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

客員専門調査員　森　崇

はじめに

- 鉄道の安全を守る信号や踏切などの鉄道信号装置は、急速にネットワーク技術の活用が進んでいます。

- 通信と鉄道の安全性の関係に関する要求事項として、国際規格であるIEC 62280*があります。

- 鉄道認証室ではIEC 62280に関する規格適合性審査を行ってきました。本発表では、審査において適用される規格を活用し、鉄道信号装置の伝送システム設計におけるポイントを示します。

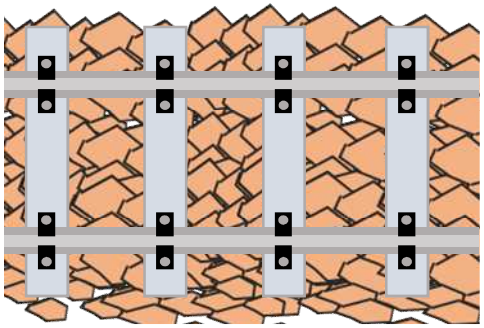
*IEC62280:2014 Railway applications – Communication, signalling and processing systems -Safety related communication in transmission systems

本日の内容

- 鉄道における「安全」担保方法
- 鉄道信号装置と通信の関係
- IEC 62280の思想を加味した設計のポイント
- 今後の重要になってくる事項

鉄道の安全確保の方法

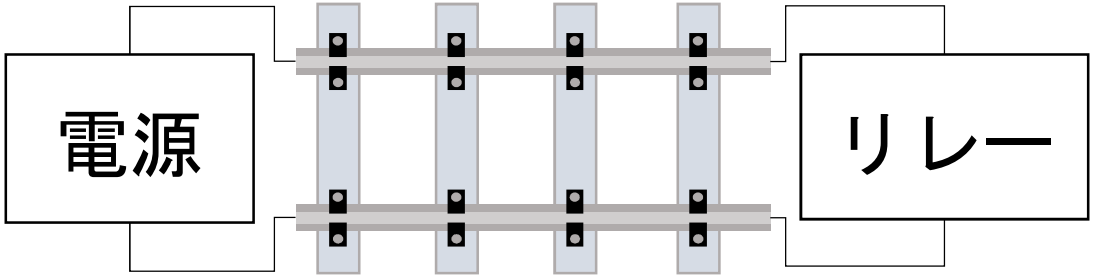
作戦1:故障しないようにする。



（レール・締結金具・枕木・バラストなど）

品質＝安全

作戦2:　故障しても安全を確保する。

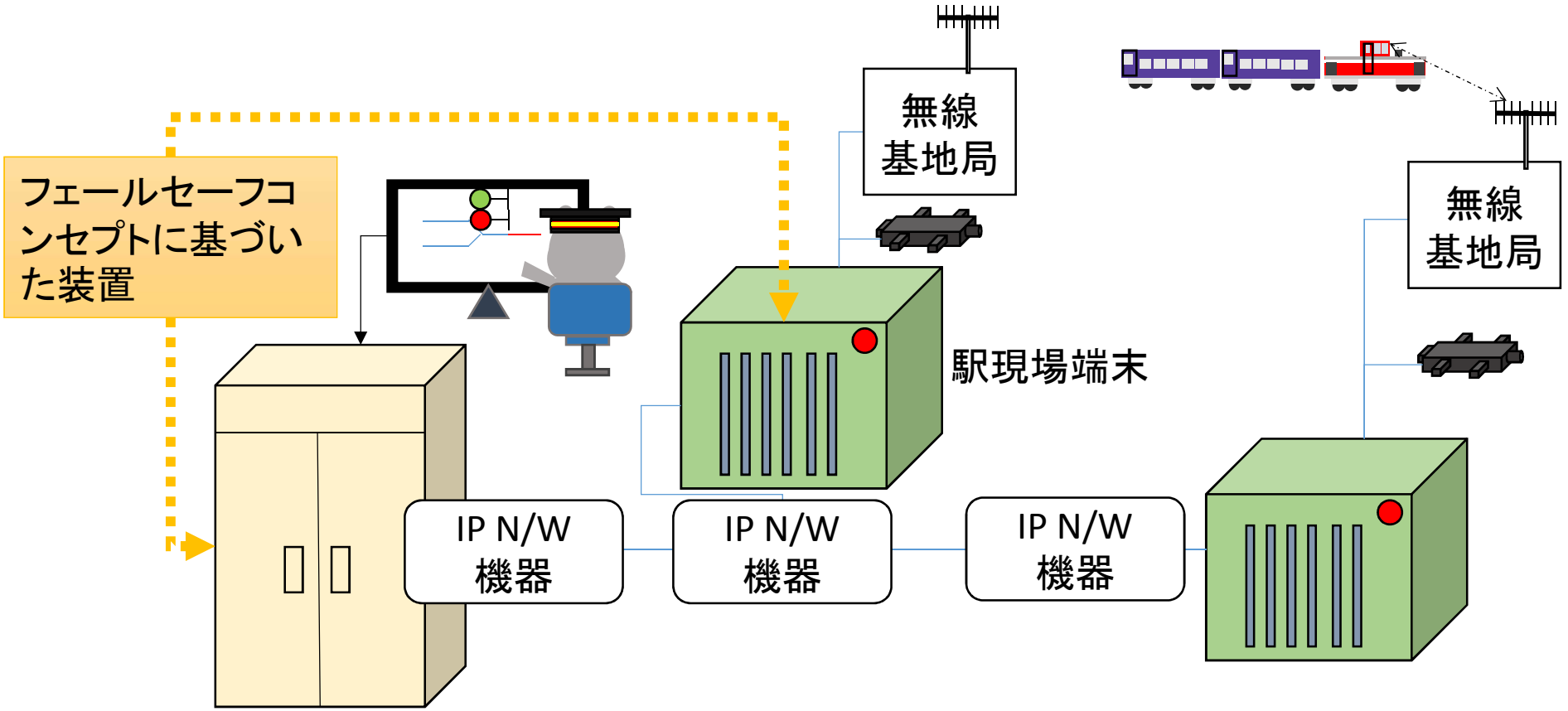


故障を想定し、その故障があっても、安全を担保する。
➔フェールセーフコンセプト

品質＝安全とは一概に言えない

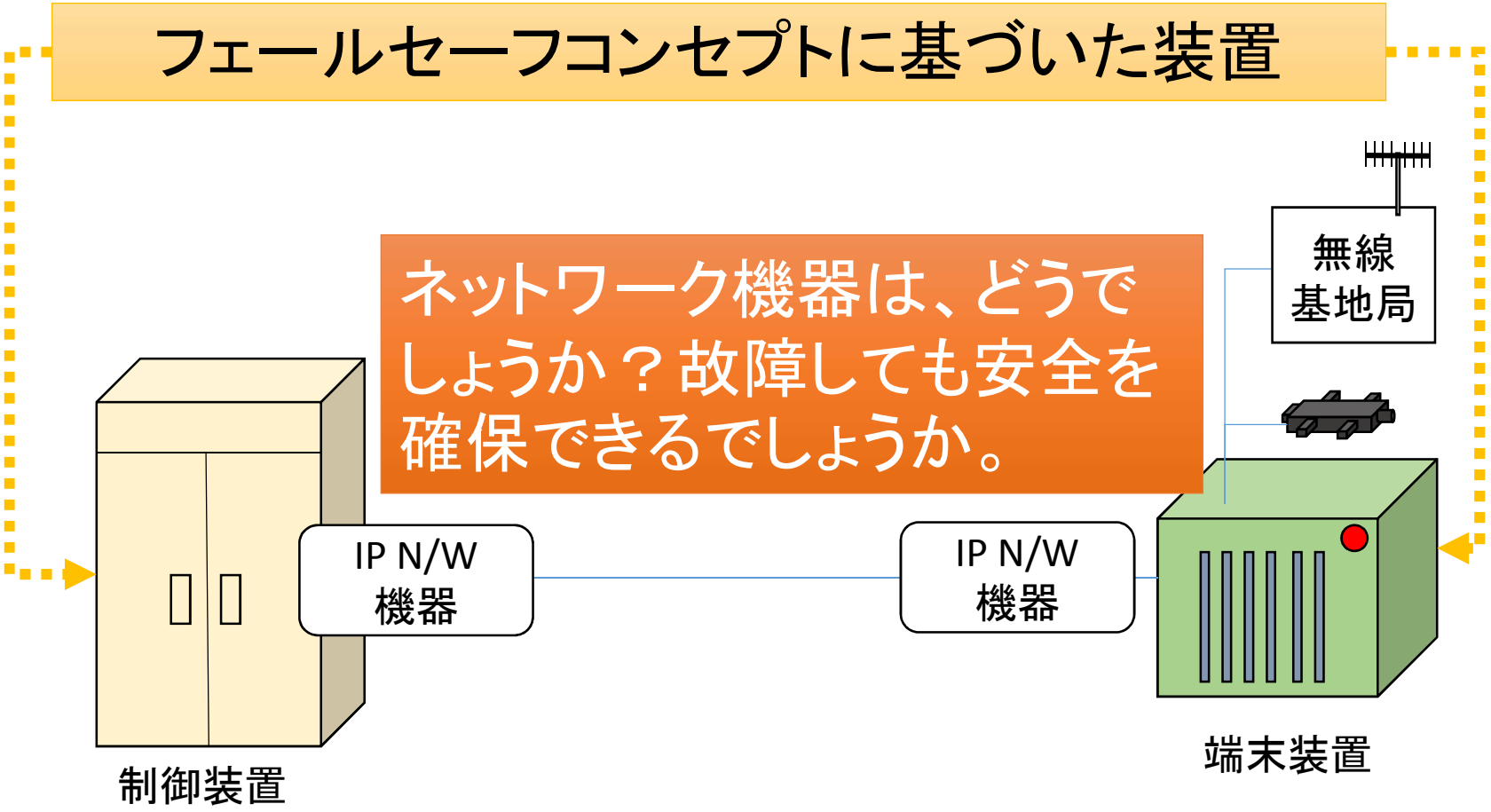
鉄道信号装置においては、基本的にはフェールセーフコンセプトを採用する。

伝送を使用した鉄道信号装置



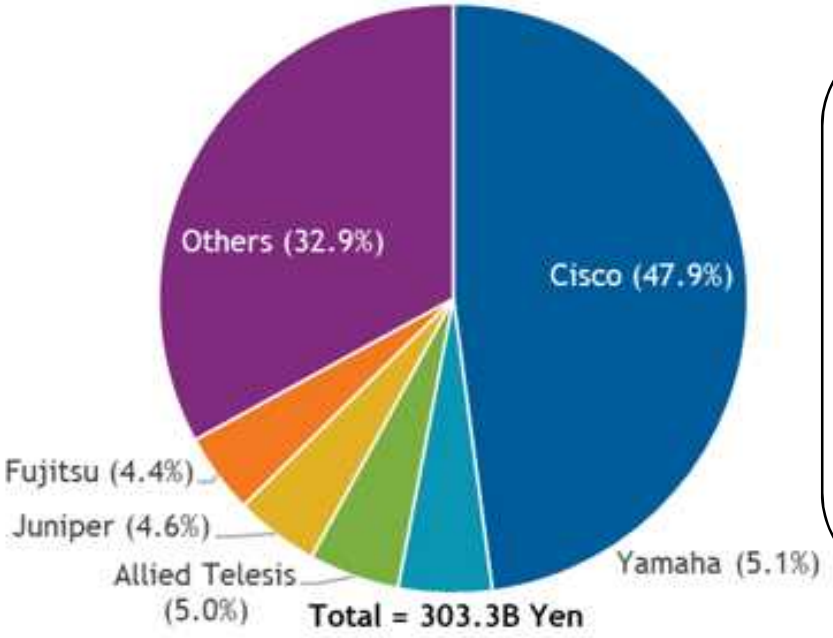
連動閉そく装置　リレー・メタル線から、電子装置＋IP、無線へ

伝送を使用した鉄道信号装置



ネットワーク機器の現実

国内ネットワーク機器市場 ベンダー別 支出額シェア実績、2018年

