無線式列車制御システムへの汎用通信回線の適用手法

北野　隆康*　　祇園　昭宏**

Methods for Applying Public Communication Network to Communication-Based Train Control Systems

Takayasu KITANO　　Akihiro GION

A method for applying public communication networks to communication-based train control systems is proposed. The application of public communication networks to train control systems differs from conventional systems in that transmission lines which cannot be controlled by railway operators, intervene between safety equipment. Therefore, in order to construct a system in which safety techniques can be applied without depending on transmission lines, a configuration in which train control function and information transmission are independent of each other is presented. Furthermore, threats posed by information transmission function from the perspective of the train control function and countermeasure requirements are presented, as well as implementation methods which satisfy these requirements at the current techniques.

キーワード：無線式列車制御，汎用通信回線，公衆通信回線，セキュリティ，システム構成

1．はじめに

将来的な人口減少に伴い，鉄道事業者が自営で保有している設備の保守・保全に携わる作業員の確保が困難になる可能性がある。このような状況下では，保守すべき地上設備を削減する技術開発への期待が高まる。地上の保安設備の削減が期待されるシステムとして，車上装置の高度化と地上―車上間の無線による情報伝送を活用した無線式列車制御システムがすでに実用化されている[1)2)]。しかし，従来の無線式列車制御システムでは，軌道回路などの従来技術に基づく地上設備は削減されるものの，地上―車上間で制御情報を伝達する伝送装置が追加で必要となることや，車上装置の機能が増加することなど，導入する線区の条件によってはシステム全体として必ずしも設備減とはならないケースがある。

今後，鉄道事業者にて設備して保守・管理する必要がある地上設備のさらなる削減を目的として，他分野で普及している汎用技術の保安装置への適用に対する期待が高まっている。特に，無線式列車制御システムにおいては，地上―車上間の制御情報の伝送に対して公衆通信回線などの汎用的に使用できる通信回線（以下，汎用通信回線と呼ぶ）を適用することで，用途に特化した専用の基地局やアンテナ等の無線設備を削減することで保守の省力化が実現できる見込みである。

そこで本報告では，自営通信回線と汎用通信回線のいずれの通信回線にも依存しない無線式列車制御システムの構築を目的として，無線式列車制御システムに汎用通信回線を適用する際の安全性確保の考え方を定義し，通信回線への要件の決定を含めたシステム開発の手順とセキュリティの実装方法を提案する。

2．汎用通信回線適用の考え方

2.1　無線式列車制御システムの概要

2.1.1　システム概要

無線式列車制御システムの概要を図1に示す。このシステムにおいては，無線を用いた地上―車上間での制御情報の伝達と，車上での列車位置検知，車上装置による主体的な制御により，柔軟な列車運行の実現と運転保安に関わる地上設備の削減を図っている[3)]。このシステムを実現する上で重要な機能として，車上装置が自列車位置を正しく認識すること，車上装置が認識した列車位置を地上装置に正しく伝達すること，地上装置にて各列車位置に従って進路を構成して停止限界を設定すること，設定した停止限界を車上装置に伝達すること，伝達された情報に従って停止パターン作成して列車を制御することなどがあげられる。

2.1.2　地上設備削減に関する課題

これまでに国内で開発された無線式列車制御システムでは，地上―車上間の情報伝達に自営の通信回線を構築して使用している。そのため，地上の保安設備は削減されるが，通信回線を構築する伝送装置が必要となり，システム全体としての設備減とならない可能性がある。

例えば，列車の在線について，従来のシステムでは軌道回路を用いて検知していたのに対し，無線式列車制御システムでは，車上装置で認識した位置を地上装置に伝達し，地上装置にて列車の在線範囲を把握することとな

