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

ITS FORUM RC-009 1.1 版

平成 23 年 4 月 27 日　策定

平成 24 年 4 月 25 日　改訂

ITS情報通信システム推進会議

ITS Info-communications Forum

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

ITS FORUM RC-009 1.1 版

平成 23 年 4 月 27 日　策定

平成 24 年 4 月 25 日　改訂

ITS情報通信システム推進会議

改定履歴

版数	年月日	改定箇所	改定理由	改定内容
1.0	平成 23 年 4 月 27 日	策定	新規策定	
1.1	平成 24 年 4 月 25 日	付録 Annex D	TG 検討内容の追加	セキュリティ情報の格納・更新・設定変更を行うプリミティブの検討

［余白］

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

目次

第 1 章 運用モデル概要と適用範囲 1
1.1 目的 1
1.2 運用管理モデル 2
1.3 適用範囲 4
1.4 用語の定義 6
1.4.1 用語 6
1.4.2 略語 7
1.5 参考文献 7
第 2 章 本ガイドラインが想定するサービス 9
2.1 車車間通信における安全運転支援サービス 9
2.1.1 左折時衝突防止 9
2.1.2 右折時衝突防止 10
2.1.3 出会い頭衝突防止（双方一時停止規制無し、郊外道路） 11
2.1.4 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） 12
2.1.5 追突防止 13
2.1.6 緊急車両情報提供 14
2.2 路車間通信における安全運転支援サービス 15
2.2.1 出会い頭衝突防止 15
2.2.2 右折時衝突防止 16
2.2.3 左折時衝突防止 17
2.2.4 追突防止 18
2.2.5 歩行者横断見落とし防止 19
2.2.6 信号見落とし防止 20
2.2.7 一時停止規制見落とし防止 21
第 3 章 運転支援通信システムの構成 23
第 4 章 システムに対する脅威とリスクの分析 25
4.1 分析対象の定義 25
4.2 システムにおける情報資産 26
4.3 脅威分析 28
4.4 リスク分析 31
4.4.1 リスク分析手法 31

4.4.2 リスク分析結果 32
4.5 結論 42
第 5 章 セキュリティに対する対策方針 47
第 6 章 セキュリティ対策 49
6.1 車車間・路車間通信におけるセキュリティ対策 49
6.1.1 真正性や完全性を確認する方式について 49
6.1.2 通信情報の機密性を維持する方式について 62
6.1.3 暗号アルゴリズムについて 62
6.2 路側機と車載器におけるセキュリティ対策 63
6.2.1 路側機と車載器が格納するセキュリティ情報 63
6.2.2 路側機と車載器の製造 63
6.2.3 路側機と車載器の実装 63
6.3 運用管理機関におけるセキュリティ対策 64
6.3.1 外部エンティティに関するセキュリティ対策 64
6.3.2 運用管理機関内部でのセキュリティ対策 69
第 7 章 付録 71
Annex A. 共通鍵アルゴリズム適用時の鍵管理について 71
Annex B. リプレイ攻撃について 73
Annex C. 路情報(間)への攻撃と対策例 75
Annex D. セキュリティ情報の格納・更新・設定変更を行うプリミティブの検討 76

第1章　運用モデル概要と適用範囲

1.1　目的

本ガイドラインは、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ガイドラインを記載する。

なお、本ガイドラインは、運用管理ガイドライン[1]記載のサービス・コンテンツ管理におけるセキュリティに対応するものである。

基本方針を以下に示す。

- 提供するサービスの品質維持のため、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。

1.2　運用管理モデル

運転支援通信システムの運用に関わる関係主体(以下、エンティティと記す)とその関連を以下に示す。

(1)　各エンティティとその関係

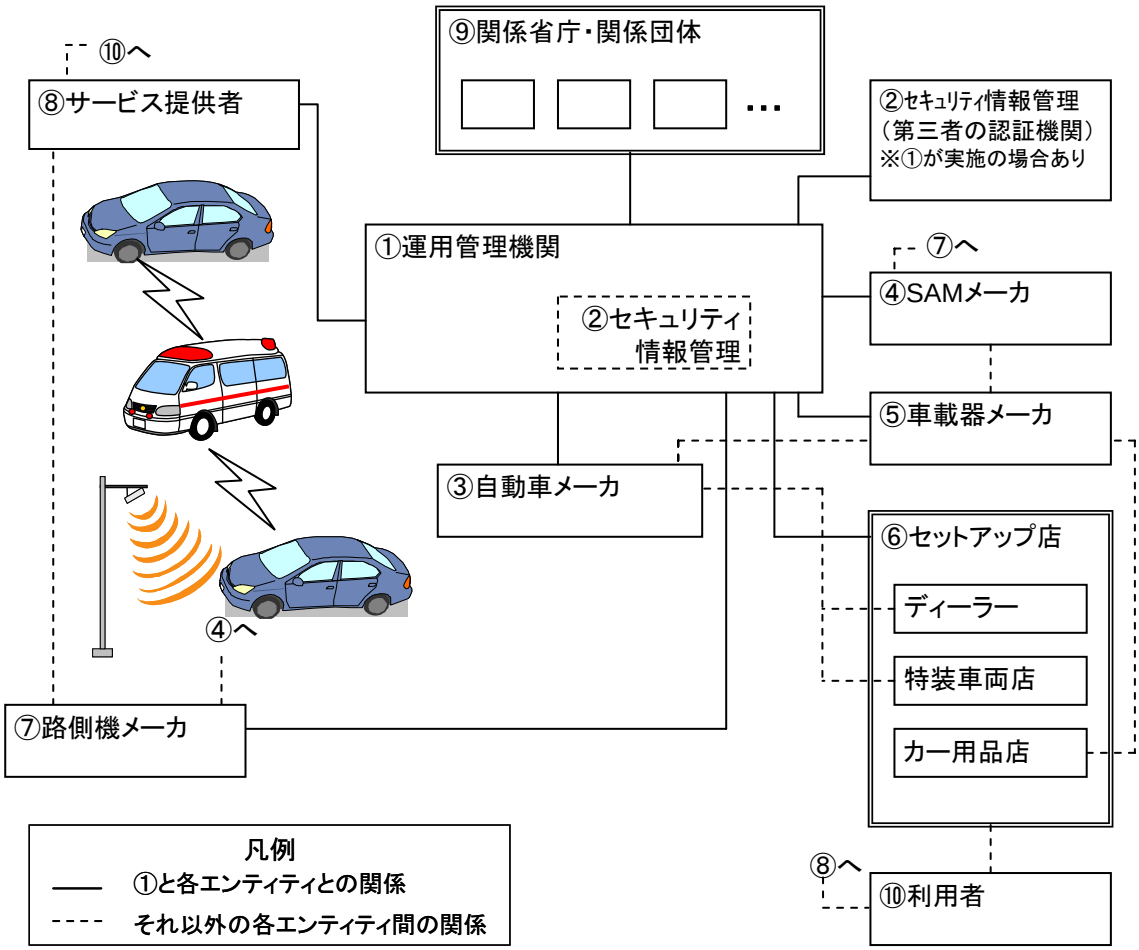


図 **1-1** 運用管理機関と各エンティティの関係

(2) 各エンティティの役割

各エンティティの主な役割（案）を以下に示す。なお、各エンティティの名称は、役割の名称を示すものであり、一つの企業・団体等が複数のエンティティの役割を担う場合もある。

表 1-1 各エンティティの役割

エンティティ	役割
①運用管理機関	・路側機や車載器などの機器管理 ・システム内、他システムとの電波管理 ・路車間通信、車車間通信の通信管理 ・システムのセキュリティなどのサービス・コンテンツ管理 ・その他、ユーザーサポートや普及促進活動など
②セキュリティ情報管理 (運用管理機関が実施する場合あり)	・路側機・車載器の認証業務
③自動車メーカ	・車載器を搭載した自動車の製造・販売
④SAM メーカ	・路側機や車載器に搭載する SAM の開発や製造
⑤車載器メーカ	・車載器の製造や販売
⑥セットアップ店 (ディーラー、特装車両店、カー用品店)	・車載器を動作可能とするための情報のセットアップ (緊急車両等は特装車両店限定)
⑦路側機メーカ	・路側機の製造・販売
⑧サービス提供者	・車載器ユーザーの管理 ・車車間通信における運転支援に関わる情報の配信などサービス全般の提供(車車間通信のみのサービス提供時) ・路車間通信における運転支援に関わる情報の収集や配信などサービス全般の提供 ・路側機の保有 ・路側機の動作確認
⑨関係省庁、関係団体	・許認可、他の安全運転関連のシステム等との連携
⑩利用者	・サービスの享受

(3) エンティティの登録と管理

運用管理機関はシステム運用のためのエンティティ契約を取り交わしたサービス提供者や各メーカ、セットアップ店などのエンティティの管理のため、エンティティ登録を行う必要がある。また、

運用管理機関は登録機能の他、運用体制構築、エンティティ管理規程などを整備し、登録された各エンティティの役割、権利と責任の範囲などを明らかにする必要がある。

1.3　適用範囲

運用管理機関の持つべき機能のうち、本ガイドラインの適用範囲とその詳細を図 1-2 に示す。

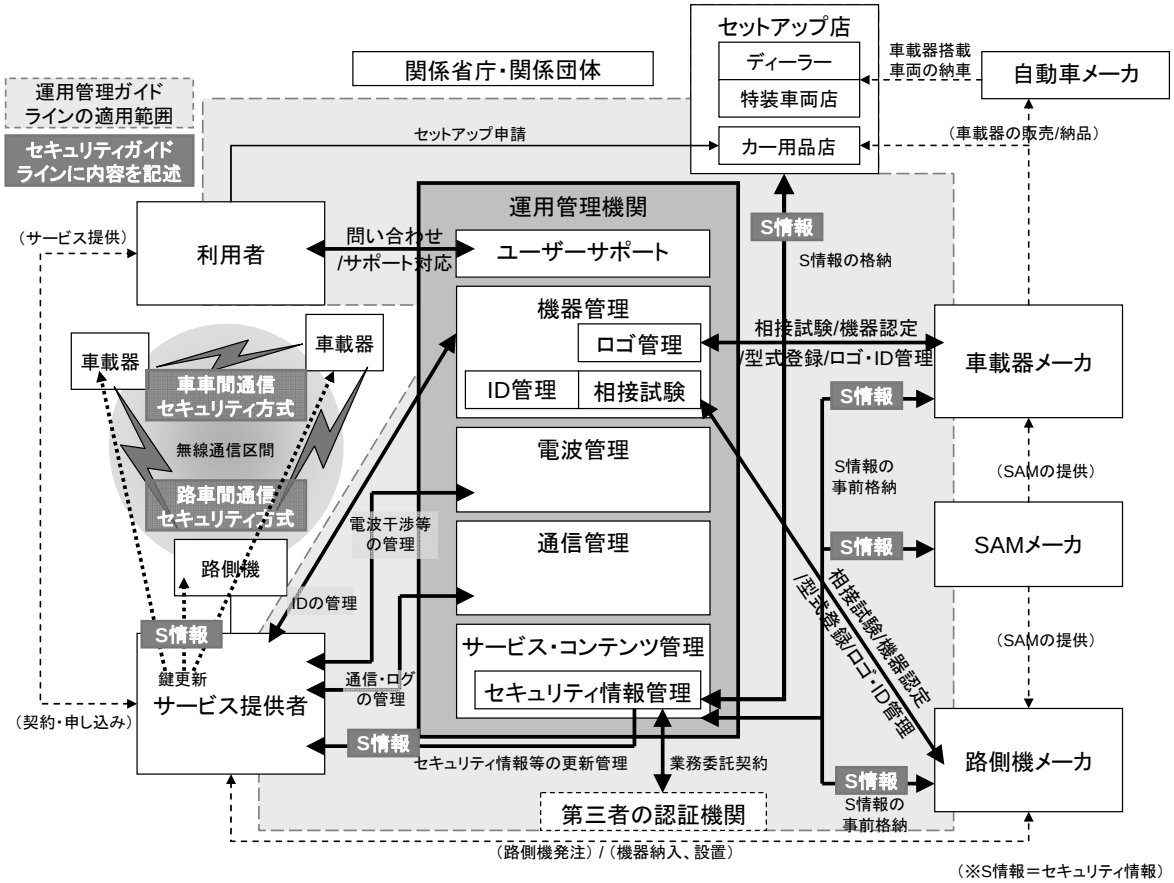


図 1-2 セキュリティガイドラインの適用範囲

運用管理機関の役割を以下に示す。

＜機器管理＞

- 路側機、車載器の相互接続性試験環境の提供
- 路側機、車載器の相互接続性試験の実施、機器の相互接続性認定
- 路側機、車載器の型式登録、ロゴの利用・管理
- 路側機、車載器の ID 管理
- 路側機、車載器の運用中の正常動作管理

＜電波管理＞

- 電波干渉管理（周波数隣接システム、他の安全運転関連システムとの干渉調整、管理など）
- 他システムとの調整（周波数隣接システム、他の安全運転関連システムとの干渉における費用分担など）
- 電波の正常動作管理（運用中の管理）

＜通信管理＞

- 通信の正常動作管理
- 通信ログの管理

＜サービス・コンテンツ管理＞

- システムのセキュリティに関する環境の提供や運用
- 機器に対するセキュリティ関連のセットアップの環境整備及び運用
- セキュリティ情報の更新管理
- セキュリティ情報の抹消

＜その他＞

- エンティティの登録・管理
- ユーザーサポート
- 体制検討・整備、普及促進活動　など

1.4　用語の定義

1.4.1　用語

本書で使用する用語を表 1-2 のように定義する。

表 1-2 用語の定義

用語	定義
車載器	他の車両又は路側機等と能率的に直接通信する無線設備機能を持ち、専らこの通信により自動車の運転支援を行うための機器であって、以下の機能の一部又は全てを備えるものをいう。 ①　当該車両上の他の機器との情報をやり取りする機能。 ②　当該車両の状態を検知するための機能 ③　当該車両の状態を変化させるための機能 ④　当該車両の搭乗者への情報提供機能 特に、本システム用の登録済みの車載器をさす。
路側機	路側センサ等で検知した交通状況や信号情報等のインフラの情報を、通信エリア内を走行する車両と能率的に通信する無線設備機能にて提供する、路側に設置される無線装置機器の事をいう。特に、本システム用の登録済みの路側機をさす。
第三者	車載器を保有していない本システム外の者。
利用者	車載器を保有する本システムの利用者。
保守員	車載器や路側機、車両を保守する者。
通信機	車載器、路側機以外の通信装置。
SAM	セキュアアプリケーションモジュール、車載器内で保有する車両情報の保護、耐タンパ性を確保するための暗号化ロジックなどが格納されたモジュール。
ネガリスト	無効な機器(車載器や路側機)の ID や公開鍵証明書のリスト。CRL や失効機器 ID リストを含む。
セキュリティ情報	車車間通信や路車間通信において、セキュアにデータのやりとりを行うために必要な通信鍵や証明書、デジタル署名など、通信に用いるセキュリティに関連する情報を一括してセキュリティ情報と呼ぶこととする。また、以後図表中では略して「S 情報」と記載する。

1.4.2 略語

AES	:	Advanced Encryption Standard
CA	:	Certificate Authority
CBC	:	Cipher Block Chaining
CCM	:	Counter with CBC-MAC
CRL	:	Certificate Revocation List
CRYPTREC	:	Cryptography Research and Evaluation Committees
CTR	:	Counter
DoS	:	Denial of Service
ECDSA	:	Elliptic Curve Digital Signature Algorithm
ETSI	:	European Telecommunications Standards Institute
GPS	:	Global Positioning System
MAC	:	Message Authentication Code
OCSP	:	Online Certificate Status Protocol
PKI	:	Public Key Infrastructure
SAM	:	Secure Application Module

1.5 参考文献

[1] “運転支援通信システムに関する運用管理ガイドライン”

[2] C. Laurendeau and M. Barbeau, “Threats to Security in DSRC/WAVE,” ADHOC-NOW Lecture Notes in Computer Science, Volume 4104, 2006 page.266-279.

[3] Bryan Parno and Adrian Perrig, “Challenges in securing vehicular networks”, In Workshop on Hot Topics in Networks (HotNets-IV), 2005

[4] M. Raya, P. Papadimitratos and J-P. Hubaux, "Securing Vehicular Networks", IEEE Wireless Communications, Volume 13, Issue 5, October 2006

[5] M. Raya and J.-P. Hubaux, “Security Aspects of Inter-Vehicle Communications”, In Proceedings of STRC 2005 (Swiss Transport Research Conference), March 2005

[6] IPA, “自動車と情報家電の組込みシステムのセキュリティに関する調査”, 2009 年 3 月

[7] M. Barbeau, “WiMax/802.16 threat analysis”, Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet), 2005

[8] IEEE 1609.2, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments -

Security Services for Applications and Management Messages, 2006/7

[9] NIST Special Publication 800-38C, “Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality”

