（別紙）

700MHz 帯安全運転支援システム構築のための
セキュリティガイドライン

1.0 版

総務省

平成 27 年７月９日

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 27 年 7 月 9 日	策定	新規策定	

目次

第 1 章　はじめに 1

1-1　概要 1
1-2　対象読者 1
1-3　適用範囲 2
1-4　参照資料 2
1-5　用語及び略語の定義 4
1-6　ガイドラインの構成 6

第 2 章　通信システムを構築するための指針 7

2-1　要求条件 7
2-1-1　通信に関する要求条件 7
2-1-2　セキュリティに関する要求条件 7
2-2　参考とした情報 8
2-3　指針とその根拠 10
2-3-1　指針 10
2-3-2　根拠 11

第 3 章　セキュリティ情報運用管理システムを構築するための指針 16

3-1　セキュリティ情報運用管理システムの概要 16
3-1-1　構成 16
3-1-2　機能 17
3-2　要求条件 19
3-3　指針と各機能におけるセキュリティの例示 23
3-3-1　指針 23
3-3-2　指針に基づいた各機能におけるセキュリティの例示 24

付録 I 32

第1章　はじめに

1-1　概要

本ガイドラインは、「700MHz 帯安全運転支援システムのセキュリティ要求事項」（以下、要求事項）に基づいて、700MHz 帯安全運転支援システムを構築するための指針を示すものである。

本ガイドラインは、要求事項、700MHz 帯安全運転支援システムに関係する規格、及び平成 26 年度総務省予算事業「次世代 ITS の確立に向けた通信技術に関する調査」結果等を踏まえて作成している（図 1-1）。

700MHz 帯安全運転支援システムの最終的なセキュリティ確保の可否は、その構築に関わる企業、団体及び省庁、特に、運用管理機関、公共路側機管理者、車両メーカ、車載機メーカ、路側機メーカ、及び SAM メーカの対応如何にかかっていることに留意すべきである。これら運用管理機関等は、本ガイドラインを踏まえつつ、セキュリティ技術や攻撃事例等の動向を踏まえて、必要かつ十分な具体的なセキュリティ方式（処理手順、暗号アルゴリズム、データフォーマット等）を定めたセキュリティ仕様書を策定し、実装及び運用管理を行うことが重要である。

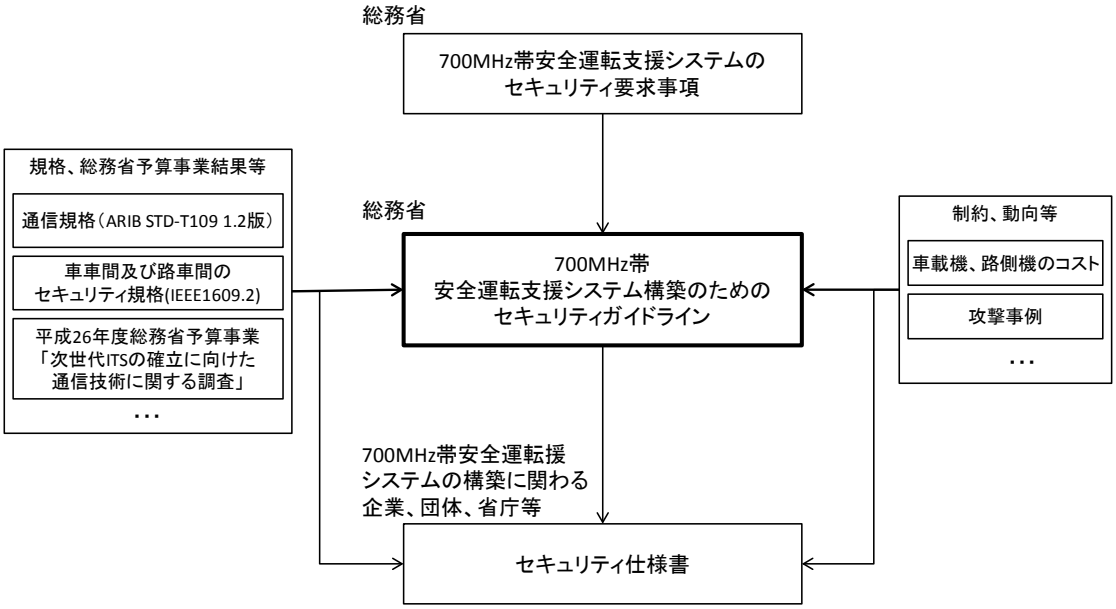

図 1-1　本ガイドラインの位置付け

1-2　対象読者

本ガイドラインは、700MHz 帯安全運転支援システムの構築に関わる企業、団体及び省庁、特に、運用管理機関、公共路側機管理者、車両メーカ、車載機メーカ、路側機メーカ、及び SAM メーカを対象読者とする。本ガイドラインにおいて、各対象読者に関係する箇所を示したものを表 1-1 に示す。

表 1-1　対象読者と参照箇所の対応

対象読者	本ガイドラインでの参照箇所
運用管理機関	第 1 章、第 2 章、第 3 章 3-1-1 項、3-1-2 項(1)(2)(4)(5)、3-2 節、3-3-1 項、3-3-2 項(1)(2)(4)(5)(6)
公共路側機管理者	第 1 章、第 2 章、第 3 章 3-3-2 項(3)(5)(6)
車両メーカ	第 1 章、第 2 章、第 3 章 3-3-2 項(3)(5)(6)
車載機メーカ	第 1 章、第 2 章、第 3 章 3-1-1 項、3-1-2 項(2)(3)(4)(5)、3-2 節、3-3-1 項、3-3-2 項(2)(3)(4)(5)(6)
路側機メーカ	第 1 章、第 2 章、第 3 章 3-1-1 項、3-1-2 項(2)(3)(4)(5)、3-2 節、3-3-1 項、3-3-2 項(2)(3)(4)(5)(6)
SAM メーカ	第 1 章、第 2 章、第 3 章 3-1-1 項、3-1-2 項(2)(3)(4)(5)、3-2 節、3-3-1 項、3-3-2 項(2)(3)(4)(5)(6)

1-3　適用範囲

本ガイドラインは、[要求事項]にて定義される「700MHz 帯安全運転支援システム」（図 1-2）の構成要素である通信システム及びセキュリティ情報運用管理システムを適用対象とするものである。

1-4　参照資料

引用文献

[要求事項]　“700MHz 帯安全運転支援システムのセキュリティ要求事項 1.0 版”，総務省，2014/6

[無線設備規則]　“無線設備規則”，総務省

[T109]　“ARIB STD-T109 1.2 版, 700MHz 帯高度道路交通システム 標準規格”，ARIB，2013/12

参考文献

[RC-009]　“ITS FORUM RC-009 1.2 版，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，2013/11

[RC-010]　“ITS FORUM RC-010 1.0 版, 700MHz 帯高度道路交通システム拡張機能ガイドライン” ITS FORUM，2012/3

[RC-013]　“ITS FORUM RC-013 1.0 版, 700MHz 帯高度道路交通システム実験用車車間通信メッセージガイドライン”，ITS FORUM，2014/3

[懇話会資料]　“700MHz 帯高度道路交通システムの標準規格の概要について”，一般社団法人電波産業会 第 94 回電波利用懇話会資料，2012/3

[IEEE 1609.2]　“IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages (IEEE 1609.2)”，IEEE，2013/4