＊　信号技術研究部　列車制御システム研究室
＊＊　情報通信技術研究部　通信ネットワーク研究室

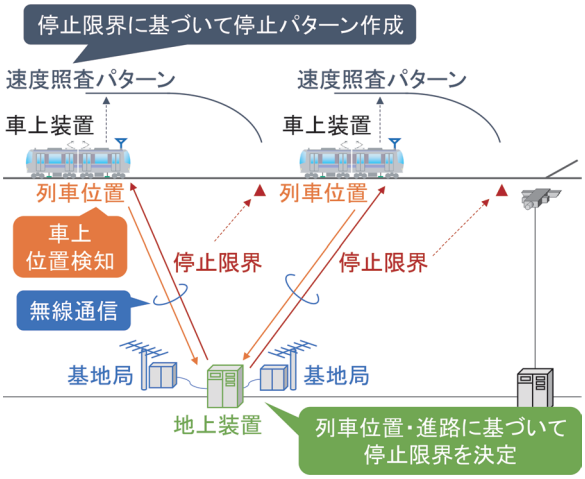


図１　無線式列車制御システムの概要

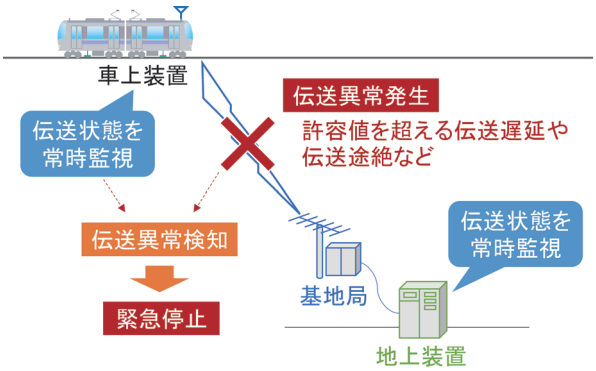


図２　無線式列車制御システムの安全側制御の例

る。この場合，列車検知の観点で軌道回路は不要となるが，従来システムにはなかった地上―車上間での情報伝送を行う装置を沿線に整備する必要がある。

特に地方線などの列車運行密度が高くない線区では，列車の運行本数に比べて相対的に設備が多くなるなど，自営設備の保守に対する負担が大きくなる傾向にある。

2.2　汎用通信回線を適用したシステム開発の方向性

2.2.1　無線式列車制御における安全確保の概要

無線式列車制御システムでは，安全性を確保する上で，地上―車上間の情報伝達に異常が発生する場合への対策が必要である。この対策の例として，図２に示すように，地上装置および車上装置にて，送受信する電文や，その送信相手となる装置が正常かつ正当なものであることをチェックする機構を設け，異常を検知すると列車を停止させることがあげられる。

2.2.2　安定した列車運行の確保

前項 2.2.1 のように伝送異常時に停止制御を行うと，伝送品質の低下などにより安定して情報が伝達できない事象が生じると，その都度，列車が停止することとなり，安定した列車運行が確保できない可能性がある。

安定した列車運行を確保するには，①保安装置の仕様や動作を踏まえて安定と見なせる通信回線を使用する，もしくは，②不安定な通信回線でも安定性が担保できるように保安システムを構成・設計する，の方針がある。

これまでに開発・実用化された無線式列車制御システムでは，上記①の方針に沿って，列車制御システムとしての動作を満足するよう，専用の通信設備により自営の通信回線を構築していた。一方，汎用通信回線を活用する場合は，通信設備に専用の機能を搭載できないことを前提として，列車制御用の設備や装置に持たせる機能を決定する必要がある[4)5)]。

なお，汎用通信回線を活用する場合，上記①と②のいずれの場合でも，安全の確保という観点で保安装置に必要となる機能は同じである。本報告では，以下，安全の確保を中心をとした，列車制御システムへの汎用通信回線の適用手法について述べる。

2.2.3　汎用通信回線適用における課題

従来の列車制御システムを構成する装置は，安全となる動作を定義した上で異常時を含めてフェイルセーフに動作することを前提に開発・設計されていたが，汎用通信回線で使用される装置は，フェイルセーフな動作を想定せずに開発・設計されている。従来の無線式列車制御システムでは，フェイルセーフな装置構成を前提にIEC62280[6)7)]を踏まえた対策を実施していたことに対して，汎用通信回線を適用する場合は，汎用的でフェイルセーフに動作しない伝送装置が保安装置の間に挿入されることを前提としてIEC62280を踏まえた対策を実施する必要があることが課題となる。

