電気学会 令和7年 電力・エネルギー部門大会
オーガナイズドセッション
「インフラストラクチャーのためのサイバーセキュリティ対策」

鉄道の運行制御システムにおける サイバー脅威と対策の考え方

公益財団法人 鉄道総合技術研究所
研究開発推進部　川﨑邦弘

Railway Technical Research Institute

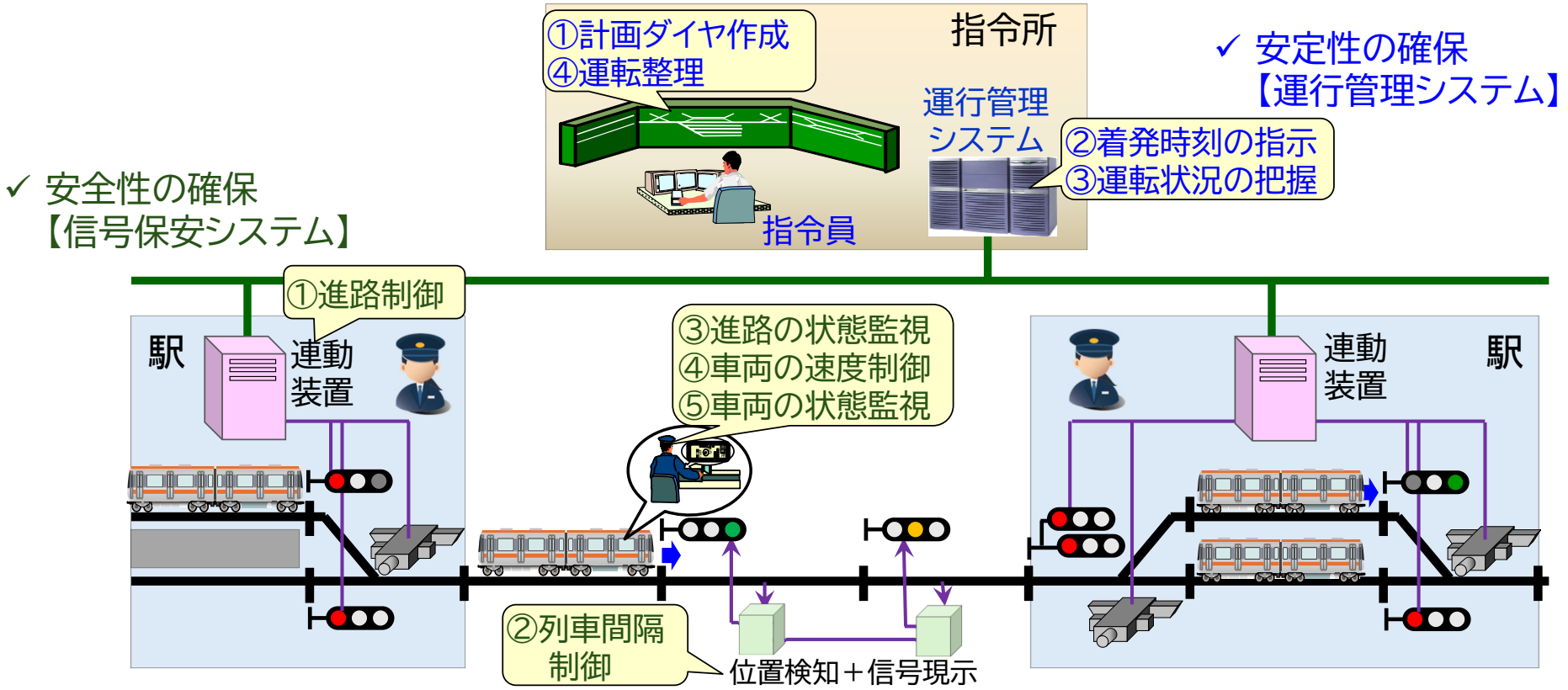
発表内容

- ◆鉄道の安全・安定運行を支えるシステム
  - ➢列車運行管理システムと信号保安システム
  - ➢電気事業との関係
- ◆列車の運行制御に係るサイバーセキュリティ
  - ➢鉄道システムにおけるサイバーセキュリティ
  - ➢列車制御システムにおいて想定される脅威と対策の考え方
  - ➢鉄道の安全性とサイバーセキュリティに関する国際標準化の動向
- ◆鉄道の将来に向けて
  - ➢将来の鉄道における情報通信の姿と課題

