（別紙）

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

平成 26 年 6 月 20 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 26 年 6 月 20 日	策定	新規策定	

目次

第1章　一般事項

1.1　概要

本書は、700MHz 帯安全運転支援システムが提供するサービスの信頼性確保に必要となるセキュリティのうち、通信システムのセキュリティに関する基本方針及び要求事項を示す。また、要求事項の１つである通信情報の機密性維持、真正性及び完全性確認に必要となるセキュリティ情報の生成、発行、配布、保管等の管理・運用を実施するセキュリティ情報運用管理システムのセキュリティに関する基本方針及び要求事項を示す。700MHz 帯安全運転支援システムの構築・運用に関わるエンティティ、すなわち運用管理機関と車載機メーカ、路側機メーカ、車両メーカ等は、ここで規定するセキュリティ要求事項を遵守する必要がある。

1.2　適用範囲

本書は、700MHz 帯安全運転支援システムの通信システム、及びセキュリティ情報運用管理システムにおけるセキュリティに関わる基本方針及び要求事項を規定する。

また、これらの基本方針及び要求事項は、700MHz 帯安全運転支援システムの構築・運用に関わるエンティティ、すなわち運用管理機関と車載機メーカ、路側機メーカ、車両メーカ等を対象として適用されるものである。

1.3　参照資料

本書で参照した規則、規格等は以下のとおりである。

[1] “無線設備規則”, 総務省

[2] “ITS FORUM RC-008 1.0 版, 運転支援通信システムに関する運用管理ガイドライン” ITS FORUM

[3] “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

[4] “ARIB STD-T109 1.1 版, 700MHz 帯高度道路交通システム 標準規格” ARIB

[5] “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

1.4 用語及び略語

本書で使用する用語及び略語の定義を表 1-1 に示す。

表 1-1 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（参照資料[1]）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。

用語・略語	定義
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。
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。
電子証明書	電子署名を生成する際に用いる鍵の真正性及び完全性を保証するもの。
電子署名	情報の真正性及び完全性を保証するもの。
路側機メーカ	路側機を製造する会社。
DoS	Denial of Service の略。
ECU	Electronic Control Unit の略。
HMI	Human Machine Interface の略。
ID	Identifier の略。
IP アドレス	Internet Protocol アドレスの略。
I/F	Interface の略。
MAC アドレス	Media Access Control アドレスの略。
NW	Network の略。
PW	Password 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。

