講演６．鉄道信号保安装置における通信と国際規格の活用

鉄道認証室　　森 崇（客員専門調査員）

１．はじめに

鉄道の安全を守るには、土木構造物、レールや枕木、ポイントなどの軌道、車両などの維持管理だけではなく、列車を制御するための信号装置や部外との交通との接続点である踏切装置等が重要な役割を果たしている。これらの装置は土木構造物や軌道等の「壊れない強度を持った安全、維持管理することにより保つ安全」ではなく、「壊れてもできるだけ安全な状態に遷移させる」というフェールセーフ思想でシステム設計が行われている。

この「フェールセーフ思想」で列車制御の安全を担保する装置を「鉄道信号保安装置」と一般的に称する。典型的な例には、列車と列車の間隔を確保し、衝突を起こさないようにする「閉そく装置」、列車に対して到着点まで安全に進路を確保する「連動装置」、「閉そく装置」や「連動装置」の情報を受け、運転士に対して進行の可否を示す「信号装置」、運転士が「信号装置」の指示に従わず運転を継続した場合に停止させる「ATS・ATC 装置」、列車の接近に応じて踏切を警報させ、踏切道に異常があれば列車を停止させる「踏切保安装置」などがある。

これらの装置は有機的に結合され、連携して動作する。この連携には、装置間の通信が使用されることになる。過去にはリレーを動作させ、そのリレー接点の ON/OFF により情報を伝送していたが、現代においては、IP(Internet Protocol,英)ネットワークや無線装置の活用が進みつつある。

このように鉄道信号保安装置の中で通信の重要性が増すにつれ、データの完全性の確保やセキュリティなど今までの鉄道信号保安装置の技術分野ではなかった事柄の重要性が増している。本発表では、鉄道保安装置におけるデータの完全性の確保、セキュリティ確保について国際規格を考慮に入れながら述べる。

２．鉄道信号保安装置への通信活用の例

鉄道信号保安装置として近年当室の認証においても増加しているのは、CBTC(Communication Based Train Control,英)である。この装置の概要を図１に示す。

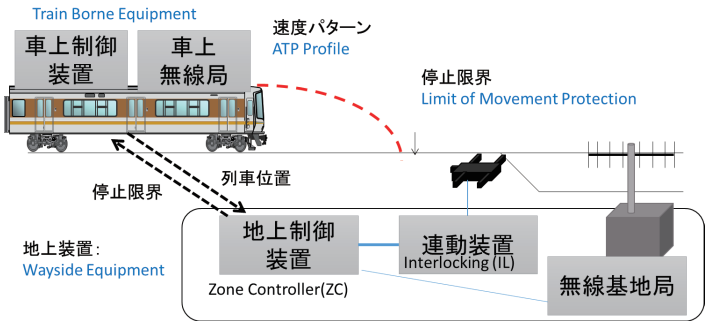

図１　CBTC の例

このシステムはいくつかの装置からなる。Interlocking(連動装置)は、列車に対して進路を確保し、CBTC wayside equipment（地上装置）が先行列車と連動装置の進路確保条件から、当該列車が進行を許可される限界である LMA(Limit of Movement Authority,英)を決定する。LMA の情報をもとに、Train-borne equipment(車上装置)は、ATP (Automatic Train Protection,英) profile を計算し、その速度を超過するとブレーキ指令を出力する。

進路確保条件が誤って CBTC 地上装置に伝わったり、誤った LMA が車上装置に伝送されると、列車の追突や脱線につながることになる。

このような事象を起こさないために、伝送データの完全性の確保は、CBTC において非常に重要であることがわかる。

３．ネットワーク設計における一般的な留意点

鉄道信号保安装置に通信ネットワークを活用する際に留意すべき点を以下に述べる。

○鉄道信号保安装置の通信ネットワークは鉄道特注品のみで構成することはほぼ不可能であり、幅広い市販品の中から構成を検討することになる。

鉄道信号保安装置は、安全性を担保するため、故障しても安全な状態に遷移させる必要があるが、通信を担う通信ネットワーク機器はそのような思想で設計されているものを選択することはほぼ不可能である。汎用化が極度に進み、現実的には使用される機器はネットワーク機器メーカが販売するものの中から選択することになる。その機器選択、ネットワーク構成やプロトコル選択については、鉄道事業者等の安全、稼働率、セキュリティ及び投資可能金額についての考え方によって大きく変わる。

