安全関連伝送に関する国際規格 IEC 62280

川﨑　邦弘*

An Outline of IEC 62280 - International Standard for Safety Related Transmission Systems

Kunihiro KAWASAKI

IEC 62280-1 and IEC 62280-2 are international standard documents that were published by International Electrotechnical Commission (IEC) in 2002. These standards define requirements for safety related transmission systems in railway systems. This paper describes the purpose and the structure of these standards, and the outlines of IEC 62280-2 which is a very important and useful standard for designing or building up radio communication networks intended to use for train control systems. And this paper also gives some information about maintenance work on IEC 62280-1 and IEC 62280-2.

キーワード：国際規格，IEC，保安システム，無線式列車制御システム，無線通信ネットワーク

1．はじめに

IEC 62280-1 および -2 は，国際電気標準会議（International Electrotechnical Commission：略称 IEC）から 2002 年に発行された国際規格である。両規格は，鉄道の保安システムにおいて安全に関わる情報の伝送を行う通信システムに対する基本的な要求事項を定義している。本稿では，IEC 62280-1 および -2 の構成と目的を述べたのち，無線式列車制御システム用の無線通信システムを設計・構成するうえで重要な規格である IEC 62280-2 の概要を紹介する。また，現在進められている改訂作業の状況と，改訂内容についても触れる。

2．IEC 62280 の目的と構成

2.1　IEC 62280 の目的

安全性に関わる装置の間で安全に関わる情報をやりとりするためには，必ず何等かの伝送システムを利用することになる。ここでいう安全性に関わる装置とは，連動装置などの信号保安装置や，無線式列車制御システムにおける拠点装置，車上制御装置などが該当する。伝送システムには，2 対の導線で装置間を直結する最も単純なものから，有線ネットワーク，あるいは無線を使うものまで，様々な手段が存在する。いずれの伝送システムを用いる場合でも，安全に関わる情報を伝送する際には，伝送システムで通信障害（伝送が途切れる，遅延する，妨害を受ける，など）が発生しても不安全な状態とならないよう，発生しうる障害を適切に想定し，しかるべき対応策を講じる必要がある。しかし，どのような障害を想定すべきか，また，どのような対策を施せば十分かは，安全関連装置の機能や安全に関わる情報の特性（情報量や頻度など），また利用する伝送システムの特性によって異なる。このため，伝送システムを利用する列車制御システムや信号システムを適切に設計するには多くの労力がかかるうえ，設計者によって想定や対策のレベルが異なってしまう恐れがある。そこで，IEC 62280 では，安全に関わる情報の伝送に必要な性能を有する伝送システムの仕様策定，実現の支援を目的として，基本的な要求事項や手順，対策の考え方を示している。重要な点は，IEC 62280 の目的は「伝送システムの性能の定義のため」であり，「安全性の確保のため」ではないことである。安全性に対する要求仕様，安全管理と品質管理の立証は，IEC 62278（RAMS 規格）によらなければならない，と規格本文に明記されている。

2.2　IEC 62280 の構成

IEC 62280 は 2 つのパートから構成されており，それぞれ IEC 62280-1, IEC 62280-2 と表記される。IEC 62280-1 のタイトルは“Railway applications – Communication, signalling and processing systems Part 1: Safety-related communication in closed transmission systems”（鉄道分野 - 通信, 信号および処理システム – 第 1 部:クローズドトランスミッションシステムにおける安全性に関する通信），IEC 62280-2 のタイトルは“Railway applications – Communication, signalling and processing systems Part 2: Safety-related communication in open transmission systems”（鉄道分野 - 通信，信号および処理システム – 第 2 部：オープントランスミッションシステムにおける安全性に関する通信）である。各パートは，英文タイト

＊　信号・情報技術研究部　ネットワーク・通信研究室

ル中の下線を引いた語句が示しているように，安全に関わる情報の伝送に使用する通信システムがクローズかオープンかによって区分されている。次の節では，この規格でいう“closed”と“open”の意味と，目次構成について述べる。

2.2.1 IEC 62280-1（closed transmission system）

IEC 62280-1 は，“closed transmission system”を利用して安全に関わる情報を伝送する場合に考慮すべき事項と要求事項を定義しているパートである。“closed transmission system”は次のように定義されている。

「既知で固定の性質をもち，ユーザー数が固定数または最大数が固定で，許可されていないアクセスのリスクが無視できる伝送システム」

すなわち，使用者が限定され，伝送システムの状態や，伝送路に流れる情報を完全に把握できるものが“closed”である。具体例としては，専用の有線回線やトランスポンダ・バリスなど密結合の伝送システムが該当する。

このパートでは，危険な事象に至る伝送システム上の障害として，情報の誤り，時間的な誤り（遅延，順序の逆転など）を想定し，6 つの防護対策（“protective measure”）を要求するとともに，安全性を確保・確認するための手続きなど 18 の要求項目を定義している。

