STAMP/STPAを用いた
自動運転システムのリスク分析

-高速道路での合流-

堀雅年*　伊藤信行†　梶克彦*
内藤克浩*　水野忠則*　中條直也*

*愛知工業大学
†三菱電機エンジニアリング

はじめに

- 近年、先進運転支援システムが発展
  - オートクルーズコントロール
  - レーンキープアシスト
- 2020年を目処にレベル３自動運転車の市場化が期待
  - 運転システムが複雑化

出典：官民ITS構想・ロードマップ2017
https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20170530/roadmap.pdf

SAE自動運転レベル

SAE level	運転者	システム	責任
0～2	基本的に 運転を実施	部分的に 運転を実施	運転者
3	システム 非対応時に 運転に介入	システム 対応領域で 運転を実施	システム (非対応時は 運転者)
4～5	運転を実施 しない	全ての 運転の実施	システム

運転者の操作とシステムのどちらを優先すべきか分からないのでハザードの可能性

http://www.sae.org/misc/pdfs/automated driving.pdf

高速道路の自動運転

- レベル3の自動運転車(2020年）
  - 高速道路や自動車専用道での利用
  - 交通量が少なく渋滞がないなどの条件つき
  - 自動運転システムへの運転者の介入を想定

- 一般的な運転者
  - 自動運転の機能を十分把握していない

合流地点で，運転者の介入により
ハザード発生の可能性

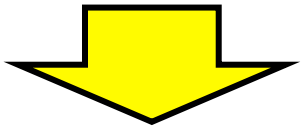
高速道路合流時の法的問題

ケース	法規定 （要旨）	実勢交通	課題
渋滞する本線上の自動車との合流時の優先関係	[道交法第75条の6第1項] 本線車道に入ろうとする場合、本線上を通行する自動車の進行妨害をしてはならない	渋滞時などは合流側が頭を差し込まないと合流できないことが多い	実勢交通の合流方法が進行妨害にあたれば違反となり自動運転車は合流困難となる

出典：日本自動車工業会
https://www.npa.go.jp/koutsuu/kikaku/jidounten/kentoiinkai/02/shiryou2.pdf#search=%27%E9%AB%98%E9%80%9F%E9%81%93%E8%B7%AF%E5%90%88%E6%B5%81%E6%99%82+%E6%B3%95%E7%9A%84%E5%95%8F%E9%A1%8C%27