○通信ネットワーク機器のライフサイクルは、製品寿命よりも保守の終了によって決まる。

ネットワーク機器のライフサイクルは鉄道保安装置の考える期間とは大きく異なり、５年から７年程度で保守サポートが終了することとなる。これはネットワーク機器がソフトウェアで動作するという特性上、ハードウェアのサポートだけではなく、ソフトウェアのサポートがあり、組み込むソフトウェアモジュールのサポートが終了すると、必然的に機器のソフトウェアのサポートを終了することになるためである。現在はサポート切れのソフトウェアを使用することは、ネットワークセキュリティの観点からは推奨されないため、その時点で機器の取り換えを行うこととなる。このため、通信ネットワーク機器においてライフサイクル管理も非常に重要な観点となる。

鉄道信号保安装置に使用される通信ネットワーク機器は、機器開発そのものをするのではなく、目的、保守ライフサイクル、鉄道事業者の考え方に応じて提供されているサービスや製品群から製品を選択し、代替可能な製品群を選択し取り替えることにより構築を行うことになる。このため、保守終了後、同一のプロトコルで動作するように、普及しているネットワークプロトコルを選択することが重要である。

４．IEC 62280 を中心にしたネットワーク構築の実際

４．１．IEC 62280 の基本的な考え方

IEC 62280（参考文献 1))は、鉄道用途の伝送、信号及び処理システムにおける、安全関連通信についての規格である。

IEC 62280 においては、reference architecture(参照構成)を定めている。これは現状を鑑み、一般の機器を用いて通信ネットワークを自営で構成することや、商用の通信ネットワークサービスを用いて鉄道信号保安装置の伝送を行うことを前提にしている。（図 2）

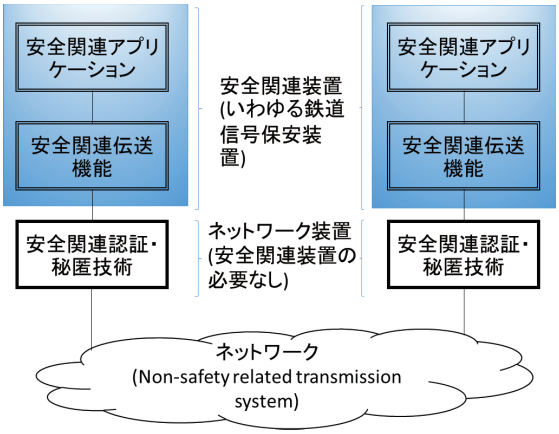

図 2　IEC 62280 参照構成

このモデルでは、安全関連伝送機能と通信ネットワークが伝送に関係する。通信ネットワークは、誤りやデータ抜け、データの重複、順序変更が発生する可能性がある。IEC 62280 では、通信ネットワークに非常に高い品質を要求するのではなく、どのような品質のものであっても、安全関連伝送機能で、その誤りなどを検出して、安全関連アプリケーションに使用しないように処理をすれば、誤ったデータで処理が行われずに、安全が担保できるという考え方に基づいている。その考え方の概要を図 3 に示す。

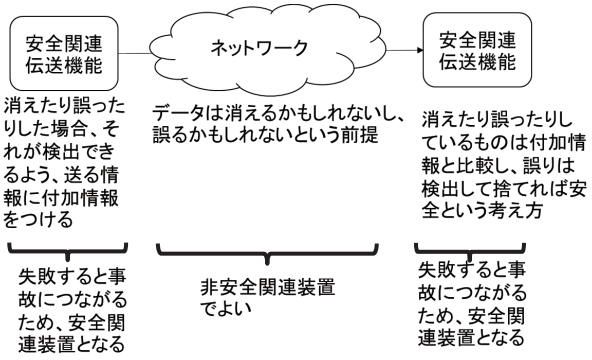

図 3　IEC 62280 の安全に対する考え方

この処理を失敗した場合、間違ったデータにより処理されてしまうため、異常の検出をできるだけ確実に行うように、ソフトウェアの品質を高め、ハードウェアの故障があった場合素早く止めなければならない。このため、安全関連伝送機能の処理は鉄道信号保安装置の中で行うことが IEC 62280 で定められている。なお、安全関連伝送機能は IEC62425(参考文献 2)鉄道用途の伝送、信号及び処理システムにおける、信号のための安全関連電子システム)に定められた技術的手法によることとなっている。

