駅構内論理装置の踏切制御機能仕様に対するSTAMP/STPA解析

Wed. 7/12/16
1st STAMP Workshop in Japan

東日本旅客鉄道株式会社
JR東日本研究開発センター
阿満 利仁(Rihito Aman)

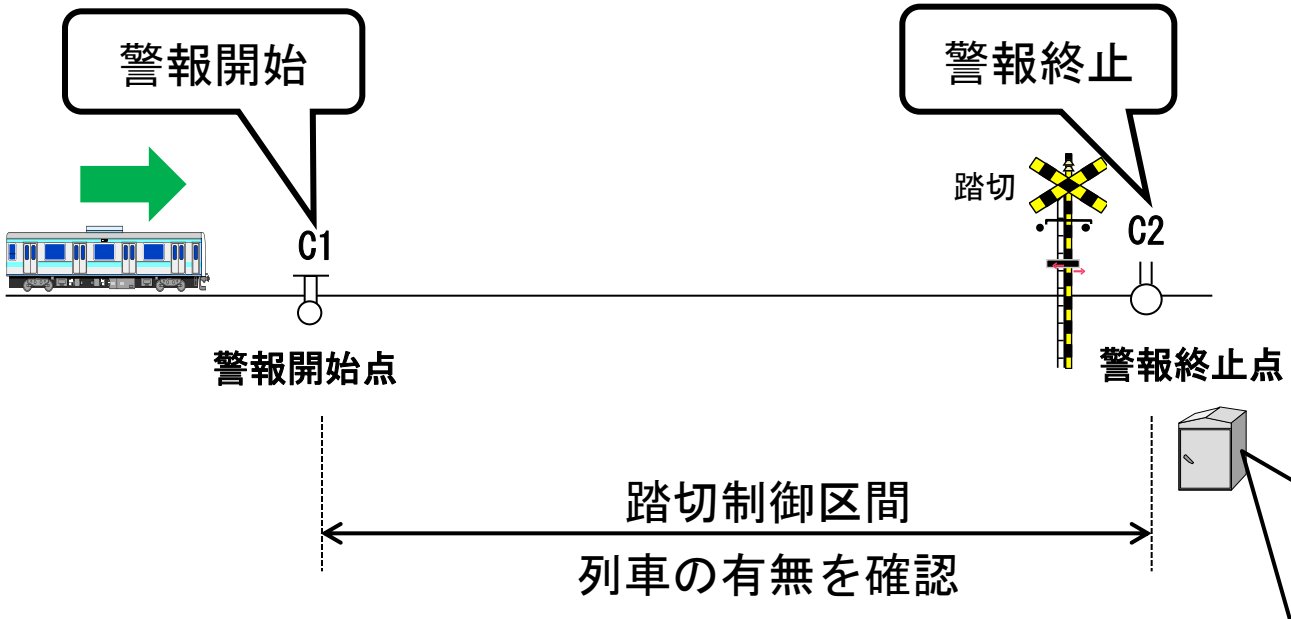
発表の流れ

1. 背景
   - 鉄道における踏切制御
2. 駅構内論理装置と踏切制御のSW化
   - 駅構内論理装置（構内LC）
   - 駅構内踏切制御SW化の課題
3. STAMP/STPAの適用
4. その他

1. 背景
   - 鉄道における踏切制御
2. 駅構内論理装置と踏切制御のSW化
   - 駅構内論理装置（構内LC）
   - 駅構内踏切制御SW化の課題
3. STAMP/STPAの適用
4. その他

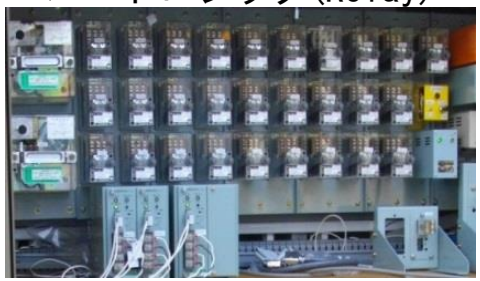
鉄道における踏切制御

踏切制御の基本：中間踏切



踏切制御装置
(Level Crossing Controller)

ハードロジック(Relay)



ソフトロジック(Computer)

中間踏切の電子制御は
20年ほど前に実用化

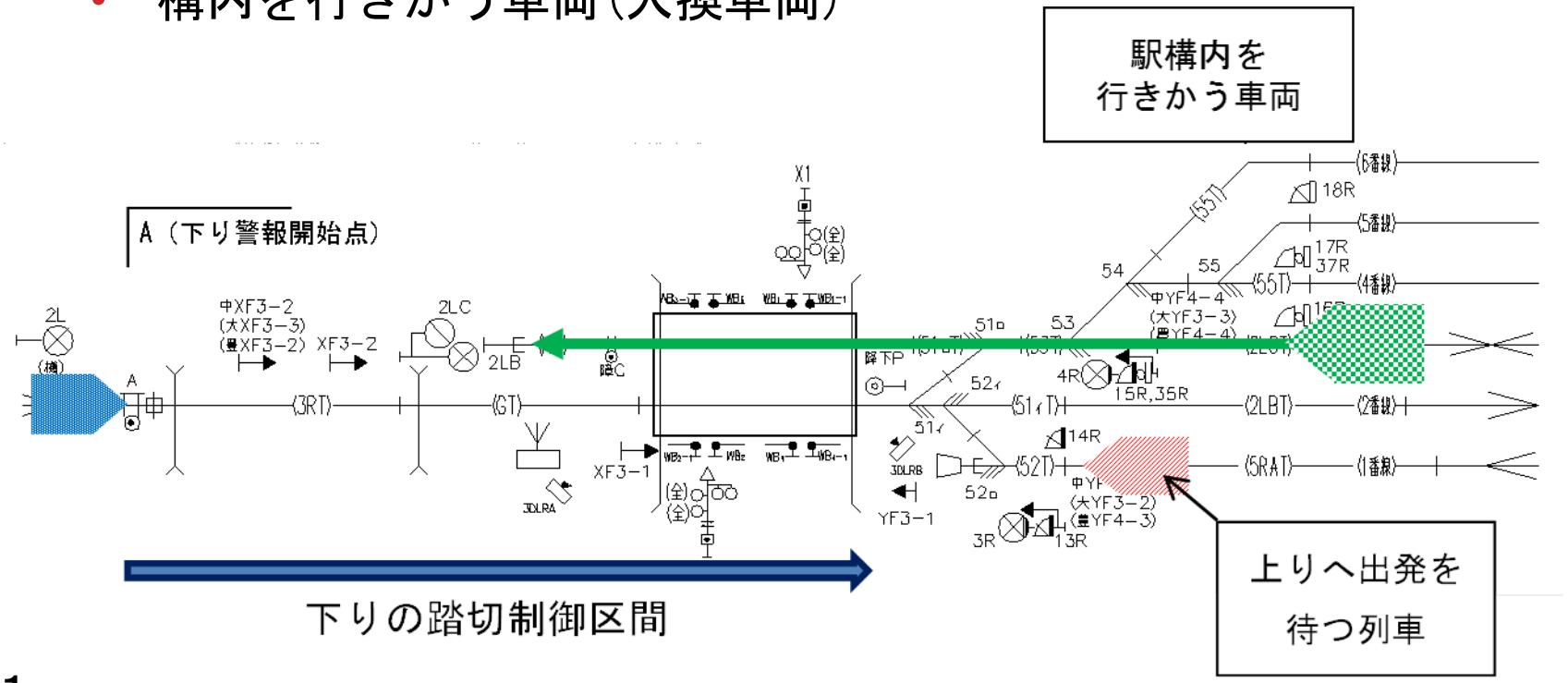
鉄道における踏切制御

- **非常に高い動作精度を要求**
  - 列車が接近しているにもかかわらず警報制御されていないことは重大なアクシデントを引き起こすハザードとなる
  - 装置故障や制御誤りを検知した場合は警報を持続させる

- 警報の持続は列車と道路通行車(者)の衝突を防ぐが、道路交通に重大な影響を与える。

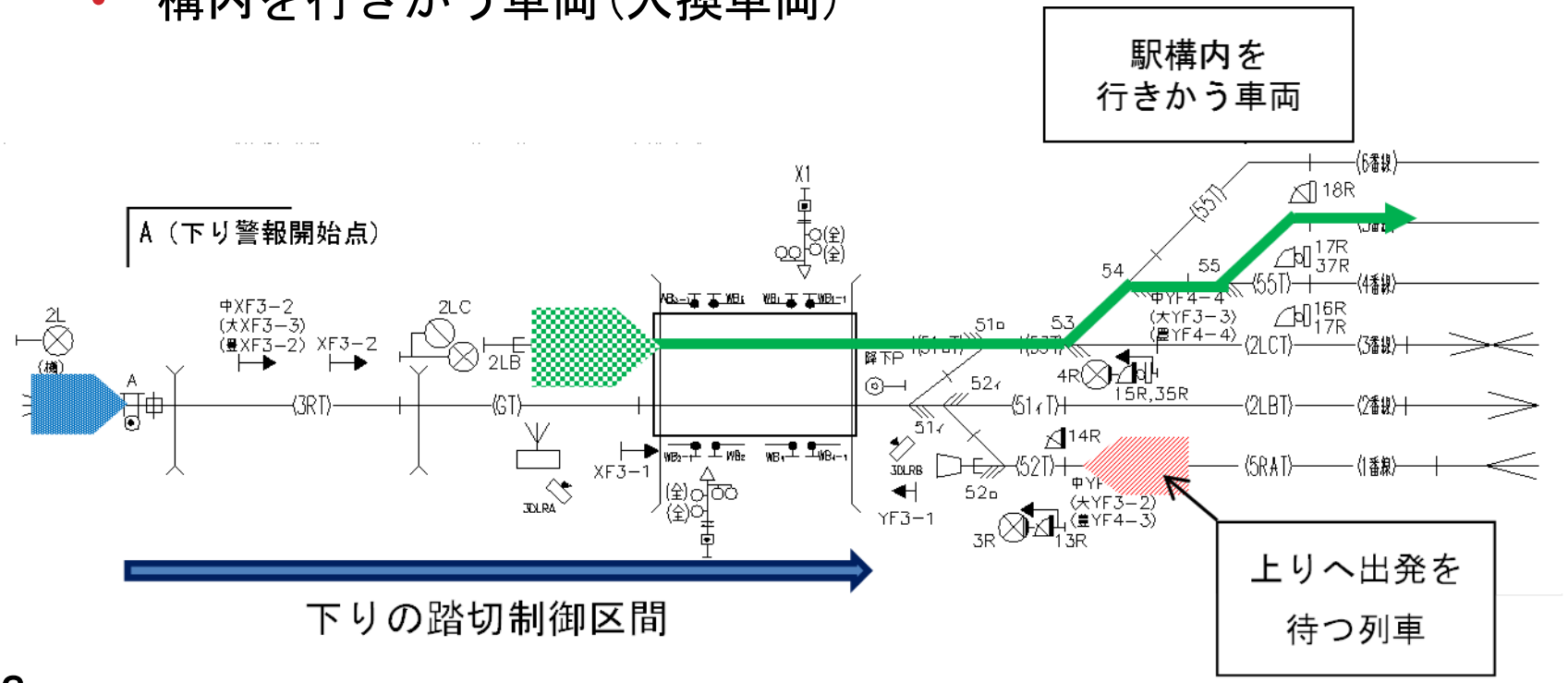
鉄道における踏切制御

- **駅構内は多くの列車が行きかうため、制御は複雑になる。**
  - **連動装置**（駅構内で列車進路を制御する装置）
  - 上下線の複数列車の取り扱い
  - 構内を行きかう車両（入換車両）



