資料３

700MHz 帯安全運転支援システム
セキュリティポリシー
（叩き台）

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を用いてサービスを提供する際のセキュリティ上の脅威を抽出し、それらの脅威への対策として必要なセキュリティ機能を示す。具体的には、車載機及び路側機が送信する情報の真正性、完全性、機密性を保証する機能が 700MHz 帯安全運転支援システムには必要となる。

1.2　適用範囲

本書は、運用管理機関が提供するセキュリティ要件を規定する。本書で規定したセキュリティ要件に従って、運用管理機関はセキュリティ仕様書を作成し、セキュリティ機能を実現させるものとする。セキュリティ仕様書は関連するエンティティに公開され、各エンティティはセキュリティ仕様書に基づいてセキュリティ機能を実現する。

運用管理機関は本書で規定したセキュリティ要件を正しく実現し、運用する責任がある。したがって、運用管理機関は、各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責任があり、問題が発生した場合には速やかに対応する必要がある。また、本書を見直す際には、セキュリティ仕様書も見直す必要がある。

1.3　規格及び仕様書

本書で参照した規格及び仕様書は以下のとおりである。

[1] “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

[2] “ITS FORUM RC-009 1.1 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

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

[4] “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 帯の通信を用いて、安全運転支援のためのサービスを行うシステム。
エンティティ	SAM メーカ、車載機メーカ、路側機メーカ、システム構築メーカ等 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。
車載機	他の車両に搭載された車載機または路側機等と直接通信する無線機能を持ち、専らこの通信による安全運転支援を行うために車側に設置される機器。
路側機	車載機と通信する無線機能を持ち、センサ等で検知した交通状態等のインフラ情報を通信エリア内の車載機に提供するために路側に設置される機器。
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・証明書と、これらを車載機・路側機に格納するために必要な鍵・証明書を指す。
DoS	Denial of Service Attack の略。
ID	Identifier の略。
I/F	Interface 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。

第2章　安全運転支援サービスの概要

安全運転支援システムのセキュリティ対象とする具体的なサービス例を表 2-1 に示す。

表 2-1　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 1.1 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[2]）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に提供する。

2.1 システム構成と役割

2.1.1 システム構成

700MHz 帯安全運転支援システムの構成を図 3-1 に示す。車載機から車載機・路側機、または路側機から車載機へ 700MHz 帯安全運転支援システム（通信規格については参照資料[3][4]を参照）を用いて運転支援サービスのための情報が送信される。

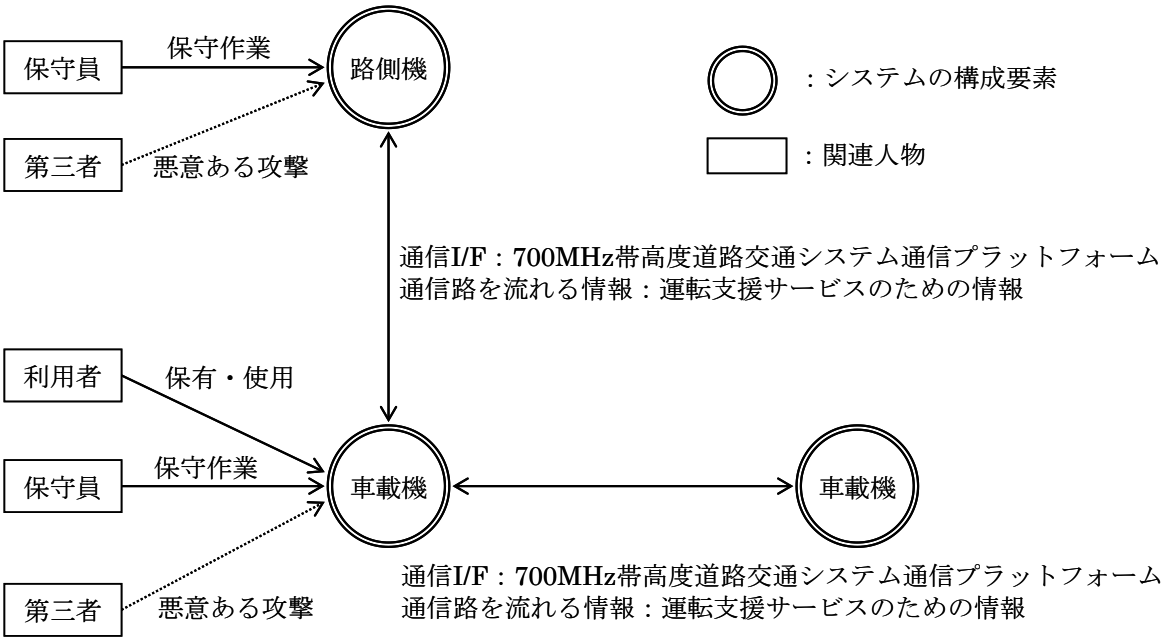

図 3-1　システム構成

2.1.2　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 3-2　構成要素の役割

構成要素	主な役割
路側機	車載機へ 2.1 で述べたサービスのための情報を送信する。
車載機	他の車載機または路側機へ 2.2 で述べたサービスのための情報を送信する。