研究目的

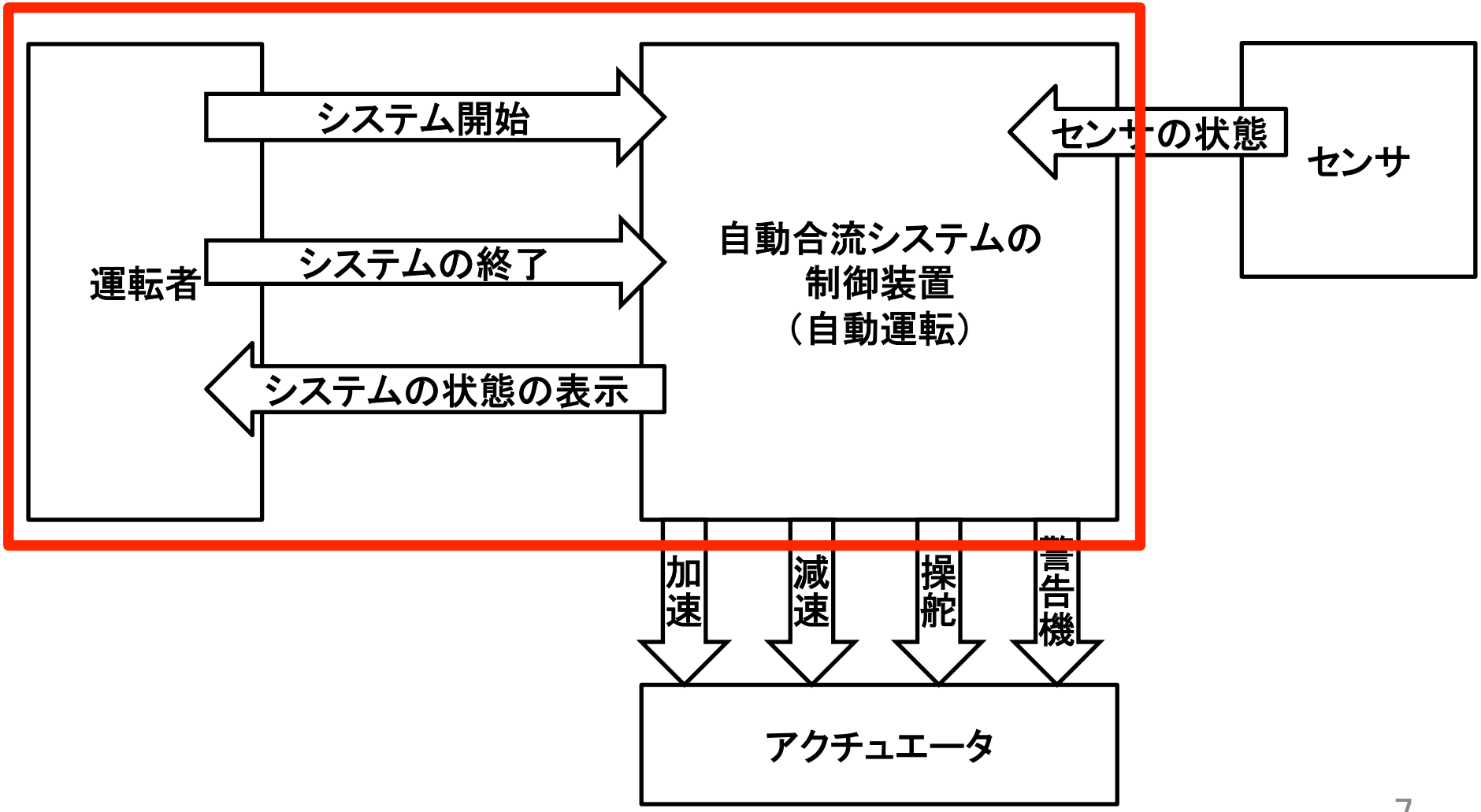
- レベル3の自動運転システム
  - 高速道路での合流部を対象
- STAMP/STPAを用いたハザード分析
  - 自動合流システムと運転者の関係に注目