そのため，従来の保安装置間で実施していた安全性技術に加えて，保安装置が外部からもたらされる安全への脅威に対する対策技術が重要となる。すなわち，保安装置間にブラックボックスな伝送装置や通信回線が介在する場合でも安全側に動作するよう，伝送装置によらず保安装置にて安全を担保する仕組みが必要となる。

3．無線式列車制御への汎用通信回線の適用

3.1　列車制御システムの構成決定手順

列車制御システムの具体的な仕様を定める前に，システムを構成する装置の機能や動作を決定する。システム構成の決定にあたり，目的や運行条件に基づいて列車制御の機能や動作を決定し，列車検知などの要素技術を適用する以下の手順を提案する[4)]。

（1）システム導入方針の明確化

汎用通信回線の活用により列車制御システムの導入コストを下げるには，汎用的な用途で開発された伝送装置を改修せずにそのまま活用することが最も効果的である。一方，汎用通信回線をそのまま活用する場合は，運

転取り扱いなどの運用において，従来と同じ運用を維持できないことがあり，運用が変更になる可能性がある。

そこで，システムを構成する方向性としては，従来の運用を維持しつつ汎用技術を活用することと，運用を変更して低コスト化を図ることのいずれかとなる。これらの方針は装置の機能や機能割り付けに関係し，システムの開発と導入に大きな影響を与えるため，列車制御方式や列車検知方式などを定める前に決定すべき事項である。

（2）列車制御方式の決定

導入線区の運用上の課題や，線区特有の事情などにより変更できない取扱いを事前に特定し，これらの要件を満足する列車制御の機能を決定する。特に，輸送量を満足するために必要となる運行面の要件を抽出することが重要である。機能を決定した後，列車の運行や保守，更新する設備などを踏まえて車上装置と地上装置に割り付ける機能を決定する。

（3）列車検知方式の決定

無線式列車制御システムでは，車上での認識した列車位置に基づいて列車検知を行うが，車上での位置認識技術と列車検知機能の機能割り付けを検討する必要がある。

前段の（2）にて抽出した導入線区の運用上の要件や，具体的な列車制御方式の機能を考慮し，列車検知機能の車上・地上への割り付けと，必要な位置認識の精度を定めたのち，適合する位置認識技術を採用する。

（4）伝送装置と通信回線の選定

地上―車上間の情報伝送を担う伝送装置と通信回線は，列車制御および列車検知の機能を定めた後，要件を定めて選定する。これらを選定するために必要となる要件の決定については 3.3 節にて後述する。

上記（1）～（4）に基づくことで，無線式列車制御システムの構成を決定できる。

3.2　列車制御システムの構成

汎用通信回線で使用される伝送装置は保安装置への適用を想定せずに開発されているため，安全に関わる機能を搭載させることができない。そのため，これまでに開発・実用化された無線式列車制御システムと同じ構成にて伝送装置のみを置き換えることができず，装置の機能の割り付けを変更する必要がある[5)]。

そこで，列車運行の安全に関わる機能と，情報の伝達を行う機能を明確に分離させ，それぞれの機能の依存関係を解消する列車制御システムの構成を提案する（図3）。この構成では，保安装置である地上装置と車上装置の間での電文の伝達において，情報伝達の機能に依存することなく，地上装置と車上装置の機能のみで安全やセキュリティを確保できるようにする。また，基地局や車上無線局が持つ情報伝達に関わる機能としては，地上―車上間で情報を伝達する機能のみとする。