本パートの目次構成は以下のようになっている。

1. 適用範囲
2. 参照規格
3. 定義
4. 参照アーキテクチャ
5. 伝送システムの特性と安全プロシージャとの関係
6. 安全プロシージャに関する要求事項
7. セーフティコードに関する要求事項

Annex A（情報）．セーフティコードの長さ

なお，“Annex”は附属書であるが，附属書には，本文と同じ位置づけの「規定（normative)」と，情報提供のための「情報（informative)」の 2 種類がある。IEC 62280-1, -2 とも，Annex は全て「情報」である。

2.2.2 IEC 62280-2（open transmission system）

IEC 62280-2 は，“open transmission system”を利用して安全に関わる情報を伝送する場合に考慮すべき事項と要求事項を定義しているパートである。“open transmission system”は，次のように定義されている。

「未知で可変かつ信用できない性質をもち，ユーザー数が不定で，許可されていないアクセスのリスクを評価すべき伝送システム」

すなわち，使用者が限定できず，通信システムの状態や通信路に流れている情報を完全には把握することができない伝送システムが“open”である。具体例としては，列車無線・無線 LAN・携帯電話などの無線伝送，有線の公衆網，インターネットなどが該当する。

このパートでは，危険な事象に至る伝送路上の障害として 7 つの脅威（規格原本では，“threat”＝スレットという単語で示されている）を定義し，それらの脅威に対応するための要求事項や対策の考え方が示されている。

本パートの目次構成は以下のようになっている。

1. 適用範囲
2. 参照規格
3. 定義
4. 参照アーキテクチャ
5. 伝送システムに対する脅威
6. 対策のための要求事項
7. 脅威に対する対策の適用性

Annex A（情報）．対策ガイド
Annex B（情報）．参考文献
Annex C（情報）．本規格の利用ガイド
Annex D（情報）．オープンな伝送システムに対する脅威

IEC 62280-2 は，現在鉄道において開発・導入が進められている無線式列車制御システムの無線通信ネットワークを設計・構築するうえで非常に重要かつ有用な規格である。次章では，IEC 62280-2 の目次構成に沿って，その概要を紹介する。

3．IEC 62280-2 の概要

3.1 第 1 章 適用範囲，第 2 章 参照規格，第 3 章 定義

第 1 章は，IEC 62280-2 を適用する範囲（“Scope”）を定義する章であり，2.1 節で述べた本規格の目的が明確に示されている。なお，以下については規定しないことも記載されている。

・オープンな伝送システムとは何か
・オープンな伝送システムに接続される装置とは何か
・解決方法
・どのような種類のデータが安全関連か否か

IEC 62280 だけでなく，規格一般に言えることであるが,「規定されていないこと」あるいは「規定がないこと」を明確に示すことも規格文書の重要な役割である。

第 2 章は, 本規格とともに参照されるべき規格として，次の 2 つの規格が挙げられている。

IEC 62278：　鉄道分野－信頼性, アベイラビリティ，保全性，安全性（RAMS）の仕様と実証

ENV 50129：鉄道分野－信号用安全関連電子システム

ENV 50129 は，信号システムの安全性に関する国際規格 IEC 62425 の基となった欧州規格案である。IEC 62280-2 が発行された当時はまだ国際規格化されていなかったため，欧州規格案が引用されている。現在行われている改訂作業（本稿の 4 章で詳述）では，IEC 62425

に修正される予定である。

第 3 章では，IEC 62280-2 の本文中で使用されている，アクセス保護や，認証，メッセージ，プロセス，即時性，正当性，といった 67 の用語が定義されている。

3.2 第 4 章 参照アーキテクチャ

第 4 章では，IEC 62280-2 が対象とするシステムの基本的な構成が定義されている。図 1 は，IEC 62280-2 に掲載されている Fig. 1 を翻訳したものである。図 1 中の「安全関連装置」は，連動装置や無線式列車制御システムの拠点装置・車上制御装置などの装置である。安全関連装置間で安全に関わる情報を，オープンな伝送システムを使って伝送するために必要となるプロセスが「安全関連伝送システム」であるとしている。このプロセスには，伝送プロセスとアクセス保護プロセスの 2 つがあり，それぞれ，伝送エラーに対する防御と，不正なアクセスに対する防御を行う。