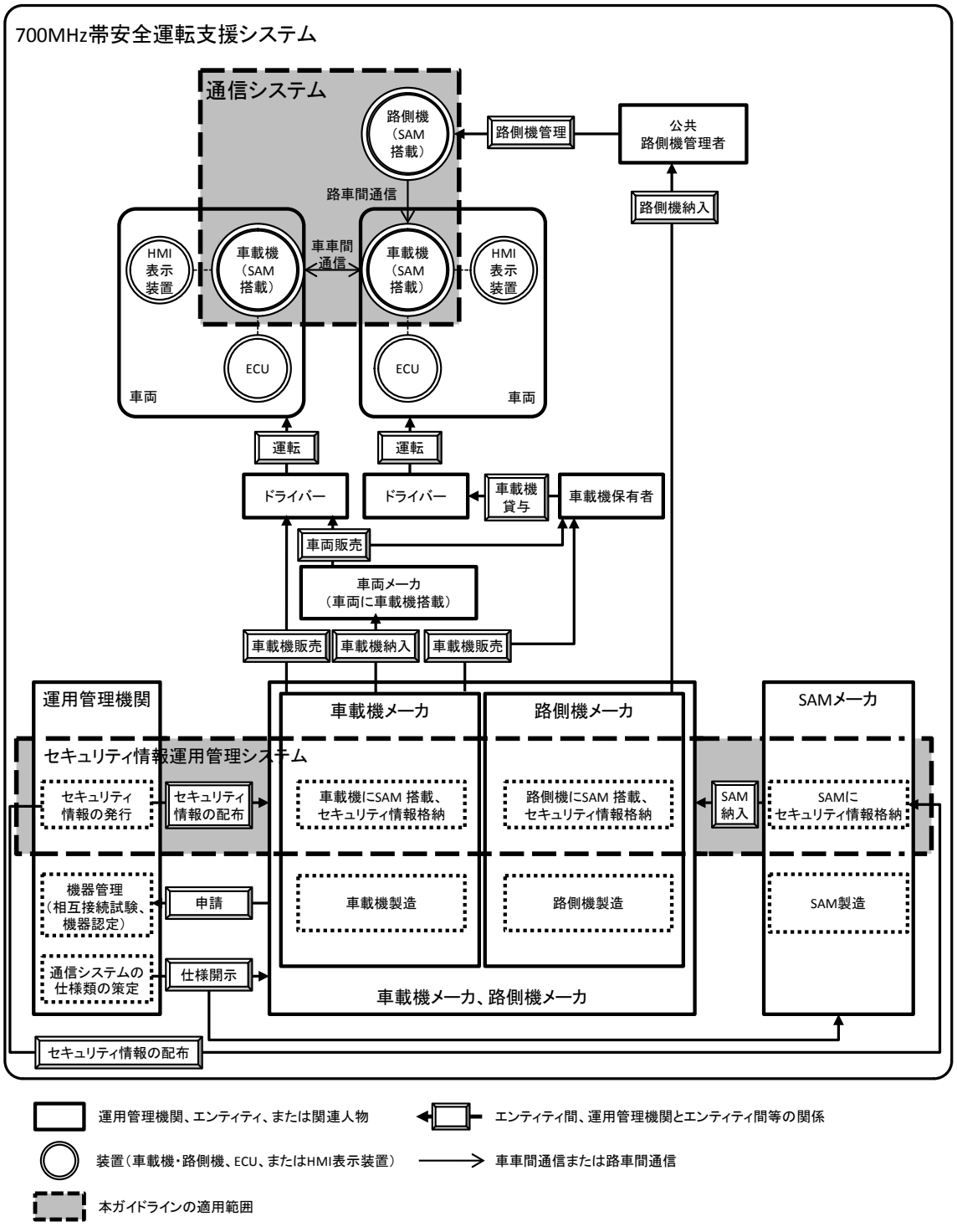

図 1-2　700MHz 帯安全運転支援システムの構成（出所：[要求事項]）

1-5　用語及び略語の定義

本ガイドラインで使用する用語及び略語の定義を表 1-2 に示す。

表 1-2　用語及び略語の定義

用語・略語	定義
700MHz 帯安全運転支援システム	700MHz 帯通信システムを用いて安全運転支援サービスの提供を行うためのシステム。
700MHz 帯通信システム	[無線設備規則]の第 49 条の 22 の 2 に記載の 700MHz 帯高度道路交通システムのことであり、陸上移動局と陸上移動局及び基地局と陸上移動局が通信を行うシステム。本書では陸上移動局を車載機、基地局を路側機、700MHz 帯通信システムを通信システムと呼ぶ。車載機は車両に搭載され、他の車載機との通信（車車間通信）により車載機自身の車両情報（位置、速度等）の送信、及び他の車載機の車両情報の受信を行う。また、車載機は路側機との通信（路車間通信）によりインフラ情報（信号情報、規制情報、歩行者情報等）を受信する。路側機は路側に設置され、路車間通信によりインフラ情報の送信を行う。
安全運転支援サービス	他の車載機や路側機から受信した情報により特定のタイミング、特定の場所、ドライバーによる特定の操作等の特定の状況が発生時にドライバーへの注意喚起、ドライバーへの客観情報通知の両方またはいずれかを行うサービス。
運用管理機関	700MHz帯安全運転支援システムを円滑に稼働させるために必要な管理を行う機関。通信システムの仕様類の策定、機器管理、セキュリティ情報の運用管理等を行うことが想定される。
エンティティ	SAMメーカ、車載機メーカ、路側機メーカ、システムメーカ等700MHz帯安全運転支援システムに関連する会社、団体、組織を指す。
公共路側機管理者	路側機を管理する会社、団体、組織等を指す。
サービス提供者	700MHz帯安全運転支援システムにおいてドライバーにサービスを提供する会社、団体、組織等を指す。
車載機保有者	車載機を保有する者。
車載機メーカ	車載機を製造する会社。
車両メーカ	車載機を搭載した車両を製造する会社。
セキュリティ情報	車車間通信や路車間通信において、車載機・路側機がセキュアにデータのやり取りを行うために必要な鍵・電子証明書（車載機メーカ向けセキュリティ情報、路側機メーカ向けセキュリティ情報、及び SAM メーカ向けセキュリティ情報）と、これらを車載機・路側機に格納するために必要な鍵・電子証明書（配布用セキュリティ情報）を指す。
セキュリティ情報運用管理システム	通信情報を保護するためのセキュリティ情報の生成、配布、保管、格納等を行うシステム。運用管理機関がセキュリティ情報の生成、配布、保管等を行い、SAM メーカ、車載機メーカ、及び路側機メーカが SAM、車載機、路側機にセキュリティ情報を格納する。

用語・略語	定義
通信情報	通信システムにおいて、路側機が車載機、または車載機が路側機や他の車載機に送信する情報で、通信ヘッダ情報とペイロード情報から構成される。通信ヘッダ情報は、路側機の送信時間割当等、通信を管理するための情報である。ペイロード情報には、インフラ情報、車両情報、及び汎用情報の 3 種類がある。インフラ情報は、信号情報や道路情報等、路側に関わる情報やインフラが検出した車両等の情報である。車両情報は、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、車両の状態に関わる情報である。汎用情報は、車載機や路側機が任意に設定する情報である。
電子証明書	電子署名を施す際に用いる鍵の真正性及び完全性を保証するもの。公開鍵証明書と同義。
電子署名データ	電子署名を施す際に情報の真正性及び完全性を保証するために生成されるもの。
ドライバー	車両を運転し、安全運転支援サービスを受ける者。車載機保有者とドライバーが異なる場合と同一の場合の両方が想定される。
路側機メーカ	路側機を製造する会社。
AES	Advanced Encryption Standard の略。
CA	Certificate Authority の略。
CCM	Counter with CBC-MAC の略。
CRL	Certificate Revocation List の略。
CTR モード	Counter モードの略。
DoS 攻撃	Denial of Service attack の略。
ECDSA	Elliptic Curve Digital Signature Algorithm の略。
EL	Extended Layer の略。
IEEE	The Institute of Electrical and Electronics Engineers, Inc.の略。 アメリカに本部がある電気・電子関係の技術者組織で、国際会議の開催、論文誌の発行、技術教育、標準化等を行っている。
ITS	Intelligent Transport System の略。
ITS 情報通信 システム推進会議	ITS、特に情報通信分野における研究開発や標準化を推進する団体。

用語・略語	定義
LAN	Local Area Network の略。
MAC	Message Authentication Code の略。
MAC アドレス	Media Access Control アドレスの略。
SAM	Secure Application Module の略。車載機や路側機に搭載され、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取りを行うためのセキュリティ処理を実行するモジュール。セキュリティ処理のための暗号化ロジックやセキュリティ情報が格納され、耐タンパー性が確保されている。
SAM メーカ	車載機、路側機に搭載する SAM を製造する会社。
WAVE	Wireless Access in Vehicular Environments の略。

1-6　ガイドラインの構成

本ガイドラインは、第 2 章において通信システムを構築するための指針、第 3 章においてセキュリティ情報運用管理システムを構築するための指針を示す。

[要求事項]においては機関毎に遵守しなければならない事項が記載されているが、本ガイドラインでは各機関が連携して取り組むべき指針が多く含まれるため、機能毎に記載し、再整理する。また、その対応関係について付録 I にまとめる。

第2章　通信システムを構築するための指針

本章では、[要求事項]を満たす通信システムを構築するためのセキュリティに関する指針を示す。2-1 節において 700MHz 帯安全運転支援システムに関係する規格等に基づく通信システム上の要求条件、及び通信システムに対するセキュリティ上の要求条件を整理する。2-2 節において指針を示すにあたって参考とした情報を整理する。2-3 節において指針及びその根拠を示す。

2-1　要求条件

本節では、通信システムを構築する際に満たさなければならない条件を示す。

2-1-1　通信に関する要求条件

700MHz 帯安全運転支援システム向け車車間及び路車間通信帯域として、周波数 755.5～764.5MHz の 9MHz 幅、1ch が割り当てられている。当該帯域向け通信規格として[T109]が策定されており、700MHz 帯安全運転支援システム向け通信システムの構築には当該通信規格を満たすことが要求される。特に当該通信規格では、車車間通信と路車間通信が 1ch を 100ms 周期の時分割で通信することが定められている。

引用規格から導き出される通信に関する要求条件を表 2-1 に示す。

表 2-1　通信に関する要求条件

No.	要求条件
1	通信の仕方（[T109]1.2 節） 同報通信とする。
2	伝送速度（[T109] 3.2.1.6 項） 5Mbps 以上とする。
3	送信時間制御機能（[T109]3.2.3.3 項） 基地局の 100ms 間における送信時間の総和は、10.5ms 以下であること。移動局の 100ms 間における送信時間の総和は、0.66ms 以下であり、かつ、送信バースト長は 0.33ms 以下であること。
4	通信周期（[T109]4.4.1.1 項） 基地局及び移動局とも、100ms 周期での通信を基本とする。
5	セキュリティのインタフェース（[T109]4.5.1.1 項） セキュリティはレイヤ 7 とインタフェースをもつ。
6	通信ヘッダのデータサイズ（[T109]第 4 章、付録 1 ） 通信ヘッダのデータサイズは 65byte である。
7	1 台の路側機が 1 周期で送信可能なパケット数（[T109]） 複数である。

2-1-2　セキュリティに関する要求条件

[要求事項]の第 2 章において通信システムにおけるセキュリティ要求事項が挙げられている。その中で、通信システムの構築に関する事項を表 2-2 に示す。それ以外の事項については第 3 章に示す。

表 2-2　通信システムの構築に関するセキュリティ要求事項

要求事項	内容
要求事項 2.3.1 項①	発信元の真正性確認 偽の第三者がなりすまして不正な通信情報を送信することで通信情報の完全性が侵害されないように、通信情報の発信元である車載機または路側機が、セキュリティ情報を用いて正しく本人が発信したことを保証し、通信情報を受信する車載機が、セキュリティ情報を用いて発信元が正しくその本人であることを確認できること。真正性確認に用いるセキュリティ情報は、SAM に格納しておくこと。
要求事項 2.3.1 項②	通信情報の完全性確認 通信の途中での改ざん等により通信情報の完全性が侵害されないように、通信情報の発信元である車載機または路側機が、セキュリティ情報を用いて送信した情報が改ざんされていないことを保証し、通信情報を受信する車載機が、セキュリティ情報を用いて受信した通信情報のペイロード情報が改ざんされていないことを確認できること。完全性確認に用いるセキュリティ情報は SAM に格納しておくこと。
要求事項 2.3.1 項③	通信情報の機密性維持 第三者による盗聴により通信情報の機密性が侵害されないように、通信情報の発信元である車載機または路側機が、セキュリティ情報を用いて通信情報のペイロード情報が第三者にわからないようにし、通信情報を受信する車載機が、セキュリティ情報を用いて発信元が送信した情報の内容をわかるようにできること。機密性維持に用いるセキュリティ情報は SAM に格納しておくこと。
要求事項 2.3.1 項④	「発信元の真正性確認」「通信情報の完全性確認」「通信情報の機密性維持」の実現方式 適切な暗号アルゴリズムと鍵長を用いて「発信元の真正性確認」「通信情報の完全性確認」「通信情報の機密性維持」を実現すること。各機能は、通信規格の制約（通信データ量、同報送信）や車載機・路側機の処理能力（処理台数、コスト）を考慮した方式を用いること。
要求事項 2.3.1 項⑥	セキュリティ情報の更新 セキュリティ情報が漏洩した場合、もしくは漏洩した可能性がある場合は、該当のセキュリティ情報を更新できること。
要求事項 2.3.2 項②	解析防止対策 車載機メーカ及び路側機メーカは、車載機・路側機が容易に解析できないようにソフトウェア・内部データの難読化等の対策を施すこと。

2-2　参考とした情報

通信システムを構築するための指針を定めるにあたっては、700MHz 帯安全運転支援システムの早期実用化を考慮し、関連団体等が実用化に向けて検討を行った結果を参考とすることにした。参考としたガイドライン、国際標準等について以下に述べる。

(1) 700MHz 帯高度道路交通システム 拡張機能ガイドライン[RC-010]

ITS 情報通信システム推進会議発行のガイドライン[RC-010]では、プロトコル機能を拡張するレイヤ EL ともセキュリティインタフェースをもつこと、及び通信情報のペイロード情報のサイズが一定以上の場合、複数パケットに分割して送信することが定められている。

(2) 700MHz 帯高度道路交通システム 実験用車車間通信メッセージガイドライン[RC-013]

ITS 情報通信システム推進会議発行のガイドライン[RC-013]では、車載機が 1 回に送信するペイロード情報のサイズは最大で 100byte 程度とすると定められている。

(3) 700MHz 帯高度道路交通システムの標準規格の概要について[懇話会資料]

一般社団法人電波産業会の[懇話会資料]で示されるように、路側機が 1 回に送信するペイロード情報のサイズは最大で 7Kbyte 程度とされている。

(4) 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]

ITS 情報通信システム推進会議発行のガイドライン[RC-009]では、通信情報の真正性・完全性保証を実現する方式として、公開鍵暗号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）と共通鍵暗号アルゴリズムによる MAC を適用した方式（以下、MAC 方式）の各方式の特徴について述べられている（表 2-3)。通信情報の機密性確保の方式は、共通鍵暗号アルゴリズムを用いた方式、特に暗号化前後でデータ長が変化しない CTR モードの暗号やストリーム暗号が適していると述べられている。

表 2-3　各方式の特徴（コスト）（出所：[RC-009] 表 6-5 を基に作成）

		電子署名方式	MAC 方式
登録工程		中 (オフライン証明書発行)	小 (オフライン共通鍵発行)
	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	・ 同一の共通鍵の発行 ・ 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（公開鍵と秘密鍵）と公開鍵証明書の更新 ・ CA 証明書の更新 ・ CRL の更新	・ 共通鍵の更新 ・ 失効機器 ID リストの更新
鍵漏洩時のメンテナンス		小 (対象機器)	大 (全ての車載機・路側機)
	作業	秘密鍵の漏洩時の作業 ・ 漏洩対象の秘密鍵更新 ・ CRL 更新 公開鍵は機密性がないため、作業不要	共通鍵の更新
各機器の必要な処理能力や規模		大 (電子署名方式の公開鍵暗号アルゴリズムは MAC 方式の共通鍵暗号アルゴリズムよりも処理負荷大)	小

