

総務省予算事業の報告

次世代ITSの確立に向けた通信技術に関する調査 実証実験の結果概要報告

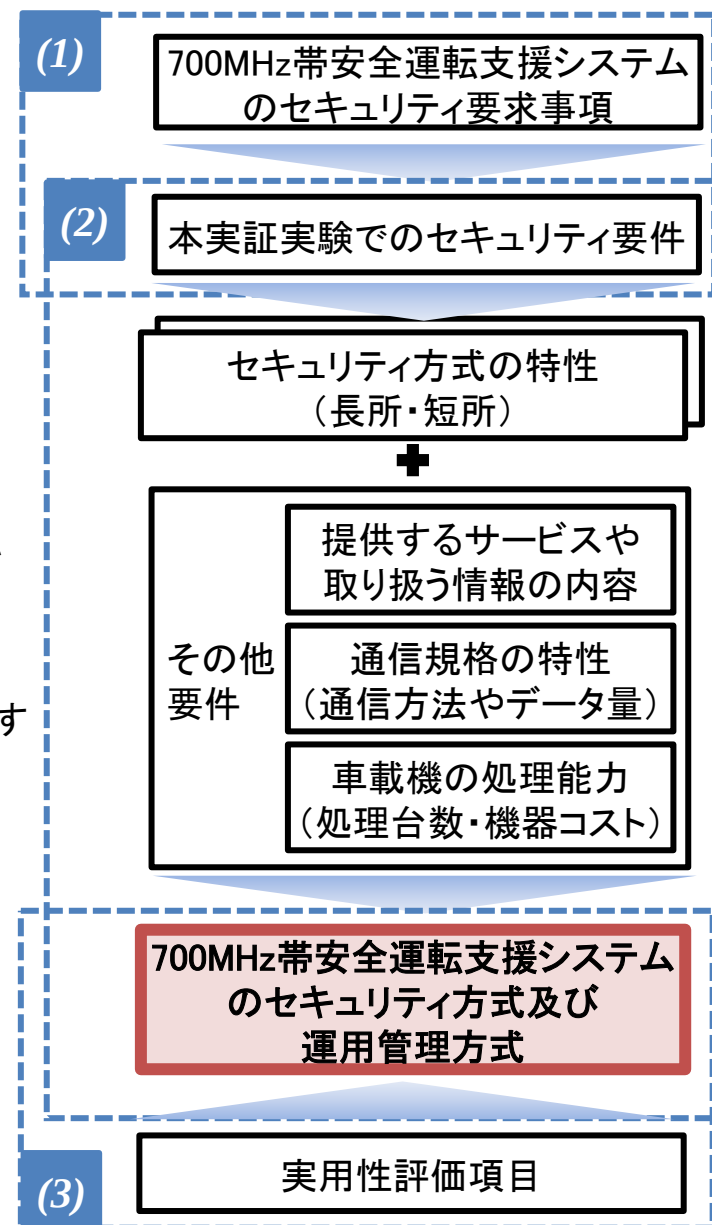