鉄道の安全・安定運行を支えるシステム

鉄道の最大の使命＝安全・安定輸送

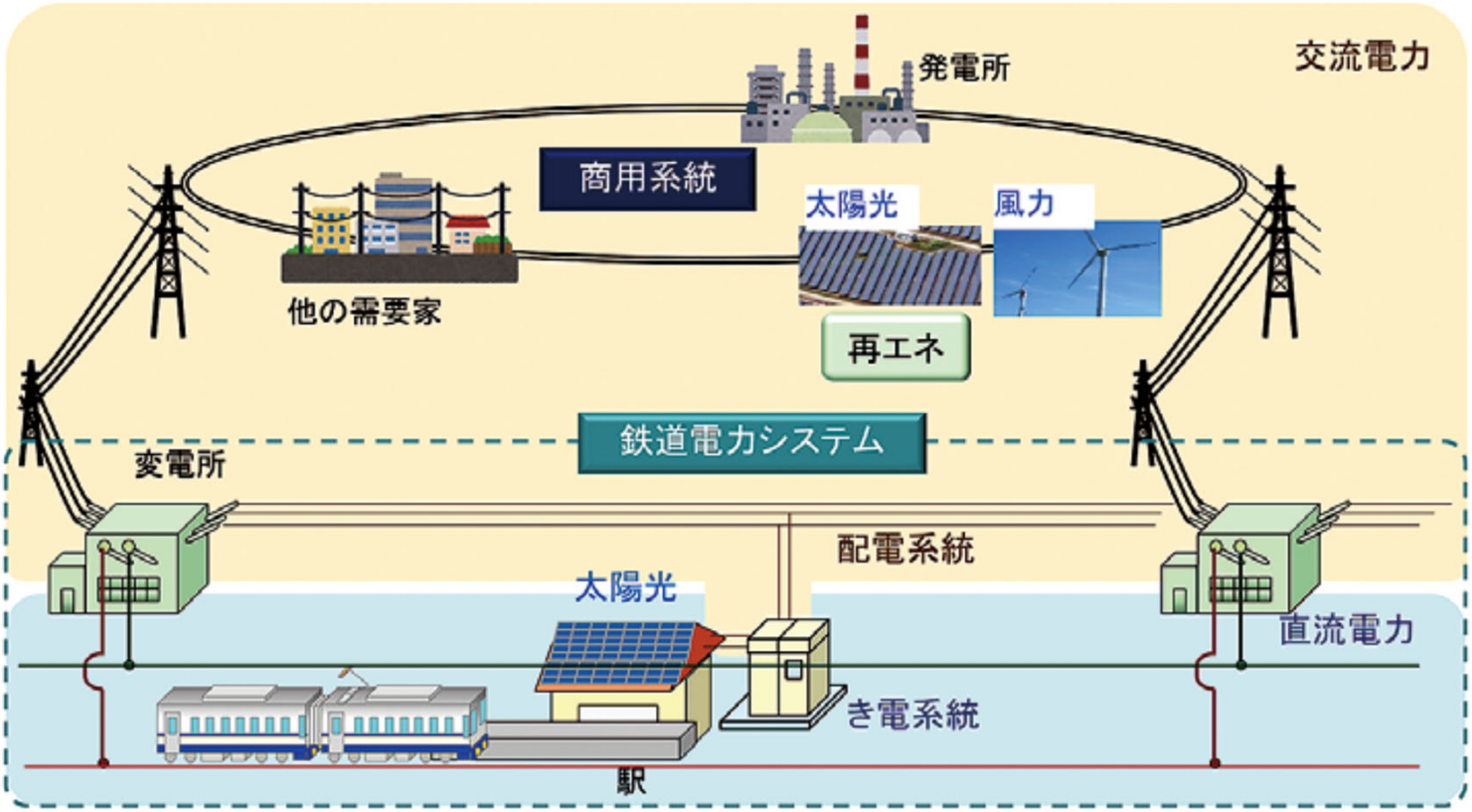
土木(構造物、軌道)、電気(電力、信号通信)、機械(車両、駅機器)、人間科学(運転)、経営(事業、サービス)などが複合した超複雑系