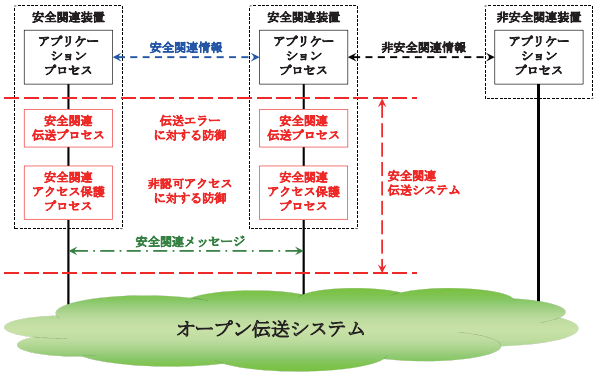

図 1　参照アーキテクチャ

3.3 第 5 章 伝送システムに対する脅威，第 6 章 対策に対する要求，第 7 章 脅威に対する対策

まず第 5 章では，伝送システムに対する脅威として，表 1 に示す 7 つの事象を定義している。そして，第 6 章では，表 1 に示した 7 つの脅威によるリスクを軽減するため，アプリケーションが必要とする範囲で，伝送システムが「メッセージの認証，一貫性，即時性，連続性」をサービスとして提供することを要求している。さらに，脅威に対する防御法として，シーケンス番号やタイムスタンプ，タイムアウト処理，送受信 ID の付加，フィードバックメッセージ，端末認証，セーフティコードや暗号化技術の利用などを挙げている。

表 1　オープンな伝送システムに対する脅威

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・ユーザーが認証されているかのように見える

規格本体の最後の章である第 7 章では，脅威と対策との関係をマトリクスとして示している。このマトリクスの概略を表 2 に示す。表 2 中，○は規格上では特に条件なく効果ありとされているもの，△はマトリクスの注記によって条件つきで効果ありとされているものである。

表 2　脅威と対策のマトリクスの概略

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					△	△		○

3.4 Annex A ～ D（附属書）

IEC 62280-2 に添付されている 4 つの Annex は，全て情報提供のための文書である。Annex A では，安全符号（safety code）と安全関連メッセージのタイプに応じた安全符号の選定方法に関する情報が提供されている（表 3）。表 3 中の「メッセージタイプ」の分類（Type A0, A1, B0, B1）は，規格での記述がやや複雑なためやや理解しにくいが，メッセージタイプごとの伝送ルートやメッセージのフォーマットの違いを図示すると図 2 のように表すことができる。図 2 に示したように，伝送ルートによってユーザーデータが平文でよいか否かが，また不正なアクセスを排除できるか否かによって暗号化の要否が分かれている。

Annex B では，情報セキュリティ技術に関する規格群（ISO/IEC 9796, 9797, 10116, 10118, 11770 など）と暗号化符号に関する論文等が，参考文献として挙げられている。Annex C では，伝送システムのタイプが 7 段階に分類されており，各タイプごとに発生しうる脅威が例示されている。最後の Annex D では，伝送システムにおけるハザードと，表 1 に示した 7 つの脅威との関係がマトリクスとして示されている。

表 3　セーフティコードとメッセージタイプの対応

種類	参照規格	安全関連伝送システムにおけるメッセージタイプ			
		A0（平文）	A1（平文）	B0（全暗号）	B1（追加情報）
CRC符号*	---	推奨	不適	使用不可	推奨
MAC**	ISO/IEC 9797	推奨	強く推奨	推奨	推奨
ハッシュ符号	ISO/IEC10118	推奨	不適	強く推奨	強く推奨
デジタル署名	ISO/IEC 9797	推奨	推奨	推奨	推奨

*) CRC＝Cyclic Redundancy Check（巡回冗長検査）
**) MAC＝Message Authentication Code（メッセージ認証コード）

