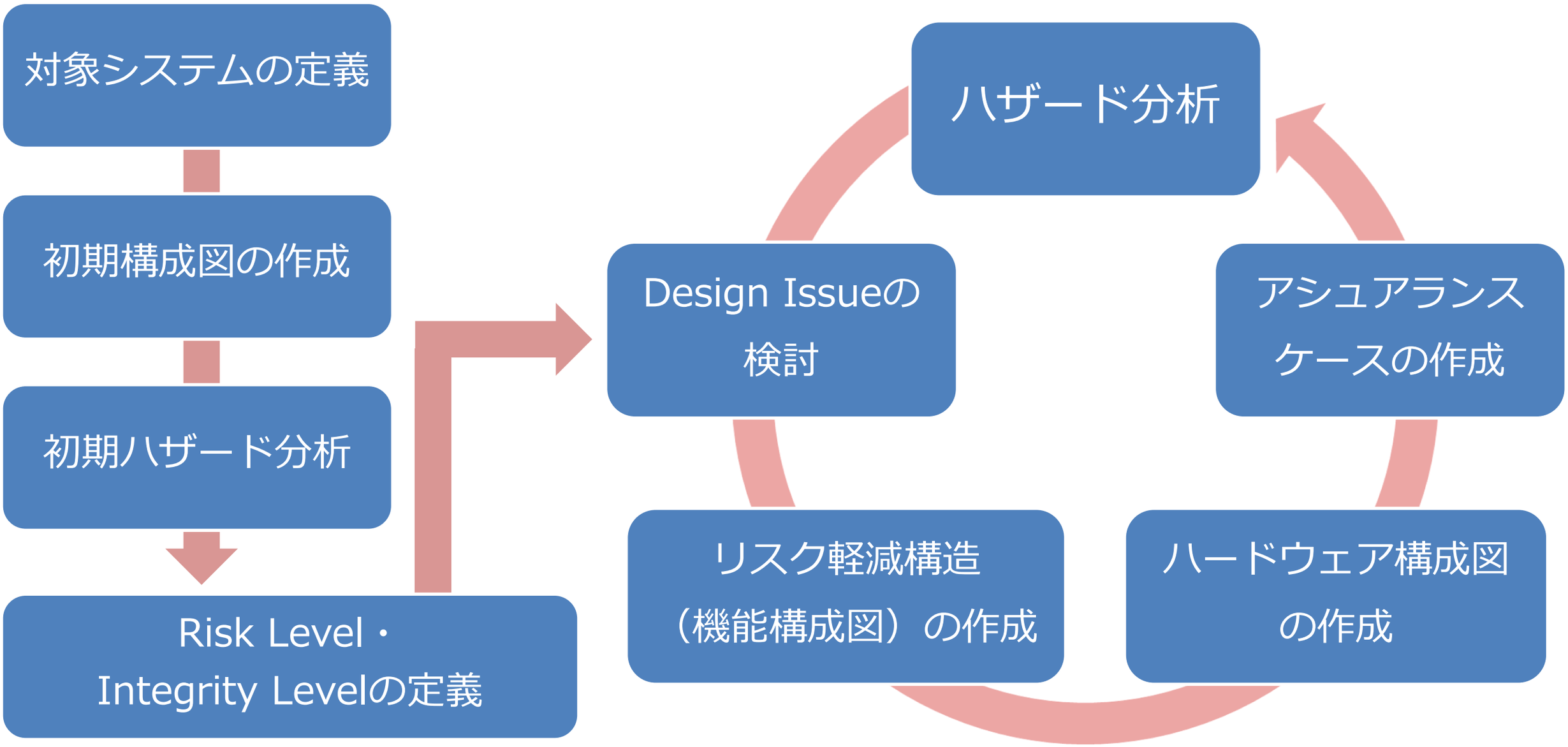
セッション4 システムアシュアランス教育

車両間アドホックネットワークにおけるシステムアシュアランスの検討

奈良先端科学技術大学院大学 情報科学研究科
情報基盤システム学研究室　鷲尾 直大

演習内容

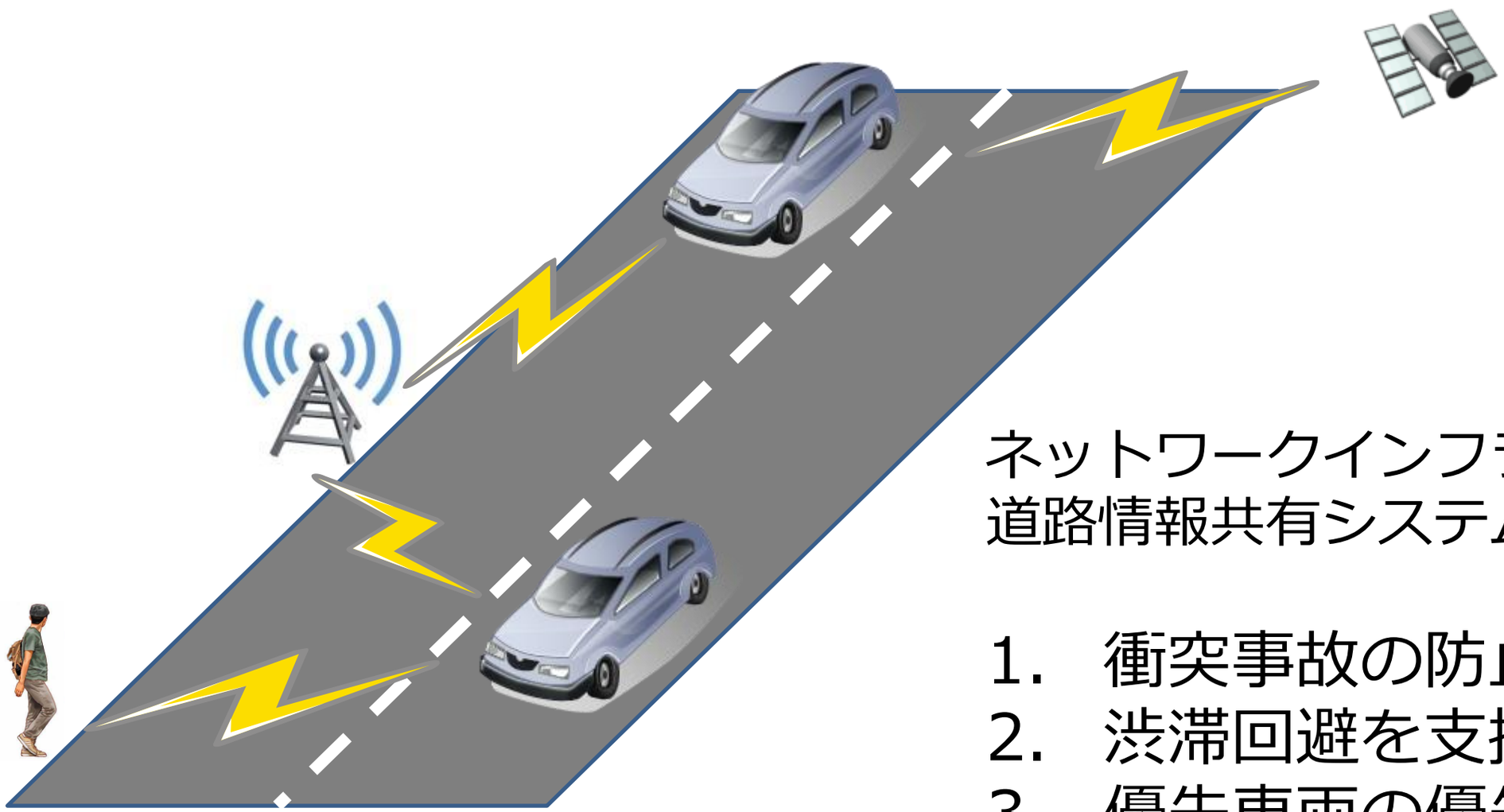
システムアシュアランスに基づくシステム設計の手順



対象システムの定義

VANET(Vehicular Ad-hoc NETwork)