- 安全性を高めるための要件を検討

コントロールストラクチャー

対象とする部分　運転者と自動合流システムとの関係

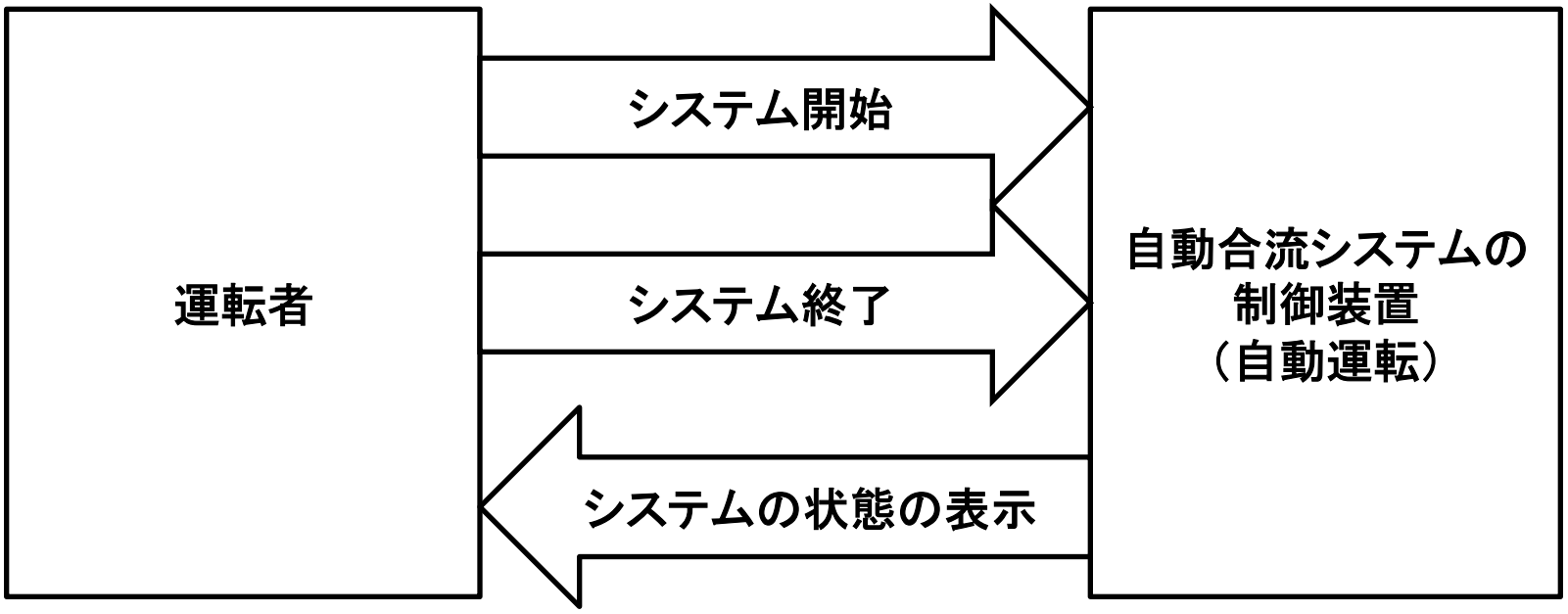


アクシデント、ハザード、安全制約

アクシデント	ハザード	安全制約
接触する	システムは開始したのに合流できない	システムは開始したら合流しなければならない
	合流中のシステム解除	合流中に運転者は意図しないシステムの解除をしない
	運転者がシステムの監視をできてない	運転者がシステムを監視できる状態でなければならない
	システムを勘違いしている	運転者はシステムを理解し、使用できる状況を理解しなければならない