第2章　本ガイドラインが想定するサービス

2.1　車車間通信における安全運転支援サービス

本ガイドラインが想定する車車間通信における具体的なサービスイメージを以下に示す。

2.1.1　左折時衝突防止

・サービスの概要

交差点において、左後方から接近する二輪車等の情報を左折しようとする車両のドライバに提供する。

・サービスイメージ

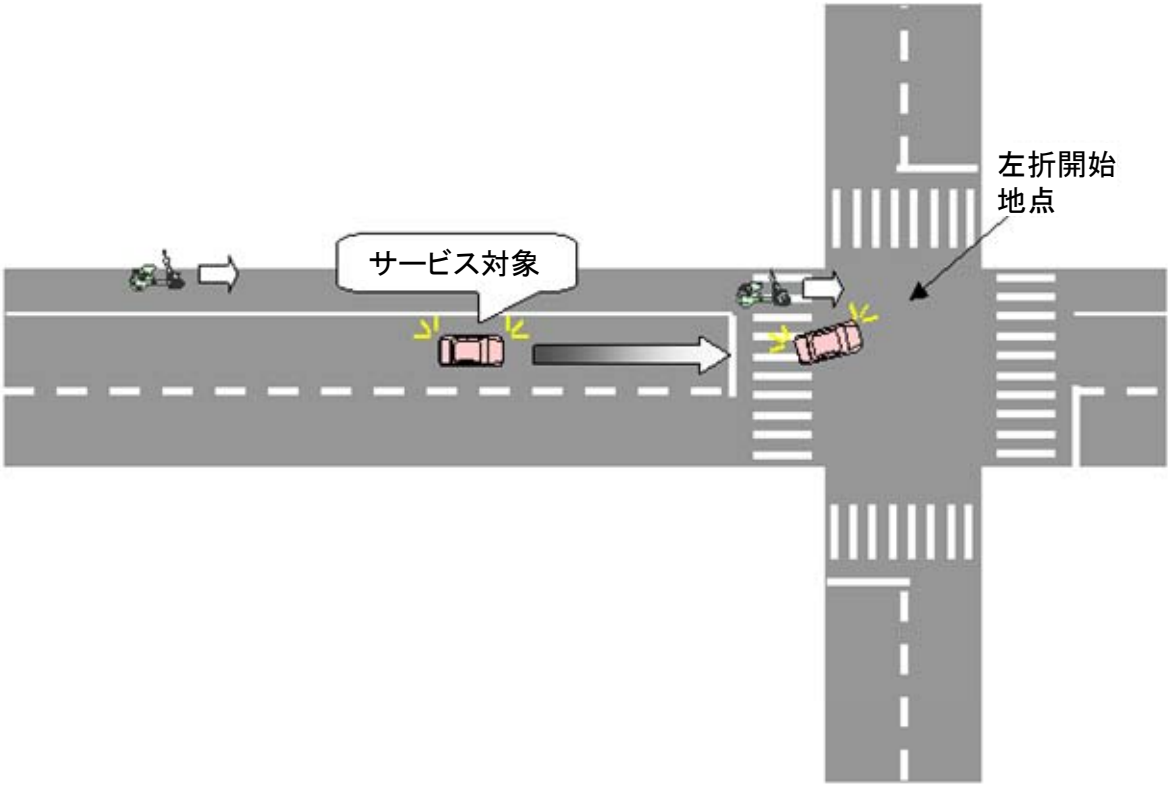


図 **2-1** 左折時衝突防止サービスのイメージ

2.1.2　右折時衝突防止

・サービスの概要

交差点において、対向直進車両等の情報を右折待ちしている車両のドライバに提供する。

・サービスイメージ

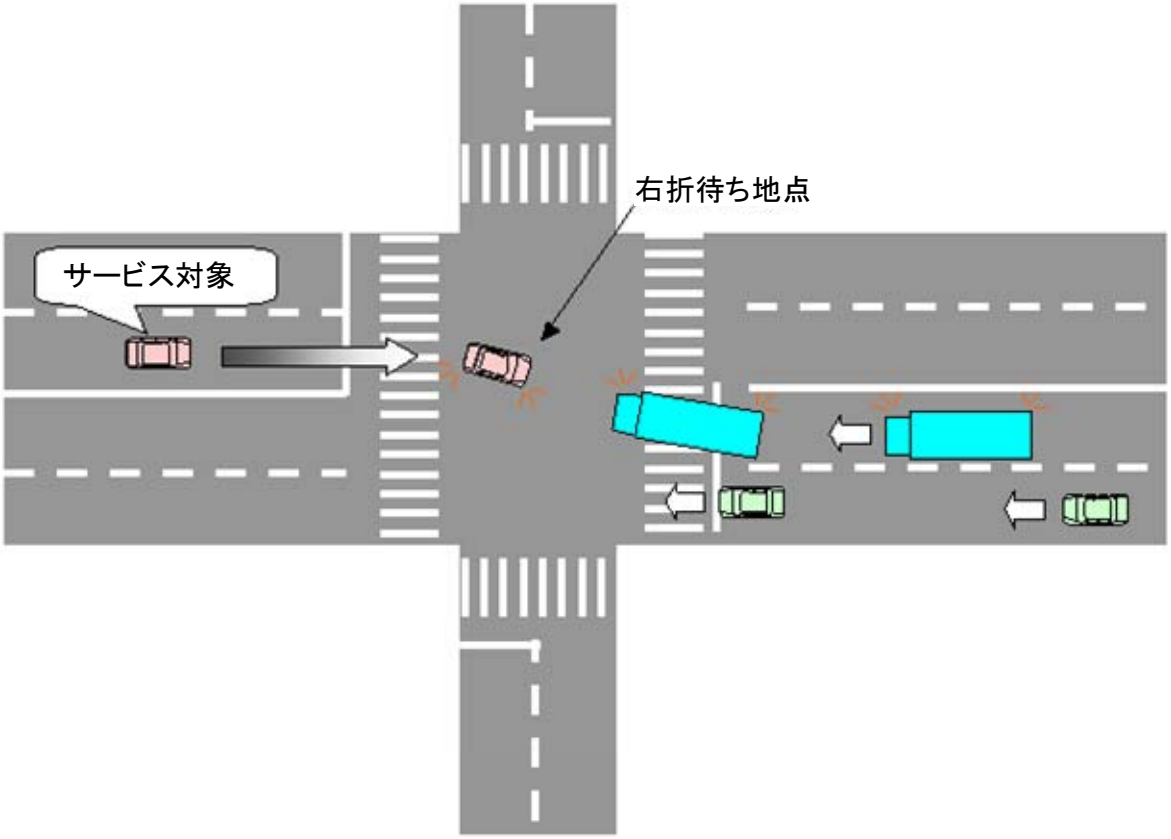


図 **2-2** 右折時衝突防止サービスのイメージ

2.1.3　出会い頭衝突防止（双方一時停止規制無し、郊外道路）

・サービスの概要

一時停止規制のない交差点において、交差する道路の車両の情報を交差点に接近する車両のドライバに提供する。

・サービスイメージ

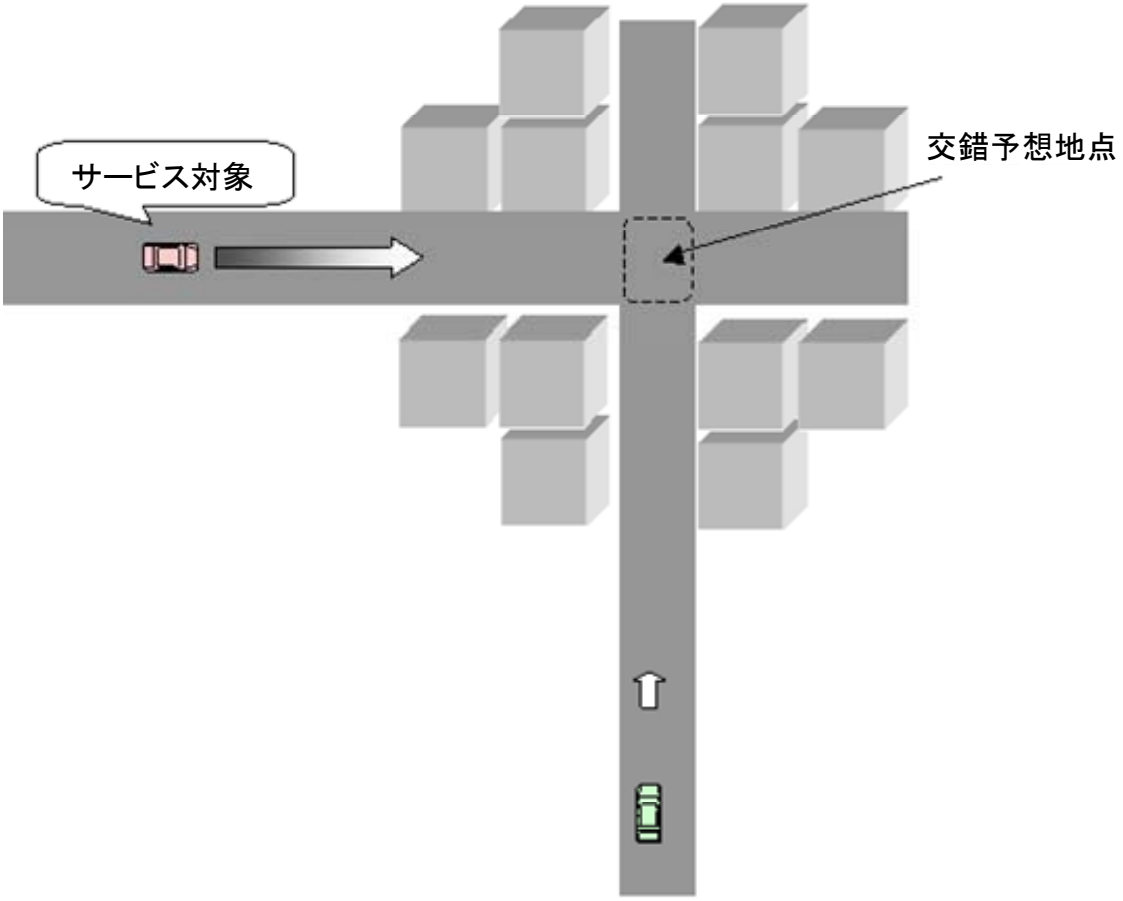


図 **2-3** 出会い頭衝突防止サービス（双方一時停止規制なし、郊外道路）のイメージ

2.1.4　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）

・サービスの概要

一時停止規制のある見通しが悪い交差点において、交差する道路の車両等の情報を交差点に接近する車両のドライバに提供する。

・サービスイメージ

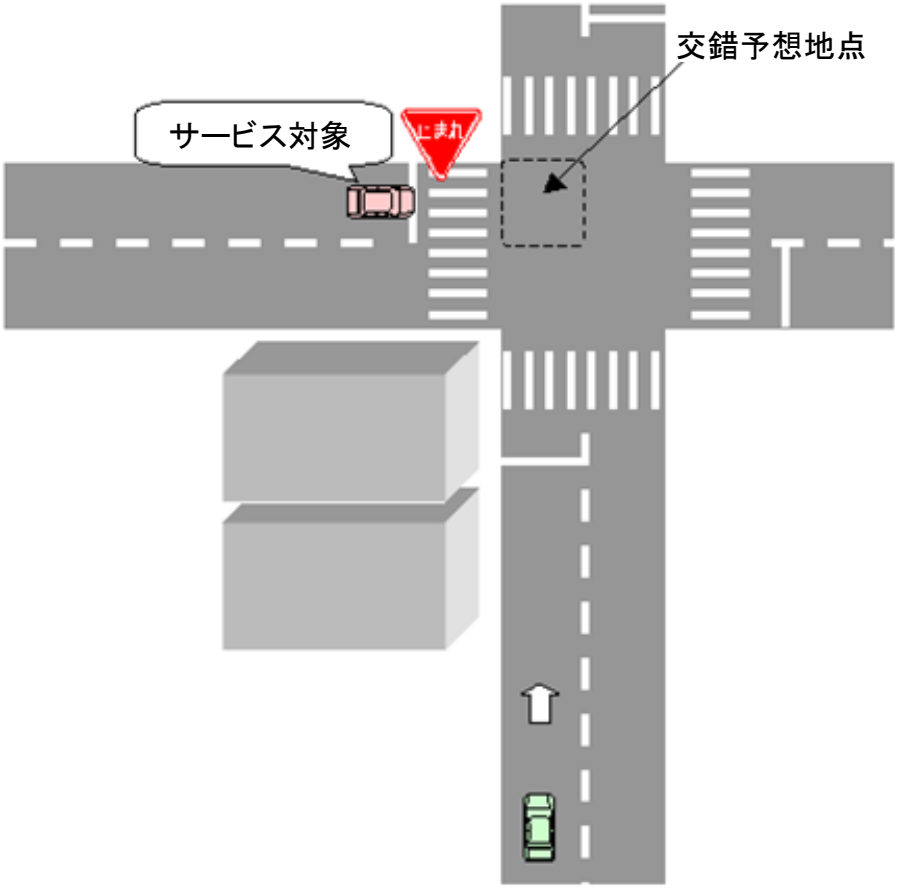


図 **2-4** 出会い頭衝突防止サービス（一時停止規制あり、見通し外）のイメージ

2.1.5　追突防止

・サービスの概要

見通しが悪い場所等において、前方の低速走行又は停止車両等の情報を同一車線後方を走行する車両のドライバに提供する。

・サービスイメージ

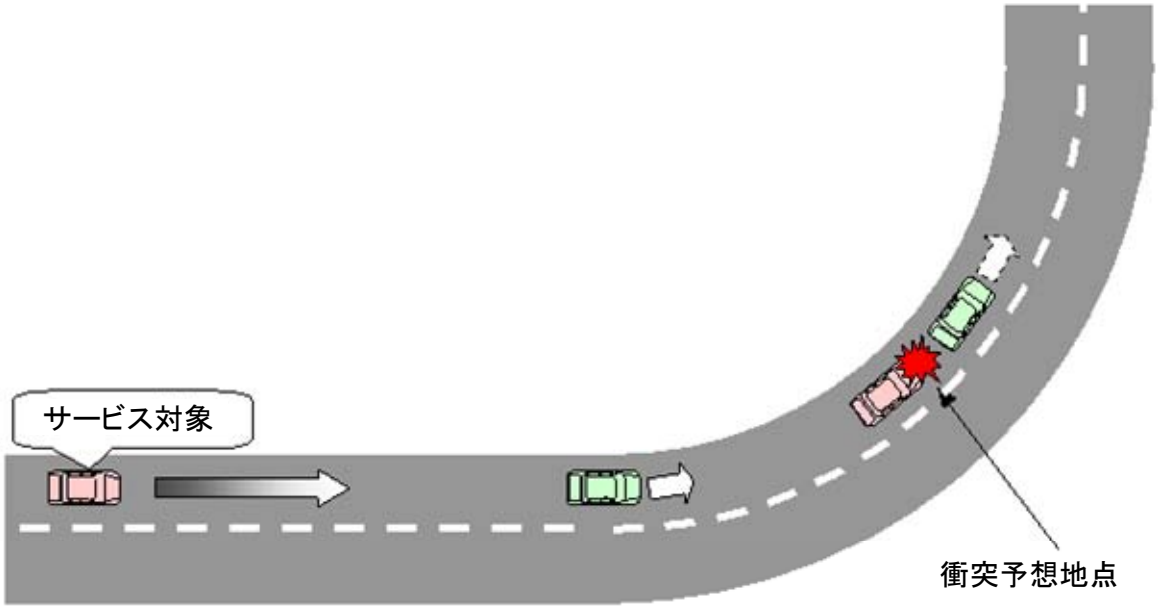


図 **2-5** 追突防止サービスのイメージ

2.1.6　緊急車両情報提供

・サービスの概要

緊急車両の緊急時の情報を周辺にいる車両のドライバに提供する。

・サービスイメージ

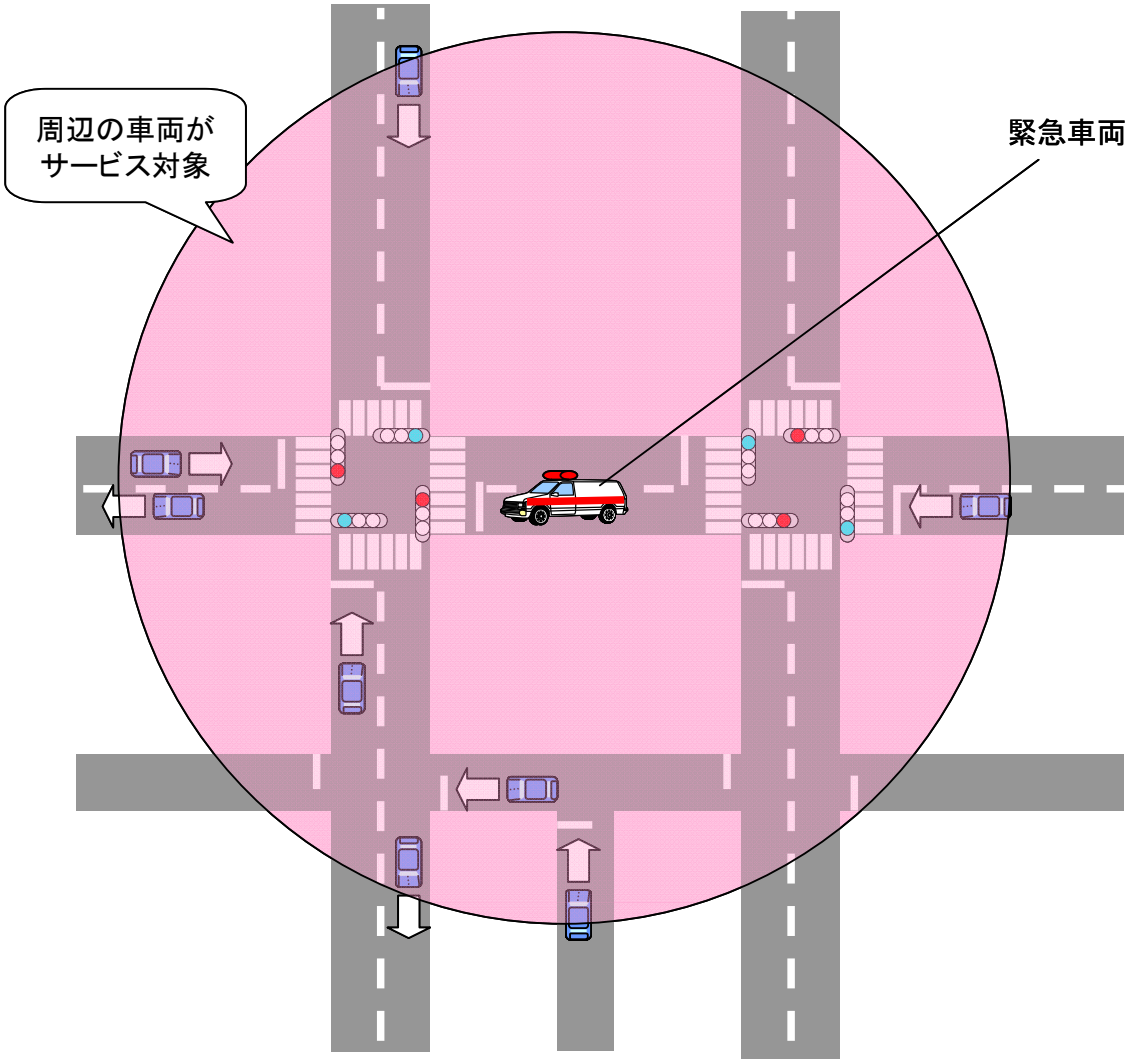


図 **2-6** 緊急車両情報提供サービスのイメージ

2.2　路車間通信における安全運転支援サービス

本ガイドラインが想定する路車間通信における具体的なサービスイメージを以下に示す。

2.2.1　出会い頭衝突防止

・サービスの概要

信号機のない交差点において、路側センサ等により交差する道路の車両を検出し、その情報を交差点に接近する車両のドライバに提供する。

・サービスイメージ

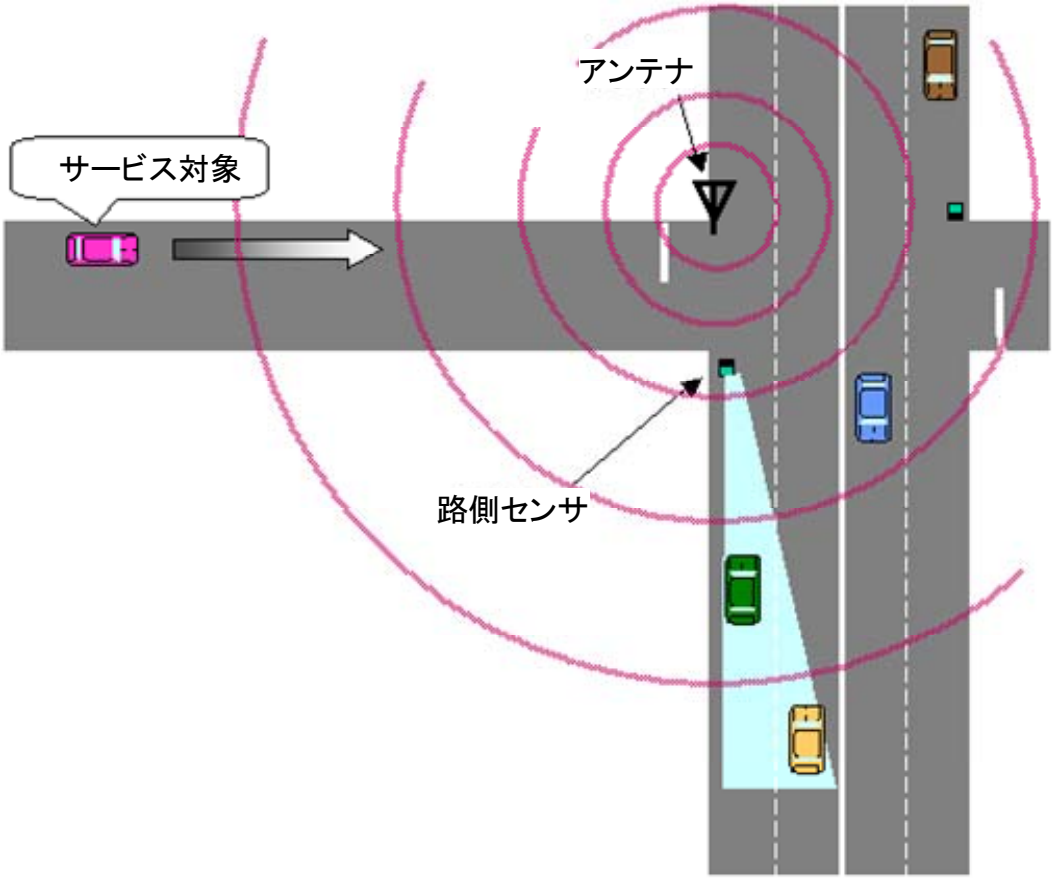


図 **2-7** 出会い頭衝突防止サービスのイメージ