各種のシステム・装置が拠点・車両・線路沿線に分布、相互に連絡・連動

電気事業と鉄道事業は密接な関係

◆電気が止まれば鉄道は動けない（電気鉄道以外も：駅、信号機、踏切、通信…）
　⇔ 鉄道が止まれば電気事業に必要な人・物資が動けない



※直流電気鉄道の場合

重枝：第34回 鉄道総研講演会 要旨集 p.20 Fig.2,2021

発表内容

- ◆鉄道の安全・安定運行を支えるシステム
  - ➢列車運行管理システムと信号保安システムの概要
  - ➢電気事業との関係
- ◆列車の運行制御に係るサイバーセキュリティ
  - ➢鉄道システムにおけるサイバーセキュリティ
  - ➢列車制御システムにおいて想定される脅威と対策の考え方
  - ➢鉄道の安全性とサイバーセキュリティに関する国際標準化の動向
- ◆鉄道の将来に向けて
  - ➢将来の鉄道における情報通信の姿と課題

鉄道におけるサイバーセキュリティへの取り組み

◆サイバー攻撃による影響は既に発生

- ➢海外：列車運行や発券・サービス、一般業務などに支障が生じた事例あり
- ➢国内：列車運行に影響した例はないが、一般業務システムやWebサイトの運用に支障が生じた事例あり

◆NISC「重要インフラのサイバーセキュリティに係る行動計画」(2025改定)

- ➢以下の3システムを重要システムとして指定
  - ① 列車運行管理システム
  - ② 座席予約システム
  - ③ 電力管理システム

⇒国土交通省「鉄道分野における情報セキュリティ確保に係る安全ガイドライン」(第5版)

- ✓ 鉄道事業者に対してサイバーセキュリティ対策の水準を明示
  - ● 組織統治、情報開示
  - ● リスクマネジメント(サプライチェーン、情報共有、人材育成、モニタリング…)

鉄道におけるサイバーセキュリティへの取り組み

◆自助:鉄道事業者による自主的な取り組み

➢「安全ガイドライン」を参考に、自主的なPDCAサイクルに沿った対策

① 列車運行管理システム ⇒ 鉄道特有の対応が必要

- 運行管理システム ： 列車運行の安定性
- 保安制御システム ： 列車運行の安全性

② 座席予約システム ⇒ 基本的にはITと同じ考え方

③ 電力管理システム ⇒ 基本的には電気事業とほぼ同じ考え方

➢運行制御システムはクローズドなネットワーク＆専用に設計・製造された装置で構築

✓通信ネットワーク・回線は外界と接続されていない自営設備が基本

✓特に保安に関わる装置に関しては、安全性に関する国際規格等を整備、規格に準じて構築

✓基本的には「枯れた」技術や部品を使用

✓ICT活用やCOTS利用の進展に伴い、必ずしも“クローズド”“専用”とは言えないケースも存在

⇒ サプライチェーンの管理、外界との分離が課題

鉄道におけるサイバーセキュリティへの取り組み

◆共助:企業・分野を超えた情報共有・連携

➢交通ISAC ： 交通・運輸分野の集団防御力の向上に資する活動

✓国土交通省所管の「重要インフラ」のうち、航空・空港・鉄道・物流の4分野間での共助体制

- 2020年4月設立、現在会員数:97事業者(正会員70事業者)

✓WG活動

- セキュリティマネジメント共有WG
- IT-OT連携WG
- 事例共有WG
- 脅威分析WG(航空、空港)
- 海事分野WG(船舶)