また、セキュリティ上の脅威に対応するため、必要に応じて「安全関連認証・秘匿技術」を付加することになっている。

４．２．IEC 62280 を中心に活用した設計

IEC 62280 は、Annex　D に"Guidelines for use of the standard(この規格の使用ガイドライン)"があり、設計ステップ（IEC 62280 D.1)が述べられている。

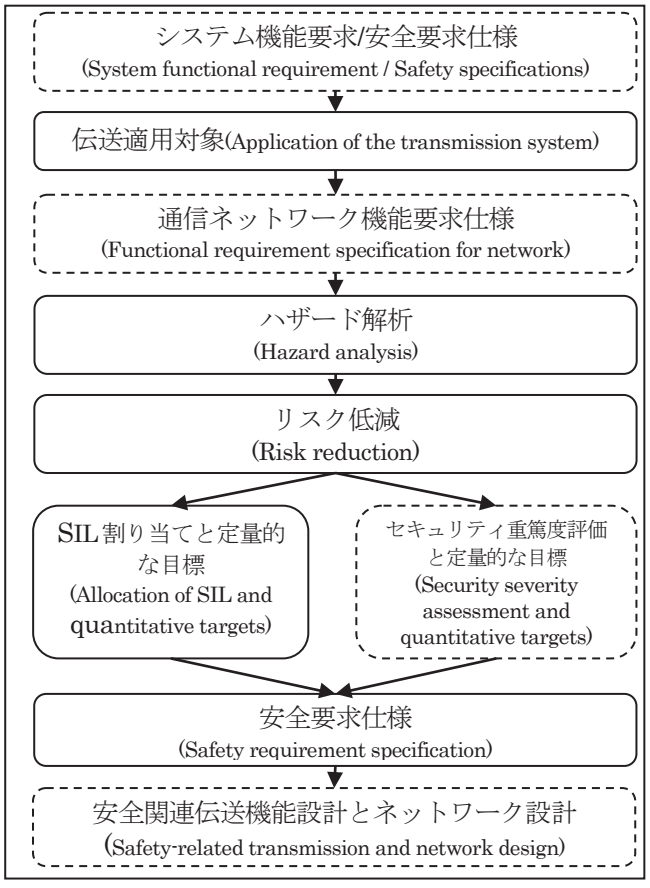

図 4　伝送機能設計の流れ

なお、図 4 における項目のうち、実線で囲われた部分は IEC 62280 Annex D に記載のある事項であり、点線で囲われた部分は、筆者が必要と思われる事項を追記したものである。各々について、重要な事項を述べる。

(1) 伝送適用対象

通信ネットワークにどのようなデータがそのような頻度で流れるかを設計者が把握する。この把握がハザードの解析の基礎となる。

(2)ハザード解析

(1)で検討したデータが、

- 繰り返し　repetition;
- 削除　deletion;
- 挿入　insertion;
- 順序逆転　re-sequencing;
- 符号破壊　corruption;
- 遅延　delay;
- なりすまし　masquerade.

があった場合どのような好ましくない事象が起こるかを考えていく。この 7 つのガイドワードを IEC 62280 では、「脅威(threat)」といっている。

この脅威は、通信ネットワークの特性により考慮しなければならない場合と、考慮の必要がない場合がある。このため、与えられた通信ネットワークにより、「専用で管理された category 1」、「専用ではないが外部からの悪意ある侵入がない category2」、「オープンでアクセス制限のない category3」に IEC 62280 では分類され、カテゴリごとの脅威への対策の必要性の有無が Annex B に示されている。

また、鉄道信号保安装置において好ましくない事象はほぼ「列車相互間の追突、衝突」、「列車の脱線」、「部外（自動車、人や土砂など）との衝突」、「運行の停止もしくは制限」とされる場合が多く、このうち人命に影響を与えるような事象を危害（harm)という。