安全運転支援のための車両-車両，車両-歩行者間通信システム

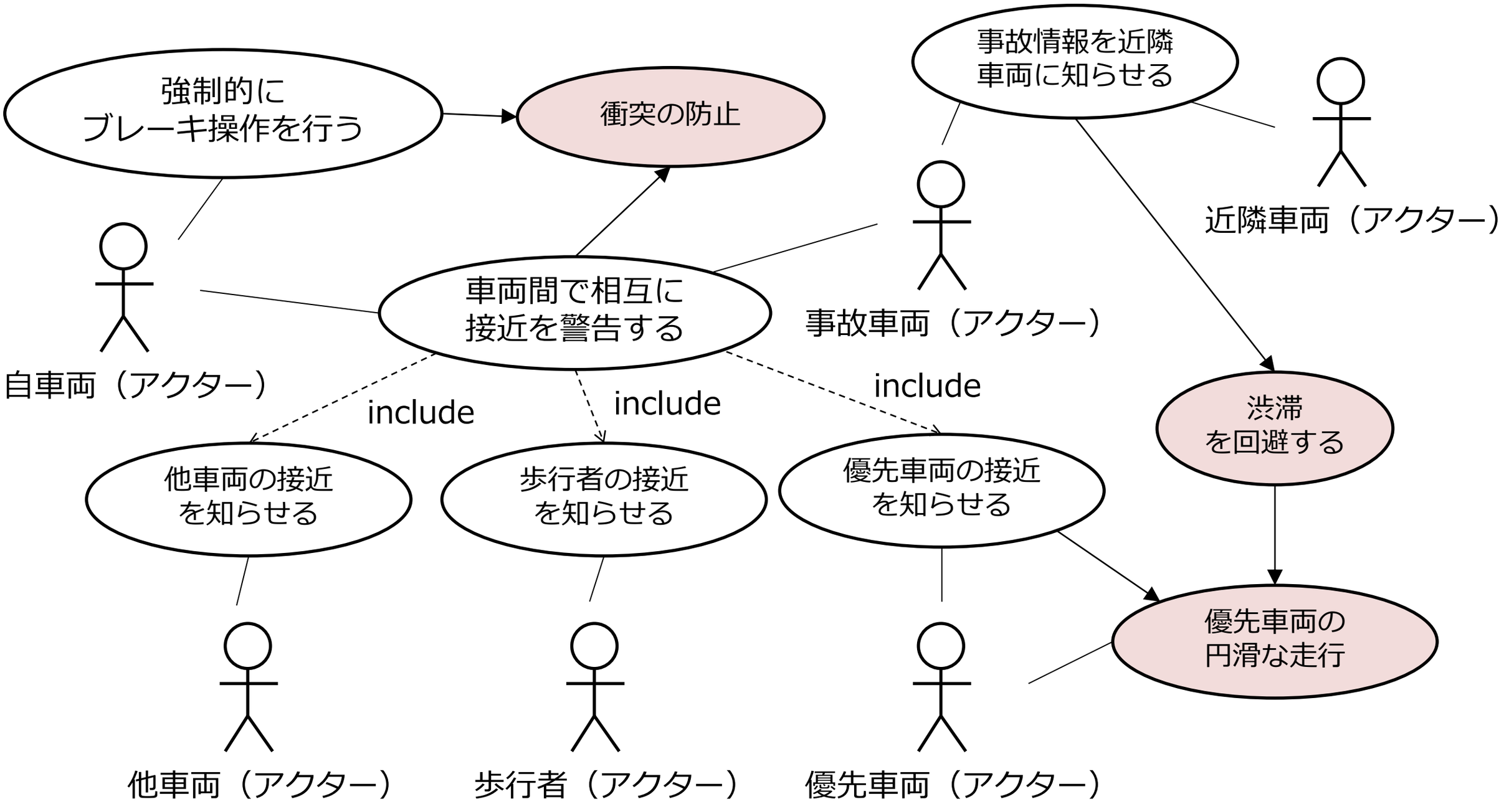


ネットワークインフラを必要としない
道路情報共有システムの目的

1. 衝突事故の防止を支援
2. 渋滞回避を支援
3. 優先車両の優先走行

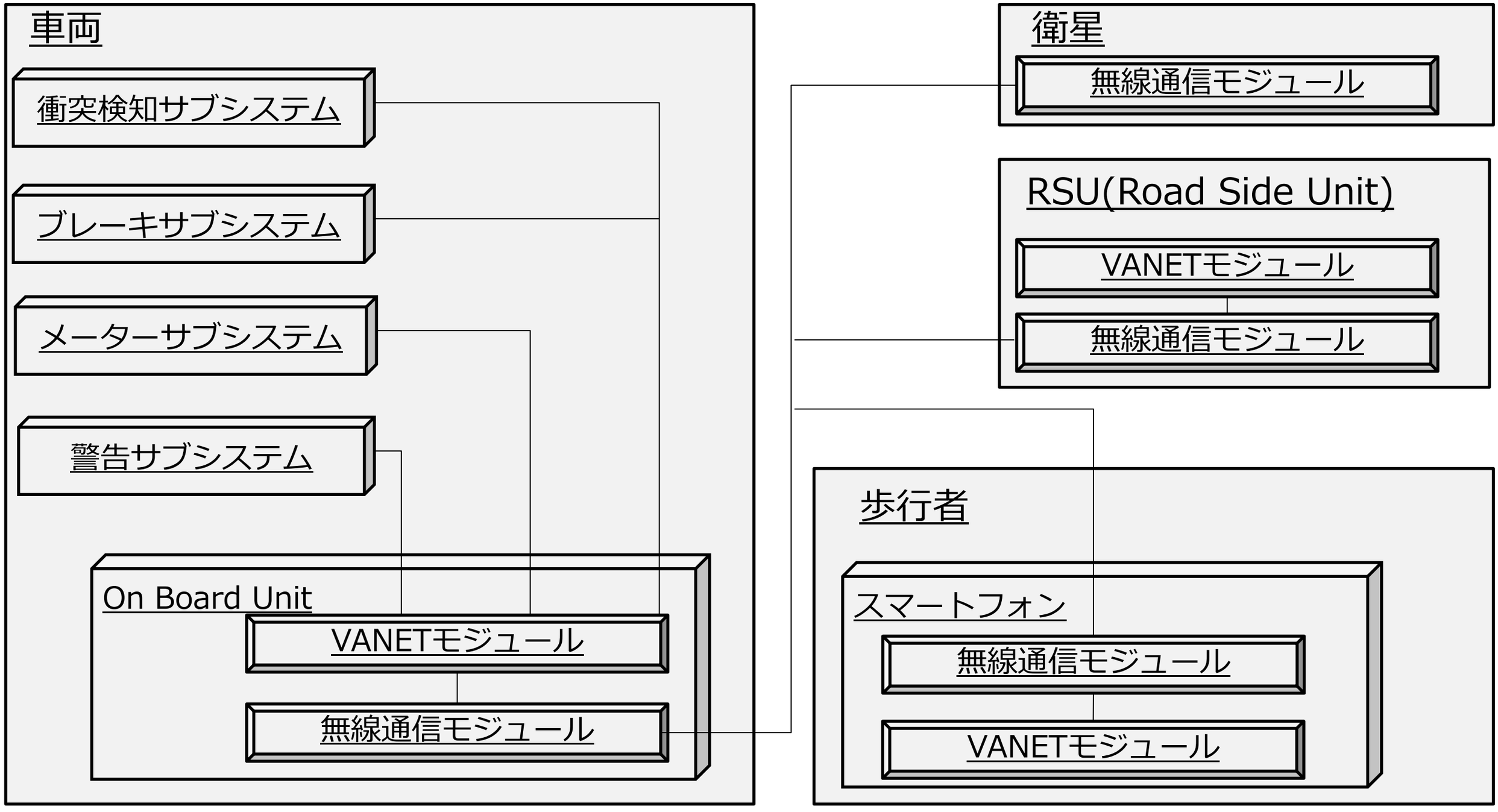
初期構成図の作成 – 機能構成

初期の機能構成図（ユースケース図により機能を決定）



初期構成図の作成－ハードウェア構成

初期のハードウェア構成図（初期の機能構成図により決定）



ハザードの分析－手法一覧

- PHA (Preliminary Hazard Analysis)
  - 初期構成図に対するハザード分析
- HAZOP (Hazard Operability Analysis)
  - リスク軽減を行う過程でのハザード分析
- FTA (Fault Tree Analysis)
  - ハザードの原因と分類に関する分析
- FMEA (Failure Mode Effects Analysis)
  - ハザードの与える影響の分析

初期ハザード分析－PHA

情報整理シート（株式会社 三菱総合研究所）

システム側の視点の分類		シート名
システム自体	個々の構成要素自体に関する情報	危険要素の特定
		機能不全に陥る条件の把握
	個々の構成要素間に関する情報	安全に関わるインターフェースの特定
	システムの制御、ソフトウェアに関する情報	安全に関わるソフトウェア設計の特定
外部とのインタフェース	システム－外部環境間に関する情報	安全性に影響する環境条件の特定
	システム－運用事象間に関する情報	運用・保守法案、非常時対応方案の整理
総合的な視点		危険物質と施設/設備の関わりの把握
		安全性に関わる機器、保護装置の把握

初期ハザード分析－PHA

ハザードチェックリスト（株式会社 三菱総合研究所）

・ソース（危険要素）

機械的	：衝突，衝撃，落下物，倒壊，転倒，落下
電気的	：感電，過熱，停電，爆発，通電，ショート
熱的	：氷結，温度変化，高温気体
可燃性	：摩擦，稲妻，強風，化学汚染

・メカニズム（事故に至る過程）

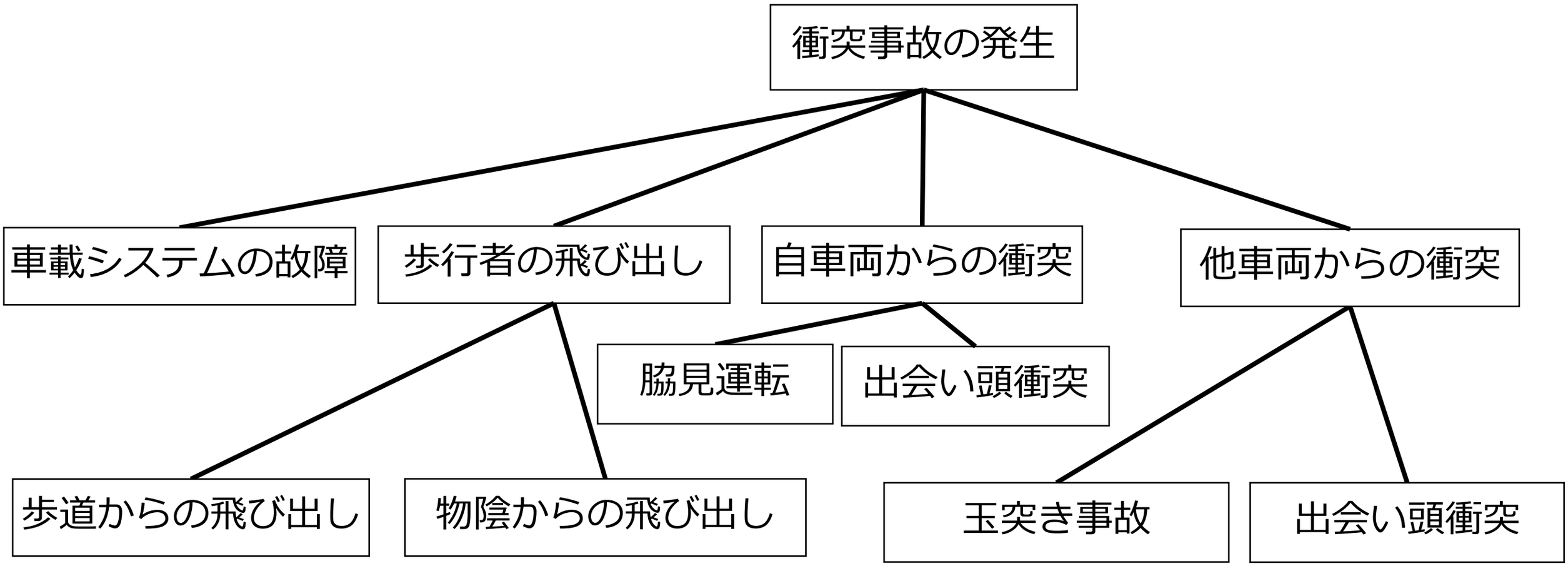
予測しない始動	：落雷，誤ったデータの送信，不慮の操作
故障モード	：センシング機能の停止，通信機能の停止
物体の破損・故障	：劣化，ブレーキの故障，カメラの故障，警報装置の故障

・アウトカム（事故事象）

物理障害	：衝突，爆発，感電，火傷
財産被害	：火災，個人情報の漏えい，車両変形，車両故障
環境被害	：汚染，無線周波の妨害

初期ハザード分析－FTA

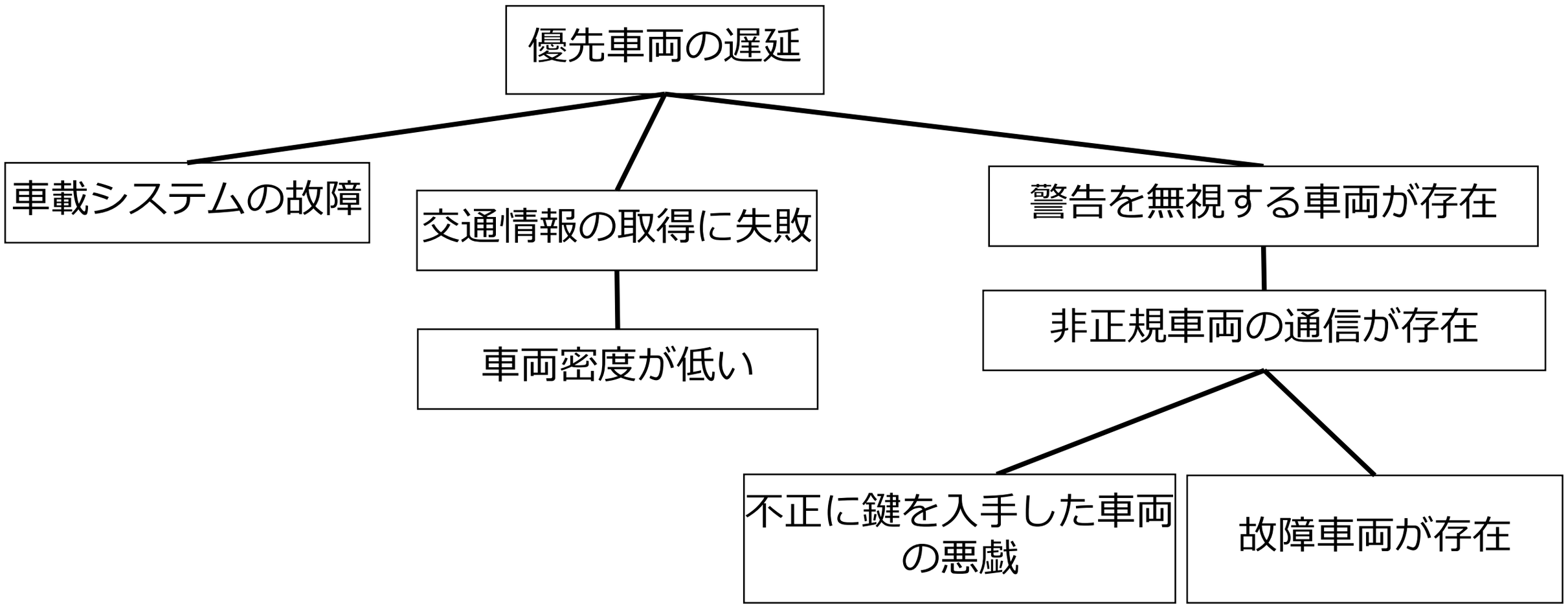
初期の簡易FTA 1
PHAによって識別されたハザードチェックリストを基にツリーを作成