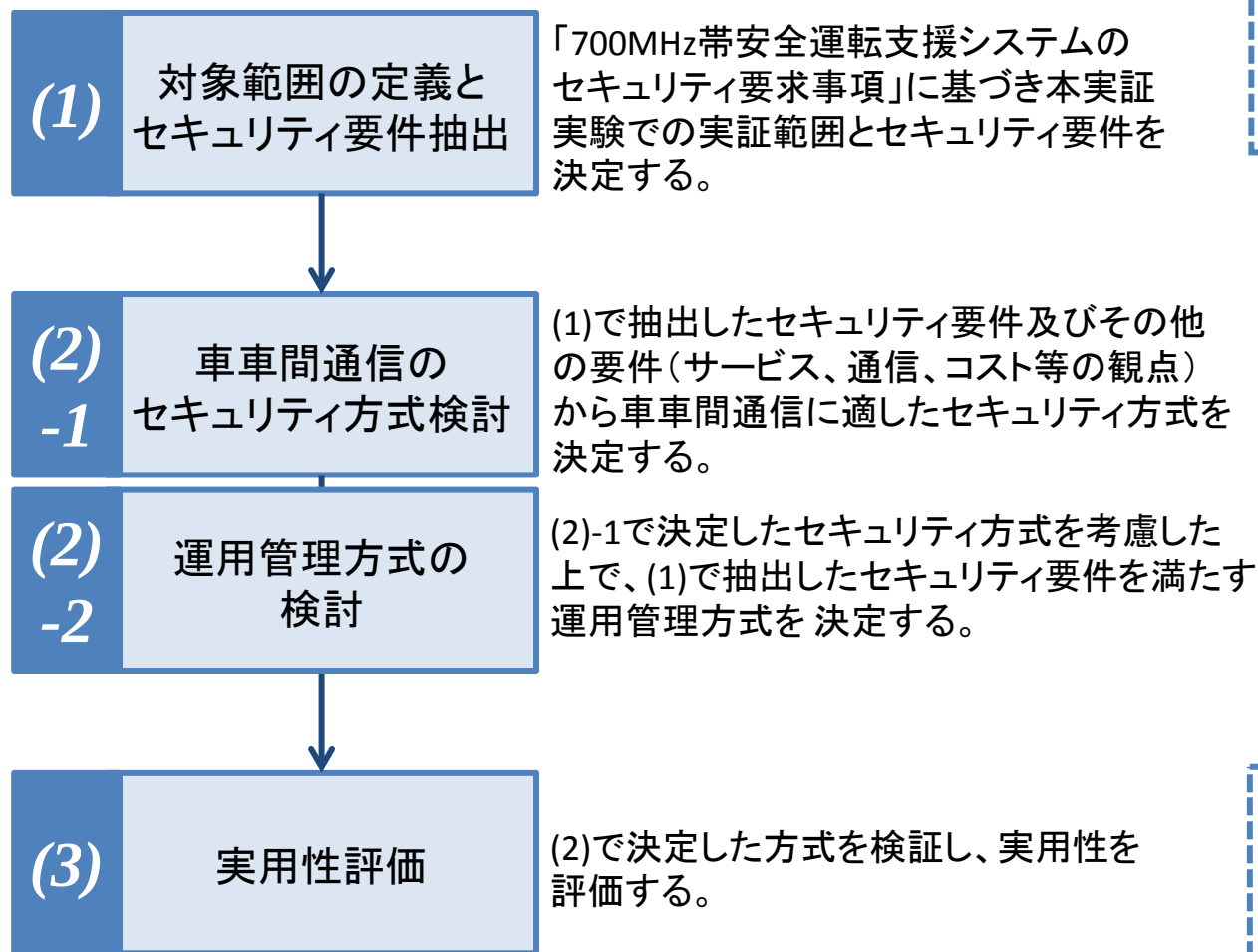
平成27年3月16日