1.5 700MHz 帯安全運転支援システムの構成

700MHz 帯安全運転支援システムの構成を図 1-1 に示す。

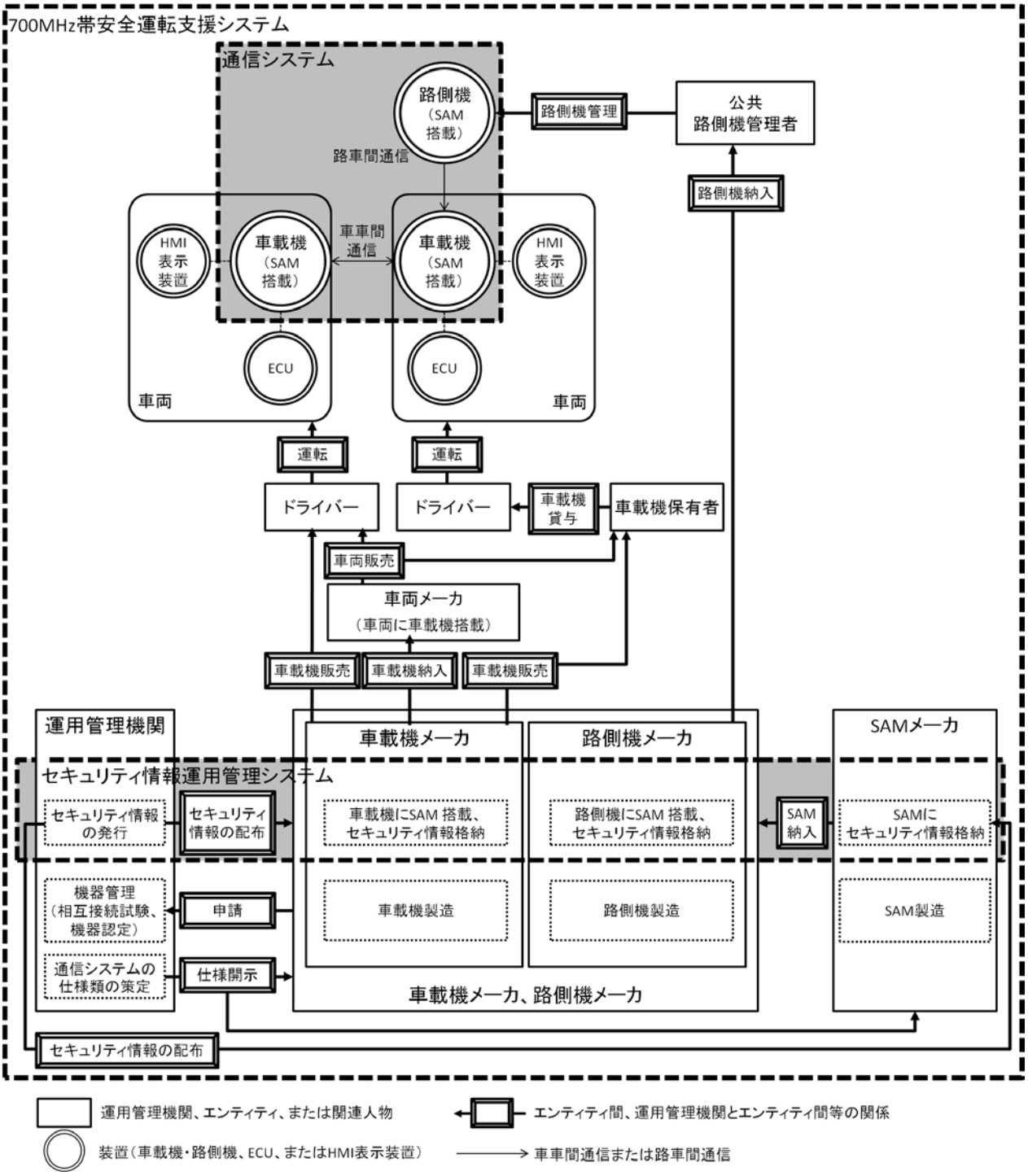

図 1-1　700MHz 帯安全運転支援システムの構成

700MHz 帯安全運転支援システムは、車載機や路側機が車車間通信や路車間通信を行い、車両情

報の送受信やインフラ情報の送受信を行う通信システムを用いて、サービス提供者がドライバーに安全運転支援サービスを提供する。運用管理機関は、700MHz 帯安全運転支援システムの運用に必要となる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。通信システムの仕様類の策定では、通信システムで車載機や路側機が送受信するメッセージのフォーマットやセキュリティ仕様等を策定する。機器管理では、車載機や路側機の相互接続性確認や認定等を行う。セキュリティ情報の運用管理では、セキュリティ仕様を実現する際に必要となるセキュリティ情報の生成、配布、保管、管理等の運用管理を行う。

本書では、第2章で通信システムのセキュリティを実現するために運用管理機関及びエンティティに要求する事項を、第 3 章で安全なセキュリティ情報の運用管理を行うために運用管理機関及びエンティティに要求する事項を述べる。

第2章　通信システムにおけるセキュリティ要求事項

本章では、700MHz 帯安全運転支援システムにおける通信システムの概要と、700MHz 帯安全運転支援システムが提供するサービスの信頼性確保のためのセキュリティに関する基本方針を示す。また、基本方針に基づいたセキュリティ実現のために、700MHz 帯安全運転支援システムの構築・運用に関わる運用管理機関及びエンティティに対して要求する事項について述べる。

2.1　通信システムの概要

2.1.1　システム構成と役割

2.1.1.1　　システム構成

700MHz 帯安全運転支援システムにおける通信システムの構成を図 2-1 に示す。車載機から車載機、もしくは路側機から車載機へ 700MHz 帯通信（通信規格については参照資料[4][5]参照）を用いて車両情報やインフラ情報が送信される。

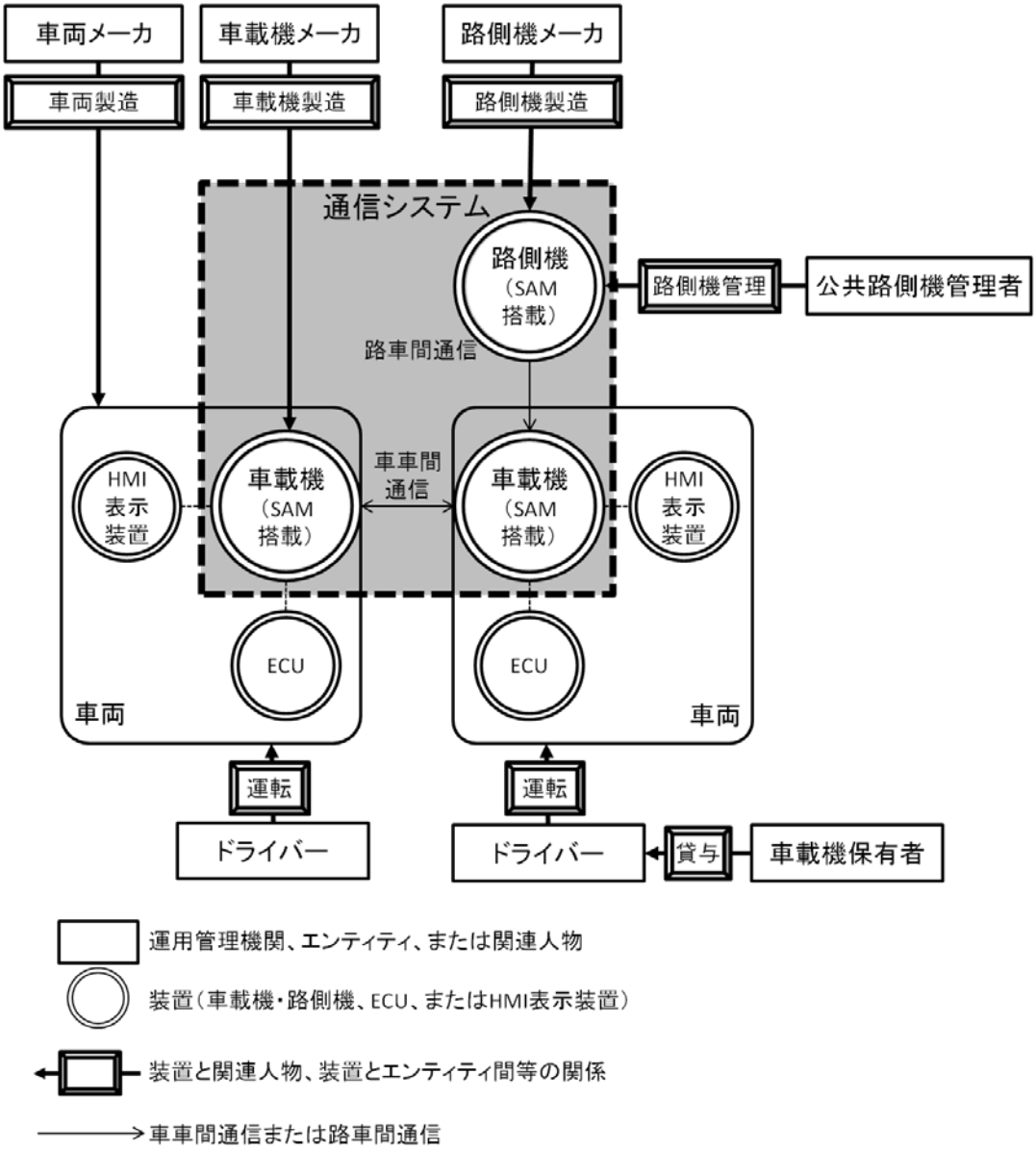

図 2-1　通信システムの構成

2.1.1.2　　構成要素の役割

図 2-1 で示したシステムの構成要素の役割を表 2-1 に示す。

表 2-1　構成要素の役割

構成要素	主な役割
車載機	他の車両また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、以下の機能の一部また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機を指す。
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、通信エリア内に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ことをいう。特に、本システム用の登録済みの路側機を指す。

