［新たなモビリティ時代のサイバーセキュリティ―セキュリティによるジャパン・ブランドの向上に向けて―］

③ 鉄道における列車の運行制御用情報ネットワークとサイバーセキュリティ

応用

川﨑邦弘 鉄道総合技術研究所　祇園昭宏 鉄道総合技術研究所

鉄道と情報ネットワーク

鉄道における情報伝送の始まりと発展

鉄道における通信は，より安全・正確・快適な鉄道運行を実現するために，さまざまな情報を収集・伝達する重要な役割を果たしている．列車を安全に走らせるためには，線路や車両，給電などの設備の状態情報と，列車の走行・停止を指示するための制御情報を伝える必要がある．鉄道システムの中で情報をやりとりする個所は，列車の定時運行を管理・制御する指令を中心として，駅，列車とその乗務員，そして列車を走行させるために必要となる各種の設備（構造物，軌道，給変電，防災，信号保安）など多岐に渡っており，鉄道の情報ネットワークは，これらの鉄道の構成要素間を有機的に結合する神経網である（図 -1）．

我が国の鉄道における通信の歴史は，1872 年に新橋～横浜間において初めて鉄道が開業した際に，3 本の裸線を用いたモールス電信を使用して閉そく運転を行ったことに始まっている．“閉そく”とは，列車同士の間隔を安全に保つために，路線をいくつかに区切る考え方で，1 つの区間には 1 列車のみが存在できることを原則とする運転方式である．鉄道通信は，列車の運転保安にかかわる情報伝送を担うために誕生した．その後，指令員や乗務員，駅員・関係個所などへの情報伝送のための通信網の構築が進み，現在，全国を網羅する通信網や列車無線システムなど，多くの通信設備が活用されている．近年は，情報通信技術の目覚ましい発展に伴い，無線による列車制御や旅客へのブロードバンド通信サービスの提供など，より高度な情報通信技術（ICT）の活用事例が登場してきている．

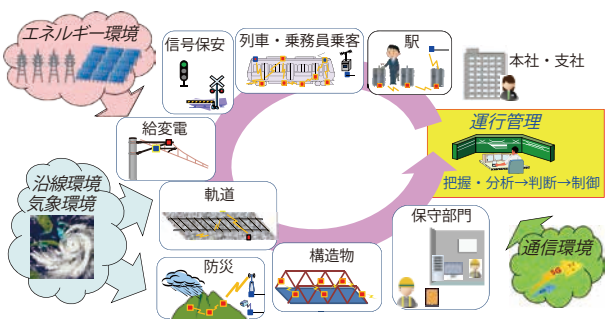
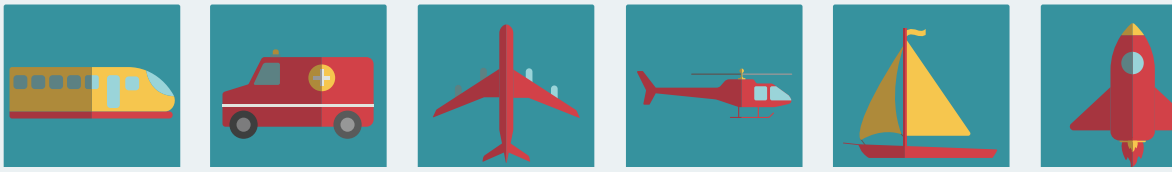


図 -1　鉄道の構成要素と周囲環境とのつながり

情報伝送の形態も時代とともに変化してきている．通信技術が今のように発達する以前は，利用できる通信リソース（伝送速度やチャンネル数）が限られていたこともあり，少ない情報でも安全・安定輸送を実現すべく，鉄道システムを構成する各種の業務分野（運輸・営業，車両，土木，軌道，電力，信号保安，など）ごとに 1 対 1 あるいは 1 対 n の通信システムが導入されてきた．光ネットワークやディジタル無線など通信技術が発展した現在においても踏襲されており，列車の運行にかかわる要員や設備どうしを結ぶ情報ネットワークが業務分野ごとに構成されている．近年，業務分野を超えて情報を共有できるネットワークづくりが始まっており，2020 年代後半には鉄道システムを構成する要員や設備のすべてが情報ネットワークで結ばれることが期待され



ている（図 -2）.

