

# 700MHz帯安全運転支援システムにおける セキュリティの検討状況

---

事務局

# ITSセキュリティ検討グループにおける主な検討事項(案)

## 既存のガイドライン

### ■ 運転支援通信システムに関する運用管理ガイドライン (RC-008)

(平成23年4月27日ITS情報通信システム推進会議策定)

- ・ 運転支援通信システムの実用化・運用・維持の際に必要な運用事項について定めたもの。
- ・ 情報セキュリティについては、各機器におけるセキュリティ情報の格納・更新・再設定・抹消の手続き等を規定。

### ■ 運転支援通信システムに関するセキュリティガイドライン (RC-009)

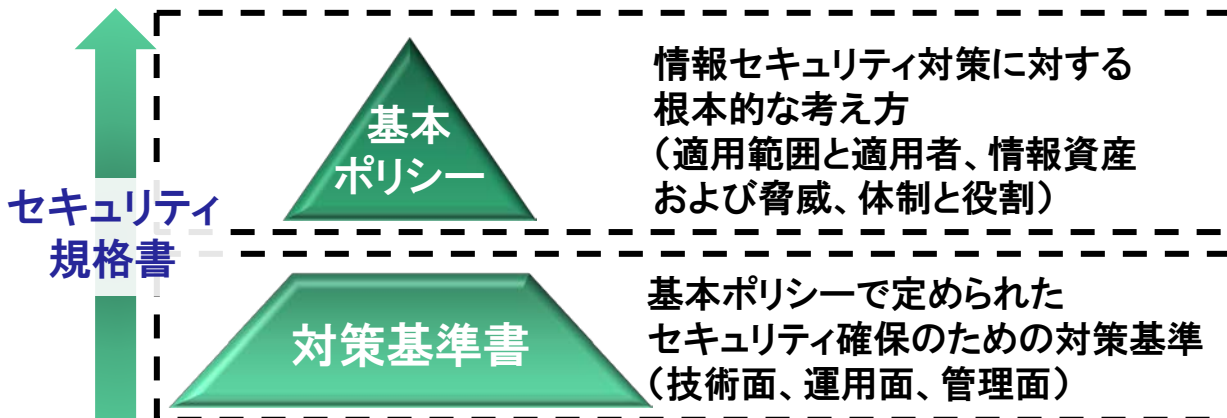
(平成23年4月27日ITS情報通信システム推進会議策定、平成24年4月25日改訂、平成25年11月25日改訂)

- ・ 運転支援システムに対する脅威とリスクを分析し、脅威に対する対策方針について定めたもの。
- ・ 情報セキュリティについては、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とともに、通信区間を流れる情報の機密性の確保を可能にすべきこと等を規定。