アシュアランスケースの目的 ：
FTAの葉となる事象への対策が行われていることを証明すること

初期ハザード分析－FTA

初期の簡易FTA２
PHAによって識別されたハザードチェックリストを基にツリーを作成



アシュアランスケースの目的 ：
FTAの葉となる事象への対策が行われていることを証明すること

Risk Levelの定義

セキュリティ

Level S3 ： 強制ブレーキの不正発動
Level S2 ： 個人情報に不正アクセス可能
Level S1 ： 車の状態の不正参照可能

事故の深刻さ

Level S4： 歩行者への危害
Level S3： ドライバーを含む同乗者への危害
Level S2： 緊急車両の遅延
Level S1： 円滑な交通の妨害

事故の頻度

Level E4： 高い
Level E3： 中程度
Level E2： 稀に起きる
Level E1： ほとんど起きない

コントローラビリティ（回避可能性）

Level C3： 回避は困難または不可能
Level C2： 普通は回避可能
Level C1： 簡単に回避可能

Integrity Levelの定義

VANET-IL assignment (ISO26262-3:2011におけるASIL決定表を参考に作成)

Severity Class	Probabillity Class	Controllability Class C1	Controllability Class C2	Controllability Class C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D
S4	E1	QM	A	B
	E2	A	B	C
	E3	B	C	D
	E4	C	D	D

