参考資料2

ITS Forum RC-008, ITS Forum RC-009概要説明

- 運用管理ガイドライン　ITS Forum RC-008
- セキュリティガイドライン ITS Forum RC-009

各ガイドラインの位置づけ

◆ 運転支援通信システムに関する運用管理ガイドライン（RC-008）
（平成23年4月27日ITS情報通信システム推進会議策定）
ARIB STD-T109（700MHz帯高度道路交通システム 標準規格）に基づく運転支援通信システムにおける運用管理モデル、想定サービス、運用管理機関の機能、運用管理手続きについてガイドラインを示したもの。

◆ 運転支援通信システムに関するセキュリティガイドライン（RC-009）
（平成23年4月27日ITS情報通信システム推進会議策定、
平成24年4月25日改定、平成25年11月25日改定）
ARIB STD-T109（700MHz帯高度道路交通システム 標準規格）に基づく運転支援通信システムに対する脅威とリスクを分析し、脅威に対する対策方針について定めたもの。

RC-008

運用管理ガイドラインの目次構成

RC-008

運用管理ガイドラインの目的

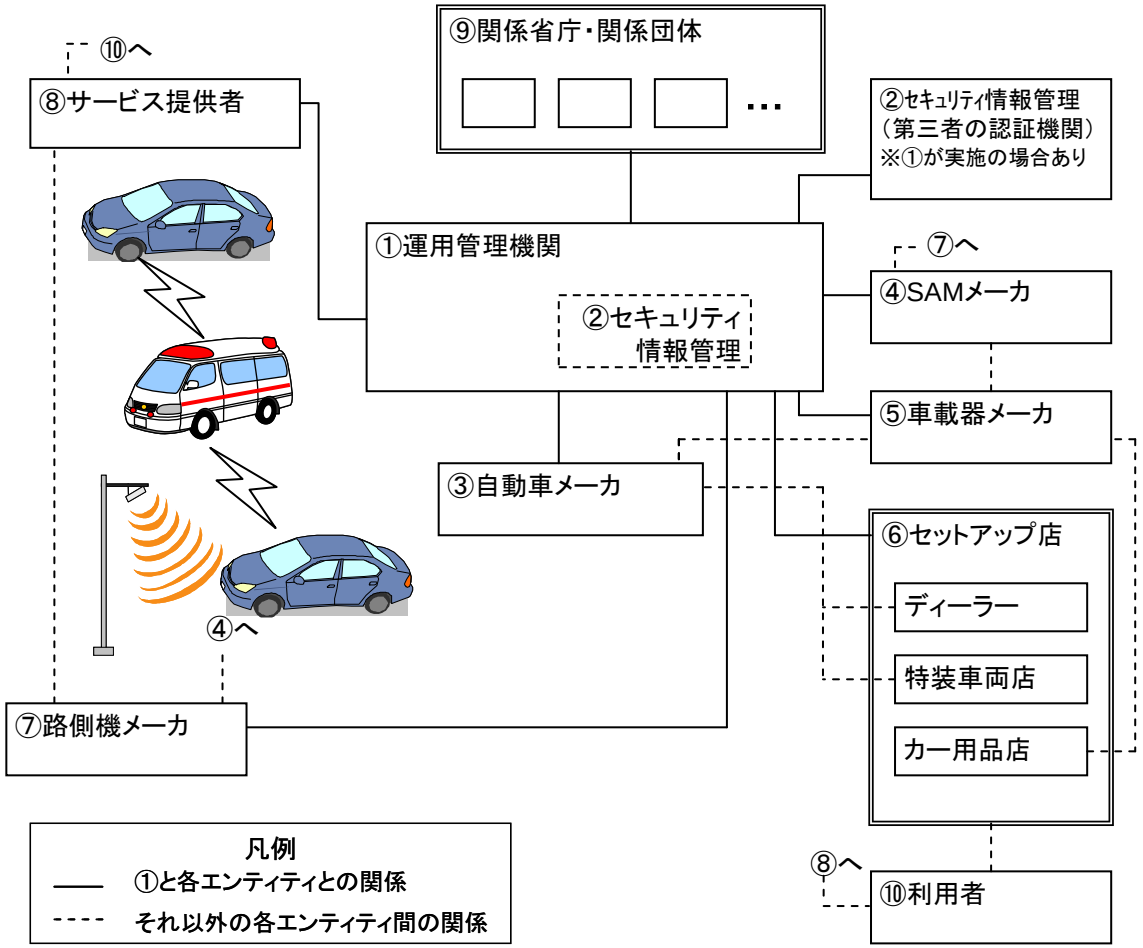
- 運転支援通信システムの運用に向けて、運用管理モデルの概要や運用管理の範囲をはじめ、適用するサービスや各システムの詳細など、運用管理機関の運用前・運用中の機能やその手順の詳細を記載する。

- 運用管理機関が運転支援通信システムの運用に必要と想定される機能と手順を網羅的に記載しており、実際には提供するサービスに応じて必要となる機能を運用管理機関が選択する。

- ただし、サービス・コンテンツ管理におけるシステムの具体的なセキュリティに関するリスク・脅威分析や方式によって異なる特徴などについてはセキュリティガイドラインにて記載する。