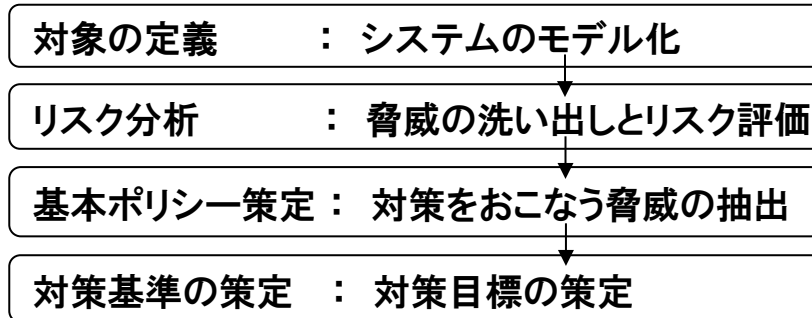
既存のガイドラインを踏まえてより具体的な検討を行う

## 検討グループにおける検討事項

これまで策定されたガイドラインを踏まえて、以下の事項について検討

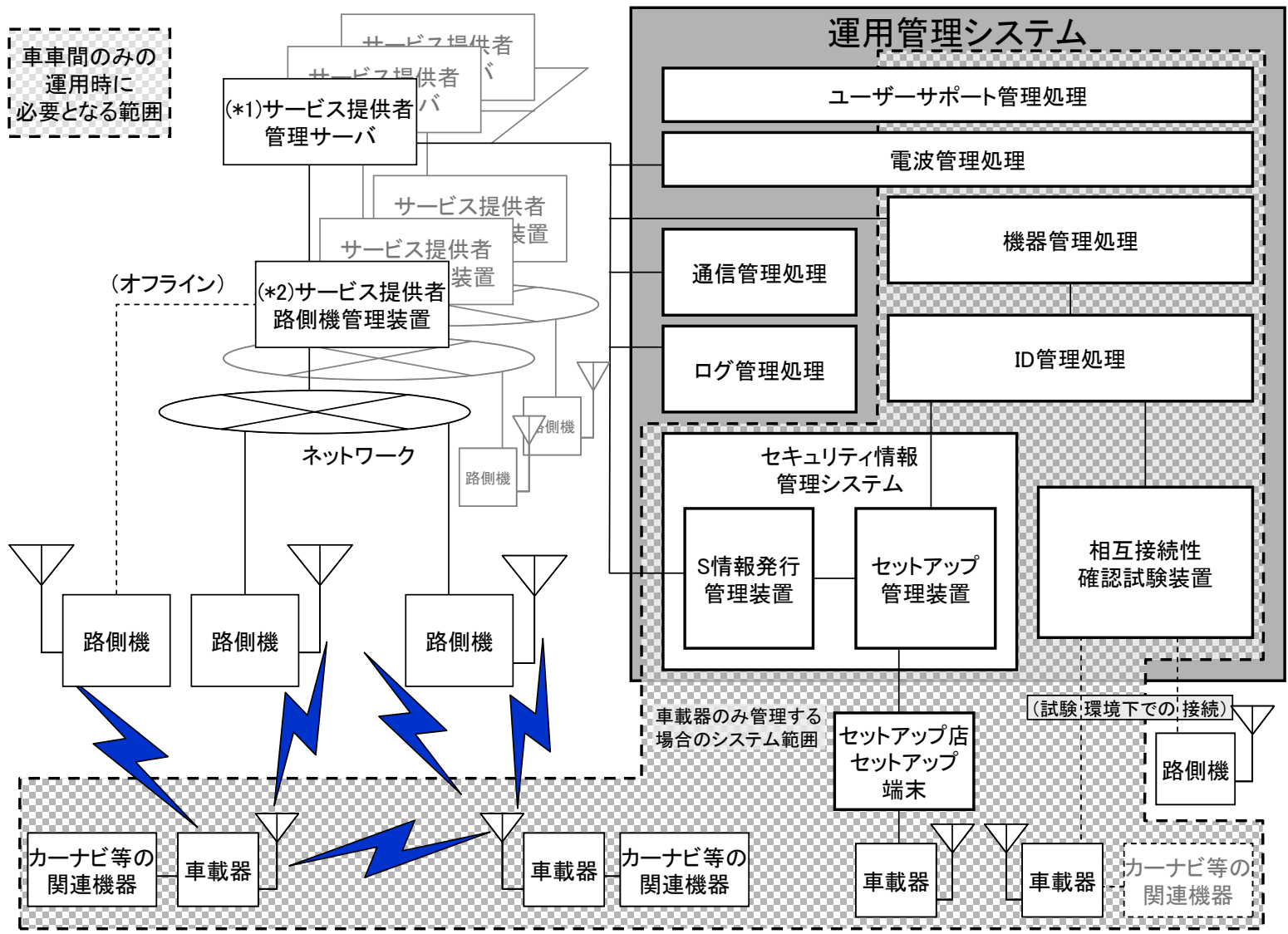


## 検討の流れ



メーカーは策定された対策基準書を参照し、基準書の内容を実現するための設計書・運用手順書を作成

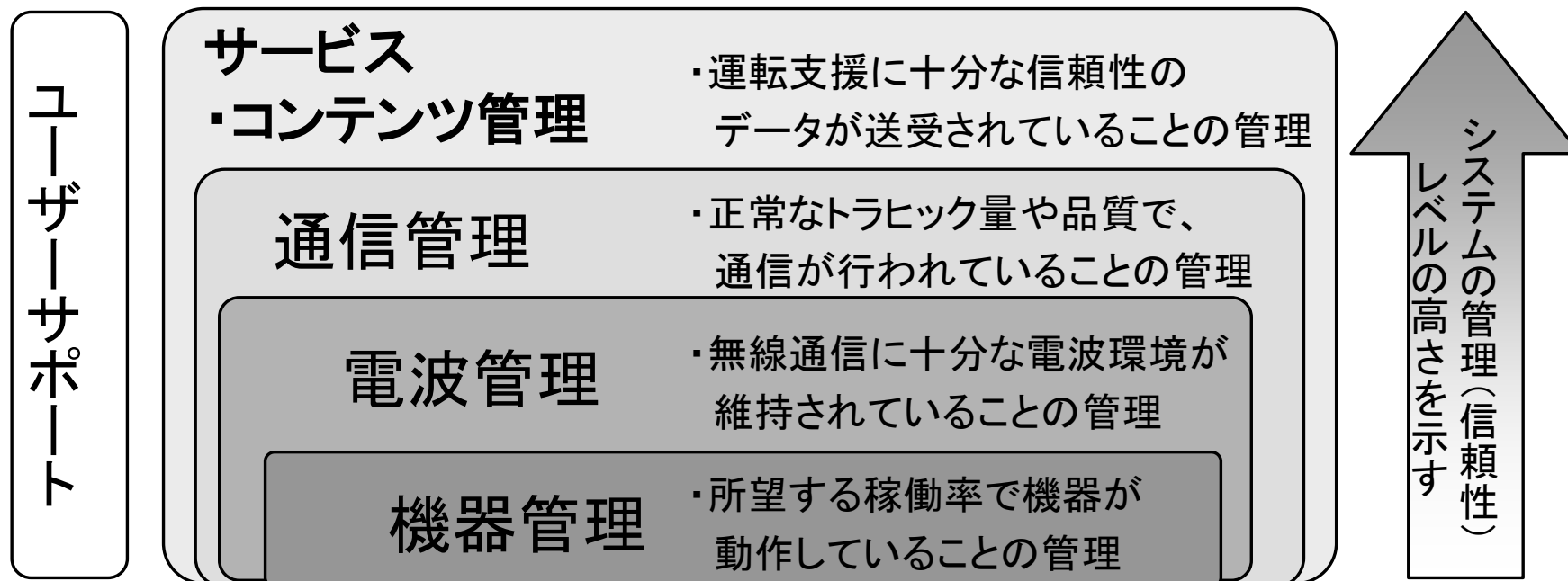
# 【RC-008】運用管理システムの構成



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

運用管理機関がシステムの実用化・運用・維持のために必要とする管理種別は、大きく以下の四つの階層に分類できる。

階層上位より、「サービス・コンテンツ管理」「通信管理」「電波管理」「機器管理」それぞれの管理機能ブロックは包含関係にあり、上位の管理は下位の管理保証も包含する。(例えば、通信管理を行わずにサービス管理を行うことは出来ない)さらに、ユーザーサポートは全ての階層について必要になる。



# 【RC-008】運用管理機関の各フェーズにおける機能の一覧

		機器管理	電波管理	通信管理	サービス・コンテンツ管理
路側機	開発	<ul style="list-style-type: none"> <li>・相互接続性確認試験</li> <li>・機器の認定</li> <li>・機器の型式登録</li> <li>・ロゴマークの管理</li> </ul>			
	製造	<ul style="list-style-type: none"> <li>・IDの管理 (製造時の路側機管理番号の管理)</li> <li>(製造時のS情報関連IDの管理)</li> </ul>			<ul style="list-style-type: none"> <li>・S情報の事前格納</li> </ul>
	設置	<ul style="list-style-type: none"> <li>・IDの管理 (設置時の路側機管理番号の管理)</li> <li>(S情報関連IDの管理)</li> </ul>	<ul style="list-style-type: none"> <li>・電波干渉管理</li> </ul>		<ul style="list-style-type: none"> <li>・S情報の設置時格納およびセットアップ</li> </ul>
	運用	<ul style="list-style-type: none"> <li>・路側機管理番号の閲覧</li> <li>・検索</li> <li>・機器の正常動作管理</li> </ul>	<ul style="list-style-type: none"> <li>・電波の正常動作管理</li> </ul>	<ul style="list-style-type: none"> <li>・通信の正常動作管理</li> <li>・ログの管理</li> </ul>	<ul style="list-style-type: none"> <li>・S情報の更新管理 (S情報のバージョン管理)</li> <li>(S情報更新機能)</li> <li>(S情報再設定機能)</li> <li>(コンテンツ管理機能)</li> </ul>
