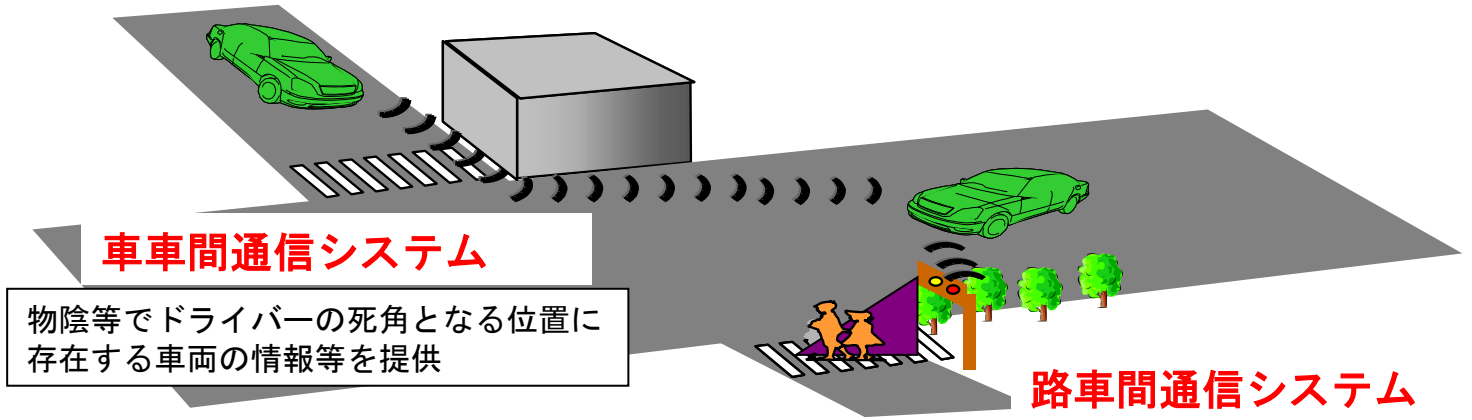
資料2

当面の検討スコープについて

事務局

安全運転支援システムの概要

◆ 車車間・路車間通信のイメージ



	システム概要	システムの特徴
車車間通信	車載器（陸上移動局）どうしが直接通信を行い、周囲の車の情報（位置、速度等）を入手し、必要に応じて安全運転支援を行う。	インフラ整備に係わらず不特定の場所で利用可能。
路車間通信	路側機（基地局）と車載器の通信により、インフラからの情報（信号情報、規制情報、歩行者情報等）を入手し、必要に応じて安全運転支援を行う。	路側機設置箇所で確実に情報提供が可能であり、事故多発地点での効果が期待される。

総務省･情報通信審議会･情報通信技術分科会･移動通信システム委員会資料より

安全運転支援システムのポリシー
～ASV通信利用型実用化システム基本設計書より～

実用化されたとしても自車周辺には非通信車両が混在していることを考慮し、「注意喚起」までの支援レベルとする

◆支援レベル

支援レベル	定義
情報提供	運転者がシステムから提供された情報により安全運転を行うための客観情報を伝える。
注意喚起	特定のタイミング、特定の場所、運転者による特定の操作または特定の状況が生じた時に注意を喚起する。
警報	検知した情報からの事故の可能性を予測し、運転者に対して即座に適切な行動・操作を促す。

◆ユーザーに対して配慮すべき事項の代表例

・ドライバーには、システムによる支援の有無にかかわらず、安全に運転する義務があること
・自車両の周辺には、システム搭載車両だけでなく、
システムを搭載していない車両や歩行者が存在している可能性があること
・通信技術には様々な理由から通信できなくなる場合があり、
通信の信頼性を100%とすることは技術的にみて無理があること
・支援の必要はないと考えられる場面でも支援してしまうような場合があること
・測位誤差は環境条件で大きく変動する性格があること　等