次世代ITSの確立に向けた通信技術に関する調査検討会
事務局
豊田通商（株）

1. セキュリティ機能の検討 検討項目の進め方

第1回調査検討会資料より

[セキュリティ検証の進め方について]



1. セキュリティ機能の検討 検討結果の報告

ア. セキュリティ機能の検討 [検討状況の報告]

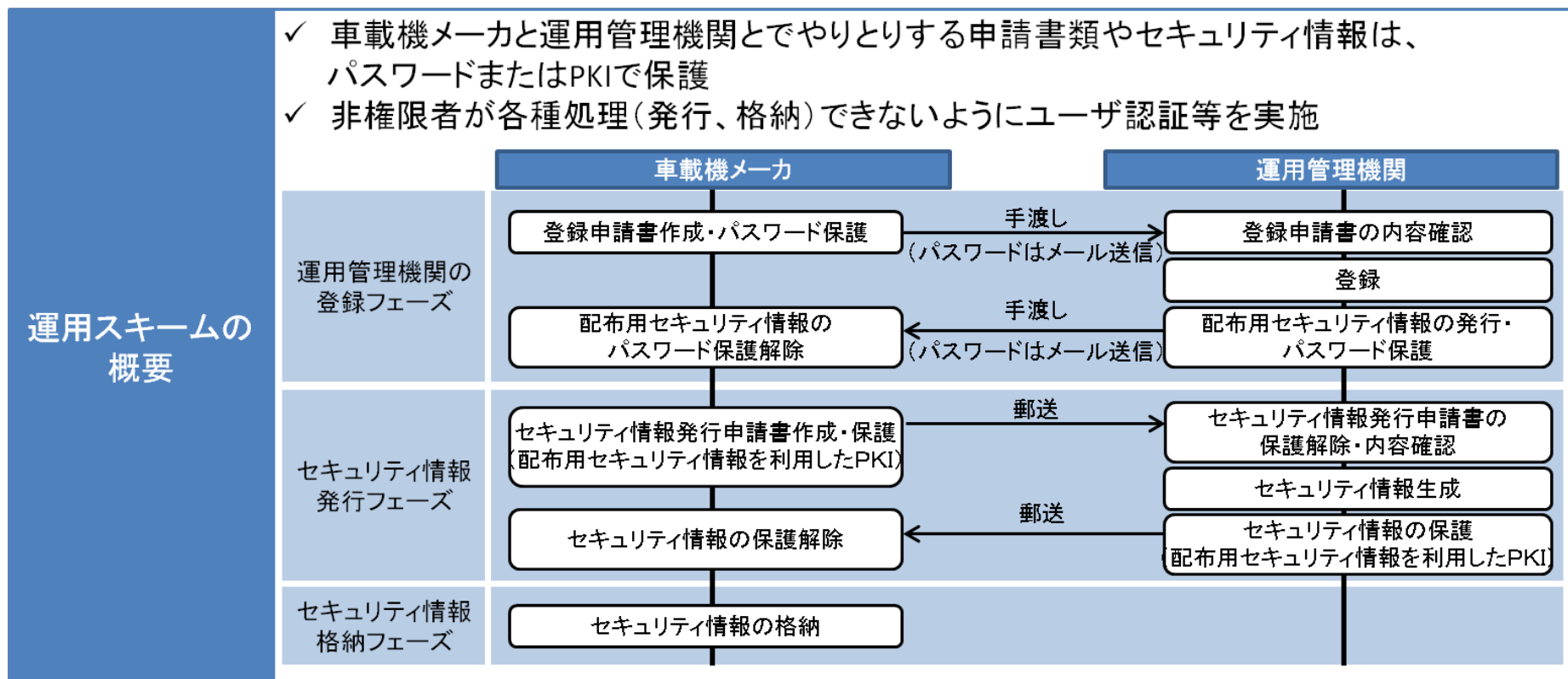
検討項目(第1回調査検討会資料のセキュリティ検証の進め方より)		検討状況
①	対象範囲の定義とセキュリティ要件抽出	「700MHz帯安全運転支援システムのセキュリティ要求事項」(以降、要求事項)を踏まえ、検証すべきセキュリティ要件を確認(第2回調査検討会で報告済)。
②-1	車車間通信のセキュリティ方式検討	・要求事項の車車間通信におけるセキュリティ要件「車載機が送信する情報の真正性・完全性、機密性の確保」を満たす方式を検討(第2回調査検討会で報告済)。
②-2	運用管理方式の検討	セキュリティ情報の発行、格納、更新時の脅威分析を実施し、セキュリティ要件を抽出。また、その他の要件を整理し、要件に基づいた運用管理方式を検討(第2回調査検討会で報告済)。
③-1	車車間通信のセキュリティ方式の実用性評価	室内環境で車載機を用いて評価を実施し、実用性を確認(第2回調査検討会で報告済)。
③-2	運用管理方式の実用性評価	②-2について「安全性」「確実性」「効率性」の観点からの検証を1月に実施。