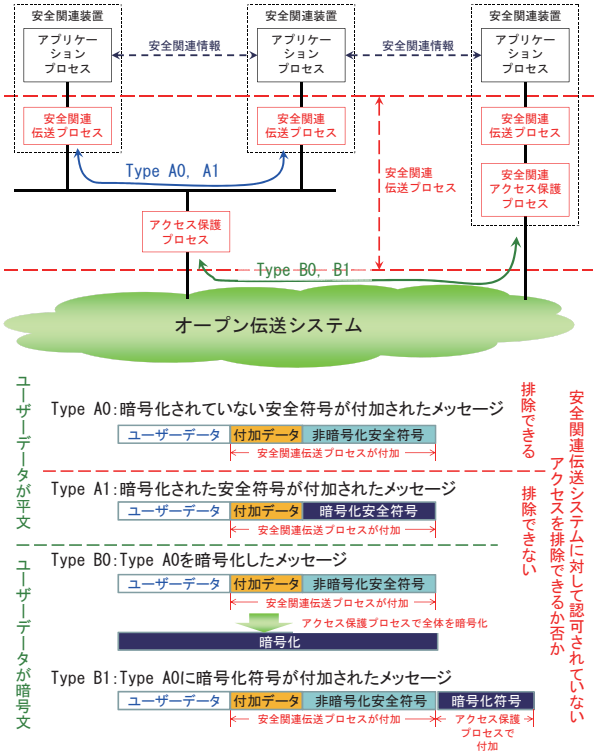

図２　メッセージタイプ（Type A0,A1,B0,B1）の定義

４．IEC 62280 の改訂

4.1　改訂の手続きと経緯

IEC 62280 に限らず，IEC・ISO から発行されている全ての IEC 規格は，一定期間ごとに内容が見直され，①そのまま存続する，②内容を改訂する，③廃棄する，のいずれかが選択される。これは，技術の進歩や利用者のニーズ，あるいは社会的な要求に対して，規格が陳腐化したり，新しい技術の普及の足かせとなることのないよう，規格を保全するための作業である。この作業は「メンテナンス」と呼ばれ，規格審議機関にとっては新しい規格の提案・作成と同様に重要なミッションである。

IEC 62280 は，欧州規格である EN 50159 をベースに作成された規格である（ほぼ内容が変更されずに発行された）。この EN 50159 が 2010 年 10 月に改訂され，IEC 62280 自体もメンテナンスの時期が到来したことから，2011 年 9 月に IEC/TC9（鉄道用電気電子機器，システムを扱う専門委員会）が改訂を行うことを決定し，2012 年 4 月に最初の改訂案（委員会原案：“CD”と呼ばれる）が提案された。本稿を執筆している時点では，CD に対する各国からの意見を改訂案に反映する作業を行っており，今後，以下のような手続きが予定されている。

2013 年 5 月 委員会投票原案（CDV）に対する国際投票

2014 年 4 月 最終原案（FDIS）に対する国際投票

2014 年 11 月 改訂版発行

なお，CD に対して大きな修正意見が出されていないことから，上記の予定よりも若干早めに改訂版が発行される可能性もある。

4.2　IEC 62280 の改訂案

今回の改訂における最も大きな変更は，パート 1 とパート 2 が統合され，1 本の IEC 62280 となる点である（表 4）。これに伴い，“closed”と“open”の大きく 2 つに分けられていた伝送システムは，3 つのカテゴリーに再分類されている（表 5）。ただし，伝送システムに対する脅威や対策の考え方など，技術的な内容については大きな変更は提案されていない。今回の改訂では，内容の刷新ではなく，パート 1 とパート 2 で重複していた部分を統合し，構成を見直すことによってより使いやすい規格に改善することが大きな目的となっている。

表４　改訂案の章構成と現行規格との対応

	改訂案の章構成(CD段階)	現行規格の該当する章 Part 1	Part 2
規定	1. 適用範囲	1.	1.
	2. 参照規格	2.	2.
	3. 用語・定義	3.	3.
	4. 参照アーキテクチャ	4.	4.
	5. 伝送システムに対する脅威	---	5.
	6. 伝送システムの分類	4.	Annex C.
	7. 対策のための要求事項	5. , 6. , 7.	6. , 7.
情報	Annex A. オープン伝送システムにおける脅威	---	Annex D.
	Annex B. 伝送システムのカテゴリ	---	Annex C.
	Annex C. 対策ガイド	Annex A.	Annex A.
	Annex D. 本規格の利用ガイド	---	Annex C.
	Annex E. 前規格からの変更点	---	---

表５　伝送システムの分類の改訂案

現行規格での分類	改訂案での分類 カテゴリ	主な特性	例
Closed	1	・全ての性質が不変 ・既知で最大数が固定のユーザーのために設計されている ・不正アクセスの機会は無視できる	・密結合の伝送（Balise等） ・システム内シリアルバス（PROFIBUS，CAN等） ・単一システム内のLAN
Open	2	・性質が，未知，部分的に未知，又は可変 ・ユーザーグループの拡張範囲に制限 ・不正アクセスの機会は無視できる ・まれに信頼できないネットワークを使用	・限定されたエリア内のLAN ・公衆回線交換網 ・公衆網における固定のP2P借用回線 ・アクセスが限定される無線システム（LCXなど）
	3	・性質が，未知，部分的に未知，又は可変 ・未知で複数のユーザーグループが使用 ・不正アクセスの機会がかなりある	・公衆パケット交換網 ・インターネット ・回線交換型デジタル無線（GSM-R等） ・パケット交換型デジタル無線（GPRS） ・短距離放送型無線（Wi-Fi等） ・制限のない無線システム

５．おわりに

本稿では，安全に関わる情報を伝送する通信システムに関連する国際規格として，IEC 62280 をとりあげ，概要と改訂の動向を紹介した。2002 年に発行された IEC 62280-1, -2 の両規格は，保安システムで通信を利用する際に非常に重要かつ有効な情報が記載されているが，必ずしも理解が容易な内容ではない。今後の改訂により，より理解しやすく，また使いやすい規格になることが期待される。