※交通ISACには鉄道に特化したWGはないが、鉄道事業者間では安全管理・対策の観点での情報交換を個別に実施

◆公助:基準策定、訓練など

➢鉄道事業法施行規則の改定など、サイバーセキュリティ確保に関わる制度整備が進行

✓2025年7月～「鉄道事業者の重要システムにおける情報セキュリティ対策等検討委員会」

➢IPA ICSCoE のプログラム

列車運行制御におけるサイバーセキュリティ

◆安全に直結する列車運行制御における対策は特に重要

➢保護すべき情報

✓列車位置情報、停止目標位置情報などの制御情報

➢想定される脅威

✓意図的な要因：外部・内部の攻撃者による情報の改竄、なりすまし、妨害、…

✓意図しない要因：誤操作、外部システム、自然災害などによる情報の消失・書換、…

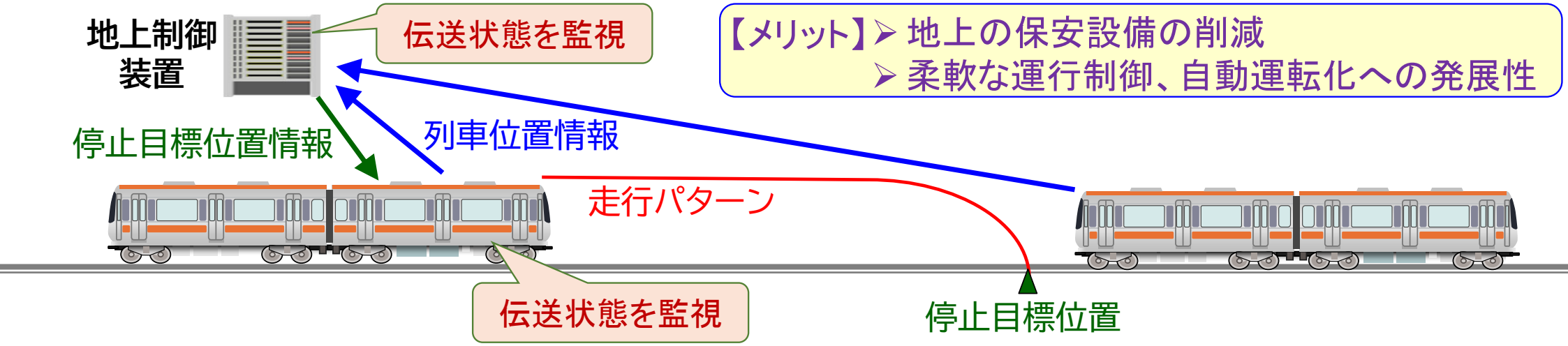
➢セキュリティが侵害された場合の影響

✓安全性の阻害（衝突、脱線）

✓安定性の阻害（列車の緊急停止、速度制限、…）

➡ 安全性の確保を最優先とする各種対策を導入

無線による列車の保安制御



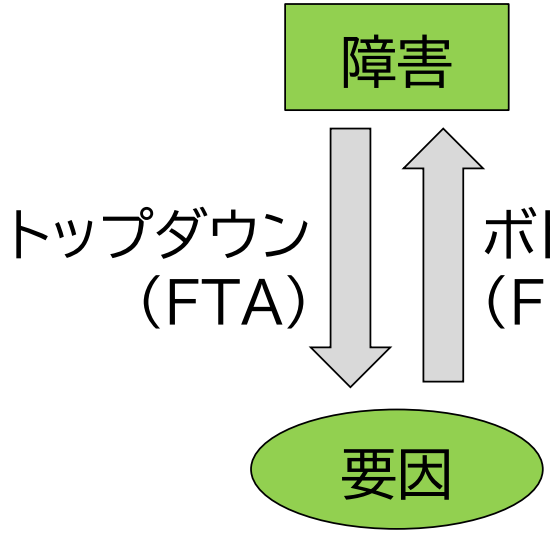
列車運行の安全性

- 「フェールセーフ」な保安装置によって安全を担保する仕組み
  - ➢ 受信電文の正常性などのチェック