2.1.1.3　関連人物の役割

図 2-1 で示したシステムの関連人物の役割を表 2-2 に示す。

表 2-2　関連人物の役割

関連人物	役割
車載機保有者	車載機を保有する。
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。

2.1.2　通信システムを用いて提供するサービスの概要

2.1.1 項で述べた通信システムを用いて提供するサービスは、安全運転支援サービスであり、具体的なサービス例を表 2-3 に示す。

表 2-3　対象サービス例

No.	通信対象	サービス名称
1-1	車車間	左折時衝突防止
1-2		右折時衝突防止
1-3		出会い頭衝突防止
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）
1-5		追突防止
1-6		緊急車両情報提供
2-1	路車間	出会い頭衝突防止
2-2		右折時衝突防止
2-3		左折時衝突防止
2-4		追突防止
2-5		歩行者横断見落とし防止
2-6		信号見落とし防止
2-7		一時停止規制見落とし防止

上記サービスは、“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（参照資料[3]）を参照した。

1.　車車間通信における安全運転支援サービス

(1-1) 左折時衝突防止

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ーに提供する。

(1-2) 右折時衝突防止

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ーに提供する。

(1-3) 出会い頭衝突防止（双方一時停止規制無し、郊外道路）

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ーに提供する。

(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）

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ーに提供する。

(1-5) 追突防止

見通しが悪い場所等において、前方の低速走行また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ーに提供する。

(1-6) 緊急車両情報提供

緊急車両の緊急時の情報を周辺にいる車両のドライバーに提供する。

2. 路車間通信における安全運転支援サービス

(2-1) 出会い頭衝突防止

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ーに提供する。

(2-2) 右折時衝突防止

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ーに提供する。

(2-3) 左折時衝突防止

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ーに提供する。

(2-4) 追突防止

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ーに提供する。

(2-5) 歩行者横断見落とし防止

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ーにその情報を提供する。

(2-6) 信号見落とし防止

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の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ーに提供する。

(2-7) 一時停止規制見落とし防止

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ーに提供する。

2.1.3 保護資産

保護資産は、路側機が車載機に送信する通信情報、及び車載機が路側機や他の車載機に送信する通信情報である。通信情報は、通信ヘッダ情報とペイロード情報で構成される。ペイロード情報は3種類ある。具体的な保護資産を表 2-4 に記す。

表 2-4　保護資産

保護資産			概要
通信情報	通信ヘッダ情報		通信を管理するための情報（例：路側機の送信時間割当）。
	ペイロード情報	インフラ情報	路側機が送信し、車載機が受信する情報。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	車載機が送信し、他の車載機が受信する情報。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	路側機が送信し、車載機が受信する情報、または車載機が送信し、他の車載機が受信する情報。内容は車載機または路側機ごとに任意に設定される。

2.1.4　前提条件

安全運転支援サービスと、車載機及び路側機に関する前提条件を記す。

(1) 安全運転支援サービスに関する前提条件

- 表 1-1 で定義したとおり、安全運転支援サービスは、ドライバーに対して情報提供・注意喚起を行うものである。
- サービス提供者は以下を実施しているものとする。
  - 通信途絶の可能性や位置誤差の影響をあらかじめ考慮して設計を行う。
  - 利用者が理解しやすく、過信や不信を招かないように支援タイミングや伝達方法を工夫する。
  - その他、保護資産が攻撃を受けることを想定し、必要に応じてフェールセーフ対策を行う（例：明らかに異常な値の情報はサービスに利用しない）。
  - 車載機保有者及びドライバーが、以下に挙げるシステムの機能限界やドライバーの責任を理解して使用できるように配慮する。
    - ✧　システム非搭載の車両や歩行者が存在している可能性があること。
    - ✧　通信の信頼性を 100%とすることは技術的に困難であること。
    - ✧　システムによる支援の有無に限らず、ドライバーには安全運転義務があること。

(2) 車載機及び路側機に関する前提条件

- 運用管理機関が認定した車載機及び路側機を本システムの正当な装置とする。
- 車載機や路側機が 700MHz 帯安全運転支援システムにおける通信システム以外の通信 I/F を有している場合、その通信路の安全性は保証されているものとする。

2.2　セキュリティに関する基本方針

運用管理機関と、車載機メーカ、路側機メーカ、車両メーカ、及び公共路側機管理者等の通信シ

ステムの構築・運用に関わるエンティティが従うべき基本方針は以下のとおりである。

- セキュリティ管理体制の構築
  セキュリティ管理体制を構築し、セキュリティの維持・向上に努める。
- 法令・規範の遵守
  法令及びその他の規範を遵守する。
- 通信情報の保護
  保護資産である通信情報に対して、セキュリティの三大要素である機密性、完全性、可用性の観点からリスク評価を行い、その結果に基づいた適切な対策を実施する。
- インシデントへの対応
  セキュリティに関するインシデントが発生した場合は、運用管理機関及び関連するエンティティが連携し、適切な対策を速やかに行う。
- 見直し及び改善
  前提条件の変化、サービス内容の変化、社会的変化、技術的変化、法令等の変更等に応じた適切な対策を実施し、セキュリティの維持・向上に努める。

2.3 セキュリティ要求事項

運用管理機関、車載機メーカ、路側機メーカ、車両メーカ等の通信システムの構築・運用に関わるエンティティは、2.3.1～2.3.2 項に示すセキュリティ要求事項に従う必要がある。

2.3.1 運用管理機関へのセキュリティ要求事項

運用管理機関が通信システムのセキュリティを実現する際の要求事項を以下に示す。

【技術面】

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。

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。

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。

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。

⑤ セキュリティ情報の生成

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。

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。

【運用面】

⑦ セキュリティ仕様書の作成・管理

上記の要求事項①～⑥を実現するためのセキュリティ仕様書を作成し、適切な車載機メーカ及び路側機メーカに開示すること。適切な車載機メーカ及び路側機メーカとは、2.3.2 項のセキュリティ要求事項を実現していることが確認できるメーカを指す。また、運用管理機関は、前提条件の変化、サービス内容の変化、社会的変化、技術的変化、法令等の変更等に伴い、セキュリティ仕様書を見直す必要がある。

