CBTC開発・導入における
国際規格の活用について

交通システム研究部　主席研究員　長谷川智紀
（前 鉄道認証室　主席研究員）

講演内容

1. 鉄道認証室の生い立ち
2. CBTCの特徴
3. 無線化による検討事項
4. 国際規格と規格適合
5. CBTCに適用される規格（例）
6. CBTCに適用される規格が求めること
7. 規格を活用することの利点
8. まとめ

1．鉄道認証室生い立ち

2008年6月 交通政策審議会 鉄道部会による提言
「今後、我が国の製品の国際規格への適合性評価のあり方を検討する必要がある。」

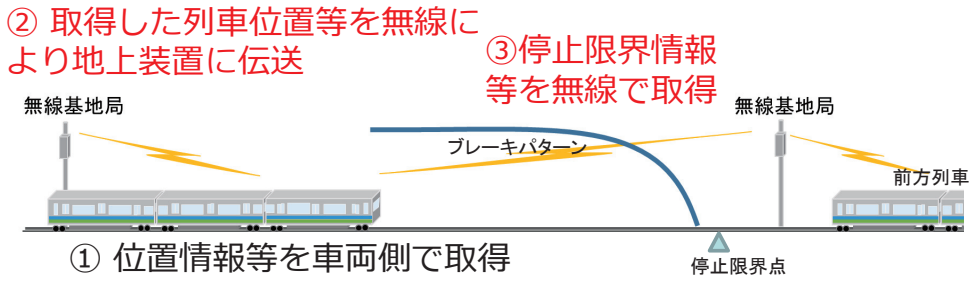
2012年9月 我が国初の鉄道分野の製品認証機関として認定を取得
（認定対象規格IEC 62425）

2016年9月 2規格の認定を取得
（認定対象規格IEC 62279、IEC 62280）

2018年5月 かねてより要望の多かったIEC 62278（RAMS）の認定を取得

2021年4月 認証対象のRAMSライフサイクルを第9Phaseまで拡大
（認定取得のためのプレ認証案件の申請待ち）

2．CBTCの特徴



<u>無線通信を使うことが特徴</u>

いままでの信号システムでは、
保安情報は、<u>有線</u>による、<u>1対1通信</u>か<u>クローズドネットワーク</u>
ただし、レール・車上受電器間や、地上子・車上子間は<u>近接通信</u>のため、意図的な攻撃等については考慮していない。

オープンエリアにおける無線通信による保安情報を送受

3．無線化による追加検討事項

無線化に伴う新たに検討すべき事項例

- データの連続受信
- データの消失
- データの挿入
- データの順番の変更
- データの破壊
- データの遅延
- データの偽装
- データが受信できない
- 他者にデータを受信される
- データの正確性　　他

検討すること多数！！
どこまで、検討しておけばよいか？
説明責任はどのようにすれば果たせるか！？

4．国際規格と規格適合

○PL指令※への対応

※PL指令：欠陥製造物に対する賠償責任に関する加盟国の法律、規制及び行政規定の等質化についての欧州諸共同体（EC：European Communities）閣僚理事会指令

以下のいずれかをメーカが立証できた場合、メーカが製造物責任を問われない。

a.流通させなかったこと
b.流通時点では欠陥がなかったこと
c.販売目的で製造された物でなかったこと
d.規制当局の指示で欠陥が発生したこと
e.当時の科学・技術的水準では、欠陥の発見は不可能だったこと（開発危険の抗弁）
f.部品の場合、完成品側の設計に欠陥があったこと

機能安全規格である
IEC 61508へ適合することで対応

4. 国際規格と規格適合

○機能安全規格とは、

技術仕様規格 → 試験により規格適合を証明
例：環境規格等

機能安全規格

技術的機能：安全性の技術的な達成
組織的機能：安全性達成業務のマネジメントの遂行

→ 両機能による安全性達成

各種証拠文書が
規格に適合していることを証明
ex. IEC 61508,IEC 62425

→「認証」による証明

5. CBTCに適用される規格（例）

• 技術要件	IEEE 1474、IEC/TS62773
• 機能安全	IEC 61508、IEC 62425
• RAMS	IEC 62278
• ソフトウェア	IEC 62279
• 通信	IEC 62280
• セキュリティ	IEC 62443