  - ➢ 異常検知時に列車停止などの安全側制御

保安装置間での情報伝送に異常が生じた際にも安全を確実に確保

安全性分析と脅威分析

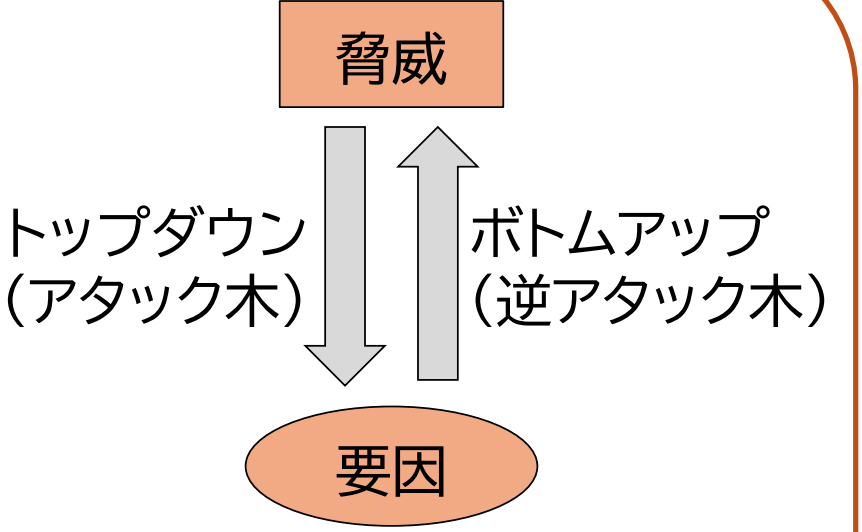
安全性分析



- FTAで障害の要因と発生プロセスを抽出、対策を可視化
- FMEAで障害の洗い出しを行う

✓ 想定される障害はシステムによって決まる
✓ 障害の発生は確率事象として扱える

脅威分析



- STRIDE等の分析手法で脅威を洗い出す
- アタック木で脅威の要因と発生プロセスを抽出、対策を可視化
- 逆アタック木でプロセスの洗い出しを行う

✓ 想定される脅威は変わっていく可能性
✓ 脅威は常に存在するものとして扱う必要

列車制御情報の伝送における脅威の分析例

列車制御に関わる機能間での情報伝送で想定される脅威

① 誤った情報が入力される
② 情報が途絶する
③ 情報が遅れて入力される

		サイバー攻撃の分類				
		なりすまし		改ざん	サービス妨害（DoS）	
		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
脅威	誤った情報が入力	✔	✔	✔		✔
	情報が途絶する				✔	
	情報が遅れて入力		✔		✔	
検証すべき情報の特性		真正性	健全性			