2.1.3　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 3-3　関連人物の役割

関連人物	役割
保守員	車載機・路側機の保守作業を行う。
利用者	車載機を搭載した車両の保有者で、700MHz 帯安全運転支援システムのサービスを利用する。
第三者	悪意を持って 700MHz 帯安全運転支援システムを使ったシステムを攻撃する。

2.2 セキュリティ環境

2.2.1 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 4-1 に記す。

表 4-4 保護資産

保護資産		概要
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	路側情報	路側機が車載機に送信する情報。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	車載機が路側機や他の車載機に送信する情報。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	車載機が路側機や他の車載機に送信する情報であり、内容は車載機毎に任意に設定される。

2.2.2 前提条件

車載機・路側機が 700MHz 帯安全運転支援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。

2.3 脅威

第 3、4 節で述べたシステムにおいて考えられる脅威を以下の表 5-1 に記す。これは、主に運転支援通信システムに関するガイドライン ITS FORUM RC-009（参照資料[2]）に基づき列挙している。表 5-2 に各脅威に対して算出したリスク値を示す。リスク値は、脅威の発生の可能性と影響度について数値化し、これらを掛け合わせることで算出した。

表 5-5　脅威

No.	脅威	内容
1	なりすまし	利用者による車載機の悪用や第三者による通信機の利用により、路側機や他の車載機（緊急車両を含む）になりすまして誤った情報を含む路側情報や車両情報及び汎用情報が送信されることで、混乱が発生する。
2	リプレイ攻撃	利用者による車載機の悪用や第三者による通信機の利用により、正当な他の路側機や車載機が送信した情報を再利用して送信されることで、混乱が発生する。
3	偽通信ヘッダ情報の送信	利用者による車載機の悪用や第三者による通信機の利用により、路側機が存在しない場所で、偽の通信ヘッダ情報（路側機の送信期間に関わる情報等）が送信されることで、車車間通信が妨害される。
4	通信ヘッダ情報の改ざん	利用者による車載機の悪用や第三者による通信機の利用により、路側機が送信した情報を改ざんして送信されることで、車車間通信や路車間通信が妨害される。
5	装置改ざん	利用者や第三者、保守員等による車載機や路側機の解析や改ざんにより、車載機や路側機のソフトウェアや内部情報が改ざんされ、誤った情報が送信されることで、混乱やシステムの利用不能が発生する。
6	マルウェア	第三者による通信情報の悪用や第三者、保守員等による路側機や車載機への物理的アクセスにより、マルウェアに感染させられることで、虚偽情報によるシステムの利用不能が発生する。
7	入力情報の改ざん	利用者等による車載機入力情報の改ざんや第三者、保守員等による路側機入力情報の改ざんにより、誤った情報が送信されることで、混乱が発生する。
8	Jamming	第三者による通信機等の利用により、妨害電波が発生されることで、通信が不能となり、システムの利用不能が発生する。
9	DoS	利用者による車載機の悪用や第三者による通信機の利用により、大量の情報が送信されることで、システムの利用不能が発生する。
10	偽 GPS 信号	第三者による GPS 信号発生器の悪用により、誤った位置を含む情報が送信されることで、混乱が発生する。
11	盗聴	利用者による車載機の悪用や第三者による通信機の利用により、通信が盗聴され、通信情報が運用管理機関の意図しないサービスへ利用される。
12	ロケーショントラッキング	利用者による車載機の悪用や第三者による通信機の利用により、受信した車両情報から特定の車両の位置がトレースされることで、個人のプライバシ侵害に利用される。