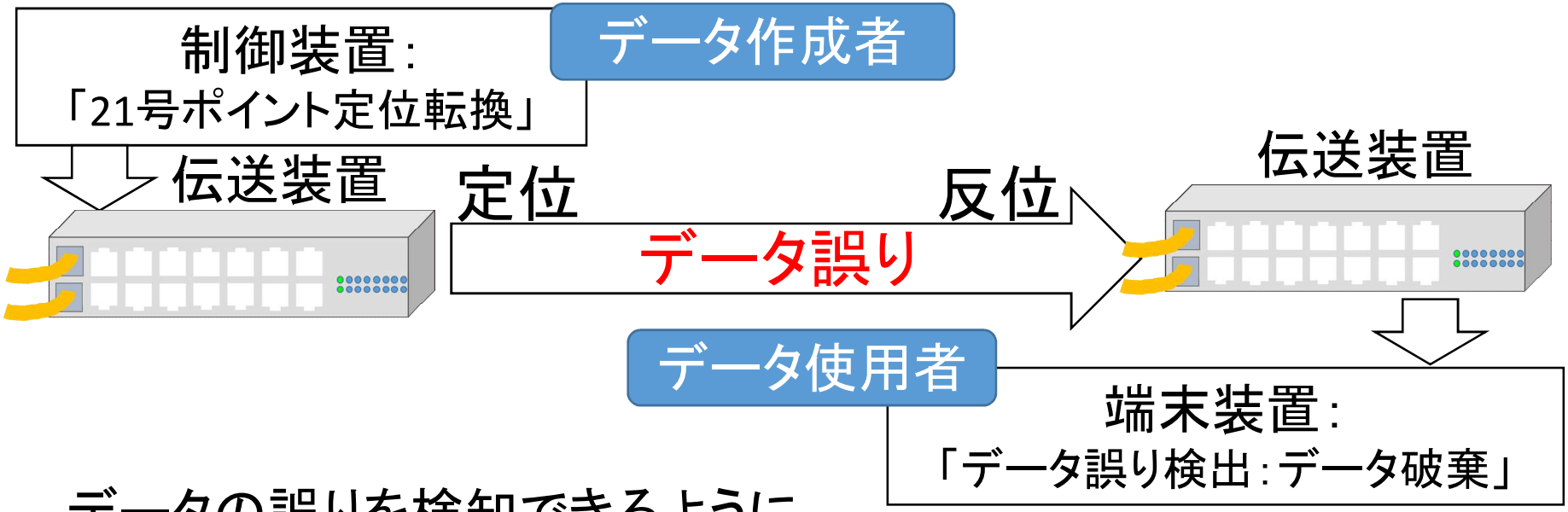


国内でも圧倒的に米国シスコ社の製品が多く、価格面や技術者の供給から考えても、鉄道でも多く活用されている現状がある。

<u>→特別な安全性を要求することは市場性からいっても困難</u>

https://www.idc.com/getdoc.jsp?containerId=prJPJ45377819

基本的な考え方：誤りは使用者で検知して対処



データの誤りを検知できるように、

- データ作成時に誤り検出符号を作成付加し、
- データ使用時に誤り検出符号を用いてデータ誤りを検知する。

誤りの検知が失敗すると、危険な状態が見逃されるため、IEC 62280では、誤りの検定は「安全関連装置」として位置づけることになっている。

IEC 62280の示している脅威と対策の基本的な考え方

IEC 62280にある対処すべき脅威

- repetition; 繰り返し
- deletion; 削除
- insertion; 挿入
- re-sequencing; 順序入れ替え
- corruption; 破壊
- delay; 遅延