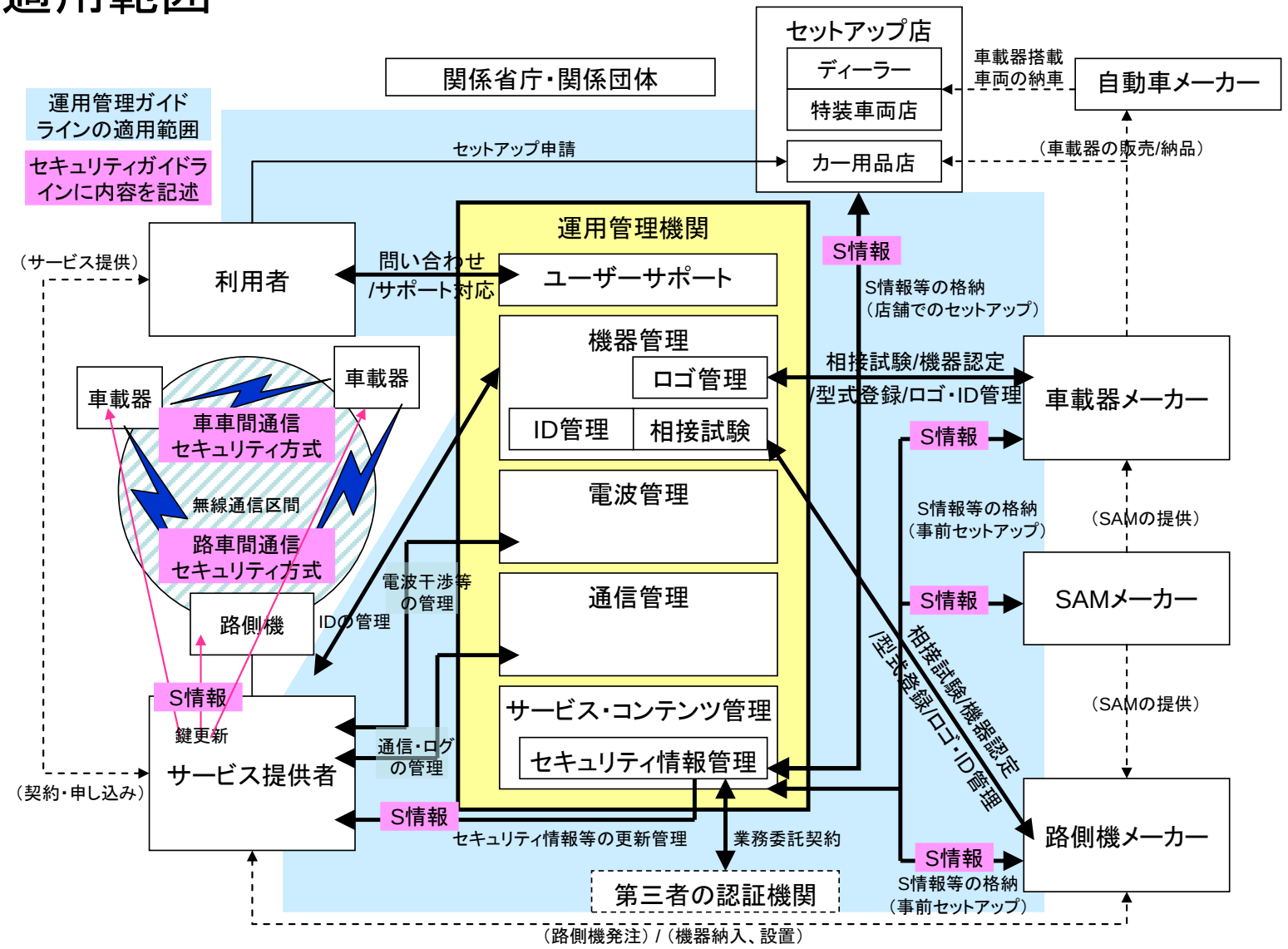
運用管理モデル概要と運用管理の範囲

- 運用管理モデル



運用管理モデル概要と運用管理の範囲

- 適用範囲



RC-008

当ガイドラインが想定するサービス

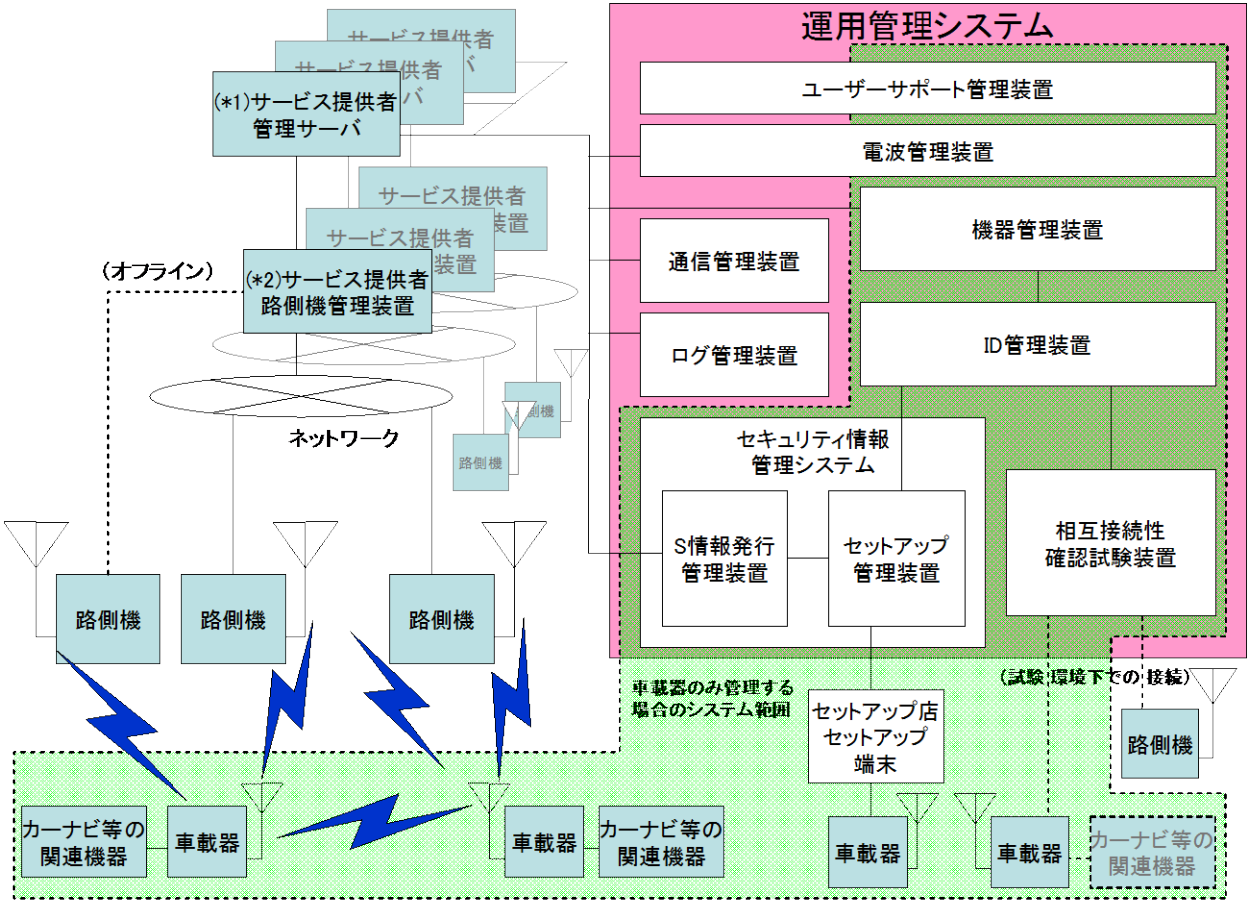
1. 車車間通信における安全運転支援サービス
   - 左折時衝突防止
   - 右折時衝突防止
   - 出会い頭衝突防止（双方一時停止規制無し、郊外道路）
   - 出会い頭衝突防止（踏み止まり支援、一時停止規制あり、見通し外）
   - 追突防止
   - 緊急車両情報提供

2. 路車間通信における安全運転支援サービス
   - 出会い頭衝突防止
   - 右折時衝突防止
   - 左折時衝突防止
   - 追突防止
   - 歩行者横断見落とし防止
   - 信号見落とし防止
   - 一時停止規制見落とし防止

RC-008

運用管理システムの構成

- システム構成図

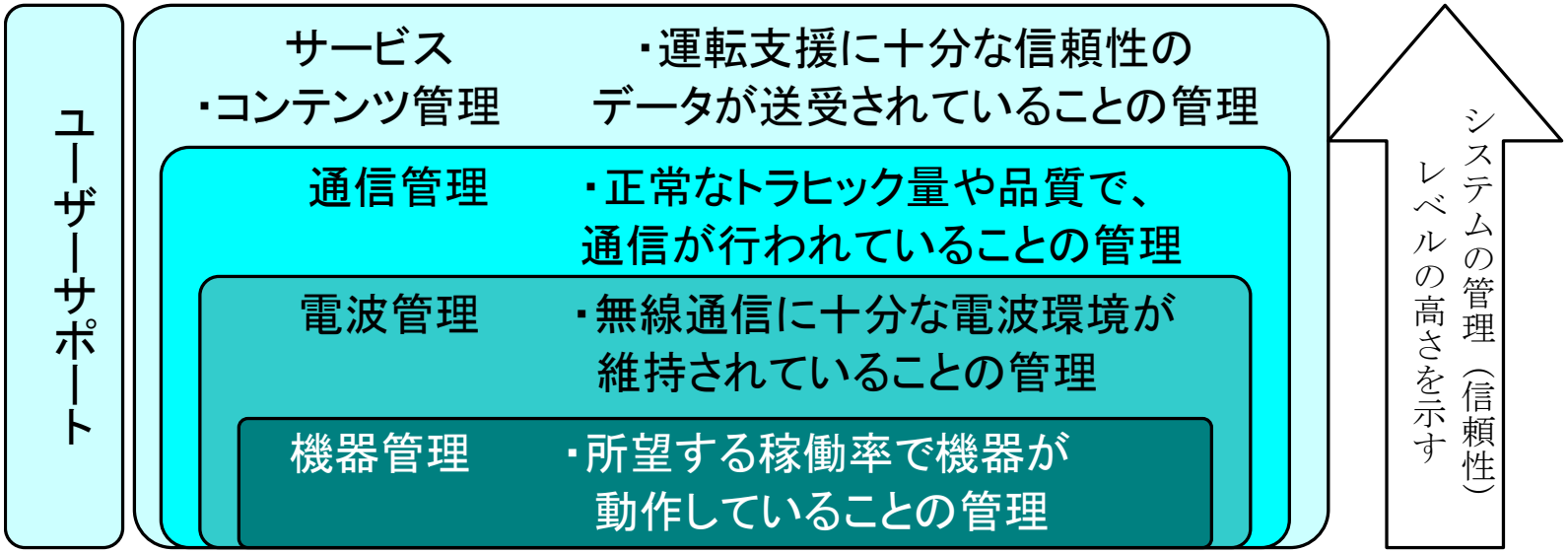


(*1)サービス提供者管理サーバ:サービス提供者毎にセキュリティや機器の正常動作、電波・通信の管理を行う機器。
サービス提供者が直接管理する。)
(*2)サービス提供者路側機管理装置:サービス提供者の所有する路側機を管理運用する装置)

運用管理機関の機能

- 管理種別

運用管理機関がシステムの実用化・運用・維持のために必要な管理機能の種別を以下の四階層に分類する。
それぞれの管理機能は包含関係にあり、上位の管理区分は下位の管理の機能保証も包含する。（例えば、通信管理を行わずにサービス・コンテンツ管理を行うことは出来ない。）
また、ユーザーサポートは全ての階層に必要な管理区分として独立で機能する。



RC-008

運用管理機関の機能

- 運用管理機能一覧

	フェーズ	機器管理	電波管理	通信管理	サービス･コンテンツ管理
路側機	開発	・相互接続性確認試験 ・機器の認定 ・機器の型式登録 ・ロゴマークの管理			
	製造	・IDの管理 （製造時の路側機管理番号の管理） （製造時のS情報関連IDの管理）			・S情報の事前格納
	設置	・IDの管理 （設置時の路側機管理番号の管理） （S情報関連IDの管理）	・電波干渉管理		・S情報の設置時格納およびセットアップ
	運用	・機器の正常動作管理	・電波の正常動作管理	・通信の正常動作管理 ・ログの管理	・S情報の更新管理 （S情報のバージョン管理） （S情報更新機能） （S情報再設定機能） （コンテンツ管理機能）
		ライフサイクル管理	ユーザーサポート（問い合わせ対応）		
	廃棄	・IDの管理（抹消） （路側機管理番号及びS情報関連IDの抹消）			・S情報の抹消
車載器	フェーズ	機器管理	電波管理	通信管理	サービス･コンテンツ管理
	開発	・相互接続性確認試験 ・機器の認定 ・機器の型式登録 ・ロゴマークの管理			
	製造	・IDの管理 （製造時の車載器管理番号の管理） （製造時のS情報関連IDの管理）			・S情報の事前格納
	販売	・IDの管理 （販売時の車載器管理番号の管理） （S情報関連ID管理） ・車両情報等の登録管理			・S情報の販売時格納およびセットアップ
	運用	・機器の正常動作管理	・電波の正常動作管理	・通信の正常動作管理 ・ログの管理	・S情報の更新管理 （S情報更新機能）
		ライフサイクル管理	ユーザーサポート（問い合わせ対応）		
	売却/廃棄	・IDの管理（抹消） （車載器管理番号及びS情報関連IDの抹消） ・車両情報などの抹消			・S情報の抹消