列車の運行制御と情報通信技術

現在の鉄道では，運行管理システムと信号保安システムの 2 つのシステムが列車の安全・安定運行を支えている．運行管理システムはダイヤに基づく列車の定時運行と遅延時の運転整理を担う．信号保安システムは保安制御装置等により，列車の安全確保を担っている．両システムとも，その時代の最先端の情報処理技術や通信技術を活用して列車の運行制御の高度化を進め，人間の負担を軽減することによって，より安全で安心して利用できる鉄道へと発展してきた.

1964 年に開業した東海道新幹線では，先行列車との間隔などから後続列車の速度を決定・指示する地上システムと，指示速度を超過しているときには自動的にその速度以下になるようブレーキを制御する車上装置で構成される自動列車制御装置（ATC）が導入された． ATC では，地上システムが決定した速度指示が列車に伝送され，運転台に表示される車上信号方式が用いられる（したがって地上の信号機が不要となる）．現在は，速度を滑らかに制御するために車上で速度パターンを演算するディジタル方式へと発展し，新幹線や首都圏の在来線で使用されている.

1970 年代からは，コンピュータの小型化・高性能化や，情報ネットワーク技術などの発展に伴い，運行管理や進路の設定（＝線路の分岐・合流個所で線路の方向を切り換える転てつ装置の制御）の自動化が行われ，1977 年には列車走行を自動で制御する自動列車運転装置（ATO）が営業線で実用化された．また，マイコンに適用するフェールセーフ技術の確立により，1985 年に国内で初めてコンピュータが保安制御に適用された．最近ではディジタル移動体通信技術を活用した無線式列車制御システムが 2011 年に営業線に導入されるなど，安全・安心な鉄道を支えるシステムの多くが最新の ICT によって実現されている.

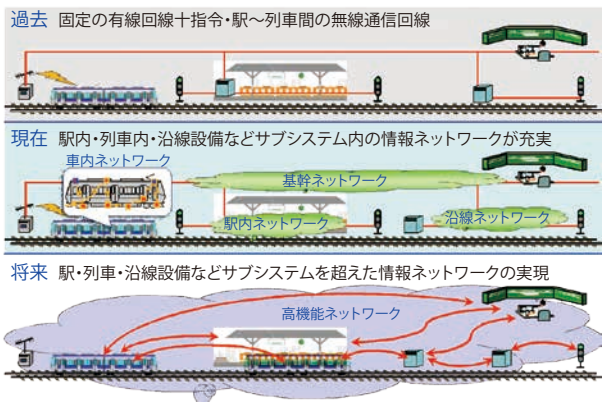


図 -2　鉄道における情報ネットワークの変遷

無線式列車制御システム

列車の安全運行を支える信号保安システムにおいて，現時点において実用化されている ICT 活用の代表例は，無線式列車制御システムである．このシステムでは，無線通信技術とデータベース技術を活用することにより，列車の位置や速度等の情報を細かく把握しながら列車を安全に制御する．世界各国で導入が進んでおり，国内においても，JR 東日本における ATACS（Advanced Train Administration and Communications System）と呼ばれるシステムの実用化を皮切りに，複数の鉄道事業者が導入に向けて検討・開発を進めている.

無線式列車制御システムの導入のメリットは，列車位置を検知するための地上設備が削減できることと，列車上で検知した詳細な位置情報を無線で地上の制御装置に伝送・集約することによって列車どうしの間隔を安全かつ柔軟に制御できることなどが挙げられる．また，予測制御や自動運転など，より高度な列車制御システムに発展させるためのベースシステムとして活用できるというメリットもある.

無線式列車制御システムは，インターネットには接続されてはいないが，制御対象である列車と転てつ機，踏切などを“モノ”ととらえれば，広い意味では IoT の一種と言えるだろう（図 -3）.