鉄道における踏切制御

- **駅構内は多くの列車が行きかうため、制御は複雑になる。**
  - **連動装置**（駅構内で列車進路を制御する装置）
  - 上下線の複数列車の取り扱い
  - 構内を行きかう車両（入換車両）



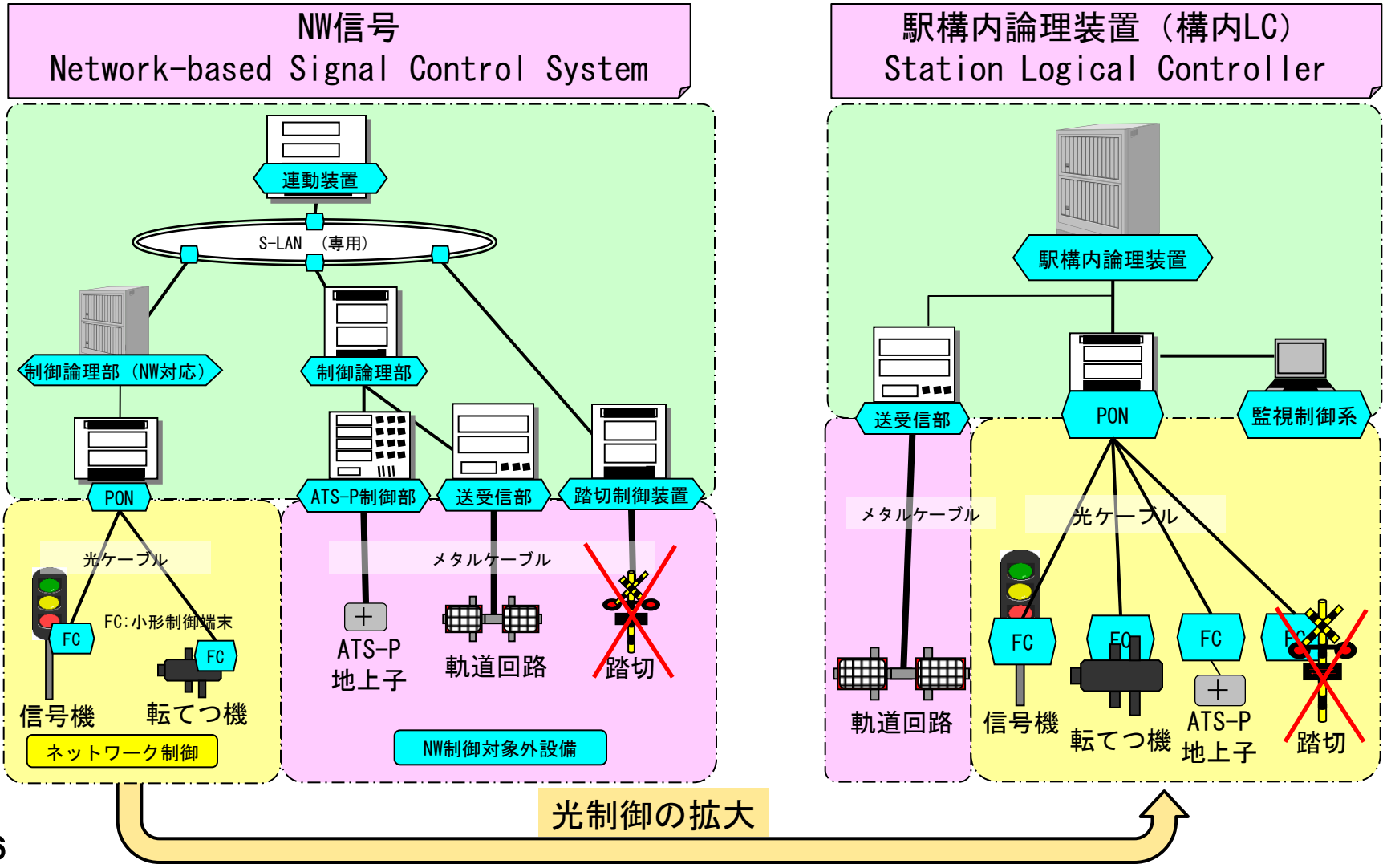
1. 背景
   - 鉄道における踏切制御
2. **駅構内論理装置と踏切制御のSW化**
   - 駅構内論理装置（構内LC）
   - 駅構内踏切制御SW化の課題
3. STAMP/STPAの適用
4. その他

駅構内論理装置（構内LC）

- **連動装置(駅構内で列車進路を制御する装置)**
  - 当社の場合、約半数はハードロジック
    継電連動装置/Relay Interlocking Device
  - 約半数はソフトロジック
    電子連動装置/Electronic Interlocking Device

- **連動装置の課題と最近の開発**
  - 現場配線…大量のメタルケーブル
    ⇒光ケーブルを使った制御の実用化(NW信号)
  - 制御論理…機能毎に個別の制御論理
    ⇒機能統合した装置の実用化(構内LC)

駅構内論理装置（構内LC）



駅構内踏切制御SW化の課題

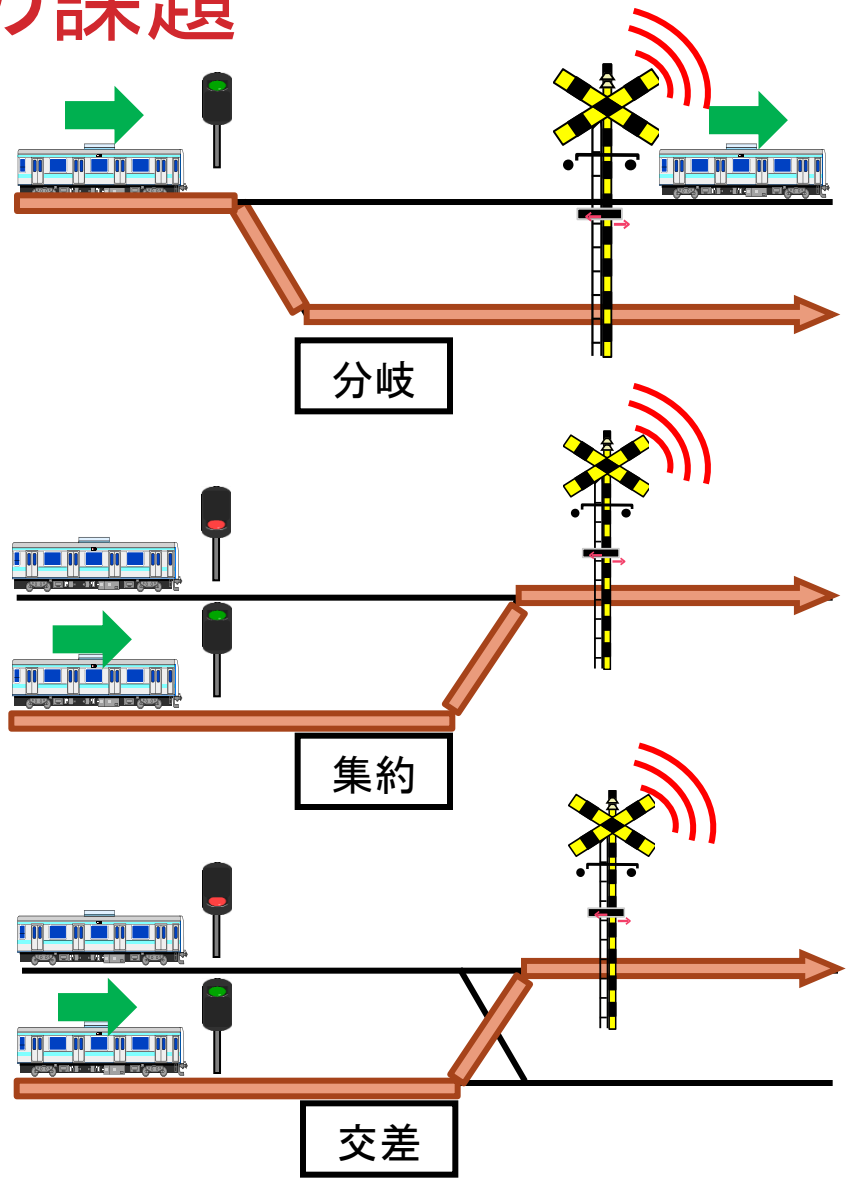
- **駅構内踏切制御をソフトウェア化し、連動制御と一体開発する試みはこれまで幾度となくなされてきた。**

- **安全性を担保する、標準的な制御論理の実装に至っていない**
  - 駅構内の形状、進路は多種多様
  - 各種装置や列車の挙動が正しくても不具合が発生
- **不具合が生じた場合は都度の改良・対策**
  - 経験の積み重ねの要素が大きい
  - 制御が一層複雑化
  - FTA/FMEAの適用が困難