→ 通信とセキュリティで何が求められるか？

6．CBTCに適用される規格が求めること

IEC 62280と情報セキュリティの要素との比較

	情報セキュリティ	IEC 62280
機密性	○	× 情報の機密性を求めていない
完全性	○	○ 削除、挿入、破壊
可用性	○	× 脅威に対する対策のため
真正性	△	○ なりすまし
責任追跡性	△	×
否認防止	△	×
信頼性	△	○ 重複、順序誤り、遅延

○：維持を求める　△：維持を求めることができる　×：維持を求めていない

6．CBTCに適用される規格が求めること

○安全対策と情報セキュリティ対策の違い

安全対策

- 一度対策を行えば、システムの変更を行わない限り、継続的に有効
- その対策システムが故障した場合、当該機器等の交換を行うことにより対策の効果を復元することが可能

情報セキュリティ対策

- 一度脆弱性として確認された場合、その対策は有効ではなくなる
- システムの状態変化が生じる際、第三者による介入の余地が生じる可能性が出る
- セキュリティ対策を設計した時点に比べ、攻撃者側の攻撃力の強化が想定される

- Operation & MaintenanceやIEC 62278のRAMSライフサイクルの観点に加え、セキュリティ対策の機能維持を継続的に行うことが重要
- 悪意を持った通信設定の改変などの脅威へのセキュリティ対策も必要

6．CBTCに適用される規格が求めること

○ IEC 62280で検討が求められていること

- 通信環境の把握と、SILに基づく通信におけるリスクの対策

Table 1 – Threats/defences matrix

Threats	Defences							
	Sequence number	Time stamp	Time-out	Source and destination identifiers	Feed-back message	Identification procedure	Safety code	Cryptographic techniques
Repetition	X	X						
Deletion	X							
Insertion	X			X [a]	X [b]	X [b]		
Re-sequence	X	X						
Corruption							X [c]	X
Delay		X	X					
Masquerade					X [b]	X [b]		X [c]

[a] Only applicable for source identifier.
Will only detect insertion from invalid source.
If unique identifiers cannot be determined because of unknown users, a cryptographic technique shall be used, see 7.3.9.

[b] Application dependent.

[c] See 7.4.3 and Clause C.2.

その対策が十分かの検討したエビデンスが必要

ex.　CRCを32bit→32bitで十分である理屈は？
　　シーケンスナンバーを3桁→3桁で十分である理屈は？

6．CBTCに適用される規格が求めること

○車上主体型列車制御システムにおける情報セキュリティ対策

IEC 62280

- 鉄道の安全関連装置の設計時に検討すべき性能については記述されているものの、その性能の維持に関する要求事項は見受けられず

JIS Q 27001・IPAガイドライン

- JIS Q 27001や、IPAのガイドラインでは、情報セキュリティへの対策のみならず、情報セキュリティへの取組として、製品のライフサイクルを「企画」「開発」「運用」「廃棄」のフェーズ毎の取組方針を定めることが望まれている

IEC 62280 に追加

- ライフサイクル全般にわたる、情報セキュリティ性能を維持するための計画、マネジメントシステムの策定
- 第三者及び内部からの攻撃を受けた際の対策の検討、具体的には、その事象及び状況の記録、解析方法及び対処方法の検討とその実行及び評価
- ライフサイクル全般を含めたセキュリティ対策の検討、実行及び評価（管理も含む）
- 運行開始、運行中（システム間ハンドオーバーも含む）、運行停止及びシステム更新時等各状態における情報セキュリティ上のリスクと対策の検討
- 策定された計画に基づく活動の実施及び評価

7. 規格を活用することの利点

- 最低限検討すべき事項が示されている
  →具体的な対策が示されているわけではないため、技術的な対策検討は必要
  →導入先の安全に関する考え方等を事前に調査・検討は必要
- （海外では）PL法の説明責任を果たしたことになる
- 同じ視点で説明されるので比較がしやすい
  →検討事項が同じように整理されるため、他者との比較が可能
- 第三者による認証制度が利用できる
  →規格適合状況を、第三者機関に委ねることが可能

8. まとめ

- 既存の信号システムと、CBTCの違いについて説明
- 国際規格への適合は、説明責任を果たすにあたって、有効なツール
- 通信の規格はセキュリティ規格の完全性への対策のみ
- CBTCの開発に当たっては、今までの安全性に通信への対策を加えるとともに、セキュリティに関するライフサイクルの考え方を加えることが有効