⑧ セキュリティ情報の配布

上記の要求事項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。

⑨ セキュリティ管理体制の構築

運用管理機関は上記の要求事項①～⑧を正しく実現し、運用する責任があるため、円滑な運用を行うための体制や手順を明確にした運用管理規定を作成すること。運用には、エンティティがセキュリティ仕様書に基づいて正しくセキュリティを実現していることを確認することも含まれる。

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。

2.3.2　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

運用管理機関が策定したセキュリティ仕様書に基づいて、車載機メーカ、路側機メーカ及び車両メーカがセキュリティを実現する際の要求事項を以下に示す。

【技術面】

① セキュリティ機能の実現

車載機メーカ及び路側機メーカは、運用管理機関から開示されたセキュリティ仕様書に基づいて正しくセキュリティ機能を実現すること。

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。

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。

【運用面】

④ セキュリティ仕様書の管理

車載機メーカ、路側機メーカは、運用管理機関から開示されたセキュリティ仕様書及びその他各種仕様を適切に管理すること。

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。

第3章　セキュリティ情報運用管理システムにおけるセキュリティ要求事項

通信情報の真正性、完全性、機密性を保証するためには、運用管理機関によるセキュリティ情報の生成、配布、保管等と、SAM メーカ、車載機メーカ及び路側機メーカによる SAM、車載機及び路側機へのセキュリティ情報の格納等のセキュリティ情報の運用管理が必要となる。

そこで、本章では、セキュリティ情報運用管理システムの概要、安全なセキュリティ情報の運用管理を実現するためのセキュリティに関する基本方針、及び基本方針に基づいたセキュリティ実現のために、セキュリティ情報の運用管理に関わる運用管理機関及びエンティティに対して要求する事項について述べる。

3.1　セキュリティ情報運用管理システムの概要

3.1.1　システム構成と役割

3.1.1.1　　システム構成

セキュリティ情報運用管理システムの構成を図 3-1 に示す。はじめに 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。そして、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。路側機メーカも車載機メーカと同様に、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、書込区域は設けなくてもよい。

