」）の高いレベルの維持管理が必要である．これらのことを十分に認識することが必要である．

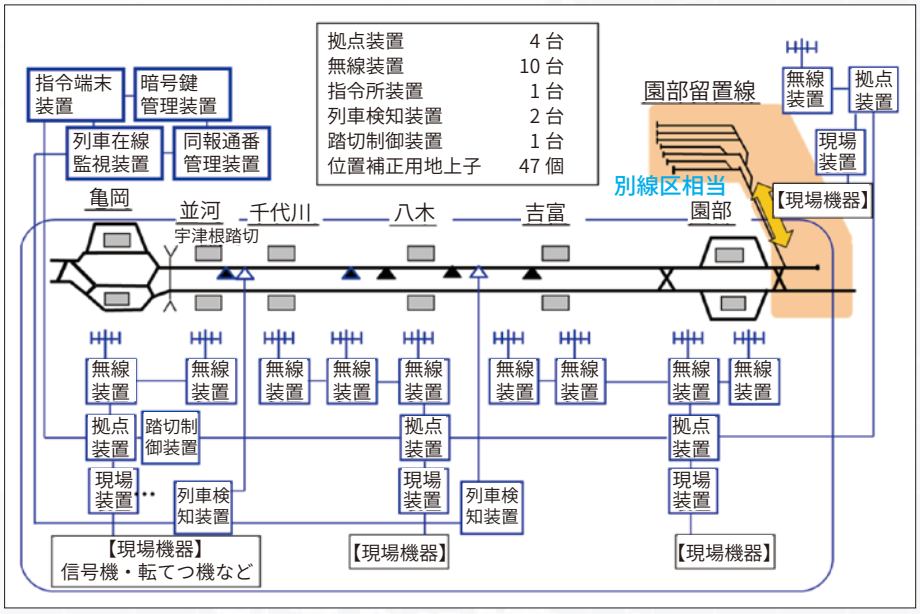

図 -5　システム構成

また，今後の少子高齢化にもとづく労働力の減少のため，人的資源の集中化が必要であり，それに伴って信号システムの統合集中化を行う必要がある．これには集中連動化，集中踏切だけではなく，今存在する各種の安全システムの機能を統合し，その基盤となるシステムの開発を行う必要があり，一部の通信による列車制御システム CBTC（Communication Based Train Control）は，このようなコンセプトを持っているものもある．統合と集中化，共用化も非常な大きなテーマとして鉄道業界では認識されている．

無線を活用した列車制御のシステム概要

無線を活用した列車制御は，一般的に**図 -4** のように構成される．先行する列車は，その「列車位置」を検定し（列車速度より移動距離を推定，ただし等間隔に地上に地上子を置き補正），車上制御装置⇒移動局⇒基地局⇒拠点装置に順に送られる．拠点装置では，線路の開通条件や列車位置から，後続の列車に対して，どこまで進行してよいかの「停止限界」を作成し車上制御装置まで伝達する（図 -4）．

車上制御装置では，「停止限界」と車両の加減速性能，線路条件から速度制限パターンを計算し，その速度制限パターンを超える運転操作は無効にし，ブレーキを自動で出力する．

JR 西日本においては，山陰本線，亀岡～園部の 14km に試験装置を設置し，各種走行試験を行っている．システムの概観を**図 -5**，**6** に示す．

図 -6　試験列車 U@tech と試験室内

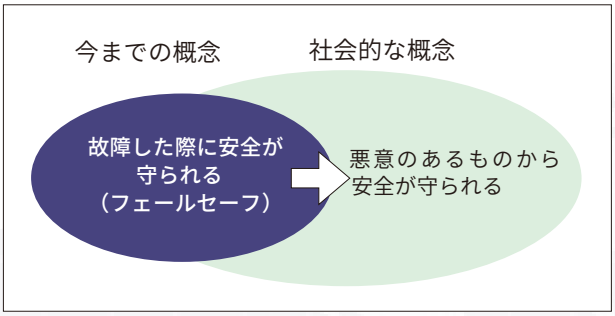

図 -7　安全概念の変化

このような列車制御を実現するためには，ネットワーク装置やプログラム電子システムを多く使用しているため，鉄道で重視されている RAMS 性だけではなく，セキュリティについての考慮が幅広く必要であることは，論を俟たない．