RC-008

運用管理の手続き

- 運用管理の手続き一覧

	対象エンティティ	機能項目	主な手続き
運用管理機関	SAMメーカ	・（エンティティ登録） ・（ＳＡＭ開発） ・セキュリティ情報の事前格納	エンティティ契約、登録、ID発行 ＳＡＭ仕様開示、ＳＡＭ開発、開示資料の返納 セキュリティ情報の貸与、媒体受領、返納
	車載器メーカ	・（エンティティ登録） ・（車載器開発） ・相互接続性確認試験 ・機器の型式登録 ・車載器管理番号の管理 ・ロゴマークの管理 ・セキュリティ情報の事前格納 ・ユーザーサポート ・ライフサイクル管理	エンティティ契約、登録、ID発行 車載器仕様開示、車載器開発、開示資料の返納 試験要領書の受領、相接用セキュリティ情報の貸与、相接受験、確認番号発行 型式申請、登録、抹消 車載器管理番号採番基準の提示、採番 ロゴマーク利用規程の提示、使用許可申請、受領 セキュリティ情報の貸与、媒体受領、返納 ユーザーサポート問合せ窓口設置 リサイクル実績の証明、受理
	路側機メーカ	・（エンティティ登録） ・（路側機開発） ・相互接続性確認試験 ・機器の型式登録 ・路側機管理番号の管理 ・ロゴマークの管理 ・セキュリティ情報の事前格納 ・ユーザーサポート ・ライフサイクル管理	エンティティ契約、登録、ID発行 路側機仕様開示、路側機開発、開示資料の返納 試験要領書の受領、相接用セキュリティ情報の貸与、相接受験、確認番号発行 型式申請、登録、抹消 路側機管理番号採番基準の提示、採番 ロゴマーク利用規程の提示、使用許可申請、受領 セキュリティ情報の貸与、媒体受領、返納 ユーザーサポート問合せ窓口設置 リサイクル実績の証明、受理
	セットアップ店	・（エンティティ登録） ・（セットアップ端末導入・返却） ・車載器へのセキュリティ情報の販売時格納およびセットアップ ・セキュリティ情報の更新管理 ・ロゴマークの管理 ・ユーザーサポート ・車載器のセキュリティ情報の抹消	エンティティ契約、登録、ID発行 セットアップ関連資料開示、端末の貸与、返納 セットアップ申請、セキュリティ情報の発行、車載器管理番号登録、車両情報登録 セキュリティ情報の更新指示、更新情報の発行、媒体受理、返納 ロゴマーク利用規程の提示、使用許可申請、受領 ユーザーサポート問合せ窓口設置 抹消申請、受理、抹消
	サービス提供者	・（エンティティ登録） ・ロゴマークの管理 ・路側機へのセキュリティ情報の設置時格納およびセットアップ ・電波干渉管理 ・機器の正常動作管理 ・電波の正常動作管理 ・通信の正常動作管理 ・ログの管理 ・セキュリティ情報の更新管理 ・コンテンツ管理 ・路側機のセキュリティ情報の抹消 ・ユーザーサポート ・ライフサイクル管理	エンティティ契約、登録、ID発行 ロゴマーク利用規程の提示、使用許可申請、受領 セットアップ申請、セキュリティ情報の発行、路側機管理番号登録 基地局設置状況等の情報収集、新設条件提示、設置状況の開示 車載器情報の検知・収集、機器管理データの検知・収集、路側機運用状態の検知・収集 車載器の異常／不正情報の検知・収集、路側機の電波状態の検知・収集 車載器の通信状態の検知・収集、路側機の通信状態の検知・収集 ログの収集、管理、開示 セキュリティ情報の更新指示、更新情報の発行、媒体受理、返納 新規コンテンツ登録申請、コンテンツID発行、抹消 抹消申請、受理、抹消 ユーザーサポート問合せ窓口設置 リサイクル実績の証明、受理
	利用者	・（利用者登録） ・ユーザーサポート	利用者情報登録申請、ID発行・管理 ユーザーサポート問合せ窓口設置

RC-009

セキュリティガイドラインの目次構成

RC-009

セキュリティガイドラインの目的

- 運転支援通信システムにおいて、車両の乗員と他の道路利用者の安全を第一優先とし、すべての車両と本システムの機能の意図する性能維持の為、車車間・路車間通信情報におけるセキュリティのガイドラインを記載する。

基本方針

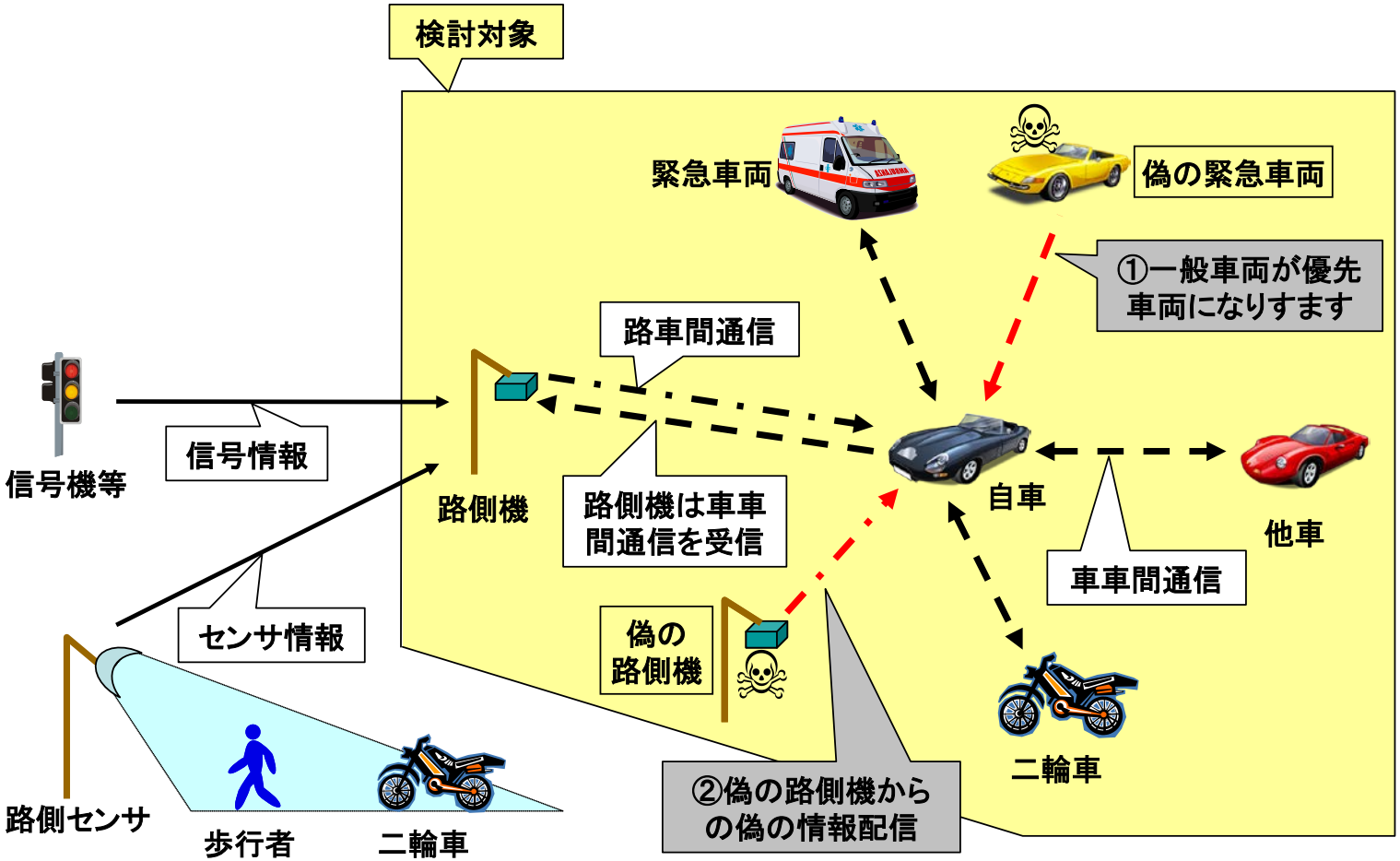
- 提供するサービスの品質維持の為、情報通信に関連する脅威から情報資産を保護することを目的とする。攻撃によって保護不可能の場合、速やかに保護を復旧できる対策をとること。
- 現在想定されている運転支援サービスのレベル以上のサービスを運用する際、サービスの性質に合わせて、ここで記載する対策だけでなく、別途検討すること。
- 提供するサービスの性質によっては、扱われる情報資産が人命と安全の確保に係わる場合がある。その情報資産は保護することは当然であるが、万一、情報資産が攻撃を受けた場合を想定して、情報セキュリティの対策だけでなく、フェールセーフ対策も施すこと。
- 提供するサービスの関連法規等、法令遵守に係わる情報も保護すること。