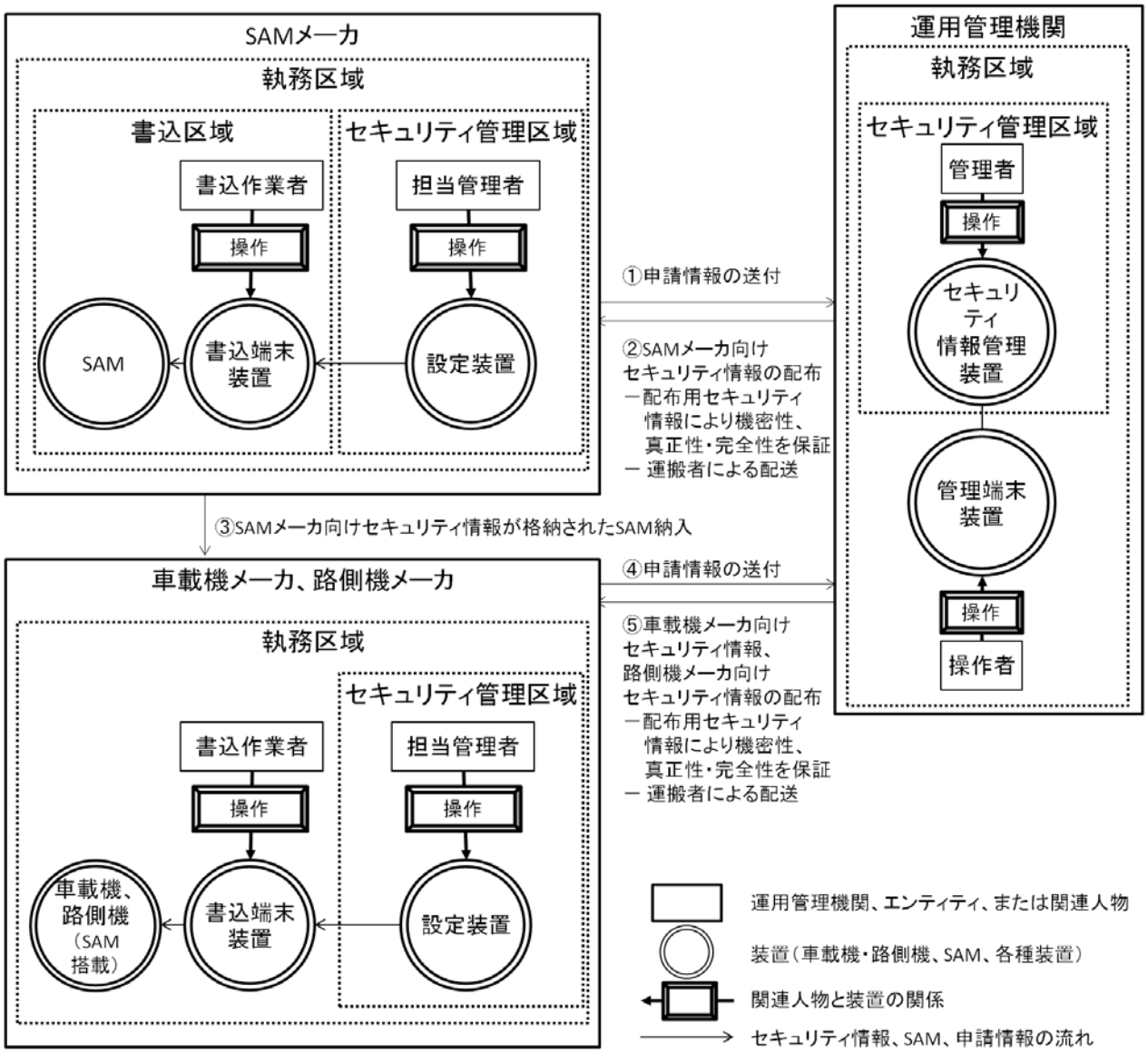

図 3-1　セキュリティ情報運用管理システムの構成

3.1.1.2　　構成要素の役割

図 3-1 で示したシステムの構成要素の役割を表 3-1 に示す。

表 3-1　構成要素の役割

構成要素		主な役割
運用管理機関	セキュリティ情報管理装置	管理端末装置からセキュリティ情報の生成要求を受け付け、セキュリティ情報の生成と保管を行う。また、管理端末装置からセキュリティ情報の配布要求を受け付け、セキュリティ情報を配布するための処理を行う。
	管理端末装置	セキュリティ情報の参照、生成、配布等の要求を行う。
SAM メーカ	設定装置	SAM メーカが、SAM にセキュリティ情報を格納する際に用いる装置である。媒体で受け取ったセキュリティ情報を取り込む。
	書込端末装置	書込作業を行う装置で、設定装置からセキュリティ情報を受け取り、SAM に書き込む。
	SAM	書込端末装置を介して SAM メーカ向けセキュリティ情報を取り込む。
車載機メーカ、路側機メーカ	設定装置	車載機メーカ及び路側機メーカが、車載機・路側機に搭載された SAM にセキュリティ情報を格納する際に用いる装置である。媒体で受け取ったセキュリティ情報を取り込む。
	書込端末装置	書込作業を行う装置で、設定装置からセキュリティ情報を受け取り、車載機・路側機に搭載された SAM に書き込む。
	車載機・路側機	書込端末装置を介して、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を、車載機・路側機に搭載された SAM に取り込む。

3.1.1.3　関連人物の役割

図 3-1 で示したシステムの関連人物の役割を表 3-2 に示す。

表 3-2　関連人物の役割

関連人物		役割
運用管理機関	操作者	運用管理機関に従事する者で、セキュリティ情報管理装置を操作し、セキュリティ情報の生成等を行う。 －執務区域への入室権限があるが、セキュリティ管理区域への入室権限はない。 －セキュリティ情報へのアクセス権限がある。
	管理者	セキュリティ情報管理装置を保守する者である。 －執務区域及びセキュリティ管理区域への入室権限がある。 －セキュリティ情報へのアクセス権限がある。
SAM メーカ	担当管理者	SAM メーカに従事する者で、運用管理機関とセキュリティ情報をやりとりする。セキュリティ情報のやりとりとは、運用管理機関に対してセキュリティ情報の生成を依頼し、受け取る行為を指す。 －セキュリティ管理区域への入室権限がある。 －セキュリティ情報へのアクセス権限がある。
	書込作業者	SAM メーカに従事する者で、セキュリティ情報の書込作業を行う。運用管理機関とのセキュリティ情報のやりとりには関与しない。 －書込区域への入室権限があるが、セキュリティ管理区域への入室権限はない。 －セキュリティ情報へのアクセス権限がある。

関連人物		役割
車載機メーカ、路側機メーカ	担当管理者	車載機メーカ、路側機メーカに従事する者で、運用管理機関とセキュリティ情報をやりとりする。セキュリティ情報のやりとりとは、運用管理機関に対してセキュリティ情報の生成を依頼し、受け取る行為を指す。 －セキュリティ管理区域への入室権限がある。 －セキュリティ情報へのアクセス権限がある。
	書込作業者	車載機メーカ、路側機メーカに従事する者で、セキュリティ情報の書込作業を行う。運用管理機関とのセキュリティ情報のやりとりには関与しない。 －執務区域への入室権限はあるが、セキュリティ管理区域への入室権限はない。 －セキュリティ情報へのアクセス権限がある。
運搬者		運用管理機関から SAM メーカ、車載機メーカ及び路側機メーカにセキュリティ情報を運ぶ者。SAM メーカ、車載機メーカ及び路側機メーカに従事する者または運搬会社が想定される。

3.1.2 保護資産

図 3-1 で示したシステムの保護資産を表 3-3 に示す。

表 3-3 保護資産

保護資産	説明
車載機メーカ向けセキュリティ情報	通信情報の真正性、完全性、機密性を保証するために必要なセキュリティ情報のうち、運用管理機関が車載機メーカに配布するセキュリティ情報。
路側機メーカ向けセキュリティ情報	通信情報の真正性、完全性、機密性を保証するために必要なセキュリティ情報のうち、運用管理機関が路側機メーカに配布するセキュリティ情報。
SAM メーカ向けセキュリティ情報	通信情報の真正性、完全性、機密性を保証するために必要なセキュリティ情報のうち、運用管理機関が SAM メーカに配布するセキュリティ情報。
配布用セキュリティ情報	運用管理機関が車載機メーカ、路側機メーカ及び SAM メーカに、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を安全に配布するために必要なセキュリティ情報。運用管理機関は、配布用セキュリティ情報を用いて、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の機密性や真正性・完全性を保証する。
申請情報	車載機メーカ、路側機メーカ及び SAM メーカが、運用管理機関に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の生成を依頼する際に申請する情報。