1. セキュリティ機能の検討 ②-2 運用管理方式の検討

第2回調査検討会資料より

[運用管理方式の検討] セキュリティ要件や前提条件等を考慮し、運用管理方式を検討

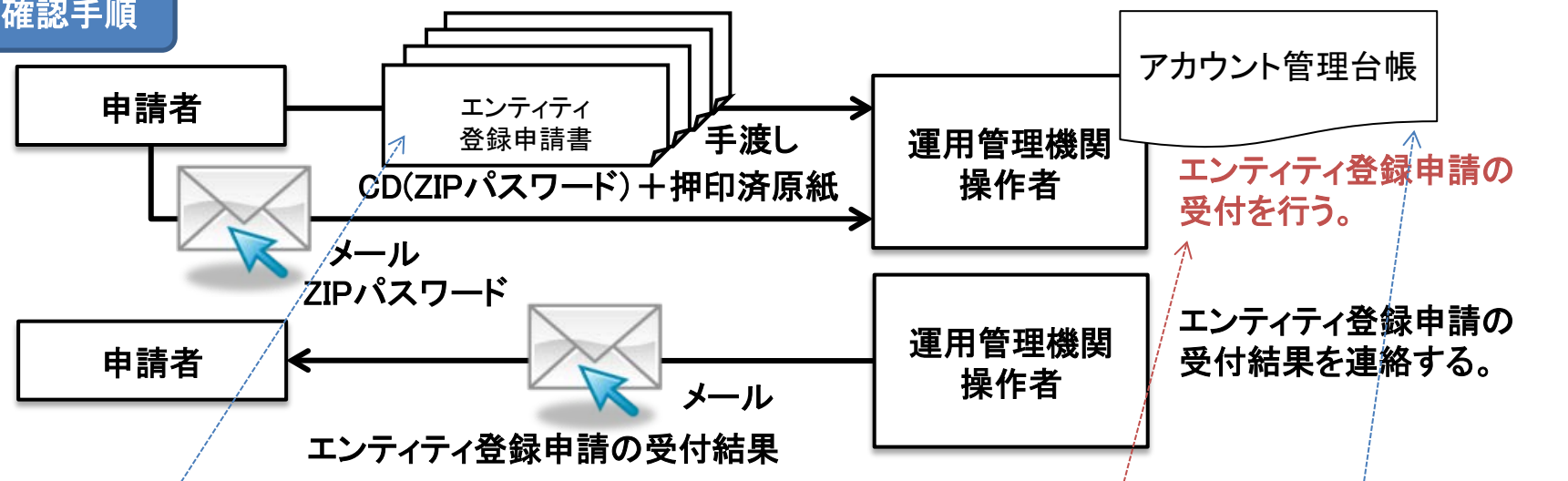
主な セキュリティ要件 (要求事項より)	(1) セキュリティ情報を適切な方法で発行すること (2) セキュリティ情報の機密性・完全性・真正性を確保すること (3) セキュリティ情報を適切な手段で格納すること
主な前提条件 (要求事項より)	(1) セキュリティ情報の発行、格納に用いられる装置は外部ネットワークに接続されない (2) セキュリティ情報は、運用管理機関から車載機メーカー等に媒体で配布される



1. セキュリティ機能の検討 ③-2 運用管理方式の実用性評価

実用性評価の検証例:エンティティ(事業者)登録

確認手順



■登録受付時のチェック内容

- CD(電子データ)の内容が原紙の内容と同一であること。(改ざんされていないこと。)
 - エンティティ登録申請書はパスワードで暗号化されていること。
 - 申請者より別途連絡されたパスワードで暗号化されていること。
- エンティティ登録申請書記載事項がアカウント管理台帳で管理されている通りであること。
 - 登録されているアカウントIDであること。

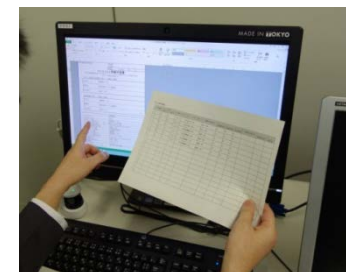
以上が満たされた場合のみ、運用管理機関はエンティティ登録申請を受け付ける。

■エンティティ登録申請書(記載項目)

- ・アカウント登録担当者(会社名、部署名、担当者名 ※署名は自筆)
- ・申請者(会社名、部署名、担当者名 ※捺印、署名は自筆)
- ・アカウントID、アカウント名称
- ・エンティティ分類
- ・代表者氏名、会社住所、
- ・電話番号、メールアドレス、FAX番号、問合せID

■アカウント台帳(記載項目)