		電子署名方式	MAC 方式
機器の耐タンパー実装	必要性	中 (各機器の秘密鍵の保護)	大 (システム全体の共通鍵の保護)
	保護情報	秘密鍵の機密性	・ 共通鍵の機密性 ・ 機器 ID や種別情報の完全性

(5) 車車間通信及び路車間通信のセキュリティに関する規格[IEEE 1609.2]

[IEEE 1609.2]は IEEE1609 のファミリー標準のひとつである。IEEE1609 は、無線 LAN ベースの規格である IEEE802.11p の上位層として存在する。米国では IEEE 802.11p と IEEE 1609 の組み合わせを WAVE と呼び、WAVE を用いた安全運転支援システムを検討している。[IEEE 1609.2]では、通信情報の真正性・完全性保証に、公開鍵暗号アルゴリズム ECDSA（鍵長 224bit または 256bit）による電子署名を、機密性維持に共通鍵暗号アルゴリズム AES（鍵長 128bit）による暗号化を定めている。

なお、上記ガイドライン、国際標準等については、平成 26 年度総務省予算事業の実証実験において用いている。

2-3 指針とその根拠

2-1 節及び 2-2 節を踏まえた上で、通信システムを構築するためのセキュリティに関する指針を 2-3-1 項に示す。また、その根拠を 2-3-2 項に示す。

2-3-1 指針

2-1 節の要求条件を満たすためのセキュリティに関する指針を表 2-4 に示す。

表 2-4 通信システムを構築するためのセキュリティに関する指針

セキュリティに関する要求条件	No.	指針
真正性・完全性保証 （要求事項 2.3.1 項① 要求事項 2.3.1 項② 要求事項 2.3.1 項④）	(1)	真正性・完全性保証の方式 車車間通信の真正性・完全性保証には、MAC 方式を用いるべきである。路車間通信の真正性・完全性保証には、電子署名方式と MAC 方式の組み合わせを用いるべきである。更に、路車間通信の場合、パケットが分割送信された場合やパケットロスが発生した場合も、通信情報の真正性・完全性が確認できるようにするべきである。
	(2)	真正性・完全性保証の対象範囲 真正性・完全性保証の範囲は、通信情報のペイロード情報（車両情報、インフラ情報、汎用情報）及びセキュリティヘッダ情報とすべきである。
機密性維持 （要求事項 2.3.1 項③ 要求事項 2.3.1 項④）	(3)	機密性維持の方式 車車間通信及び路車間通信の機密性維持には、共通鍵暗号アルゴリズムを用いた暗号化を行うべきである。
	(4)	暗号化の対象範囲 暗号化の対象範囲は、通信情報のペイロード情報及びセキュリティフッタとすべきである。

セキュリティに関する要求条件	No.	指針
解析防止対策 （要求事項 2.3.2 項②）	(5)	解析防止対策 車載機メーカ及び路側機メーカは、車載機及び路側機からセキュリティ情報が容易に解析されないような対策を施すべきである。
セキュリティ情報の更新（要求事項 2.3.1 項⑥）	(6)	セキュリティ情報の更新 セキュリティ情報の漏洩もしくはその可能性がある場合、セキュリティ情報を更新し､漏洩もしくはその可能性があるセキュリティ情報が利用されて悪影響を及ぼさないようにすべきである。

2-3-2　根拠

表 2-4 に示した指針の根拠を以下に示す。

(1) 真正性・完全性保証の方式

[RC-009]を参考に、真正性・完全性保証の方式として電子署名方式及び MAC 方式について検討する。真正性・完全性保証を行うためには、通信情報に電子署名データまたは MAC と、その確認に必要なデータ（例：電子署名方式の場合、公開鍵証明書）を付与する必要があり、これらのデータや処理負荷は方式に拠って異なる。したがって、通信システムにおいて真正性・完全性保証を実現する方式を、データサイズ及び処理負荷の観点から検討した結果を述べる。なお、通信データの真正性・完全性保証を実現する際に、電子署名方式では通信主体間で秘密情報の共有を必要としないのに対し、MAC 方式では通信主体間で暗号鍵を事前共有している必要がある。多通信主体間で通信データの真正性・完全性保証を実現する際、表 2-3 に示すように電子署名方式と MAC 方式では、必要となる暗号鍵の管理負荷が異なっているため、選択した方式に応じ適切な暗号鍵管理を行うべきである。

（ア） 車車間通信

車車間通信において、1 台の車載機が送信する通信情報に付与できる真正性・完全性保証用のデータのサイズを、表 2-1　通信に関する要求条件の No.2,3,6 及び 2-2 節(2)から求めると、最大 26byte 程度となる。電子署名データは MAC に比べて送信するデータのサイズが大きく、公開鍵暗号の中では電子署名データのサイズが小さい ECDSA（鍵長 224bit）の場合でも、電子署名データのサイズは 56byte となる。一方、共通鍵暗号アルゴリズム AES（鍵長 128bit）を用いた場合の MAC のサイズは、最大 16byte になる。したがって、データサイズの観点から車車間通信の真正性・完全性保証には、MAC 方式を用いるべきである。

（イ） 路車間通信

路車間通信において、1 台の路側機が送信する通信情報に付与できる真正性・完全性保証用のデータのサイズを、表 2-1　通信に関する要求条件の No.2,3,6,7 及び 2-2 節(3)から求めると、数百 byte のデータが送信可能である。ただし正確な送信データのサイズは各種パラメータに依存する。2-2 節(5)で述べたとおり、[IEEE 1609.2]では、公開鍵暗号アルゴリ

ズム ECDSA（鍵長 224bit または 256bit）による電子署名と、200byte 程度の公開鍵証明書のフォーマットが定められている。[IEEE 1609.2]の電子署名データと公開鍵証明書のデータサイズは 200byte 強となり、700MHz 帯安全運転支援システムの路車間通信においても送信可能なサイズである。上記（ア）と同様に MAC 方式のデータサイズは最大 16byte であることから､データサイズの観点からは電子署名方式及び MAC 方式の両方式を用いることが可能である。

処理負荷に関しては、一般的に電子署名方式は MAC 方式と比較して車載機及び路側機への処理負荷が大きい。しかし、電子署名方式の処理負荷は、処理対象データが数百 byte オーダーの場合には、データサイズよりも対象となる電子署名処理の回数に大きく依存し、また 100ms 間に路側機が送出するパケット数は[T109]により 1 桁に収まっている。したがって、路車間通信のみに電子署名方式を用いる場合は、処理すべき電子署名データ数が少なくなり車載器への処理負荷が問題となるほどには大きくならないため、電子署名方式を用いることが可能となる。また、2-2 節(1)のとおり路側機はパケットを分割して送信することを想定しているが、分割前のパケットデータ全体を対象とした電子署名を施すことはパケットロス時に署名検証が不可能となり、一方で複数パケットへ単純に電子署名を施すことは電子署名処理の回数増大に繋がり得策ではない。これに対し、各複数パケットの MAC を包含したデータに対し電子署名データを付与すれば、電子署名処理の回数増加を抑えながらパケットロスへの対応を実現することが可能である。

なお、路側機が送出する通信情報は、公的な安全運転支援情報として、車載機が送出する情報よりも信頼性が重視される可能性が高いため、鍵漏洩時の影響範囲を限定する観点から可能な限り電子署名方式を採用すべきである。

以上より、路車間通信の真正性・完全性保証には、電子署名方式と MAC 方式を組み合わせた方式を用いるべきである。

(2) 真正性・完全性保証の対象範囲

[RC-010]で定められている車載機と路側機のアーキテクチャを図 2-1 に示す。通信情報のペイロード情報は、アプリケーションで生成される。表 2-1　通信に関する要求条件の No.5 及び 2-2 節(1)より、電子署名データや MAC の生成及び検証は、レイヤ 7 または EL を介してセキュリティ管理で行われる。したがって、真正性・完全性保証の対象範囲は、通信情報のペイロード情報、及び真正性・完全性検証に必要な情報（例：公開鍵証明書等）とし、通信情報のペイロード情報の前後に、真正性・完全性確認に必要な情報をセキュリティヘッダ情報として、真正性・完全性を示す電子署名データや MAC をセキュリティフッタ情報として付与すべきである（図 2-2)。なお、セキュリティ管理とのアクセスポイントはレイヤ 7 からと拡張機能からの 2 つがある。運用時にどちらのアクセスポイントを使用するかは運用管理機関が指定するものである。

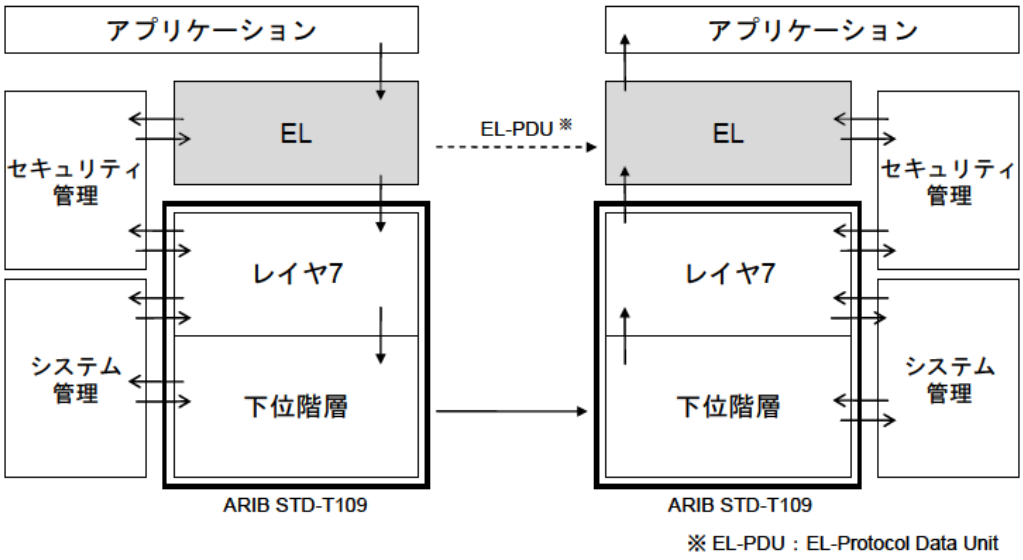

図 2-1　車載器または路側機のアーキテクチャ（出所：[RC-010] 図 2.1）

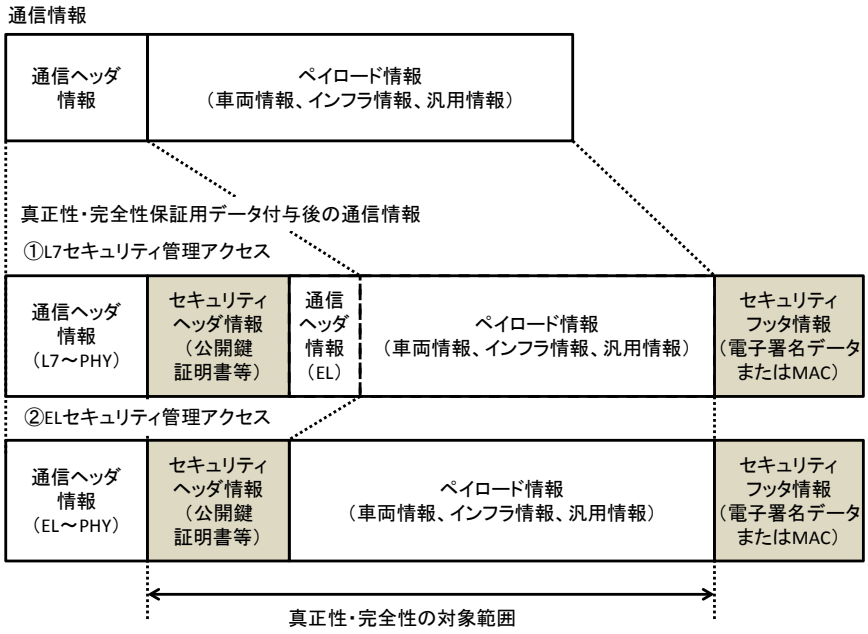

図 2-2　真正性・完全性保証の対象範囲

(3) 機密性維持の方式

一般的に、機密性維持の方式には、共通鍵暗号アルゴリズムを用いた暗号化と公開鍵暗号アルゴリズムを用いた暗号化がある。公開鍵暗号アルゴリズムを用いた暗号化は、共通鍵暗号アルゴリズムを用いた場合より、処理速度が小さい。車車間通信の場合、1 台の車載機の周囲には 100～250 台程度の車載機が存在することを想定しているため、100ms の間に 100～250 回の復号が発生する。したがって、公開鍵暗号アルゴリズムを用いた暗号化は、車載