表 5-6　リスク値の算出

No.	脅威	発生の可能性			影響度	リスク値
		動機	技術的困難度			
1	なりすまし	M	M	2	3	6
2	リプレイ攻撃	M	L	3	2	6
3	偽通信ヘッダ情報の送信	L	M	1	1	1
4	通信ヘッダ情報の改ざん	L	M	1	1	1
5	装置改ざん	M	M	2	3	6
6	マルウェア	M	M	2	3	6
7	入力情報の改ざん	M	M	2	3	6
8	Jamming	M	L	3	2	6
9	DoS	M	M	2	2	4
10	偽 GPS 信号	M	M	2	2	4
11	盗聴	H	M	3	1	3
12	ロケーショントラッキング	H	M	3	1	3

動機・技術的困難度は、L＝Low、M＝Middle、H＝High を示す。

2.4　セキュリティ要件

2.4.1　セキュリティ対策方針

表 5-1 で挙げた脅威への対策を表 6-1 に示す。

脅威の No.1～4 は無線通信信号に対する攻撃であり、運用管理機関が対策責任を負う。対策として、無線通信へのセキュリティ導入が挙げられる。特に緊急車両へのなりすましは、周辺の交通への影響が大きいため、特別な対策が必要となる。No.3、4 の脅威については、リスク値が低いことから対策不要とする。

脅威の No.5～7 は車載機や路側機及びそれらへの接続機器に対する攻撃であり、車載機メーカ、路側機メーカ、車両メーカが対策責任を負う。対策としては種々考えられるが、どのような対策が適用可能かについては、機器の形態や実装方法に大きく依存するため、対策内容については各メーカが判断するものとする。

脅威の No.8～10 は無線通信（GPS 含む）に対する違法な無線機を用いた攻撃であり、運用管理機関や機器メーカの責任範囲外となり、関係省庁による取締りが対策となる。

脅威の No.11、12 は受信した情報を悪用する攻撃であり、700MHz 帯安全運転支援システムに対する妨害や混乱といった被害は発生しないものの、700MHz 帯安全運転支援システムへの利用者の信頼性を損なわせるものである。これらへの対策として、無線通信へのセキュリティ導入が挙げられる。ただし、無線通信セキュリティ通過後の受信情報を悪用されることが考えられるため、アプリケーションデータのレベルでの対策（例えば、車両 ID を車載機の起動の度に切替えるなど）も必要である。

表 6-7　脅威への対策方針

No.	脅威	リスク値	攻撃対象	対策	対策責任者
1	なりすまし		無線通信信号	無線通信への セキュリティ導入	運用管理機関
2	リプレイ攻撃				
3	偽通信ヘッダ情報の送信			無線機で通信規格への準拠を確認	
4	通信ヘッダ情報の改ざん				
5	装置改ざん		車載機・路側機	入力 I/F の防護、 ソフトウェア・ 内部データの難読化等	車載機・ 路側機メーカ
6	マルウェア		車載機・路側機、 車載機・路側機への 接続機器	ソフトウェアの脆弱性への対処、接続機器へのセキュリティソフトの導入等	車載機・ 路側機メーカ、 車両メーカ
7	入力情報の改ざん		車載機・路側機への 接続機器	接続仕様の非公開等	
8	Jamming		無線通信	（法規制）	関係省庁
9	DoS			（法規制）	
10	偽 GPS 信号		無線通信信号 （GPS）	（法規制）	
11	盗聴		無線通信信号	無線通信への セキュリティ導入	運用管理機関
12	ロケーショントラッキング				

2.4.2　セキュリティ機能要件

6.1 で示したセキュリティ方針に基づき、運用管理機関が対策責任者となる脅威「なりすまし」、「リプレイ攻撃」に必要な対策を、700MHz 帯安全運転支援システムのセキュリティ機能要件として以下に記す。

(1) 発信元の真正性の確認

通信情報の発信元が正しくその本人であり、偽の第三者がなりすましていないことを確認できること。真正性の確認に用いるセキュリティ情報は耐タンパー性のあるエリアに格納しておくこと。

(2) 通信情報の完全性確認

受信した通信情報のペイロード情報が、正しく発信元が送信した情報と同じものであり、通信の途中において改ざんされていないことが確認できること。完全性確認に用いるセキュリティ情報は耐タンパー性のあるエリアに格納しておくこと。