すでに海外ではサービスが始まっている“5G”と呼ばれる第五世代の移動体通信網が2020年春から国内でも利用できるようになる予定であるが，5Gを列車の運行制御へ適用するための基礎的な検討も始まっている．5Gを活用し，鉄道システムに求められる高い安全性と信頼性が確立された暁には，無線式列車制御システムにおける制御情報も5Gネットワーク上で伝送されるようになり，巨大なIoTの一部となる可能性もある．

情報ネットワークを活用した新しい鉄道システムの将来像

前節で述べた無線式列車制御システムでは，詳細な列車位置や速度などの情報を得ることができる．これらの詳細な制御情報を活用して，各列車の運転パターンをリアルタイムで生成することで，安全確保とダイヤ管理とを融合した新しい運行制御システムの実現が可能となった．これにより，旅客の集中や列車の遅延等の状況に応じて列車の運行を柔軟に制御でき，遅延の拡大の抑制，ダイヤ乱れの早期復旧が容易に実現可能となる．鉄道総研では，2015年度から，情報ネットワークにより運行管理と保安制御の機能を融合し，運転曲線（路線上での列車の位置と速度の関係を表す曲線．走行パターンとも呼ばれる）をリアルタイムに再計算して個々の列車や進路を制御するシステムの開発に取り組んでいる．

このシステムを実現する上で，最も重要な基盤となるのが情報ネットワークである．この情報ネットワークに，列車の制御情報だけでなく，沿線のセンサや制御機器などの状態情報，改札機からの情報を載せることで，鉄道の運行状態，設備の状態，そして旅客の流れなどをすべてデータ化し，鉄道システム全体の動作状況を各業務分野の管理部門で把握するとともに，関係する部門間で共有し再利用することが可能となる．これらのデータを基にコンピュータ上のサイバー空間で現場の状態や列車の運行状態の再現・予測ができれば，設備の状態を把握して運行可否を判断するためにかかっている多くの労力と時間を大幅に削減でき，気象災害などの異常時の早期運転再開や，メンテナンスにかかる負荷の軽減が期待できる（図-4）．これは，いわば鉄道版の“サイバーフィジカルシステム”と言える．

このシステムでは，鉄道設備が自律的に不具合個所や交換時期等の情報を発信し，列車自身が安全・安定輸送に必要なさまざまな情報を自ら取得して自律的に判断しながら走行することも可能となる．このような情報共有のためのネットワークについては，各方面で研究開発が進められており，鉄道総研でも鉄道における情報伝送の特徴や要件を踏まえたネットワークプロトコルの開発を行っている．なお，2020年度からは，上で述べた列車が自律的に走行する運行制御システムと情報通信基盤の実現に向けた研究開発もスタートさせる．

現在，MaaS（Mobility as a Service）と呼ばれる

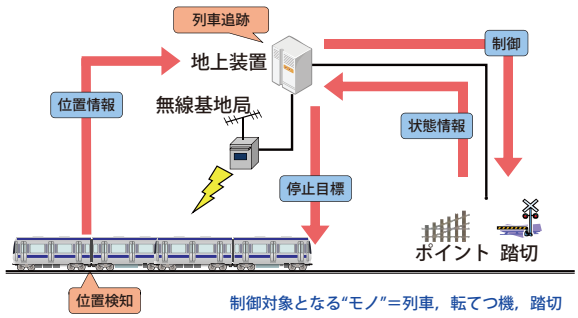


図-3　無線式列車制御システム

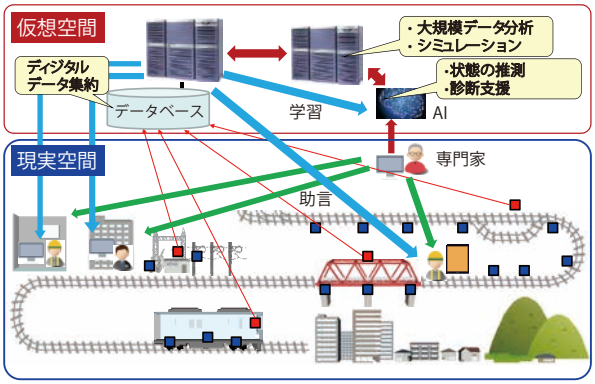
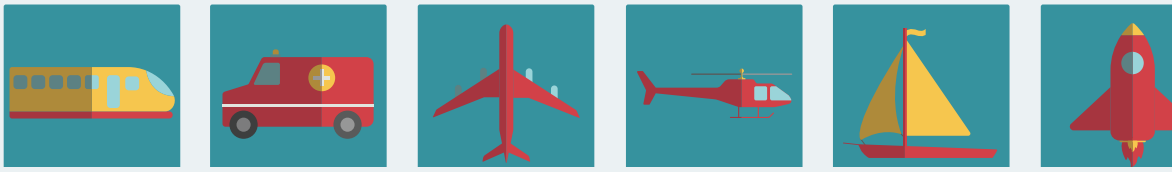