機への処理負荷が大きくなる。路車間通信の場合も、パケットの分割送信が発生した場合、(2)と同様に、パケットロスが発生しても復号できるように分割したパケット毎に暗号化すると車載機への処理負荷が大きくなる。したがって、処理負荷の観点から 700MHz 帯安全運転支援システムにおける通信情報の機密性維持には、共通鍵暗号アルゴリズムによる暗号化を用いるべきである。なお、[RC-009]においても、通信情報の機密性維持には、車車間通信及び路車間通信ともに、共通鍵暗号アルゴリズムを用いた方式が適していると述べられており、[IEEE 1609.2]においても共通鍵暗号アルゴリズム AES（鍵長 128bit）の CCM モードによる暗号化が定められている。

暗号化された通信情報を復号するために必要な情報（例：共通鍵の識別子）は、通信情報の真正性・完全性保証方式で示したフォーマットに基づいてセキュリティヘッダ情報に加えるべきである。

(4) 暗号化の対象範囲

(2)(3)で述べたとおり、通信情報のペイロード情報の前後にはセキュリティヘッダ情報、及びセキュリティフッタ情報を付与する。したがって、車車間通信及び路車間通信における通信情報の暗号化対象範囲は、通信情報のペイロード情報、及びセキュリティフッタ情報とすべきである。

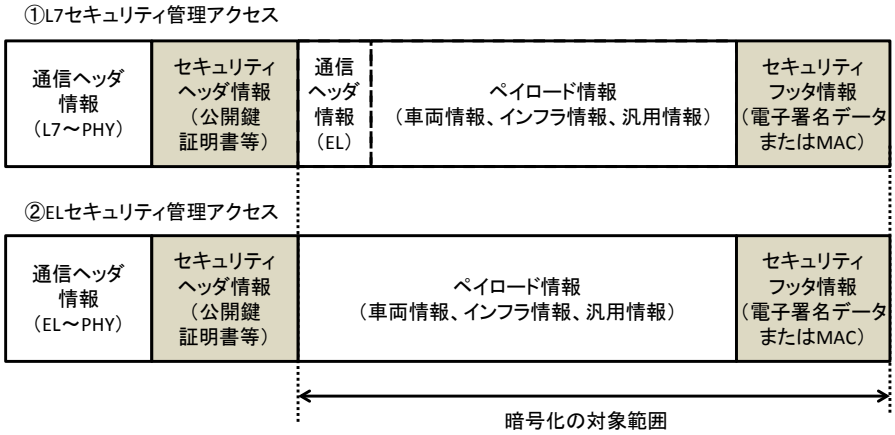

図 2-3　暗号化の対象範囲

(5) 解析防止対策

(1)で述べたとおり、車車間通信の真正性・完全性保証には、共通鍵暗号アルゴリズムによる MAC を適用した方式が用いられるべきである。表 2-1　通信に関する要求条件の No.1 より車車間通信は同報通信であるため、全ての車載機が同じ共通鍵を共有することになる。共通鍵等のセキュリティ情報が漏洩した場合、全ての車載機のセキュリティ情報を更新する必要がある。したがって、車載機メーカ及び路側機メーカは、車載機や路側機からセキュリティ情報が漏洩しないようにできるだけの解析防止対策を実施すべきである。

⑹ セキュリティ情報の更新

(5)で述べたように、車車間通信の真正性・完全性保証では、全ての車載機が同じ共通鍵を共有するため、共通鍵等のセキュリティ情報の管理は非常に重要である。車載機や路側機からのセキュリティ情報漏洩防止に加え、万が一、セキュリティ情報の漏洩発生、またはその疑いがある場合、700MHz 帯安全運転支援システムに悪影響を及ぼさないよう、セキュリティ情報を更新可能とすべきである。また、セキュリティ情報を生成、配布、格納する際にも漏洩が発生しないように対策を実施すべきであり、第 3 章で詳細を述べる。

第3章　セキュリティ情報運用管理システムを構築するための指針

本章では、[要求事項]を満たすセキュリティ情報運用管理システムを構築するためのセキュリティに関する指針を示す。[要求事項]では、運用管理機関及びエンティティ毎に対して要求事項を挙げているが、セキュリティ情報運用管理システムには運用管理機関とエンティティとの連携が必要な機能もあるため、本ガイドラインでは機能毎に指針を示す。3-1 節でセキュリティ情報運用管理システムの構成及び機能を述べ、3-2 節で要求条件を整理する。3-3 節でセキュリティ情報運用管理システムを構築するためのセキュリティに関する指針を示す。

3-1　セキュリティ情報運用管理システムの概要

本節では、[要求事項]で述べられているセキュリティ情報運用管理システムの構成及び機能について述べる。

3-1-1　構成

セキュリティ情報運用管理システムは、通信情報を保護するためのセキュリティ情報の生成、配布、保管、格納等を行うシステムであり、その構成を図 3-1 に示す。まず SAM メーカが SAM メーカ向けセキュリティ情報を運用管理機関から受け取り、SAM に格納し、車載機メーカまたは路側機メーカに SAM を納める。車載機メーカ、路側機メーカは SAM を車載機・路側機に搭載する。次に車載機メーカは車載機メーカ用セキュリティ情報を運用管理機関から受け取り、車載機に搭載した SAM に格納する。車載機メーカと同様に路側機メーカは、路側機メーカ向けセキュリティ情報を運用管理機関から受け取り、路側機に搭載した SAM に格納する。SAM メーカには、運用管理機関から受け取ったセキュリティ情報を管理するセキュリティ管理区域と SAM にセキュリティ情報を書き込む書込区域という専用区域がある。一方、車載機メーカ及び路側機メーカにはセキュリティ管理区域はあるが、書込区域の設置に関する記載はない。

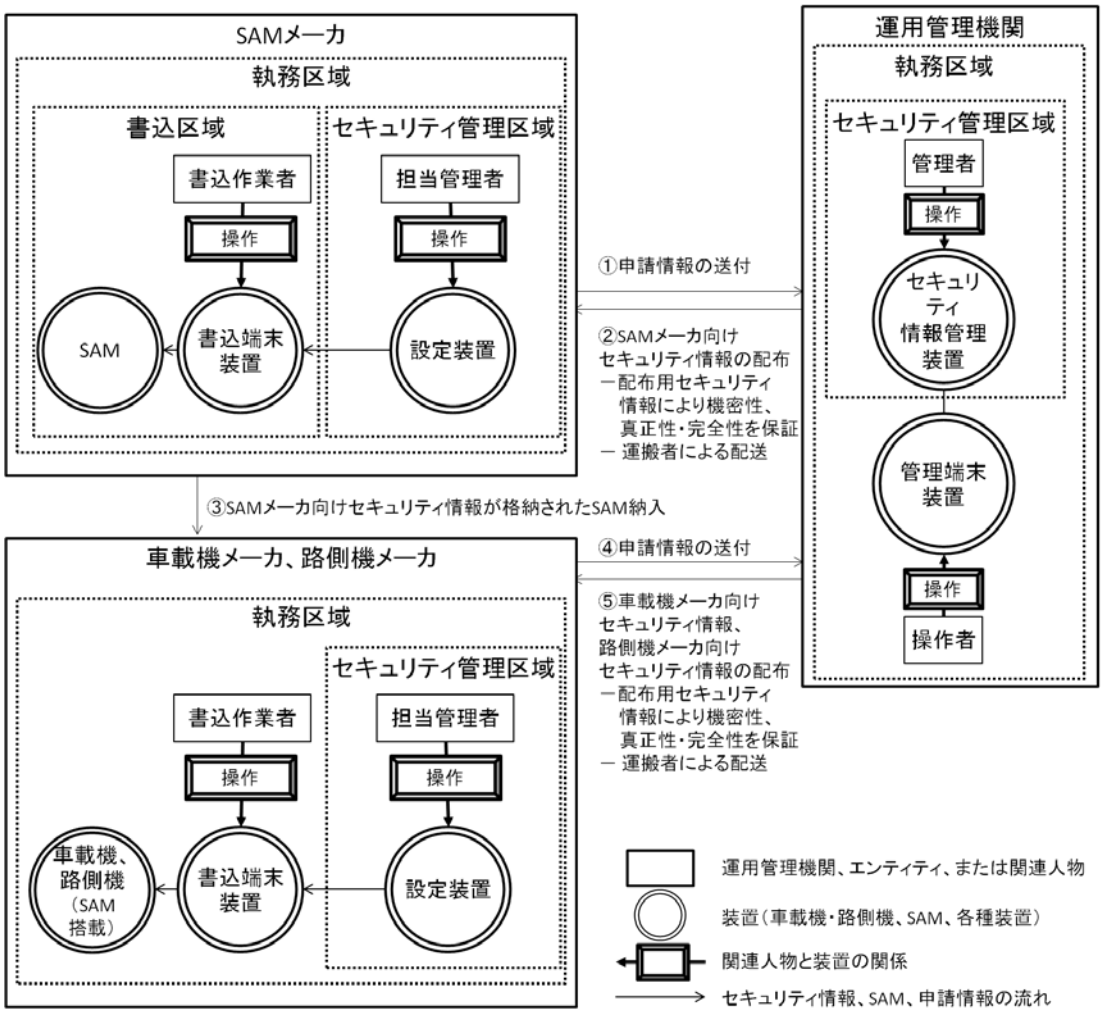

図 3-1　セキュリティ情報運用管理システムの構成（出所：[要求事項]　図 3-1）

3-1-2　機能

セキュリティ情報運用管理システムの機能を(1)～(5)に示す。2-3-2 項(6)で述べられているとおり、セキュリティ情報の管理は非常に重要である。したがって、本ガイドラインではセキュリティ情報の生成、配布、保管及び格納に加えて、万が一、セキュリティ情報が漏洩した場合に備えて、更新及びインシデント対応もセキュリティ情報運用管理システムの機能として記載する。

(1) セキュリティ情報の生成及び保管

運用管理機関はセキュリティ情報を発行する。セキュリティ管理区域にあるセキュリティ情報管理装置でセキュリティ情報は生成される。車載機メーカ、路側機メーカ及び SAM メーカから受け取った申請書類の内容に基づいて、運用管理機関の操作者が執務区域にある管理端末装置から必要な情報を入力し、セキュリティ情報を発行する（図 3-1）。[要求事項]で