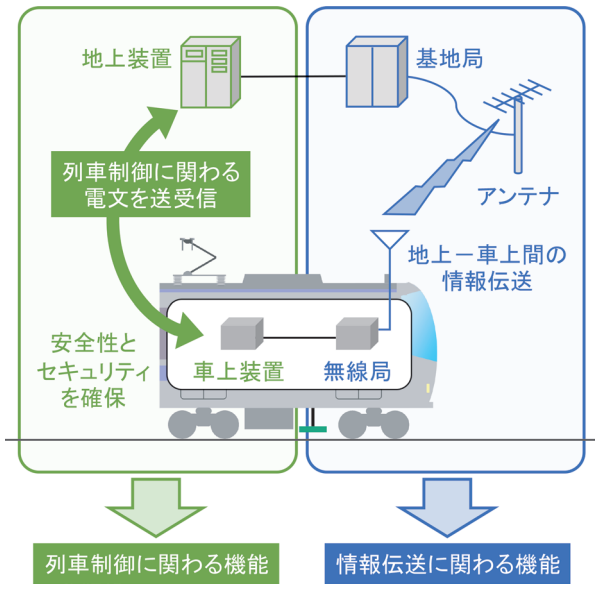


図３　保安制御と無線伝送の機能分離

なお，本報告では，以降，情報伝達の媒体や手法に依存せず，安全に列車を制御するために必要な機能を「列車制御に関わる機能」と定義する。また，指定された装置間での情報伝送を担う機能を「情報伝送に関わる機能」と定義し，それを担う伝送装置と通信回線を含めたシステムを「伝送システム」と定義する。

3.3　伝送システムに対する要件の決定

地上―車上間で，列車制御に関わる機能を満足するために必要な情報を確実に伝達できることが重要である。

列車制御を実現するうえで必要となる制御装置の要件や，線区における運用条件に基づいて，装置間で必要となる情報の情報量と伝送周期および，伝送品質（誤り率，遅延時間）を要件として定義し，満足する伝送システムを適用することが必要である。これを手順化したものを図 4 に示す。3.1 節に示したように，列車制御システムの構成を決定した後，各装置の機能の動作に必要となる情報を抽出し，その情報の入出力への要件を策定する，という手順である。なお，この方法は，IEC/TS 62773 で定義された手順にも対応する。このとき，図 5 に示すように列車制御に関わる機能に注目して伝送システムを一般化することで，安全側制御に必要な機能の抽出と伝送システムへの要件の定義が容易になる。

4．汎用通信回線適用時のセキュリティ対策

4.1　伝送システムにおける脅威と要件

4.1.1　サイバー攻撃

伝送システムからの脅威に対して想定されるサイバー攻撃の分類としては，なりすまし（Spoofing），改ざん

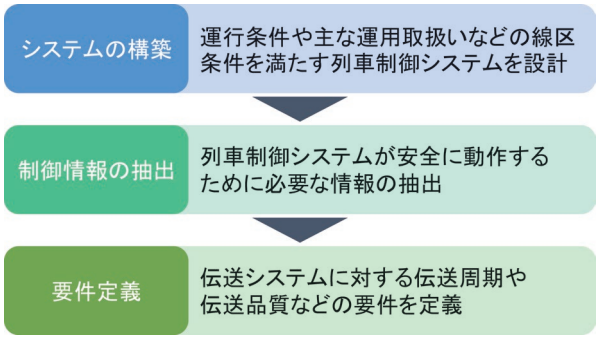


図４　伝送システムへの要件の決定手順

（Tampering），DoS（Deny of Service）攻撃がある。

なりすましでは，相手装置なりすましとリプレイ攻撃が想定される。相手装置なりすましについては，外部の第三者がシステム内の装置のひとつであるかのように振る舞って「なりすます」ことである。リプレイ攻撃は，外部の第三者がシステム内の装置が送信する電文を記録しておき，異なるタイミングで過去に送信されたものと同じ電文を再送する攻撃である。

改ざんは，電文の送受信の過程に第三者が介入して情報を改ざんすることである。

DoS 攻撃は，攻撃対象の装置に対して無関係な大量の情報を送信することで，正常な動作を阻害する攻撃である。攻撃された装置は，送信された大量の電文を処理することになり，処理が遅延する可能性や，異常な動作をする可能性がある。