対象のコントロールストラクチャー

- 運転者と自動合流システムのみを抽出



Unsafe Control Action

運転者の操作が正しく伝わらない

運転者の操作が正しくない

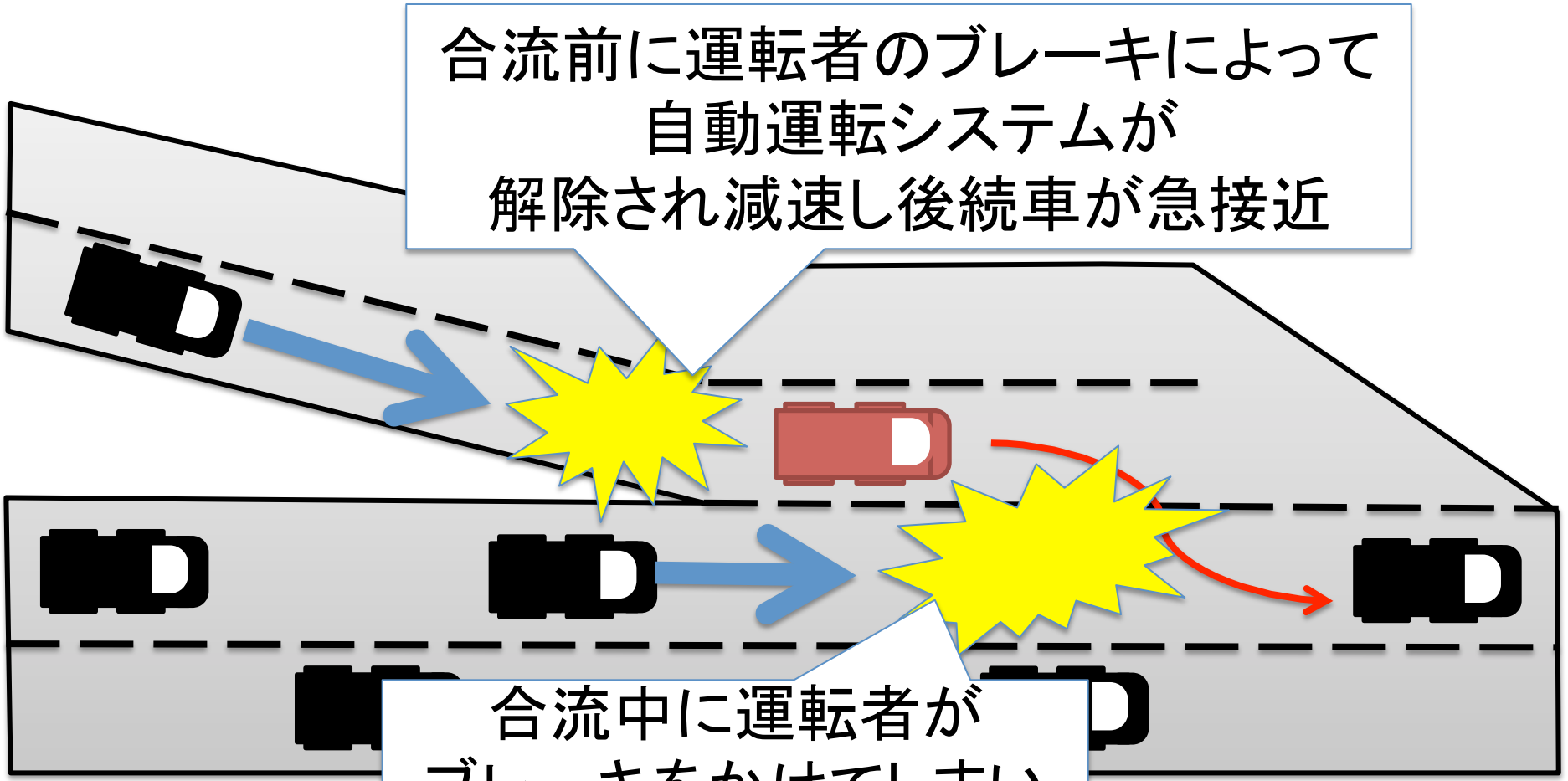
UCA		ling d		Stop too soon / Applying too long
システム開始	自動運転が開始しない（ハザード）	自動運転が開始する	合流が るのにシステ が開始して い（ハザード	
システム終了	運転者が危険と判断したのに合流を続ける（ハザード）	合流中にシステムが終了する(ハザード)	合流しきってないのに終了してしまう(ハザード)	
システムの状態の表示	運転者が状態を分からない(ハザード)	間違ったものが表示される(ハザード)	間違ったものが表示される(ハザード)	状態が更新されない(ハザード)

UCA	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
システム開始（合流開始）	自動運転が開始しない（ハザード）		合流が始まるのにシステムが開始してない（ハザード）	
システム開始（合流中）		自動運転が開始できない箇所で開始（ハザード）	合流中に開始してしまう（ハザード）	
システム終了	運転者が危険と判断したのに合流を続ける（ハザード）	合流中にシステムが終了する(ハザード)	合流しきってないのに終了してしまう(ハザード)	
システムの状態の表示	運転者が状態を分からない(ハザード)	間違ったものが表示される(ハザード)	間違ったものが表示される(ハザード)	状態が更新されない(ハザード)

Hazard Causal Factor

HCF	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
システム終了	部品故障、経年変化	外部環境変化による終了 運転者が間違ってブレーキ	外部環境変化による終了 運転者が間違ってブレーキ	

高速道路の合流のハザード



想定する合流システムと運転者にはハザード別のセンサを用いて安全性を高める必要性
路車間通信による情報提供を検討

対策

		causes hazard	Too late	soon / Applying too long
システム終了	運転者が危険と判断したら運転者に操作を返す	センサで運転者を監視し、どちらを優先するか判断	合流中なら解除しない	