は、セキュリティ情報管理装置及び管理端末装置は外部ネットワークに接続しないことが前提となっている。

⑵ セキュリティ情報の配布／受取

運用管理機関は、車載機メーカ、路側機メーカ、及び SAM メーカに(1)で生成したセキュリティ情報を配布する。[要求事項]では、運用管理機関のセキュリティ情報管理装置及び管理端末装置は、外部ネットワークに接続しないことが前提となっているため、セキュリティ情報の配布は郵送または手渡しで行われる。

⑶ セキュリティ情報の保管及び格納

（ア） 車載機メーカ及び路側機メーカ

車載機メーカ及び路側機メーカはセキュリティ情報を車載機または路側機に格納する。運用管理機関から受け取ったセキュリティ情報はセキュリティ管理区域にある設定装置に保存される。車載機または路側機にセキュリティ情報を書き込む場合は、書込作業者が書込端末装置から設定装置にアクセスし、セキュリティ情報を車載機または路側機に格納する（図 3-1)。セキュリティ情報が格納された車載機及び路側機は、車両メーカや公共路側機管理者に納められ、車両への車載機搭載や道路等への路側機設置が行われる。[要求事項]では、設定装置及び書込端末装置は外部ネットワークに接続しないことが前提となっている。

（イ） SAM メーカ

SAM メーカはセキュリティ情報を SAM に格納する。運用管理機関から受け取ったセキュリティ情報はセキュリティ管理区域にある設定装置に保存される。SAM にセキュリティ情報を書き込む場合は、書込作業者が書込端末装置から設定装置にアクセスし、セキュリティ情報を SAM に格納する（図 3-1)。[要求事項]では、設定装置及び書込端末装置は外部ネットワークに接続しないことが前提となっている。

⑷ セキュリティ情報の更新

セキュリティ情報の漏洩発生、もしくはその疑いがある場合、運用管理機関、車載機メーカ、路側機メーカ、及び SAM メーカが連携し、セキュリティ情報を更新する必要がある。[要求事項]では、セキュリティ情報の更新の前提条件については明記されていない。

⑸ インシデント対応

セキュリティ情報の漏洩等のインシデントが発生した場合、その影響を最小限にとどめるため、セキュリティ情報運用管理システムに関わる運用管理機関、車載機メーカ、路側機メーカ、及び SAM メーカが連携し、更には路側機を管理する公共路側管理者、及び車載機を搭載した車両を販売する車両メーカとも連携して、迅速な対応が必要である。[要求事項]の

付録で、インシデント対応の体制及び全体フローが記載されている。

3-2　要求条件

本節では、セキュリティ情報運用管理システムを構築する際に満たさなければならない条件を示す。[要求事項]で挙げられている要求事項のうち、セキュリティ情報運用管理システムの構築に関係するものを表 3-1 に示す。

表 3-1　セキュリティ情報運用管理システムの構築に関する要求条件

要求条件	内容
要求事項 2.3.1 項 通信システムにおける運用管理機関へのセキュリティ要求事項	
要求事項 2.3.1 項⑤	セキュリティ情報の生成 2.3.1 項④で用いるセキュリティ情報は、運用管理機関が適切な方法で生成すること。
要求事項 2.3.1 項⑧	セキュリティ情報の配布 2.3.1 項⑤に基づいて生成したセキュリティ情報を適切な手段で、車載機メーカ、路側機メーカに配布すること。
要求事項 2.3.1 項⑩	インシデント対応体制の構築 セキュリティに関するインシデントが発生した場合に、迅速かつ円滑な対応を可能とするため、車載機メーカ、路側機メーカ及び車両メーカ等の関連するエンティティとの連絡体制や手順を明確にしておくこと。
要求事項 2.3.2 項 通信システムにおける車載機メーカ、路側機メーカ及び車両メーカへのセキュリティ要求事項	
要求事項 2.3.2 項③	マルウェア検知対策 車載機メーカ、路側機メーカ及び車両メーカは、車載機や路側機に接続する機器に対して、マルウェア検知ソフト等の適切なセキュリティ対策を施すこと。
要求事項 2.3.2 項⑤	インシデント対応体制の構築 セキュリティに関するインシデントが発生した場合、運用管理機関と連携し、迅速かつ円滑な対応に努めること。
要求事項 3.3.1.1 項 運用管理機関の執務区域へのセキュリティ要求事項	
要求事項 3.3.1.1 項①	入退室認証 第三者が執務区域に侵入できないようにすること。
要求事項 3.3.1.1 項②	管理端末装置のユーザ認証 操作者以外が管理端末装置を操作できないようにすること。
要求事項 3.3.1.1 項③	管理端末装置認証 管理端末装置以外の端末装置からセキュリティ情報管理装置に接続できないようにすること。
要求事項 3.3.1.1 項④	セキュリティ情報の機密性確保 セキュリティ情報を出力する場合には、適切な暗号アルゴリズムと鍵長を用いて暗号化を実施すること。

要求条件	内容
要求事項 3.3.1.1 項⑤	申請情報の真正性・完全性確認 車載機メーカ、路側機メーカ及び SAM メーカからの申請情報を基にセキュリティ情報を生成する際に、適切な暗号アルゴリズムと鍵長を用いて申請情報の真正性・完全性を確認できること。
要求事項 3.3.1.1 項⑥	否認防止 操作者やシステム管理者が実施した操作を否認できないように努めること。
要求事項 3.3.1.1 項⑦	操作ミスや不正操作の防止 操作者や管理者が、故意もしくは過失による正しくない操作を行わないように複数人での操作確認を行う等の操作ミスや不正操作の防止に努めること。
要求事項 3.3.2 項 運用管理機関のセキュリティ管理区域へのセキュリティ要求事項	
要求事項 3.3.1.2 項①	入退室認証 管理者以外がセキュリティ管理区域に侵入できないようにすること。
要求事項 3.3.1.2 項②	管理端末装置によるセキュリティ情報管理装置の認証 管理端末装置は正しいセキュリティ情報管理装置に接続していることを確認できること。
要求事項 3.3.1.2 項③	セキュリティ情報の機密性確保 管理者がセキュリティ情報管理装置からセキュリティ情報を出力する必要がある場合には、適切な暗号アルゴリズムと鍵長を用いて暗号化を実施すること。
要求事項 3.3.1.2 項④	申請情報の真正性・完全性確認 管理者がセキュリティ情報管理装置から車載機メーカ、路側機メーカ及び SAM メーカからの申請情報を基にセキュリティ情報を生成する必要がある場合には、適切な暗号アルゴリズムと鍵長を用いて申請情報の真正性・完全性を確認できること。
要求事項 3.3.1.2 項⑤	否認防止 管理者が実施した操作を否認できないように努めること。
要求事項 3.3.1.2 項⑥	セキュリティ情報管理装置のプログラム管理 管理者がセキュリティ情報管理装置のプログラムを誤って書き換えないようにすること。不正な書き換えが発覚したときに、書き換えた人物を特定できるようにしておくこと。
要求事項 3.3.1.2 項⑦	操作ミスや不正操作の防止 管理者が故意もしくは過失による正しくない操作を行わないように、複数人での操作確認を行う等の操作ミスや不正操作の防止に努めること。
要求事項 3.3.3 項 セキュリティ情報配布時のセキュリティ要求事項	
要求事項 3.3.1.3 項①	セキュリティ情報の機密性維持 運用管理機関は、運搬者以外にセキュリティ情報を入れた媒体が渡ってもセキュリティ情報が漏洩しないように適切な暗号アルゴリズムと鍵長を用いて暗号化しておくこと。
要求事項 3.3.1.3 項②	セキュリティ情報の真正性・完全性確認

要求条件	内容
	運用管理機関は、車載機メーカ、路側機メーカ及び SAM メーカが、受け取ったセキュリティ情報の真正性及び完全性を適切な暗号アルゴリズムと鍵長を用いて確認できるようにしておくこと。
要求事項 3.3.1.3 項③	運搬者の選定 運用管理機関は、信頼できる運搬者を選定すること。
要求事項 3.3.1.3 項④	否認防止 運用管理機関は、運搬者が運用管理機関からセキュリティ情報を受け取ったことを否認できないようにしておくこと。
要求事項 3.3.1.4 項 インシデント対応への要求条件	
要求事項 3.3.1.4 項	インシデント対応 セキュリティに関するインシデントが発生した場合に、迅速かつ円滑な対応を可能とするため、車載機メーカ、路側機メーカ及び車両メーカ等の関連するエンティティとの連絡体制や手順を明確にしておくこと。
要求事項 3.3.2.1 項 車載機メーカ及び路側機メーカの執務区域への要求条件	
要求事項 3.3.2.1 項①	入退室認証 第三者が執務区域に侵入できないようにすること。
要求事項 3.3.2.1 項②	書込端末装置のユーザ認証 書込作業者以外が書込端末装置を操作できないようにすること。
要求事項 3.3.2.1 項③	書込端末装置の認証 書込端末装置以外が設定装置に接続できないようにすること。
要求事項 3.3.2.1 項④	書込端末装置の管理 書込端末装置が持ち出されたり、不正な装置に置き換えられたりしないこと。
要求事項 3.3.2.1 項⑤	接続に関する前提条件を満たすための対策 書込端末装置は外部ネットワークに接続しないようにすること。また、USB メモリ等を書込端末装置に接続する際にはマルウェア感染等に十分気をつけること。
要求事項 3.3.2.1 項⑥	操作ミスや不正操作の防止 書込作業者が故意もしくは過失による正しくない操作を行わないように、複数人での操作確認を行う等の操作ミスや不正操作の防止に努めること。
要求事項 3.3.2.2 項 車載機メーカ及び路側機メーカのセキュリティ管理区域への要求条件	
要求事項 3.3.2.2 項①	入退室認証 セキュリティ管理区域への入室が認められていない人物が、セキュリティ管理区域に侵入できないようにすること。
要求事項 3.3.2.2 項②	設定装置のユーザ認証 担当管理者以外が設定装置を操作できないようにすること。
要求事項 3.3.2.2 項③	セキュリティ情報の機密性維持 設定装置から書込端末装置以外にセキュリティ情報を出力する必要がある場合には、適切な暗号アルゴリズムと鍵長を用いて暗号化しておくこと。

要求条件	内容
要求事項 3.3.2.2 項④	セキュリティ情報の真正性・完全性確認 設定装置は、運用管理機関から受け取ったセキュリティ情報の真正性及び完全性を適切な暗号アルゴリズムと鍵長を用いて確認できるようにしておくこと。
要求事項 3.3.2.2 項⑤	設定装置の管理 設定装置が持ち出されたり、不正な装置に置き換えられたりしないこと。
要求事項 3.3.2.2 項⑥	操作ミスや不正操作の防止 担当管理者が故意もしくは過失による正しくない操作を行わないように、複数人での操作確認を行う等の操作ミスや不正操作の防止に努めること。
要求事項 3.3.2.3 項 車載機メーカ及び路側機メーカにおけるセキュリティ情報受取時の要求条件	
要求事項 3.3.2.3 項	セキュリティ情報受取時 車載機メーカ及び路側機メーカは、信頼できる運搬者を選定すること。
要求事項 3.3.2.4 項 インシデント対応への要求条件	
要求事項 3.3.2.4 項	インシデント対応 セキュリティに関するインシデントが発生した場合、運用管理機関と連携し、迅速かつ円滑な対応に努めること。
要求事項 3.3.3.1 項 SAM メーカの執務区域への要求条件	
要求事項 3.3.3.1 項①	入退室認証 書込区域への入室が認められていない人物が書込区域に侵入できないようにすること。
要求事項 3.3.3.1 項②	書込端末装置のユーザ認証 書込作業者以外が書込端末装置を操作できないようにすること。
要求事項 3.3.3.1 項③	書込端末装置の認証 書込端末装置以外が設定装置に接続できないようにすること。
要求事項 3.3.3.1 項④	セキュリティ情報の機密性維持 セキュリティ情報を SAM に格納する以外に、書込端末装置からセキュリティ情報を出力する必要がある場合には、適切な暗号アルゴリズムと鍵長で暗号化を実施すること。
要求事項 3.3.3.1 項⑤	書込端末装置の管理 書込端末装置が持ち出されたり、不正な端末装置に置き換えられたりしないこと。
要求事項 3.3.3.1 項⑥	操作ミスや不正操作の防止 書込作業者が故意もしくは過失による正しくない操作を行わないように、複数人での操作確認を行う等の操作ミスや不正操作の防止に努めること。
要求事項 3.3.3.2 項 SAM メーカのセキュリティ管理区域への要求条件	
要求事項 3.3.3.2 項①	入退室認証 セキュリティ管理区域への入室が認められていない人物が、セキ