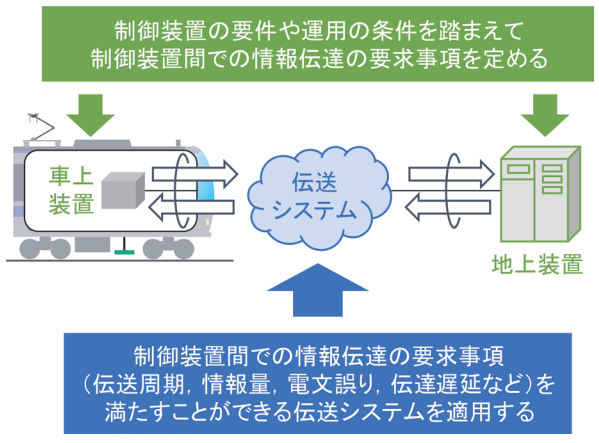


図５　伝送システムに対する要件を決定する考え方

4.1.2　伝送システムにおける脅威

安全関連伝送に関する国際規格として IEC 62280 が規格化され[6)7)]，伝送システムにおいて発生しうる７つの脅威（重複，挿入，順序誤り，破壊，削除，遅延，なりすまし）が定義されている。これらについて，保安装置である車上装置または地上装置の入力情報への脅威という観点で整理すると，表１に示すように，「誤った情報が入力される」「情報が途絶する」「入力情報が遅延を含む」の３つに整理できる。なお，重複，挿入，順序誤り，破壊，および，なりすましについては，いずれも保安装置への入力としては誤った情報として整理できる。

4.1.3　第三者による脅威への対策

列車制御システムの伝送システムにおける脅威として，ノイズなどの自然発生的な要因による「非意図的な誤り」と外部からの第三者による「意図的な誤り」がある。これまでの列車制御システムでは，非意図的な誤りに対して，通番やタイムスタンプ，安全符号に基づく電文の検定や伝送途絶の検知により検証している。さらに，意図的な誤りに対しては，電文の暗号化により，機密性に重点を置いた対策を実施している。これらの対策については IE62280 でも定義されている[7)]が，汎用通信回線を適用する場合は，意図的な誤りに対する検証が特に重要となる。これについて，情報入力先の装置が正しい相手であることを示す「真正性（Authenticity）」，および，情報が正確かつ最新である「完全性（Integrity）」を検証する方法が有力である（図 6）。

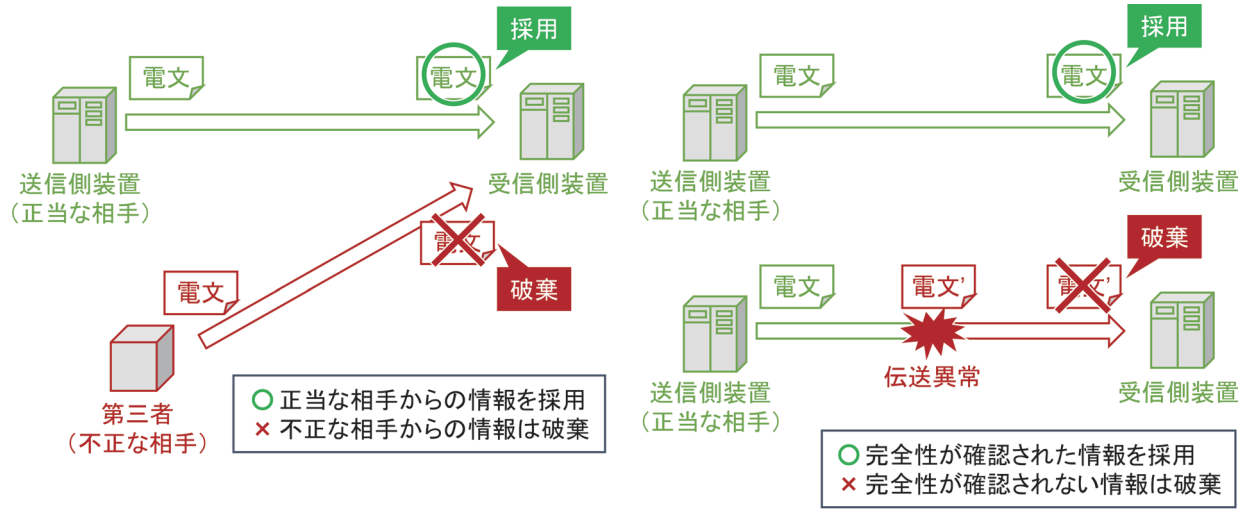
そこで，意図的な誤りに対する攻撃分類と安全に対する脅威およびその対策について表２に示す。