相反する対策

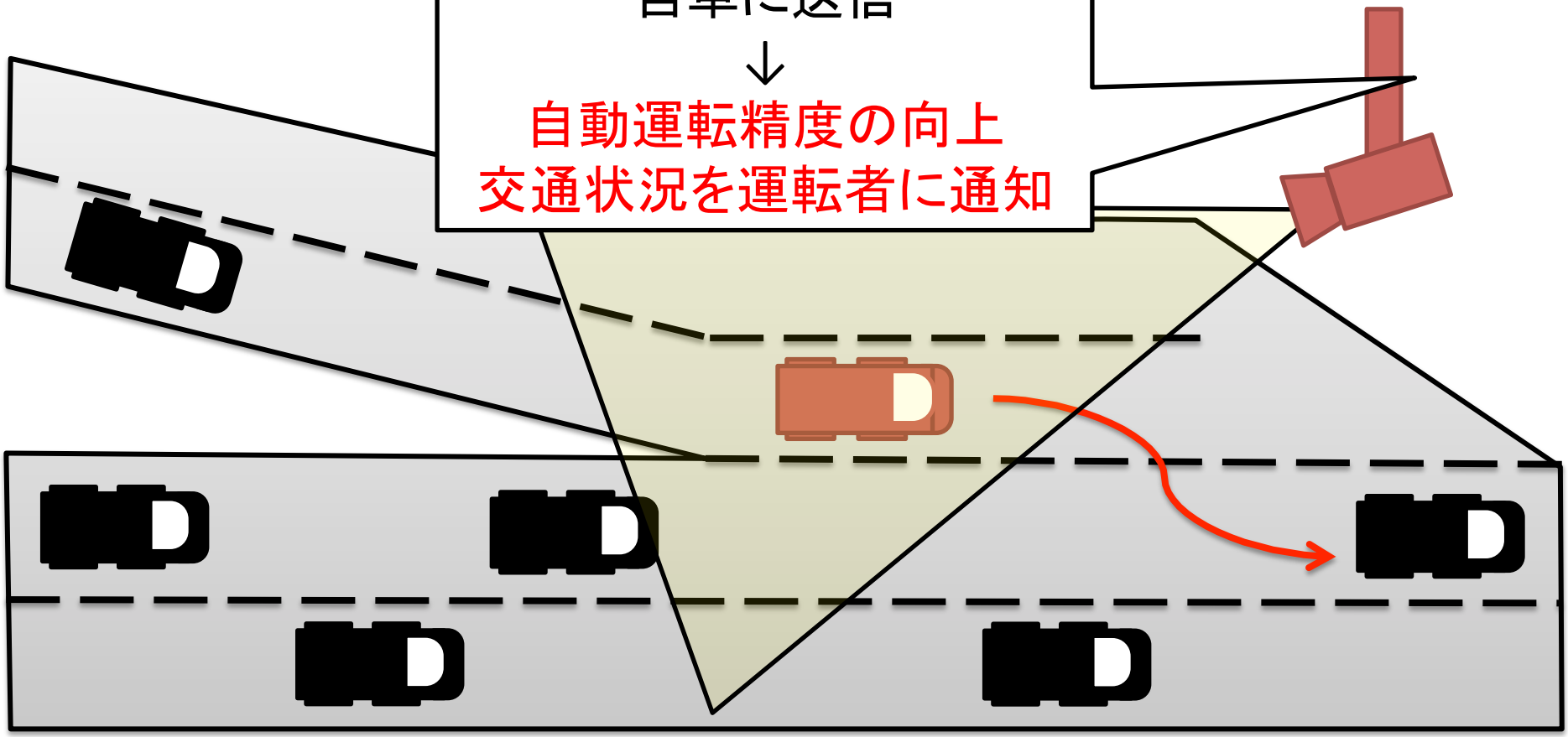
システムより運転者の操作を優先する

カメラなどで運転者の状態を見て優先するか判断

運転者よりシステムの操作を優先する

路車間通信を加えた合流

他の車両状況を
自車に送信
↓
自動運転精度の向上
交通状況を運転者に通知