	ユーザーサポート(問い合わせ対応)				
廃却	<ul style="list-style-type: none"> <li>・IDの管理(抹消) (路側機管理番号及びS情報関連IDの抹消)</li> </ul>				<ul style="list-style-type: none"> <li>・S情報の抹消</li> </ul>

※S情報: 通信における鍵などのセキュリティ情報の略称として表記する

# 【RC-008】運用管理機関の各フェーズにおける機能の一覧

		機器管理	電波管理	通信管理	サービス・コンテンツ管理	
車載機	開発	<ul style="list-style-type: none"> <li>・相互接続性確認試験</li> <li>・機器の認定</li> <li>・機器の型式登録</li> <li>・ロゴマークの管理</li> </ul>				
	製造	<ul style="list-style-type: none"> <li>・IDの管理 (製造時の車載器管理番号の管理)</li> <li>(製造時のS情報関連IDの管理)</li> </ul>			<ul style="list-style-type: none"> <li>・S情報の事前格納</li> </ul>	
	販売	<ul style="list-style-type: none"> <li>・IDの管理 (販売時の車載器管理番号の管理)</li> <li>(S情報関連ID管理)</li> <li>・車両情報等の登録管理</li> </ul>			<ul style="list-style-type: none"> <li>・S情報の販売時格納およびセットアップ</li> </ul>	
	運用	<ul style="list-style-type: none"> <li>・車載器管理番号の閲覧・検索</li> <li>・機器の正常動作管理</li> </ul>	ライフサイクル管理	<ul style="list-style-type: none"> <li>・電波の正常動作管理</li> </ul>	<ul style="list-style-type: none"> <li>・通信の正常動作管理</li> <li>・ログの管理</li> </ul>	<ul style="list-style-type: none"> <li>・S情報の更新管理 (S情報更新機能)</li> </ul>
	ユーザーサポート(問い合わせ対応)					
	売却／廃却	<ul style="list-style-type: none"> <li>・IDの管理(抹消) (車載器管理番号及びS情報関連IDの抹消)</li> <li>・車両情報などの抹消</li> </ul>				<ul style="list-style-type: none"> <li>・S情報の抹消</li> </ul>