- ・申請番号
- ・受付(受付日、受付者)
- ・登録日
- ・アカウントID、・アカウント名称
- ・登録担当者氏名、・削除担当者氏名



1. セキュリティ機能の検討

③-2 運用管理方式の実用性評価

運用管理方式の実用性評価

想定する攻撃は第2回調査検討会で報告済、
確実性の一部及び効率性検証はヒアリング評価を実施

安全性検証において想定する攻撃	主な検証結果
車載機メーカーへのなりすまし	・攻撃者が車載機メーカーになりすまし、運用管理機関に登録申請書を持ってきた場合、登録を受け付けないことを確認 ・攻撃者が車載機メーカーになりすまし、運用管理機関にセキュリティ情報発行申請書を送付した場合、発行申請書の真正性確認でなりすましを検知することを確認
車載機メーカーと運用管理機関でやりとりする情報の配布経路での攻撃(*)	・登録申請書はパスワードで保護されていることを確認 ・セキュリティ情報はPKI親展保護されていることを確認
非権限者による勝手な処理実施	・権限者以外はセキュリティ情報管理システムにログインできないことを確認 ・権限以外の業務画面にアクセスできないことを確認
確実性検証において想定するミス	主な検証結果
申請書の不備、及びシステムへの入力ミス	ヒアリングの結果、申請書記入・システム入力内容で少々不明点が判明、実用化開始時にはマニュアル等の充実化を図るよう提言
配布先ミス	各種申請書及びセキュリティ情報発行申請書はセキュリティ保護した上で配布することで、配布先ミス時の情報漏洩対策を施していることを確認
発行、格納処理ミス	ヒアリングの結果、今回の検証範囲では、ミスが発生しそうな箇所は見当たらなかった
効率性検証	ヒアリング
非効率と思う点をヒアリング	多数の車載機メーカーを登録する場合(普及期)に向けて、効率化の余地があることが判明

普及期に向けての課題はあるものの、実用化に向けた
今回の検討範囲においては、大きな課題は見当たらなかった

(*)盗難、紛失、すり替え、改ざん

2. 総合検証 検討項目の進め方

エ. 総合検証

700MHz帯車車間通信等の通信の観点からの運用に関する検討

ア. セキュリティ機能

- ✓ セキュリティ要件抽出
- ✓ セキュリティ方式検討
- ✓ 運用管理方式の検討
- ✓ 実用性評価



【アウトプット】

- ・SAM: Secure Access Module
- ・セキュリティ情報(鍵)

イ. メッセージセット及び通信プロトコル

- ✓ メッセージ情報抽出
- ✓ 仕様の検討
- ✓ メッセージセット及び通信プロトコルの策定



【アウトプット】

- ・メッセージセット
- ・通信プロトコル

ウ. 相互接続試験

- ✓ 仕様・規定などの整備
- ✓ 試験内容の妥当性検証
- ✓ 試験実施の準備
- ✓ 手順・試験の実証



【アウトプット】

- ・試験要領書/試験用治具
- ・機器認定判定基準

エ. 総合検証

ア. イ. ウ. の要件を満たす車載機を搭載した車両を用い実際に車車間通信ができることを検証

- ✓ 車車間通信によりセキュリティ情報やメッセージセットで伝達される情報が判別できる
- ✓ 動的に変化する情報が車車間通信により伝達されることを確認する
- ✓ 複数車両メーカーの車両と複数車載機メーカーの車載機を組み合わせ検証する
- ✓ 公道を模擬した実験環境(テストコース)と公道で検証する

2. 総合検証 実験概要

[実験概要]