安全の 2 つの概念：セーフティとセキュリティ

安全とは何かというと，一般には「危険な状態から守られていること」を指す場合や，「受け入れられないリスクがないこと」（IEC 61508-4:2010 3.1.11）とされることが多い．このとき，普通は，悪意を持った人間による人為的な攻撃や犯罪行為によるリスクではなく，ランダムな装置故障による偶発的で非人為的な不慮の事故のリスクが考慮される．

これらのことを考えると，鉄道の安全とは，「受け入れることができるリスクレベルを関係者で合意し」，「実際に合意したリスクレベルを下回っている」ことを示すことが求められる．鉄道において，これを実現するためには 2 つのアプローチがある．1 つは，土木構造物やレールのように，ライフサイクル全体で品質を一定以上に保ち，その中でリスクが受け入れ可能なレベルに継続的に押さえこんでいく方法と，いわゆる，「フェールセーフコンセプト」で対処し，装置が故障したときには，列車を止める動作を行うことにより列車の衝突や，脱線を防ぐよう，危険な状態に遷移しないように事前設計しておき，その設計を実装において実現させる方法がある．

鉄道のシステムにおける安全のうち，このような非人為的リスクが受け入れ可能となっている状態を「セーフティ」といってきた．

今までは，このコンセプトは，機器の故障において，安全側に遷移することが必要とされていたが，世の中において，昨今「テロの脅威を防ぎ安全な社会の実現」，「安心安全な IT 社会の実現」などの言葉からは，その範囲を超える安全が必要であるという社会的合意ができつつある（**図 -7**）．社会が高度化し，より安全で快適なサービスが求められるようになると，社会的に受け入れ可能であると合意されるリスクのレベルも下がっていく．このような社会の期待にこたえていかない限り，鉄道事業は社会から退場を迫られることであろう [1)]．

そのなかでも，注目されていることに，「情報セキュリティ」が挙げられる．非人為的な故障や異常に対応する「セーフティ」だけではなく，悪意のある攻撃に対し対策を行う「セキュリティ」を考慮していくことが重要であることは当然であろう．

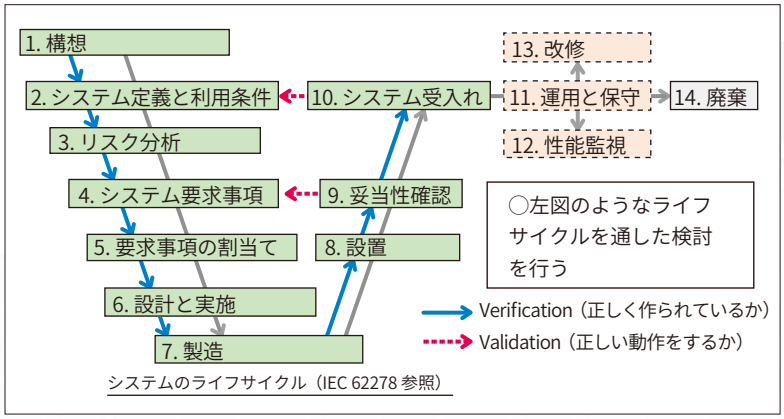

図 -8　RAMS14 段階

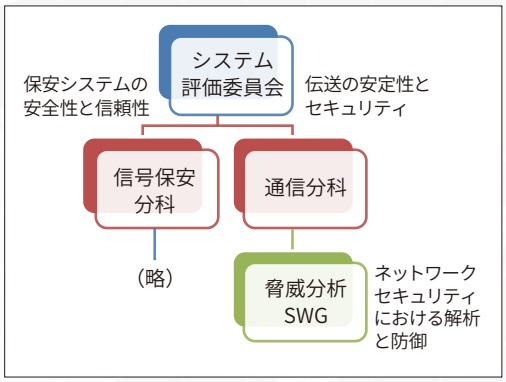

図 -9　システムの妥当性評価を行う体制

安全を守るための管理

システムのコンセプト段階から装置の製造，設置，運用を経て廃棄までを「ライフサイクル」と呼ぶ．鉄道におけるライフサイクル全般において RAMS 性を維持管理するための方法は，国際規格 IEC 62278[2]（以下「RAMS 規格」）に述べられている．

各段階において，R，A，M，S の観点で Verification を行い，そして設置後，Validation を行う V&V モデルとなっている（**図 -8**）☆1．このモデルには，情報セキュリティは含まれていないが，作業を進めていくためには十分に参考になる．