要求条件	内容
	ュリティ管理区域に侵入できないようにすること。
要求事項 3.3.3.2 項②	設定装置のユーザ認証 担当管理者以外が設定装置を操作できないようにすること。
要求事項 3.3.3.2 項③	セキュリティ情報の機密性維持 設定装置から書込端末装置以外にセキュリティ情報を出力する必要がある場合には、適切な暗号アルゴリズムと鍵長を用いて暗号化しておくこと。
要求事項 3.3.3.2 項④	セキュリティ情報の真正性・完全性確認 設定装置は、運用管理機関から受け取ったセキュリティ情報の真正性及び完全性を適切な暗号アルゴリズムと鍵長を用いて確認できるようにしておくこと。
要求事項 3.3.3.2 項⑤	設定装置の管理 設定装置が持ち出されたり、不正な装置に置き換えられたりしないこと。
要求事項 3.3.3.2 項⑥	接続に関する前提条件を満たすための対策 設定装置は外部ネットワークに接続しないようにすること。また、USB メモリ等を設定装置に接続する際にはマルウェア感染等に十分気をつけること。
要求事項 3.3.3.2 項⑦	操作ミスや不正操作の防止 担当管理者が故意もしくは過失による正しくない操作を行わないように、複数人での操作確認を行う等の操作ミスや不正操作の防止に努めること。
要求事項 3.3.3.3 項 SAM メーカにおけるセキュリティ情報受取時の要求条件	
要求事項 3.3.3.3 項	セキュリティ情報受取時 SAM メーカは、信頼できる運搬者を選定すること。
要求事項 3.3.3.4 項 インシデント対応への要求条件	
要求事項 3.3.3.4 項	インシデント対応 セキュリティに関するインシデントが発生した場合、運用管理機関と連携し、迅速かつ円滑な対応に努めること。

3-3　指針と各機能におけるセキュリティの例示

3-1-1 項で､[要求事項]を満たすセキュリティ情報運用管理システムを構築するためのセキュリティに関する指針を示す。3-3-2 項では、3-3-1 項で示した指針に基づき、セキュリティ情報運用管理システムの各機能におけるセキュリティを例示する。

3-3-1　指針

セキュリティ情報の漏洩等の脅威が発生した場合の影響範囲は広いため、セキュリティ情報の運用管理におけるセキュリティは重要である。脅威は、発生させる人や手段に拠って手順が異なるため、複数の対策を施し、脅威発生を防止すべきである。例えば、脅威は第三者からの

攻撃だけでなく、運用管理機関の操作者のミスにより発生する場合もあるため、攻撃防止への対策だけでなく操作ミス防止の対策も実施すべきである。

3-3-2　指針に基づいた各機能におけるセキュリティの例示

(1) セキュリティ情報の生成及び保管

運用管理機関がセキュリティ情報を発行する場合、セキュリティ情報の配布と同様にセキュリティ情報漏洩や改ざん等の脅威が想定される。[要求事項]で記載されているこれらの脅威への対策を図 3-2 に、その具体的な例を表 3-2 に示す。例えば、「第三者が運用管理機関に侵入し、管理端末装置を使って不正にセキュリティ情報を出力した結果、セキュリティ情報が漏洩する」という脅威に対して、攻撃の最初の手順となる「運用管理機関への侵入」に対しては「入退室認証」という対策で防ぐ。万一、第三者が運用管理機関への侵入に成功した場合においても、次の手順である「管理端末装置の利用」に対して「ユーザ認証」という対策が施されている。さらに「セキュリティ情報の不正出力」に対して「不正操作防止（具体的対策例：承認者の設定)」という対策がある。このように、複数の対策を実施し、脅威発生の機会をできるだけ減らすように努めるべきである。対策の具体的な方法は、運用管理機関がコスト等を考慮した上で判断すべきである。

[要求事項]では、セキュリティ情報管理装置及び管理端末装置は外部ネットワークに接続されていないことを前提としているが、外部ネットワークに接続する必要が出てきた場合（例：車載機普及によるセキュリティ情報の発行機会の増加）は、ネットワークでの対策も検討すべきである。

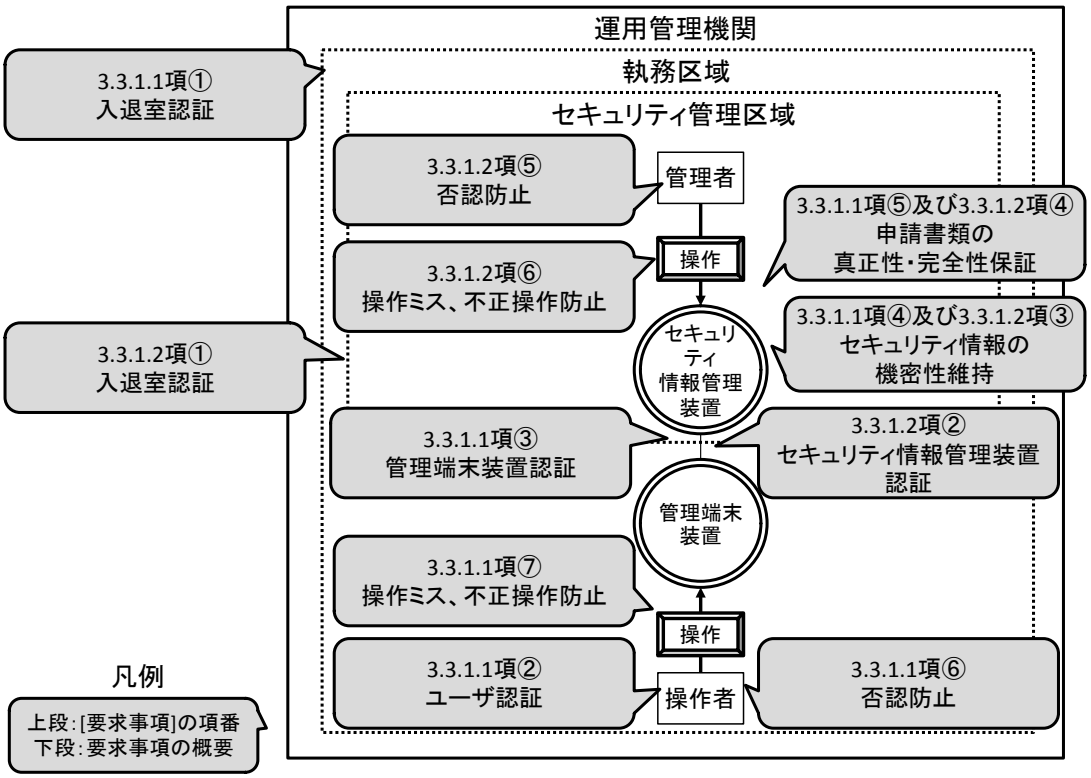

図 3-2　セキュリティ情報生成におけるセキュリティ

表 3-2　セキュリティ情報生成における具体的対策例

要求条件		具体的対策例
3.3.1.1 項① 3.3.1.2 項①	入退室認証	・知識認証（パスワード認証等） ・所有物認証（カード認証等） ・生体認証（静脈認証等） ・認証と監視カメラの組み合わせ
3.3.1.1 項②	ユーザ認証	・知識認証（パスワード認証等） ・所有物認証（カード認証等） ・生体認証（静脈認証等） ・複数の認証の組み合わせ
3.3.1.1 項③ 3.3.1.2 項②	装置認証（管理端末装置認証、セキュリティ情報管理装置認証）	・MAC アドレス認証、 IP アドレス認証 ・電子証明書を用いた認証
3.3.1.1 項④ 3.3.1.2 項③	セキュリティ情報の機密性確保	・セキュリティ情報の暗号化保存 ・セキュリティ情報の外部媒体への出力禁止
3.3.1.1 項⑤ 3.3.1.2 項④	申請書類の真正性・完全性確認	・申請情報への電子署名データ付与
3.3.1.1 項⑥ 3.3.1.2 項⑤	否認防止	・操作ログの記録 ・操作ログと監視カメラの組み合わせ ・操作ログと生体認証の組み合わせ
3.3.1.1 項⑦ 3.3.1.2 項⑦	操作ミスや不正操作の防止	・承認者の設定 ・マニュアルの整備
3.3.1.2 項⑥	セキュリティ情報管理装置のプログラム管理	・複数人による確認 ・プログラムへの電子署名データ付与

⑵ セキュリティ情報の配布／受取

運用管理機関から車載機メーカ、路側機メーカ、及び SAM メーカにセキュリティ情報を配布する場合、セキュリティ情報漏洩や改ざん等の脅威が想定される。[要求事項]で記載されているこれらの脅威への対策を図 3-3 に、その具体的な例を表 3-3 に示す。例えば、「第三者が運搬者になりすまし、セキュリティ情報を入手し、セキュリティ情報の漏洩が発生する」という脅威に対して、「信頼できる運搬者を選定する（運搬者の選定）」という対策で第三者のなりすましを防止し、セキュリティ情報の漏洩を防ぐ。万一、第三者にセキュリティ情報が格納された媒体が渡った場合でも「セキュリティ情報の暗号化（セキュリティ情報の機密性維持）」を実施し、セキュリティ情報が漏洩しないようにする。このように、複数の対策を施し、脅威発生の機会をできるだけ減らすように努めるべきである。対策の具体的な手段は、運用管理機関がコスト等を考慮した上で判断すべきである。

[要求事項]では、外部ネットワークを介したセキュリティ情報配布は、想定されていないが、外部ネットワークを介したセキュリティ情報配布の必要が出てきた場合（例：車載機普及によるセキュリティ情報の発行機会の増加）は、ネットワークでの対策も検討すべきである。