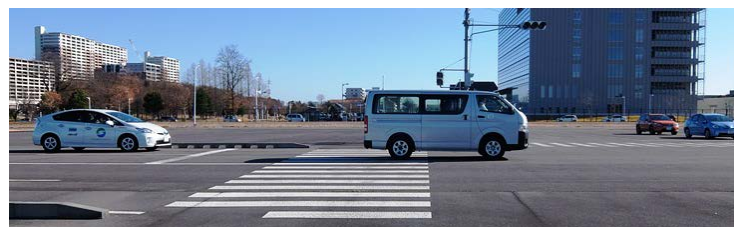
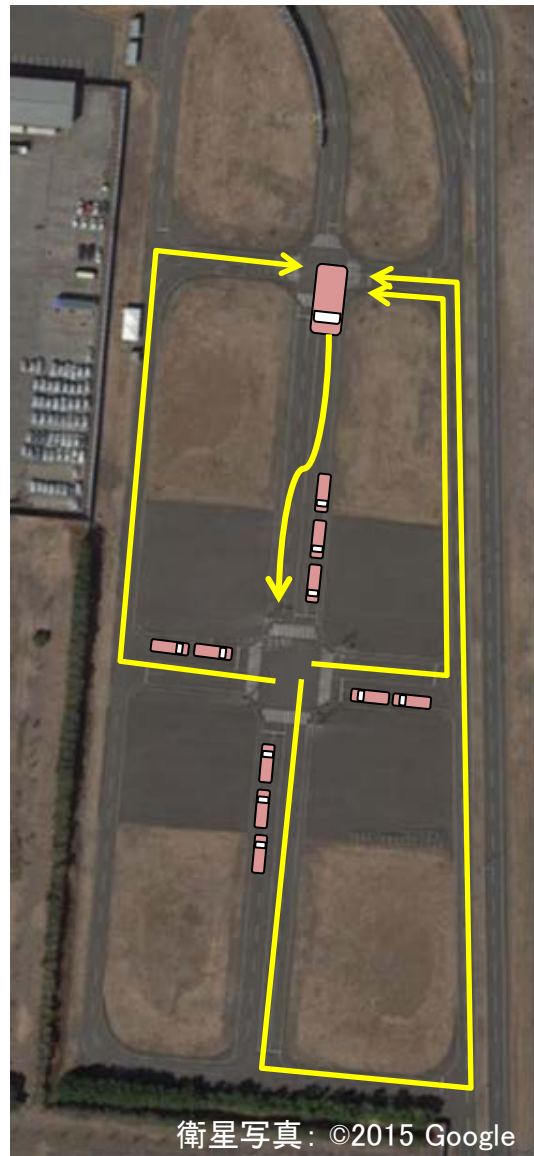
実験場所	実験内容	目的
テストコース (JARI模擬市街路)	・緊急車両×なりすまし緊急車両	セキュリティ情報による緊急車両判別の検証 ・メッセージセット: 緊急車両 ・セキュリティ: 緊急車両×一般車両
	・一般車両メッセージ受信(静止)	メッセージ内容判別の検証 ・伝達情報の内容確認
	・緊急車両メッセージ受信(状態変化) ・一般車両メッセージ受信(走行)	動的に変化する情報の車車間通信による伝達の検証 ・緊急車両状態変化(緊急⇄通常)判別の検証 ・伝達情報の内容確認
公道(YRP:横須賀市)	・一般車両メッセージ受信(走行)	実環境における情報伝達の検証 ・伝達情報の内容確認 ・実環境の情報伝達に与える影響の把握

[実験規模]

実験場所	車両種別	台数	役割
テストコース (JARI模擬市街路)	緊急車両	1	実際の緊急車両を模擬する
	なりすまし緊急車両	1	緊急車両なりすまし(一般車用セキュリティ)
	一般車両	10	車車間通信データの取得
公道(YRP:横須賀市)	一般車両	6	車車間通信データの取得

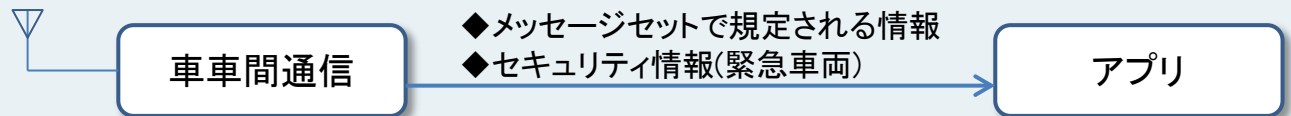
2. 総合検証 実証実験結果報告(テストコース)

[テストコース: JARI模擬市街地路] 実験の様子 (平成26年12月23日～25日実施)



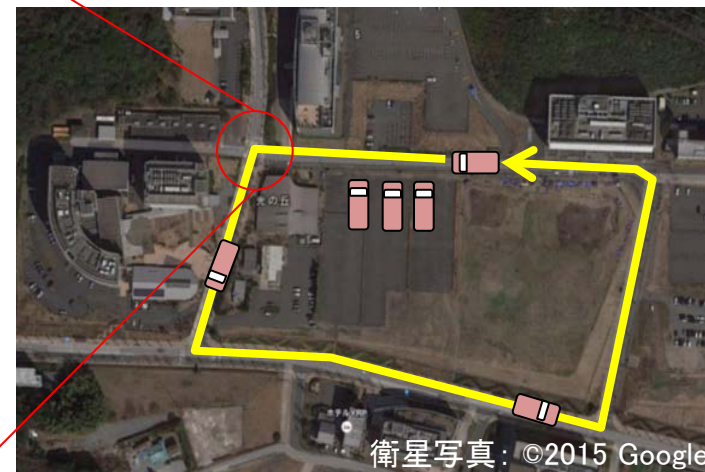
2. 総合検証 実証実験結果報告(テストコース)