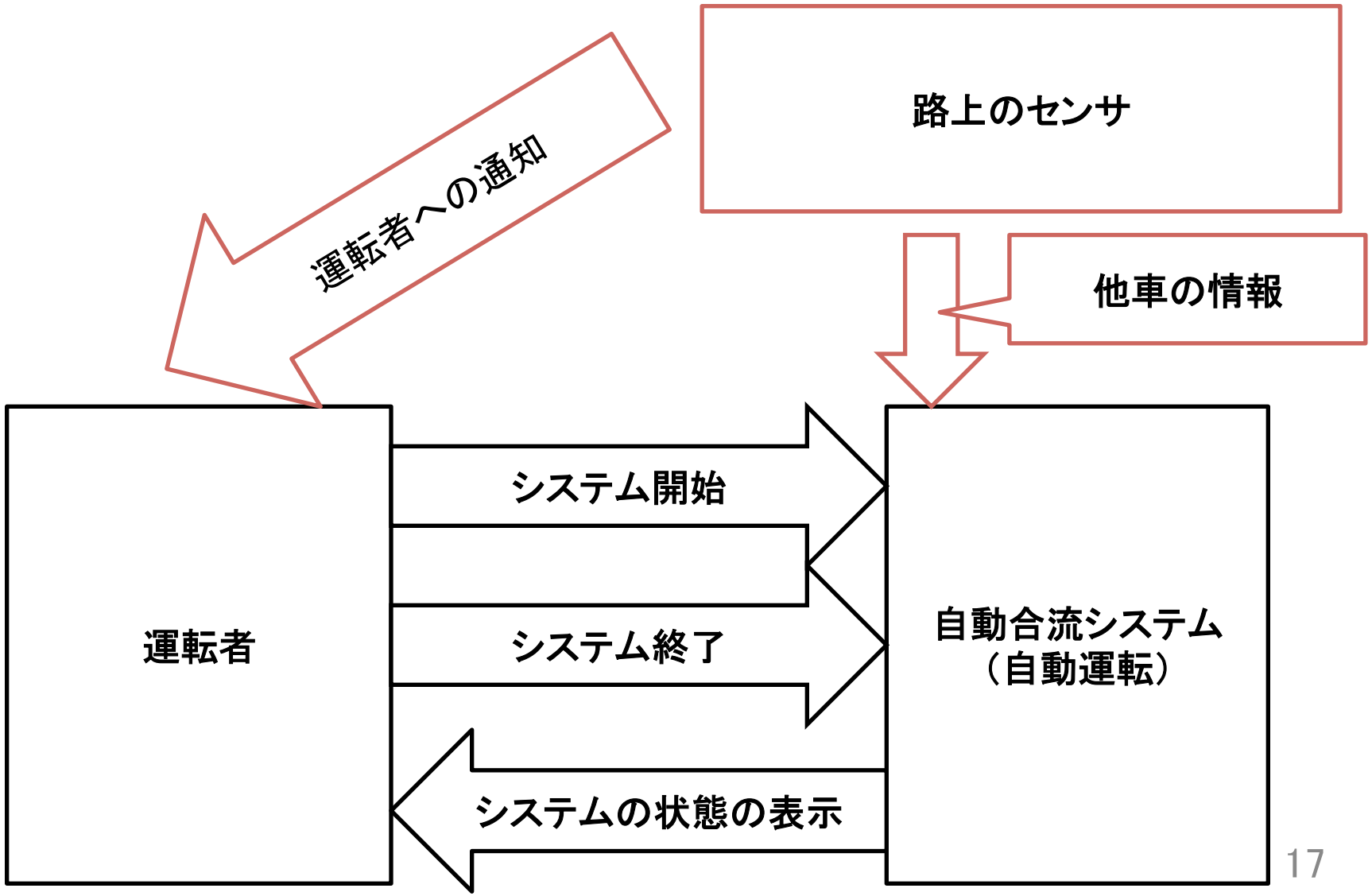


路車間通信を加えた分析

- 路車間通信は今後の自動運転に必要不可欠
- 情報を多く与えることで，より正確な判断を自動合流システムができる

- 改良により課題に対応できるかを分析
  - 課題：急なブレーキなどによる
    システム終了による接近
    ：運転者の不安を取り除く