なりすましに対しては，送信装置になりすました他装置から，危険となる動作を誘発するような「誤った情報が入力される」ことが脅威となる。これに対しては，送信された電文の送信相手の真正性を検証することにより対策が可能である。

リプレイ攻撃は，電文そのものはシステム内の装置間で伝達されるものと同じであることから，リプレイ攻撃目的で送信された電文を受信した装置が，現在の状態を誤認して動作することで危険な事象となる可能性がある。この場合，「入力情報に遅延を含む」ことと，「誤った情報が入力される」ことの両方が脅威となる。改ざんについては，「誤った情報が入力される」ことが脅威と

表１　保安装置への入力における伝送システム上で発生する脅威の影響

	重複	挿入	順序誤り	破壊	削除	遅延	なりすまし
誤った情報が入力される	✔	✔	✔	✔			✔
情報が途絶する					✔		
入力情報に遅延を含む						✔	✔



(a) 真正性の確認　　(b) 完全性の確認

図６　相手装置の真正性と情報の完全性

表２　伝送システムにおけるサイバー攻撃手法

攻撃分類 / 脅威	なりすまし		改ざん	DoS 攻撃	
	相手装置なりすまし	リプレイ攻撃	電文の途中改ざん	伝送遮断（遅延）	大量電文
誤った情報が入力される	✔	(✔)	✔		✔
情報が途絶する				✔	
入力情報に遅延を含む		✔		(✔)	
検証方法	真正性	完全性			

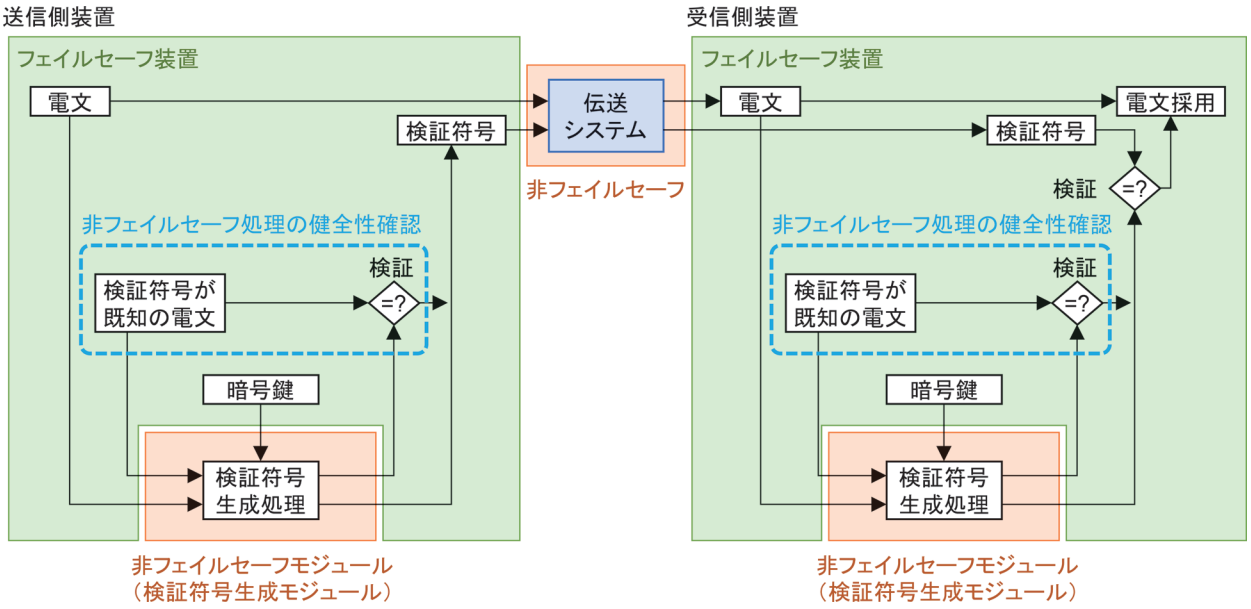


図７　メッセージ認証における処理と検証の分離構成

なる。DoS 攻撃は，大量電文に処理が膨大になる結果として，「情報が途絶する」ことや「伝送遅延が発生」することとなる。また，大量のランダムな情報が送信される場合，「誤った情報が入力される」可能性もある。リプレイ攻撃，改ざん，DoS 攻撃に対しては，送信された電文の完全性の検証により対策が可能である。