2.2.2　右折時衝突防止

・サービスの概要

交差点において、路側センサ等により対向直進車両等を検出し、その情報を右折しようとする車両のドライバに提供する。

・サービスイメージ

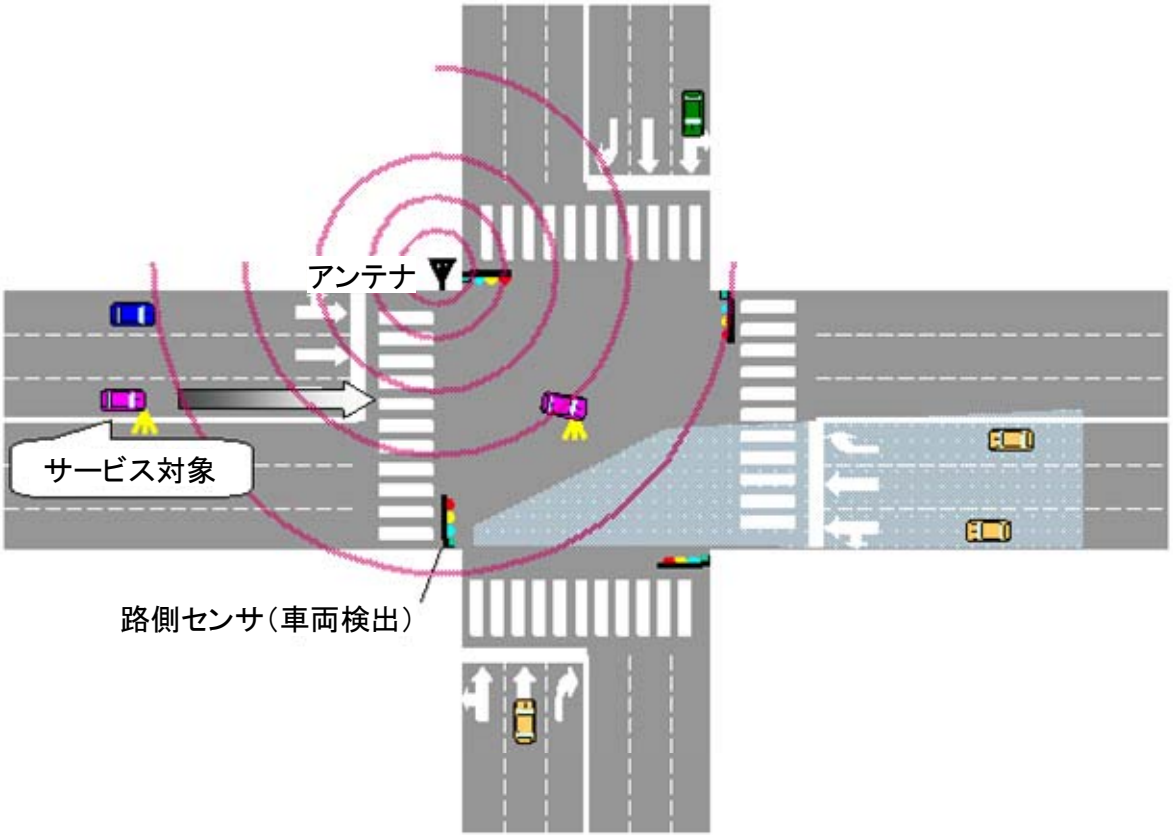


図 **2-8** 右折時衝突防止サービスのイメージ

2.2.3　左折時衝突防止

・サービスの概要

交差点において、路側センサ等で左後方から接近する二輪車等を検出し、その情報を左折しようとする車両のドライバに提供する。

・サービスイメージ

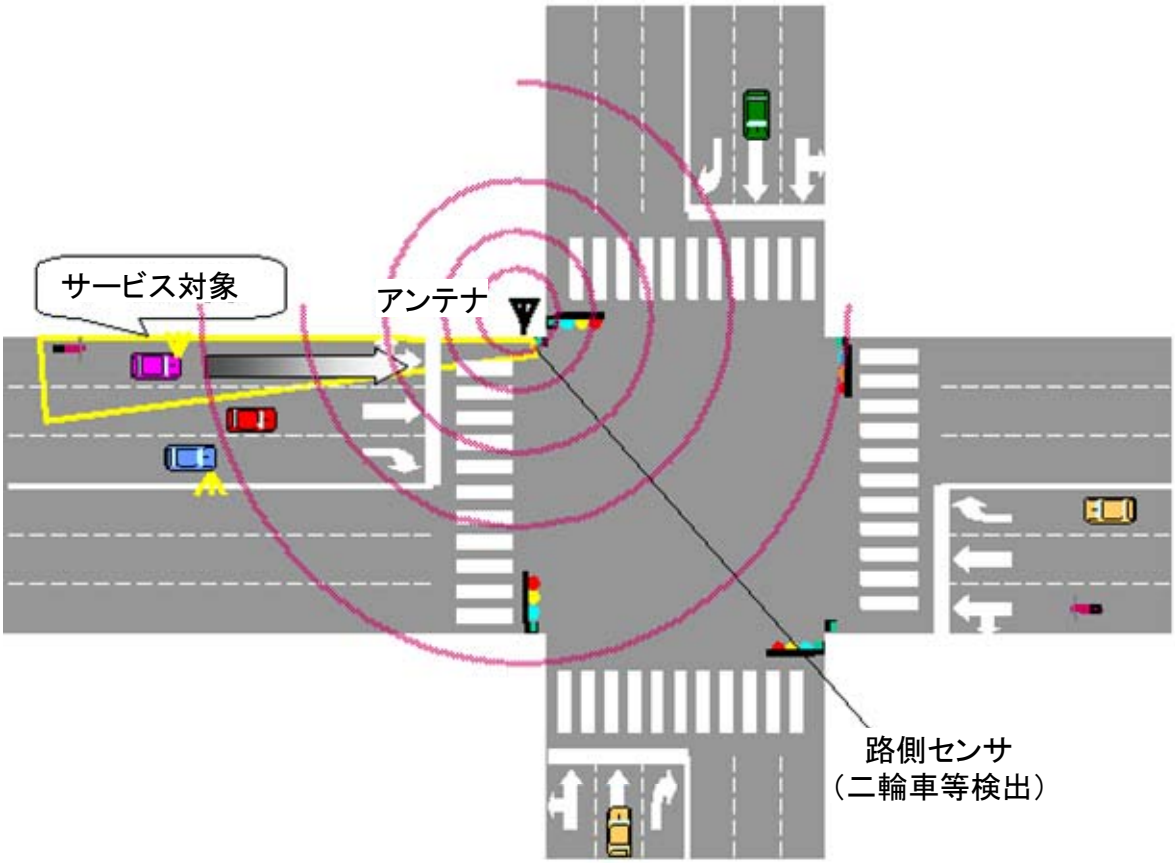


図 **2-9** 左折時衝突防止サービスのイメージ

2.2.4　追突防止

・サービスの概要

見通しが悪い場所等において、路側センサ等で前方の車両等を検出し、その情報を同一車線後方を走行する車両のドライバに提供する。

・サービスイメージ

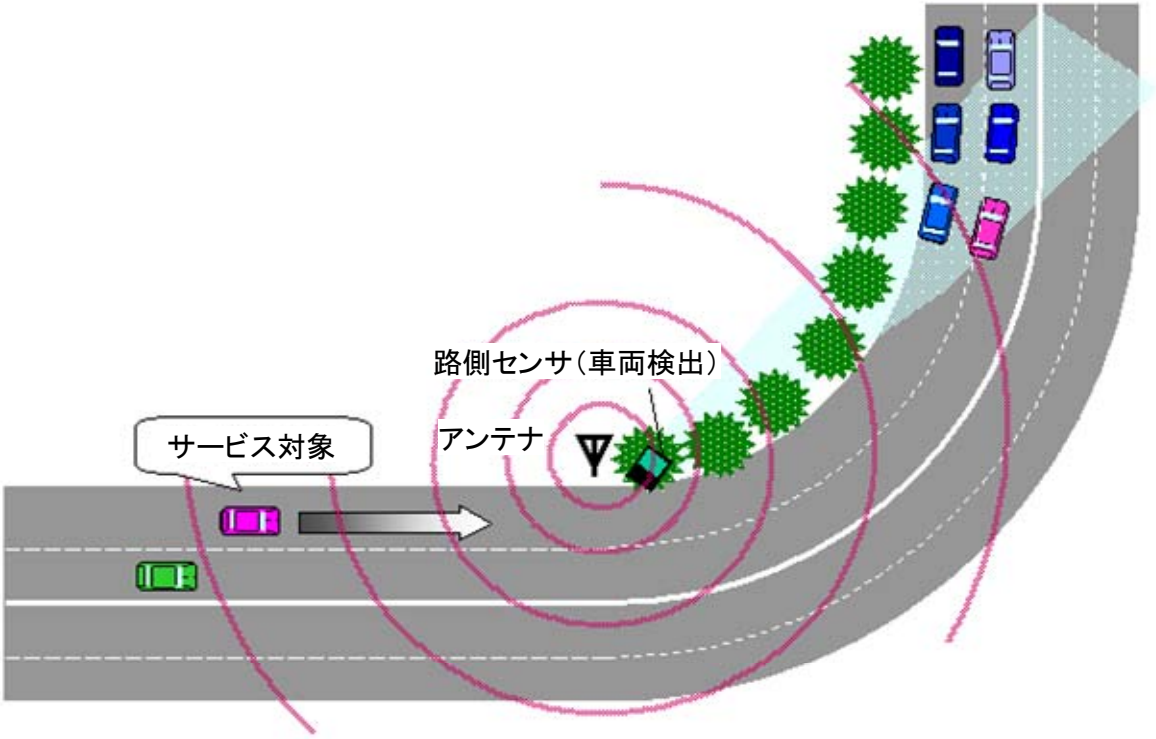


図 **2-10** 追突防止サービスのイメージ

2.2.5　歩行者横断見落とし防止

・サービスの概要

路側センサ等で横断歩道上の歩行者等を検出し、交差点を右左折しようとする車両のドライバにその情報を提供する。

・サービスイメージ

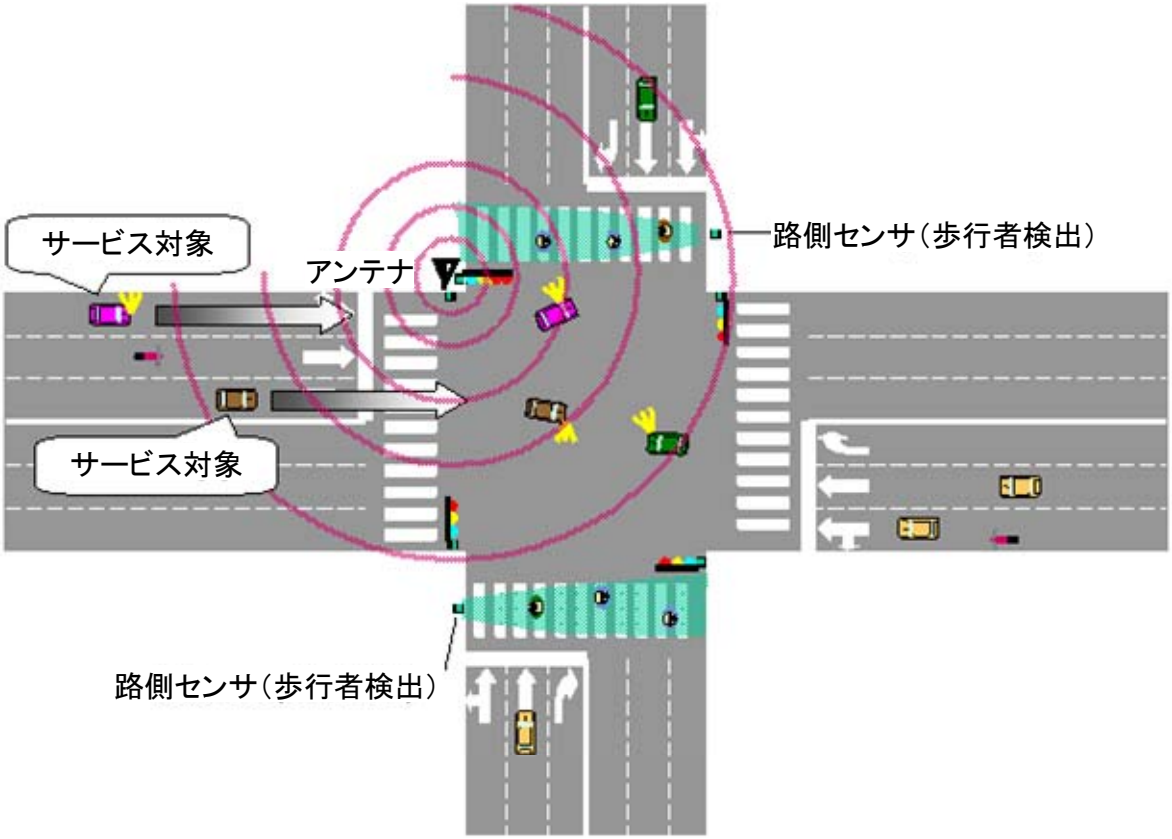


図 **2-11** 歩行者横断見落とし防止サービスのイメージ

2.2.6　信号見落とし防止

・サービスの概要

信号がある交差点において、赤信号の見落としなど信号に関連ある事故を防止するために、信号機の灯色に関する情報を車両のドライバに提供する。

・サービスイメージ

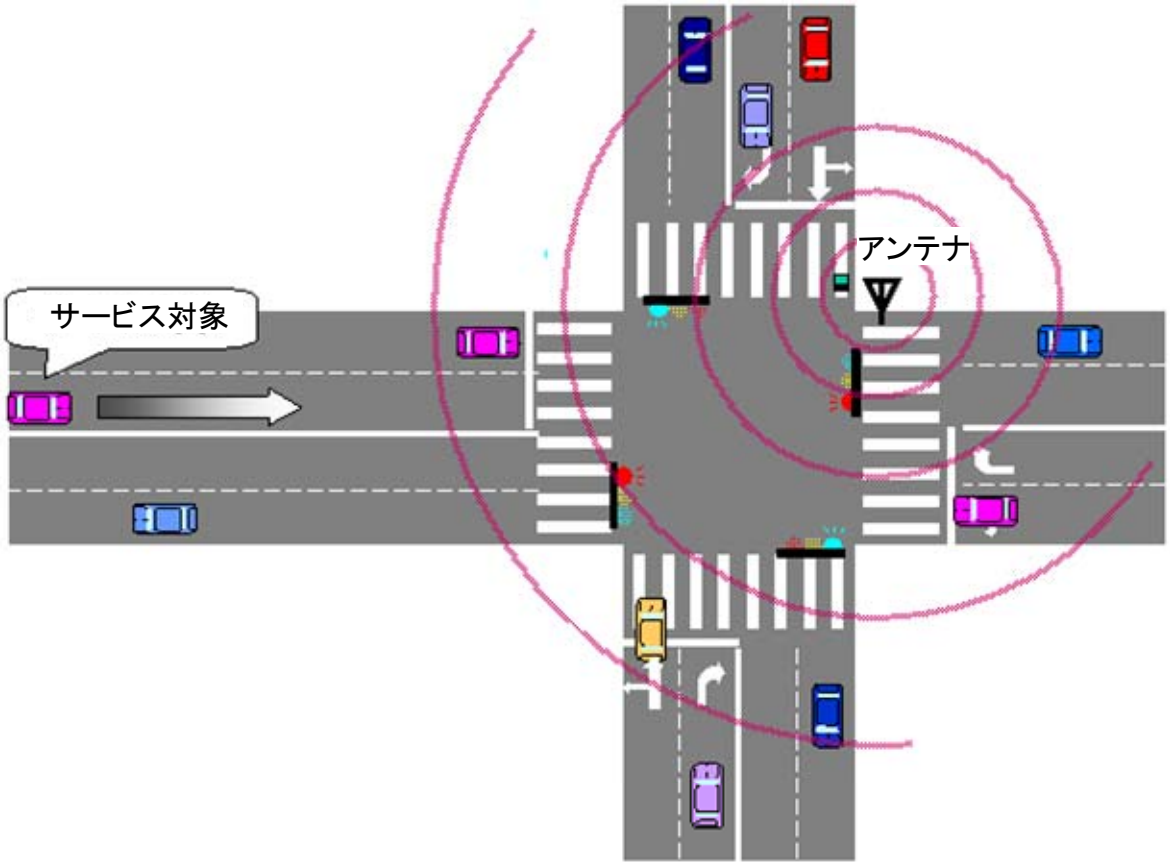


図 **2-12** 信号見落とし防止サービスのイメージ

2.2.7　一時停止規制見落とし防止

・サービスの概要

信号がない交差点において、一時停止等の規制情報の見落としなどによる事故を防止するために、規制に関する情報を車両のドライバに提供する。

・サービスイメージ

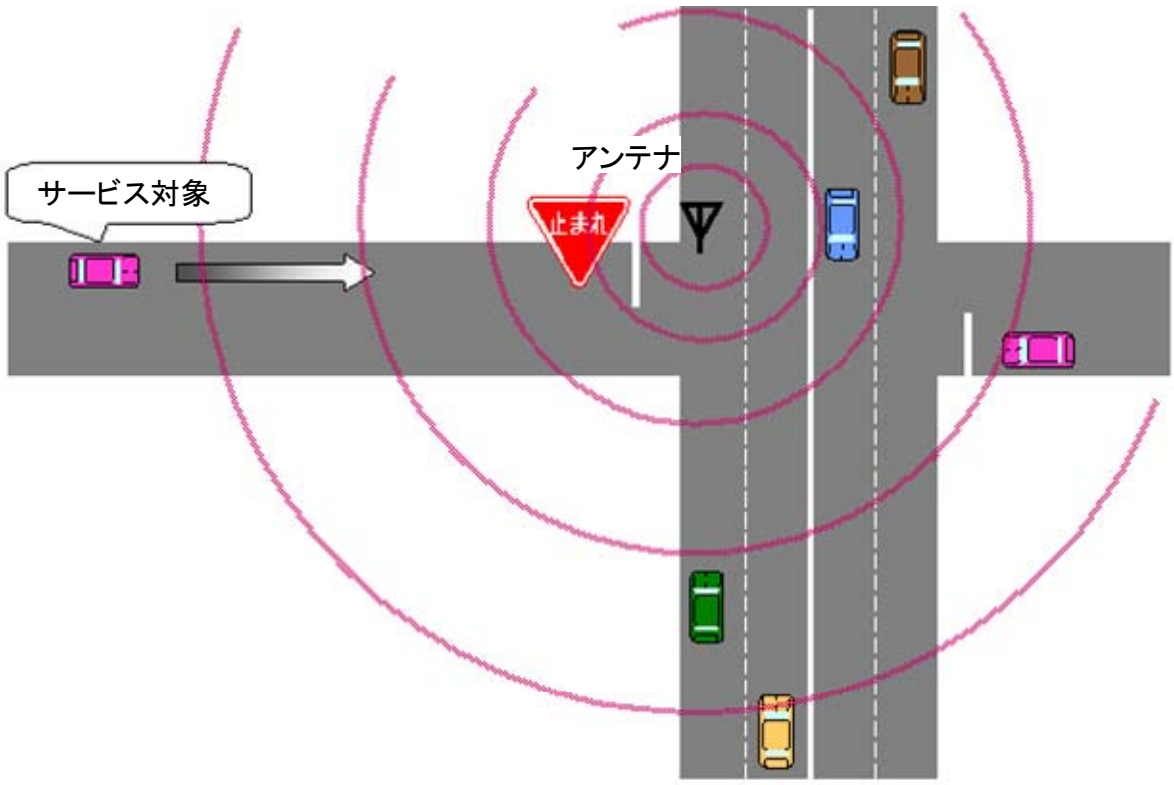


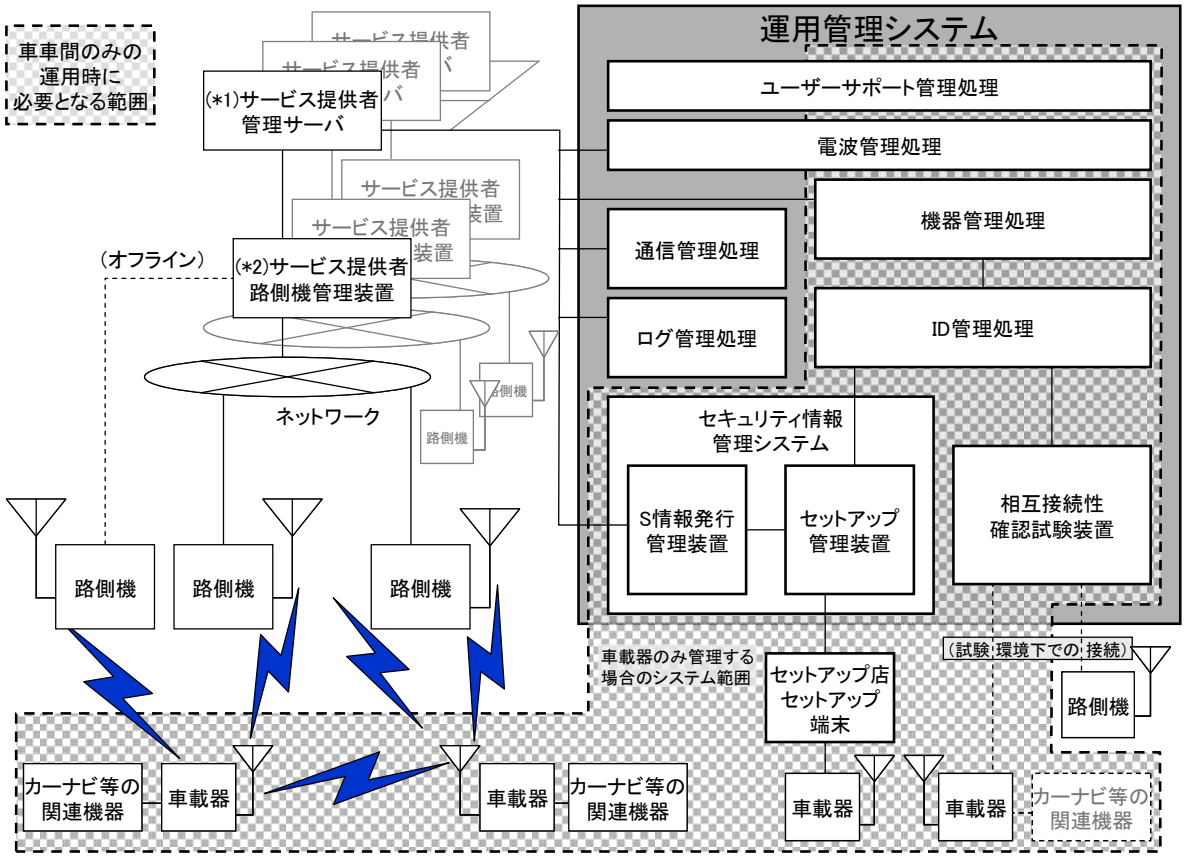
図 **2-13** 一時停止規制見落とし防止サービスのイメージ

［余白］

第3章　運転支援通信システムの構成

前章で示した具体的なサービスを実現するために必要な機器のシステム構成図を以下に示す。

なお、本ガイドラインでは想定されるシステム構成についても網羅的に示しており、複数のサービス提供者がそれぞれ保有する路側機と、それを管理する管理装置やサーバが運用管理機関の各装置と連携して運用され、それらインフラ機器にユーザー保有の車載器が繋がる全体図を以下の図3-1に示す。特にサービス提供者が路側機を用いず、車載器のみで運用する場合も必要となる機器・システム構成として破線枠で囲んだ範囲を定めた。