(3) 通信情報の機密性の維持

通信情報を暗号化することで、第三者による盗聴を防ぐことができること。機密性の維持に用いるセキュリティ情報は耐タンパー性のあるエリアに格納しておくこと。

2.4.3 対策機能要件

6.2 で示したセキュリティ機能要件を満たすために対策機能の要件を以下に記す。

(1) セキュリティ情報の生成

運用管理機関が、発信元の真正性の確認及び受信情報の完全性確認に必要なセキュリティ情報を生成する機能を有すること。

(2) セキュリティ情報の格納及び解析防止

車載機・路側機は耐タンパー性のあるエリア（SAM）を有し、(1)のセキュリティ情報は SAM に格納され、外部から容易に解析できないこと。

(3) 路車間通信の発信元の真正性の確認及び通信情報の完全性確認

路側機が送信する通信情報のペイロード情報は、運用管理機関が各路側機に発行するセキュリティ情報及び全ての車載機・路側機に発行する共通のセキュリティ情報にて、真正性、完全性が担保されること。

(4) 車車間通信の発信元の真正性の確認及び通信情報の完全性確認

車載機が送信する通信情報のペイロード情報は、運用管理機関が全ての車載機・路側機に発行する共通のセキュリティ情報にて、真正性、完全性が担保されること。

(5) セキュリティ情報の更新

路車間または車車間通信の発信元の真正性の確認及び通信情報の完全性確認に必要な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。

第3章　セキュリティ情報管理システムの概要

700MHz帯安全運転支援システムの真正性、完全性、機密性を保証するためには(参照文献[5][6])、セキュリティ情報の生成等を行うセキュリティ情報管理システムが必要となる。セキュリティ情報管理システムの役割は「セキュリティ情報の生成、配信・配布、保管、切替、更新」である。

3.1　システム構成と役割

3.1.1　システム構成

セキュリティ情報管理システムの構成、車載機・路側機メーカのセキュリティ情報格納に関するシステムの構成を図 3-1 に示す。セキュリティ情報管理システムが生成したセキュリティ情報は、車載機・路側機メーカ、路側機管理者に配信・配布され、車載機・路側機に格納される。