- **インタラクション要素が大きい駅構内踏切制御はSTAMPが有効**

駅構内踏切制御SW化の課題

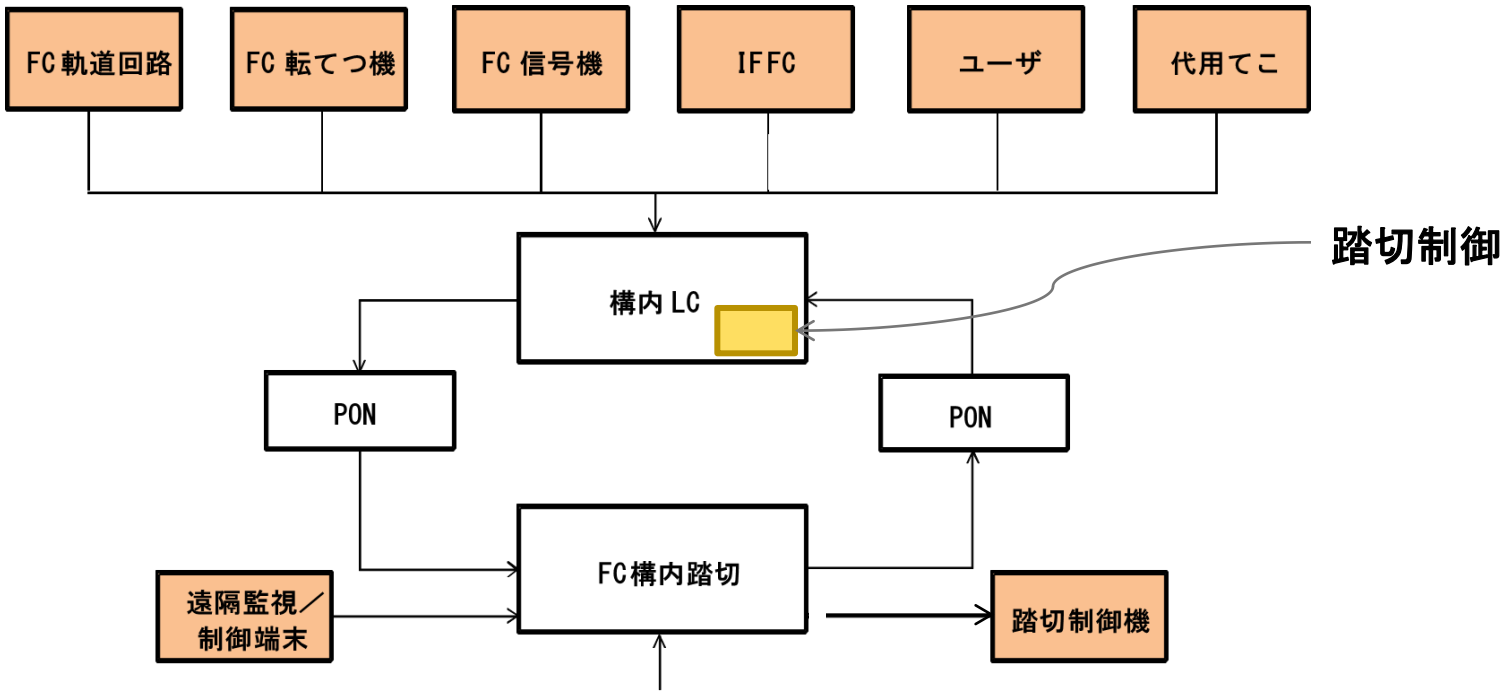
列車数	中間	構内
単一列車	単行	単行
複数列車	続行	続行
	対向	対向
	—	分岐
	—	集約
	—	交差



1. 背景と目的
   - 鉄道における踏切制御
2. 駅構内論理装置とその踏切制御機能のSW化
   - 駅構内論理装置（構内LC）
   - 駅構内踏切制御SW化の課題
3. STAMP/STPAの適用
4. その他

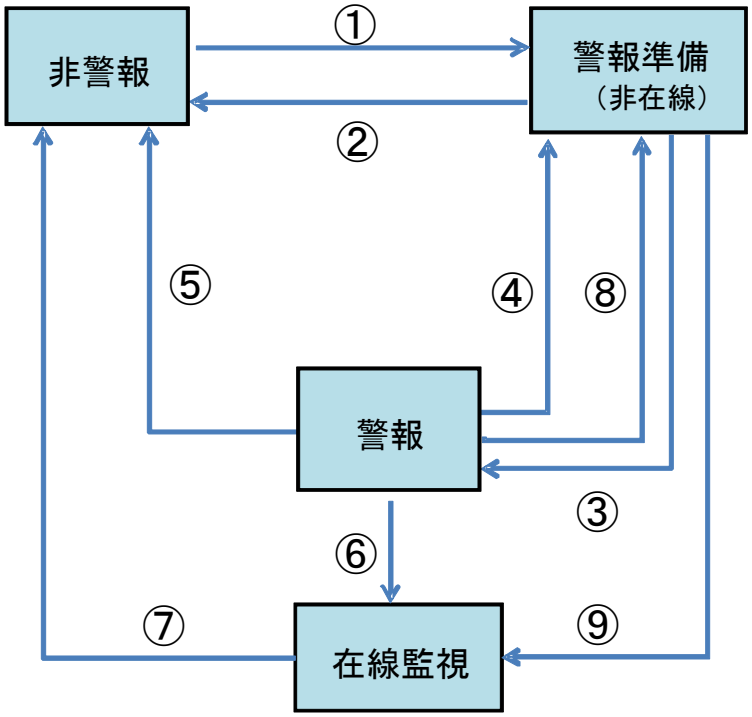
STAMP/STPAの適用

- 構内LCとその踏切制御(含むFC構内踏切)のコントロールループを中心にしたシステム全体の図



STAMP/STPAの適用

- **構内LCの踏切制御における状態遷移**

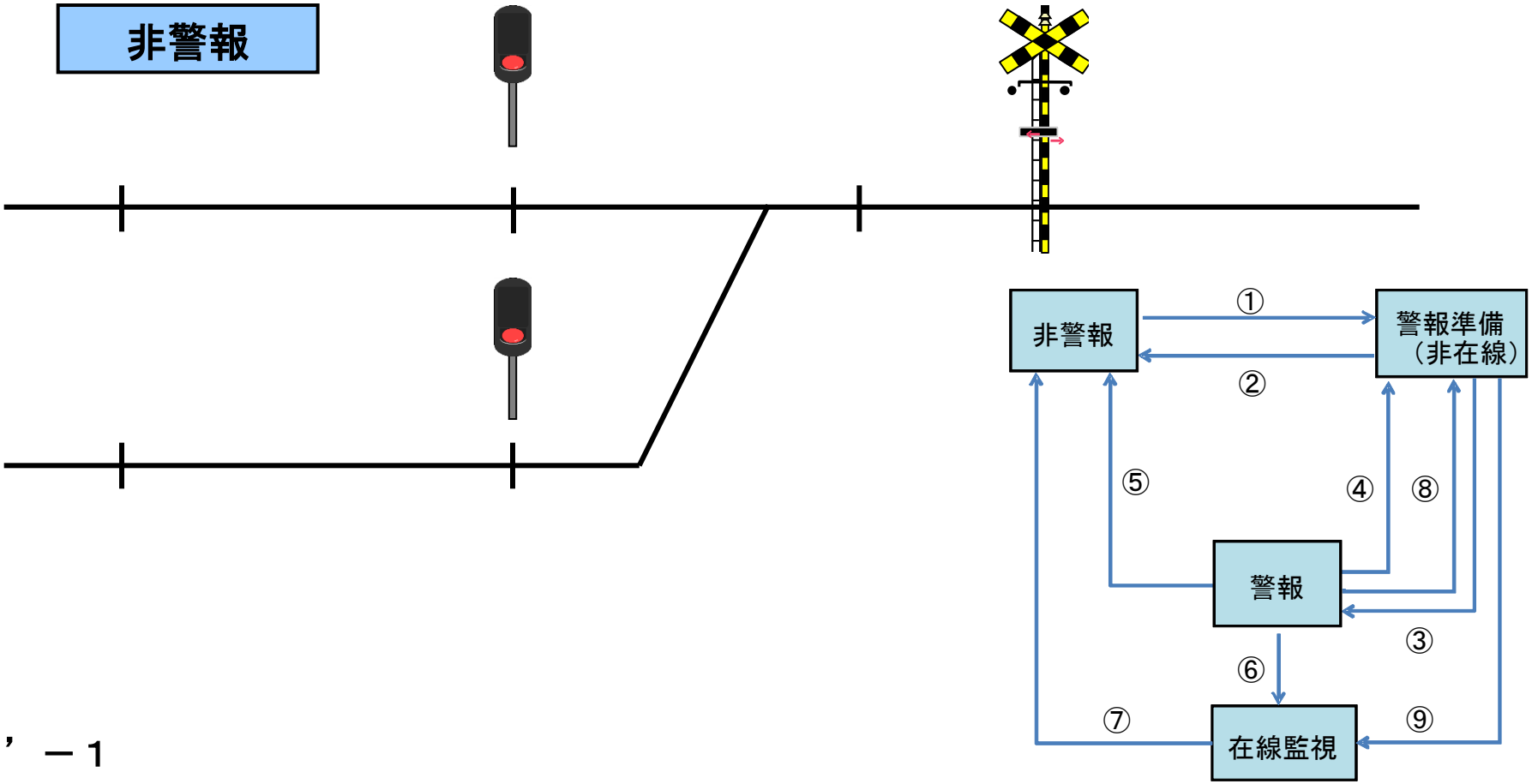


NO.	状態	遷移条件
①	警報準備	当該警報区分進路に列車非在線かつ区分進路予約が成立
②	非警報	当該警報区分進路の接近又は進路予約が不成立。または、転てつ器転換等により進路非開通
③	警報	当該警報区分進路が進入または進入完了
④	警報準備	当該警報区分進路が進出で進路予約が成立
⑤	非警報	当該警報区分進路が進出で進路予約なし
⑥	在線監視	当該区分進路が追跡異常
⑦	非警報	当該警報区分進路が在線監視終了
⑧	警報準備	当該警報区分進路の進路予約が不成立
⑨	在線監視	当該区分進路が追跡異常