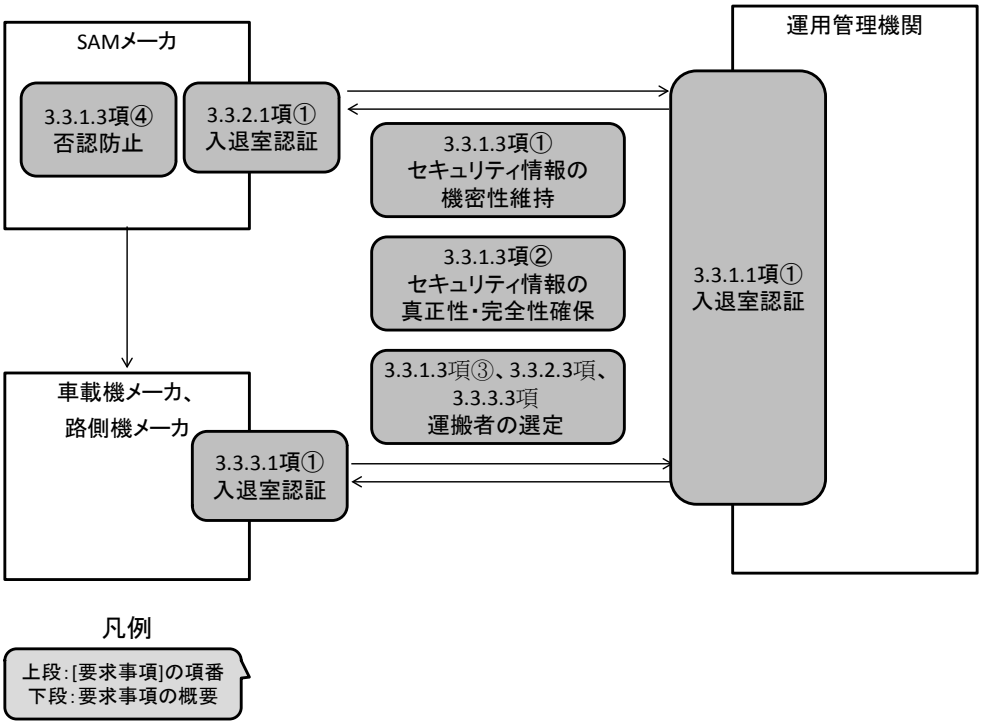

図 3-3　セキュリティ情報の配布／受取におけるセキュリティ

表 3-3　セキュリティ情報の配布／受取における具体的対策例

要求条件		具体的対策例
3.3.1.1 項① 3.3.2.1 項① 3.3.3.1 項①	入退室認証	・知識認証（パスワード認証等） ・所有物認証（カード認証等） ・生体認証（静脈認証等）
3.3.1.3 項①	セキュリティ情報の機密性確保	・セキュリティ情報の暗号化
3.3.1.3 項②	セキュリティ情報の真正性・完全性確保	・セキュリティ情報への電子署名データの付与
3.3.1.3 項③、 3.3.2.3 項、 3.3.3.3 項	運搬者の選定	・信頼できる運搬業者の選定 ・受け取りに行く人の適切な人選と運用管理機関への事前連絡（車載機メーカ、路側機メーカ、及び SAM メーカの人が直接取りに行く場合）
3.3.1.3 項④	否認防止	・配達記録が残る運搬方法の選択 ・運用管理機関への受け取り確認書の送付

⑶ セキュリティ情報の保管及び格納

（ア） 車載機メーカ及び路側機メーカ

車載機メーカ及び路側機メーカがセキュリティ情報を格納する場合においても、セキュリティ情報の配布／受取と同様にセキュリティ情報漏洩や改ざん等の脅威が想定される。[要求事項]で記載されているこれら脅威への対策を図 3-4 に、その具体的な例を表 3-4 に示す。例えば、「第三者が車載機メーカに侵入し、管理端末装置を使って不正なセキュリティ情報を格納した結果、不正なセキュリティ情報が格納された車載機が出回り、正しい安全運転支援サービスを受けられない」という脅威に対して、攻撃の最初の手順となる「車載機メーカへの侵入」に対しては「入退室認証」という対策で防ぐ。万一、第三者が車載機メーカへの侵入に成功した場合でも、次の手順である「管理端末装置の利用」に対して「ユーザ認証」や「装置の管理」という対策が施されている。更に「不正なセキュリティ情報の格納」に対して「セキュリティ情報の真正性・完全性確保」という対策もある。このように、複数の対策を施し、脅威発生の機会をできるだけ減らすように努めるべきである。対策の具体的な方法は、車載機メーカや路側機メーカがコスト等を考慮した上で判断すべきである。

なお、車載機が車両に搭載されて販売される場合においては、車両メーカは、車載機の保管及び取付けにおけるリスク（例：車両への車載機の不正な取付け）を理解するとともに、適切なセキュリティを実施すべきである。また、公共路側機管理者は、設置及び保守時等の路側機の管理におけるリスクを理解するとともに、適切なセキュリティ（例：路側機の物理的保護等）を実施すべきである。[要求事項]では、設定装置及び書込端末装置は外部ネットワークに接続されていないことを前提としているが、外部ネットワークに接続する必要が出てきた場合（例：ネットワークを介したセキュリティ情報の配布）は、ネットワークでの対策も検討すべきである。

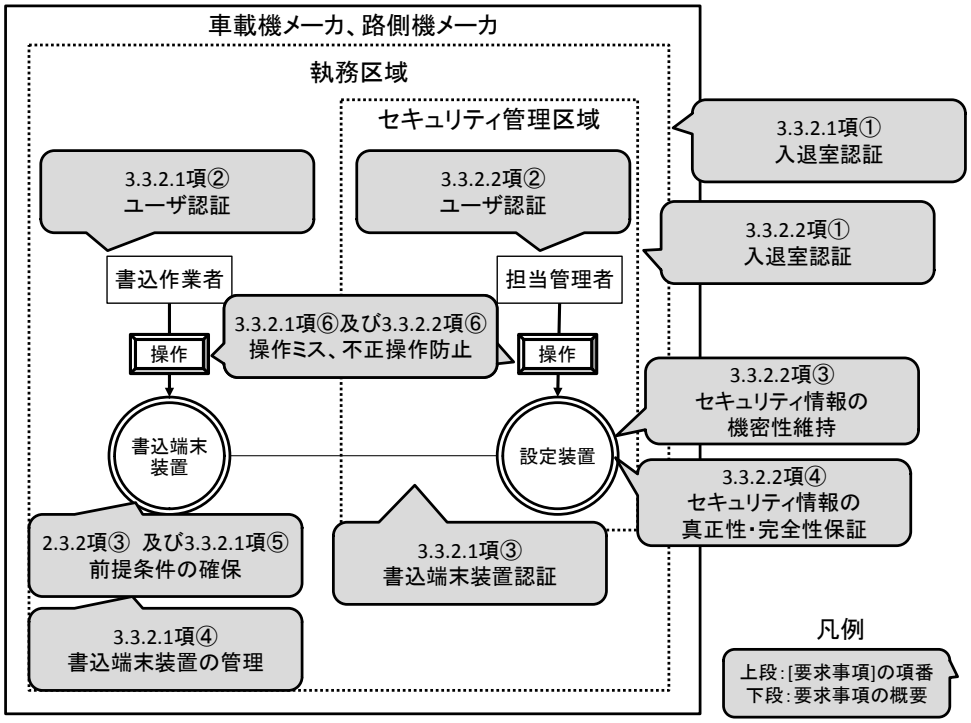

図 3-4　車載機メーカ及び路側機メーカにおけるセキュリティ情報格納のセキュリティ

表 3-4　車載機メーカ及び路側機メーカにおけるセキュリティ情報格納の具体的対策例

要求条件		具体的対策例
3.3.2.1 項①、 3.3.2.2 項①	入退室認証	・知識認証（パスワード認証等） ・所有物認証（カード認証等） ・生体認証（静脈認証等） ・認証と監視カメラの組み合わせ
3.3.2.1 項②、 3.3.2.2 項②	ユーザ認証	・知識認証（パスワード認証等） ・所有物認証（カード認証等） ・生体認証（静脈認証等） ・複数の認証の組み合わせ
3.3.2.1 項⑥、 3.3.2.2 項⑦	操作ミスや不正操作の防止	・承認者の設定 ・マニュアルの整備
3.3.2.1 項③	書込端末装置の認証	・MAC アドレス認証、 IP アドレス認証 ・電子証明書を用いた認証
3.3.2.1 項④、 3.3.2.2 項⑤	装置の管理	・施錠付きエリアでの保管
2.3.2 項③、 3.3.2.2 項⑥	接続に関する前提条件を満たす対策	・外部ネットワークへの接続禁止 ・マルウェア検知 ・接続機器の制限
3.3.1.1 項④、 3.3.1.2 項③	セキュリティ情報の機密性確保	・セキュリティ情報の暗号化保存 ・セキュリティ情報の外部媒体への出力禁止
3.3.1.1 項⑤、 3.3.1.2 項④	セキュリティ情報の真正性・完全性確認	・セキュリティ情報への電子署名データ付与

（イ） SAM メーカ

SAM メーカがセキュリティ情報を格納する場合においても、セキュリティ情報の配布／受取と同様にセキュリティ情報漏洩や改ざん等の脅威が想定される。[要求事項]に記載されているこれらの脅威への対策を図 3-5 に、その具体的対策例を表 3-5 に示す。例えば、「第三者が SAM メーカに侵入し、書込端末装置から設定装置にアクセスし、セキュリティ情報を入手した結果、セキュリティ情報が漏洩する」という脅威に対して、攻撃の最初の手順となる「SAM メーカへの侵入」に対しては「入退室認証」という対策で防ぐ。万一、第三者が SAM メーカへの侵入に成功した場合でも、次の手順である「管理端末装置の利用」に対して「ユーザ認証」や「装置の管理」という対策が施されている。更に「セキュリティ情報の入手」には「セキュリティ情報の機密性確保」が施されているため、セキュリティ情報が容易に漏洩することはない。このように、複数の対策を施し、脅威発生の機会をできるだけ減らすように努めるべきである。対策の具体的な方法は、SAM メーカがコスト等を考慮した上で十分に検討すべきである。

[要求事項]では、設定装置及び書込端末装置は外部ネットワークに接続されていないことを前提としているが、外部ネットワークに接続する必要が出てきた場合（例：ネットワークを介したセキュリティ情報の配布）は、ネットワークでの対策も検討すべきである。