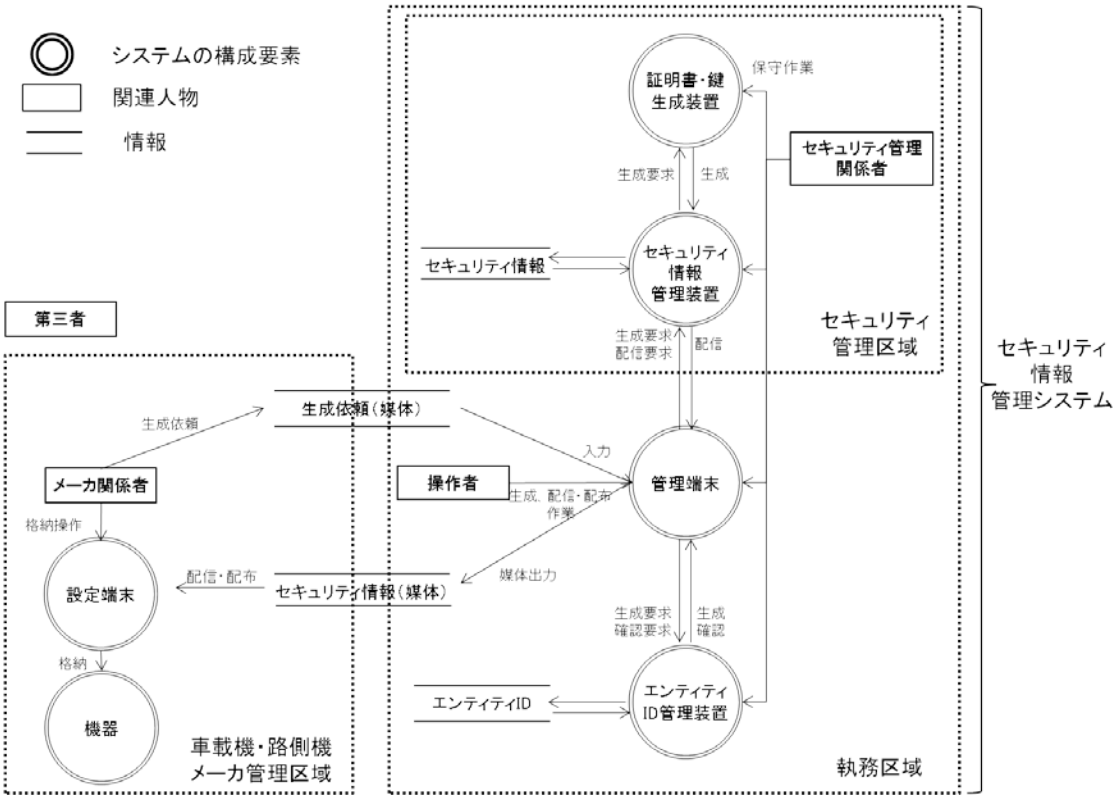

図 3-1　システム構成

3.1.2 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
証明書・鍵生成装置	通信路を保護するために必要となるセキュリティ情報を生成する。
セキュリティ情報管理装置	管理端末からセキュリティ情報の生成要求を受け付け、証明書・鍵生成装置に対して、セキュリティ情報の生成を要求し、生成されたセキュリティ情報を管理する。また、管理端末からセキュリティ情報の配信・配布要求を受け付け、セキュリティ情報を配信・配布するための処理を行う。
管理端末	セキュリティ情報の参照、生成、配信・配布等の要求を行う。
エンティティ ID 管理装置	エンティティ ID を管理する。
設定端末	車載機・路側機メーカが機器にセキュリティ情報を格納する際に用いる端末である。
機器	設定端末から与えられたセキュリティ情報を耐タンパー性のあるエリアに書き込む。

3.1.3 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
運用管理関係者	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システムを操作し、セキュリティ情報の生成等を行う。
	操作者以外	運用管理機関に従事する者だが、セキュリティ情報管理システムの操作が認められていない。
セキュリティシステム管理関係者		セキュリティ情報管理システムを保守する人であり、 運用管理機関への出入りが認められている。
メーカ関係者		車載機･路側機メーカに従事する者で､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。
第三者		上記以外の人物でセキュリティ情報管理システムを攻撃する。

3.2 セキュリティ環境

3.2.1 保護資産

図 3-1 で示したシステムの保護資産を表 4-1 に示す。

表 4-3 保護資産

保護資産	説明
機器のセキュリティ情報	機器（路側機・車載機）に格納されるセキュリティ情報。セキュリティ情報管理システムが車載機・路側機メーカに媒体で配布する。
運用管理機関のセキュリティ情報	機器のセキュリティ情報を保証するためのセキュリティ情報。 運用管理機関のセキュリティ情報の一部は、機器（路側機・車載機）に格納される。
エンティティのセキュリティ情報	セキュリティ情報を生成依頼するエンティティ（SAM メーカ、 車載機･路側機メーカ)にセキュリティ情報を安全に配布するのに必要なセキュリティ情報。
生成依頼	機器のセキュリティ情報を生成してもらうために必要な情報。メーカがセキュリティ情報管理システムに媒体で配布する。

3.2.2 前提条件

図 3-1 で示したシステムの前提条件を表 4-2 に示す。

表 4-4 前提条件

分類		前提条件
物理的	装置(*1)	ID/PW でのログイン（アカウント：セキュリティシステム管理関係者）が必要である。
	管理端末	ID/PW でのログイン（アカウント：操作者、セキュリティシステム管理関係者）が必要である。
	設定端末	ID/PW でのログイン（アカウント：メーカ関係者、セキュリティシステム管理関係者）が必要である。
人的	関連人物	第三者による過失はないが、その他の関連人物は過失／故意ともにある。
接続	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。
	管理端末	媒体（例：CD-ROM、USB メモリ）の I/F があるが、外部 NW 接続はない。
	設定端末	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	生成依頼	生成依頼には署名が付与される。
	機器のセキュリティ情報	機器のセキュリティ情報は暗号化及び署名が付与される。

(*1)セキュリティ情報管理システムの管理端末以外の装置

3.3 脅威

第 3、4 節で述べたシステムにおいて考えられる脅威をリスク評価した。

表 5-5 脅威

No.	脅威	内容
1	権限者の否認	権限者（セキュリティシステム管理関係者、操作者、メーカ関係者）が過失もしくは故意に脅威（情報漏洩、改ざん等）を発生させたが、その行為を否定する。
2	権限者による保護資産の改ざん、削除、偽保護資産の追加	権限者が、生成依頼やセキュリティ情報を改ざん、削除する。または偽の情報を追加する。
3	権限者による装置／プログラムのなりすまし	権限者が、セキュリティ情報管理システムの装置または管理端末のプログラムを不正なものに置き換える。もしくは装置ごと置き換える。
4	セキュリティシステム管理関係者の保守ミス	設定ミスし、脆弱性を作ってしまう。 例）操作者にセキュリティ管理権限等与えてしまう。
5	権限者によるセキュリティ情報の漏洩	権限者が、セキュリティ情報を暗号化せずに媒体出力し、持ち出す。
6	権限者によるマルウェア感染	権限者が、セキュリティ情報管理システムの装置または管理端末をマルウェア感染させ、システムを停止させる。
7	権限者による DoS 攻撃	権限者が、セキュリティ情報管理システムを DoS 攻撃する。
8	非権限者による保護資産の改ざん、削除、偽保護資産の追加	非権限者が、生成依頼やセキュリティ情報を改ざん、削除する。または偽の情報を追加する。
9	非権限者による装置／プログラムのなりすまし	非権限者が、セキュリティ情報管理システムの装置または管理端末のプログラムを不正なものに置き換える。もしくは装置ごと置き換える。
10	非権限者によるセキュリティ情報の漏洩	非権限者が、セキュリティ情報を暗号化せずに媒体出力し、持ち出す。
11	非権限者によるマルウェア感染	非権限者が、セキュリティ情報管理システムの装置または管理端末をマルウェア感染させ、システムを停止させる。
12	非権限者による DoS 攻撃	非権限者が、セキュリティ情報管理システムを DoS 攻撃する。