・警報区分進路：連動論理で処理される進路から作成される、その進路に列車が進入した場合踏切警報の対象となる進路のこと。

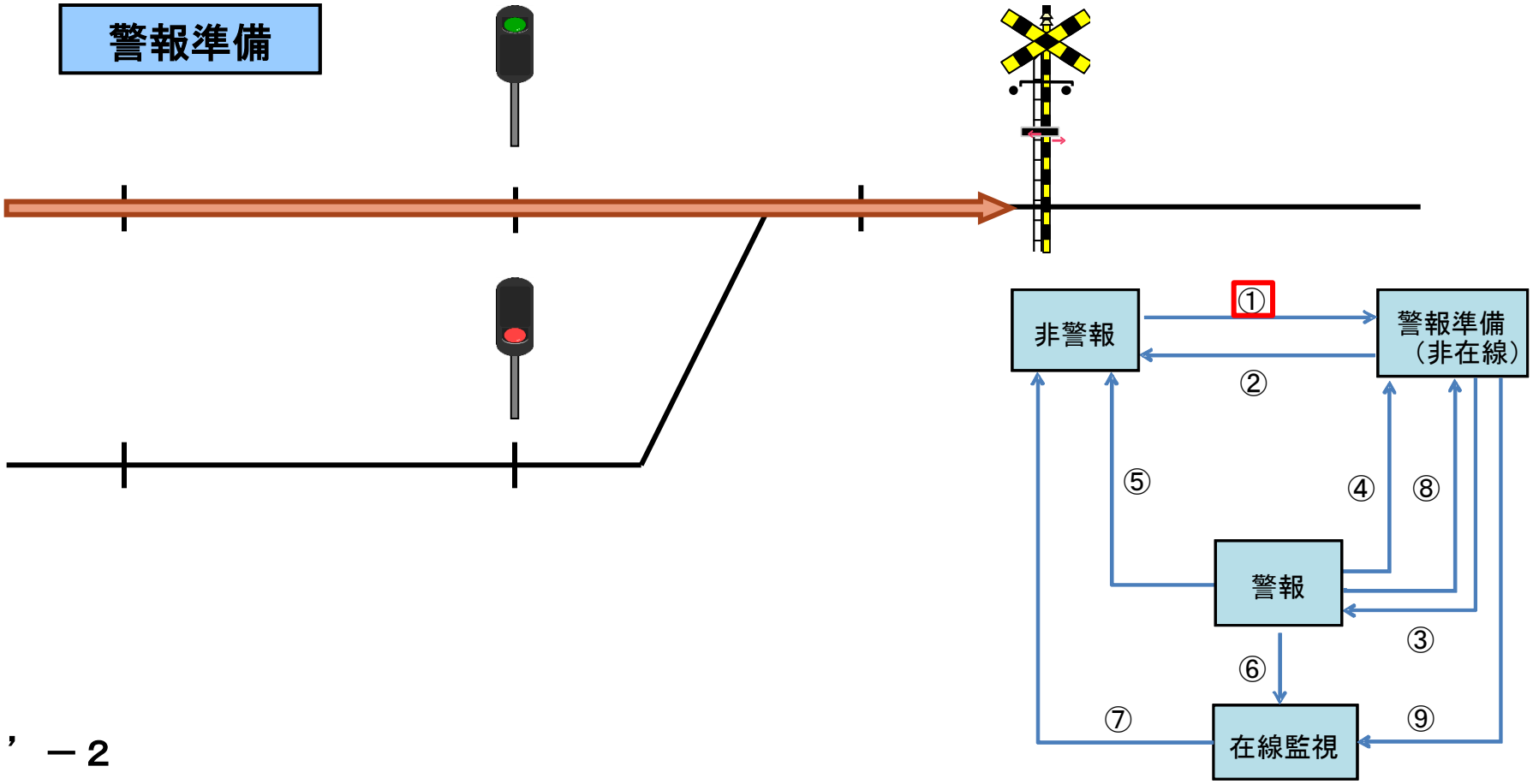
STAMP/STPAの適用

- 構内LCの踏切制御における状態遷移



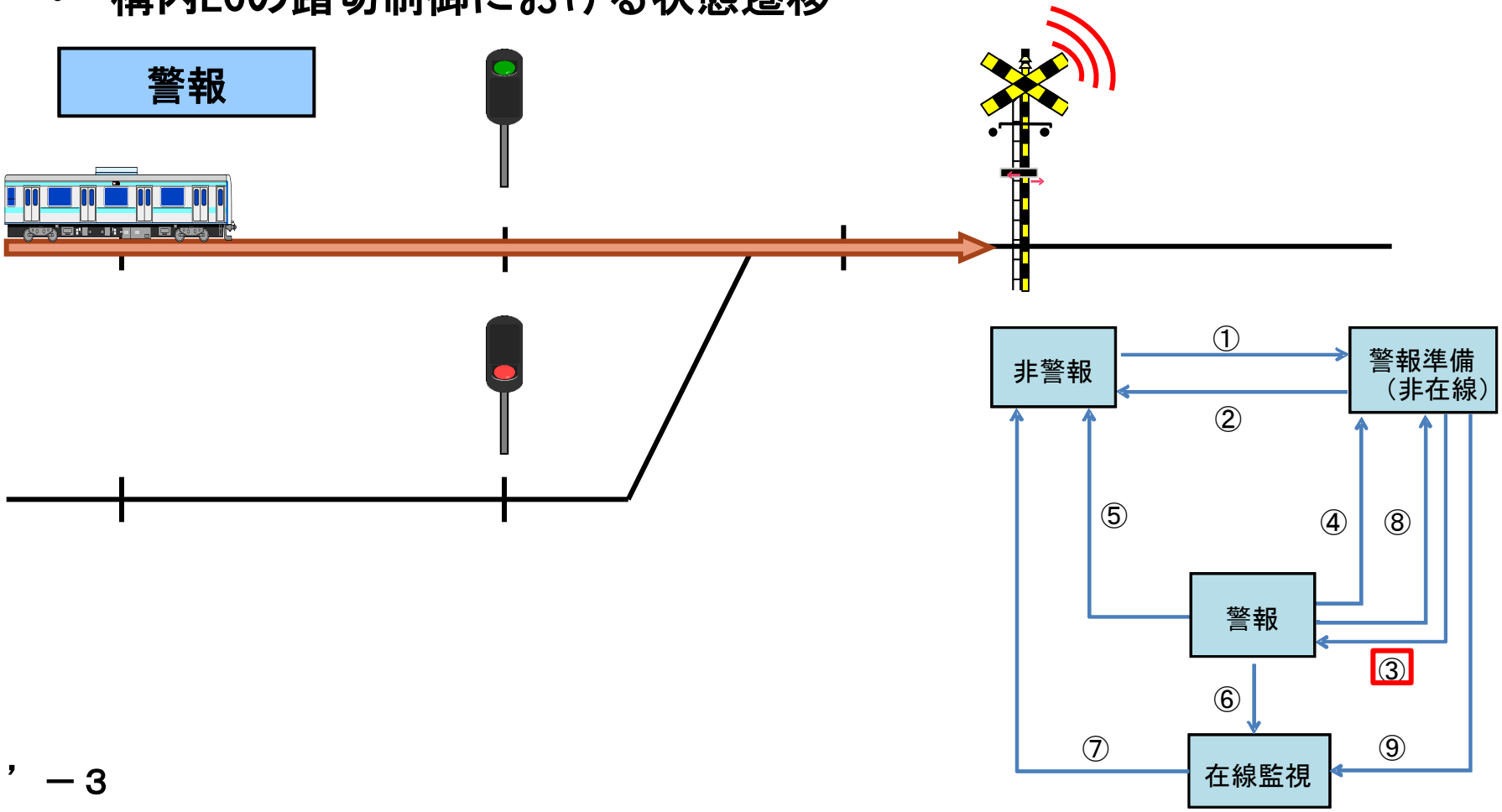
STAMP/STPAの適用

- 構内LCの踏切制御における状態遷移



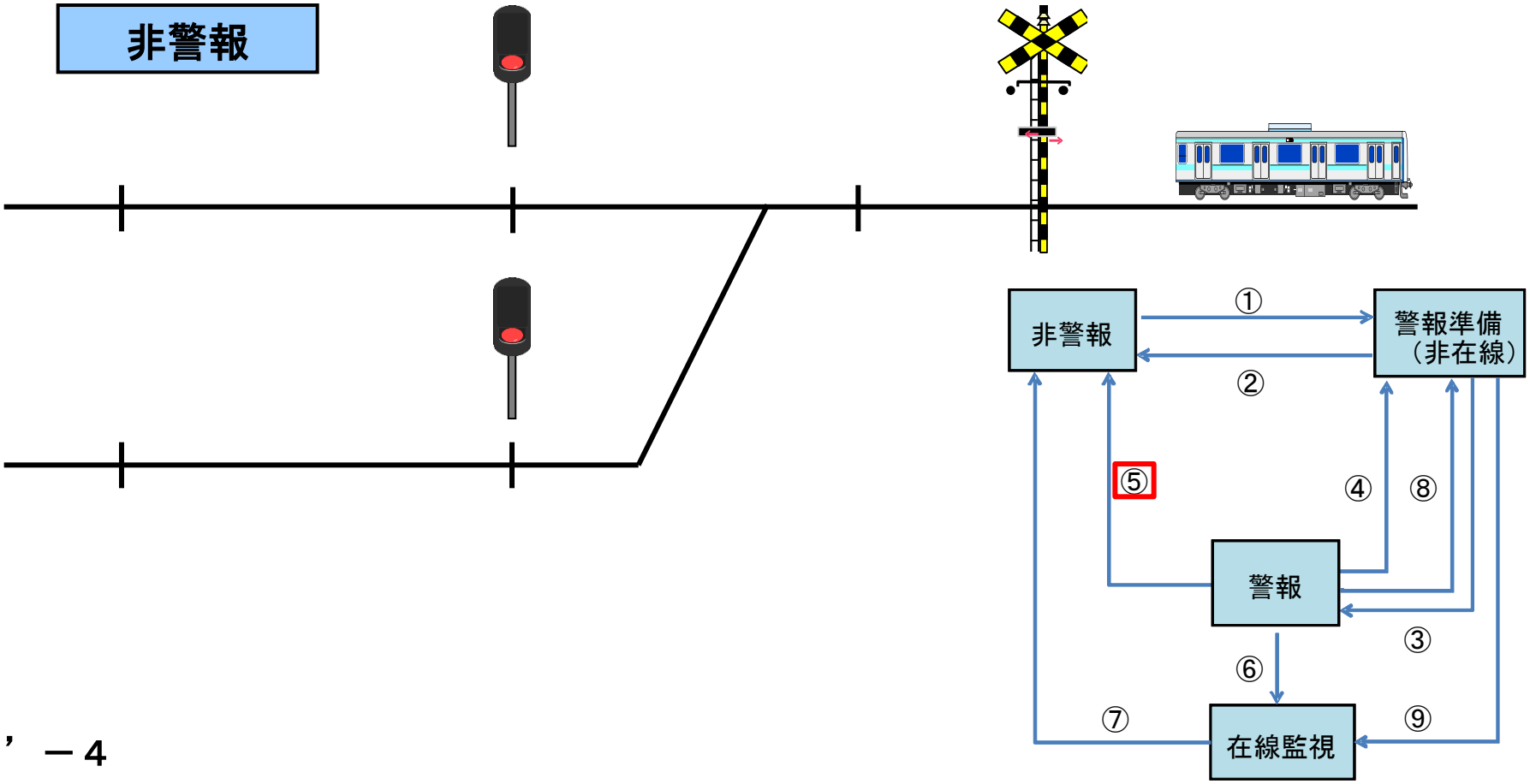
STAMP/STPAの適用

- 構内LCの踏切制御における状態遷移



STAMP/STPAの適用

- 構内LCの踏切制御における状態遷移



STAMP/STPAの適用

- Step0-1：ハザードの識別

H1 ： 列車が在線で踏切が遮断しない
H2 ： 踏切が遮断後に列車が在線にもかかわらず開く
H3 ： 警報時間の不足
H4 ： 警報時間の過剰
H5 ： 列車が非在線で踏切が遮断する