Design Issueの検討

例：歩行者の識別に関して

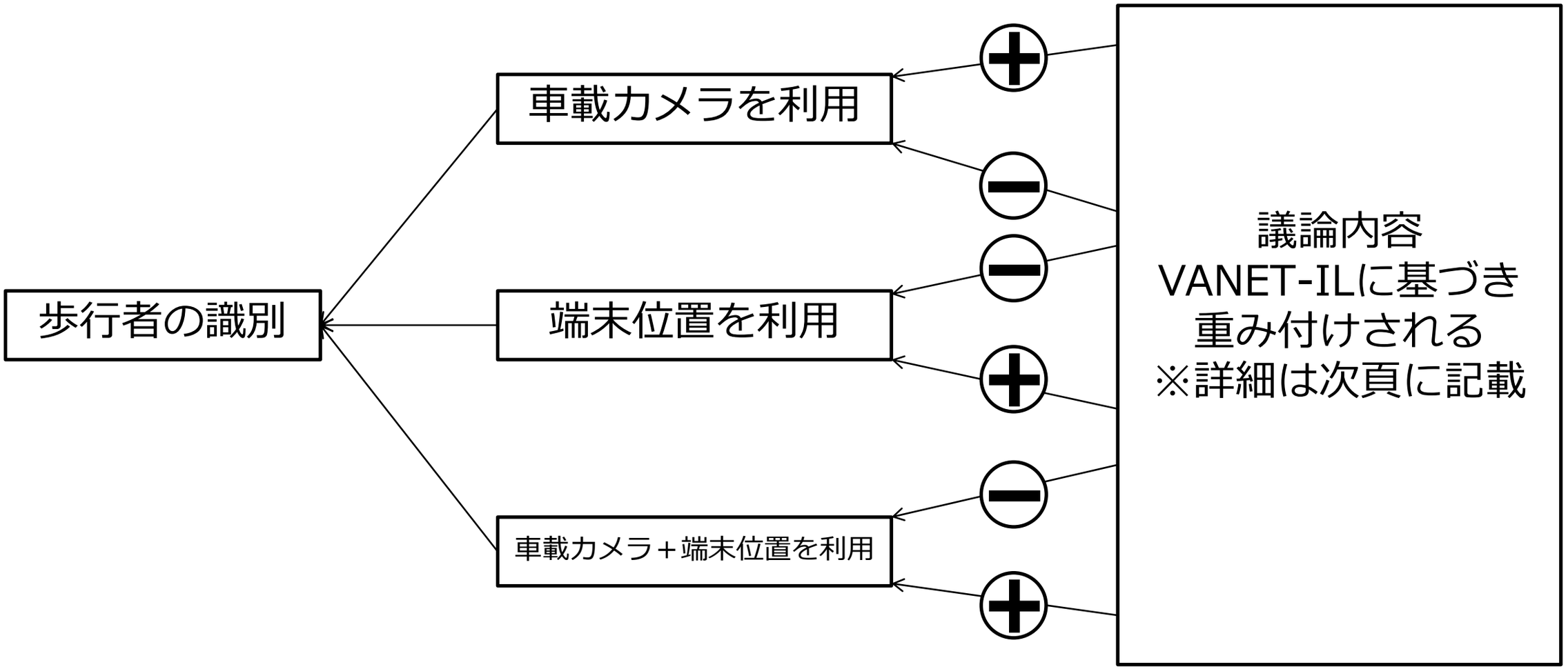
1.車載カメラを利用する
　画像処理を用いて端末を持たない歩行者に対応可能

2.端末位置情報を利用する
　歩行者の死角からの飛び出しに対応可能

3.車載カメラと端末位置情報を両方利用する

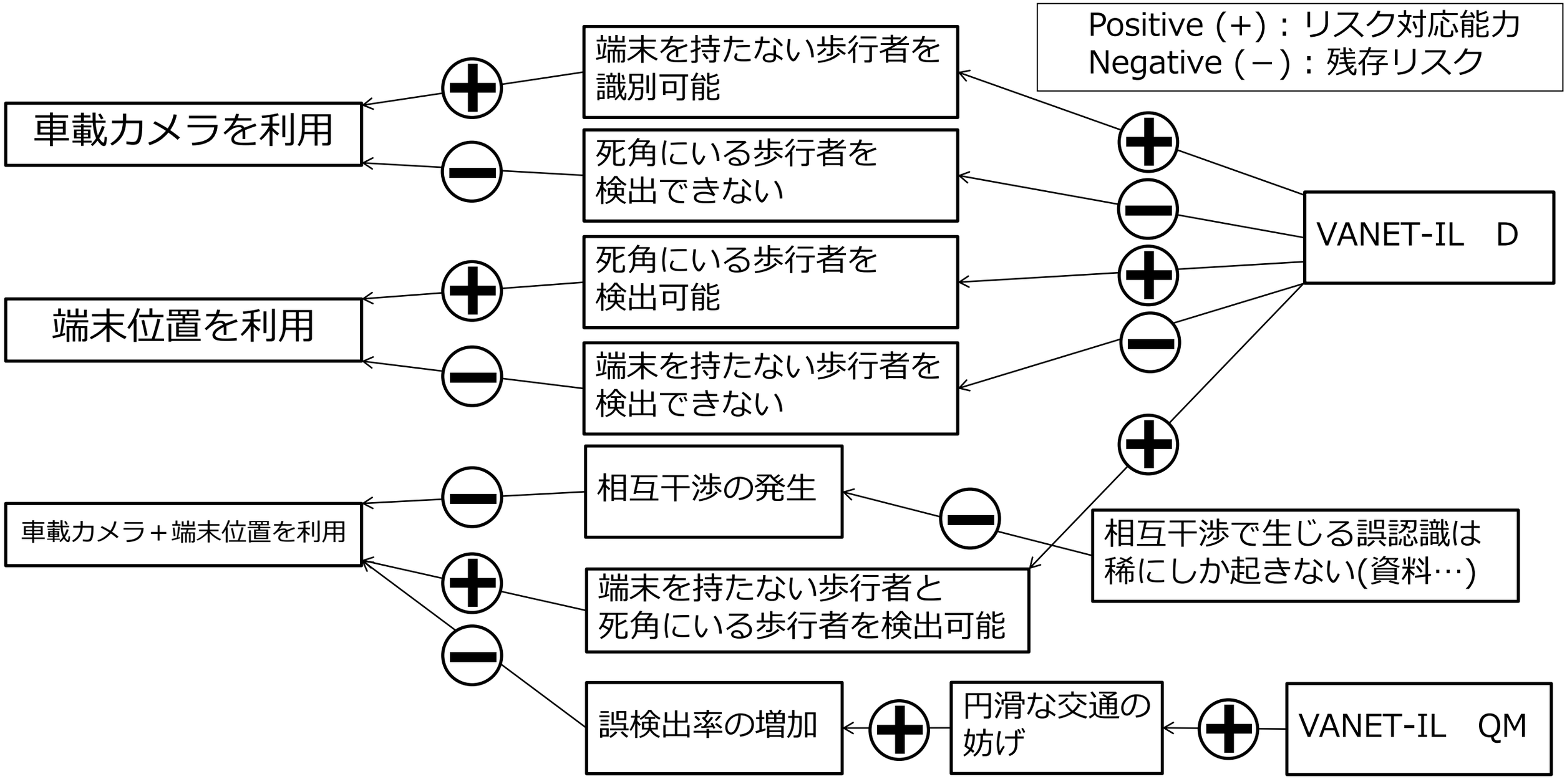
Design Issueの検討

IBISとVANET-ILの組み合わせによる評価



Design Issueの検討

IBISとVANET-ILの組み合わせによる評価

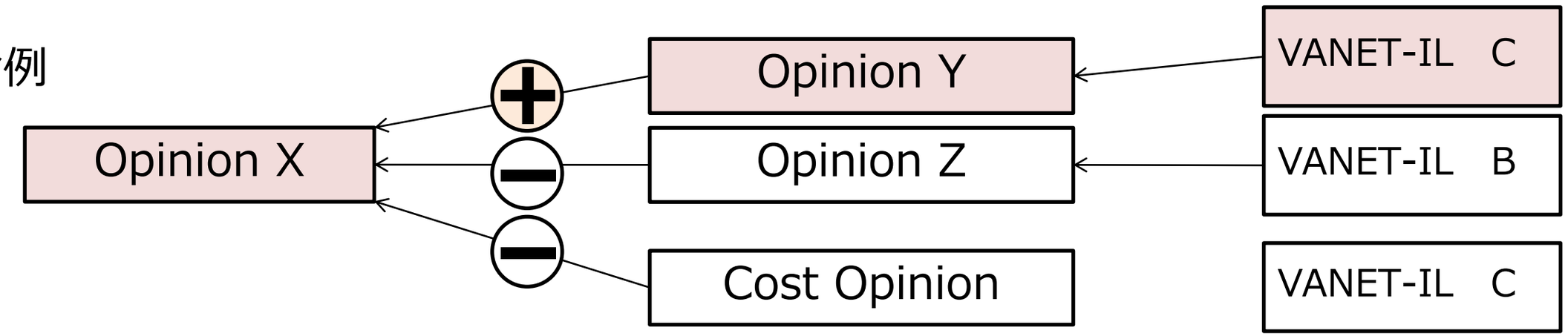


Design Issueの検討

IBISとVANET-ILの組み合わせによる評価

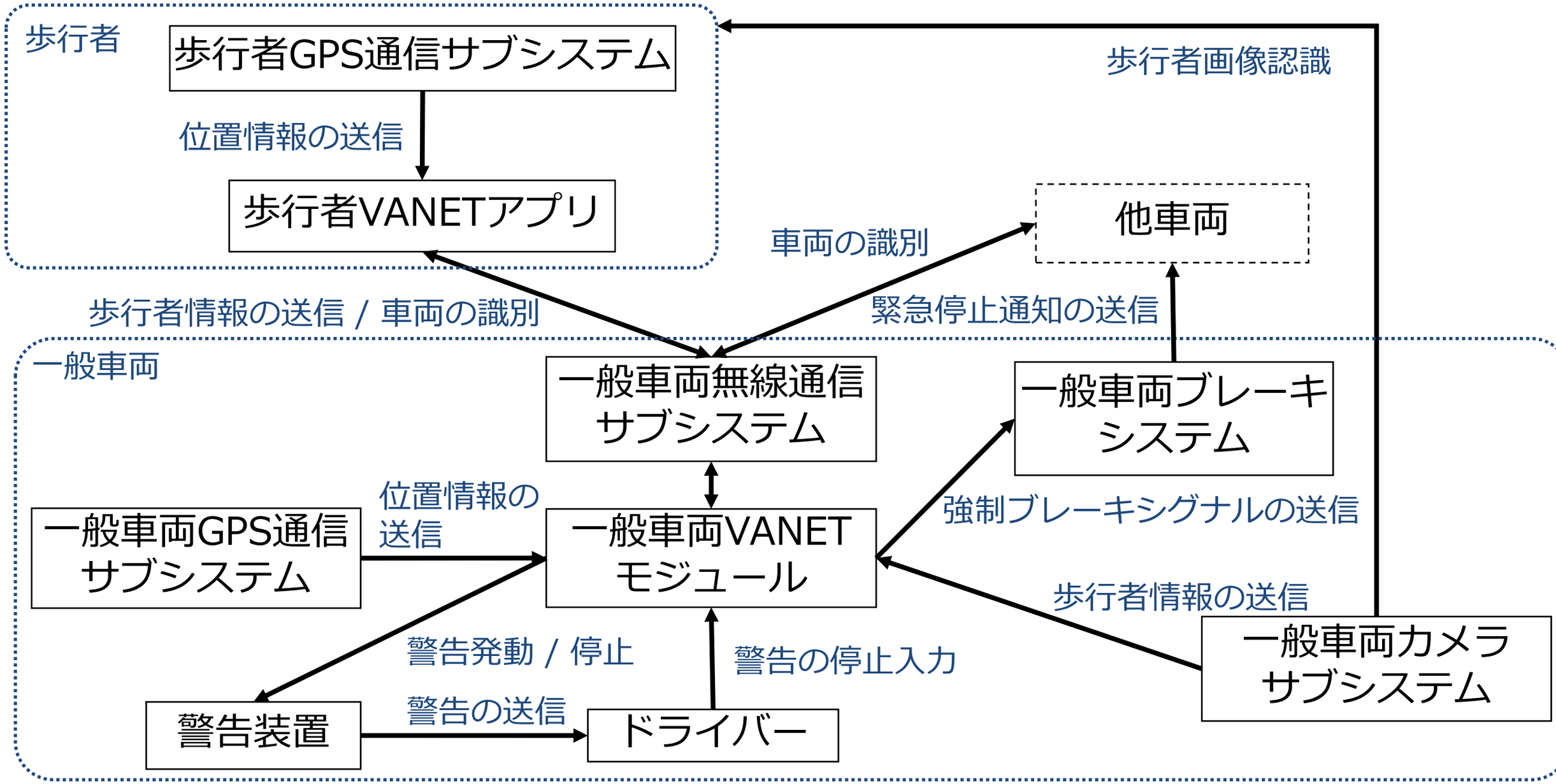
	リスク対応能力(+)	残存リスク(－)	コスト(－)
VANET-IL A	0.2	0.2	0.1
VANET-IL B	0.4	0.4	0.3
VANET-IL C	0.6	0.6	0.5
VANET-IL D	0.8	0.8	0.7