非人為的な脅威

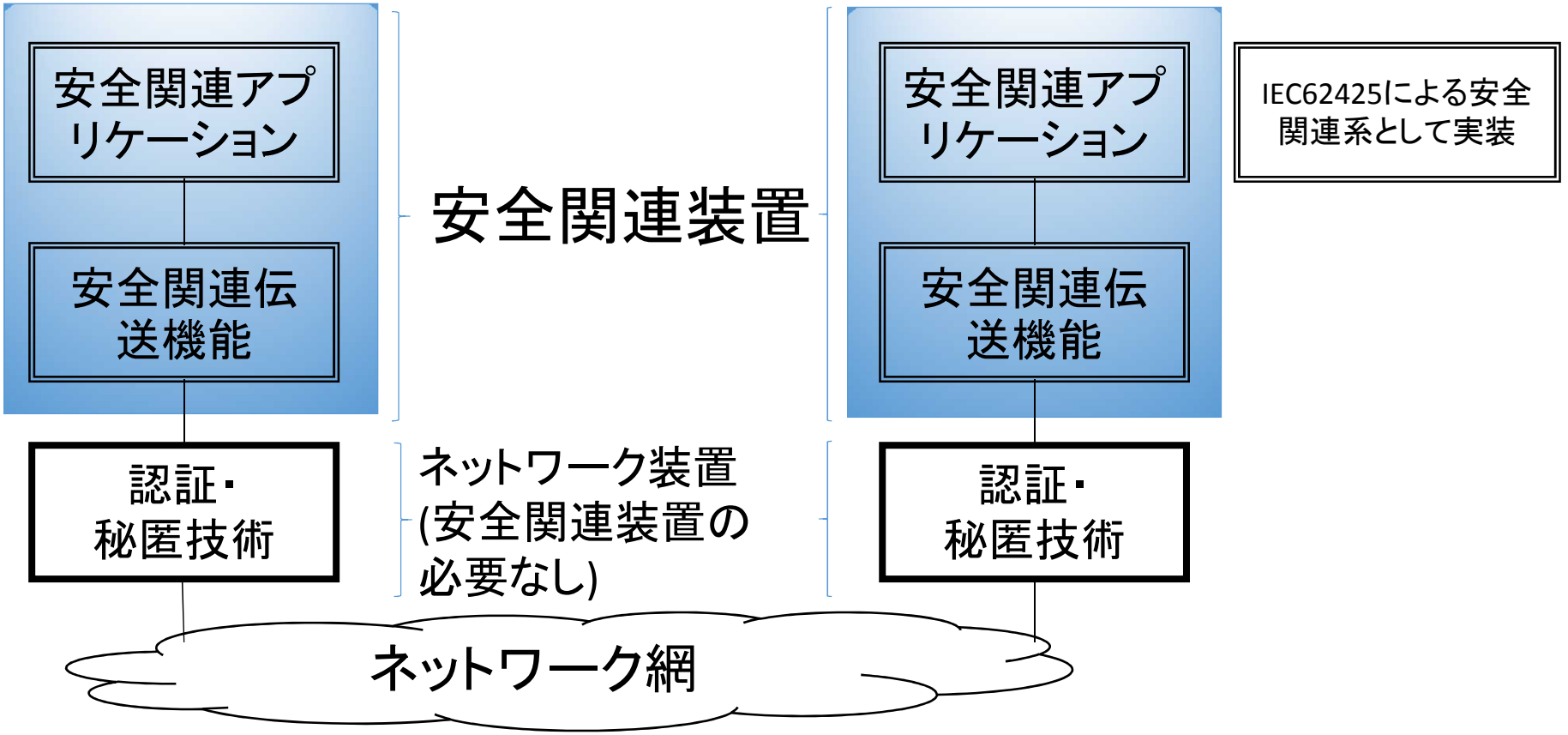
- masquerade なりすまし

人為的な脅威

がIEC 62280では7つの脅威といわれている。

IEC 62280規格に適合した一般的な構成

- figure 1にモデルがあります。



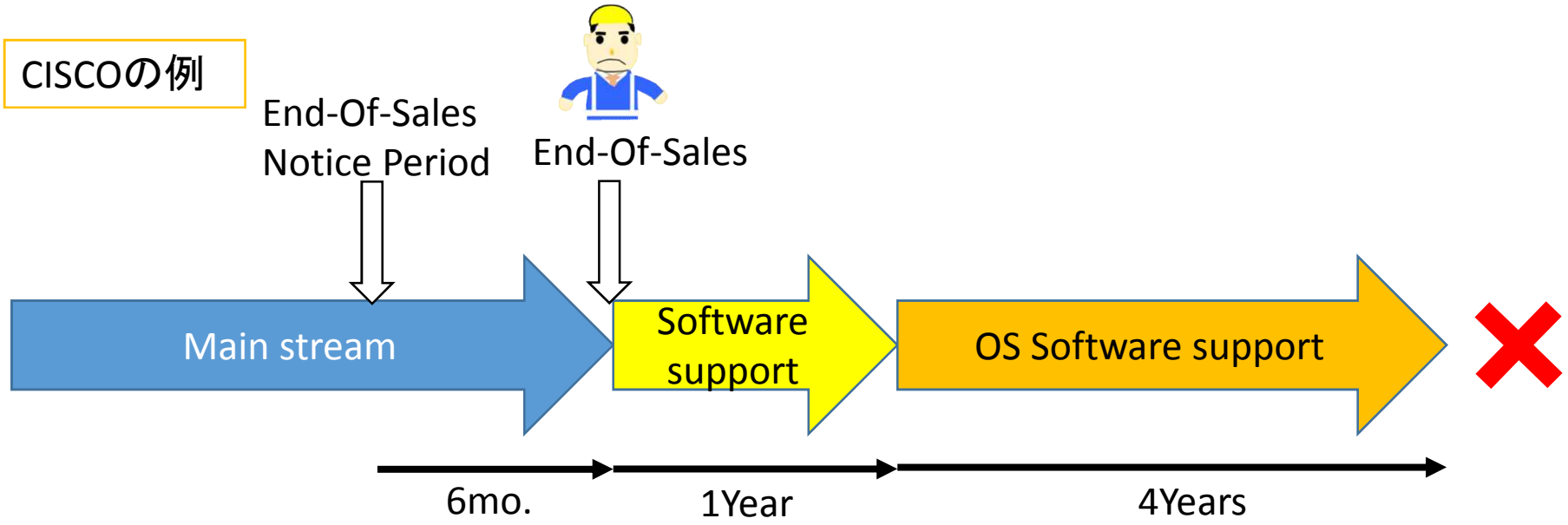
認証・秘匿技術は安全関連装置のライフサイクルと比べ短いため、別に構築してもよい。

IEC 62280の基本的な安全への考え方

- ネットワーク装置は、汎用品を使ってもよいです。
- 伝送データが誤るのでそのデータを使う・使わないは、使う方で判断してください。
- 判断する部分は、失敗すると大変だから、保安装置として位置づけてください。
- 誤ったとき、どんなハザードがあるかは、しっかり確認して、データを使う方で対策してください。