図-4　鉄道版サイバーフィジカルシステム



シームレスなモビリティサービスの実現に向けた取り組みが本格化しているが，少子高齢化が進み，自然災害が激甚化する時代の中でさらに安全でスムーズなモビリティサービスを実現するためには，図-4に示したような新しい鉄道システムへと変革していく必要があると考えている．

本節で挙げたように，列車の運行制御に情報ネットワークを活用していく上では，サイバーセキュリティへの対策が必須の課題となる．次章では，本章で述べた無線式列車制御システムを主たる対象として，情報セキュリティに関する動向と今後の課題について述べる．

鉄道の情報ネットワークと情報セキュリティ

情報セキュリティと制御システム

一般的にいう「セキュリティ」は，「安全」「防犯」「安全保障」などの意味で使用されるが，原義はラテン語の“se curitas”＝“freedom from care（不安・心痛からの解放）”とのことである．セキュリティ対策を検討する際には，「何を保護すべきか」「何から保護すべきか（＝脅威は何か）」「セキュリティが侵害された場合の影響はどのようなものか」の3点に対して，明確な目標を設定することが重要とされる．「情報セキュリティ」では，情報処理システムや情報通信システムなどの情報システムが扱う「情報」が外部の脅威から守るべき資産となる．情報システム（IT）におけるセキュリティと，無線式列車制御システムなどの制御システム（OT）のセキュリティとの違いは，表-1のように整理できる．

情報セキュリティの動向と鉄道

インターネットや携帯電話網等の情報ネットワークの拡大と，スマートフォンやタブレットも含む各種情報端末の爆発的な普及に伴い，サイバー攻撃による被害も急速に増えており，サイバーセキュリティの確保に向けた官民学連携の活動が本格化している．かつては愉快犯的な攻撃が主であったが，近年はサイバー攻撃が“ビジネス”になっているとも言われる．企業や工場ばかりでなく，電気やガス，交通機関といった重要インフラをターゲットとするサイバー攻撃の脅威は高まっており，国内外で実害が生じた事例も報告されている．内部不正による情報漏えい，サプライチェーンリスクと呼ばれる外部委託における情報漏えいおよび不正部品・マルウェアの混入により，流出した情報が闇サイトを通じて売買され，サイバー攻撃に用いられるケースもある．このような脅威に対応するため，セキュリティ対策を後付けとせず，製品の企画・設計段階から組み込む Secure by Design という考え方が適用されつつある．

国内におけるサイバーセキュリティに関する専門機関である IPA（独立行政法人情報処理推進機構）では，さまざまな議論・情報共有の場や機会を設け，啓蒙活動も積極的に展開している．2017年4月には，「産業サイバーセキュリティセンター」を設置し，サイバーセキュリティに関する実践的なスキルを持つ専門家を産業分野ごとに育成する事業をスタートさせた．なお，鉄道関係でも，IPA に「鉄道 IT 情報共有グループ」が置かれ，意見交換と情報共有が行われている．

表-1　IT と OT

	IT（Information Technology） **情報システム**	OT（Operational Technology） **制御システム**
保護対象	情報そのもの	制御プロセス （対象となる人やモノ）
重要視する 主な脅威	情報の漏えい 情報の改ざん	制御手順・情報の改ざん 意図的な誤制御（なりすまし） 制御不能・制御遅延 非意図的な誤制御
維持すべき 特性	機密性，完全性	完全性，真正性 可用性，信頼性
技術的仕様	標準化された ものが多い	独自仕様が多いが， 標準仕様に準じるものや IT系と間接的に接続される ものが急速に増加