(*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)

図 3-1 本システムのシステム構成図

［余白］

第4章　システムに対する脅威とリスクの分析

前章で示したシステムに対する脅威を識別し、そのリスクを分析する。以下にこれらの手順を示す。

なお、本分析では、まず、路車間及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。

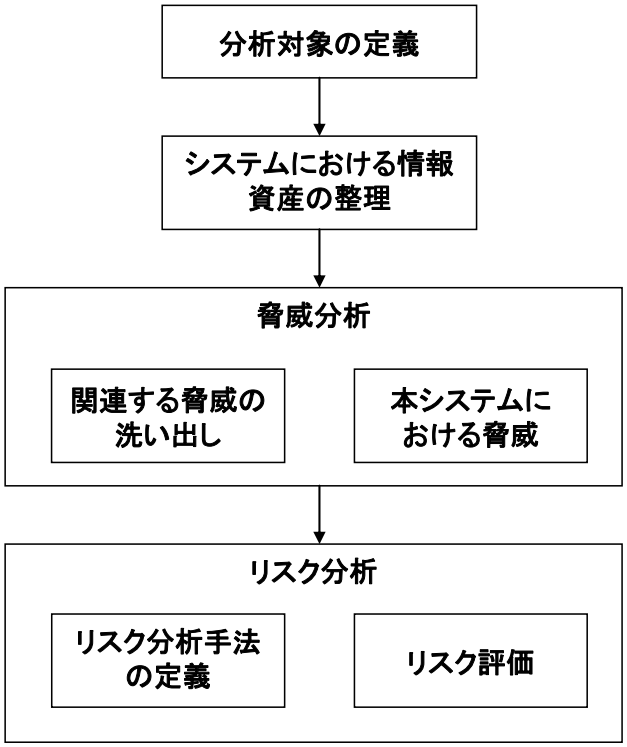


図 **4-1** 脅威及びリスク分析の手順

上記手順に従って、分析した結果を本章で述べる。

4.1　分析対象の定義

図 4-2 に示すように、本分析での検討対象は、路側機と車載器間、車載器間での通信部分である。これらの通信は同報通信(ブロードキャスト)である。また、路側機に関連して、歩行者や二輪車を検知する路側センサ、信号機等は対象外である。さらに、前章で述べたように安全運転支援を対象としているので、路車間での決済情報の通信は対象外である。

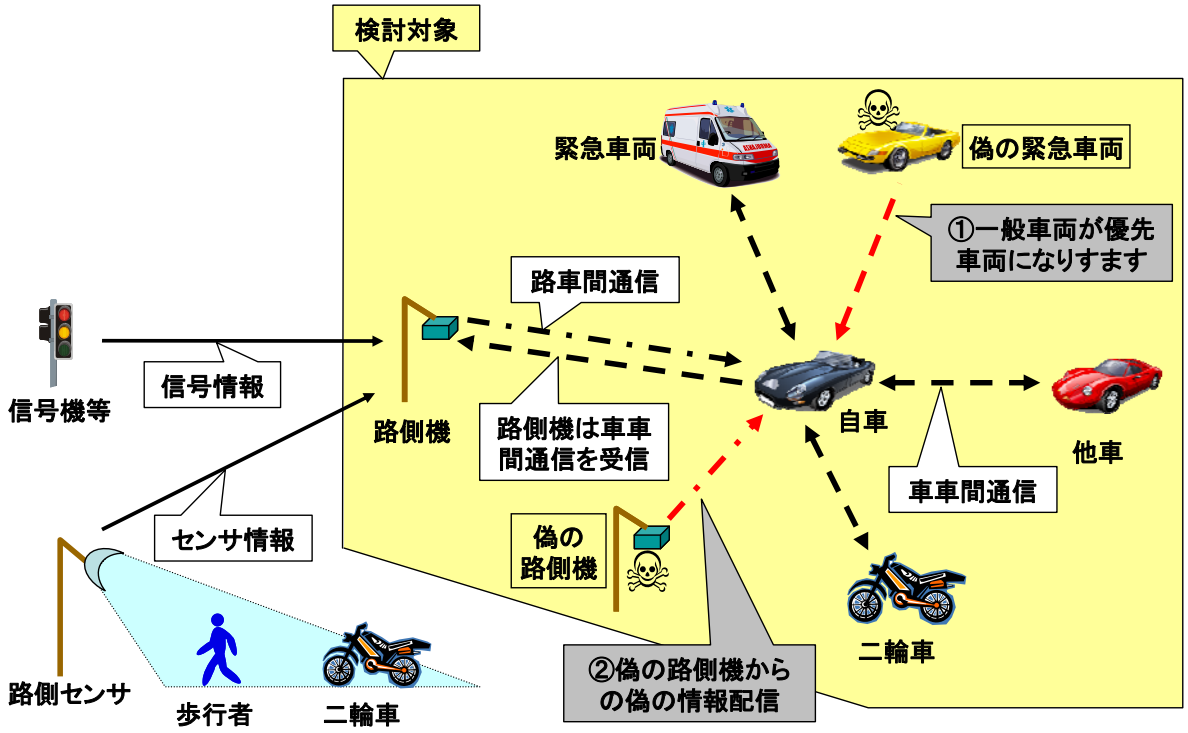


図 4-2 分析対象

図中に示すように、上記のシステムでは

1. 一般車両が偽の優先車両の情報を配信し、優先車両になりすます
2. 偽の路側機から偽の情報を配信する(e.g. 先行車と後続車に矛盾する情報を送信)

などの脅威が存在する。これらによって、目視確認できない優先車両の存在や受信した虚偽のメッセージによって混乱が発生し、その混乱による事故が発生すると考えられる。従って、路車間通信や車車間通信による運転支援通信システムにおいて通信時のセキュリティは必要である。

4.2 システムにおける情報資産

表 4-1 に車車間・路車間通信における情報資産を通信ケースと共に示す。

路側機が直接車載器に配信する情報は路情報(直)であり、路側機の送信時間割当等を示す通信管理情報と、信号情報や道路情報などを示す路側機情報からなる。

車載器が路側機や他の車載器に配信する情報には、走行情報、汎用情報と、路側機から受信した路情報(間)がある。走行情報は自車の位置や速度、種別、緊急車両の場合にはその走行状態等、走行に関わる情報であり、汎用情報は車両毎に自由に利用できる領域の情報である。路情報(間)は、路情報(直)の一部である通信管理情報であり、路側機から受信した車載器がその内容を変更して他の車載器へ転送する。

表 4-1 通信ケースと通信情報

ケース	通信ケースと通信情報	備考
①	路側機 → 自車 路側機 → 他車 路情報(直)	—
②	自車 → 路側機 他車 → 路側機 走行情報	車車間通信での情報を路側機が受信
③	路側機 → 自車 → 他車 路側機 → 他車 → 自車 路情報(直)　路情報(間)	路側機が送信した情報を中継
④	自車 → 他車 走行情報 汎用情報	—
⑤	他車 → 自車 走行情報 汎用情報	—

4.3 脅威分析

まず、路車間通信や車車間通信のシステムにおいて考えられる脅威をリストアップするために、公開されている論文を調査した。調査対象は参考文献[2]～[6]である。その調査結果をまとめたものを表 4-2 に示す。

表 4-2 考えられる脅威一覧

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

前章で述べたシステムにおいて、4.2 節で述べた情報資産と関連する上記脅威を分析した。その結果を表 4-3 に示す。表 4-2 で示した脅威において、他の脅威と関連しているものもある(e.g. リプレイ攻撃によってなりすます)ため、表 4-3 に示すようにまとめた。

なお、表中、脅威の()内の数字は表 4-2 中の ID を示す。

表 4-3 脅威分析

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(悪意の有無に関係なく)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(悪意の有無に関係なく)保守員による車載器入力情報の改ざんや(悪意の有無に関係なく)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、(悪意の有無に関係なく)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。

情報資産	脅威		内容
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。

表 4-2 に記載されている脅威で表 4-3 に記載されていない対象外の脅威は以下の脅威である。

- スパム(5) ： 本脅威は車車間・路車間通信にて広告を配信するサービス適用時に想定されるものであり、広告サービスは想定外であるため。

- ブラックホール(14) ： 路情報(間)を転送しない本脅威は、転送しない攻撃者のみが本攻撃の影響を受けるため。

4.4　リスク分析

表 4-3 に分析された脅威について、リスク分析を行った。

4.4.1　リスク分析手法

リスク分析手法は参考文献[2]の論文記載の手法を適用した。

本手法は、ETSI(European Telecommunications Standard Institute、欧州電気通信標準化協会)の手法を改良したものである。以下にその手法について説明する。

リスク値は、発生可能性の値と影響の値との積で表される。発生可能性と影響の定義について表 4-4 に示す。この手法が ETSI の手法である。

表 4-4 発生可能性と影響の定義

項目	ランク	値	定義
発生可能性	Likely	3	すべての要素が存在する
	Possible	2	いくつかの要素が存在する
	Unlikely	1	重要な要素が抜けている
影響	High	3	利用者やサービスに深刻な影響を与える
	Medium	2	短期間のサービス停止に陥る
	Low	1	利用者やサービスに影響を与える

参考文献[2]では、参考文献[7]にて定義された発生可能性を動機と技術的困難さに詳細化して評価する手法を採用している。動機と技術的困難さの定義を以下に示す。

表 4-5 動機と技術的困難さの定義

項目	ランク	定義
動機	High	攻撃する人や組織にとって多くの利益(報酬等)がある
	Moderate	サービスの混乱(愉快犯等)
	Low	あまり利益は得られない
技術的困難さ	None	技術的、経済的に容易に攻撃が可能（前例あり）
	Solvable	理論的には攻撃が可能
	Strong	理論的、技術的、経済的にも攻撃が大変困難

上記二つをまとめ、リスク値との関係を以下に示す。リスク値は以下の定義である。

リスク値　(9,6)　→ Critical：　対策は必須
(4)　→ Major：　要注意
(3,2,1)　→ Minor：　早急な対策は不要

表 4-6 リスク値の定義

<table>
<tr><th rowspan="2">動機</th><th rowspan="2">技術的
困難さ</th><th rowspan="2">発生可能性</th><th colspan="3">影響</th></tr>
<tr><th>High(3)</th><th>Medium(2)</th><th>Low(1)</th></tr>
<tr><td rowspan="2">High</td><td>None</td><td rowspan="3">Likely(3)</td><td colspan="2" rowspan="4">Critical(9,6)</td><td rowspan="4"></td></tr>
<tr><td>Solvable</td></tr>
<tr><td rowspan="2">Moderate</td><td>None</td></tr>
<tr><td>Solvable</td><td>Possible(2)</td><td>Major(4)</td></tr>
<tr><td>Low</td><td>Any</td><td>Unlikely(1)</td><td colspan="3" rowspan="2">Minor(3,2,1)</td></tr>
<tr><td>Any</td><td>Strong</td></tr>
</table>

4.4.2　リスク分析結果

上記手法に従って、4.3 節に述べた脅威に対してリスク分析を実施し、リスク値を求めた。その結果を表 4-8 に示す。

なお、表中の ID は本表にて新たに振りなおした識別子であり、以降に示す根拠と対応している。また、表中では表 4-7 に示す略語を用いた。

表 4-7 以降の表で使用する略語

項目	名称	表で使用する名称
動機	High	High
	Moderate	Mod.
	Low	Low
技術的困難さ	None	None
	Solvable	Sol.
	Strong	Str.
発生可能性	Likely	Like.
	Possible	Poss.
	Unlikely	Unl.

項目	名称	表で使用する名称
影響	High	High
	Medium	Med.
	Low	Low
リスク値	Critical	Crt.
	Major	Maj.
	Minor	Min.

本分析では、攻撃手法や攻撃の主体が異なる脅威は区別して記載し、保守員は不正行為を行わないとした(動機を Low とした)。

実用化にあたっては、このリスク分析結果については、運用管理機関及びサービス主体によって見直しが必要である。

表 4-8 リスク分析結果

ID	脅威	内容	動機	技術的困難さ	発生可能性	影響度	リスク値
A	DoS	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。	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)
B	Jamming	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。	Mod.	None	Like. (3)	Med. (2)	Crt. (6)
C	偽 GPS 信号	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。	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)
D	マルウェア(1)	第三者や利用者による通信メッセージの悪用、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。	Mod.	Sol.	Poss. (2)	High (3)	Crt. (6)

ID	脅威	内容	動機	技術的困難さ	発生可能性	影響度	リスク値
E	マルウェア(2)	保守員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。	Low	Sol.	Unl. (1)	High (3)	Min. (3)
F	装置外情報の改ざん(1)	利用者による車載器入力情報の改ざん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。	Mod.	Sol.	Poss. (2)	High (3)	Crt. (6)
G	装置外情報の改ざん(2)	保守員による車載器入力情報の改ざんや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。	Low	Sol.	Unl. (1)	High (3)	Min. (3)
H	盗聴(1)	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)。	—	Sol.	—	—	— (後述)
I	盗聴(2)	第三者が受信機を用いて、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)。	High	Sol.	Like. (3)	Low (1)	Min. (3)

ID	脅威	内容	動機	技術的困難さ	発生可能性	影響度	リスク値
J	装置改ざん(1)	第三者や利用者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。	Mod.	Sol.	Poss. (2)	High (3)	Crt. (6)
K	装置改ざん(2)	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。	Low	Sol.	Unl. (1)	High (3)	Min. (3)
L	路側機なりすまし偽路情報送信	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。	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)
M	路側機なりすましリプレイ攻撃	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。	Mod.	None	Like. (3)	Med. (2)	Crt. (6)
N	車両なりすまし偽走行情報送信	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。	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)

ID	脅威	内容	動機	技術的困難さ	発生可能性	影響度	リスク値
O	車両 なりすまし 偽汎用情報送信	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。	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)
P	車両 なりすまし リプレイ攻撃	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。	Mod.	None	Like. (3)	Med. (2)	Crt. (6)
Q	ロケーショントラッキング(1)	第三者による受信機の利用、利用者による車載器の悪用によって、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)。	High	Sol.	Like. (3)	Low (1)	Min. (3)
R	ロケーショントラッキング(2)	第三者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)。	High	Str.	Unl. (1)	Low (1)	Min. (1)
S	ロケーショントラッキング(3)	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)。	Low	Str.	Unl. (1)	Low (1)	Min. (1)
T	中継車両による改ざん	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。	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)

ID	脅威	内容	動機	技術的困難さ	発生可能性	影響度	リスク値
U	偽路情報(間)送信	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。	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)

表 4-8 に示したリスク分析結果の根拠について表 4-9 に示す。

表 4-9 リスク分析の根拠

ID	脅威	項目	ランク	根拠
A	DoS	動機	Moderate	混乱目的
		困難さ	Solvable	有線システムでは攻撃の前例が有り、無線システムでは理論的に攻撃が可能
		影響度	Medium	攻撃を受けた場所での限定的な影響
B	Jamming	動機	Moderate	混乱目的
		困難さ	None	攻撃の前例あり
		影響度	Medium	攻撃を受けた場所での限定的な影響
C	偽 GPS 信号	動機	Moderate	混乱目的
		困難さ	Solvable	理論的には攻撃が可能
		影響度	Medium	攻撃を受けた場所での限定的な影響
D	マルウェア(1)	動機	Moderate	混乱目的
		困難さ	Solvable	理論的には攻撃が可能
		影響度	High	システム全体に広がる可能性があり、駆除する必要あり
E	マルウェア(2)	動機	Low	保守員の動機はなし
		困難さ	Solvable	理論的には攻撃が可能
		影響度	High	システム全体に広がる可能性があり、駆除する必要あり
F	装置外情報の改ざん(1)	動機	Moderate	混乱目的
		困難さ	Solvable	理論的には攻撃が可能
		影響度	High	改ざん後の修正が必要
G	装置外情報の改ざん(2)	動機	Low	保守員の動機はなし
		困難さ	Solvable	理論的には攻撃が可能
		影響度	High	改ざん後の修正が必要
H	盗聴(1)	動機	—	汎用情報の内容が不明のため判断不可能(後述)
		困難さ	Solvable	理論的には攻撃が可能
		影響度	—	汎用情報の内容が不明のため判断不可能(後述)

ID	脅威	項目	ランク	根拠
I	盗聴(2)	動機	High	不正車載器の販売による収益目的
		困難さ	Solvable	理論的には攻撃が可能
		影響度	Low	正当な利用者やサービスには影響はない 本脅威が脅威になるか否かは運用管理機関の方針に依存
J	装置改ざん(1)	動機	Moderate	混乱目的
		困難さ	Solvable	理論的には攻撃が可能
		影響度	High	改ざん後の改修が必要
K	装置改ざん(2)	動機	Low	保守員の動機はなし
		困難さ	Solvable	理論的には攻撃が可能
		影響度	High	改ざん後の改修が必要
L	路側機なりすまし 偽路情報送信	動機	Moderate	混乱目的
		困難さ	Solvable	理論的には攻撃が可能
		影響度	Medium	送信された場所での限定的な影響
M	路側機なりすまし リプレイ攻撃	動機	Moderate	混乱目的
		困難さ	None	攻撃の前例あり
		影響度	Medium	攻撃を受けた場所での限定的な影響
N	車両なりすまし 偽走行情報送信	動機	Moderate	混乱目的
		困難さ	Solvable	理論的には攻撃が可能
		影響度	Medium	送信された場所での限定的な影響
O	車両なりすまし 偽汎用情報送信	動機	Moderate	混乱目的
		困難さ	Solvable	理論的には攻撃が可能
		影響度	Medium	送信された場所での限定的な影響
P	車両なりすまし リプレイ攻撃	動機	Moderate	混乱目的
		困難さ	None	攻撃の前例あり
		影響度	Medium	攻撃を受けた場所での限定的な影響
Q	ロケーショントラッキング(1)	動機	High	特定個人のプロファイリング目的と明確な目的があり、利益は大
		困難さ	Solvable	理論的には攻撃が可能
		影響度	Low	特定個人への影響であり、通信距離内での追跡が必要でストーキングと同じ(後述)

ID	脅威	項目	ランク	根拠
R	ロケーショントラッキング(2)	動機	High	特定個人のプロファイリング目的と明確な目的があり、利益は大
		困難さ	Strong	複数の路側機の悪用が必要なため、攻撃は困難(後述)
		影響度	Low	特定個人への影響
S	ロケーショントラッキング(3)	動機	Low	保守員の動機はなし
		困難さ	Strong	複数の路側機の悪用が必要なため、攻撃は困難(後述)
		影響度	Low	特定個人への影響
T	中継車両による改ざん	動機	Moderate	混乱目的
		困難さ	Solvable	理論的には攻撃が可能
		影響度	Medium	攻撃を受けた場所での限定的な影響(後述)
U	偽路情報(間)送信	動機	Moderate	混乱目的
		困難さ	Solvable	理論的には攻撃が可能
		影響度	Medium	攻撃を受けた場所での限定的な影響(後述)

以下に、車載器がブロードキャストする汎用情報の盗聴(H)、走行情報や汎用情報に対するロケーショントラッキング(Q と R)、車載器か路側機からの情報を中継して他の車載器に転送する路情報(間)に対する中継車両が改ざん(T)、偽路情報(間)送信(U)について、表 4-9 に示した根拠を補足する。