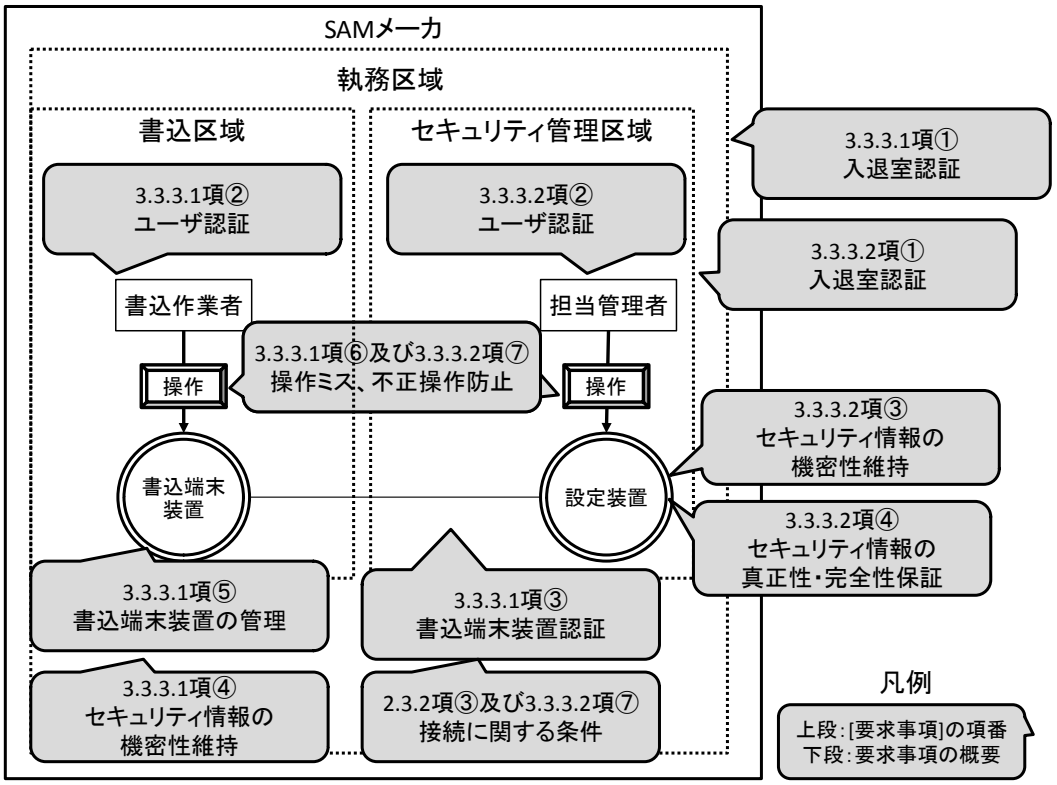

図 3-5 SAM メーカのセキュリティ情報格納におけるセキュリティ

表 3-5　SAM メーカのセキュリティ情報格納における具体的対策例

要求条件		具体的対策例
3.3.3.1 項①、 3.3.3.2 項①	入退室認証	・知識認証（パスワード認証等） ・所有物認証（カード認証等） ・生体認証（静脈認証等） ・認証と監視カメラの組み合わせ
3.3.3.1 項②、 3.3.3.2 項②	ユーザ認証	・知識認証（パスワード認証等） ・所有物認証（カード認証等） ・生体認証（静脈認証等） ・複数の認証の組み合わせ
3.3.3.1 項⑥、 3.3.2.2 項⑦	操作ミスや不正操作の防止	・承認者の設定 ・マニュアルの整備
3.3.3.1 項③	書込端末装置の認証	・MAC アドレス認証、 IP アドレス認証 ・電子証明書を用いた認証
3.3.3.1 項④、 3.3.3.2 項⑤	装置の管理	・施錠付きエリアでの保管
2.3.2 項③ 3.3.3.2 項⑥	接続に関する前提条件を満たす対策	・外部ネットワークへの接続禁止 ・マルウェア検知 ・接続機器の制限
3.3.1.1 項④、 3.3.1.2 項③	セキュリティ情報の機密性確保	・セキュリティ情報の暗号化保存 ・セキュリティ情報の外部媒体への出力禁止
3.3.1.1 項⑤、 3.3.1.2 項④	セキュリティ情報の真正性・完全性確認	・セキュリティ情報への電子署名データの付与

(4) セキュリティ情報の更新

セキュリティ情報の漏洩発生、もしくはその疑いがある場合、セキュリティ情報を更新する必要がある。

郵送または手渡し等のネットワーク以外の方法で配布する場合、運用管理機関、車載機メーカ、路側機メーカ、及び SAM メーカはセキュリティ情報の配布と受け取りと同様にセキュリティ情報漏洩や改ざん等への対策を十分に検討すべきである。ネットワークを介して配布する場合、不正アクセスやマルウェア感染等による情報漏洩や改ざん、DoS 攻撃等による配布不可への対策を十分に検討すべきである。

書込端末装置を用いてセキュリティ情報を更新する場合、車載機メーカ、路側機メーカ及び SAM メーカはセキュリティ情報の格納と同様にセキュリティ情報漏洩や改ざん等への対策を十分に検討すべきである。ただし、入退室認証の実現が難しい環境下でのセキュリティ情報更新を行なう場合には、書込端末装置を第三者に触れさせないように書込端末装置の管理を十分に行うべきである。700MHz 帯通信等通信を介して更新する場合、なりすまし等による情報漏洩や改ざん等への対策を十分に検討すべきである。

(5) インシデント対応

セキュリティを施してもインシデントが発生する可能性は残るため、以下のことを十分に

考慮した上で、運用管理機関と公共路側機管理者、車両メーカ、車載機メーカ、路側機メーカ、及び SAM メーカは相互に連携し、インシデント対応体制の構築や対応手順の整備を行うべきである（[要求事項]2.3.1 項⑩、2.3.2 項⑤、3.3.1.4 項、3.3.2.4 項、3.3.3.4 項）。

- ✓ 迅速なインシデント対応を可能とするために、想定可能なインシデントは事前に明確化した上で対応手順を策定すべきである（[要求事項]付録 A.1）。
- ✓ 運用管理機関と、公共路側機管理者、車両メーカ、車載機メーカ、路側機メーカ、及び SAM メーカはセキュリティ事象の報告を相互に行い、適切な連絡経路を通して、できるだけ速やかに情報共有を図る体制を整えるべきである。さらに、運用管理機関等は、上記関係者以外のドライバーからもセキュリティ事象の報告を受ける体制を整えるべきである（[要求事項]付録 A.2）。
- ✓ 運用管理機関、公共路側機管理者、車両メーカ、車載機メーカ、路側機メーカ、及び SAM メーカは相互に連携し、システムもしくはサービスの中で発見した、または疑いをもったセキュリティ上の弱点について、どのようなものでも記録し、報告するように要求するべきである（[要求事項]付録 A.2）。
- ✓ 運用管理機関等は、検知、初期対応、回復及び事後対応で実施するインシデント対応手順、及びインシデント管理台帳や報告書のフォーマット等を定め、その手順やフォーマットに従ったインシデント対応をとるべきである。更に、検知においては、セキュリティ事象・インシデントの分類基準を定め、その基準に基づいて収集したセキュリティ事象を評価し、インシデントに分類するか否かを決定するべきである。初期対応や回復においても、証拠となり得る情報の特定、収集、取得、及び保存のための手順を定め、その手順を適用するべきである（[要求事項]付録 A.3）。

運用管理機関等は上記に加えて、事後対応終了後には、インシデントの分析及び解決から得られた知識を、インシデントが将来起こる可能性またはその影響を低減するために用いるべきである。

(6) その他

セキュリティ情報運用管理システムにより発行されたセキュリティ情報が、然るべき車載機または路側機に格納されていることを担保することも重要である。運用管理機関、公共路側機管理者、車両メーカ、車載機メーカ、路側機メーカ及び SAM メーカは相互に連携し、上記の担保が確実に行われるよう対策を検討すべきである。また、車載機は車両に搭載された状態で販売されるだけでなく、図 1-2 に示されるドライバーや車載機保有者へ直接販売される場合があることに十分に留意すべきである。

付録 I

本付録では、[要求事項]で挙げられた各要求事項と本ガイドラインとの対応関係を示す。[要求事項]の通信システムへのセキュリティ要求事項との対応関係を表 I-1 に、セキュリティ情報運用管理システムへのセキュリティ要求事項との対応関係を表 I- 2 に示す。

表 I-1 [要求事項] 第 2 章　通信システムへのセキュリティ要求事項

[要求事項]		本ガイドラインでの記載箇所
2.3.1 項　運用管理機関への要求事項		―
①	発信元の真正性確認	2-3 節
②	通信情報の完全性確認	2-3 節
③	通信情報の機密性維持	2-3 節
④	「発信元の真正性確認」「通信情報の完全性確認」「通信情報の機密性維持」の実現方式	2-3 節
⑤	セキュリティ情報の生成	3-3-2 項(1)
⑥	セキュリティ情報の更新	2-3 節、3-3-2 項(4)
⑦	セキュリティ仕様書の作成・管理	－
⑧	セキュリティ情報の配布	3-3-2 項(2)
⑨	セキュリティ管理体制の構築	－
⑩	インシデント対応体制の構築	3-3-2 項(5)
2.3.2 項　車載機メーカ、路側機メーカ及び車両メーカへの要求事項		―
①	セキュリティ機能の実現	－
②	解析防止対策	2-3 節
③	マルウェア検知対策	3-3-2 項(3)
④	セキュリティ仕様書の管理	－
⑤	インシデント対応体制の構築	3-3-2 項(5)

表 I- 2 ［要求事項］ 第 3 章　セキュリティ情報運用管理システムへのセキュリティ要求事項

［要求事項］		本ガイドラインでの記載箇所
3.3.1 項　運用管理機関へのセキュリティ要求事項		―
3.3.1.1 項　運用管理機関の執務区域への要求事項		―
①	入退室認証	3-3-2 項(1)
②	管理端末装置のユーザ認証	3-3-2 項(1)
③	管理端末装置認証	3-3-2 項(1)
④	セキュリティ情報の機密性確保	3-3-2 項(1)
⑤	申請情報の真正性・完全性確認	3-3-2 項(1)
⑥	否認防止	3-3-2 項(1)
⑦	操作ミスや不正操作の防止	3-3-2 項(1)
3.3.1.2 項　セキュリティ管理区域への要求事項		―
①	入退室認証	3-3-2 項(1)
②	管理端末装置によるセキュリティ情報管理装置の認証	3-3-2 項(1)
③	セキュリティ情報の機密性確保	3-3-2 項(1)
④	申請情報の真正性・完全性確認	3-3-2 項(1)
⑤	否認防止	3-3-2 項(1)
⑥	セキュリティ情報管理装置のプログラム管理	3-3-2 項(1)
⑦	操作ミスや不正操作の防止	3-3-2 項(1)
3.3.1.3 項　セキュリティ情報配布時の要求事項		―
①	セキュリティ情報の機密性維持	3-3-2 項(2)
②	セキュリティ情報の真正性・完全性確認	3-3-2 項(2)
③	運搬者の選定	3-3-2 項(2)
④	否認防止	3-3-2 項(2)

[要求事項]			本ガイドラインでの記載箇所
	3.3.1.4 項　インシデント対応への要求事項		3-3-2 項(5)
3.3.2 項　車載機メーカ、路側機メーカへの要求事項			―
	3.3.2.1 項　執務区域への要求事項		3-3-2 項(3)の（ア）
	①	入退室認証	3-3-2 項(3)の（ア）
	②	書込端末装置のユーザ認証	3-3-2 項(3)の（ア）
	③	書込端末装置の認証	3-3-2 項(3)の（ア）
	④	書込端末装置の管理	3-3-2 項(3)の（ア）
	⑤	接続に関する前提条件を満たすための対策	3-3-2 項(3)の（ア）
	⑥	操作ミスや不正操作の防止	3-3-2 項(3)の（ア）
	3.3.2.2 項　セキュリティ管理区域への要求事項		―
	①	入退室認証	3-3-2 項(3)の（ア）
	②	設定装置のユーザ認証	3-3-2 項(3)の（ア）
	③	セキュリティ情報の機密性維持	3-3-2 項(3)の（ア）
	④	セキュリティ情報の真正性・完全性確認	3-3-2 項(3)の（ア）
	⑤	設定装置の管理	3-3-2 項(3)の（ア）
	⑥	操作ミスや不正操作の防止	3-3-2 項(3)の（ア）
	3.3.2.3 項　セキュリティ情報受取時の要求事項		3-3-2 項(2)
	3.3.2.4 項　インシデント対応への要求事項		3-3-2 項(5)
3.3.3 項　SAM メーカへの要求事項			―
	3.3.3.1 項　執務区域への要求事項		3-3-2 項(3)の（イ）
	①	入退室認証	3-3-2 項(3)の（イ）
	②	書込端末装置のユーザ認証	3-3-2 項(3)の（イ）
	③	書込端末装置の認証	3-3-2 項(3)の（イ）

[要求事項]			本ガイドラインでの記載箇所
	④	セキュリティ情報の機密性維持	3-3-2 項(3)の（イ）
	⑤	書込端末装置の管理	3-3-2 項(3)の（イ）
	⑥	操作ミスや不正操作の防止	3-3-2 項(3)の（イ）
	3.3.3.2 項　セキュリティ管理区域への要求事項		―
	①	入退室認証	3-3-2 項(3)の（イ）
	②	設定装置のユーザ認証	3-3-2 項(3)の（イ）
	③	セキュリティ情報の機密性維持	3-3-2 項(3)の（イ）
	④	セキュリティ情報の真正性・完全性確認	3-3-2 項(3)の（イ）
	⑤	設定装置の管理	3-3-2 項(3)の（イ）
	⑥	接続に関する前提条件を満たすための対策	3-3-2 項(3)の（イ）
	⑦	操作ミスや不正操作の防止	3-3-2 項(3)の（イ）
	3.3.3.3 項　セキュリティ情報受取時の要求事項		3-3-2 項(2)
	3.3.3.4 項　インシデント対応への要求事項		3-3-2 項(5)