列車の運行制御システムに対するセキュリティ関連の規格と動向

列車の運行制御システムにおける保安情報の伝送においては，通信遅延，通信誤り，通信妨害などによって危険側動作とならないよう，必ず対策がとられる．鉄道システムにおいて安全にかかわる情報を伝送する通信システムに対しては，国際電気標準会議（IEC）から IEC 62280（鉄道の安全関連伝送に関する国際規格）が 2014 年 2 月に発行されており，利用する伝送システムのタイプに応じて検証すべき事項や想定すべき脅威（表 -2）が定められ，脅威に対する対策の考え方が示されている（表 -3）．なお，表 -3 中の○は規格上で特に条件なく効果ありとされている対策，△は規格上の注記によって条件つきで効果ありとされている対策である．

また，列車制御に適用される無線通信システムに関しては，無線通信システムに対する性能要求を決定する手順が IEC/TS 62773（無線式列車制御用無線通信システムの設計手順に関する国際的な技術仕様）として 2014 年 4 月に発行されている．この技術仕様では，環境条件，線区条件，運転条件，システム条件と無線伝送の性能要求との相関が定義されているほか，暗号化となりすましに対する対策をセキュリティに関する設計パラメータとして考慮することとしている（図 -5）．

さらに，鉄道の信号通信における情報セキュリティについて，国際鉄道連合（UIC）から「鉄道におけるサイバーセキュリティのガイドライン」が 2018 年 6 月に発行された．このガイドラインは，鉄道業界がサイバー攻撃に対する脆弱性を軽減し，ライフサイクル全般にわたって鉄道システムとデータのアベイラビリティ，完全性（健全性），機密性を確保することのサポートを目的として，鉄道信号と通信への ISO/IEC 27000 シリーズ（ISO と IEC が共同で策定している情報セキュリティマネジメントシステムに関する規格群）の適用が示されている．サイバーセキュリティリスクに対して信号システムの安全とアベイラビリティを確保する方策として，情報セキュリティ管理実践の規範である ISO/IEC 27002 をベースに鉄道向けの考え方がまとめられているほか，特にライフサイクル全般について考慮すべきセキュリティと，ソフトウェア開発におけるセキュリティ確保について述べられている．

表 -2　IEC 62280 が定める伝送上の脅威

脅威（Threat）	定義
重複（Repetition）	単一のメッセージが2回以上受信される
削除（Deletion）	メッセージがメッセージストリームから除去される
挿入（Insertion）	メッセージストリームにメッセージが追加される
順序誤り（Resequence）	メッセージストリーム中のメッセージの順番が変化する
破壊（Corruption）	メッセージが改変される
遅延（Delay）	意図した時刻より遅れた時刻にメッセージが受信される
なりすまし（Masquerade）	認証されていないメッセージ・ユーザが認証されているかのように見える

表 -3　IEC 62280 に示されている対策例

脅威	対策							
	シーケンス番号	タイムスタンプ	タイムアウト	送受信ID	フィードバック	端末認証	セーフティコード	暗号化技術
重複	○	○						
削除	○							
挿入	○			△	△	△		
順序誤り	○	○						
破壊							○	○
遅延		○	○					
なりすまし					△	△		○

列車の運行制御システムにおける情報セキュリティの今後の課題

これまでの鉄道における運行制御システムは，安

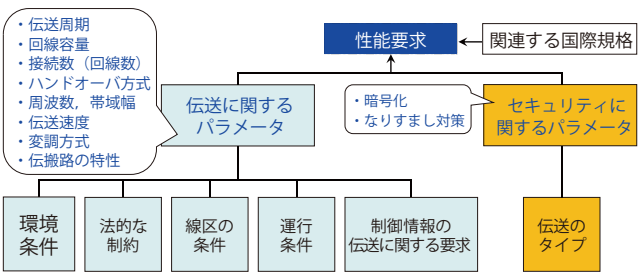
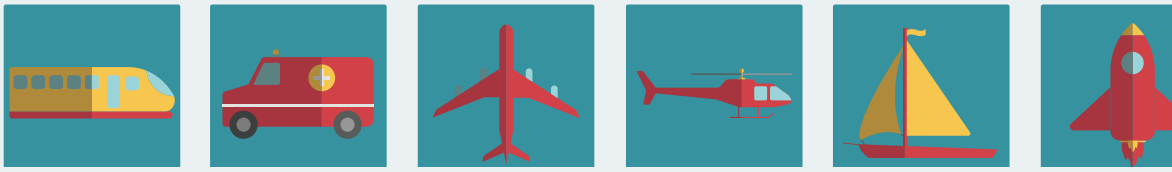