3.1.3 前提条件

図 3-1 で示したシステムの前提条件を表 3-4 に示す。

表 3-4　前提条件

分類		前提条件
物理的	セキュリティ情報管理装置	運用管理機関のセキュリティ情報管理装置には、ユーザ認証の仕組みが備わっている。
	車載機メーカ、路側機メーカ、SAM メーカ	車載機メーカ、路側機メーカ及び SAM メーカの執務区域に入る際には社員証等での確認がある。
	管理端末装置	運用管理機関の管理端末装置には、ユーザ認証の仕組みが備わっている。
	設定装置	車載機メーカ、路側機メーカ及び SAM メーカの設定装置には、ユーザ認証の仕組みが備わっている。
	書込端末装置	車載機メーカ、路側機メーカ及び SAM メーカの書込端末装置には、ユーザ認証の仕組みが備わっている。
接続	車載機・路側機	媒体（例：CD-ROM、USB メモリ）の I/F があるが、外部 NW 接続はない。
	管理端末装置	媒体（例：CD-ROM、USB メモリ）の I/F があるが、外部 NW 接続はない。
	設定装置	媒体（例：CD-ROM、USB メモリ）の I/F があるが、外部 NW 接続はない。
	書込端末装置	媒体（例：CD-ROM、USB メモリ）の I/F があるが、外部 NW 接続はない。
その他	申請情報	配布用セキュリティ情報を用いて申請情報の真正性・完全性が保証される。
	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	車載機メーカ向けセキュリティ情報及び路側機メーカ向けセキュリティ情報を用いて、通信情報の機密性、真正性・完全性が保証される。更に、運用管理機関が車載機メーカ、路側機メーカに配布する際には、配布用セキュリティ情報を用いて機密性、真正性・完全性が保証される。
	SAM メーカ向けセキュリティ情報	配布用セキュリティ情報を用いて機密性、真正性・完全性が保証される。
	運用管理機関とエンティティ間のやりとり	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は、運用管理機関から車載機メーカ、路側機メーカ及び SAM メーカに媒体で配布される。

3.2　セキュリティに関する基本方針

運用管理機関、車載機メーカ、路側機メーカ及び SAM メーカが従うべき基本方針は以下のとおりである。

- セキュリティ管理体制の構築

セキュリティ管理体制を構築し、セキュリティの維持・向上に努める。

- 法令・規範の遵守

  法令及びその他の規範を遵守する。

- セキュリティ情報の保護

  保護資産であるセキュリティ情報に対して、セキュリティの三大要素である機密性、完全性、可用性の観点からリスク評価を行い、その結果に基づいた適切な対策を実施する。

- インシデントへの対応

  セキュリティに関するインシデントが発生した場合、運用管理機関及び関連するエンティティが連携し、適切な対策を速やかに行う。

- 見直し及び改善

  前提条件の変化、セキュリティ情報運用管理において実施すべき内容の変化、社会的変化、技術的変化、法令等の変更等に応じた適切な対策を実施し、セキュリティの維持・向上に努める。

3.3 セキュリティ要求事項

3.2 節のセキュリティに関する基本方針に基づいて運用管理機関、車載機メーカ、路側機メーカ及び SAM メーカへのセキュリティ要求事項を示す。

3.3.1 運用管理機関へのセキュリティ要求事項

執務区域とセキュリティ管理区域におけるセキュリティ要求事項を以下に示す。

3.3.1.1 執務区域におけるセキュリティ要求事項

【技術面】

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。

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。

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。

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。

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。

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。

【運用面】

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。

3.3.1.2 セキュリティ管理区域におけるセキュリティ要求事項

【技術面】

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。

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。

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。

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。

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。

【運用面】

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。

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。

3.3.1.3 セキュリティ情報配布時の要求事項

【技術面】

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。

② セキュリティ情報の真正性・完全性確認

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。

【運用面】

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。

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。

3.3.1.4 インシデント対応に関する要求事項

【運用面】

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。

3.3.2 車載機メーカ、路側機メーカへのセキュリティ要求事項

車載機メーカ、路側機メーカの執務区域とセキュリティ管理区域におけるセキュリティ要求事項を以下に示す。

3.3.2.1 執務区域におけるセキュリティ要求事項

【技術面】

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。

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。

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。

【運用面】

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。

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 NW 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。

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。

3.3.2.2 セキュリティ管理区域におけるセキュリティ要求事項

【技術面】

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。

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。

③ セキュリティ情報の機密性維持

設定端末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。

④ セキュリティ情報の真正性・完全性確認

設定端末装置は、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。

【運用面】

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。

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。

3.3.2.3 セキュリティ情報受取時の要求事項

【運用面】

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。

3.3.2.4 インシデント対応に関する要求事項

【運用面】

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。

3.3.3 SAM メーカへのセキュリティ要求事項

書込区域とセキュリティ管理区域におけるセキュリティ要件を以下に示す。

3.3.3.1 書込区域におけるセキュリティ要求事項

【技術面】

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。

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。

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。

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。

【運用面】

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。

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。

3.3.3.2 セキュリティ管理区域におけるセキュリティ要求事項

【技術面】

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。

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。

③ セキュリティ情報の機密性維持

設定端末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。

④ セキュリティ情報の真正性・完全性確認

設定端末装置は、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。

【運用面】

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。

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 NW 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。

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。

3.3.3.3 セキュリティ情報受取時の要求事項

【運用面】

SAM メーカは、信頼できる運搬者を選定すること。

3.3.3.4 インシデント対応に関する要求事項

【運用面】

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。

付録A　インシデント対応

2.2 節及び 3.2 節の基本方針に示したとおり、700MHz 帯安全運転支援システムの構築・運用に関わるエンティティや運用管理機関は、セキュリティに関するインシデントが発生した場合には速やかに対応する必要がある。そこで、本付録にインシデント対応に必要な体制や対応の流れを記す。700MHz 帯安全運転支援システムの構築する際には、運用管理機関や関連するエンティティは、本付録を参考に具体的な体制は対応手順を検討することが望ましい。

A.1　インシデントの例

本書において想定するセキュリティに関するインシデントの例を表 A-1 に示す。

表 A-1　インシデントの例

No.	分類	インシデント
1	機密性	車載機・路側機の解析によるセキュリティ情報漏洩
2		メーカの設定端末装置等からのセキュリティ情報漏洩
3		運用管理機関のシステムからのセキュリティ情報漏洩
4		媒体の盗難・紛失（メーカ、配送経路、運用管理機関）によるセキュリティ情報漏洩
5		セキュリティ仕様書の盗難・紛失によるセキュリティ仕様の漏洩
6		ロケーショントラッキングによるプライバシ侵害
7		暗号アルゴリズムの危殆化や暗号モジュールの脆弱性によるセキュリティ情報漏洩
8	完全性	車載機・路側機の改ざん、偽 GPS 信号等による偽情報送信、リプレイ攻撃による安全運転支援サービスの質低下
9	可用性	DoS 攻撃、Jamming 等による安全運転支援サービスの利用不可
10		運用管理機関のセキュリティ情報管理装置停止（マルウェア感染、操作ミス等）