3.4　セキュリティ要件

3.4.1　セキュリティ対策方針

運用管理機関は、通信情報の発信元の真正性確認及び通信情報の完全性確認を実現するために必要なセキュリティ情報を安全に管理する責任を負う。そのためのセキュリティ対策方針を本節で述べる。

セキュリティ対策は脅威を発生させる手順のできるだけ早い段階で実施されるほど、対策効果が大きい。すなわち、攻撃を防止できる対策、防止はできないが攻撃を検知できる対策、攻撃発覚後に復旧できる対策の順に対策効果が大きい。本書では攻撃者のタイプ（権限者または非権限者）と動機（過失または故意）に応じてセキュリティ対策方針を規定する（図 6-1）。非権限者の攻撃はできるだけ防止対策を実施し、権限者の悪意ある攻撃は防止策の実施は難しいため、検知対策で対応する。

対策方針に基づいて、表 5-1 で挙げた脅威への対策を表 6-1 に示す。対策は、ICT を用いた対策と運用等による対策に分類し、それぞれを更に防止効果、検知効果、復旧効果があるものに分類する。

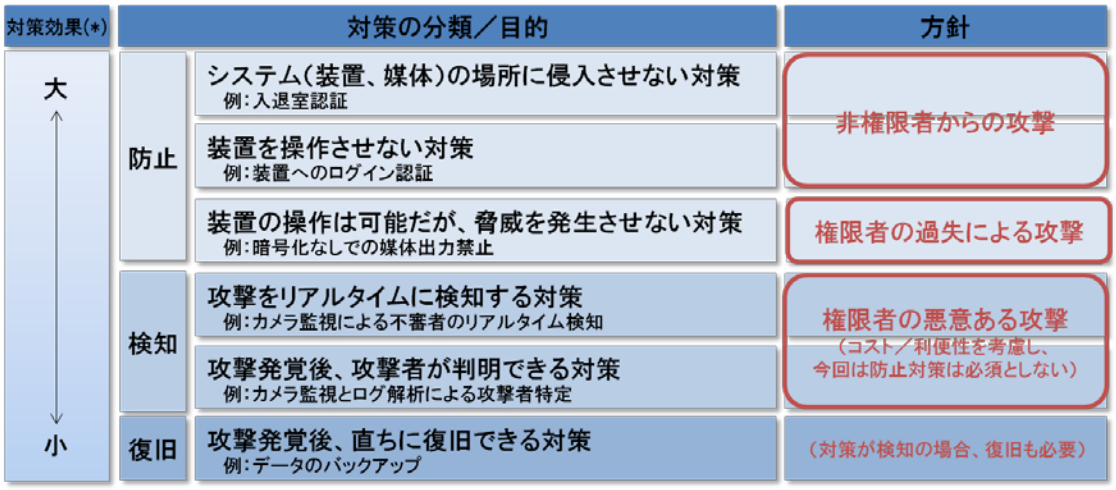

図 6-2　セキュリティ対策方針

表 6-6　セキュリティ対策

No.	脅威	対策								
		ICT							運用	
		防止				検知		復旧	防止	
		A	B	C	D	E	F	G	H	I
		入退室認証	ログイン認証	機器認証・プログラム認証	媒体データ出力制限	媒体データ入力制限	攻撃者検知	バックアップ	仕様書の機密管理	媒体の管理
1	権限者の否認						○			
2	権限者による保護資産の改ざん、削除、偽保護資産の追加					○	○	○		
3	権限者による装置・プログラムのなりすまし			○			○			
4	セキュリティシステム管理関係者の保守ミス						○			
5	権限者によるセキュリティ情報の漏洩				○		○			
6	権限者によるマルウェア感染						○	○		
7	権限者による DoS 攻撃						○			
8	非権限者による保護資産の改ざん、削除、偽保護資産の追加	○	○			○	○	○		
9	非権限者による装置・プログラムのなりすまし	○	○	○			○		○	
10	非権限者によるセキュリティ情報の漏洩	○	○		○		○			○
11	非権限者によるマルウェア感染	○	○				○	○		
12	非権限者による DoS 攻撃	○	○				○			