以上により，外部の第三者からの攻撃に対しては，真正性および完全性にて対策することが有効である。列車制御システムに汎用通信回線を適用する際は，保安制御機能にて表 2 に従った対策が実施されていることを確認して列車制御システムを設計することが重要となる。

4.2　脅威への対策を実装する手法の提案

4.2.1　メッセージ認証の適用

相手装置の真正性と情報の完全性を検証するためには，メッセージの改ざん対策であるメッセージ認証が有効である。これは，メッセージに対応した検証符号（MAC）を鍵情報より生成し，鍵情報の秘匿によって第三者によるメッセージの改ざんを検知する手法である。しかし，MAC の生成処理は，処理性能に応じて解析に必要な時間が複雑であることをもって暗号の安全性が確保される「計算量的安全性」に基づくため処理負荷が高く，現在のフェイルセーフ CPU で実施することは困難である。また，メッセージ認証で使用されるような暗号化技術はライフサイクルが早く，当該機能のみ交換できる構成であることが望ましい。

これに対して，非フェイルセーフで処理が高速なモジュールに暗号化技術に基づく処理を割り当てることが考えられるが，非フェイルセーフモジュールが正常に動作していない場合，改ざんを検知できず危険側となる可能性がある。

そこで，暗号化技術に基づいた電文の検証符号の生成処理を非フェイルセーフモジュールに割り当てたうえで，フェイルセーフ CPU にて非フェイルセーフモジュールの完全性を検証する手法を図 7 のように提案する。なお，図 7 では，検証符号が既知の電文を使用して検証符号の生成処理の完全性を確認している。

4.2.2　提案した構成の利点と留意点

鉄道信号用の保安装置等の産業システムと，一般的な情報システムではライフサイクルが異なるが，汎用の非フェイルセーフなモジュールと組み合わせることで，情報セキュリティ技術の更新への対応が容易になる。ただし，汎用通信回線を用いて保安情報を伝送する場合，保安装置に搭載されたフェイルセーフなモジュールで検証する事項の分析や抽出を含め，システム全体としての安全側動作を考慮することが重要である。

5．まとめ

本報告では，公衆通信回線などの汎用通信回線を無線式列車制御システムに適用する手法について提案した。汎用通信回線を適用する場合，従来の列車制御システムと比較すると，保安装置の間の情報伝送にコントロールできない伝送装置と通信回線を介在する点が異なる。そこで，「列車制御に関わる機能」と「情報伝送に関わる機能」を機能的に独立させるシステム構成を提案した。列車制御と情報伝送の機能を切り分けて考えることで，伝送回線に依らず安全性を担保する技術の適用が可能となる。さらに，列車制御に関わる機能の観点で伝送システムから与えられる脅威と対策の要件を示すとともに，現在の技術水準でその要件を満たす構成を提案した。今後，公衆通信回線を適用した列車制御システムの実用化に向けて，仕様策定と装置の試作を行う予定である。

文　献

1）八木圭介，山口智敬，内山大輔：デジタル無線を用いた列車制御システム（ATACS）の導入について，計測と制御，Vol.55，No.05，pp.443-447，2016

2）小川祥吾：丸の内線への CBTC システム導入，JREA，Vol.59，No.8，pp.28-32，2016

3）北野隆康：無線を用いた列車制御，RRR，Vol.73，No.4，pp.28-31，2016

4）北野隆康，熊澤一将，小川祥吾，藤田浩由，祇園昭宏：無線を用いた列車制御におけるシステム構成プロセスに関する検討，電気学会全国大会，5-150，2021

5）北野隆康：列車制御システムにおける無線通信技術の活用と展望，信学技報，vol.119，no.244，RCS2019-186，pp.45-50，2019

6）IEC 62280 : 2014 : Railway applications-Communication, signalling and processing systems-Safety related communication in transmission systems, 2014.

7）川﨑邦弘：安全関連伝送に関する国際規格 IEC 62280，鉄道総研報告，Vol.27，No.2，pp.41-44，2013