A.2　インシデント対応の関係者

インシデント対応関係者の関連を図 A-1 に示す。運用管理機関は、資産に対する管理責任を負い、セキュリティ対策、事故対応の指示を出すセキュリティ管理委員会と、具体的なセキュリティ対策や事故対応を行うセキュリティ管理部門を設ける。また、車載機保有者、ドライバー、または各メーカからの問合せを受け付ける部門や、専門的な意見や助言を得るためにセキュリティ有識者との連携体制も必要となる。

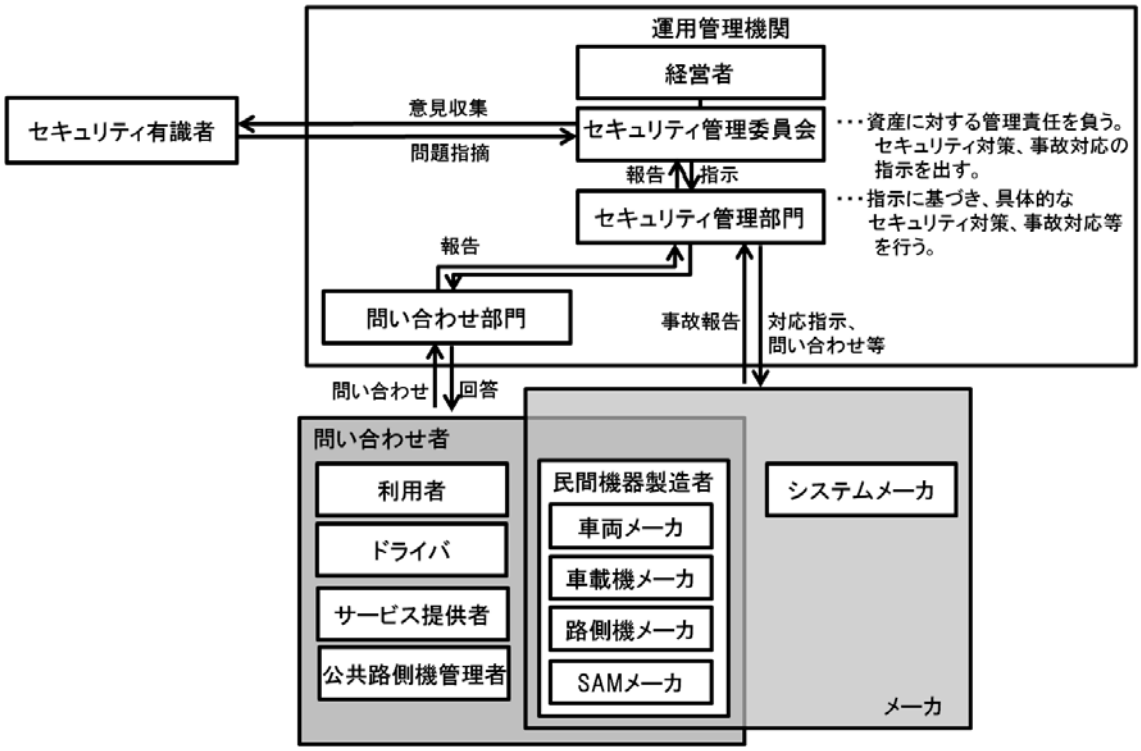

図 A-1　インシデント対応関係者

A.3 インシデント対応の全体フロー

セキュリティ管理委員会がインシデント対応を実施する際のフローを図 A-2 に示す。インシデント対応は、検知、初期対応、回復、事後対応の 4 つのフェーズに分類できる。

【検知フェーズ】

検知フェーズではインシデントを検知する。インシデントの検知は以下の 3 パターンが想定される。

- 車載機保有者やドライバー等からの問合せ
  車載機保有者やドライバー等から問合せがあった場合は、セキュリティに関連するかどうかの判断後、初期対応のフェーズに進む。
- 事故発生の発生報告
  車載機メーカ、路側機メーカ、SAM メーカまたは運用管理機関でセキュリティ情報の漏洩が発生した等の事故報告がある場合は、直ちに初期対応を実施する。
- 問題指摘
  セキュリティ有識者、車載機メーカ、路側機メーカまたは SAM メーカ等からアルゴリズムの危殆化や、類似システムでの事故発生報告を受けた場合は、本システムに関係する、かつ即座の対応が必要な場合は直ちに初期対応フェーズに進む。本システムに関係するが、即座

の対応が求められない場合は、いつまでに対応すべきかを判断し、事後対応フェーズの今後の対応計画の決定に進む。

【初期対応フェーズ】

初期対応のフェーズでは被害を最小限にとどめるために以下の 3 つの項目を実施する。

(1) 事実関係の確認

① 被害状況の確認と報告

被害範囲や原因等、今後の対応に必要な情報の収集をセキュリティ管理部門に依頼する。また、車載機保有者やドライバー、サービス提供者、公共路側機管理者にインシデント状況を報告する必要があるかを判断し、適切な方法で報告する。