- 汎用情報の盗聴

現在、汎用情報の用途や含まれる内容が不明であるため、攻撃をする人や組織の動機やその影響

度が判断つかない。従って、今後、汎用情報の用途等が決定した場合、適応されるサービスの性質に沿ったセキュリティ対策の検討が必要である。

● ロケーショントラッキング

図 4-3 において、ロケーショントラッキングは車両 A が地点 X→Y→Z に行った事実の暴露やその事実から個人像をプロファイリングする脅威を言う。車両 A は、本システムに対応している車載器を搭載し、一意に識別可能な情報(e.g. 車載器 ID、MAC アドレス等)と位置情報等をブロードキャストして走行している。このような状態で以下の理由からロケーショントラッキングの影響を Low とした。

A. 車載器や通信機の悪用

ブロードキャストメッセージから①車両Aの特定②位置のトラッキングが可能である。しかし、継続的なトラッキングのためには、トラッキングを行う車両は A の通信範囲内に存在する必要があり、これはストーキング(尾行)と同じである。

B. 路側機の悪用

路側機 D で車両の特定が可能である。しかし、路側の通信範囲内にいる車両のみが対象となるので、ロケーショントラッキングは不可能である。また、複数の路側機を悪用するロケーショントラッキングが考えられるが、この場合でも行先不明の特定個人をトラッキングするためにはすべての路側機を使用する必要があり、非常に困難と思われる(路側サーバに不正侵入して情報を得たほうが効率的である)。

C. 路側サーバの悪用

本分析の対象外であるが、路側機が受信した全メッセージを収集する路側サーバがある場合、路側サーバへの不正侵入や悪意のあるサーバ操作者によって①車両Aの特定②位置の割り出しにより、トラッキングが可能となる。従って、車両⇔車載器 ID⇔位置の紐付けを困難にする管理方法や、車両⇔ID と ID⇔位置の操作役割の分割、不正侵入対策などの対策が必要である。

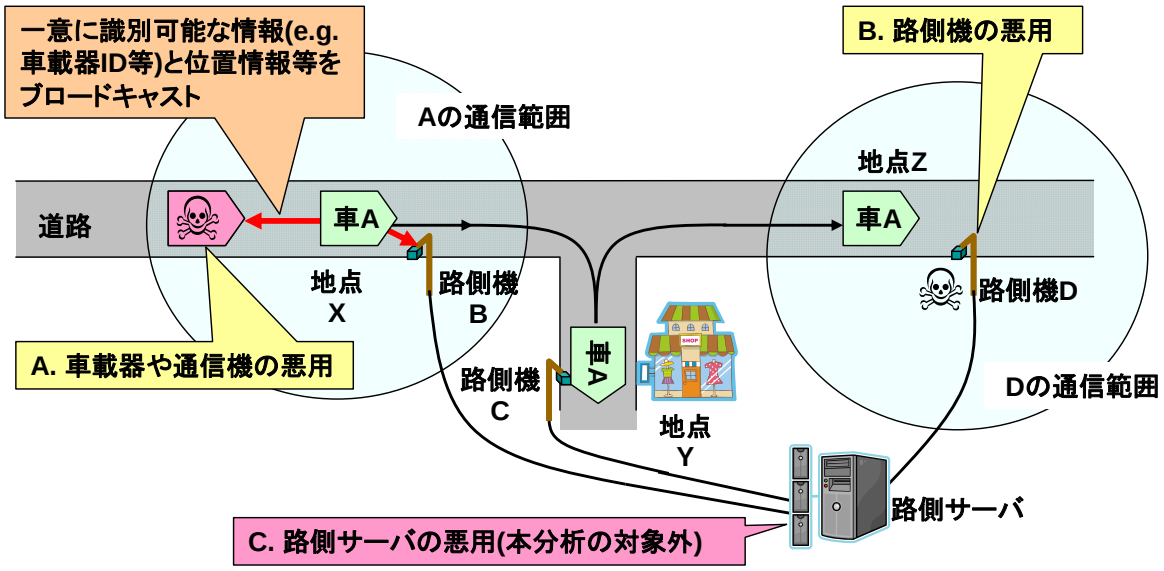


図 4-3 ロケーショントラッキング

● 中継車両による改ざんや偽路情報(間)送信

これらは、路側機からの路情報(直)を受信した車両が他の車両に路情報(間)を転送する際の路情報(間)の改ざんや、路情報(直)を受信していないのに(i.e. 路側機が存在しない)に偽の路情報(間)を送信する脅威である。路情報(間)は、路側機の送信時間割り当て等の通信管理に関わる情報であり、路側機から直接受信できない車載器はこの情報を受信することで近辺の路側機の存在を知ることができる。このような中継車両によって路情報(間)が改ざんされた場合、以下のような限定的な影響が想定されるため、影響度を「Medium」とした。

1) 路側機の送信期間が長いのに、短いと偽られると、改ざんされた情報を受信した車両は、差分の期間に車車間通信をしてしまい、路側機の通信範囲内かつ、改ざんされた情報を受信した車両の通信範囲内の車両が通信不能になる。

2) 路側機の送信期間が短いもしくは存在しないのに、長いと偽られると、改ざんされた情報を受信した車両は差分の期間に走行情報や汎用情報を配信せず、車車間通信しない場合がある。

4.5 結論

表 4-8 に示した脅威と、その脅威に対抗する通信、装置、運用の観点から対策方針を表 4-10 に示す。ただし、表 4-8 に示したリスク値が Critical もしくは Major の脅威について表し、Minor の脅威は対象外とした。また、汎用情報の盗聴に関する脅威も上述した理由により、対象外とした。ただし、盗聴(2)の脅威に対しては後述する理由により対策を示した。

表 4-10 対策が必要な脅威とそのセキュリティ対策

ID	脅威	リスク値	対策方針			備考
			通信	装置	運用	
A	DoS	Major(4)	—	車載器の耐タンパ性	法律等による規制	—
B	Jamming	Critical(6)	—	—	法律等による規制	—
C	偽 GPS 信号	Major(4)	—	—	法律等による規制	—
D	マルウェア(1)	Critical(6)	—	規定外データの受信拒否(実装レベル) 路側機や車載器の耐タンパ性	—	—
E	マルウェア(2)	Minor(3)	—	—	—	—
F	装置外情報の改ざん(1)	Critical(6)	—	路側機の耐タンパ性	車両点検	後述
G	装置外情報の改ざん(2)	Minor(3)	—	—	—	—
H	盗聴(1)	—	—	—	—	—
I	盗聴(2)	Minor(3)	メッセージの機密性維持	—	認定制度	後述
J	装置改ざん(1)	Critical(6)	—	車載器や路側機の耐タンパ性	—	—
K	装置改ざん(2)	Minor(3)	—	—	—	—
L	路側機なりすまし 偽路情報送信	Major(4)	発信元の真正性確認 メッセージの完全性確認	車載器の耐タンパ性	—	—

ID	脅威	リスク値	対策方針			備考
			通信	装置	運用	
M	路側機なりすまし リプレイ攻撃	Critical(6)	発信元の真正性確認	—	—	後述
N	車両なりすまし 偽走行情報送信	Major(4)	発信元の真正性確認 メッセージの完全性確認	車載器の耐タンパ性	—	—
O	車両なりすまし 偽汎用情報送信	Major(4)	発信元の真正性確認 メッセージの完全性確認	車載器の耐タンパ性	—	—
P	車両なりすまし リプレイ攻撃	Critical(6)	発信元の真正性確認	—	—	後述
Q	ロケーション トラッキング(1)	Minor(3)	—	—	—	—
R	ロケーション トラッキング(2)	Minor(1)	—	—	—	—
S	ロケーション トラッキング(3)	Minor(1)	—	—	—	—
T	中継車両による 改ざん	Major(4)	受信データの整合性検証	—	路車間通信時間比率の規定	後述
U	偽路情報(間) 送信	Major(4)	受信データの整合性検証	—	路車間通信時間比率の規定	後述

以下、表 4-10 の備考欄に後述と示した脅威について補足する。

- 装置外情報の改ざん(1)について

車両から車載器へ入力される速度等の情報が改ざんされた場合、通信や装置でのセキュリティでは対抗できない。従って、改ざんされた情報を含むメッセージを配信する車載器を、真正性の確認によって一意に特定できる仕組みが必要である。

- 盗聴(2)について

他サービスへの適用性や運用管理機関の方針に依存するため、システムとして機密性の維持も対応可能にする必要がある。

- リプレイ攻撃について

具体的には、メッセージの送信時刻の検証等の対策になるが、これは発信元の真正性確認に含まれているとしている。

- 中継車両による改ざんや偽路情報(間)送信について

通信での対策は、受信データと通信規格の整合性を検証し、規格に反する受信データは棄却することである。また、車車間通信の妨害を防ぐため、運用において、路車間通信時間の割合(最大値)を規定することが望ましい(Annex C参照)。なお、通信での上記対策は、通信仕様に関わる対策であるため、これ以降、本書では対象外とする。

以上の脅威及びリスク分析結果より、通信で対策が必要な脅威はなりすましや偽情報の送信、リプレイ攻撃であり、その対策はメッセージの機密性維持、発信元の真正性確認、メッセージの完全性確認である。

［余白］

第5章　セキュリティに対する対策方針

前章で示した脅威に対抗するための対策方針を以下に示す。

1．　車車間・路車間通信において、暗号技術を用いて発信元の真正性確認やメッセージの完全性確認を行う。また、通信区間を流れる情報の機密性の確保も可能とする。なお、暗号アルゴリズムに関しては、CRYPTREC の電子政府推奨暗号リストから選択する。

2．　上記真正性確認、完全性確認や機密性確保に用いられる鍵情報が漏洩した場合に被害の拡大を最小限に留めるように対策を図る。

3．　車車間・路車間通信区間以外に流れる情報や機器に蓄積される情報は、当該区間の回線や機器を管理する主体が適切な保護を行う。

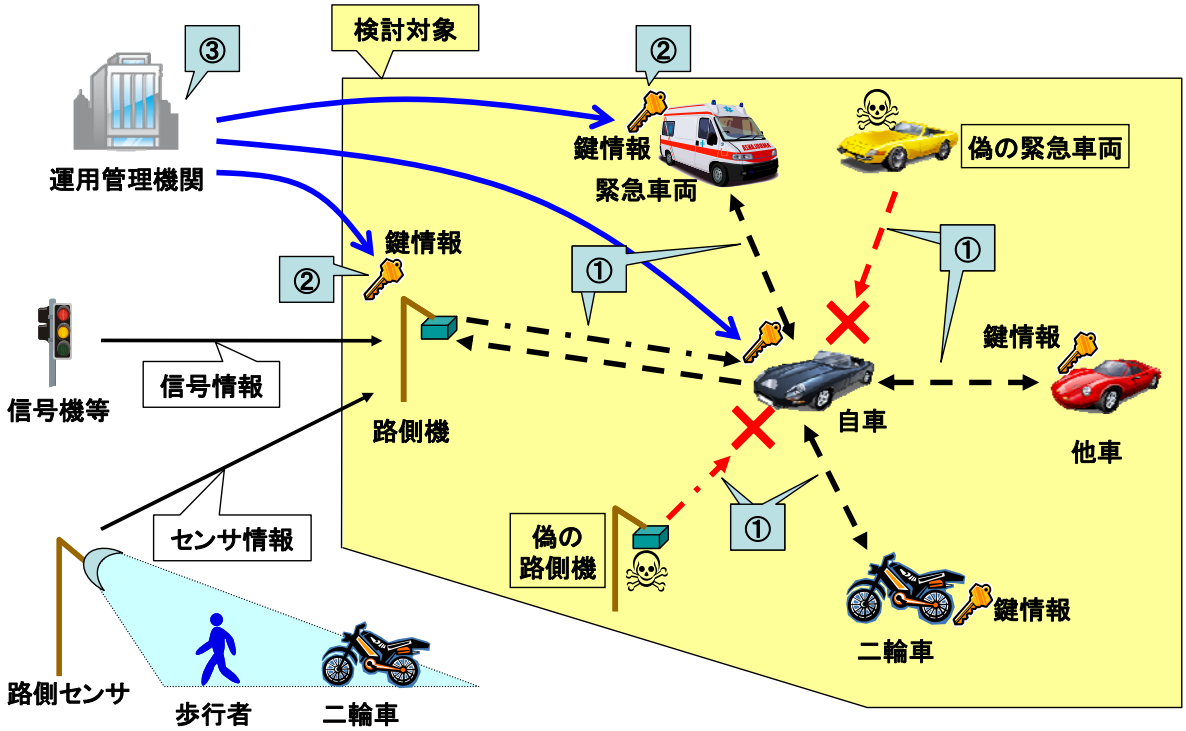


図 5-1 セキュリティに対する対策方針

［余白］

第6章　セキュリティ対策

車車間・路車間通信におけるセキュリティ対策、車載器や路側機などの通信機器のセキュリティ対策、インフラ側システムを含めた運用でのセキュリティ対策について述べる。

6.1　車車間・路車間通信におけるセキュリティ対策

暗号技術を用いた発信元の真正性やメッセージの完全性を確認する方式と通信情報の機密性を維持する方式について述べる。

6.1.1　真正性や完全性を確認する方式について

真正性や完全性を確認する方式としては、公開鍵アルゴリズムによる電子署名を適用した方式(以下、電子署名方式)と共通鍵アルゴリズムによるメッセージ認証コード(Massage Authentication Code、以下 MAC)を適用した方式(以下、MAC 方式)がある。以下、これらについて説明する。

6.1.1.1　電子署名方式

車車間・路車間通信のセキュリティ規格として、米国で検討されている IEEE1609.2 がある(参考文献[8])。国際協調の観点では、IEEE1609.2 を本運転支援通信システムのセキュリティに適用することが望ましい。IEEE1609.2 で定義されている Signed Message は公開鍵アルゴリズムによる電子署名を適用した方式である。4.5 節で述べた通信時のセキュリティ対策である発信元の真正性確認やメッセージの完全性確認は、IEEE1609.2 によってカバーされている。以下、本方式をベースに説明する。

(1) 概要

本方式では、受信側において、メッセージに対する電子署名の検証と送信元公開鍵証明書の検証によって真正性と完全性の確認が実現される。図 6-1 に本方式の概要を示す。

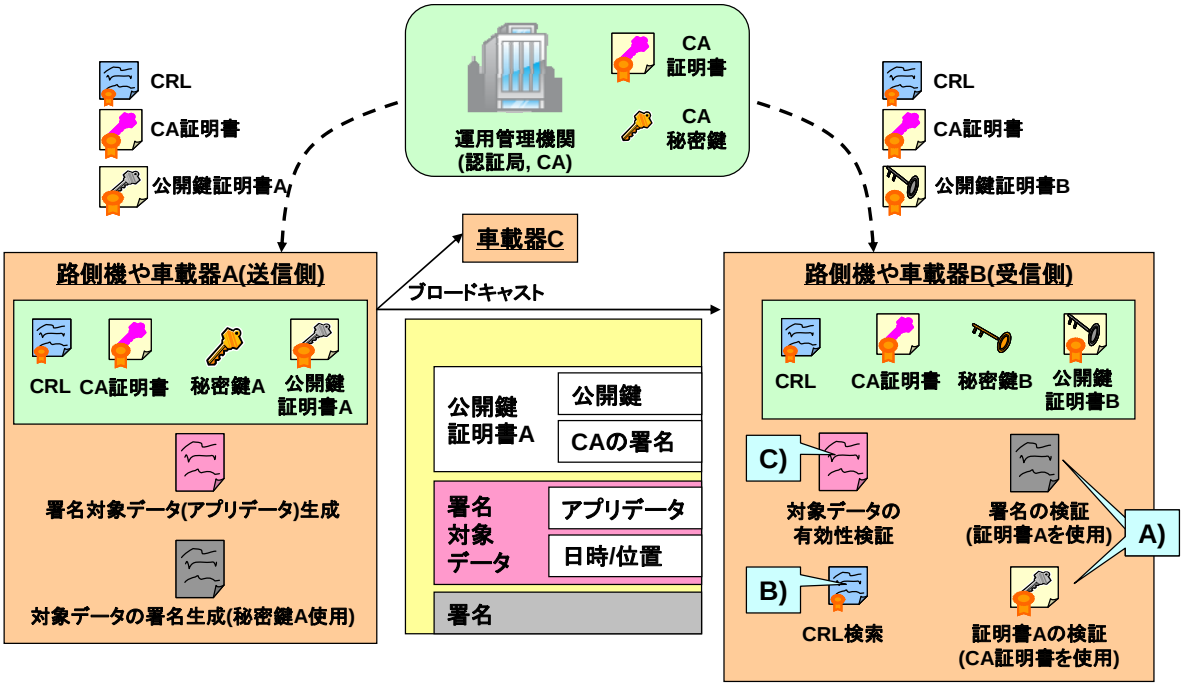


図 6-1 電子署名方式の概要

本方式は PKI(公開鍵暗号基盤)を適用した方式である。車載器や路側機は、通信で使用する固有の秘密鍵と公開鍵証明書を持ち、送信側と受信側で異なる鍵(秘密鍵と公開鍵)を使用する。公開鍵証明書は、その秘密鍵と対となる公開鍵の所有者を証明する証明書として、信頼できる第三者機関である認証局(CA, Certification Authority)によって電子署名を付与されたもので、保有している機器を一意に特定できる。本システムの場合、CA は運用管理機関のセキュリティ情報管理がその役割を担うプライベート CA を想定しているが、別途信頼できる第三者機関による CA でもよい。また、CA は階層構造になる場合も考えられる。その場合は、複数の CA 証明書が存在し、機器にも複数の CA 証明書を設定する必要がある。

送信側はブロードキャストするアプリケーションデータ(車載器の場合走行情報や汎用情報、路側機の場合路情報)や必要な情報に対して自身の秘密鍵で電子署名を生成する。そして、アプリケーションデータ、生成したその署名と公開鍵証明書等をブロードキャストする。

受信側では、受信したメッセージから以下の処理を行う。

A) メッセージの真正性・完全性検証

公開鍵証明書の検証(CA 証明書(内の CA 公開鍵)を用いて公開鍵証明書内の CA の署名を検証)と、アプリケーションデータに対する電子署名の検証(公開鍵証明書(内の公開鍵)を用いてアプリケーションデータの署名を検証)を行う。これにより、受信したアプリケーションデータの送信元が正当な公開鍵証明書を持つこと、アプリケーションデータが改ざんされていなこと、

そのアプリケーションデータの送信元が公開鍵証明書の保有者であることを確認することができる。

B) ネガリスト検索

受信した公開鍵証明書が、ネガリストである証明書失効リスト(CRL、Certification Revocation List)に掲載されていないことを確認する。IEEE1609.2 では、公開鍵証明書のダイジェスト(証明書のハッシュ値)がリストに掲載されている。これにより、(秘密鍵漏洩等により)失効した公開鍵証明書でなく、有効な証明書であることを確認できる。CRL には CA の電子署名が付与されており、CA 証明書を用いて CRL が改ざんされていないこと、CRL の発行元が CA であることを確認することができる。

また、ネガリスト検索の方法として、CRL 配布による証明書の失効確認ではなく、OCSP（Online Certificate Status Protocol）による証明書の失効確認という方法も考えられる。OCSP が効果的な場合は、CRL のサイズが大きくなりネットワーク帯域や機器のメモリの不足が予想される、かつ機器が認証局と常時通信できる場合である。例えば、路側機は認証局と常時接続されている、かつ路側機は車載器の証明書の失効確認をおこなう必要があるが、全国の失効車の数が多い場合、車載器の証明書のシリアル番号を認証局に送付し、認証局からは確認結果のみを取得するという OCSP を採用することで路側機に必要なメモリを抑えることができる。

C) メッセージの有効性検証

メッセージに含まれている日時や位置の情報を検証する。これにより、アプリケーションデータの新しさ(配信済みデータの再送検出)や地理的有効範囲を確認する。

(2) セキュリティ情報の格納

車載器や路側機には事前に固有の秘密鍵と公開鍵証明書を格納しておく必要がある。公開鍵証明書は CA の電子署名が必要であり、この署名生成には CA の秘密鍵が用いられる。また、秘密鍵は機密性維持が必要である。これらの事前の格納方式には以下の二つの方式が考えられる。

1. 各機器(車載器や路側機)にて、公開鍵ペア(秘密鍵と公開鍵)を生成し、公開鍵を CA に送付する。CA にて公開鍵証明書を生成し、各機器に公開鍵証明書を格納する。
2. CA にて、公開鍵ペアを生成し、その公開鍵から公開鍵証明書を生成する。秘密鍵と公開鍵証明書を各機器に格納する。