我々は，無線を活用した列車制御を実現するため，このライフサイクル管理を重視し，システムを継続してセキュアに運用できるよう工夫し開発を行っている．

情報セキュリティを守るための仕組みづくり

我々はセキュリティの専門家ではない．情報セキュリティに関して従来は鉄道のコア技術とは思われていなかったため，鉄道事業者側の経験が不足しており，慎重に取り扱う必要があると思われる．したがって，どのようにセキュアな通信を確立していくかは，専門家の知識を活用することが必須である．また利害の関係しない第三者の専門家の意見を活用することは，RAMS 規格の原則であり，またセキュリティだけではなく，システムセーフティや信頼性，稼働率確保の面からも重要である．そのため，まず，システムの妥当性を検討する場として，「システム評価委員会」を立ち上げ，通信分野では，通信のネットワークの安定性と安全性（ビットエラーなど偶発的脅威への対処）[3]，セキュリティ（人為的な脅威への対処）について議論する場を設けた（**図 -9**）．ここは，客観的で率直に議論できる場となるように，JR 西日本の社員のほかに，研究所や大学の有識者，行政機関，通信事業者，システムを製作する会社等に参画していただいた．ここで，本システムの伝送系が担う役割，リスク分析，その対処方法，それらの V&V についての評価を行っている．

列車制御にかかわる通信の情報セキュリティの基本的な方針

システムを構築するにあたり，「通信における基本的な考え方」を定めた．ここでは，「国際規格などを参考にしつつ対策を行うこと」とした．秘匿された暗号方式（暗号アルゴリズムなどを含めた手法一式）でセキュリティを保つという考えもあるが，これまでの前例が教えるところでは，暗号方式を秘匿し続けることは難しい．そのためこの考え方は採用せず，日本[4]および各国の政府関係の団体や国際規格から推奨されている「暗号アルゴリズム」，「ハッシュ関数」，「相互認証方式」，「メッセージ認証符号」を組み合わせて使用することとした．また，鍵の寿命についても考慮することとした．

方式を公開するということは，秘匿するものがなけ

☆1　Validation は，たとえば第 9 段階においては，構成されたシステムが第 4 段階の要求事項を満たしているか，その意味で妥当であるかを検査する．この図の矢印は，システムをどの段階の要求事項に照らして検査するかを表現している．

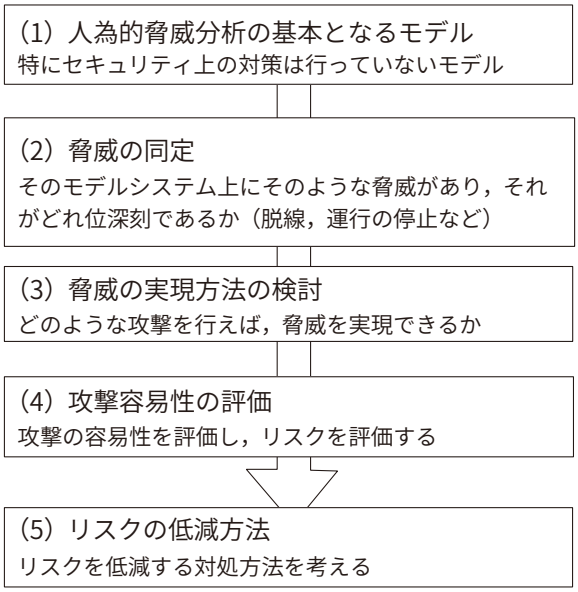

図 -10　人為的脅威分析の流れ

れば，攻撃者から見れば対策は無力でしかない．このため，「鍵管理装置」により暗号鍵の発生，配信，寿命の管理を集中化して中央で厳重に行うこととし，また操作をなるべく自動化することでできるだけ人手に頼らない鍵の生成と配信を行うことにした．

□ リスク分析における脅威の抽出，評価とリスクの低減

リスクを分析するためには悪意ある攻撃の脅威を同定し，その脅威がどのような手法をとれば実現できるのか，攻撃の容易性と被害の深刻度の評価を行い，必要があればその低減手法を検討することになる．

そのために，鉄道において，安全上の脅威である，「列車の異常な加速」，「衝突」と，運用上の脅威である「稼働率の低下」（列車の意図しない停止）を脅威とし，何もセキュリティ上の対策を行っていないシステム上での脅威の実現方法と容易性を検討し，そのリスク低減方策を決定していくという方策を採った[5]（**図 -10**）．