議論例



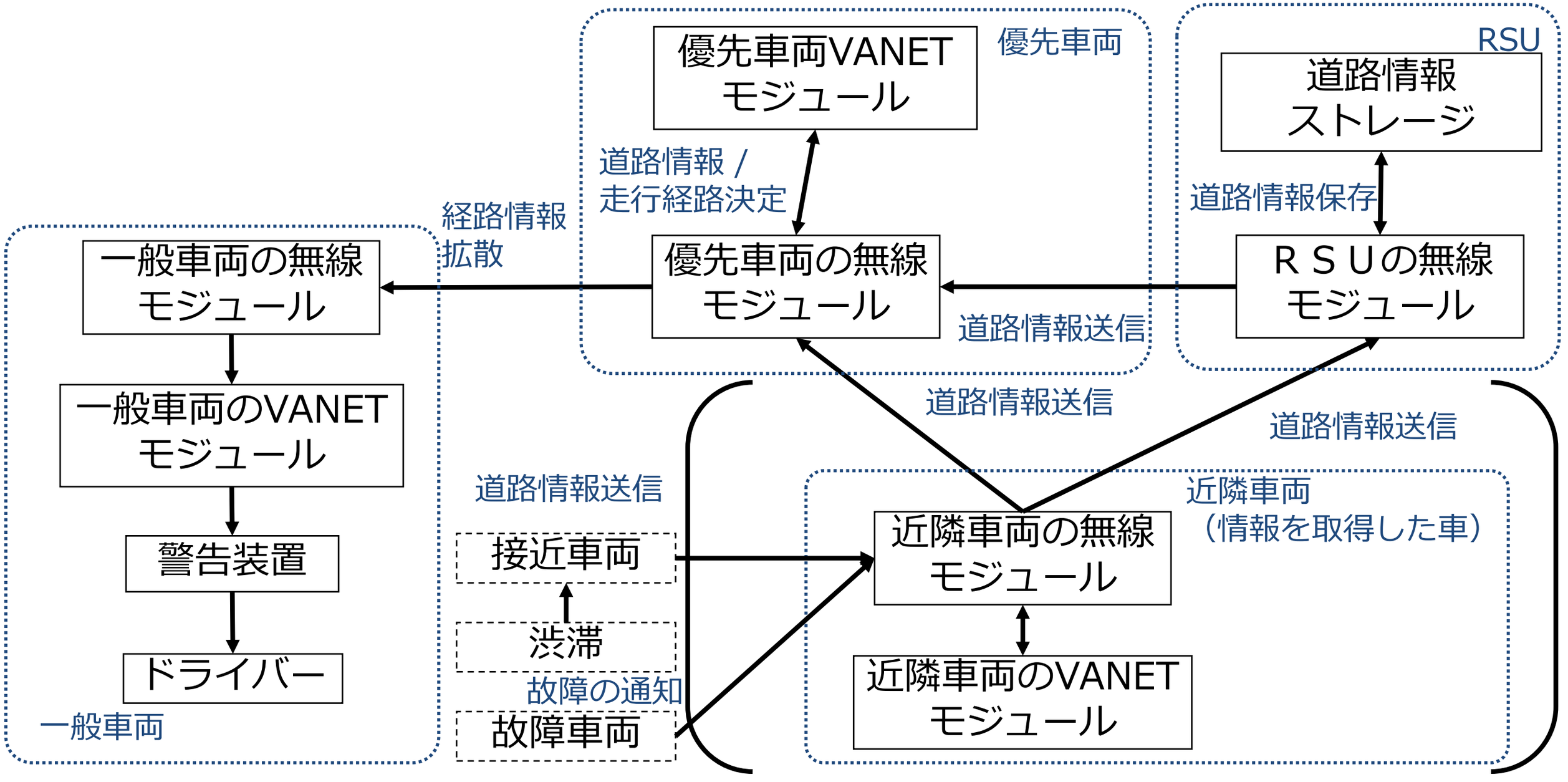
リスク軽減構造の作成

衝突事故の防止を支援するためのリスク軽減構造（機能構成図１）



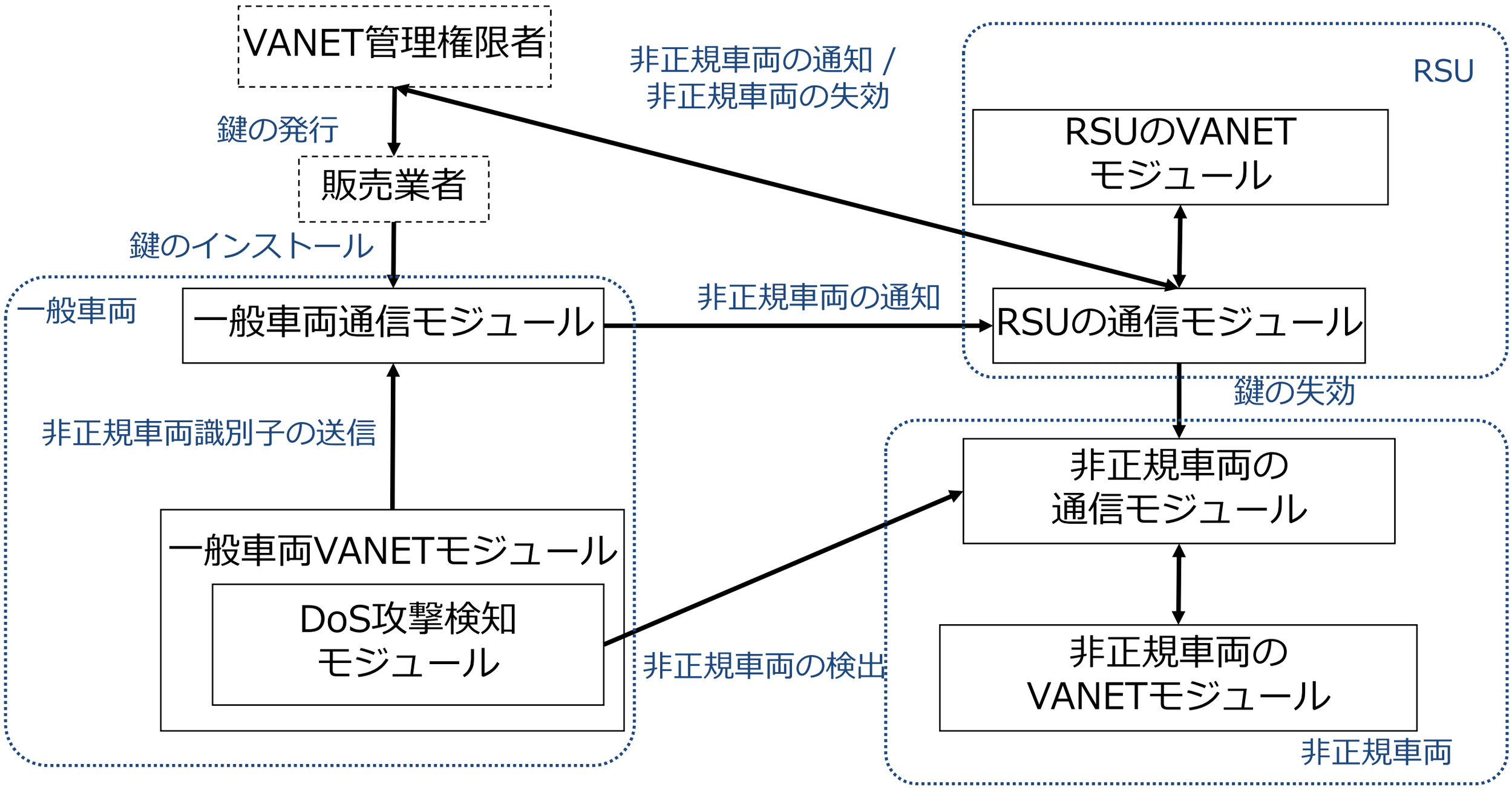
リスク軽減構造の作成

優先車両を優先的に走行させるためのリスク軽減構造（機能構成図２）



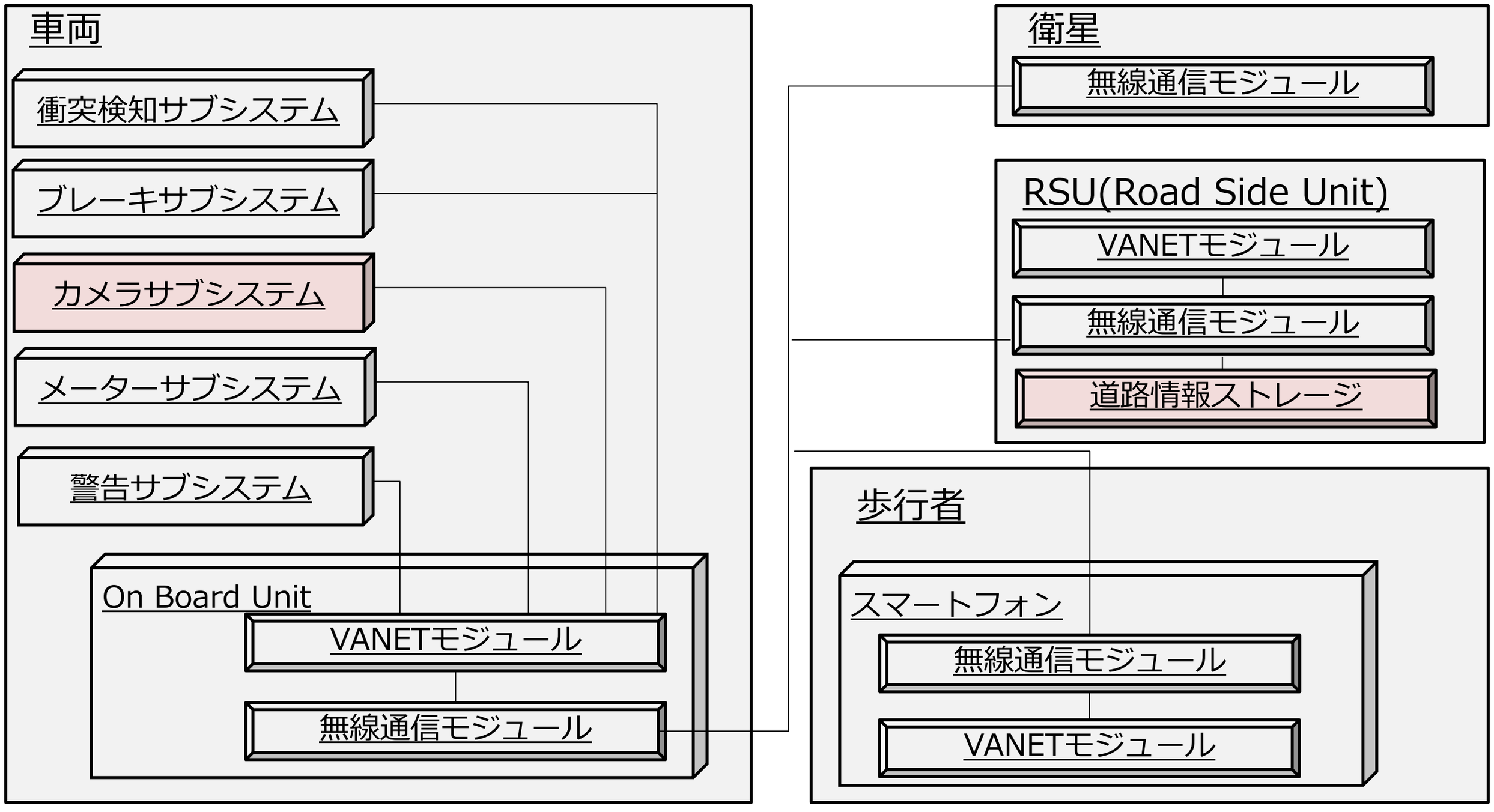
リスク軽減構造の作成

非正規車両のアクセスを禁止するためのリスク軽減構造（機能構成図３）



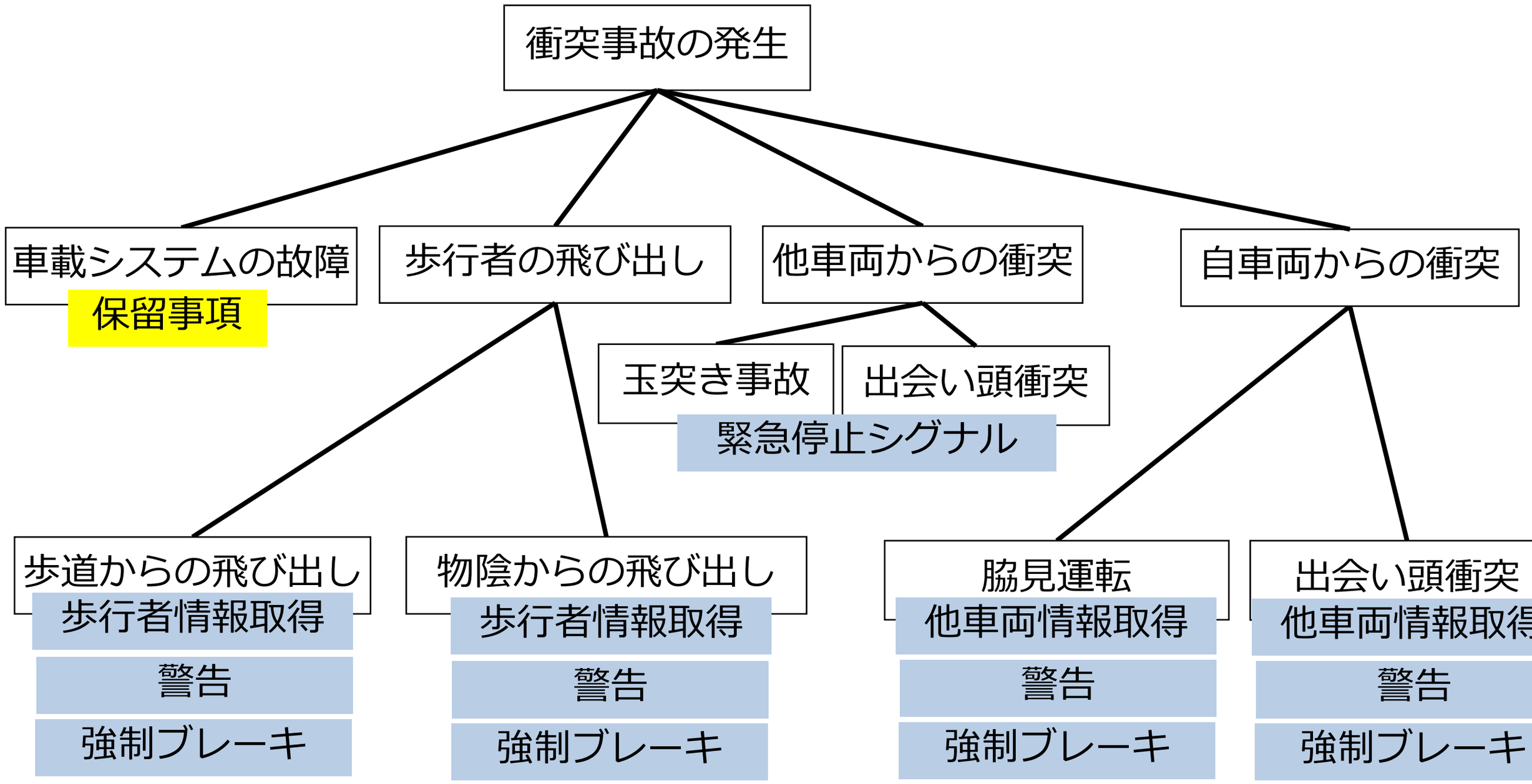
ハードウェア構成図の作成

ハードウェア構成図（機能構成図により決定）