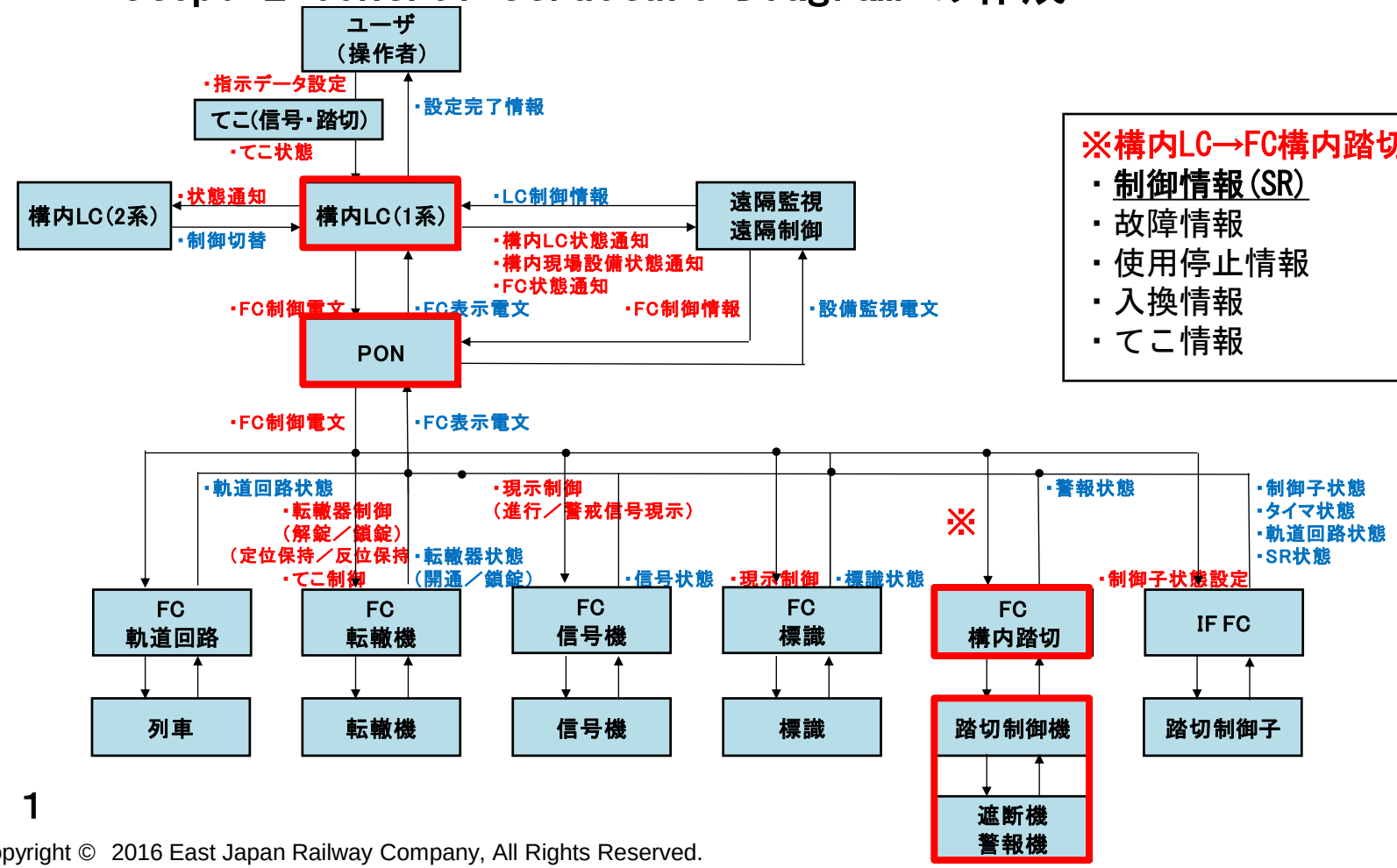
アクシデント：列車と人・車が踏切内で衝突する

アクシデント：踏切が開かず、交通が渋滞する
⇒本件では評価対象外

- 構内LCからFC構内踏切（踏切制御）への制御電文のうち、踏切の遮断に最も関わる「”SR”の扛上、落下」を分析対象のControl Actionと整理

STAMP/STPAの適用

- Step0-2:Control Structure Diagram の作成



※構内LC→FC構内踏切
- 制御情報(SR)
- 故障情報
- 使用停止情報
- 入換情報
- てこ情報

STAMP/STPAの適用

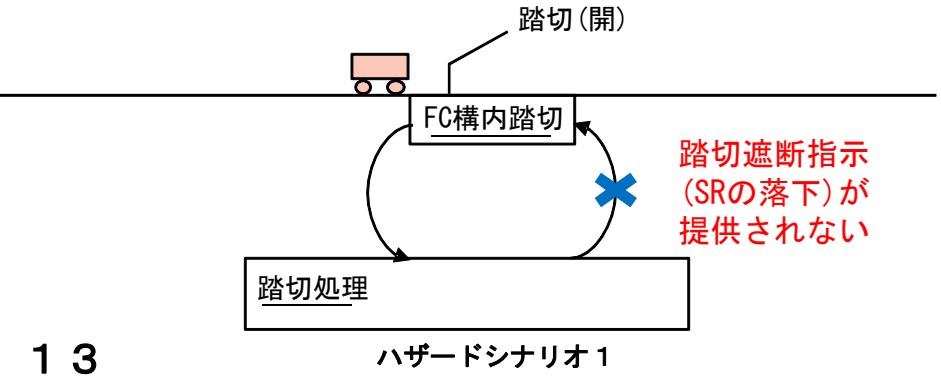
- Step1:Unsafe Control Action の抽出とハザードシナリオ

制御アクション	提供されない Not Provided	誤って提供される Incorrectly Provided	早すぎる／遅すぎる ／順序が違う Too early too late	途中で停止する ／（過剰に長引く） stop to soon
SR落下	**列車が警報区分進路に在線しており、 ・警報準備経由で警報中となる条件 ・在線監視となる条件 ・非警報から警報中となる条件 が合致する状況において、SR落下が提供されないと、H1「列車が在線で踏切が遮断しない」に至る。**	列車が警報区分進路に実際に在線しておらず、 ・警報準備経由で警報中となる条件 ・在線監視となる条件 ・非警報から警報中となる条件 が合致しない状況において、SR落下が提供されるとH5「列車が非在線で踏切が遮断する」に至る。	列車が警報区分進路に実際に在線しているが、 ・警報準備経由で警報中となる条件 ・在線監視となる条件 ・非警報から警報中となる条件 が合致しない状況において、早まってSR落下が提供されるとH4「警報時間の過剰」に至る。 列車が警報区分進路に実際に在線しており、 ・警報準備経由で警報中となる条件 ・在線監視となる条件 ・非警報から警報中となる条件 が合致する状況において、遅れてSR落下が提供されるとH3「警報時間の不足」に至る。	列車が警報区分進路に実際に在線しているときに、SRの落下出力が停止してもSR扛上が提供されないので、H2「踏切が遮断後に列車が在線にも関わらず開く」には至らない 列車が警報区分進路に実際に在線しておらず、 ・警報準備経由で警報中となる条件 ・在線監視となる条件 ・非警報から警報中となる条件 が合致しない状況において、SR落下が過剰に長引くとH4「警報時間の過剰」に至る。

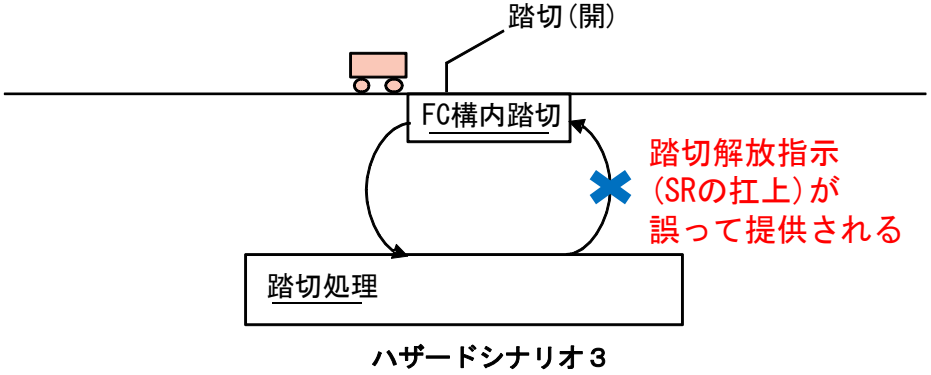
STAMP/STPAの適用

- Step1:Unsafe Control Action の抽出とハザードシナリオ

No.	ハザードシナリオ
1	列車が警報区分進路に実際に在線しており、SR落下が合致する状況において、**SR落下が提供されないと、ハザードH1「列車が在線で踏切が遮断しない」**に至る。
2	列車が警報区分進路に実際に在線しており、SR落下が合致する状況において、遅れてSR落下が提供されると、ハザードH3「警報時間の不足」に至る。
3	列車が警報区分進路に実際に在線しており、SR扛上のいずれも合致しない状況において、**SR扛上が提供されると、ハザードH2「踏切が遮断後に列車が在線にもかかわらず開く」**に至る。
4	列車が警報区分進路に実際に在線しておらず、SR扛上のいずれも合致しない状況において、早まってSR扛上が提供されると、ハザードH3「警報時間の不足」に至る。