機密性の観点では、1.の場合、秘密鍵は各機器の外部に出ることはないが、2.の場合は CA で生成された秘密鍵を各機器に格納するため、格納時の機密性を維持する必要がある。一方、1.の場合、各機器には公開鍵ペアを生成する機能が必要となるが、2.の場合は CA に公開鍵ペア生成機能があればよい。また、上記方式に関わらず、秘密鍵・公開鍵証明書と機器との紐付けが必要である。

各機器固有の公開鍵ペアの他に、各機器には CA 証明書と CRL を格納する必要がある。これらの機密性維持は不要であるが、完全性維持が必要である。CA 証明書や CRL は CA 証明書内の CA 公開鍵による署名検証によって完全性を確認できる。

以上のように、CA 証明書は、他の情報を検証する際に用いられる情報である。上述のように改ざんは検出できるが、他の偽 CA 証明書へのすり替えは検出できないため、運用前に各機器に正しく格納する手段が必要である。

(3) セキュリティ情報の更新

本方式で必要な更新は、各機器の秘密鍵や公開鍵証明書の更新、各機器に格納する CA 証明書の更新、CRL の更新である。

各機器の秘密鍵や公開鍵証明書の更新は、上記の事前格納と同様の方式が考えられ、機器への格納は、ディーラー等における更新、路側機利用による更新が考えられる。更新時には、正当な機器の更新申請であることの確認、機器と CA 間の通信路での改ざんや漏洩(秘密鍵を含む場合)対策、更新情報(新しい証明書など)と対応する機器との紐付けが必要である。

各機器に格納する CA 証明書の更新は、機密性は不要である。また、完全性も上述の通り確認できる。正当な CA から発行された CA 証明書であることを各機器が確認できなければならない。

CRL の更新は、上述のように改ざん検知や CA から発行された正当なリストであることは、CA 証明書を利用して各機器が確認できる。ただし、更新されたリストを早く各機器に配布する必要がある。

(4) 通信フォーマット例

IEEE1609.2 での通信フォーマット例を以下に示す。セキュリティに関係するデータ(セキュリティデータ)の長さ(アプリケーションデータを除く)は 196B である。

なお、IEEE1609.2 では様々なオプションがあるが、以下に示したフォーマットはデータ長を最短にした場合のものである。図中、()は長さを示し、B はバイトである。電子署名の対象範囲は、アプリケーションデータ及び日時情報等のセキュリティデータとする。

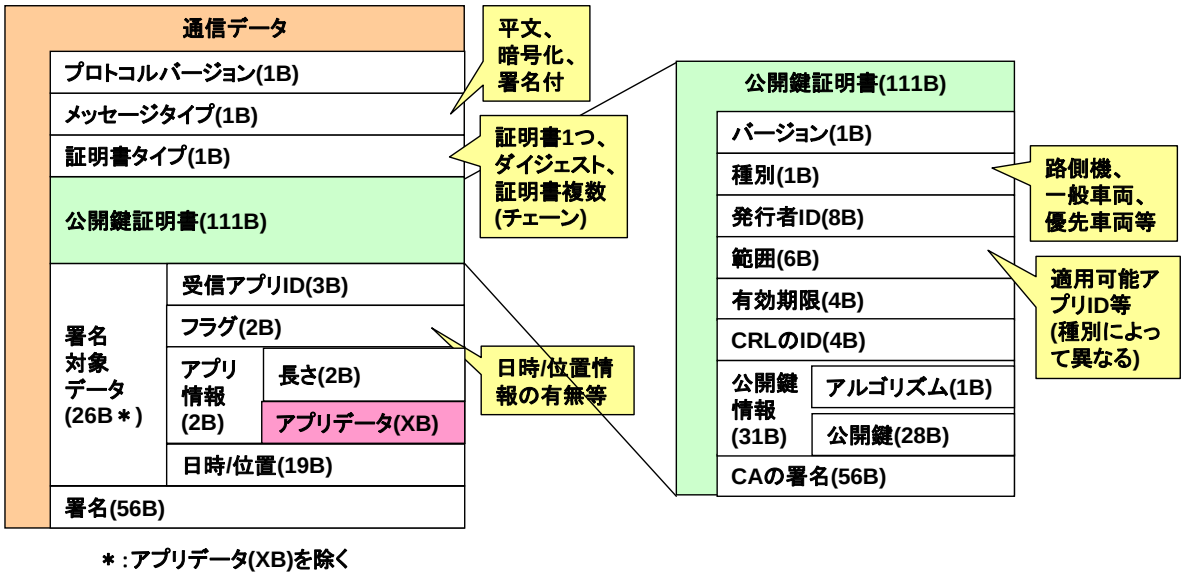


図 6-2 電子署名方式での通信フォーマット(IEEE1609.2)

電子署名方式で使用する情報を以下にまとめる。機密性と完全性の欄は○が必要、×が不要を意味する。

表 6-1 電子署名方式で使用する情報

情報	発行元	格納先	使用時	機密性	完全性	備考
CA の秘密鍵	CA	CA	・証明書発行 ・CRL 発行	○	○	本鍵が漏洩した場合、全システムが危殆化
CA の公開鍵証明書	CA	(CA) 各機器	・他の機器から受信した公開鍵証明書の検証 ・受信した CRL の検証	×	○	CA の公開鍵に CA の秘密鍵で署名したもの
各機器の秘密鍵	①各機器 ②CA	各機器	送信メッセージの署名生成	○	○	本鍵が漏洩した場合、対象の機器が危殆化
各機器の公開鍵証明書	CA	(CA) 各機器	他の機器から受信したメッセージの署名検証	×	○	・各機器の公開鍵に CA の秘密鍵で署名したもの ・①の場合、各機器で生成された公開鍵から CA にて証明書発行

情報	発行元	格納先	使用時	機密性	完全性	備考
CRL	CA	(CA) 各機器	他の機器からメッセージ受信	×	○	有効期限内で失効した証明書ダイジェスト(証明書のハッシュ値下位 10 バイト)のリストに CA の秘密鍵で署名したもの

6.1.1.2　MAC方式

共通鍵アルゴリズムは公開鍵アルゴリズムに比べて処理負荷が低いため、ある同一時間内での処理を考えると、処理能力のより低い機器で実現できる。しかし、共通鍵アルゴリズムは送信側と受信側で共通の鍵を使用しなくてはならず、そのため、不特定多数の機器が通信する場合、システム 1 つの鍵で通信せざるを得ない(Annex A参照)。従って、システム 1 つの鍵が漏洩した場合にはすべての機器での鍵更新が必要となる。また、鍵による機器の特定はできず、特定は機器IDによるものとなる。そのため、他の機器へのなりすましに対抗するためには、機器内部に格納されている機器IDが改ざんされないという前提条件が必要となる。

(1) 概要

共通鍵アルゴリズムの場合、暗号化と MAC が考えられるが、前者は主に機密性、後者は完全性や真正性を対象としている。今回、必要な対策が真正性や完全性であるので、MAC が適している。

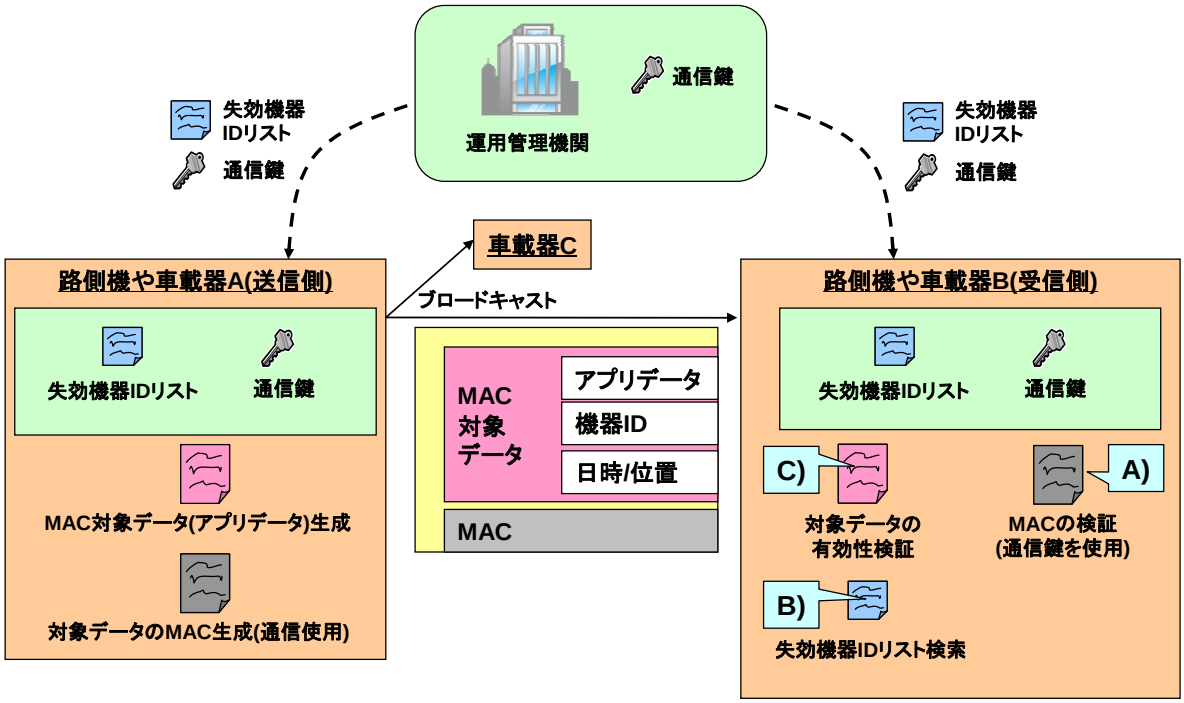


図 6-3 MAC方式の概要

本方式での車載器や路側機は、通信で使用する共通の通信鍵を持つ。通信鍵は、送信側と受信側で同じ鍵を用いる。

送信側はブロードキャストするアプリケーションデータ(車載器の場合走行情報や汎用情報、路側機の場合路情報)や機器 ID 等必要な情報に対して通信鍵で MAC を生成する。そして、アプリケーションデータ、生成した MAC や機器 ID 等をブロードキャストする。

受信側では、受信したデータから以下の処理を行う。

A) メッセージの真正性・完全性検証

アプリケーションデータに対する MAC の検証(通信鍵を用いてアプリケーションデータの MAC を生成し、受信した MAC との比較検証)を行う。これにより、受信したアプリケーションデータの送信元が正当な通信鍵を持つこと、アプリケーションデータが改ざんされていないことを確認することができる。

B) ネガリスト検索

受信したメッセージ内の機器 ID が、失効した機器 ID のリスト(失効機器 ID リスト)に掲載されていないことを確認する。これにより、送信元が無効な機器でないことを確認できる。

C) メッセージの有効性検証

メッセージに含まれている日時や位置の情報を検証する。これにより、アプリケーションデータの新しさ(配信済みデータの再送検出) や地理的有効範囲を確認する。

(2) セキュリティ情報の格納

車載器や路側機には通信前に通信鍵を格納しておく必要があり、また、通信鍵は機密性維持が必要である。従って、運用管理機関で発行された通信鍵は機密性を維持された状態で各機器に格納されなければならない。本方式の場合、共通の通信鍵を各機器に格納する必要があるため、通信鍵漏洩時はすべての機器の鍵更新が必要となる。

また、通信鍵の他に、各機器には失効機器 ID リストを格納する必要がある。失効機器 ID リストは電子署名方式の CRL に相当するものであり、機密性は不要であるが、運用管理機関が発行した正当なリストであることとそのリストが改ざんされていないという真正性と完全性の維持が必要である。

(3) セキュリティ情報の更新

本方式で必要な更新は、各機器の通信鍵の更新、失効機器 ID リストの更新である。

各機器の通信鍵の更新は、ディーラー等における更新、路側機やテレマティクスの利用による更新が考えられるが、正当な機器であることの確認、機器や運用管理機関間の改ざんや漏洩対策が必要である。

失効機器 ID リストの更新は、上述のように改ざん検知や運用管理機関から発行された正当なリストであることの確認が必要である。

(4) 通信フォーマット例

本方式のフォーマット例を以下に示す。本例でのセキュリティデータ長は 53B となる。ただし、送信元の種別情報(路側機や車載器等を表す情報)を 1 バイト、機器 ID を 6 バイトとしている。図中、()は長さを示し、B はバイトである。MAC の対象範囲は、アプリケーションデータ及び日時情報、機器 ID 等のセキュリティデータとする。

＊:アプリデータ(XB)を除く

図 6-4 MAC 方式の通信フォーマット例

MAC 方式で使用する情報を以下にまとめる。機密性と完全性の欄は○が必要、×が不要を意味する。

表 6-2 MAC 方式で使用する情報

情報	発行元	格納先	使用時	機密性	完全性	備考
通信鍵	運用管理機関	(運用管理機関) 各機器	・送信メッセージの MAC 生成 ・他の機器から受信したメッセージの MAC 検証	○	○	本鍵が漏洩した場合、全システムが危殆化
失効機器 ID リスト	運用管理機関	(運用管理機関) 各機器	他の機器からメッセージ受信	×	○	無効な機器の機器 ID リスト

6.1.1.3　各方式の特徴

以下に電子署名方式と MAC 方式の特徴を比較する。

表 6-3 各方式の特徴(概要)

		電子署名方式	MAC 方式	備考
方式		電子署名	MAC	—
アルゴリズム例(鍵長)		ECDSA(224bit)	AES(128bit)	—
各機器に格納する鍵情報*		・ CA 公開鍵証明書 ・ 各車載器や路側機の秘密鍵 ・ 各車載器や路側機の公開鍵証明書	通信鍵	* 鍵情報をセキュアに格納・更新するための鍵は含めず
通信で使用する鍵		各車載器/路側機固有	すべての車載器/路側機で同一	—
各機器の処理	送信時	署名生成	MAC 生成	—
	受信時	署名検証(2 回*)	MAC 生成・比較	* 検証済み証明書の場合 1 回
機密情報	車載器 路側機	各車載器/路側機の秘密鍵	通信鍵	—
	システム	CA の秘密鍵	通信鍵	—
要更新情報		・ CA の秘密鍵や公開鍵証明書 ・ 各車載器・路側機の秘密鍵や公開鍵証明書 ・ CRL	・ 通信鍵 ・ 失効機器 ID リスト	—
セキュリティデータ長*		196B	53B	* 図 6-2、図 6-4 参照

表 6-4 各方式の特徴(セキュリティ)

		電子署名方式	MAC 方式
通常時	第三者によるなりすまし	第三者は CA 発行の公開鍵証明書がないため、公開鍵証明書の検証で検出可能	第三者は通信鍵を知らないため、MAC 検証で検出可能
	利用者による他機器へのなりすまし	他機器の秘密鍵を知らないため、公開鍵証明書やメッセージの署名検証で検出可能	機器 ID を対象とした MAC 検証で検出可能 (格納された機器 ID が改ざんされていない条件要)
	機器出力データの改ざん	メッセージの署名検証で検出可能	メッセージの MAC 検証で検出可能
	機器内部保持データ(鍵情報や機器 ID、種別情報)の改ざん	公開鍵証明書やメッセージの署名検証で検出可能	検出不可
	外部入力データの改ざん	対抗不可	対抗不可
	機器の特定	公開鍵証明書により特定可能	機器 ID により特定可能 (格納された機器 ID が改ざんされていない条件要)
	リプレイ攻撃	日時や場所情報等の検証により検出可能	日時や場所情報等の検証により検出可能
通信鍵漏洩時	他機器へのなりすまし	漏洩した機器以外へのなりすましは不可(CRL による検出可能)	任意の機器 ID でメッセージが生成できるため、なりすまし可能
	漏洩した機器の特定	公開鍵証明書により特定可能	特定不可
	各機器の機密情報漏洩時の対処	・ 対象機器の秘密鍵や公開鍵証明書を更新 ・ CRL 更新	すべての車載器・路側機の通信鍵を更新
	漏洩の再発性	漏洩した機器を特定できるため、対策可能	漏洩した機器を特定できないため、再発の可能性あり

		電子署名方式	MAC 方式
ネガリスト		公開鍵証明書のダイジェスト(証明書のハッシュ値の一部)のリスト(CRL)	失効した機器 ID のリスト(失効機器 ID リスト)
	改ざん	CA 証明書による署名検証で検出可能	別途改ざん検知の仕組みが必要
	遅延リスク(ネガリストの更新)	更新された CRL を受信するまで失効した公開鍵証明書が利用される可能性あり	更新された失効機器 ID リストを受信するまで無効な機器が利用される可能性あり

表 6-5 各方式の特徴(コスト)

		電子署名方式	MAC 方式	備考
登録工程		中 (オフライン証明書発行)	小 (オフライン通信鍵発行)	—
	作業	・機器毎の公開鍵証明書発行 ・CA 証明書の発行 ・CRL の発行	・同一の通信鍵の発行 ・失効機器 ID リストの発行	—
通常 メンテナンス		大 (オンライン CRL 更新)	大 (オンライン失効機器 ID リスト更新)	—
	作業	・機器毎の鍵ペアと証明書の更新 ・CA 証明書の更新 ・CRL の更新	・通信鍵の更新 ・失効機器 ID リストの更新	—
鍵漏洩時の メンテナンス		小 (対象装置)	大 (すべての車載器・路側機)	—
	作業	■秘密鍵の漏洩 ・漏洩対象の鍵更新 ・CRL 更新	■通信鍵の漏洩 通信鍵の更新	—
各機器の必要な 処理能力や規模		大	小	電子署名方式の公開鍵アルゴリズムは MAC 方式の共通鍵アルゴリズムよりも処理負荷大
機器の耐タンパ 実装	必要性	中 (各機器の秘密鍵の保護)	大 (システム全体の通信鍵の保護)	—
	保護 情報	秘密鍵の機密性	・通信鍵の機密性 ・機器 ID や種別情報の完全性	—

6.1.2　通信情報の機密性を維持する方式について

機密性を維持する方式は、共通鍵アルゴリズムによる暗号化がある。

暗号化には様々なモードがあるが、暗号結果長が変化しない CTR(Counter)モードやストリーム暗号が適していると思われる。また、暗号鍵などが変わらない場合、同一データに対する暗号処理結果は同じになるため、同一の鍵/データを処理しても異なる暗号処理結果になるように nonce(同一の鍵で繰り返し使用されない変数)を利用する。暗号化だけではデータの完全性は保証できないため、前節で述べた電子署名や MAC と組み合わせて利用すべきである。また、共通鍵アルゴリズムを適用しているため、暗号化に使用する鍵は、6.1.1.2 節で述べたようにシステム 1 つの鍵で通信せざるを得ない(Annex A 参照)。

機密性維持の目的は、第 4 章で述べたように、盗聴したメッセージを想定外サービスへ適用することへの対抗であるため、暗号化の対象範囲は、アプリケーションデータとセキュリティデータ(鍵 ID など平文である必要があるデータを除く)である。

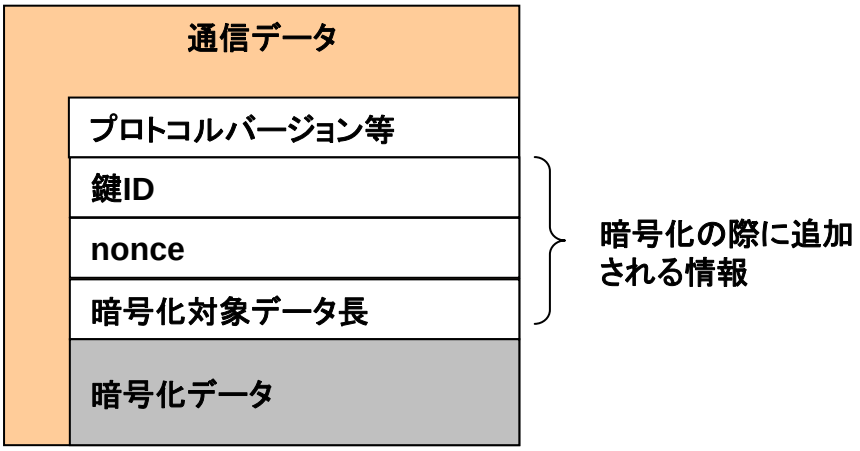


図 6-5 nonce を利用した暗号化の例

なお、IEEE1609.2[8]でも機密性維持のため公開鍵アルゴリズムと共通鍵アルゴリズムの両方を用いた方式が定義されている。これは、送信側が生成した共通鍵で保護対象データを暗号化し、その共通鍵を送信先の公開鍵によって暗号化するものである。すなわち、送信先がわかっている場合に適用できる方式である。しかし、今回の機密性維持は(正当な機器を用いない)第三者による通信データの盗聴からの保護であり、すべての正当な機器にデータを配信する本システムでは、IEEE1609.2 の暗号鍵共有方式は適さない。