RC-009

システムに対する脅威とリスクの分析

- 分析対象

路車間および車車間通信時におけるセキュリティ方式を検討するために、装置を含めた路車間と車車間での通信部分を検討対象としている。



RC-009

システムに対する脅威とリスクの分析

- 脅威分析

路車間および車車間通信時におけるセキュリティ方式を検討するために、
装置を含めた路車間と車車間での通信部分を検討対象としている。

ID	脅威	内容
1	DoS	路側機や車載器に対して大量のメッセージを送信する
2	Jamming	同周波数を発生させる機器によって妨害電波を発生させる
3	マルウェア	車載器や路側機がウィルス等に感染(アップデート時も含む)する
4	リプレイ攻撃	以前に使用されたメッセージを再利用する
5	スパム	スパムメッセージを送信する
6	装置外情報の改ざん	車載器や路側機が使用する装置外の情報(速度や位置、時間、歩行者検出等)を改ざんする
7	偽GPS信号	GPS信号発生器を悪用し、偽のGPS信号を送信する
8	なりすまし(1)	路側機になりすます
9	なりすまし(2)	他の車載器や優先車両になりすます
10	偽メッセージの送信	偽造したメッセージを送信する
11	メッセージの改ざん	通信メッセージを改ざんする
12	盗聴	通信ネットワーク内外の者が通信データを盗聴する
13	ロケーショントラッキング	通信ネットワーク内外の者が受信データから個人の位置をトレースする
14	ブラックホール	転送情報を故意に転送しない(遅くする)
15	装置改ざん	車載器や路側機のソフトウェアや内部データ、送信メッセージを改ざんする

RC-009

システムに対する脅威とリスクの分析

- 情報資産と関連する脅威の分析

情報資産	脅威		内容
路情報走行情報 汎用情報	Dos(1)		第三者による通信機の利用や利用者による車載器の悪用によって、大量のメッセージの送信し、システムを利用不能にする。
	Jamming(2)		第三者による妨害電波の発生により、通信が不能となり、システムを利用不能にする。
	偽GPS信号(7)		第三者によるGPS信号発生器の悪用により、誤った位置を含むメッセージが配信されて、混乱が発生する。
	マルウェア(3)		第三者や利用者による通信メッセージの悪用や(悪意の有無関係なく)保守員や第三者による路側機や車載器への物理的アクセスによりマルウェアに感染し、虚偽メッセージによる混乱やシステムの利用不能が発生する。
	装置外情報の改ざん(6)		利用者や(悪意の有無関係なく)保守員による車載器入力情報の改ざんや(悪意の有無関係なく)保守員や第三者による路側機入力情報の改ざんによって、誤った情報を含むメッセージが配信されて、混乱が発生する。
	盗聴(12)		汎用情報に機密情報が含まれる場合、利用者による車載器の悪用や第三者による通信機の利用によって受信した汎用情報に含まれる機密情報が漏洩する(走行情報や路情報はすべての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)。
			第三者が通信機を用いて、通信メッセージを盗聴し、運用管理機関の意図しないサービスに利用する(運用管理機関の方針に依存)。
	装置改ざん(15)		第三者や利用者、(悪意の有無関係なく)保守員による車載器や路側機の解析や改ざんによって、車載器や路側機のソフトウェアや内部データ等を改ざんされる。これにより、虚偽メッセージが配信されて混乱やシステムの利用不能が発生する。
路情報(直)	路側機 なりすまし(8)	偽路情報送信(10)	利用者による車載器の悪用や第三者による通信機の利用により路側機になりすまし、誤った情報を含む路情報が配信されて混乱が発生する。
		リプレイ攻撃(4)	路側機が配信した情報を再利用して送信し、路側機になりすましたり、再利用されたメッセージによって混乱が発生する。
走行情報 汎用情報	車両 なりすまし (8, 9)	偽走行情報送信(10)	利用者による車載器の悪用や第三者による通信機の利用により他の車載器(緊急車両を含む)になりすまし、誤った情報を含む走行情報が配信されて混乱が発生する。
		偽汎用情報送信(10)	利用者による車載器の悪用や第三者による通信機の利用により他の車載器になりすまし、誤った情報を含む汎用情報が配信されて混乱が発生する。
		リプレイ攻撃(4)	正当な他の車載器が配信した情報を再利用して送信することにより、他の車載器になりすましたり、再利用されたメッセージによって混乱が発生する。
	ロケーショントラッキング(13)		第三者による通信機の利用、利用者による車載器の悪用や保守員による路側機の悪用によって、受信メッセージから個人の位置をトレースし、個人のプロファイリングをする(プライバシ侵害)。
路情報(間)	中継車両による改ざん(11)		路側機が配信した情報を改ざんして送信することによって、車車間通信や路車間通信が妨害される。
	偽路情報(間)送信(10)		路側機が設置されていない場所において、利用者による車載器の悪用や第三者による通信機の利用によって偽の路情報(間)を送信することで、周囲の車載器に路側機が存在すると偽り、車車間通信が妨害される。

RC-009

システムに対する脅威とリスクの分析

- 対策が必要な脅威と対策方針

リスクの高い脅威として以下をリストアップし、その対策方針を示す。太字下線が通信のセキュリティ対策によるものである。

No.	脅威	内容（概略）	小分類	対策方針
①	DoS	大量メッセージ送信		車載器の耐タンパ性 法律等による規制
②	Jamming	妨害電波		法律等による規制
③	マルウェア	ウィルス感染	第三者や利用者による感染	規定外データの受信拒否 路側機や車載器の耐タンパ性
④	リプレイ攻撃	使用されたメッセージの再利用	路のリプレイ	**発信元の真正性の確認**
			車のリプレイ	**発信元の真正性の確認**
⑤	装置外情報の改ざん	装置外情報の改ざん	第三者や利用者による改ざん	路側機の耐タンパ性 **発信元の真正性の確認**
⑥	偽GPS信号	偽GPS信号の送信		法律等による規制
⑦	なりすまし[1]	路側機になりすます	なりすまして偽情報送信	路側機の耐タンパ性 **発信元の真正性の確認** **メッセージの完全性の確認**
⑧	なりすまし[2]	他の車載器や優先車両になりすます	なりすまして偽情報送信	車載器の耐タンパ性 **発信元の真正性の確認** **メッセージの完全性の確認**
⑨	偽メッセージの送信	偽メッセージの送信	路車車による偽路情報送信	受信データの整合性検証
⑩	メッセージの改ざん	メッセージの改ざん	路車車による改ざん	受信データの整合性検証
⑪	装置改ざん	装置の改ざん	第三者や利用者による改ざん	路側機や車載器の耐タンパ性

DoS：Denial of Service　大量のデータを送信してサービスの提供を不能な状態にしたりセキュリティホールを攻撃するもの
耐タンパ性：装置内部の情報を物理的・論理的に読み取ったり書き換えることに対する耐性

RC-009

セキュリティ対策

- 必要となるセキュリティ対策は以下となる。

①発信元の真正性の確認

通信における情報の発信元が正しくその本人であり、偽の第三者がなりすましていないことが確認できること

②メッセージの完全性の確認

通信によって受信したメッセージが、正しく発信元が送信したメッセージと同じものであり、通信の途中において改ざんされていないことが確認できること

③情報の機密性の確保

通信区間で流れる情報が第三者から傍受できないこと。

路車・車車ITS専用通信システムそのものに対するリスクは低いが、路側機からの通信内容（例えば交通信号情報）を傍受され、その情報を別の目的に悪用されること防止するような場合は、機密性の確保が必要となる。

RC-009

セキュリティ対策

- セキュリティ対策の種類

必要なセキュリティ対策		実現方式
発信元の真正性	通信における情報の発信元が正しくその本人であり、偽の第三者がなりすましていないこと	・電子署名方式 →公開鍵アルゴリズム ・メッセージ認証コード方式 （MAC方式） →共通鍵アルゴリズム
メッセージの完全性	通信によって受信したメッセージが、正しく発信元が送信したメッセージと同じものであり、通信の途中において改ざんされていないこと	
情報の機密性	通信区間で流れる情報が第三者から傍受できないこと	・暗号化 →共通鍵アルゴリズム

MAC: Message Authentication Code

発信元の真正性、メッセージの完全性の確認には「電子署名方式」と「MAC方式」の2種類がある。

RC-009

セキュリティ対策

- 路車・車車ITS専用通信システムのセキュリティ方式

セキュリティ方式の比較

	電子署名方式	MAC方式
暗号方式	公開鍵暗号	共通鍵暗号
通信で使用するセキュリティ用の通信鍵	各機器で固有	全ての機器で共通
真正性の検証	公開鍵証明書で検証可能	正当な通信鍵を所持しているということをもって間接的に検証
セキュリティデータ長	大	小
鍵漏洩時の対応	漏洩対象機器のみの通信鍵や公開鍵証明書を更新	すべての車載器・路側機の通信鍵を更新
各機器の必要な処理能力	大	小
機器の耐タンパ※実装の重要性 （※秘密情報格納の堅牢性）	中 （各機器の秘密鍵の保護）	大 （システム共通の鍵の保護）
国際協調	欧米で路車間・車車間通信のセキュリティの国際標準として検討されている。 (IEEE1609.2)	—