3.4.2　セキュリティ機能要件

図 3-1 に示すとおり、「執務区域」「セキュリティ管理区域」「車載機・路側機メーカ管理区域」の 3 つのエリアに分けられ、エリア毎に権限者・非権限者が異なる。例えば、操作者は執務区域では権限者だが、セキュリティ管理区域では非権限者となる。そこで、6.1 のセキュリティ対策方針に従い、エリア毎にセキュリティ対策機能の実施有無（必須または任意）を表 6-2 に記す。表 6-2 の(プ)(機)はそれぞれプログラム認証、機器認証を示す。すなわち、(プ)MUST と記載されている場合は、プログラム認証の実施は必須である。

車載機・路側機メーカ管理区域における権限者（メーカ関係者）の攻撃（セキュリティ情報の漏洩・改ざん）への対策機能「D：媒体データ入力制限」「E：媒体データ出力制限」「F：攻撃者検知」は MAY（任意）とした。これは車載機・路側機メーカ管理区域内において、セキュリティ情報は暗号化及び署名が施されており、脅威発生の可能性が低いと判断したためである。

表 6-2 に記載されていない対策機能「G：バックアップ」「H：仕様書の機密管理」「I：媒体の管理」は情報セキュリティ管理システムとして必要なものであり、「執務区域」「セキュリティ管理区域」の区別に関係しない。車載機・路側機メーカ管理区域では「G：バックアップ」は特に必要ないが、「H：仕様書の機密管理」「I：媒体の管理」は必須である。

また、車載機・路側機の SAM を製造する SAM メーカ管理区域のセキュリティ機能要件については別途規定する必要がある。

表 6-7　セキュリティ対策機能実施の有無

記号	対策機能	対象	実施有無 MUST：必須 MAY：任意	根拠
A	入退室認証	執務区域	MUST	非権限者（第三者）は攻撃手順の一番早い段階で防止する。
		セキュリティ管理区域	MUST	非権限者（操作者、操作者以外、第三者）は攻撃手順の一番早い段階で防止する。
		車載機・路側機メーカ管理区域	MUST	非権限者（第三者）は攻撃手順の一番早い段階で防止する。
B	ログイン認証	執務区域内装置	MUST	管理端末の前に座ることができる非権限者（操作者以外）が存在するため。
		セキュリティ管理区域内装置	MAY	非権限者がログインするまでに防止策が複数存在するため。
		車載機・路側機メーカ管理区域内装置	MAY	非権限者がログインするまでに防止策が存在するため。
C	プログラム・機器認証	執務区域内装置	(プ)MAY	非権限者（第三者、操作者以外）は入退室認証またはログイン認証で防止する。権限者の過失は運用で防止し、故意は検知策で対応する。
			(機)MUST	入室可能な非権限者（操作者以外）による攻撃を防止するため。
		セキュリティ管理区域内装置	(プ)MAY	執務区域装置と同じ。
			(機)MUST	権限者の過失は本対策で防止し、故意による脅威発生は検知策で対応する。
		車載機・路側機メーカ管理区域内装置	(プ)MAY	執務区域装置と同じ。
			(機)MAY	スタンドアローンでの動作を想定のため。
D・E	媒体データ入力制限・媒体データ出力制限・	執務区域内装置	MUST	非権限者（第三者、操作者以外）は入退室認証またはログイン認証で防止する。権限者の過失を本対策で防止し、故意は検知策で対応する。
		セキュリティ管理区域内装置	MUST	執務区域装置と同じ。
		車載機・路側機メーカ管理区域内装置	MAY	非権限者の攻撃は入退室認証で防止する。権限者（メーカ関係者）の故意による攻撃への対策は必須としない。
F	攻撃者検知	執務区域	MUST	権限者の故意による攻撃を検知する。
		セキュリティ管理区域	MUST	権限者の故意による攻撃を検知する。
		車載機・路側機メーカ管理区域	MAY	権限者（メーカ関係者）の故意による攻撃への対策は必須としない。