⇒ 危険側である「状態誤認」や「錯誤出力」とならないことが重要

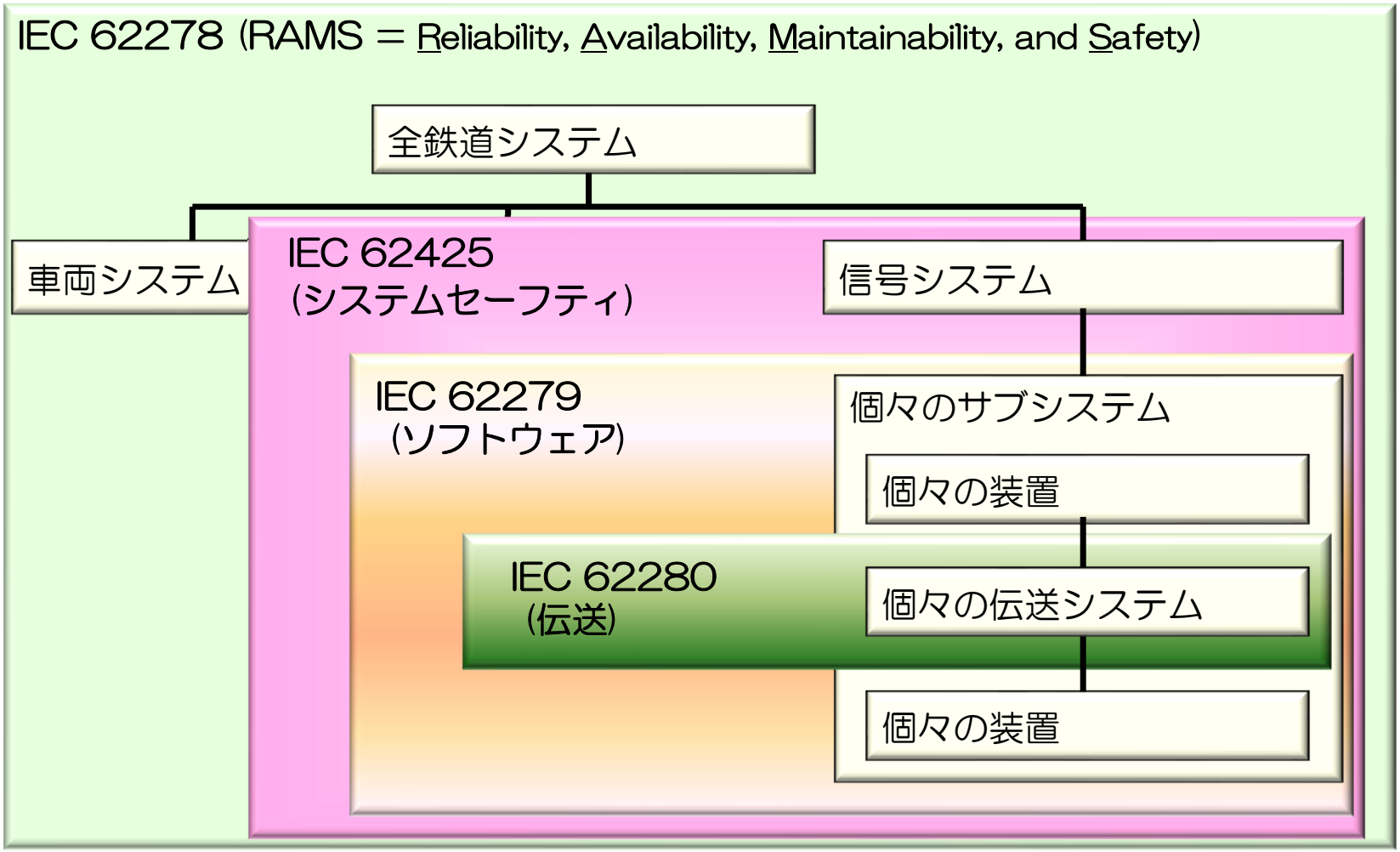
UIC 鉄道向けサイバーセキュリティガイドライン

◆Guidelines for Cyber-Security in Railway

- ➢2018年6月発行
- ➢ISO/IEC 27000シリーズを基に鉄道向けに策定
  - ✓鉄道向けの”IEC 62443”相当の文書
- ➢主な内容
  - ✓管理プロセス
    （ISO/IEC 27001ベース）
  - ✓解決策
    （ISO/IEC 27002ベース）

- ➢設計開発段階から運用に至るまでのセキュリティ確保と管理方法について、考え方・考慮すべき事項を記載
  …ただし具体的な対策方法など技術的な事項は提示されていない

鉄道の安全性に関する主なIEC規格



IEC 62280

◆安全に直結する情報の伝送を担う鉄道用通信システムに対する要件を定義

- ➢7つの脅威を想定、メッセージ認証・一貫性・即時性・連続性の提供を要求
- ➢脅威と対策例の関係は「情報」として提示

脅威 (Threat)	対策例							
	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(Repetition)	○	○						
削除(Deletion)	○							
挿入(Insertion)	○			△	△	△		
順序誤り(Resequence)	○	○						
破壊(Corruption) ➡ STRIDEの“T”, “D”に対応							○	○
遅延(Delay) ➡ STRIDEの“I”, “S”に対応	○		○					
なりすまし(Masquerade) ➡ STRIDEの“S”に対応					△	△		○

IEC/TC 9におけるサイバーセキュリティ規格の開発

◆Project IEC 63452

- ➢Title：Railway applications – Cybersecurity
- ➢Scope：
  - ✓鉄道アプリケーションのサイバーセキュリティを管理するための一貫したアプローチを提供
  - ✓鉄道車両、固定設備、鉄道運行のための運用管理システムが対象
    - ● 監視、情報、通信、信号など各種のシステムを包含
  - ✓IEC 62443シリーズ規格の関連部分を鉄道分野に適用
    - ● サイバーセキュリティ管理、ゾーン分け、リスク管理、サプライチェーン管理、サイバーセキュリティ要件、サイバーセキュリティ保証、および運用、保守、廃止要件を詳細に規定
  - ✓安全確保は対象としないが、サイバーセキュリティと安全の関係に関する指針も提供

◆開発経緯・発行予定

- ➢2022年5月：プロジェクト開始（エキスパート：9ヵ国から参加）
- ➢2023年9月：委員会原案（1st CD）回付
- ➢2025年4月：各国からのコメント集（CC）回付
- ➢2025年7月：委員会投票原案（CDV）回付