この解析結果を基に、どのような脅威が具体的に存在し、危害などの好ましくない事象のリスクを評価し、通信ネットワークがどのカテゴリにあるのかにより、リスク低減が必要かどうかを決定する。またなりすましによる、人為的な攻撃については、確率的なアプローチが困難なため、章を改め説明する。

表 1 に解析の例を示す。

表１　ボトムアップアプローチによる解析

地上－車上間伝送の例（Category 3）

情報種別	脅威	ハザード	好ましくない事象	原因	頻度	評価
臨時速度制限	繰り返し	アプリケーション処理遅延・停止	列車運行不能	N/W 機器故障	B	対策必要
	削除	切断によるデータ更新なし	速度超過による脱線での複数死亡	断線	A	対策必要
	挿入	機器故障によるデータ挿入	不正な速度低下	N/W 機器故障	B	対策必要
	:	:	:			
	なりすまし	ハッキングによるデータ操作	速度超過による脱線での死亡 列車運行不能	無線区間ハッキング		別途検討
:	:	:	:			

(3)リスク低減、SIL の割り当てと定量的な目標

リスク低減の対処が必要な場合、脅威を引き起こす原因である hazardous event を解析し、通信ネットワークで事象発生頻度を低減するか、hazardous event があっても安全関連伝送機能で不正データを採用しないことにより対処することになる。安全関連伝送機能で脅威対処を行う方法について IEC 62280 7 章で考え方が示されている。以下に概要を示す。

表２　脅威とリスク低減手法

	低減手法							
脅威	シーケンス番号	タイムスタンプ	タイムアウト	ID	フィードバック	認証	安全コード	暗号技術
繰り返し	X	X						
削除	X							
挿入	X			X	X	X		
順序逆転	X	X						
符号破壊							X	X
遅延		X	X					
なりすまし					X	X		X

表 2 の通りリスク低減手法例は規格に示されている。しかしながら、シーケンス番号や安全コードの長さなどについては示されていない。

例えば、ある保安装置の機能に 10^{-9}/h を許容危険側遷移頻度として割り当てた場合、一般的にその装置の SIL (Safety Integrity Level,英)は 4 となる。その伝送を担う安全関連伝送機能にも SIL 4 を割り当てた場合、符号破壊の見落としもそれを下回ることが要求される。

一般的に安全符号 ICV (Integrity check value,英)において符号脆弱性がない場合、その符号衝突確率は、安全符号長を n とすると、$2^{-n/2}$ となる。仮にメッセージを 1 秒間に 100 回伝送し、伝送路におけるメッセージの誤り率が 10^{-5} の仮定の下で、符号誤り見逃し頻度を 10^{-10}/h を要求する場合、

$$100\times 2^{-n/2}\times 3600<10^{-5}$$

を満たす n となる 71 ビット以上の安全符号長が必要である。このように、「安全符号を採用する」だけではなく、「脆弱性のない○○ビット長の安全符号を採用する」というレベルまでの検討が必要である。

５．人為的な脅威についての留意点

なりすましなど人為的な脅威は、その他の脅威とは異なり、確率論的なアプローチのみで議論できない。また技術進化によりリスクが増大する場合があることに留意した方が好ましい。

人為的な脅威は、ハッキングを行う人の能力、それによる利益、技術的及び環境などのハッキングの行いやすさにより攻撃が成功するかどうか決まる。一般的に安全を語る際、確率×重篤性がリスクと言われるが、セキュリティについては、「実行可能性×ハッカーの利益」が評価指標となるため、ハッキングを行った際の利益やその利益の高い部分への重点的な対処が必要である。また、技術進化により一般的にはリスクは増大するため、人為的脅威は日頃から脅威を監視する必要性がある。IEC 62280 におけるなりすましへの対策について、上記のような視点が望まれると考える。

６．最後に

鉄道認証室において、データ伝送を活用したシステムの審査は今後ともますます増えていくと思われる。規格適合性において、システムが規格に合致することのみを目的とするのではなく、その規格の精神を生かし、より安全でセキュアなシステムを構築するために規格を活用していただけると幸いである。

鉄道認証室においても限られたメンバーではあるが、これからも伝送系における安全とセキュリティについての調査研究を進めて参りたい。

参考文献

1) IEC, “Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems ” IEC 62280 (2014)

2) IEC, ″Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling″ IEC 62425 (2007)