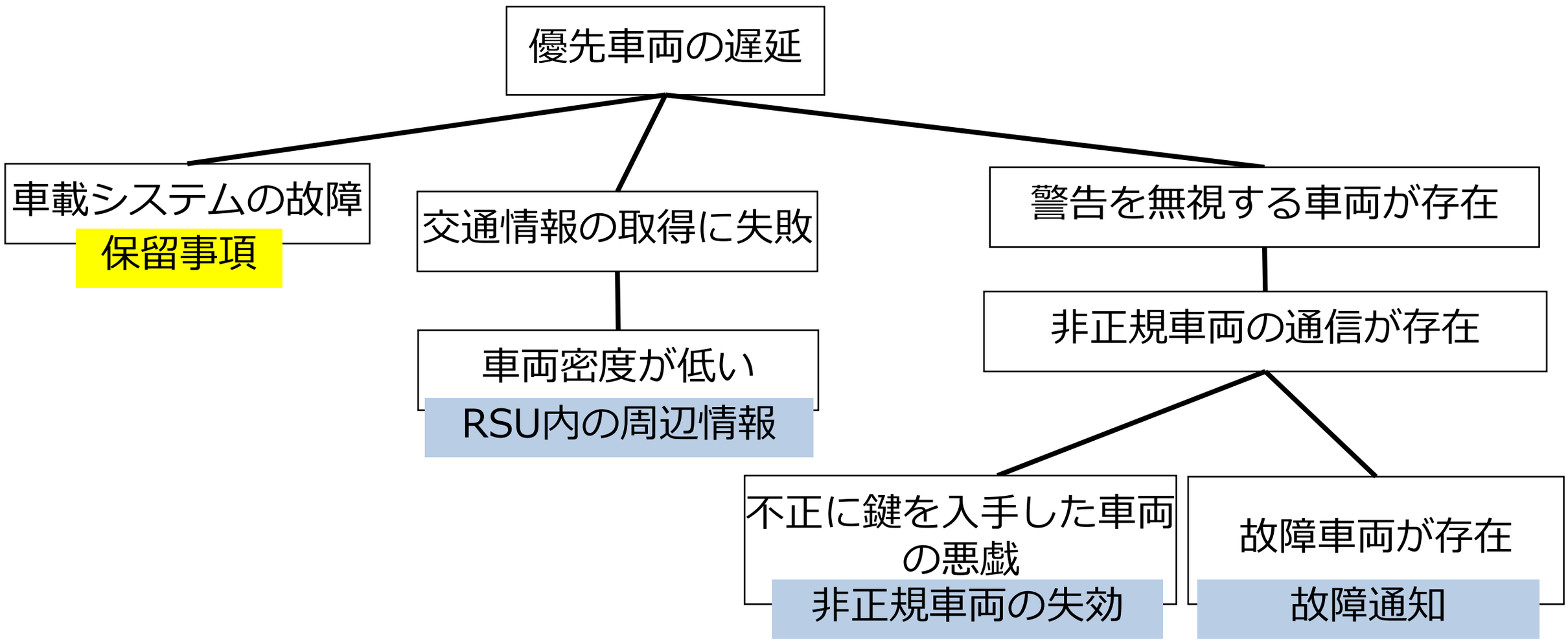
アシュアランスケースの作成準備

初期の簡易FTAのハザードを回避するための機能を記述
※車載システムの故障については再度検討



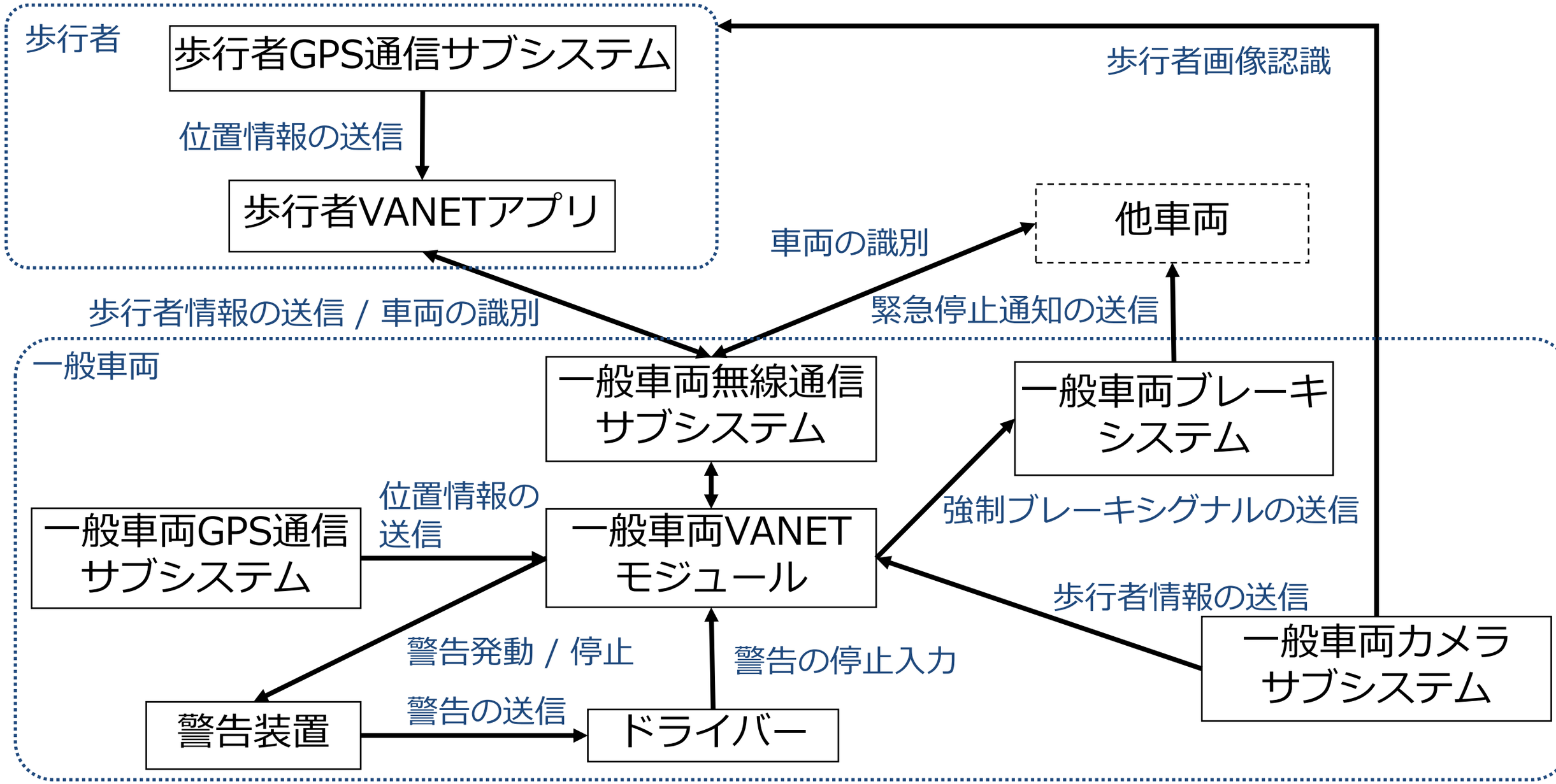
アシュアランスケースの作成準備

初期の簡易FTAのハザードを回避するための機能を記述
※車載システムの故障については再度検討



詳細なハザード分析

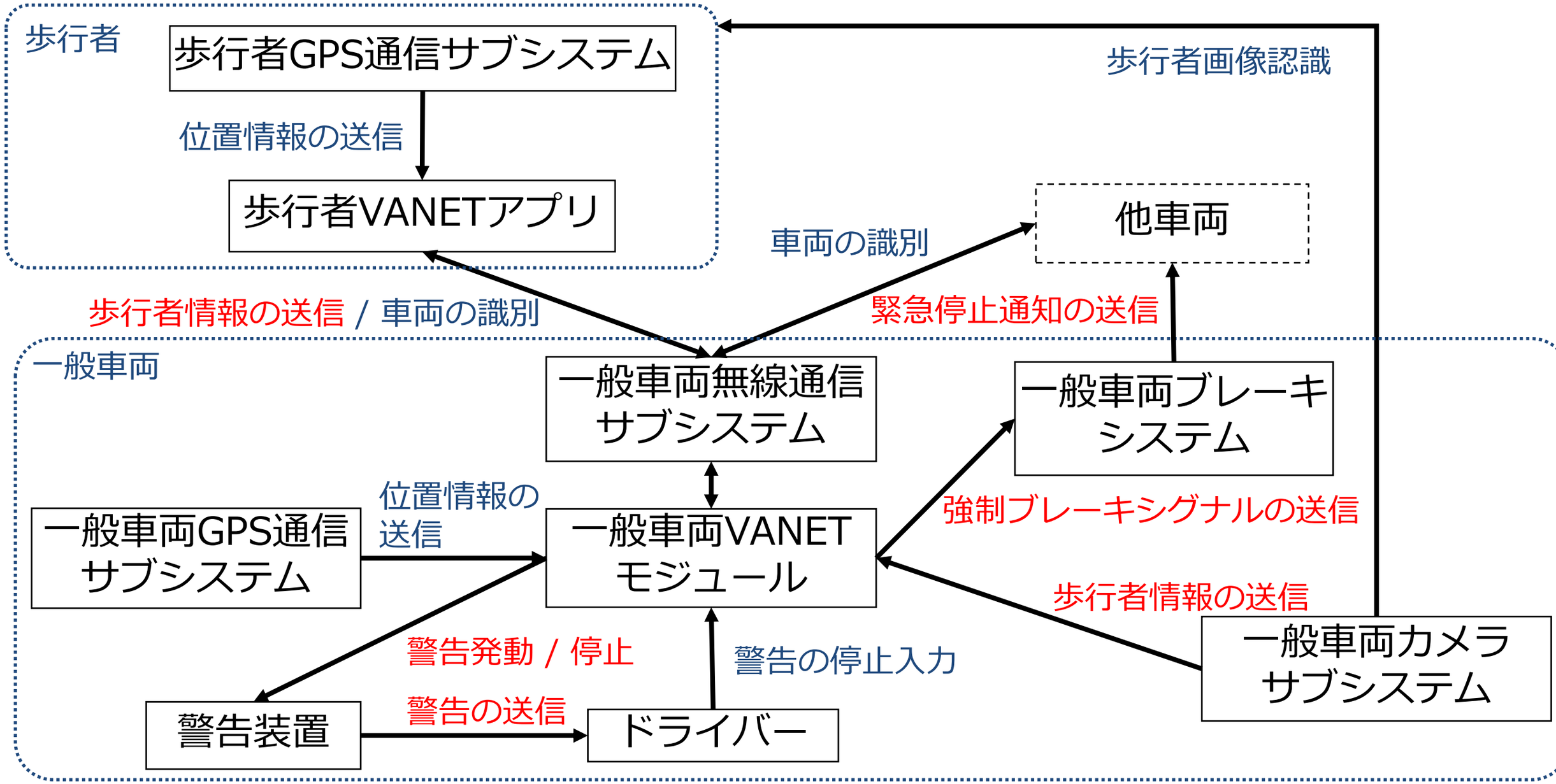
機能構成図１に対して，機能が正常に動作しない場合を検討



詳細なハザード分析

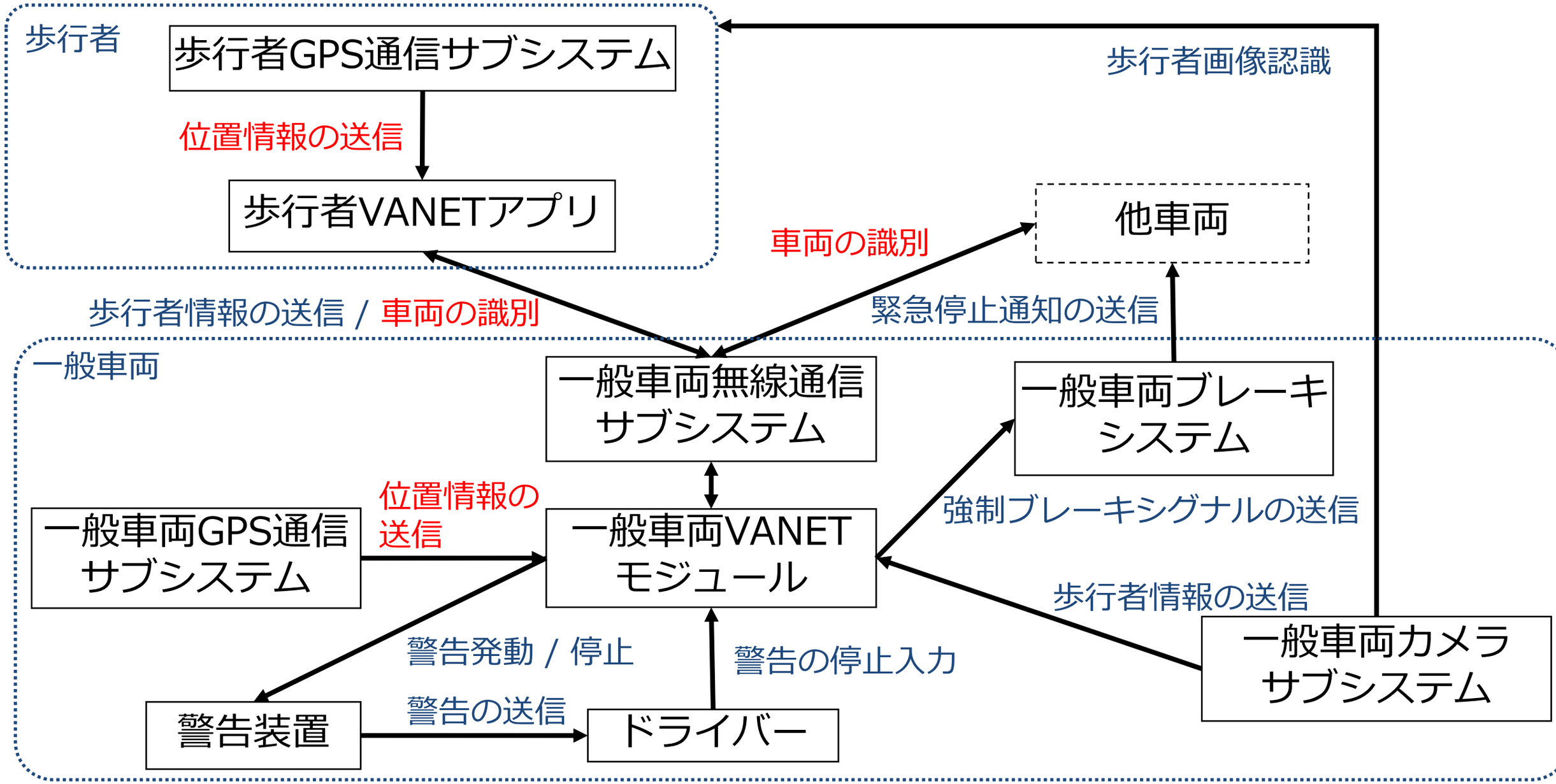