RC-008

RC-009

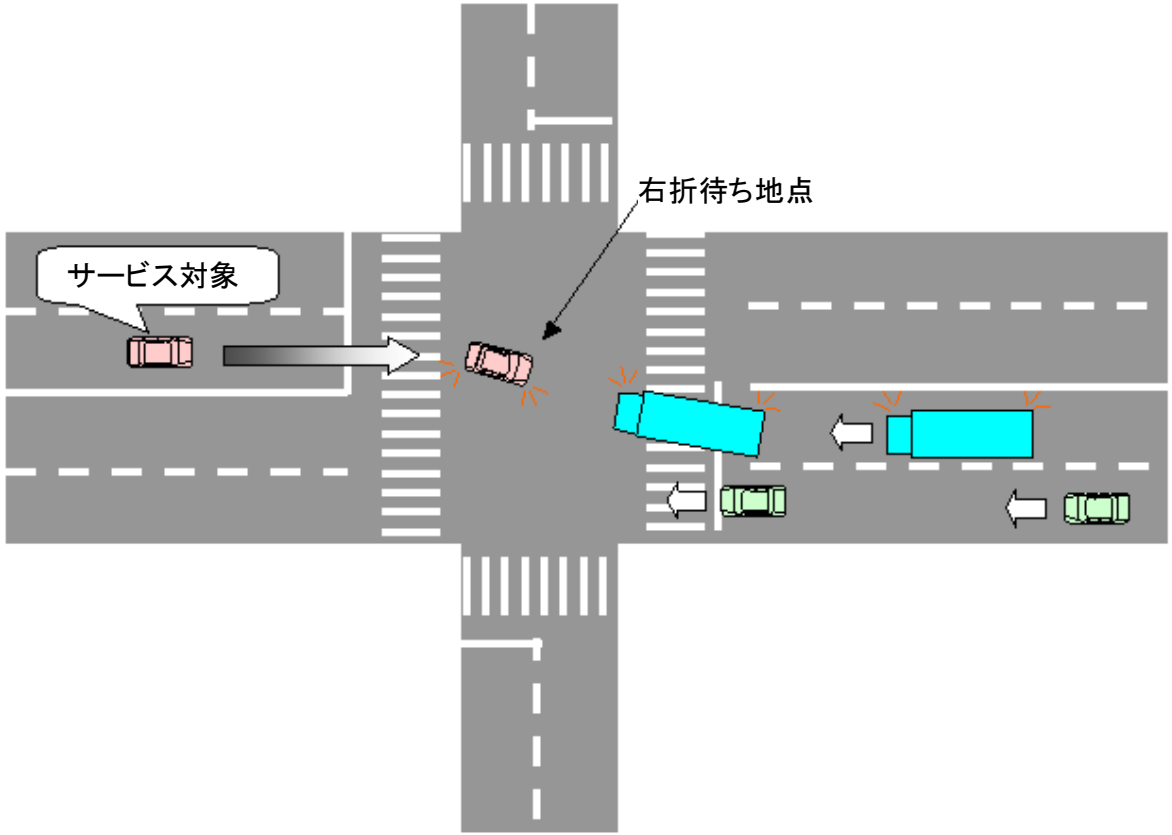
添付資料集

- 当ガイドラインが想定するサービスイメージ

当ガイドラインが想定するサービスイメージ

1. 車車間通信における安全運転支援サービス

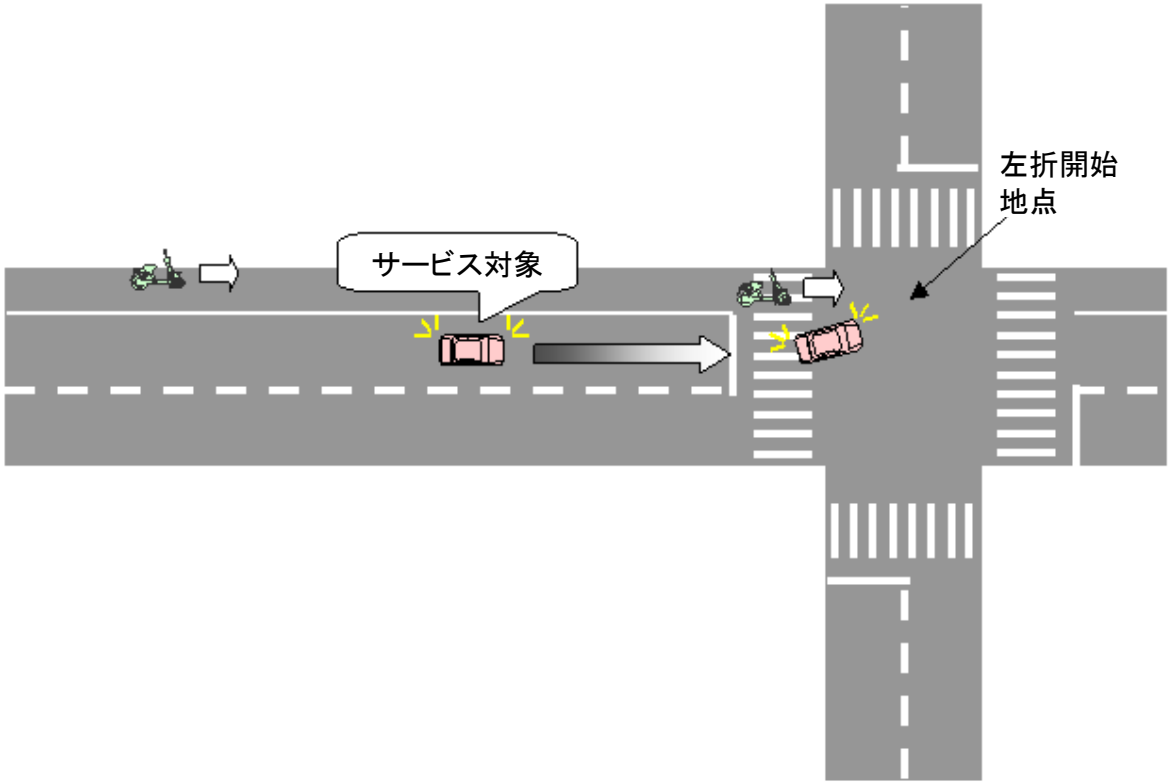
① 右折時衝突防止



当ガイドラインが想定するサービス

1. 車車間通信における安全運転支援サービス

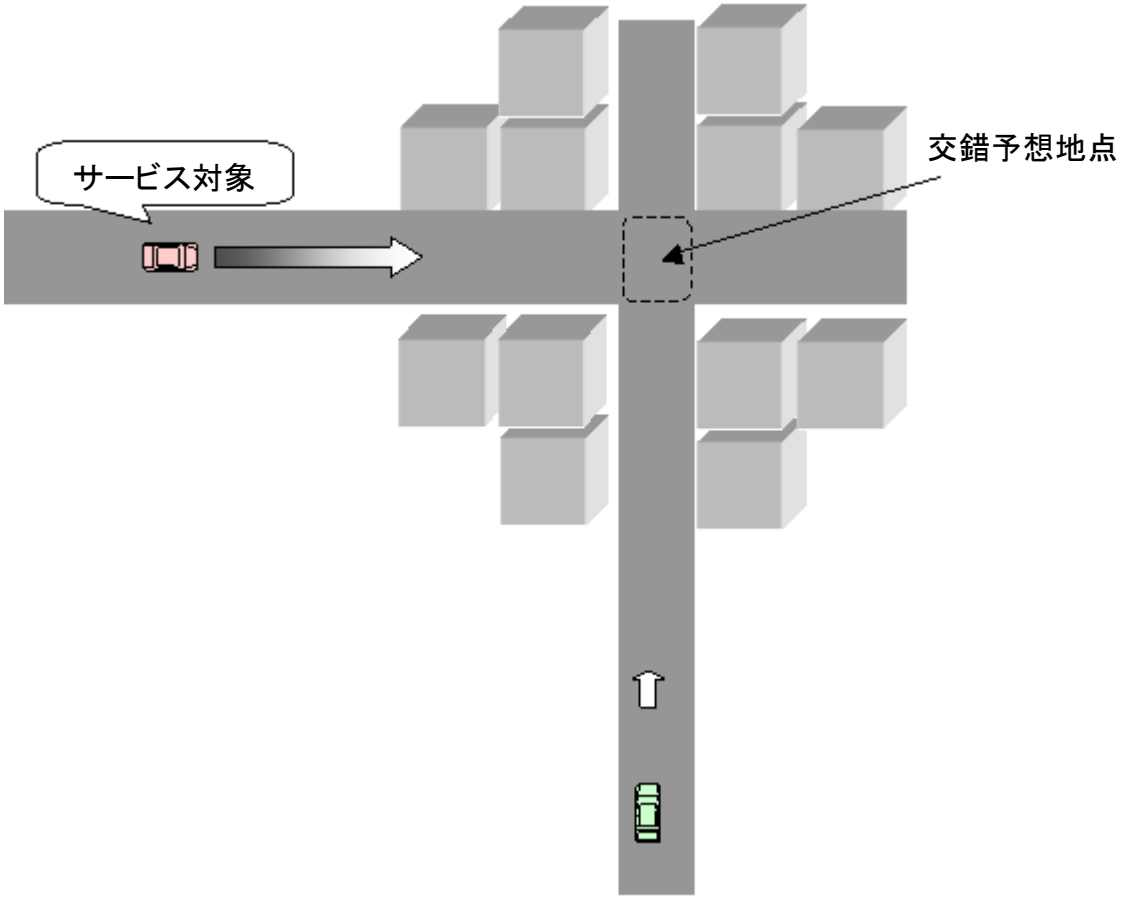
② 左折時衝突防止



当ガイドラインが想定するサービス

1. 車車間通信における安全運転支援サービス