[テストコース: JARI模擬市街地路]

	実験内容	目的
1	・緊急車両×なりすまし緊急車両	セキュリティ情報による緊急車両判別の検証 ・メッセージセット: 緊急車両 ・セキュリティ: 緊急車両×一般車両
	✓ 車車間通信のメッセージセットによる緊急車両情報のやり取りが確認できた ✓ セキュリティ情報を利用して緊急車両のなりすましが検出できることを確認できた 	
2	・一般車両メッセージ受信(静止)	メッセージ内容判別の検証 ・伝達情報の内容確認
	✓ 車車間通信のメッセージセットによる伝達情報が正しいことが確認できた	
3	・緊急車両メッセージ受信(状態変化)	動的に変化する情報の車車間通信による伝達の検証 ・緊急車両状態変化(緊急⇄通常)判別の検証 ・伝達情報の内容確認
	✓ 車車間通信のメッセージセットによる伝達情報が正しいことが確認できた	
4	・一般車両メッセージ受信(走行)	実環境における情報伝達の検証 ・伝達情報の内容確認 ・実環境の情報伝達に与える影響の把握
	✓ 車車間通信のメッセージセットによる伝達情報が正しいことが確認できた	

2. 総合検証 実証実験結果報告(公道)

[公道:YRP周辺路] 実験の様子 (平成27年1月13日～14日実施)



2. 総合検証 実証実験結果報告(公道)

[公道:YRP周辺路]

	実験内容	目的
1	走行車両からの必須項目情報受信(1)	メッセージセットで必須項目とされる情報が正しく伝わっていることの確認 車両①②③が周回、④⑤⑥が駐車 【必須情報】 時刻情報、位置情報、車両状態情報、車両属性情報
	✓ 車車間通信のメッセージセットによる伝達情報が正しいことが確認できた	
2	走行車両からの必須項目情報受信(2)	メッセージセットで必須項目とされる情報が正しく伝わっていることの確認 車両④⑤⑥が周回、①②③が駐車 【必須情報】 時刻情報、位置情報、車両状態情報、車両属性情報
	✓ 車車間通信のメッセージセットによる伝達情報が正しいことが確認できた	
3	走行車両からの必須項目情報受信(3)	メッセージセットで必須項目とされる情報が正しく伝わっていることの確認 車両①②③が左回り周回、④⑤⑥が右回り周回 【必須情報】 時刻情報、位置情報、車両状態情報、車両属性情報
	✓ 車車間通信のメッセージセットによる伝達情報が正しいことが確認できた	

2. 総合検証 まとめ

まとめ

- 公道外に構築した模擬環境(JARI模擬市街路)及び、公道(YRP周辺路)において、「セキュリティ機能」、「メッセージセット及び通信プロトコル」、「相互接続」が適切に動作することを10台以上の車載機と車両を用いて確認することができた。
- セキュリティ情報を発行・管理するシステムの要件、試験実施者が守るべき相互接続性確認試験要領及び被試験車が守るべき運用ガイドライン、車車間通信プロトコル及びメッセージセット等について、反映すべき事項は特になかった。