**これらの事項をユーザーが理解して使用できるよう、
メーカーが配慮する必要がある**

ASV：Advanced Safety Vehicle（先進安全自動車）

ASV　HMIガイドライン

～「インフラ協調による安全運転支援システムに係るHMIの配慮事項について」より～

【作動状況等の確認】

（1）ドライバがシステムの作動状況や支援内容を確認できるよう配慮する

[具体例]　・システムのON/OFFがわかるように表示
・支援に必要な情報を取得したことを提示

【分かりやすい情報伝達】

（2）ドライバにとって分かりやすく、使いやすいシステムであるとともに、安心して使えるよう配慮する

[具体例]　・短時間に理解できるよう、文字数等の情報量に配慮
・複数の情報伝達手段を持つ場合は、表示・音・触覚等を適切に組み合わせ

【確実な情報伝達】

（3）安定した情報伝達となるよう配慮する

[具体例]・警報や注意喚起を行う場合には、音とともに資格や触覚等により情報伝達

【緊急度の容易な理解】

（4）ドライバが支援レベル（情報提供、注意喚起及び警報）を容易に理解できるよう配慮する

[具体例]・色によって支援レベルを表現
（警報：赤系統、注意喚起：黄色系統、情報提供：その他の色）

【過信・不信の防止】

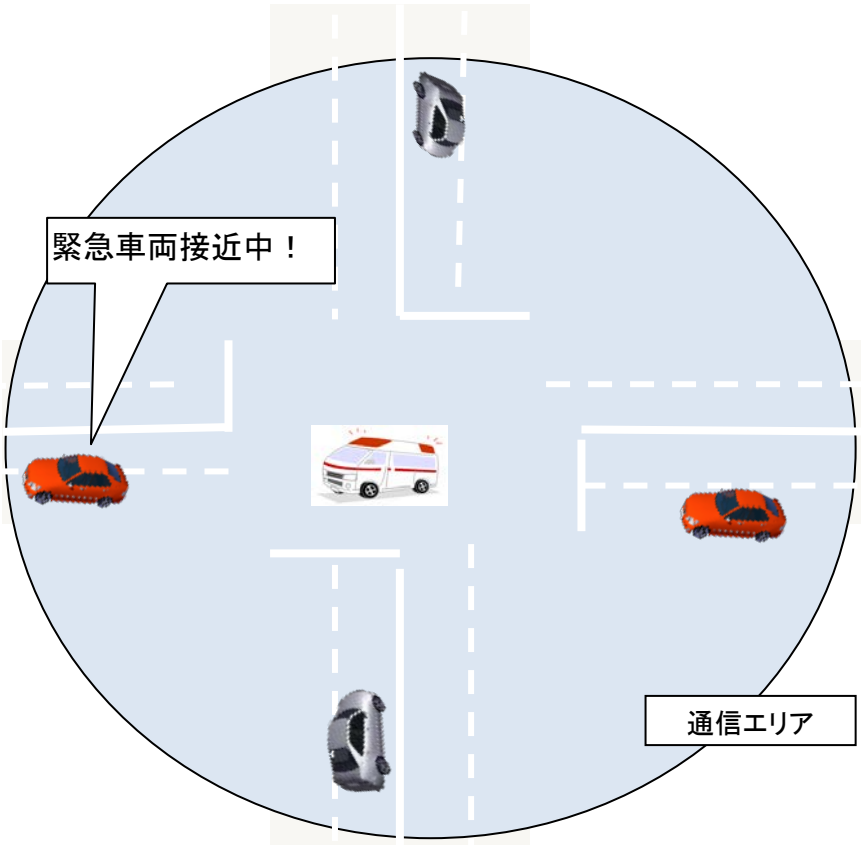
（5）ドライバがシステムに過度な依存や不信を抱かないよう適正な信頼が得られるように配慮する