→ 2026年3月の発行を予定

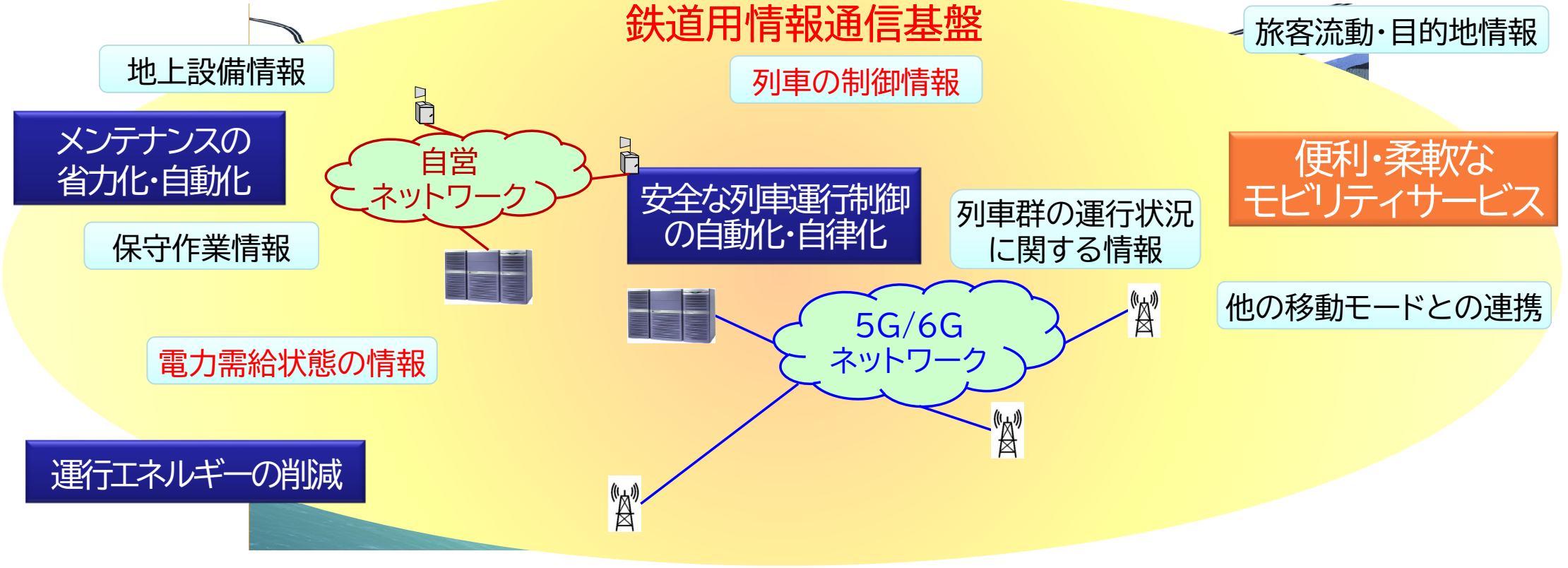
発表内容

- ◆鉄道の安全・安定運行を支えるシステム
  - ➢列車運行管理システムと信号保安システムの概要
  - ➢電気事業との関係
- ◆列車の運行制御に係るサイバーセキュリティ
  - ➢鉄道システムにおけるサイバーセキュリティ
  - ➢列車制御システムにおいて想定される脅威と対策の考え方
  - ➢鉄道の安全性とサイバーセキュリティに関する国際標準化の動向
- ◆鉄道の将来に向けて
  - ➢将来の鉄道における情報通信の姿と課題