② 関係者の招集

招集するエンティティ（発生したインシデントの対応に必要なエンティティ）を決定する。暗号アルゴリズムの危殆化等の場合はセキュリティ有識者も招集する。

③ インシデント管理台帳への記載

発生発覚日、解決日、内容、対応策、ステータス等を記載するインシデント管理台帳に本インシデントを記載する。

④ 対応計画の立案

被害拡大防止策や回復策の決定の期限、それに向けての役割分担を明確にする。

(2) 被害拡大防止策決定

① 被害拡大防止策決定の決定

招集したエンティティとともに被害を最小限にするための当面の対応策（内容、担当者、期限）を決定する。

② 関係者への報告の必要性確認

車載機保有者やドライバー、サービス提供者、公共路側機管理者にインシデント状況及び被害拡大防止策について報告する必要があるかを判断し、適切な方法で報告する。

(3) 関係者への被害拡大防止策実施依頼と確認

セキュリティ管理委員会は(2)の①で決定した内容に従ってセキュリティ管理部門やエンティティに指示／依頼を出す。また、被害拡大防止策実施結果を確認する。

【回復フェーズ】

回復のフェーズではインシデント発生前の状態に戻すために以下の 2 つの項目を実施する。

(1) 回復策決定

① 回復策の決定

招集したエンティティとともにインシデント発生前の状態に戻すための対応策（内容、担当者、期限）を決定する。

② 関係者への報告の必要性確認

車載機保有者やドライバー、サービス提供者、公共路側機管理者にインシデント状況

及び回復策について報告する必要があるかを判断し、適切な方法で報告する。

(2) 関係者への回復策実施依頼と確認

セキュリティ管理委員会は(1)の①で決定した内容に従ってセキュリティ管理部門やエンティティに指示／依頼を出す。また、回復策実施結果を確認する。

【事後対応フェーズ】

事後対応のフェーズではインシデントの再発を防止するために以下の 2 つの項目を実施する。

(1) 再発防止策決定

① 再発防止策の決定

招集したエンティティとともにインシデント発生の原因や経緯等から再発を防止するための対応策（内容、担当者、期限）を決定する。

② 関係者への報告の必要性確認

車載機保有者やドライバー、サービス提供者、公共路側機管理者にインシデント状況及び再発防止策について報告する必要があるかを判断し、適切な方法で報告する。

(2) 関係者への再発防止策実施依頼と確認

セキュリティ管理委員会は(1)の①で決定した内容に従ってセキュリティ管理部門やエンティティに指示／依頼を出す。また、再発防止策実施結果を確認する。

(3) インシデント対応最終報告

インシデント発生経緯、原因、対応のプロセス等を報告書としてまとめる。

なお、検知フェーズで即座の対応が必要ないと判断された場合、例えば暗号アルゴリズムの危殆化が報告され、危殆化による即座のセキュリティ情報漏洩の可能性はないが、数年後までの対応が必要と判断された場合には、暗号アルゴリズムや鍵長の変更に向けて以下の2つの項目を実施する。

(1) 今後の対応計画決定

対応計画の検討に必要なエンティティを招集し、対応計画（内容、担当者、期限）を決定する。

(2) 関係者への対応依頼

セキュリティ管理委員会は、(1)で決定した対応計画に従ってセキュリティ管理部門やエンティティに指示／依頼を出す。また、必要に応じて対応計画の進捗を確認する。

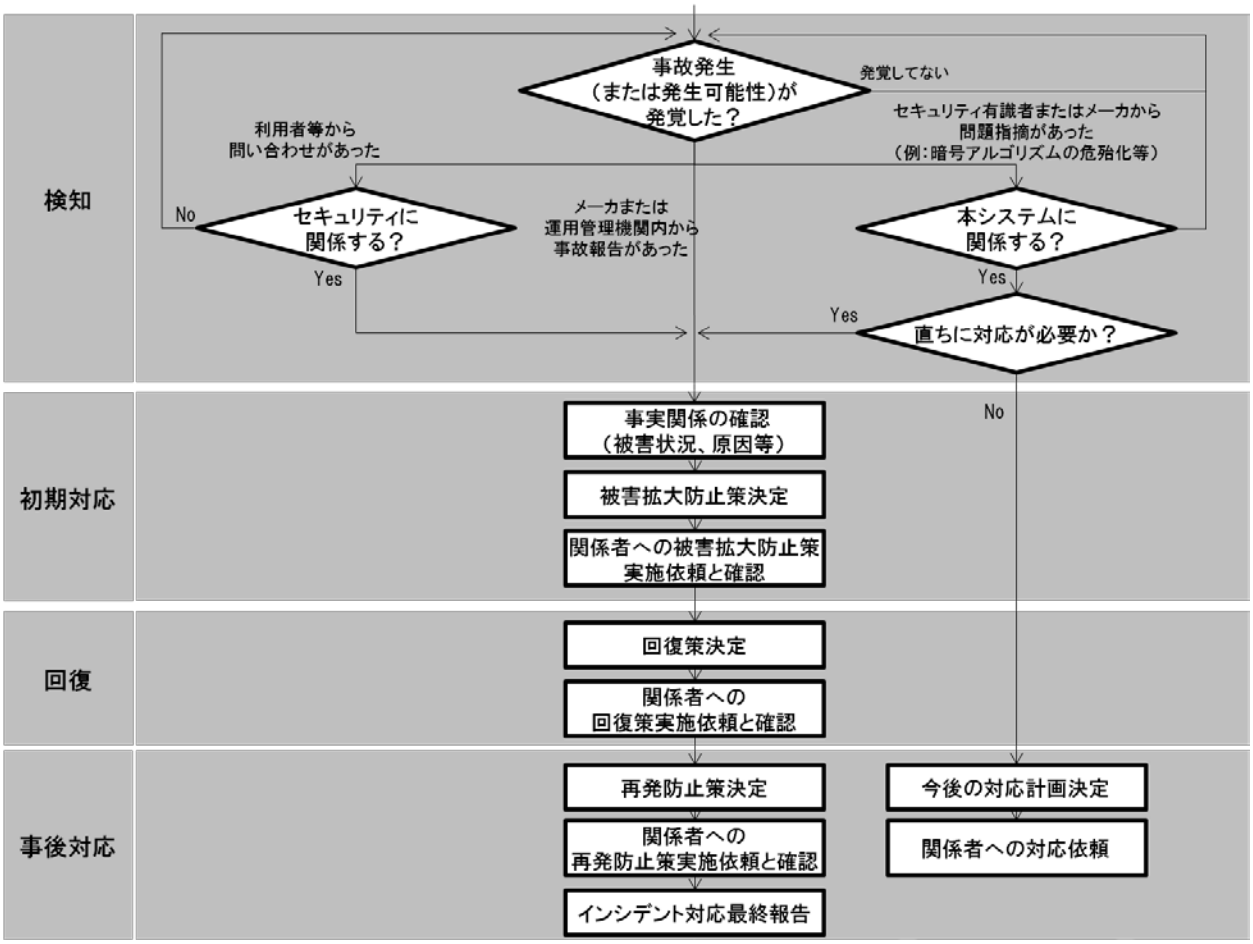

図 A-2　セキュリティ管理委員会のインシデント対応フロー