[具体例]　・支援レベル、ドライバ反応時間、システム遅延時間等を考慮した支援タイミングで情報伝達
・システムの機能限界をマニュアル等によりドライバに周知

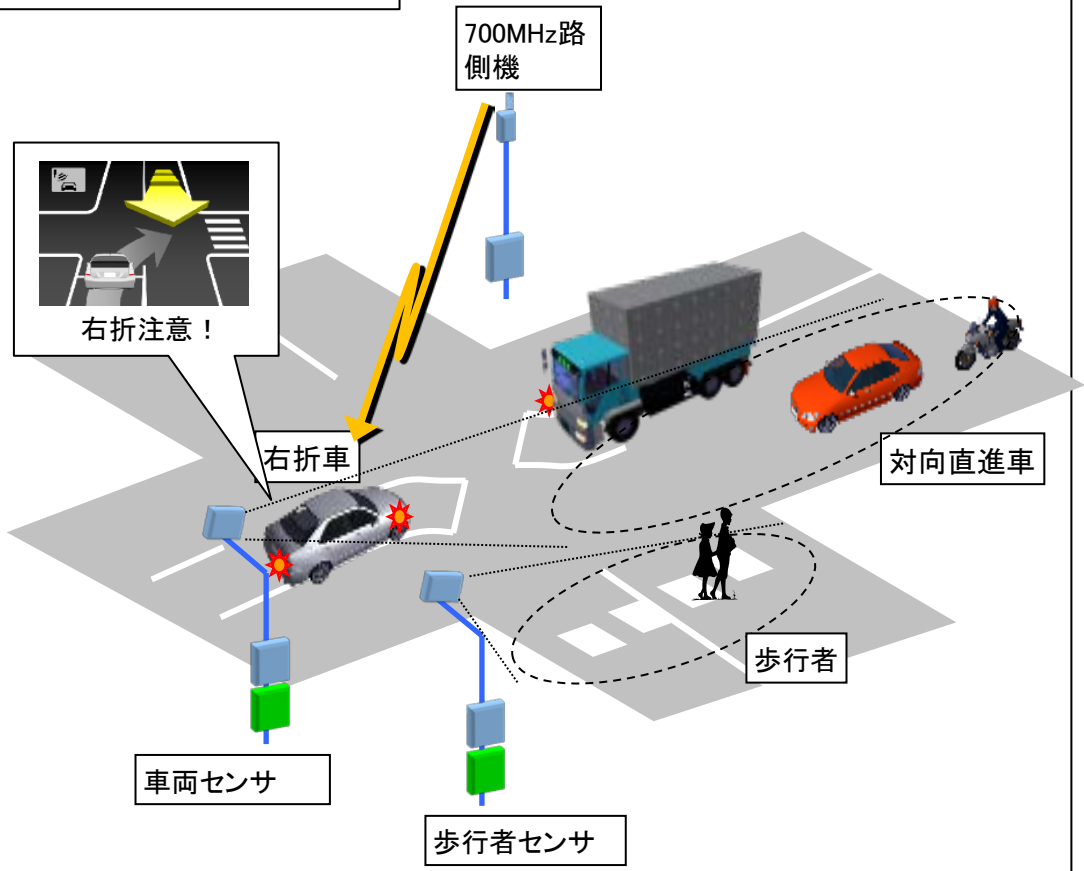
ユースケース

本検討グループでは、ASVにおける支援レベルの考え方を踏襲し、700MHzの車車間通信・路車間通信については「情報提供」・「注意喚起」レベルのユースケースを前提として、セキュリティの検討を進める。

情報提供・注意喚起の代表例



緊急車両情報提供



右折時衝突防止支援
歩行者横断見落とし防止支援

脅威分析

情報提供・注意喚起レベルのユースケースで想定される脅威のうち、
本検討グループではRC-009等の考え方を踏襲し、セキュリティの検討を進める

	No.	主な脅威	リスク(*)	攻撃対象	主な対策（案）
RC-009	1	なりすまし	4	無線通信	無線通信へのセキュリティ導入 アプリレベルでの偽情報の識別（車種、送信時間等）
	2	リプレイ攻撃	6		
	3	装置改ざん	6	車載機・路側機	車載機・路側機の耐タンパー性確保 （入力I/Fの防護、ソフトウェア・内部データの難読化等）
	4	マルウェア	6	車載機・路側機、 車載機・路側機への 接続機器	車載機・路側機の耐タンパー性確保 （ソフトウェアの脆弱性への対処、 接続機器へのセキュリティソフトの導入等）
	5	入力情報の改ざん	6	車載機・路側機への 接続機器	車載機・路側機の耐タンパー性確保 （接続仕様の非公開等）
	6	Jamming	6	無線通信	法規制
	7	DoS	4		法規制
	8	偽GPS信号	4	無線通信（GPS）	法規制
	9	盗聴	3	無線通信	ー （車載器にブロードキャストされる情報であるので、 機密性はない）
	10	ロケーショントラッキング	3	無線通信	車載機の悪用：尾行と同じであり、法規制による対策が必要 路側機の悪用：技術的に困難
ASV等	11	車内ユニット間通信へのアタック		車内ネットワーク	各社CAN仕様の公開範囲の管理
	12	長時間ログによる個人の特定		無線通信	個人が特定されないIDを採用

(*)具体的なリスク値算出方法はRC-009参照

ITSセキュリティ検討グループの当面のスコープ（案）

信号管制センタ

セキュリティ管理システム

信号機

路側センサ

インフラ

他車両

後付ナビ

スマホ

通信機

HMI表示部

ECU

なりすまし、リプレイ攻撃への対策

・無線通信へのセキュリティ導入

・アプリレベルでの偽情報の識別（車種、送信時間等）

装置改ざん、マルウェア、入力情報の改ざんへの対策

・機器認定スキーム

・セキュリティ情報の発行、格納等のフロー

※車載機・路側機の耐タンパー性確保のための個別具体な対策については検討対象外。

ITSセキュリティ検討項目（案）

サービス提供や運用管理に関する脅威と対策について検討し、**セキュリティポリシー（想定システムの脅威に対するセキュリティの考え方）をアウトプットとして策定する**

				検討対象	進め方／検討内容
検討項目		サービス提供		○	RC-009をもとに以下を議論する ・システム定義（サービスレベル・通信の制約条件を含む）、保護資産 ・脅威と対策方針 RC-008をもとに以下を議論する ・運用管理システム構成、保護資産 ・運用管理における脅威と対策方針
		通信のセキュリティ方式		○	セキュリティポリシーを満たす方式かを議論する
	運用管理	機器管理 （相互接続性、機器認定、車両情報等の管理）		○	機器認定スキーム（セキュリティ情報発行タイミングとの関係） 等
		サービス・コンテンツ管理 （運転支援に十分な信頼性のデータが送受されていることの管理）	セキュリティ情報のライフサイクル管理（発行、格納等）	○	RC-008をもとに以下を議論する ・セキュリティ情報の発行、格納等のフロー ・インシデント発生時の対応フレームワーク
			プライバシー	○	RC-009をもとに以下を議論する ・対象システムにおける機密情報の取り扱いの有無 ・機密情報を取り扱う場合のプライバシー対策方針
		ユーザサポート		○	インシデント対応に関わる部分 等