ハザードシナリオ１

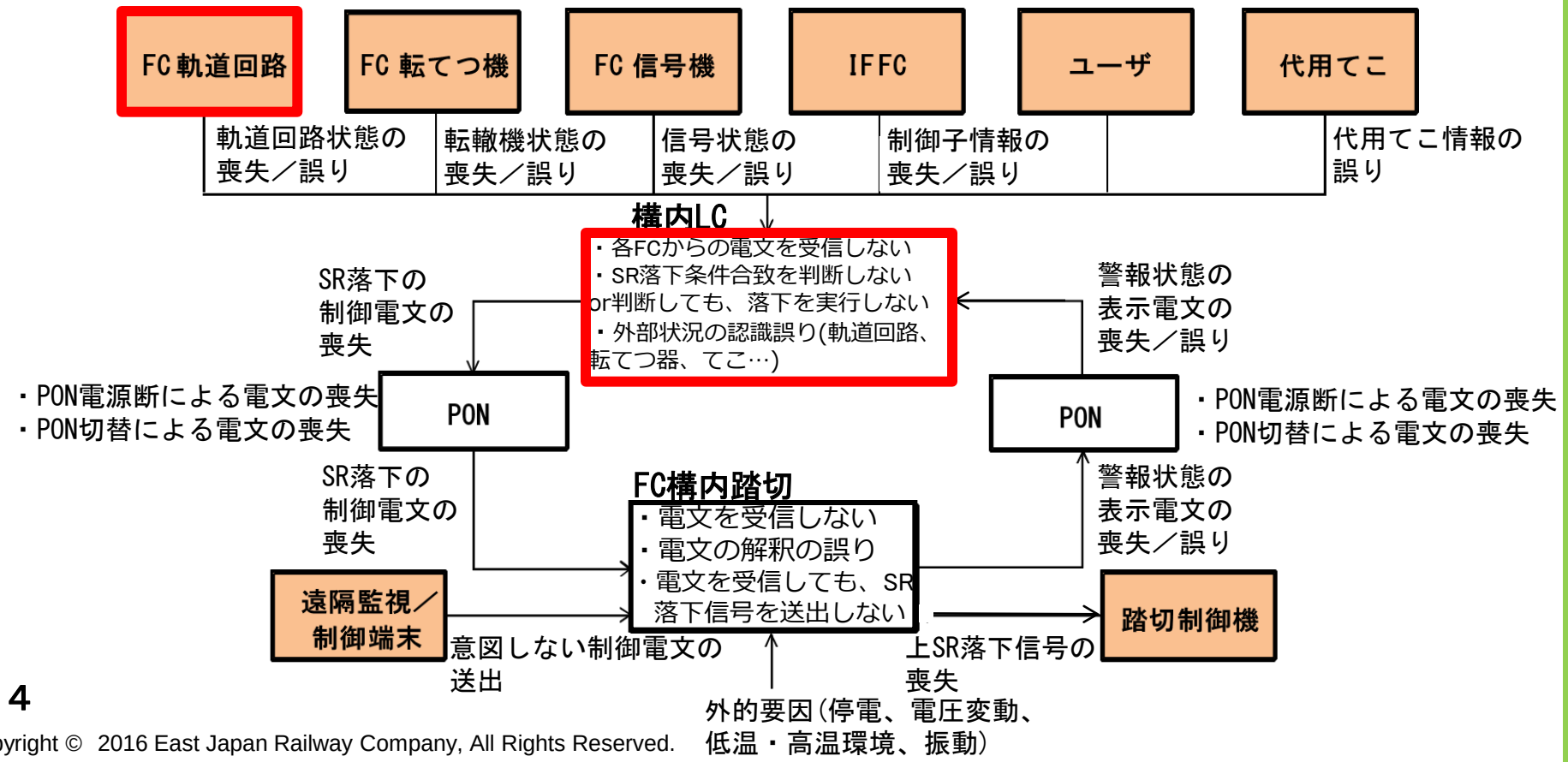


ハザードシナリオ３

STAMP/STPAの適用

- **Step2：Hazard Causal Factor の特定**

シナリオNo.1：列車が警報区分進路に実際に在線しており、SR落下が合致する状況において、SR落下が提供されないと、ハザードH1「列車が在線で踏切が遮断しない」に至る。



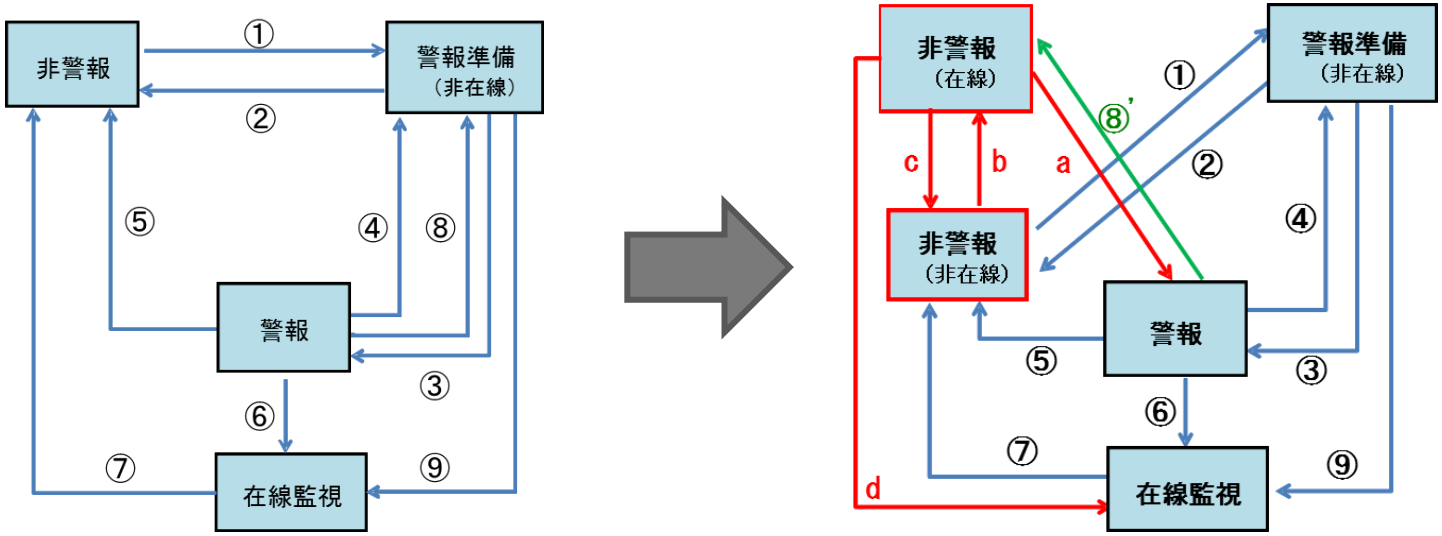
STAMP/STPAの適用

- **Step3：安全制約の識別**
  - ハザードシナリオ１～４の合計で、111件の安全制約（安全要求）を識別
- **シナリオNo.1に対する安全制約の例**

制御対象	被制御対象	ハザード要因	安全制約（安全要求）
構内LC	PON	SR落下の制御電文の喪失	制御電文を喪失しない、喪失を検知する
PON	FC構内踏切	SR落下の制御電文の喪失	制御電文を喪失しない、喪失を検知する
FC構内踏切	PON	警報状態の表示電文の喪失・誤り	制御電文を喪失しない、喪失を検知する
PON	構内LC	警報状態の表示電文の喪失・誤り	制御電文を喪失しない、喪失を検知する
各種FC	構内LC	各々の状態の喪失・誤り	各FCからの電文を喪失しない or 喪失を検知する
FC構内踏切	踏切制御機	SR落下信号の喪失	制御信号を喪失しない or 喪失の検知をする
構内LC 軌道回路状態の認識		・軌道回路状態の「進出」を判断しない ・軌道回路情報と踏切制御子情報が合致しない	・現在の状態で、軌道回路を正しく判断する ・合致しない場合は安全側に制御（警報）
外部環境		停電・電圧変動、低温・高温、振動	これら条件でも、FC構内踏切の制御を誤らない

STAMP/STPAの適用

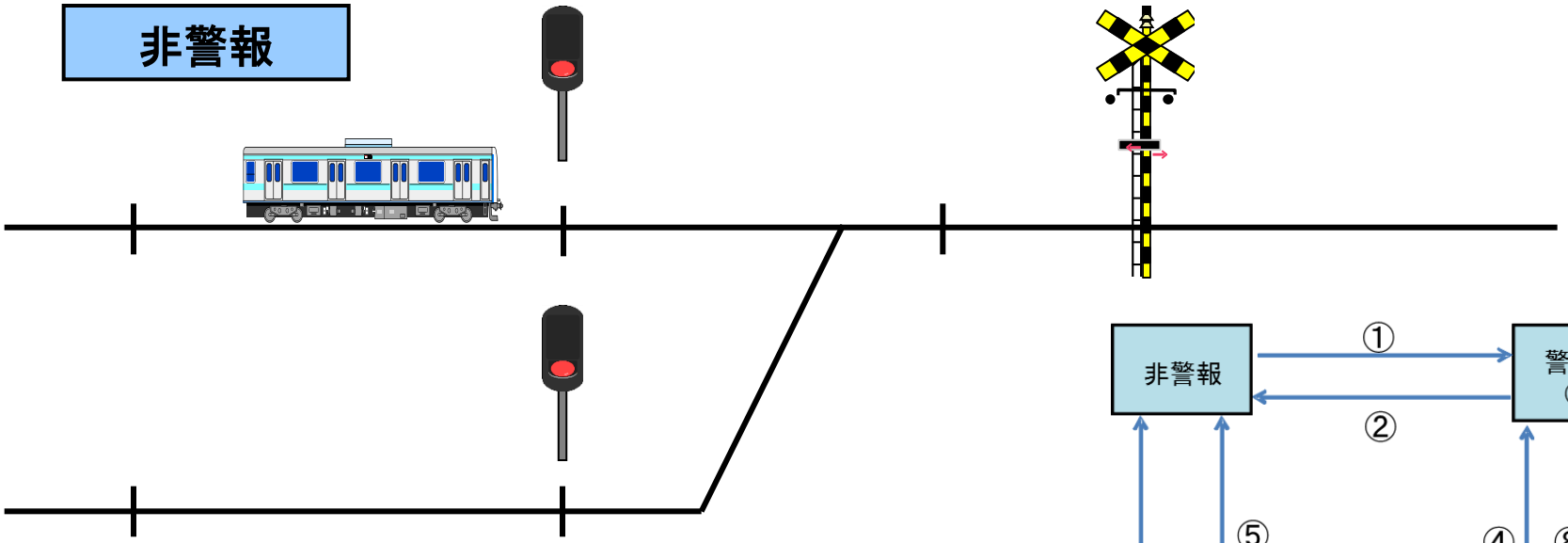
- **状態遷移図の修正**
  - STAMP/STPA Step1,2（ハザードシナリオ及びその要因を識別する過程）において、H1ハザードに至る警報状態遷移の抜け・誤りを識別したため、警報状態遷移図を修正