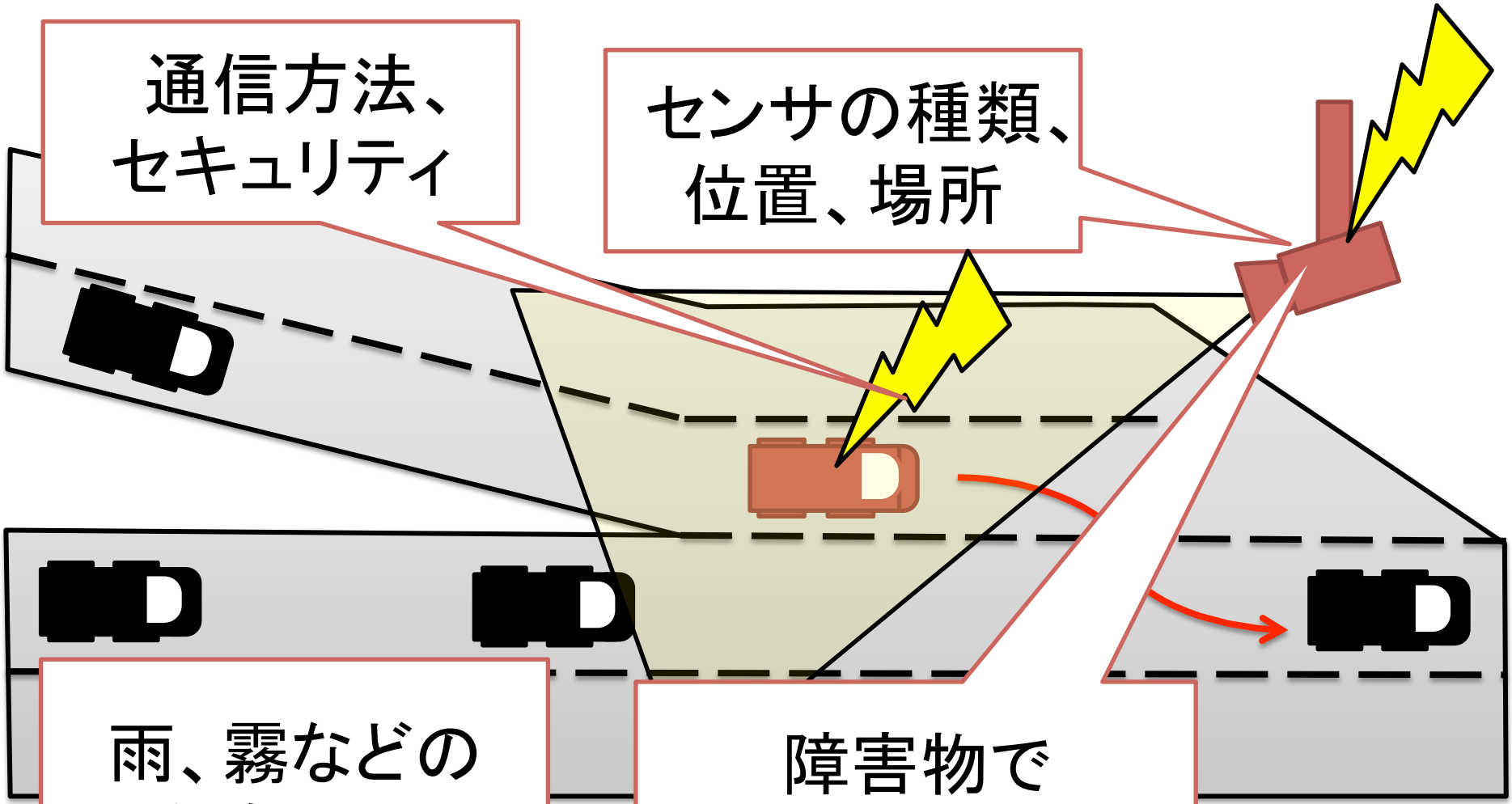
路車間通信を加えたCS



路車間通信を加えた分析結果

- 外部センサの情報でより正確な操作が可能
  - システム判断の信頼性が向上
  - 外部センサに誤りがなければ運転者の操作をキャンセル
- 外部のカメラなどから俯瞰的な交通状況を運転者に通知
  - 不安の軽減