機能構成図１に対して，機能が正常に動作しない場合を検討

1. 誤ったデータの送信



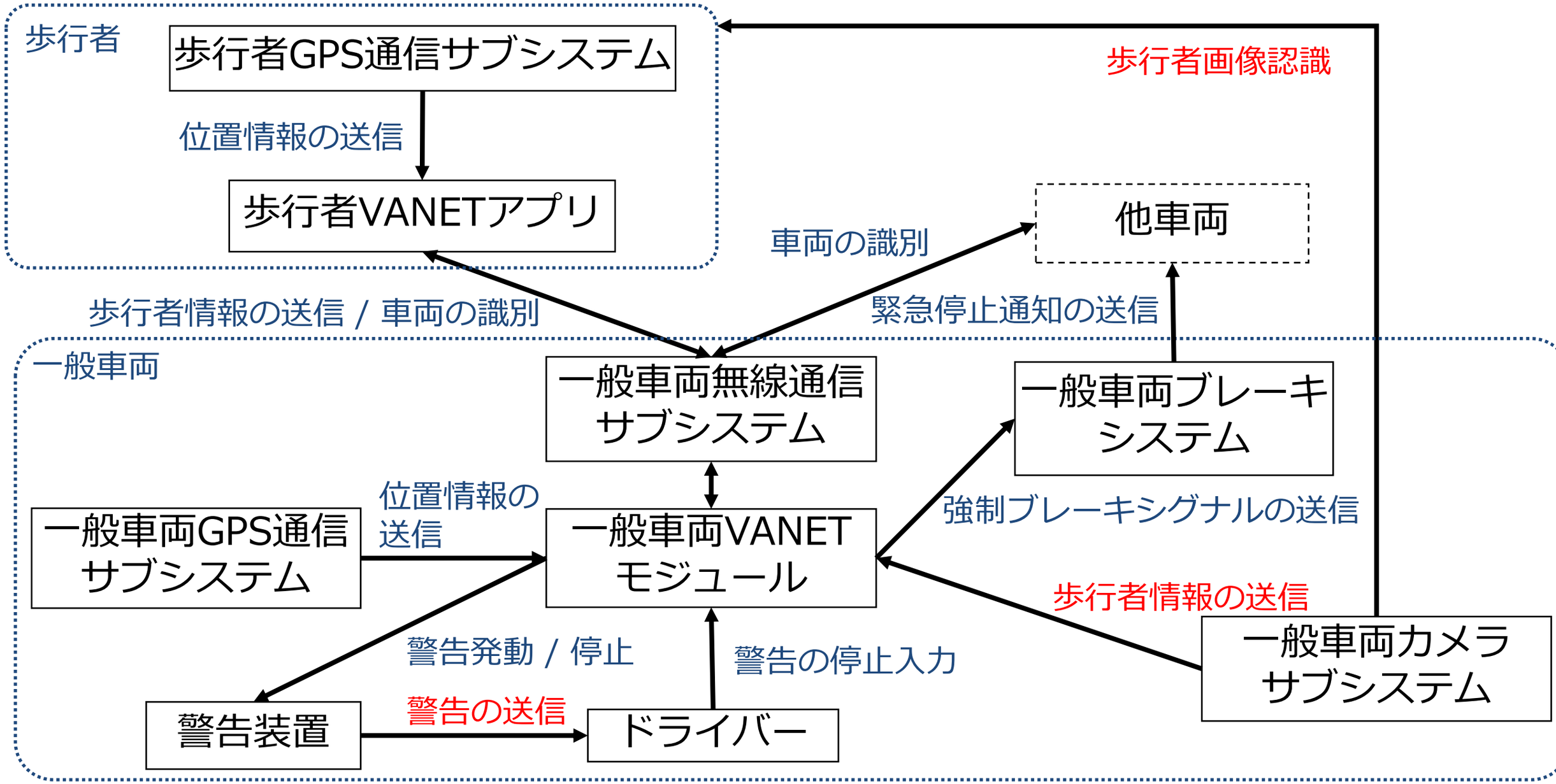
詳細なハザード分析

機能構成図 1 に対して，機能が正常に動作しない場合を検討
2. 位置情報の誤差



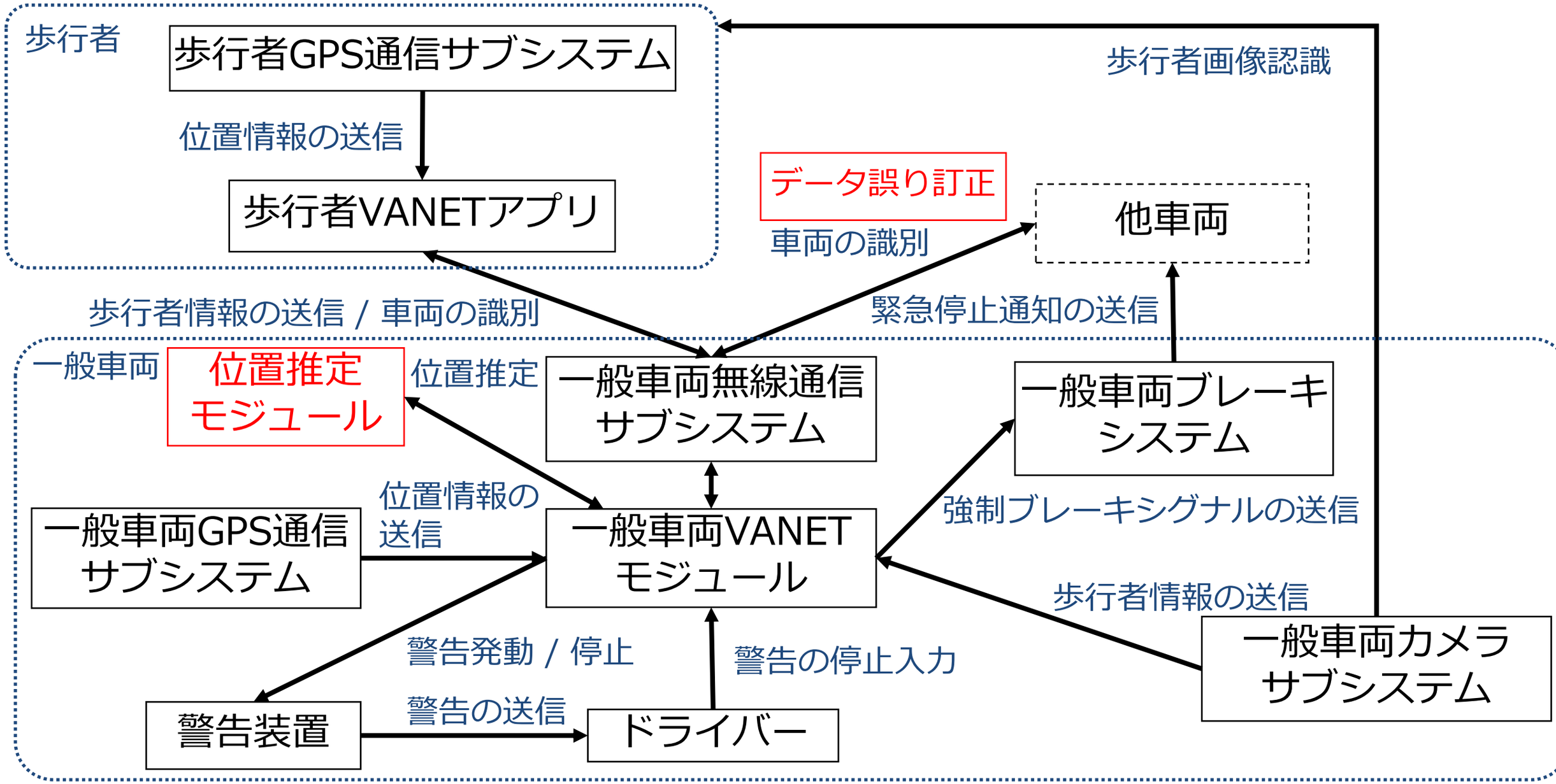
詳細なハザード分析

機能構成図 1 に対して，機能が正常に動作しない場合を検討
3. 車載装置の故障



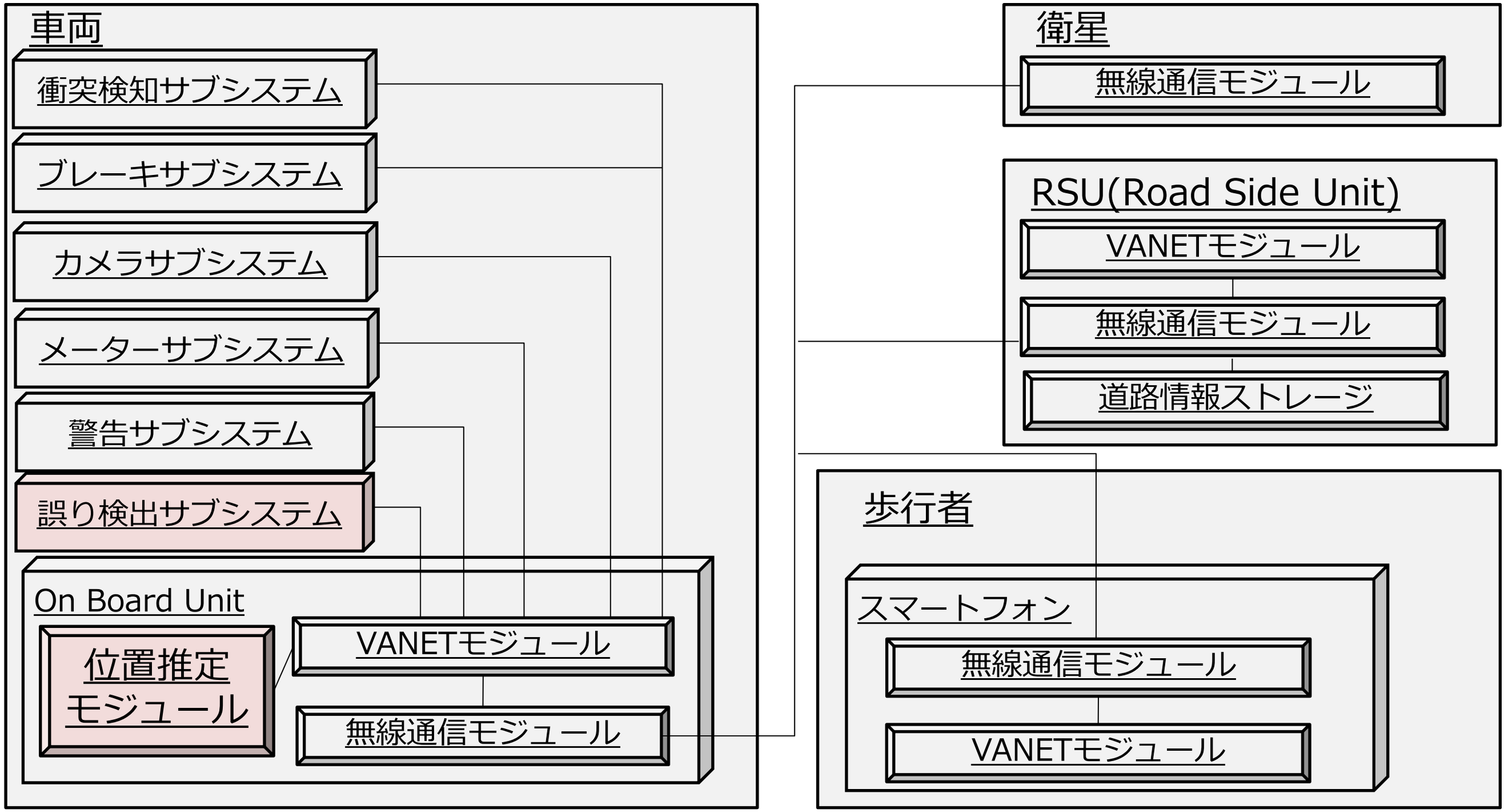
リスク軽減構造の更新

機能構成図 1 に対して，機能の追加（Design Issue検討後）