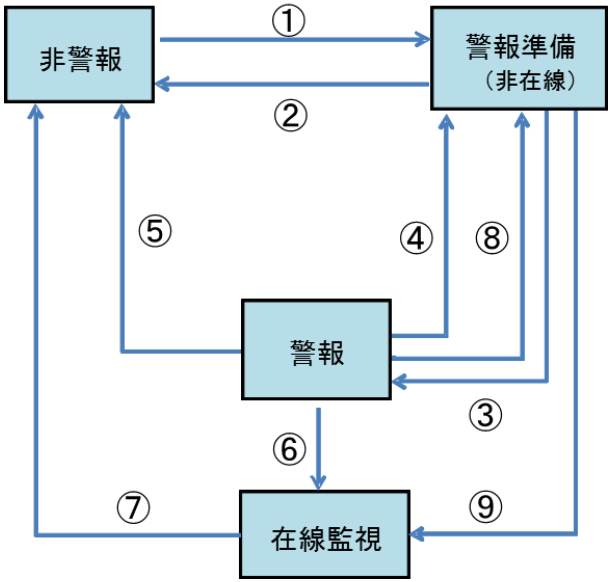


  - a：警報状態が「非警報」で軌道回路状態（警報区分進路）が「進入」のとき、進路予約状態が「成立」した場合の遷移

STAMP/STPAの適用

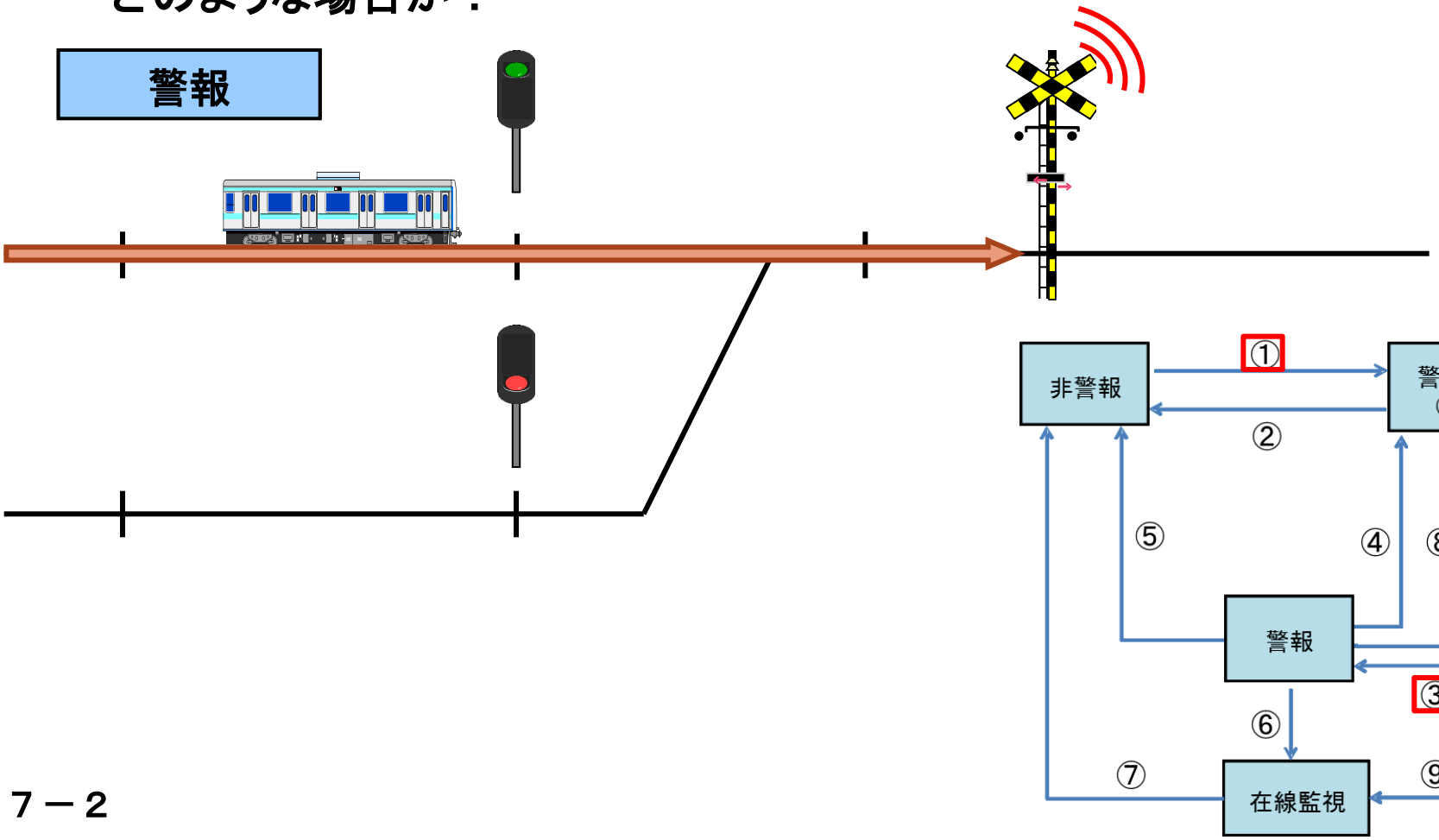
- どのような場合か？





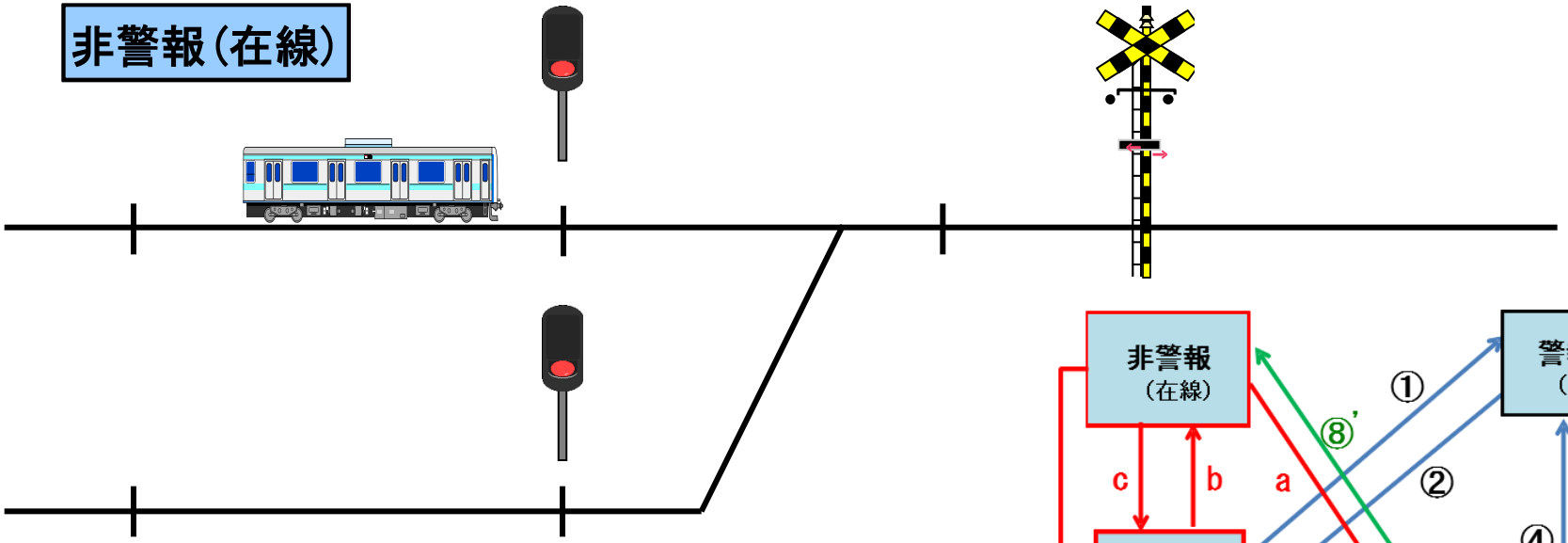
STAMP/STPAの適用

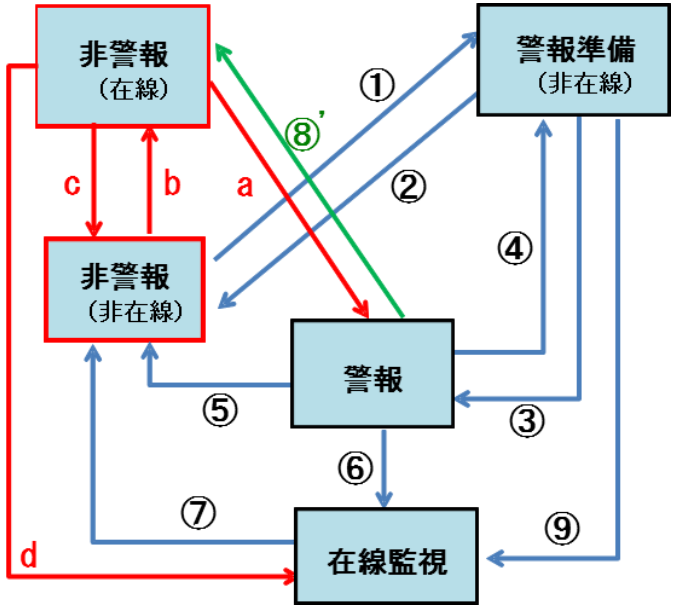
- どのような場合か？



STAMP/STPAの適用

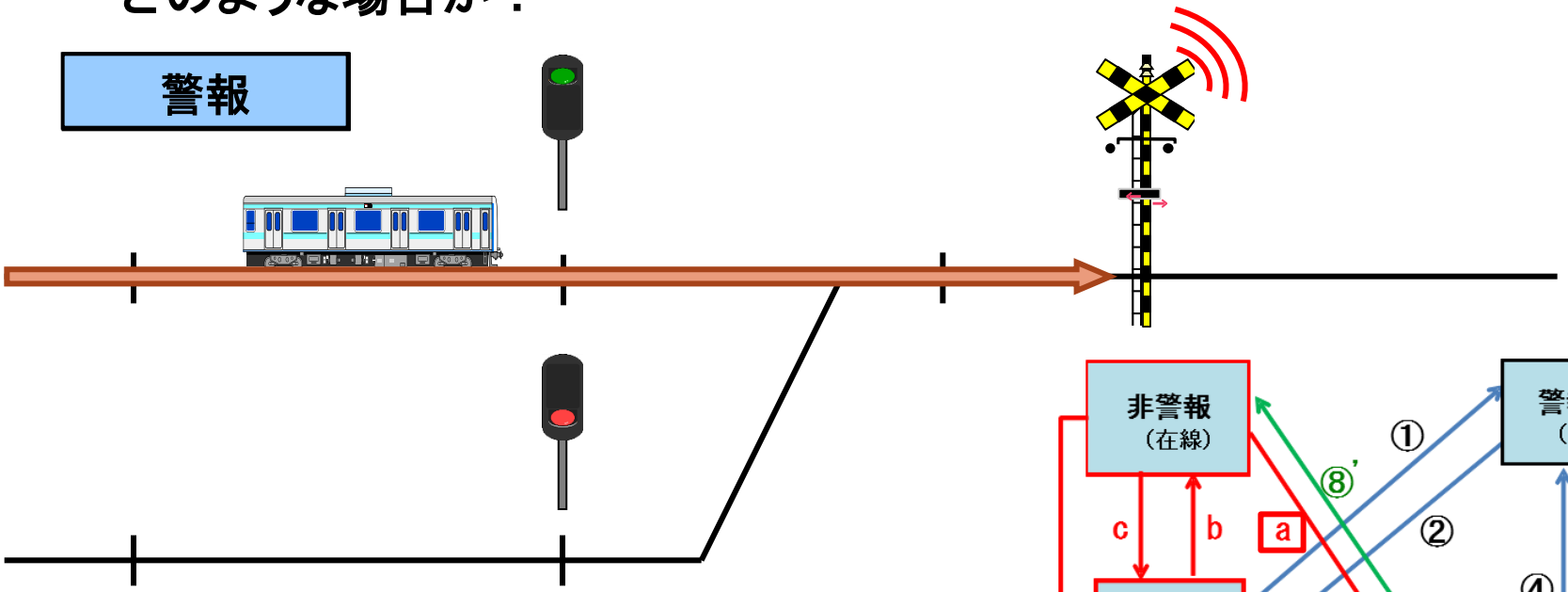
- どのような場合か？

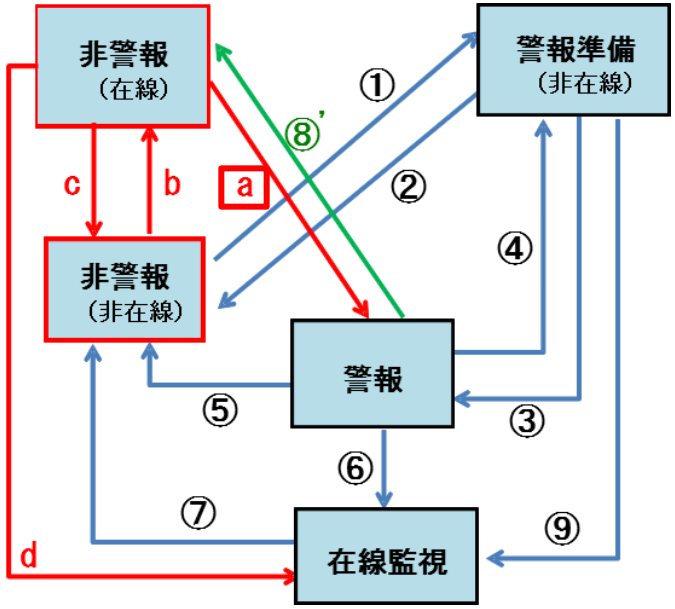




STAMP/STPAの適用

- どのような場合か？

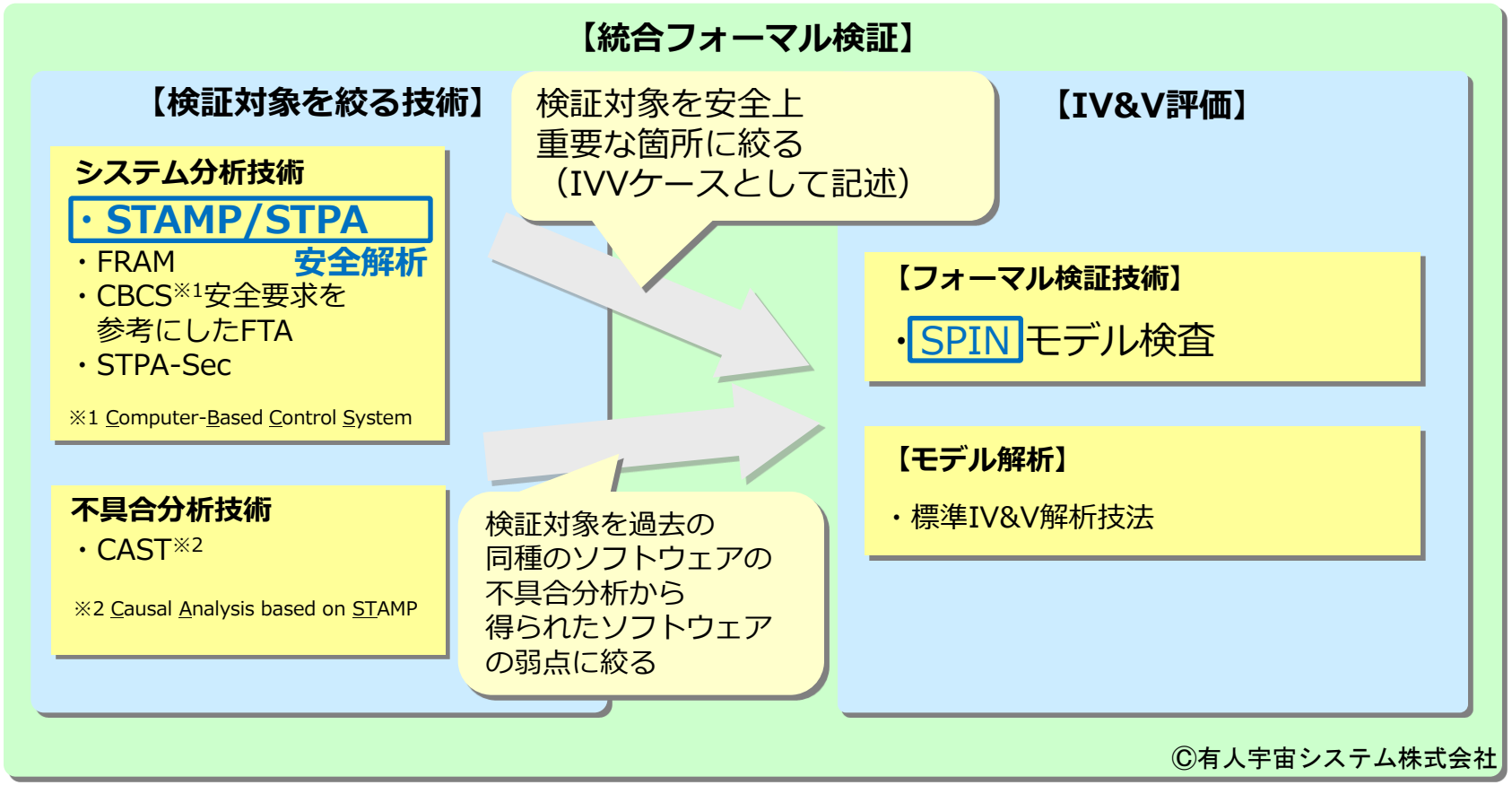