路車間通信を用いた合流の課題

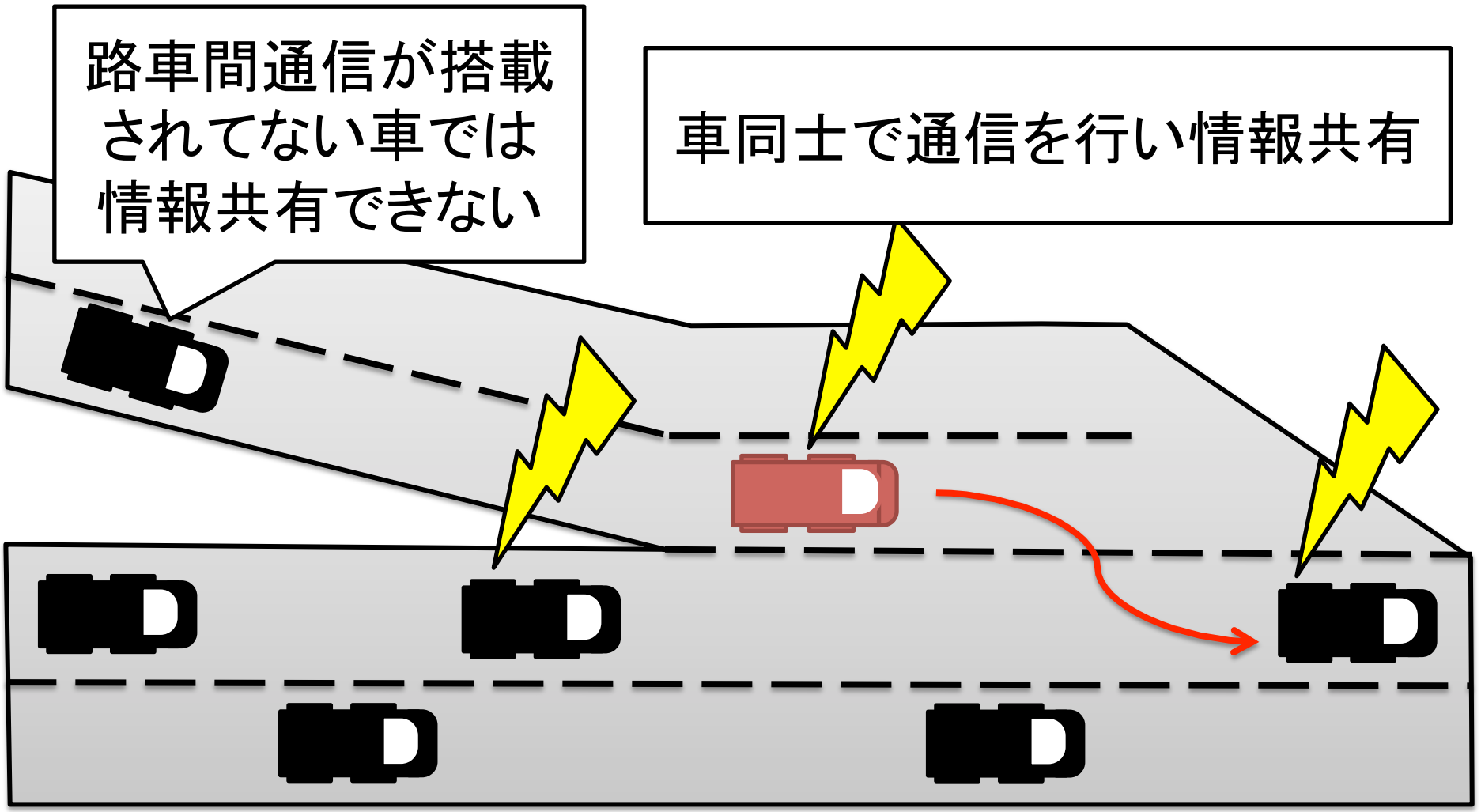


今後の課題

- 路車間通信の導入で別なハザードの可能性
  - 再分析の必要性がある

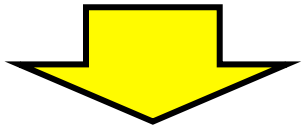
- 運転者状態がモニターできれば、優先度が決定できるか
  - 運転者のセンシング技術を含めた分析が必要

車車間通信



おわりに

- レベル3の自動運転システム
  - 高速道路での合流部を対象
- STAMP/STPAを用いたリスク分析
  - 自動合流システムと運転者の関係に注目



- 安全性を高めるための要件を検討
  - 自動合流システムと運転者の優先度に課題
  - 路車間通信、車車間通信による対策の可能性（再分析要）