通信装置の現実　ライフサイクルの違い

CISCOの例



鉄道信号装置はおおむね20年以上程度使用することを考えると、セキュリティーに課題がある状態で使用し続けるか、ネットワーク機器の更新が必要。

セキュリティーに脆弱性があるまま、使い続けるというのはかなり問題があるため、ネットワーク機器を取り換えやすい構成にしておくことが必要！

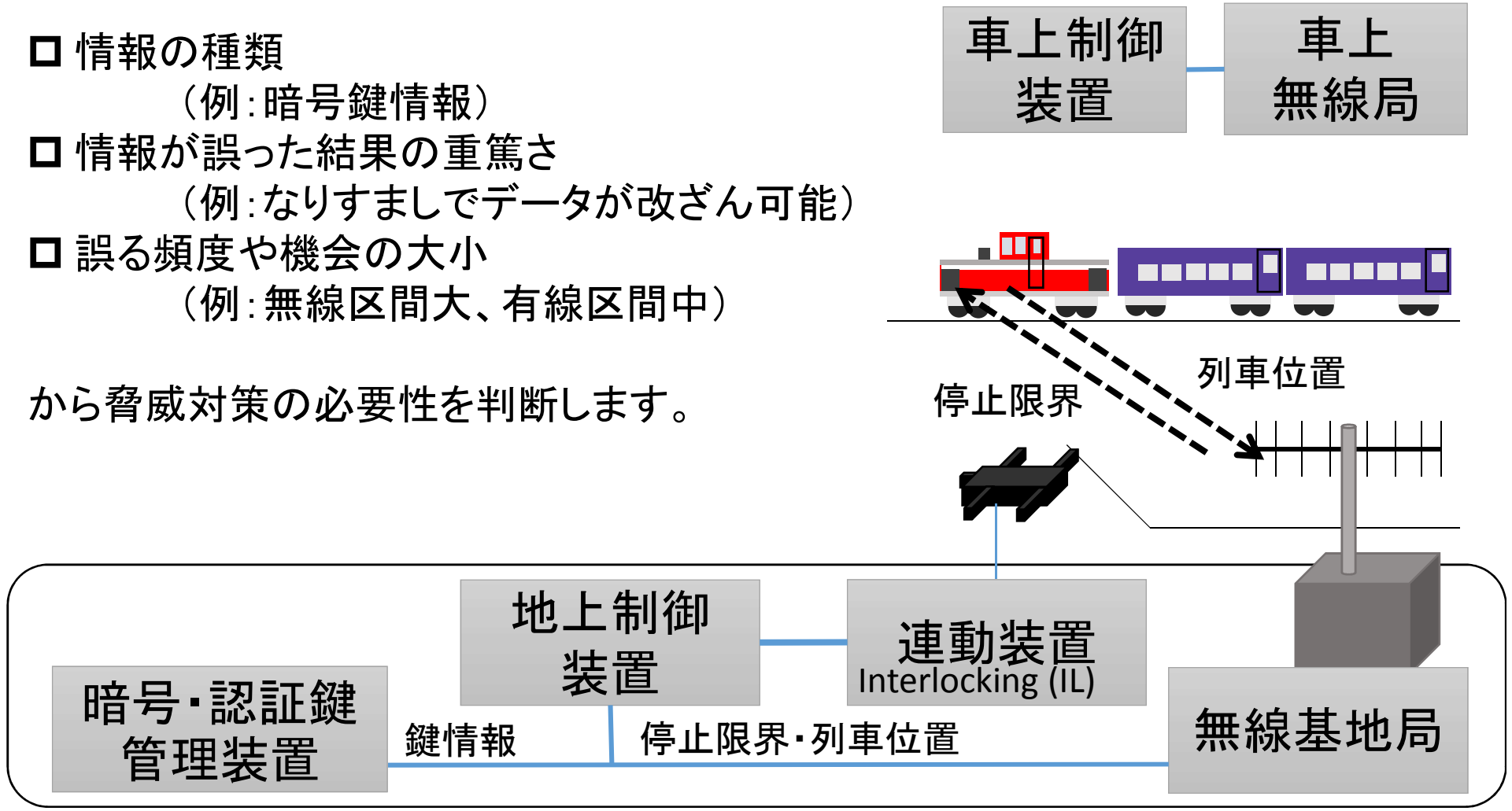
IEC 62280と実際のネットワーク設計のポイント

IEC 62280　Annex　D　"Guidelines for use of the standardを中心に

ハザードの解析

- 情報の種類
  （例：暗号鍵情報）
- 情報が誤った結果の重篤さ
  （例：なりすましでデータが改ざん可能）
- 誤る頻度や機会の大小
  （例：無線区間大、有線区間中）