ここで問題となるのは，我々のような鉄道事業者は，攻撃による脅威の実現方法の検討と，その容易性について評価することが非常に困難であるということであった．これには，セキュリティ研究を行っている研究所や大学に支援をいただき，自動車分野で使用されている車載ネットワークのセキュリティ評価手法[6]を参考に，一つひとつの項目についてリスク低減の必要性を検討していった（**図 -11**）．

これらにより，各種攻撃について網羅的に想定し，想定した攻撃に対して対策を決定し，システムの設計，製作，改修を行い，指定された対策が行われているかどうか試験を通し確認する体制を整えている．

情報処理に期待すること

本稿では，無線を活用した列車制御システムとセキュリティのかかわりについて述べたが，もう少し枠を広げて今後の列車制御と情報処理のかかわりについて考えてみる．

列車制御系などのミッションクリティカルな分野での組込みソフトウェアの管理については，安全度水準（Safety Integrity Level）に応じた対応可能な従事者を変えることや，品質の管理体制を変えるということが欧米では一般的に行われている．しかしながら，ソフトウェア開発への従事者の能力の評価が困難であることや，ソフトウェアの動作は複雑であり不具合が起きたときの原因究明が難しいため「こういう基準を

No.	攻撃目的（Attack Goal）	攻撃目的の部分目標（Attack Objective）			攻撃手段（Attack Method）				
1					装置に間違った制御を行わせる攻撃	地上無線装置に偽装し，誤った情報を発信する	偽通信機器から，「地上無線装置からの電文を改竄した信号」を送信する	地上無線装置る	
								速度制限情報成る	
								攻撃となる信	
2							偽通信機器から，「過去に地上無線装置から送信された信号」を送信する	地上無線装置る	
								攻撃となる信	

図 -11　攻撃とその手段の一例

満たしていればこのソフトウェアは不具合を起こさない」という基準（ソフトウェア品質の客観的評価基準）を定めることが難しい．そのため結局 Validation として試験に時間をかけ，品質を確認しているという状況である．ソフトウェア検査の自動化や，仕様書からの Validation リストの自動化など，短時間で品質の確認ができる方策の検討が必要だと考える．

また，無線においても，SDR（Software Defined Radio）や，SDN（Software Defined Network）など，無線を活用した制御システムの通信インフラとして，ソフトウェアで定義された通信装置がこれから大幅に導入されることが予想される．これらを安定的にまたセキュアに使用できるように，これからの情報処理技術について，我々も大きな関心を持って事業運営にあたっていきたい．

参考文献

1) 森　　崇：オープンネットワークと暗号技術（1）―保安装置とセキュリティの技術（1）―，鉄道と電気技術，pp.61-64 (2016).
2) IEC 62278/EN 50126 Railway Applications - The Specification and Demonstration of Reliability, Availability Maintainability and Safety (RAMS).
3) IEC 62280/EN 50159 Railway Applications - Communication, Signalling and Processing Systems – Safety Related Communication in Transmission Systems. IEC.
4) CRYPTREC，http://www.cryptrec.go.jp/（2016 年 3 月 29 日参照）
5) Schneier, B. : Attack Trees : Modeling Security Threats, Dr. Dobb's Journal of Software Tools, 24(12), pp.21-29 (1999).
6) EVITA, Deliverable D2.3: Security Requirements for Automotive on-board Networks based on Dar-side Scenarios.

（2016 年 3 月 29 日受付）

❖森　　崇　takashi-mori@westjr.co.jp

1987 年神戸大学工学部電気工学科卒業，1992 年同大学院工学研究科電子工学専攻修了．同年西日本旅客鉄道（株）入社．2005 年放送大学教養学部社会と経済専攻卒業．現在，西日本旅客鉄道（株）鉄道本部技術開発部列車制御システム PT 担当課長．

❖矢田部俊介　syunsuke-yatabe@westjr.co.jp

2003 年神戸大学大学院自然科学研究科修了（博士（理学））．同年より同大工学部教務補佐員，教務職員，大学院工学研究科助手．2007 年産業技術総合研究所特別研究員，研究員（2 号）．2013 年西日本旅客鉄道（株）入社．現在，鉄道本部技術開発部列車制御システム PT 課員．