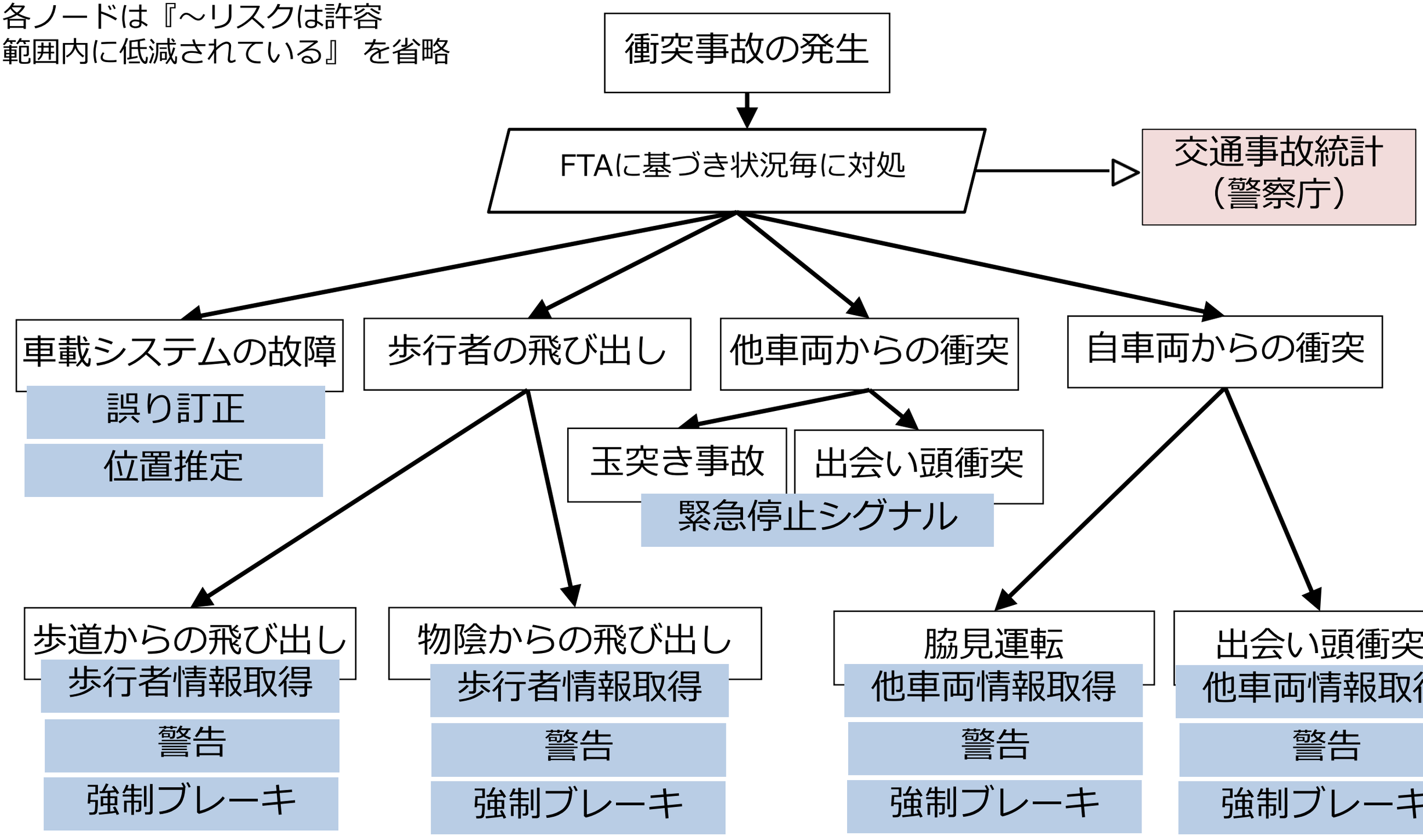
ハードウェア構成図の更新

ハードウェア構成図（機能構成図により決定）



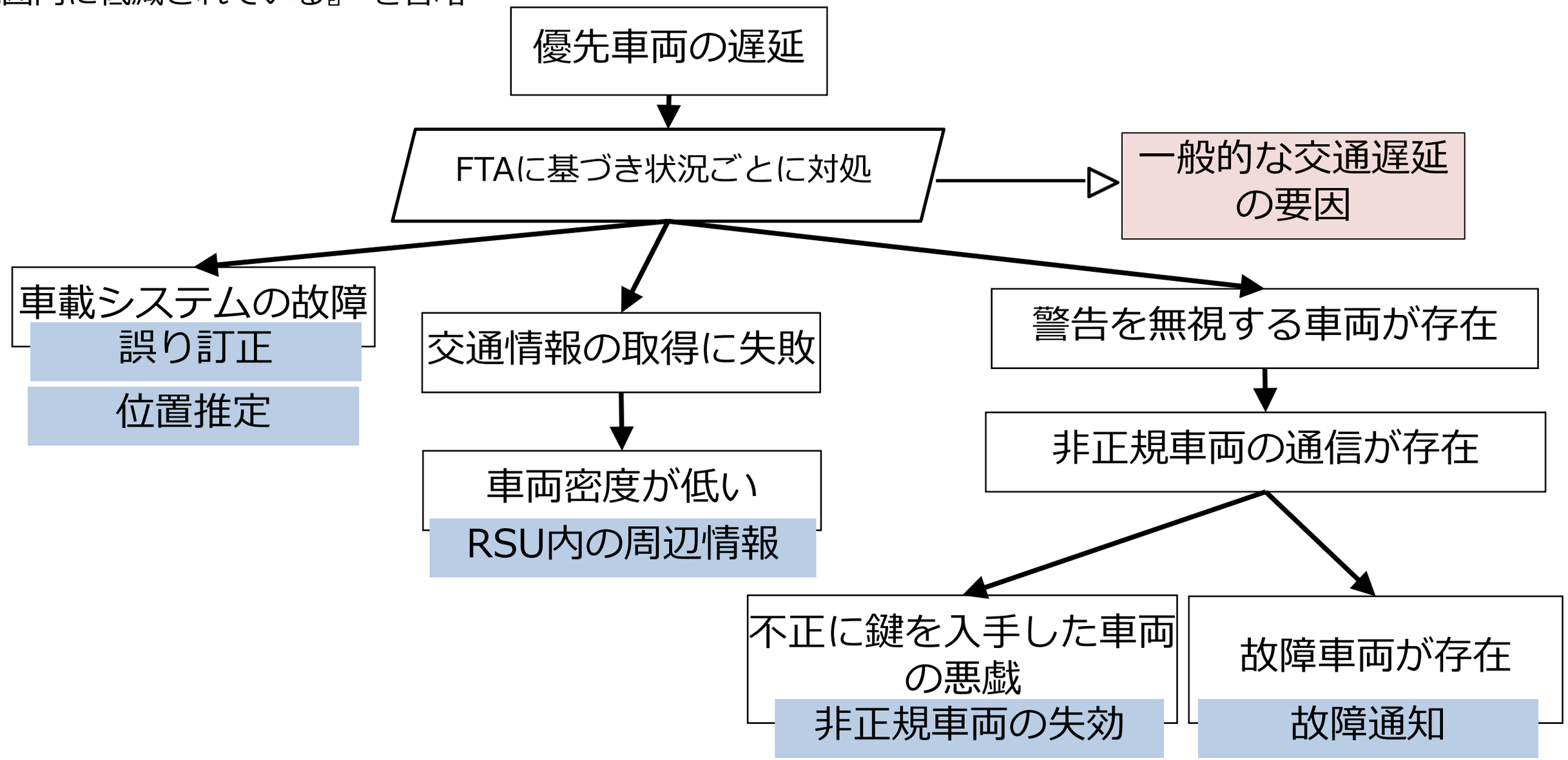
アシュアランスケースの作成

各ノードは『～リスクは許容
範囲内に低減されている』 を省略



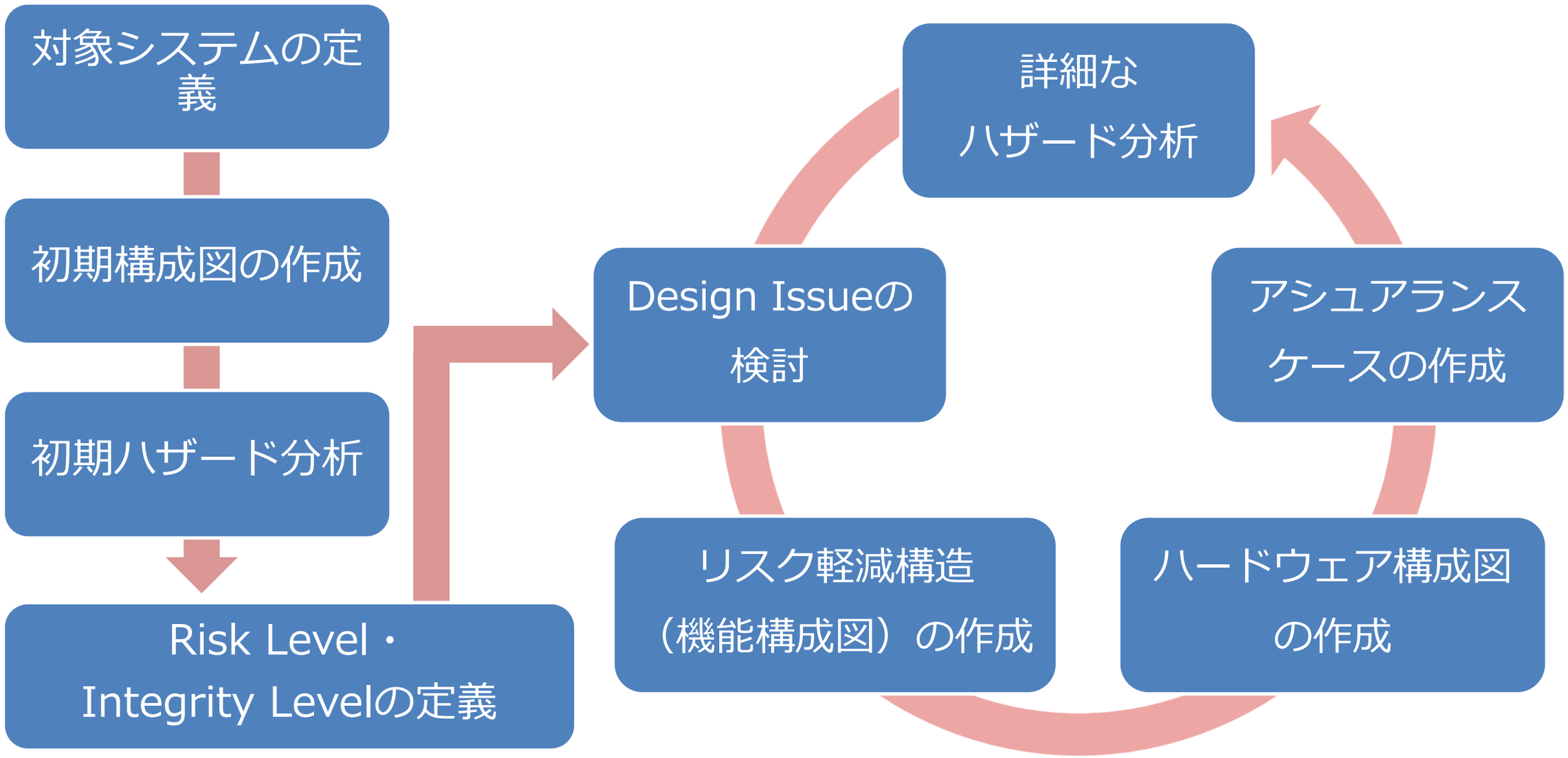
アシュアランスケースの作成

各ノードは『～リスクは許容
範囲内に低減されている』 を省略



今回のまとめ

VANETにおけるシステムアシュアランスを検討



アシュアランスケースを作成することによって，
ハザードへの対策が行われていることを示した．