将来の鉄道における情報通信の姿

◆ 少子高齢化、災害の激甚化、エネルギー問題、多様なニーズへの対応が喫緊の課題

➡ AI・5G/6Gなど最新の情報通信技術の活用 ＋ 情報を共有して連携できる基盤づくり

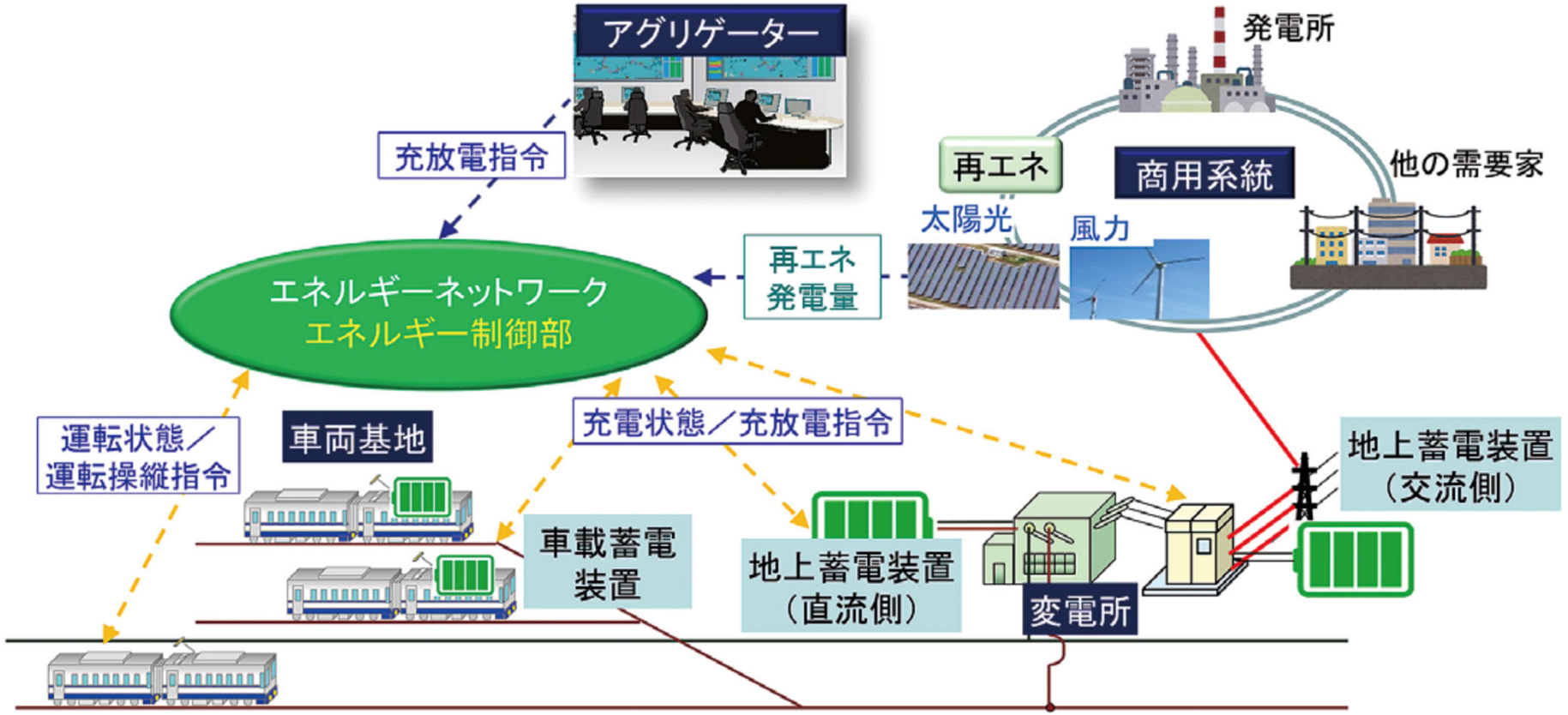


実現に向けては、増大するサイバー攻撃の脅威への対応は最重要課題の一つ

電気事業との連携・協調に関する研究開発事例

◆脱炭素化に向けた「スマート蓄電システム」

➢鉄道システム内の需要調整＋車載・地上の蓄電池を活用した連携



重枝：第34回 鉄道総研講演会 要旨集 p.22 Fig.5, 2021

おわりに

◆鉄道の維持発展に情報通信技術の活用と関連分野との連携は不可欠
- ➢より安全で、少ないリソースでも安定して運営できる鉄道へ

◆サイバーセキュリティの重要性は益々高まる
- ➢情報通信技術を活用する際に考慮すべき必須の課題
  - ✓特に「安全」を確保しながら「安定」を維持するための仕組み、考え方
  - ✓無線利用の拡大、ネットワーク化、COTS活用の広まりによる“侵入口”の増加、システム全体への波及に対する考慮
- ➢思いもよらぬ攻撃を如何に想定するか：ゼロトラスト

◆専門家との連携、関係者間でのスムーズな情報共有ができる環境づくり
- ➢様々な議論・共有の場をフルに活用
- ➢関連規格の活用＋鉄道向け規格の提案も視野に