から脅威対策の必要性を判断します。



リスクの低減

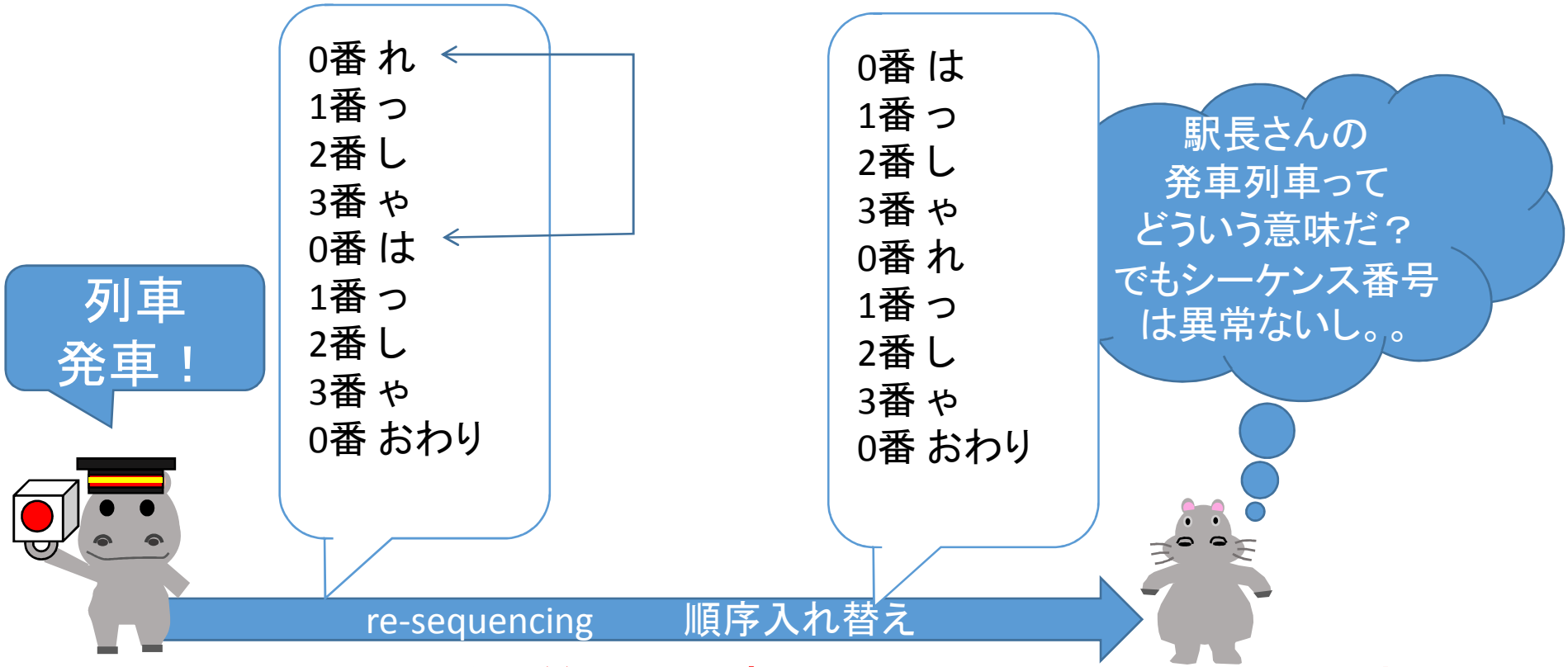
IEC 62280における脅威と低減手法

	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

低減させると決定した脅威は上記低減手法から選択することになりますが、低減手法の強度の検討が必要です。

脅威対策の強度の検討

「順序入れ替えの脅威対策のために、シーケンス番号を導入します」



シーケンス番号など対策には、考えられる誤りに対応した強度（冗長符号長など）が必要です。

なりすましにおける低減手法

	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

認証や暗号技術を低減手法としてあげてられているが、具体的にはどのような方法をとるかが重要である。

なりすまし(人為的な脅威)への対応について

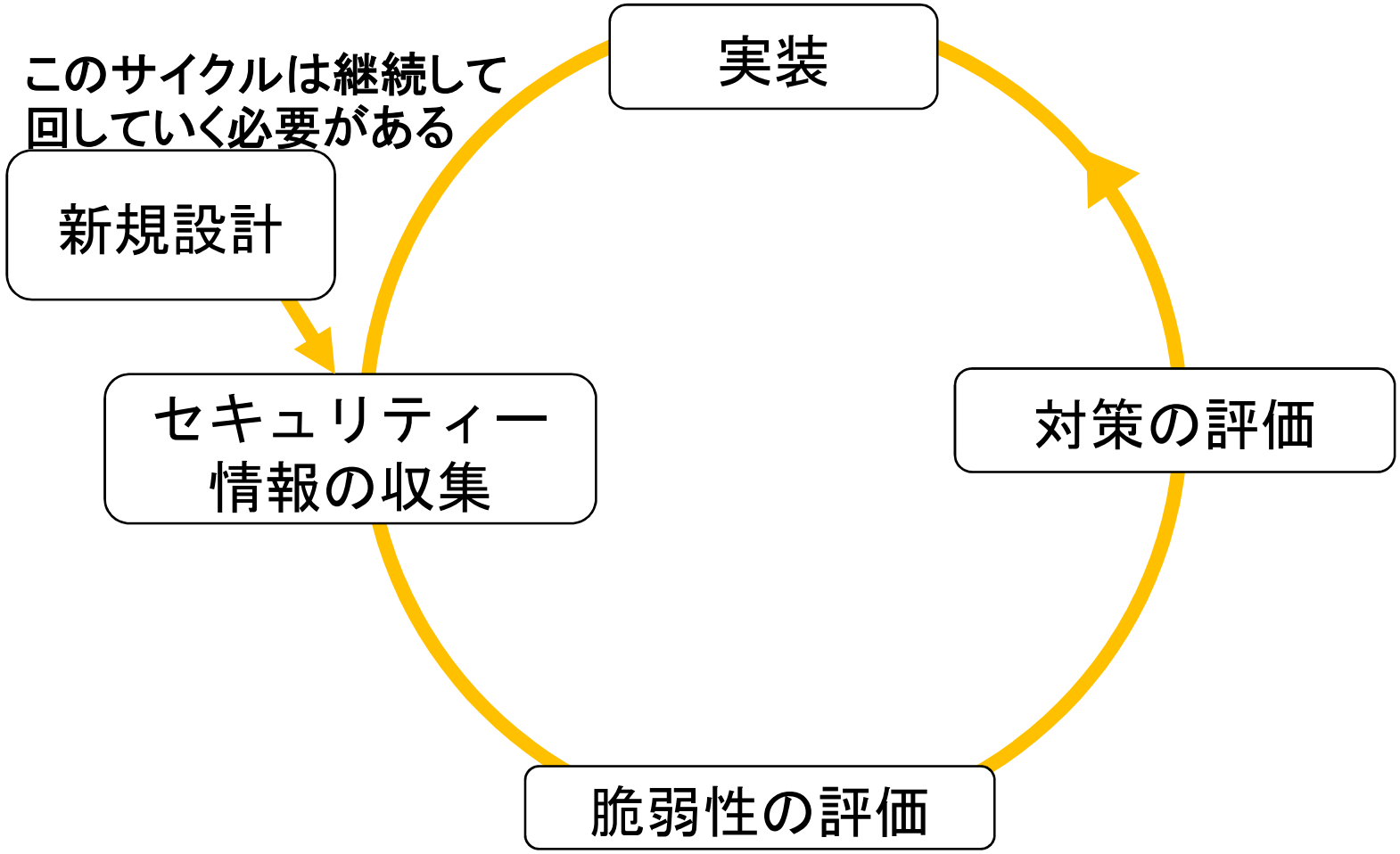
- IEC 62280はなりすまし対策についてはほぼ記述されていない。

→一部の暗号アルゴリズム（ECB）の使用制限が述べられているのみであり、
Well-known and well-tested algorithms such as [FIPS PUB 197] are recommendedと書かれているだけである。

（常識的な線で対応する）

対策の継続的な見直し

安全は、システムの変更があったときにインパクトアナリシスと対策評価を行うが、セキュリティーについては、相手先が継続的に進化していくため、安全ライフサイクルで使用するVモデルでは語れない。



終わりに

- 信号保安装置におけるデータ伝送について、講演概要の内容を踏まえ、ポイントを示させていただいた。
- IEC 62280においては、信号保安装置に使用するデータ伝送における留意点を述べている。これは伝送装置自体に誤りがないことを求めるのではなく、誤りがあっても安全関連伝送機能で検出し、適切な処理をすればよいことが述べられている。
- 信号保安装置の伝送装置を設計する際、脅威を推定し、必要となる対策をとることが重要である。
- ネットワークセキュリティーは継続的なチェック&アクションが必要である。