③出会い頭衝突防止（双方一時停止規制無し、郊外道路）

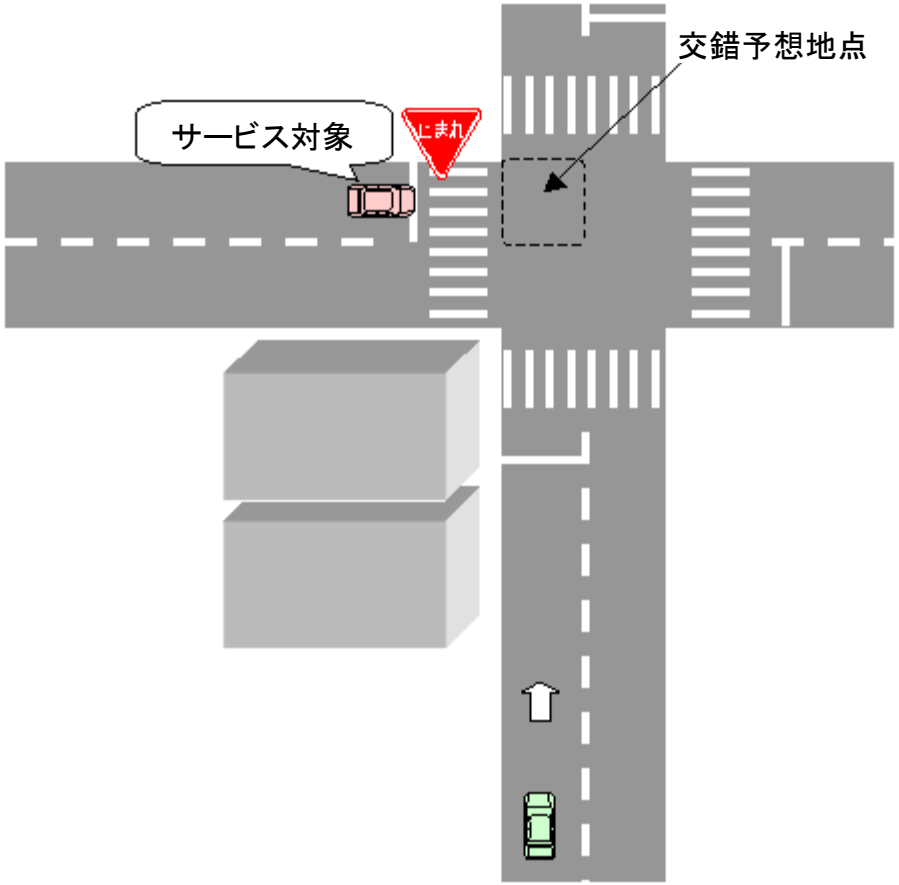


RC-008
RC-009

当ガイドラインが想定するサービス

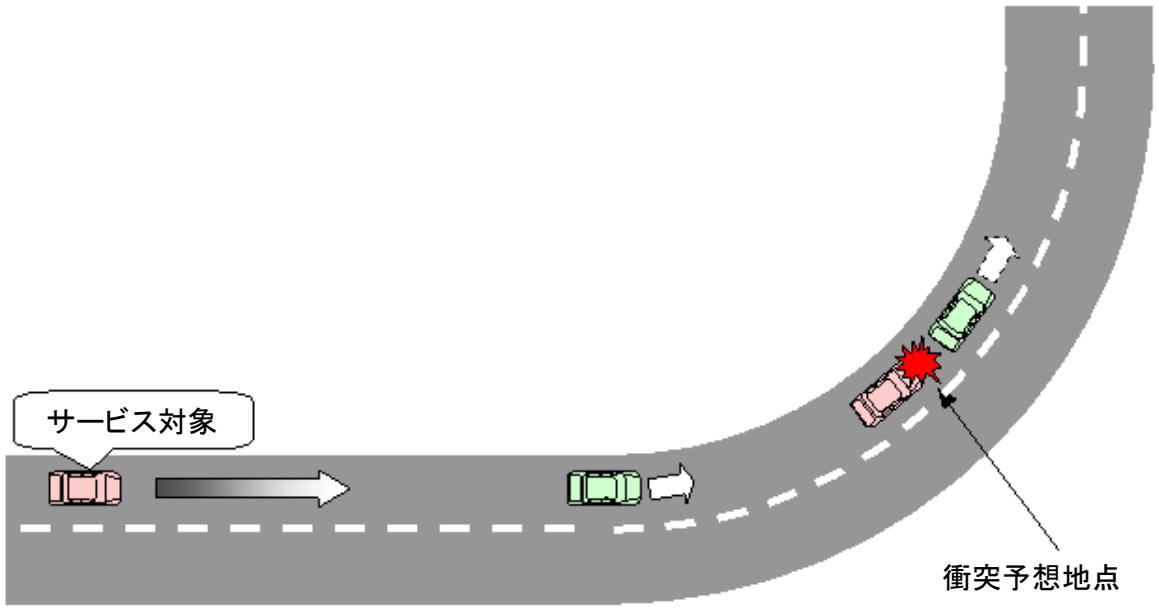
1. 車車間通信における安全運転支援サービス

④出会い頭衝突防止（踏み止まり支援、一時停止規制あり、見通し外）



当ガイドラインが想定するサービス

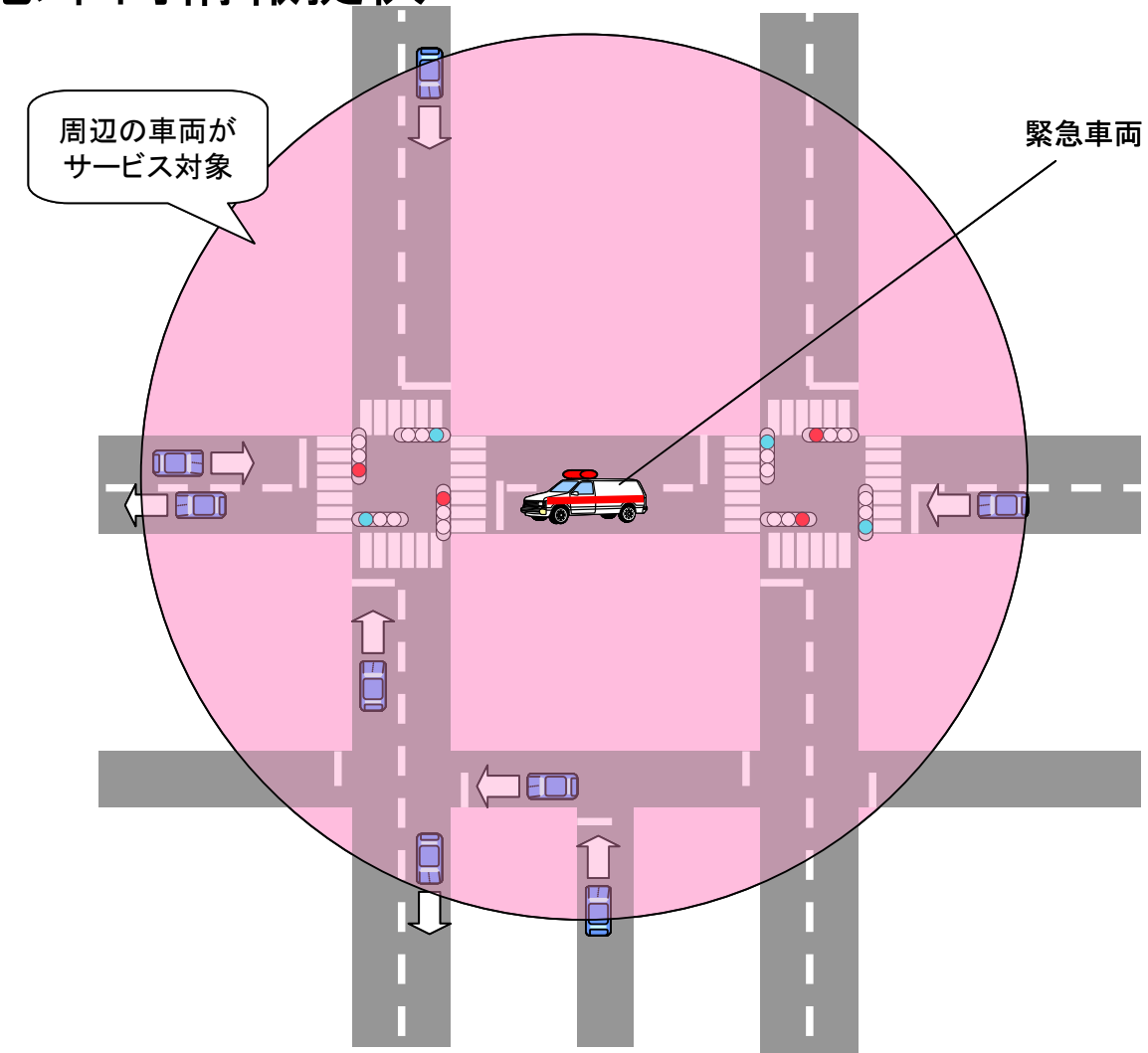
1. 車車間通信における安全運転支援サービス
⑤追突防止



当ガイドラインが想定するサービス