6.1.3　暗号アルゴリズムについて

暗号アルゴリズムに関しては、CRYPTREC の電子政府推奨暗号リストから選択することが望ましい。また、本システムにおいて選択された暗号アルゴリズムの危殆化に関する情報を適宜入手することが望ましい。アルゴリズムが危殆化した場合、鍵長やアルゴリズムの見直しが必要である。

6.2　路側機と車載器におけるセキュリティ対策

6.2.1　路側機と車載器が格納するセキュリティ情報

6.1 節で述べたセキュリティを維持するために路側機又は車載器は、必要に応じて以下の情報を格納する。

- 鍵情報

車車間通信又は路車間通信においてメッセージの完全性確認や機密性維持のためには、鍵情報が必要である。車車間通信又は路車間通信で使用する鍵の他に、通信で使用する鍵を初期登録あるいは更新する時にセキュアに路側機又は車載器に格納するための鍵や、下記ネガリストの正当性を確認するための鍵などもある。鍵の詳細は、暗号方式に依存する。

- 種別情報

発信元の種別を偽った路側機へのなりすまし、車両へのなりすましに対抗するためには、路側機や一般車両向け車載器、優先車両向け車載器といった送信元の種別を区別するための種別情報が必要である。

- 機器 ID

改ざんされた路側機や車載器を一意に識別するためには、機器ＩＤが必要である。

- 日時情報

送信タイミングを変えてのリプレイ攻撃に対抗するためには、メッセージの送信日時を示す日時情報が必要である（Annex B 参照）。

- 位置情報

送信位置を変えてのリプレイ攻撃に対抗するためには、メッセージの送信位置を示す位置情報が必要である。

- ネガリスト

受信側の路側機又は車載器において、改ざんされた路側機や車載器からのメッセージを排除するために、ネガリストが必要である。

6.2.2　路側機と車載器の製造

路側機及び車載器の内部でセキュリティ情報を扱う機能モジュールは、セキュリティ情報の漏洩及び改ざんを阻止するように管理した上で製造される必要がある。

6.2.3　路側機と車載器の実装

路側機及び車載器の内部でセキュリティ情報を扱う機能モジュールは、出荷後の状態で以下の耐タンパ性を満たすよう実装される必要がある。

- セキュリティ情報に関わる処理の解析が困難であること。
- 公開鍵以外の鍵情報が外部から読み出せないこと。

- セキュリティ情報の更新を目的として設計された機器又は技術以外によって、セキュリティ情報の変更及びセキュリティ情報に関わる処理の変更や無効化がされないこと。

6.3 運用管理機関におけるセキュリティ対策

運用管理機関におけるセキュリティ対策を、機器メーカ等の外部エンティティに関する対策と運用管理機関内部での対策の観点で述べる。

6.3.1 外部エンティティに関するセキュリティ対策

外部エンティティとの関係におけるセキュリティ対策を車載器や路側機の開発・製造フェーズ、設置・販売フェーズ、運用フェーズにて取り扱う各情報の観点で述べる。

6.3.1.1 開発・製造フェーズ

車載器や路側機の開発・製造フェーズでは、セキュリティ仕様書やテストで使用するテスト鍵情報等をメーカに貸与する必要がある。

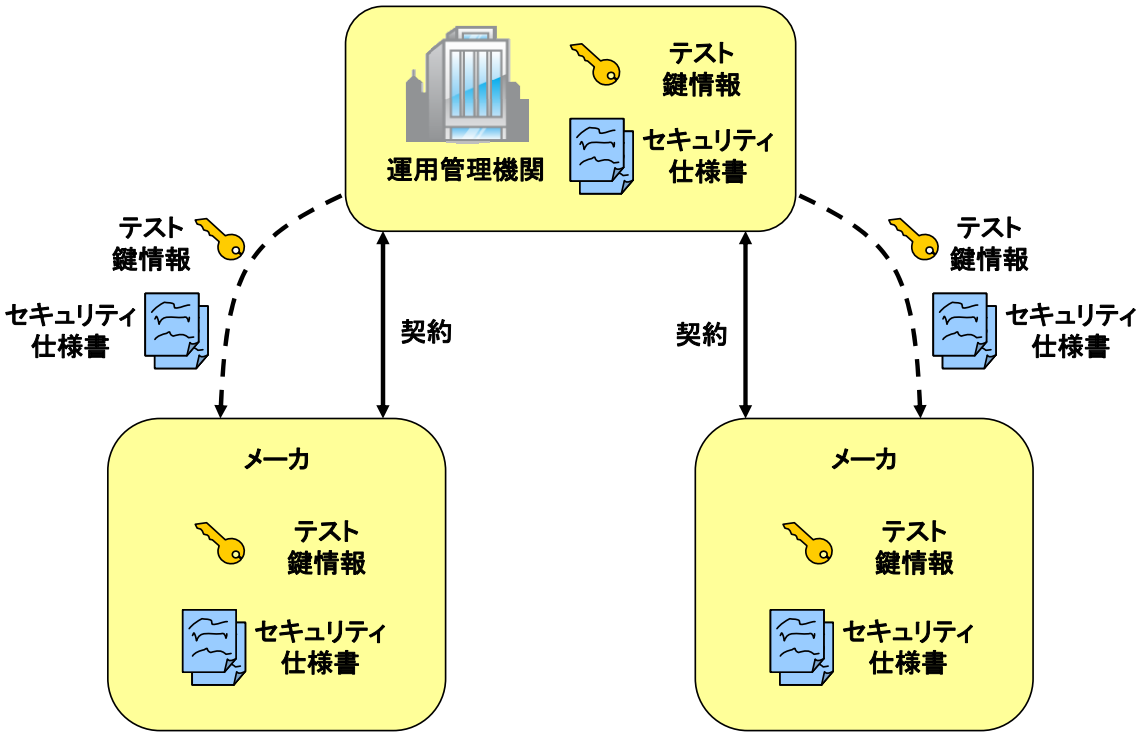


図 6-6 開発・製造フェーズ

運用管理機関は、セキュリティ仕様書やテスト鍵情報を貸与する場合には、貸与先を審査し、契約を締結する必要がある。運用管理機関は、貸与先に対して、セキュリティ仕様書やテスト鍵情報

等の機密保持を徹底させる必要がある。また、これらの受け渡し時において機密性を維持する必要がある。これらの情報を使用しないメーカに対しては、貸与した情報の返却を要求することが望ましい。

6.3.1.2　設置・販売フェーズ

設置・販売フェーズでは、図 6-7 に示すように、鍵情報と初期ネガリストを提供し、各機器に格納する必要がある。

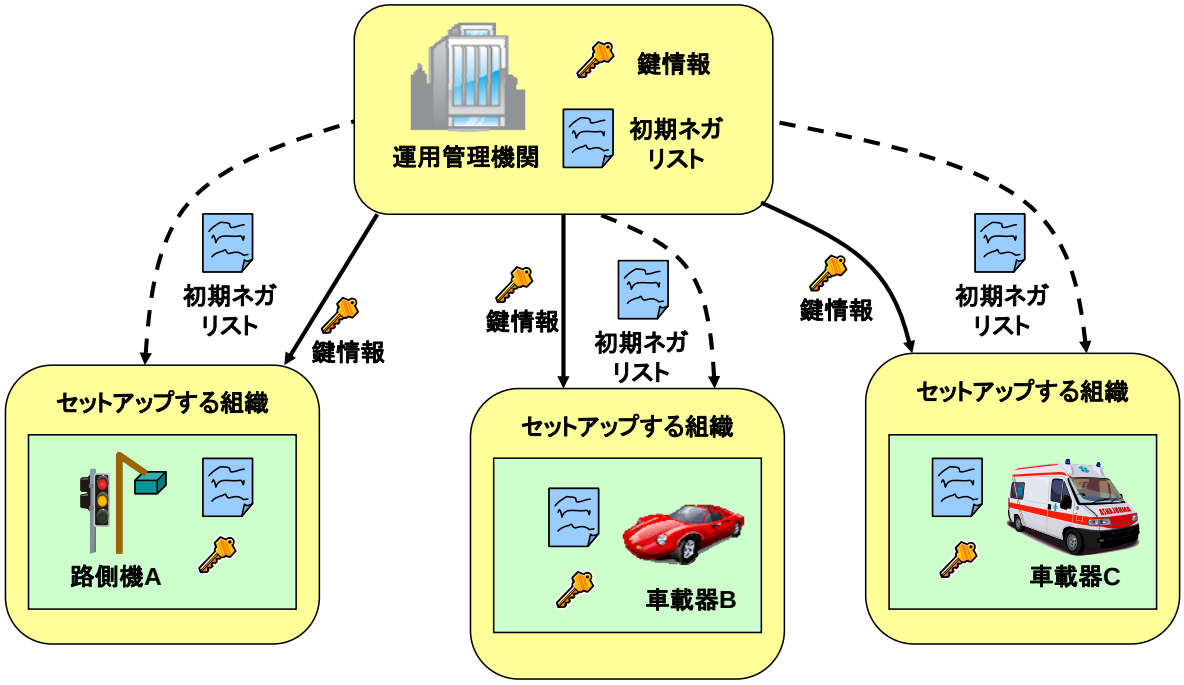


図 6-7 設置・販売フェーズ

各機器に格納する鍵情報は、6.1 節で述べた方式によって異なる。表 6-6 に方式と各鍵情報を示す。必要なセキュリティ対策は機密性と完全性の観点で表し、(済み)はその方式によって対策されていることを示す(例えば、各機器の公開鍵証明書は CA の公開鍵証明書で検証可能)。各機器の秘密鍵は①各機器で生成②CA で生成したものを各機器に格納の二通りある。

表 6-6 各機器に格納する鍵情報

目的	方式	鍵情報	必要なセキュリティ対策
真正性確認 完全性確認	電子署名	CA の公開鍵証明書	完全性(済み)
		各機器の秘密鍵	機密性、完全性
		各機器の公開鍵証明書	完全性(済み)
	MAC	通信鍵	機密性、完全性
機密性維持	暗号化	暗号鍵	機密性、完全性

電子署名方式では各機器に格納する上記鍵情報の他に、運用管理機関にて生成された CA 秘密鍵があり、本鍵の機密性・完全性が維持されなければならない。

初期ネガリストについて表 6-7 に示す。CRL には CA の署名が付加されており、CA 証明書を用いて完全性を検証できる。

表 6-7 各機器に格納するネガリスト

対策	方式	ネガリスト	必要なセキュリティ対策
真正性確認 完全性確認	電子署名	CRL	完全性(済み)
	MAC	失効機器 ID リスト	完全性

以下に、設置・販売フェーズで必要なセキュリティ対策を述べる。

- 運用管理機関における CA 秘密鍵の管理(電子署名方式)

CA 秘密鍵が漏洩したり、改ざんされた場合、第三者が偽公開鍵証明書や偽 CRL を発行でき、すべての機器の公開鍵証明書を変更する必要がある。従って、機密性・完全性を維持する必要がある。

- 運用管理機関の真正性維持

第三者が運用管理機関と偽って、不正な CA 証明書や通信鍵を機器メーカに配布すると、その偽鍵情報を格納した機器は通信できない。従って、鍵情報を受領する機器メーカが、正当な運用管理機関から鍵情報を受領できるように運用管理機関の真正性を確認できる仕組みが必要である。

- 鍵情報を受領する機器メーカの真正性維持

運用管理機関が不正な第三者組織に鍵情報を配布した場合、その鍵情報を悪用される恐れがあるため、運用管理機関は機器メーカの真正性を確認できる手段が必要である。

- 運用管理機関と機器メーカ間の通信路の保護

運用管理機関と機器メーカとの間の通信路における鍵情報等の漏洩や改ざんに対抗するために、通信路での機密性・完全性維持が必要である。ただし、機密性が必要な情報や完全性が必要な情報

は方式によって異なる(表 6-6 や表 6-7 参照)。

- 機器メーカにおける鍵情報の機密性・完全性維持

鍵情報が機器メーカから漏洩したり、機器メーカにて改ざんされた場合、その鍵情報は使用できない。従って、運用管理機関から受領した鍵情報について、機器メーカにおける機密性・完全性維持が必要である。ただし、機密性が必要な情報や完全性が必要な情報は方式によって異なる(表 6-6 や表 6-7 参照)

- 失効機器 ID リストの完全性維持(MAC 方式)

第三者が発行した偽失効機器 ID リストや正当なリストを改ざんした不正な失効機器 ID リストが各機器へ格納されると、正常な通信が行えない。従って、失効機器 ID リストの完全性維持が必要である。

6.3.1.3 運用フェーズ

運用フェーズでは、図 6-8 に示すように、各機器に格納した鍵情報とネガリストを更新する必要がある。

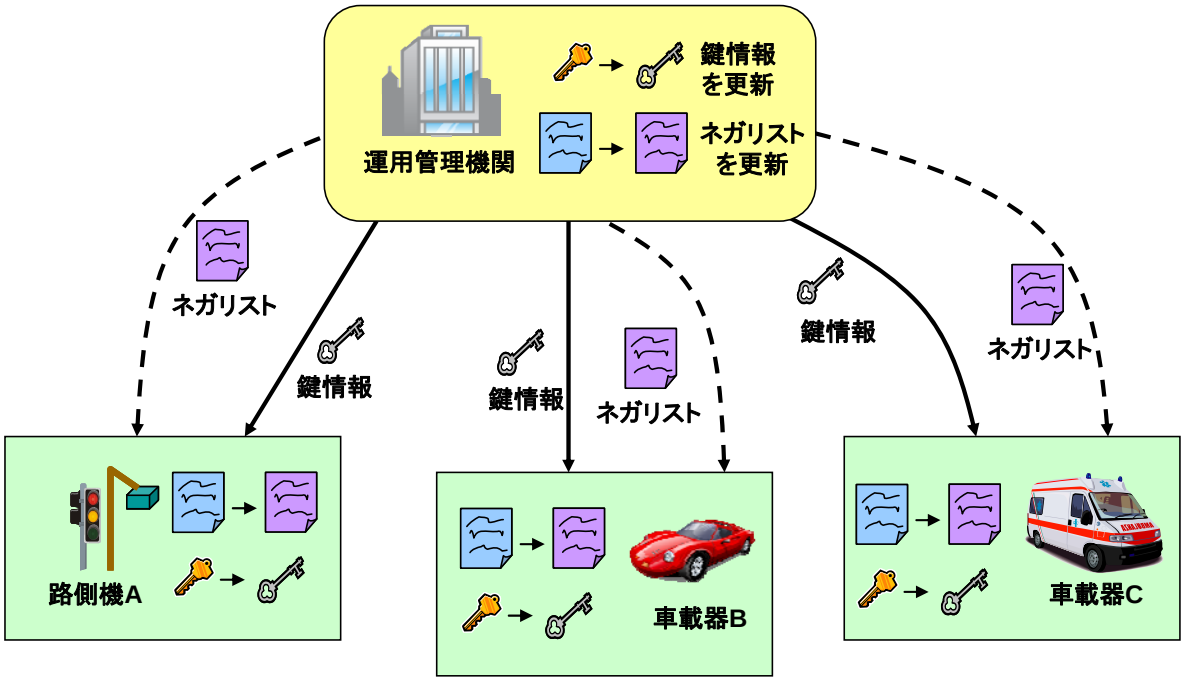


図 6-8 運用フェーズ

各機器に格納されている鍵情報は、6.1 節で述べた方式によって異なる。表 6-8 に方式と各鍵情報を示す。電子署名方式において、各機器の秘密鍵の更新は①各機器で生成②CA で生成したものを各機器に格納の二通りある。

表 6-8 各機器にて更新が必要な鍵情報

目的	方式	鍵情報	必要なセキュリティ対策
真正性確認 完全性確認	電子署名	CA の公開鍵証明書	完全性(済み)
		各機器の秘密鍵	機密性、完全性
		各機器の公開鍵証明書	完全性(済み)
	MAC	通信鍵	機密性、完全性
機密性維持	暗号化	暗号鍵	機密性、完全性

電子署名方式では上記鍵情報の他に、運用管理機関にて更新された CA 秘密鍵があり、本鍵の機密性・完全性が維持されなければならない。

ネガリストについて表 6-9 に示す。

表 6-9 各機器にて更新が必要なネガリスト

対策	方式	ネガリスト	必要なセキュリティ対策
真正性確認 完全性確認	電子署名	CRL	完全性(済み)
	MAC	失効機器 ID リスト	完全性

以下に、運用フェーズで必要なセキュリティ対策を述べる。

- 運用管理機関における CA 秘密鍵の管理(電子署名方式)

販売・設置フェーズと同様に、CA 秘密鍵が漏洩したり、改ざんされた場合、第三者が偽公開鍵証明書や偽 CRL を発行でき、すべての機器の公開鍵証明書を変更する必要がある。従って、CA 秘密鍵の機密性・完全性を維持する必要がある。

- 運用管理機関の真正性維持

第三者が運用管理機関と偽って、不正な CA 証明書や通信鍵を車載器や路側機に配布すると、その偽鍵情報を格納した機器は通信できない。従って、正当な運用管理機関が発行した鍵情報やネガリストであることを確認できる手段が車載器や路側機に必要である。

- 鍵情報を更新する機器の真正性維持

不正な機器からの更新要求等により、運用管理機関が不正な機器に鍵情報を配布した場合、その鍵情報を悪用される恐れがあるため、運用管理機関は正当な機器であることの確認が必要である。

- 運用管理機関と機器間の通信路の保護

運用管理機関と機器との間の通信路における鍵情報等の漏洩や改ざんに対抗するために、通信路での機密性・完全性維持が必要である。ただし、機密性が必要な情報や完全性が必要な情報は方式によって異なる(表 6-8 や表 6-9 参照)。

- 失効機器 ID リストの完全性維持(MAC 方式)

第三者が発行した失効機器 ID リストや正当な失効機器 ID リストの改ざんした不正な失効機器 ID リストが各機器へ更新されると、正常な通信が行えない。従って、失効機器 ID リストの完全性維持が必要である。

6.3.2 運用管理機関内部でのセキュリティ対策

運用管理機関では、図 6-9 に示すように、システムで使用する鍵情報とネガリストをセキュアに管理する必要がある。

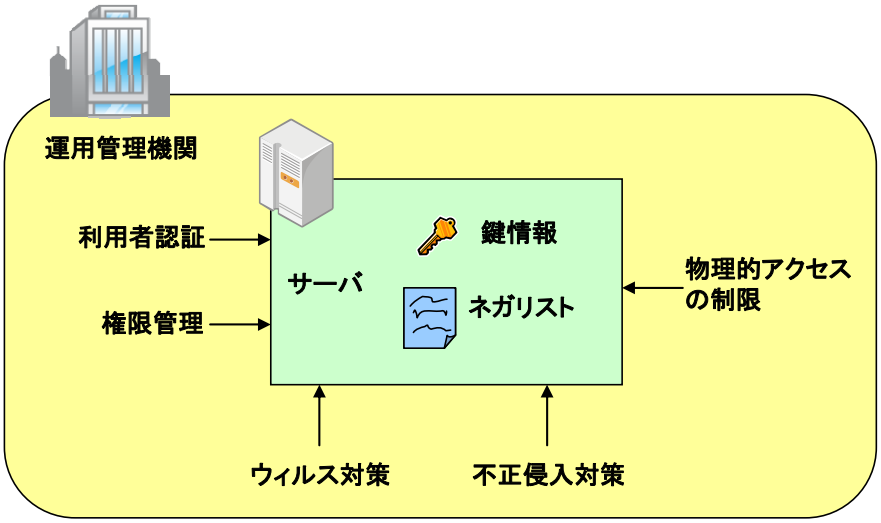


図 6-9 運用管理機関内部でのセキュリティ対策

鍵情報やネガリストを管理・発行する運用管理機関のサーバについて、外部からの不正侵入やウィルス感染等への対策、また、サーバでの利用者認証やアクセス権管理などの対策が必要である。特に、CA 秘密鍵や通信鍵などの鍵情報が漏洩した場合、すべての機器の鍵情報を変更する必要があるため、鍵情報は耐タンパ性を有したハードウェアセキュリティモジュールによる管理が望ましい。さらに、サーバへの物理的アクセスの制限など設置環境における対策も必要である。

［余白］

第7章　付録

Annex A. 共通鍵アルゴリズム適用時の鍵管理について

一般的に、共通鍵アルゴリズムを用いたシステムでは、データ通信前に通信用のセッション鍵(共通鍵)を、事前に格納された格納鍵(共通鍵)を用いて共有するトランザクションが必要となる。セッション鍵は、その通信に使用する使い捨ての鍵である(長期に渡った同じ鍵によるデータ暗号化は危険)