図 -5　IEC/TS 62773 が規定している列車制御用無線通信システムの設計パラメータ



全確保を最優先として，独自の方式やプロトコルを採用し，クローズドなシステムとして実装，使用されてきた．

しかし，制御システムのオープン化・ネットワーク化が進み，クローズドなシステムとオープンな仕様のシステムが接続されるようになっている．鉄道の列車運行制御においても，クローズドシステムとオープンシステムとの接続はすでに始まっており，今後さらに接続される範囲や対象が広がることが予想される．従来の鉄道のシステムと，オープン仕様の世界のシステムとでは，信頼性や可用性に対する考え方が異なっており，また設備や機器の更新スピードにも大きな差異がある．両者のバランスをいかにとりながらセキュリティを確保するかが，今後の課題となろう．

また，これまでの鉄道の保安制御は，フェールセーフの考え方に基づいて構築されており，故障や異常が生じた際には列車を止める，という仕組みで事故を防いできた．今後も，進路の安全が確保できない限り列車を進行させない，という大原則は守らなければならない．しかしその一方で，情報セキュリティの観点からは，障害事象が同時多発的に起きること，またシステムの安定動作を阻害されることも想定する必要があり，サイバー攻撃によって輸送サービスが妨害される事態も考慮しなければならない．安全を最優先に確保しつつ，サービスレベルの低下を最低限にする（＝できるだけ運行し続ける）ための仕組み･対策の構築も重要な課題の１つである．

より安全でスムーズな モビリティサービスの実現に向けて

情報ネットワーク技術を始め，急速な発展を遂げているさまざまなディジタル技術は，今後鉄道を維持していくために欠かせないツールであり，またさらなる発展のための強力な武器ともなる．ただし，情報ネットワークを利用するためには，サイバーセキュリティに関する課題への対応が必須である．特に安全に直結する制御システムにおいては，安全を確保しつつシステムをできるだけ止めないようにするための考え方の整理と，具体的な制御手法の構築，そして実際にシステムを防護するための体制や，運用･管理の基準･ガイドライン類の整備が欠かせない．システムのネットワーク化やオープン化がさらに進むことによる侵入口の増加は不可避であり，システム全体への波及の可能性に対する考慮をしながら思いもよらぬ攻撃をいかに想定し，システムを守り，サービスレベルへの影響を最小限とするかなど，解決すべき課題は多く，また難易度も高い．鉄道の信号通信の専門家と，情報セキュリティの専門家が連携し，情報共有しながらこれらの課題に取り組まないかぎり，ICT 活用による鉄道システムの革新は現実のものとできないと言っても過言ではないだろう．

鉄道におけるディジタル技術の本格的な活用はまさにこれからであり，安全でスムーズなモビリティサービスが提供できる新しい鉄道の実現に向けて，鉄道事業者や先端技術を有する大学，研究機関，メーカと連携しながら，地に足をつけた研究開発に取り組んでいきたいと考えている．

（2020 年 1 月 12 日受付）

川﨑邦弘　kawasaki.kunihiro.29@rtri.or.jp
1989 年慶應義塾大学理工学部卒業．同年，鉄道総合技術研究所入社．現在，鉄道総合技術研究所 信号・情報技術研究部 部長．鉄道業務用無線通信システムと電磁環境に関する研究開発，国際規格審議に従事．電気学会，電子情報通信学会，IEEE 各会員．

祗園昭宏　gion.akihiro.61@rtri.or.jp
2008 年神戸大学大学院自然科学研究科修了．同年，鉄道総合技術研究所入社．現在，鉄道総合技術研究所 信号・情報技術研究部 列車制御研究室 副主任研究員．列車制御システムと安全性評価手法に関する研究開発に従事．電気学会，IRSE 各会員．