※S情報:通信における鍵などのセキュリティ情報の略称として表記する

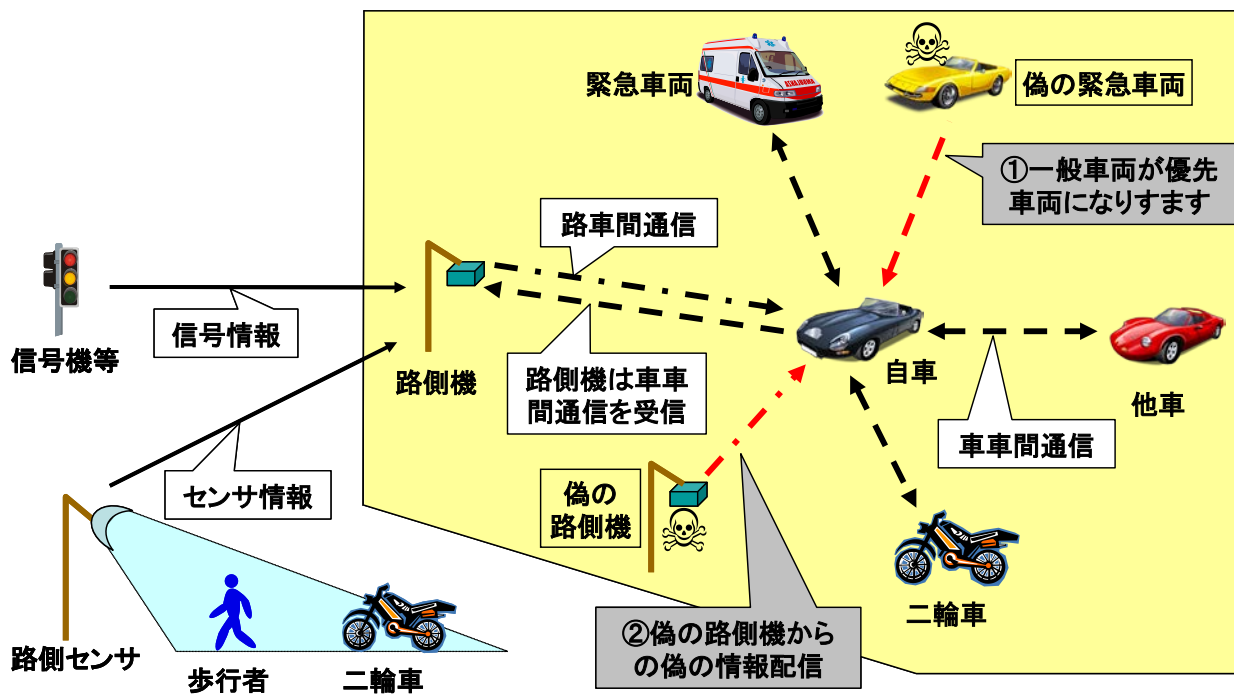
運転支援通信システムの通信路を対象に、脅威分析と対策を検討し、セキュリティの必要性を確認

## 脅威

- ① 一般車両による優先車両へのなりすまし
- ② 偽情報配信による交通の混乱や事故の発生
- ③ 通信内容漏洩による別目的への悪用

## 対策

- ① 発信元の真正性の確認
- ② メッセージの完全性の確認
- ③ 情報の機密性の確保



# 【RC-009】脅威分析結果

運用管理機関としては、なりすまし、リプレイ攻撃対策として  
メッセージの完全性・真正性の確保が必要

No.	主な脅威	リスク (*)	攻撃対象	対策	対策責任者
1	なりすまし	4	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	6			
3	装置改ざん	6	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
4	マルウェア	6	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
5	入力情報の改ざん	6	車載機・路側機への 接続機器	接続仕様の非公開等	
6	Jamming	6	無線通信	(法規制)	関係省庁
7	DoS	4		(法規制)	
8	偽GPS信号	4	無線通信信号(GPS)	(法規制)	
9	盗聴	3	無線通信信号	サービスアプリレベルの セキュリティ導入	サービス提供者
10	ロケーショントラッキング	3	-	-	-

(\*)具体的なリスク値算出方法はRC-009参照