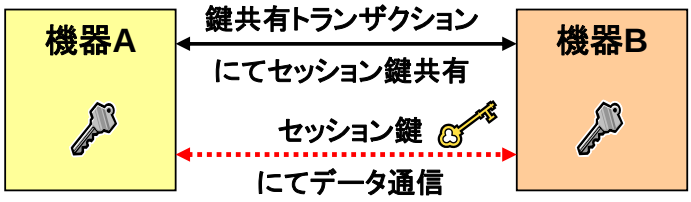


図 7-1 共通鍵を用いた一般的なシステム

従って、複数の機器(B、C)と通信する親の機器(A)は、通信相手分(B、C)の格納鍵を持つ必要がある。

図 7-2 複数の機器との通信

一方、車車間通信では、すべての車載器が親の機器になるため、すべての車載器分の格納鍵を持つ必要がある。

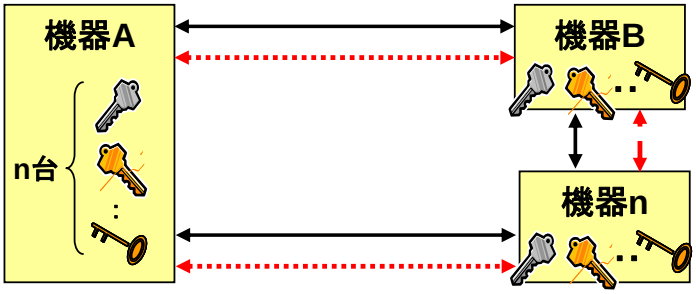


図 7-3 車車間通信(1)

しかし、すべての車載器分の格納鍵を持つことは現実的に不可能であり、同報通信のため鍵共有トランザクションも適用できない。従って、車車間通信では、システム 1 つの鍵で通信するしかない(すべての車載器に同じ共通鍵を格納)。

図 7-4 車車間通信(2)

Annex B. リプレイ攻撃について

日時データの取り扱いとリプレイ攻撃を検証する。

1. 日時データなし・カウンター値による対策なしの場合
   - 送信タイミングは攻撃者の任意の時間、任意の送信相手に対して攻撃可能。
     （攻撃者は受信した急ブレーキ情報等を蓄積し、特定の車両に対して、存在しない車両の急ブレーキ情報を受信させて混乱させたり、緊急車両を止めたりすることも可能。重大な事故に繋がる可能性もあり）
2. 日時データなし・カウンター値による対策ありの場合
   - 日時と無関係な、送信回数等のカウンター値を使用。
   - 車載器はカウンターの検証の為、送信元の ID と最新カウンター値の保持が必要。
   - 受信したメッセージとの比較を行い、受信済みメッセージの再送や受信済み以前のメッセージの再送に対して検出可能(保持している範囲内で検出可能)。
   - 受信済み以降を含めた未受信のメッセージの再送に対しては検出が不可能。

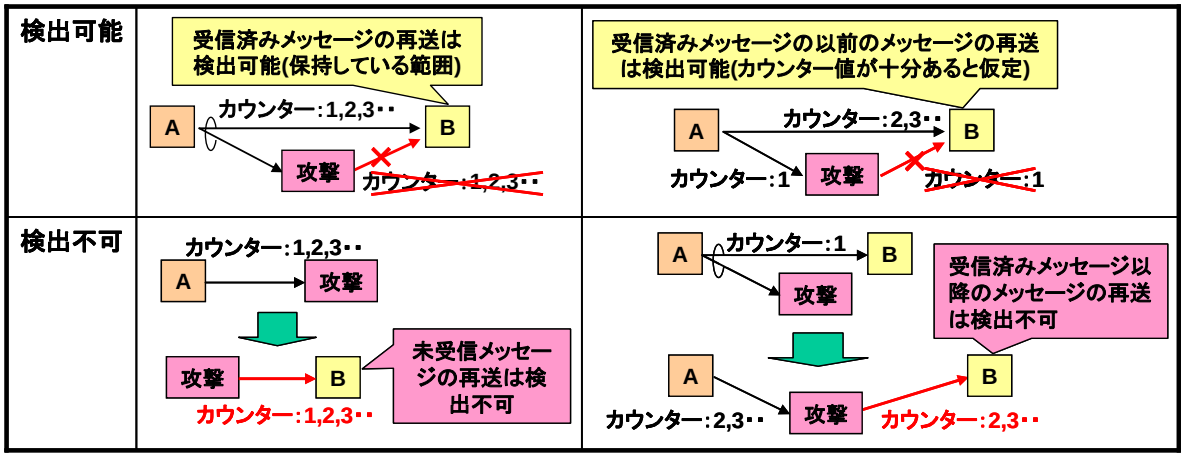


図 7-5 日時データなし・カウンター値による対策ありの場合

3. 日時データ（時分秒）あり・カウンター値による対策なしの場合
   - 年月日がないため、翌日以降の同じ時間に再送された攻撃は検出不可能。

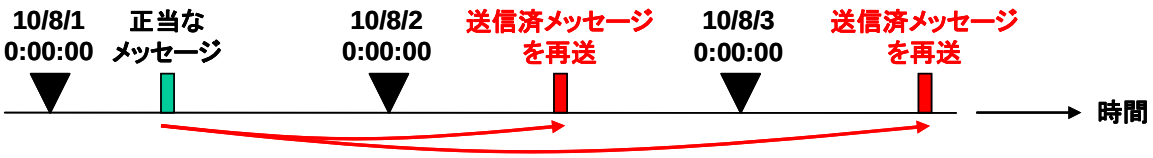


図 7-6 翌日以降の同じ時間に再送されたリプレイ攻撃

- 秒単位以下で再送されたリプレイ攻撃は検出不可能。

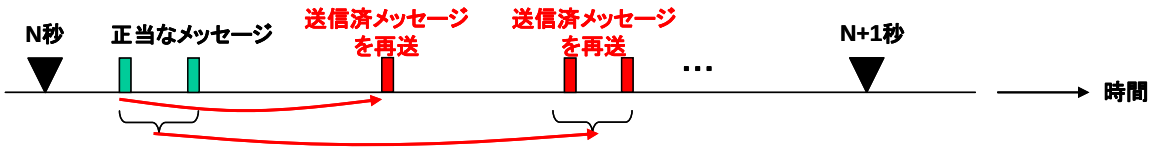


図 7-7 秒単位以下で再送されたリプレイ攻撃

4. 日時データ（時分秒）あり・カウンター値による対策ありの場合

- 日時データに年月日がないため、翌日以降の同じ時間に再送された攻撃は検出不可能。
- カウンター値を日時データ（時分秒）に付加することで、秒単位以下での攻撃は検出可能。
- 秒単位以下で再送されたメッセージに対しては、受信したメッセージとの比較を行い、受信済みメッセージの再送や受信済み以前のメッセージの再送に対して攻撃検出可能。
  （ただし車載器は送信元の ID と最新カウンター値の保持が必要で、保持している範囲内で可能）
- 受信済み以降を含めた未受信のメッセージの秒単位以内の再送に対しては検出不可能。

5. 日時データ（年月日時分秒）あり・カウンター値による対策なしの場合

- 秒単位以下で再送されたリプレイ攻撃は検出不可能。

6. 日時データ（年月日時分秒）あり・カウンター値による対策ありの場合

- カウンター値を日時データ（年月日時分秒）に付加することで、秒単位以下での攻撃検出可能。
- 秒単位以下で再送されたメッセージに対しては、受信したメッセージとの比較を行い、受信済みメッセージの再送や受信済み以前のメッセージの再送に対して攻撃検出可能。
  （ただし車載器は送信元の ID と最新カウンター値の保持が必要で、保持している範囲内で可能）
- 受信済み以降を含めた未受信のメッセージの秒単位以内の再送に対しては攻撃検出が不可能。

Annex C. 路情報(間)への攻撃と対策例

対策案	攻撃 1 送信時刻改ざん	攻撃 2 路車間時間改ざん	攻撃 3 路車間時間偽造	コスト	通信仕様への影響	長所	短所
1. 転送回数規定	△ (転送無しは○)	△	×	○	○	・ 対策容易	・ 攻撃者存在エリアで路車間通信成功率が低下
2. 矛盾検出後、車車間通信	○(*1)	○(*1)	○(*1)	○	詳細検討要	・ 車車間通信に対する妨害を抑制可能 ・ 攻撃者存在エリアでのみ影響 ・ 路側機設定ミスの影響を軽減可能	・ 攻撃者存在エリアで路車間通信成功率が車車間通信レベルまで低下
3. 路情報(間)の暗号化	○	○	○	×	×	・ 路情報(間)全体を保護可能	・ 通信仕様への影響大 ・ 高コスト
4. サービスレベル規定(*2)	△	△	△ (対策 2 との組合せは○)	○	○	・ 路車間通信時間の偽造へ対抗可能	・ 路車間通信時間の比率の規定要 ・ 車車間通信サービスは路車間通信サービスとの共存が前提

*1 攻撃者が存在しても車車間通信の通信期間を確保する

*2 以下の 2 点を満足するようにサービスレベルを調整する

- 路車間通信時間の比率(最大値)を規定する
- 車車間通信サービスは、路車間通信との共存を前提とする

Annex D. セキュリティ情報の格納・更新・設定変更を行うプリミティブの検討

車車間、路車間通信におけるセキュリティの処理を規定するプリミティブ以外に、システムを運用していく上でセキュリティ情報の格納・更新やセキュリティ設定の変更など、セキュリティ管理を行うプリミティブを規定する必要がある。

以下に、セキュリティ情報としての鍵の格納や更新、セキュリティ情報の取得、設定変更を実施するセキュリティ管理に必要となるプリミティブ（例）とセキュリティ管理の手順（例）を示す。

1. セキュリティ管理に必要なプリミティブ（例）

以下に示すプリミティブにより、機器のセキュリティ部に対する管理を行う。

・SecurityCont.Request(Security Control Information, Security Control Data Length, Security Control Data)	・SecurityCont.Response(Security Control Information, Security Control Data Length, Security Control Data)

（Security Control Information：セキュリティ処理部関連情報　長さ１バイト）
（Security Control Data Length：セキュリティ管理データ長　長さ２バイト）
（Security Control Data：セキュリティ管理データ　長さ Security Control Data Length で指定）

＜参考＞通信におけるセキュリティ処理のためのプリミティブと処理手順（例）
［Security.Request、Security.Response、Unsecurity.Request、Unsecurity.Response］
によるセキュリティ処理手順
・L7層がセキュリティフラグを見て、セキュリティ処理の実行を判断する。

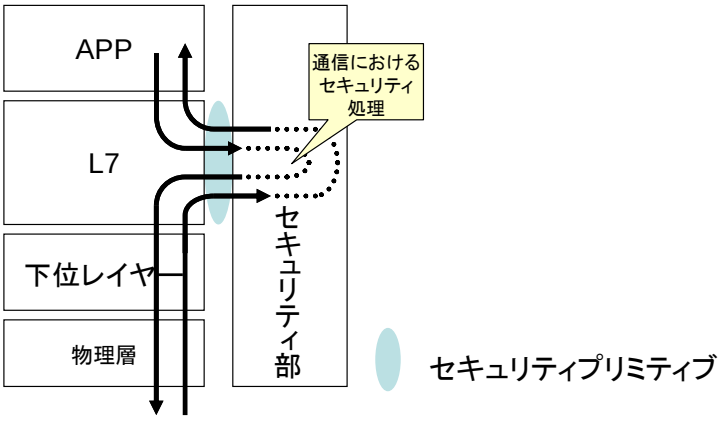


図 7-8 通信におけるセキュリティ処理手順（例）

2. セキュリティ管理の手順（例）

a) システム管理部が外部 I/F を用いてセキュリティ管理を行う場合

下図にあるとおり、機器に接続された外部 I/F（例えば、IC カードリーダや USB ポート、シリアルポートなど）を用いて、セキュリティ管理に必要なセキュリティ情報（新たなセキュリティ情報や更新データ、セキュリティ設定変更指示など）の入出力をシステム管理部が行う場合、以下の手順で実施される。

① 機器のシステム管理部と物理的に接続された外部 I/F からセキュリティ管理データを入力

② セキュリティ管理データは一旦システム管理部にて受信される。

③ システム管理部でセキュリティ管理データを分析・判定する。

④ 必要に応じてセキュリティ部にセキュリティ管理データを受け渡す。（プリミティブ：SecurityCont. Request）

⑤ セキュリティ部は入力されたセキュリティ管理データに基づき管理処理を行う。

⑥ セキュリティ部は処理結果をシステム管理部に返す。（プリミティブ：SecurityCont.Response）

この場合、システム管理部とセキュリティ部との間にセキュリティ管理プリミティブを設ける必要がある。

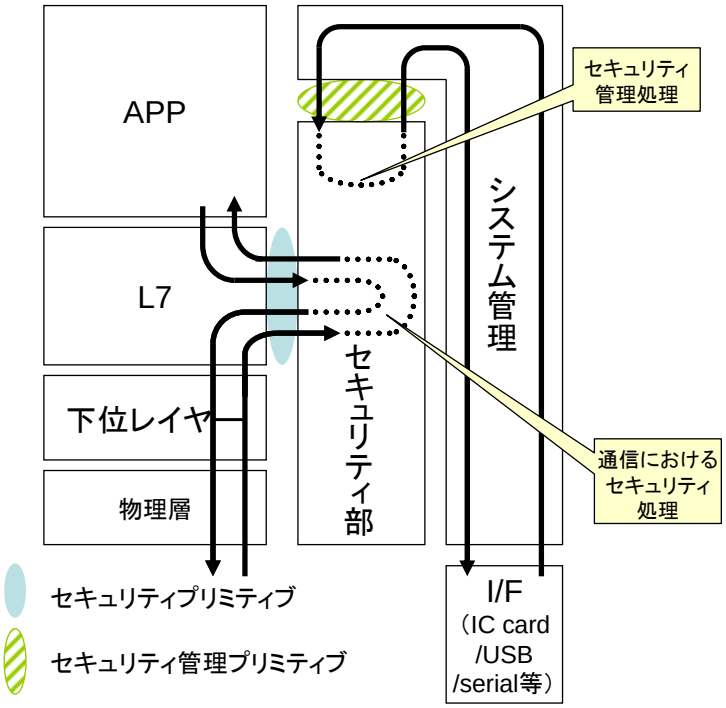


図 7-9 システム管理部が外部 I/F を用いてセキュリティ管理を行う場合

b）セキュリティ管理アプリが外部 I/F を用いてセキュリティ管理を行う場合

下図にあるとおり、機器に接続された外部 I/F を用いて、セキュリティ管理に必要なセキュリティ情報の入出力をセキュリティ管理アプリが行う場合、以下の手順で実施される。

① 機器のシステム管理部と物理的に接続された外部 I/F からセキュリティ管理データを入力
② セキュリティ管理データは一旦システム管理部にて受信される。
③ システム管理部はセキュリティ管理データをセキュリティ管理アプリに受け渡す。
④ セキュリティ管理アプリ部でセキュリティ管理データを分析・判定する。
⑤ セキュリティ管理アプリは必要に応じてセキュリティ部にセキュリティ管理データを受け渡す。（プリミティブ：SecurityCont. Request）
⑥ セキュリティ部は入力されたセキュリティ管理データに基づき管理処理を行う。
⑦ セキュリティ部は処理結果をセキュリティ管理アプリに返す。（プリミティブ：SecurityCont.Response）
⑧ セキュリティ管理アプリは処理結果のデータ等を必要に応じてシステム管理部に渡す。

この場合、APP 層とセキュリティ部との間にセキュリティ管理プリミティブを設ける必要がある。また、APP 層とシステム管理部との間にもデータ収受のプリミティブを設ける必要がある。

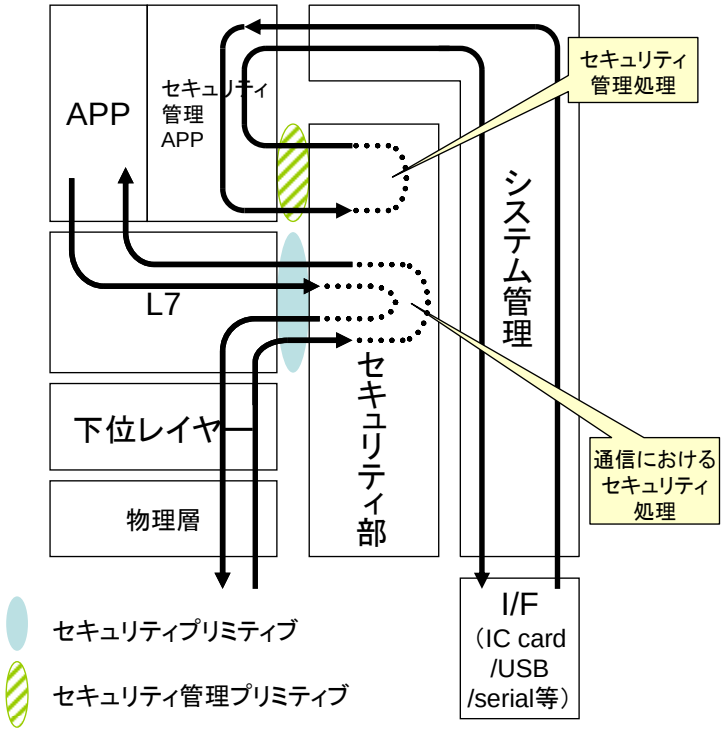


図 **7-10** セキュリティ管理アプリが外部 **I/F** を用いてセキュリティ管理を行う場合

c）セキュリティ管理アプリが通信を用いてセキュリティ管理を行う場合

下図にあるとおり、通信を用いてセキュリティ管理に必要なセキュリティ情報の入出力を行う場合、以下の手順で実施される。

① L7 層とセキュリティ部との間で、通信におけるセキュリティ処理を実施した後、APP 層にアプリケーションのデータとしてセキュリティ管理データが入力される。

② APP 層は一旦、データを受信して受渡し先を振り分ける。(セキュリティ管理アプリなのか、一般のアプリなのか)

③ セキュリティ管理アプリ部は受信したセキュリティ管理データを分析・判定する。

④ セキュリティ管理アプリは必要に応じてセキュリティ部にセキュリティ管理データを受け渡す。（プリミティブ：SecurityCont. Request）

⑤ セキュリティ部は入力されたセキュリティ管理データに基づき管理処理を行う。

⑥ セキュリティ部は処理結果をセキュリティ管理アプリに返す。（プリミティブ：SecurityCont.Response）

⑦ セキュリティ管理アプリは処理結果のデータ等を必要に応じて L7 層に渡す。

この場合、APP 層とセキュリティ部との間にセキュリティ管理プリミティブを設ける必要がある。

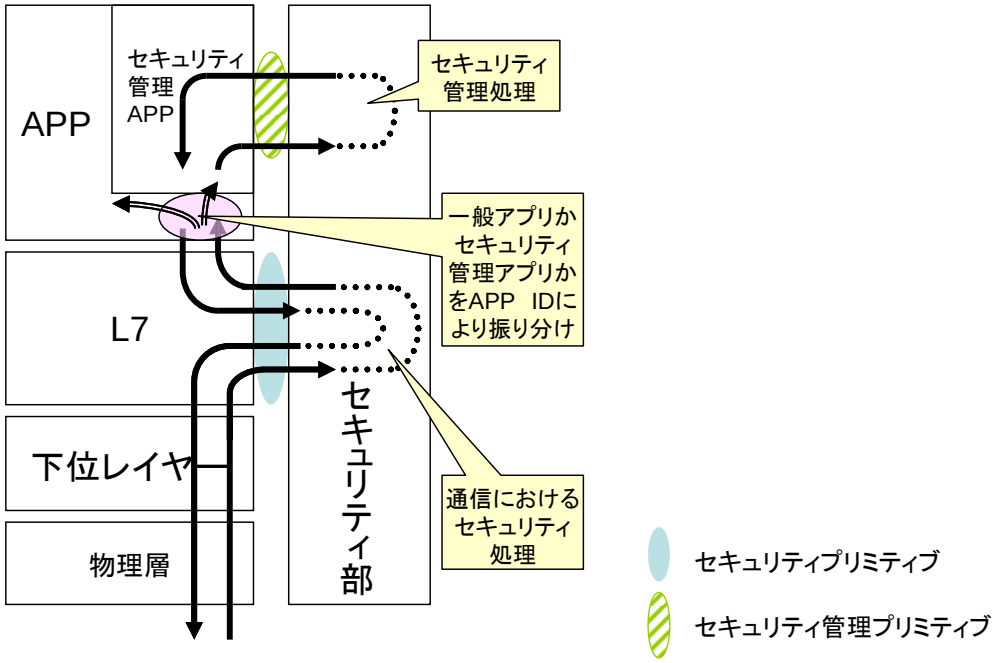


図 7-11 セキュリティ管理アプリが通信を用いてセキュリティ管理を行う場合

以上