3.4.3　対策機能要件

セキュリティ対策機能の要件のレベルを表 6-3 に規定し、エリア毎に実施が求められるセキュリティ対策機能の要件レベルを表 6-4 に記す。

表 6-8　セキュリティ対策機能の要件レベル

記号	対策機能	レベル	具体的手段（例）	要件
A	入退室認証	低	PW 認証、カード認証	権限者と非権限者を区別できること。
		中	生体認証	権限者へのなりすましが困難なこと（権限者から非権限者へ認証情報が渡りにくいこと）。
		高	「低」「中」の認証手段＋監視カメラ	中レベルの要件に加えて、共連れ防止ができること。
B	ログイン認証	低	PW 認証、カード認証	権限者と非権限者を区別できること。
		中	生体認証	権限者へのなりすましが困難なこと（権限者から非権限者へ認証情報が渡りにくいこと）。
		高	多要素認証(PW＋IC カード、PW＋生体認証、IC カード＋生体認証等)	多重防御でひとつの認証情報が非権限者に渡った場合でもログインできないこと。
C	プログラム・機器認証	低	MAC 認証、 IP アドレス認証 （クライアント認証）	登録外機器がセキュリティ情報管理システムに接続できないこと。
		中	電子証明書を用いた認証（クライアント認証）	認証に用いる情報が簡単に入手できないこと。
		高	電子証明書を用いた認証（相互認証）	中レベルの要件に加えて、相互に認証ができること。
D	媒体データ出力制限	低	承認者の設定	権限者による不正な出力の防止。
		中	暗号化なしでの出力禁止	低レベルの要件に加えて、更なる不正出力防止と紛失時のリスクを低減できること。
		高	媒体の分割	中レベルの要件に加えて、紛失時の更なるリスクを低減できること。
E	媒体データ入力制限	低	承認者の設定	権限者による不正な入力の防止。
		中	入力データの署名確認	低レベルの要件に加えて、入力データ作成元が確認できること。
		高	ウィルスチェック、プログラム認証	中レベルの要件に加えて、入力データがシステムに悪影響を与えないことを確認できること。
F	攻撃者検知	低	操作ログ（操作者、操作時刻、管理端末・装置、操作の種類、操作結果等）	攻撃発生が発覚したときに、攻撃時刻、攻撃内容等の解析ができること。
		中	操作ログ＋監視カメラ、操作ログ＋生体認証でのログイン	攻撃者の特定ができること。
		高	操作ログ＋監視カメラ（リアルタイム検知）	中レベルの要件に加えて、リアルタイムに異常を検知できること。

表 6-9　実施が求められるセキュリティ対策機能の要件レベル

エリア	記号	対策機能	実施有無 MUST：必須 MAY：任意	実施 レベル	根拠
執務区域	A	入退室認証	MUST	低	第三者が管理端末の操作等していると目につきやすく、疑われやすい。
	B	ログイン認証	MUST	高	執務区域への入室権限があるが、管理端末の操作権限がない人の攻撃を防止するため（カードは権限者の目を盗んで利用される可能性あり）。
	C	機器認証	MUST	中	執務区域への入室権限があるが、管理端末の操作権限がない人の攻撃を防止するため（MAC 認証、 IP アドレス盗聴は容易）。
	D・E	媒体データ出力制限・媒体データ入力制限	MUST	中	セキュリティ情報の不正生成・漏洩は影響が大きいため。
	F	攻撃者検知	MUST	中	権限者の否認を防止することが目的のため。
セキュリティ管理区域	A	入退室認証	MUST	中	第三者（非権限者）は執務区域内の入退室認証で防止できる。セキュリティ管理区域内の装置は資産価値が高い情報を扱うため、執務区域内より高いレベルとする。
	B	ログイン認証	MAY	-	-
	C	機器認証	MUST	中	権限者の故意による攻撃をできるだけ防止するため、中とする（機器のなりすましは影響が大きいため、攻撃しにくくする）。
	D・E	媒体データ出力制限・媒体データ入力制限	MUST	中	セキュリティ情報の不正生成・漏洩は影響が大きいため。
	F	攻撃者検知	MUST	中	権限者の否認を防止することが目的のため。
車載機・路側機 メーカ管理区域	A	入退室認証	MUST	低	第三者がメーカ内にいると目につきやすく、疑われやすい。
	B	ログイン認証	MAY	-	-
	C	機器認証	MAY	-	-
	D・E	媒体データ出力制限・媒体データ入力制限	MAY	-	-
	F	攻撃者検知	MAY	-	-

第4章　インシデント対応