1. 背景と目的
   - 鉄道における踏切制御
2. 駅構内論理装置とその踏切制御機能のSW化
   - 駅構内論理装置（構内LC）
   - 駅構内踏切制御SW化の課題
3. STAMP/STPAの適用
4. その他

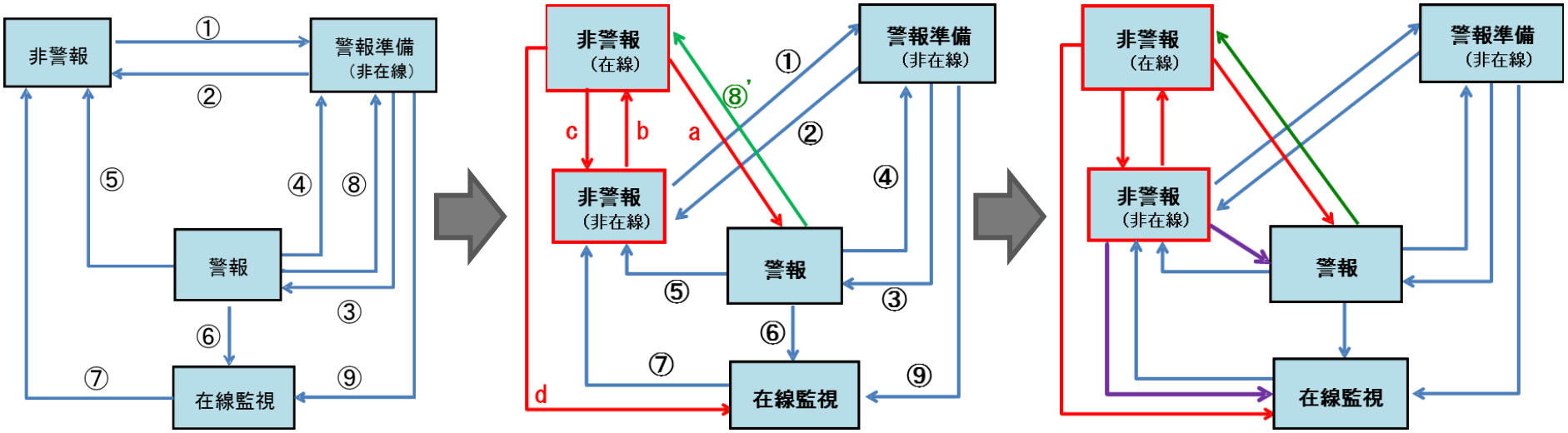
その他

- **統合フォーマル検証**



その他

- モデル検査を通じての状態遷移の修正



その他

- **駅構内踏切制御にSTAMP/STPAは有効**
  - 駅構内論理装置の踏切制御機能について、暗黙知化されていた状態遷移の区分化・明確化を達成
  - 連動装置と踏切制御装置のより厳密な情報のやり取りが必要であることも示された。

- **鉄道分野でSTAMPが幅広く活用出来る可能性**
  - 列車運行管理システム
    - 連動装置、列車、ダイヤ、指令などのインタラクション
  - 車両制御システム
    - ドライバー、ブレーキ、先行列車などのインタラクション
    - 車両だけでもモデルが作成可能(ドア開閉とその表示)