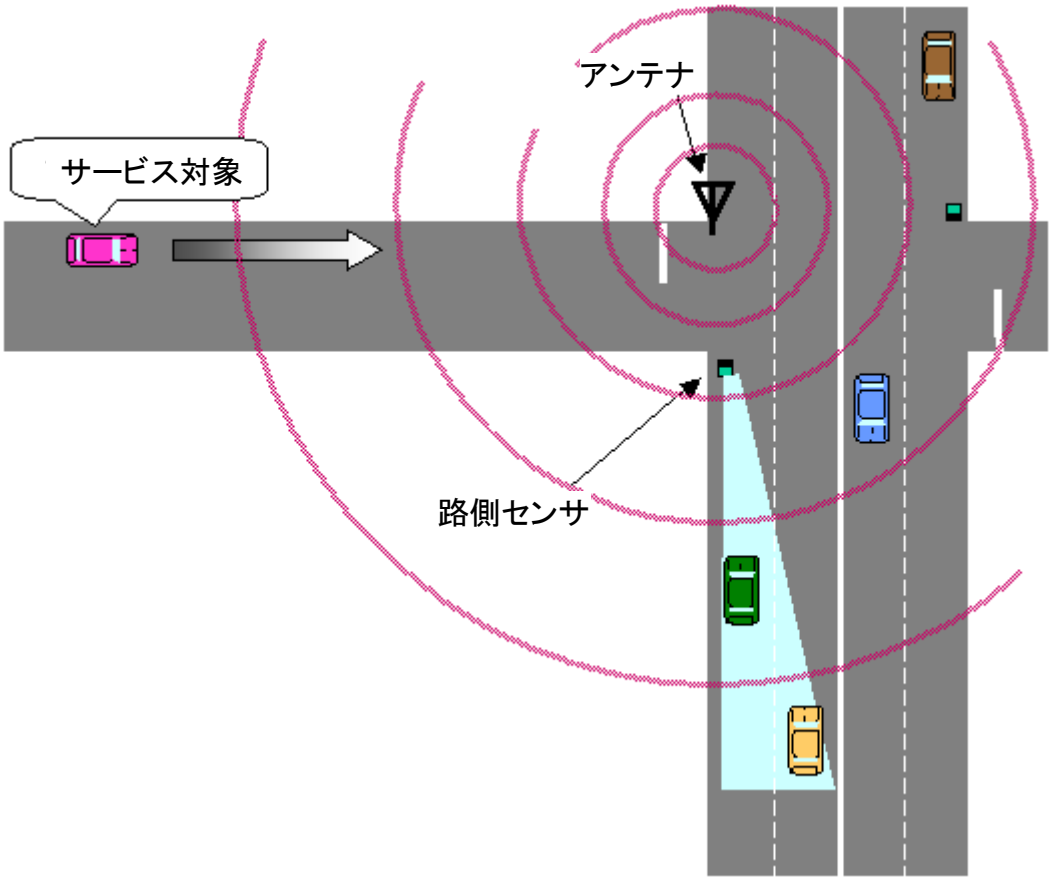
1. 車車間通信における安全運転支援サービス

⑥緊急車両情報提供



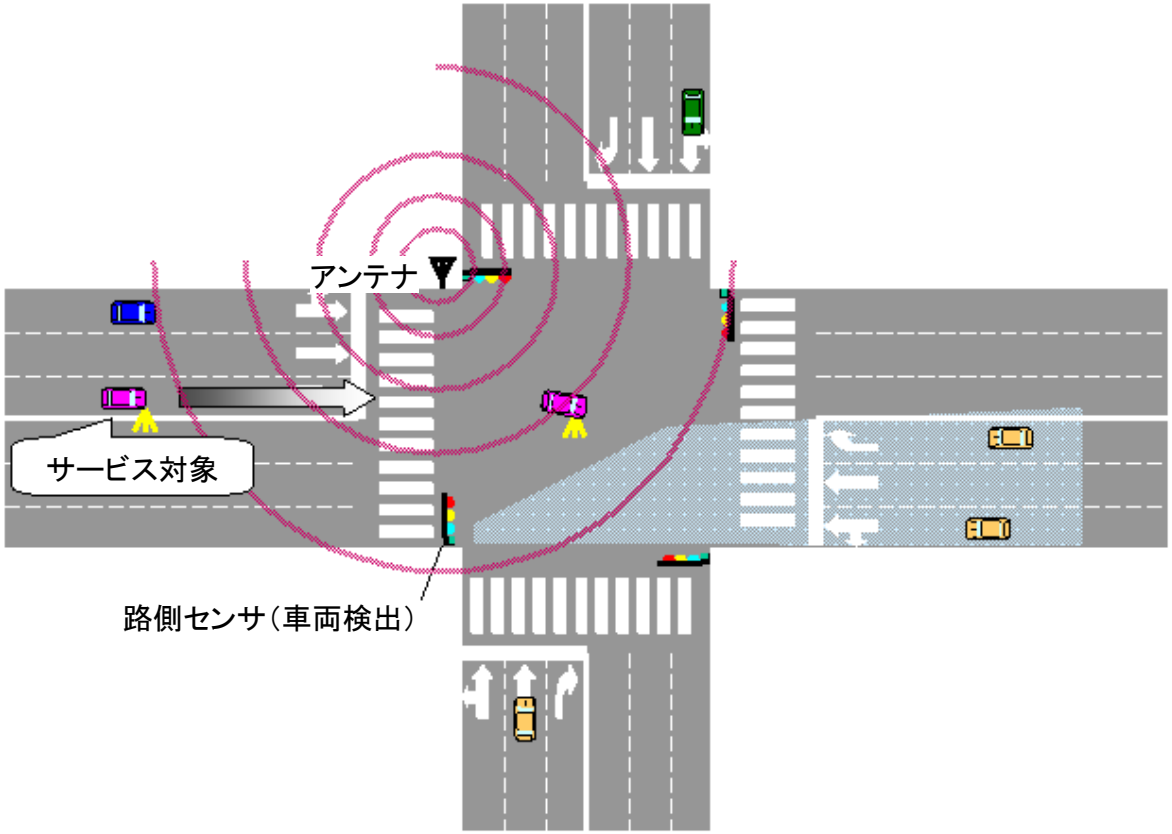
当ガイドラインが想定するサービス

2. 路車間通信における安全運転支援サービス
①出会い頭衝突防止



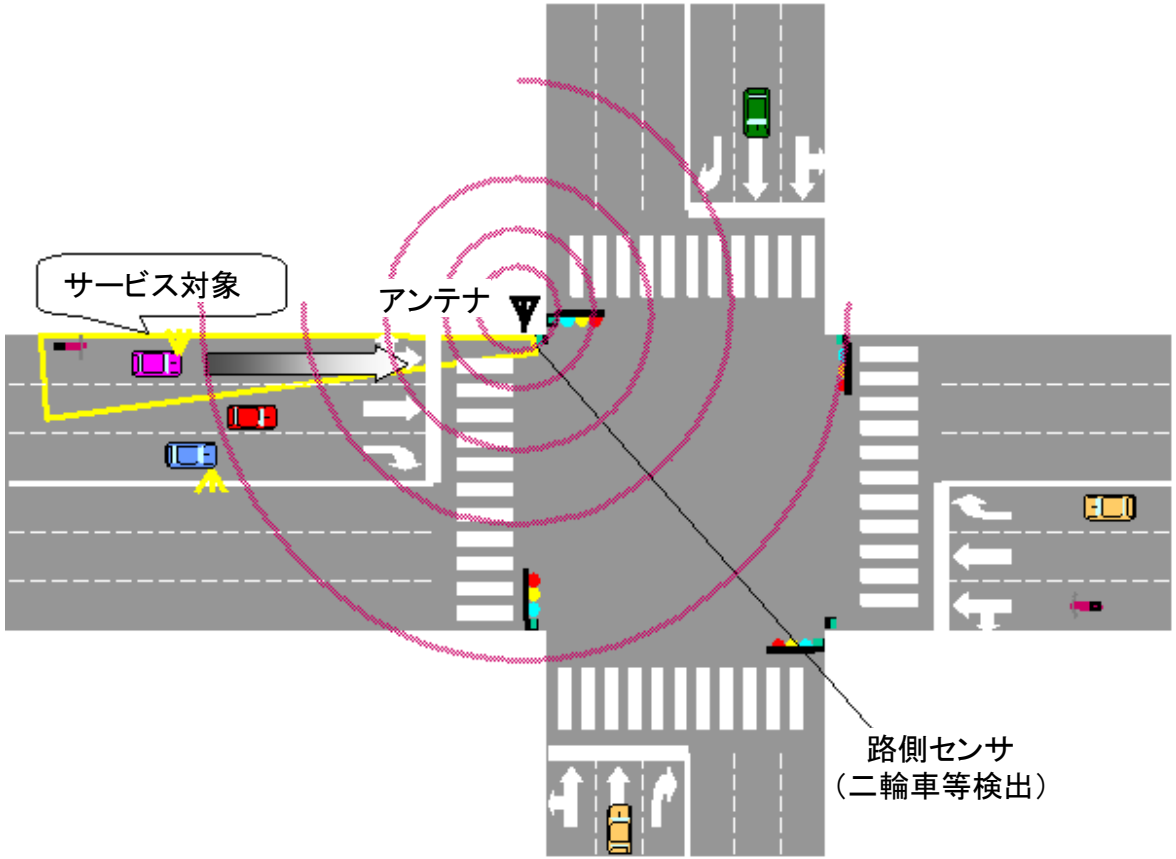
当ガイドラインが想定するサービス

2. 路車間通信における安全運転支援サービス
②右折時衝突防止



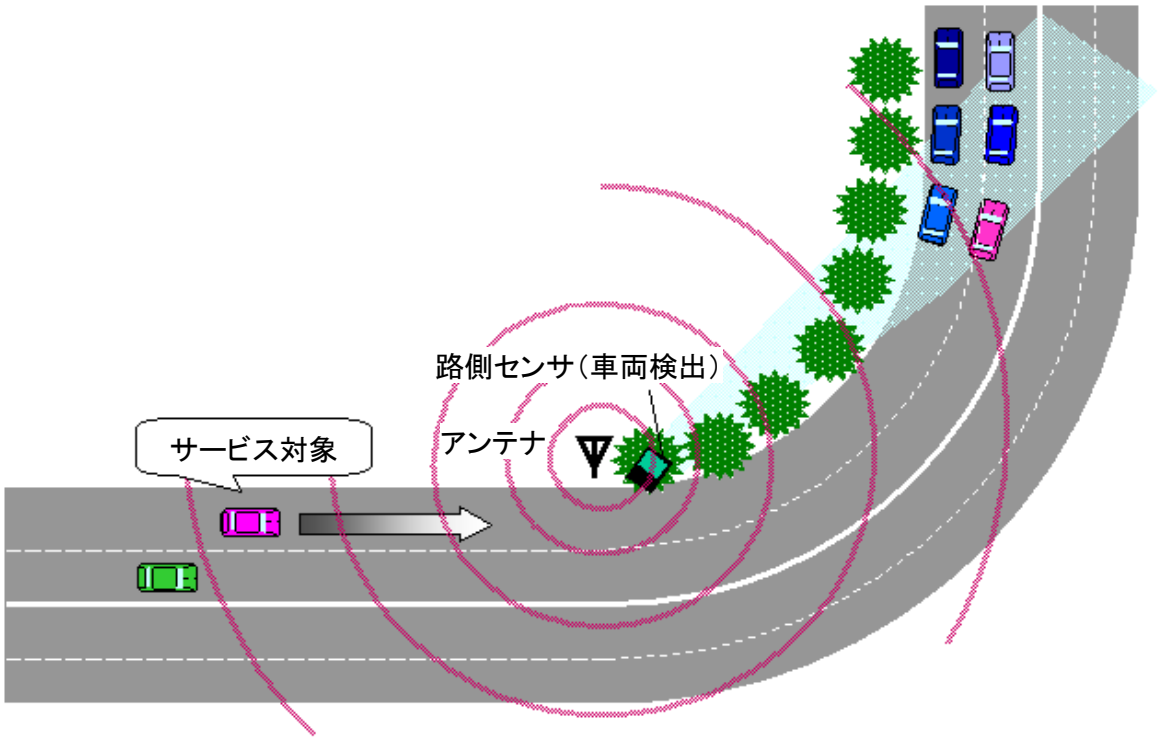
当ガイドラインが想定するサービス

2. 路車間通信における安全運転支援サービス
③左折時衝突防止



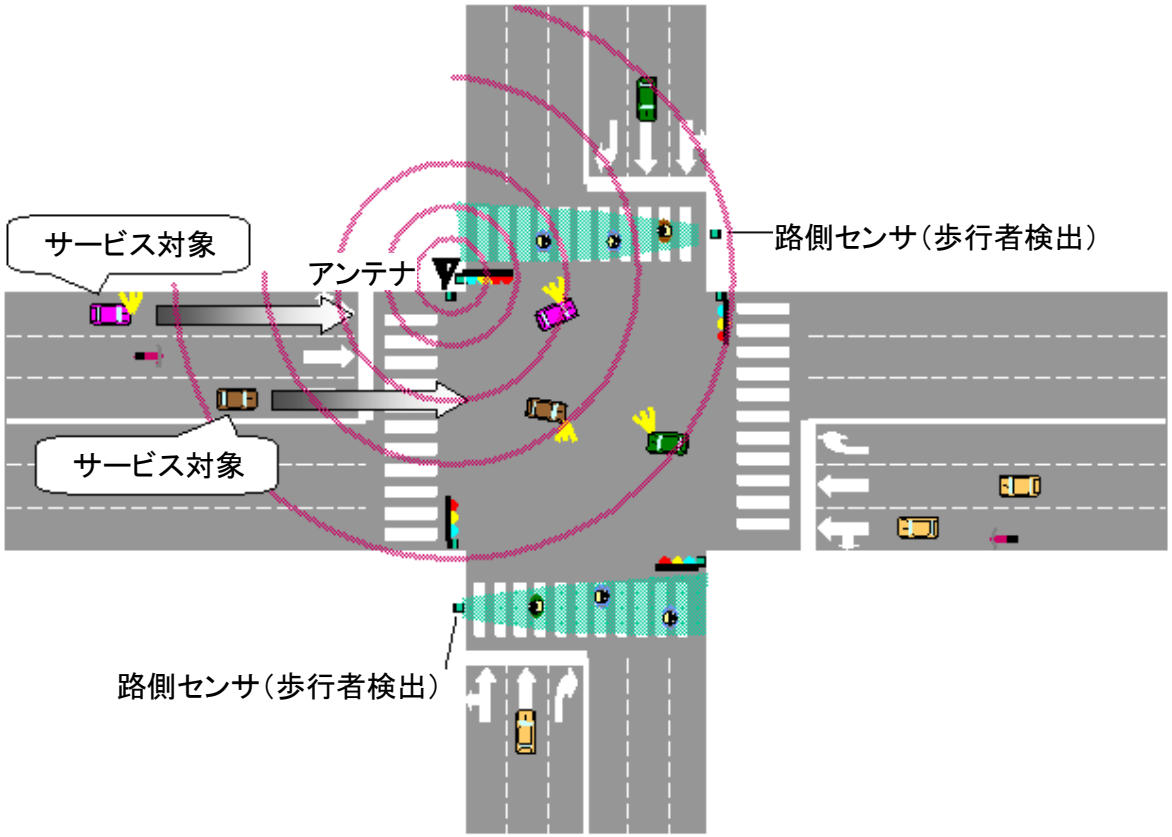
当ガイドラインが想定するサービス

2. 路車間通信における安全運転支援サービス
④追突防止



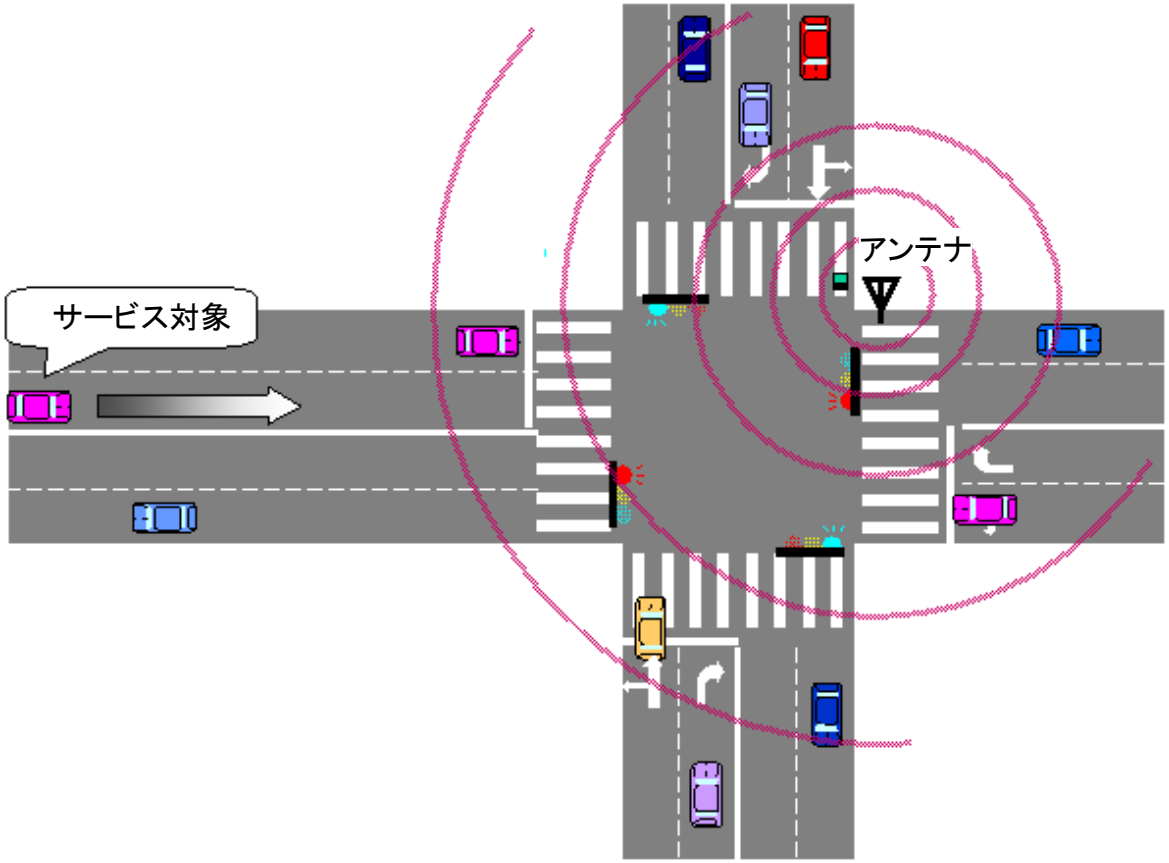
当ガイドラインが想定するサービス

2. 路車間通信における安全運転支援サービス
⑤歩行者横断見落とし防止



当ガイドラインが想定するサービス

2. 路車間通信における安全運転支援サービス
⑥信号見落とし防止



当ガイドラインが想定するサービス

2. 路車間通信における安全運転支援サービス
⑦一時停止規制見落とし防止