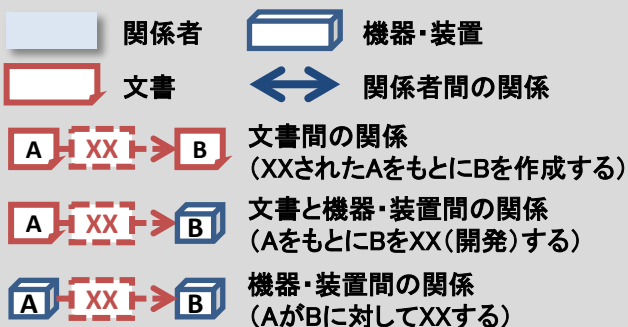


SIPへの連携として、実証実験(横須賀、名古屋、神戸)において、本調査検討にて検証された車載機が活用され、実験後にフィードバックされる。

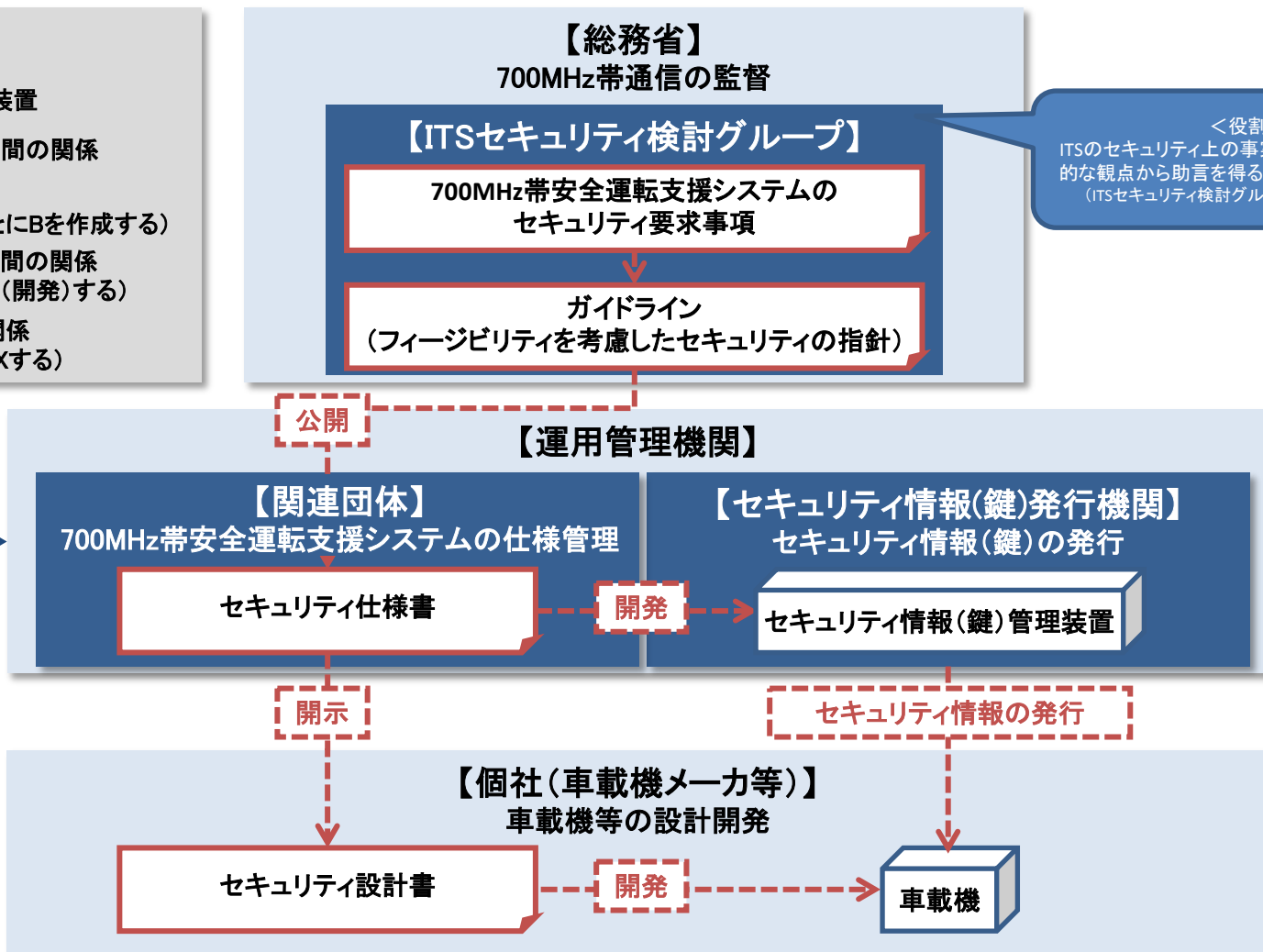
ITSセキュリティ検討グループの役割

ITSセキュリティ検討グループでは、
700MHz帯安全運転支援システムのセキュリティ要求事項をもとに
セキュリティ仕様を検討する際の指針(ガイドライン)を策定する。

凡例

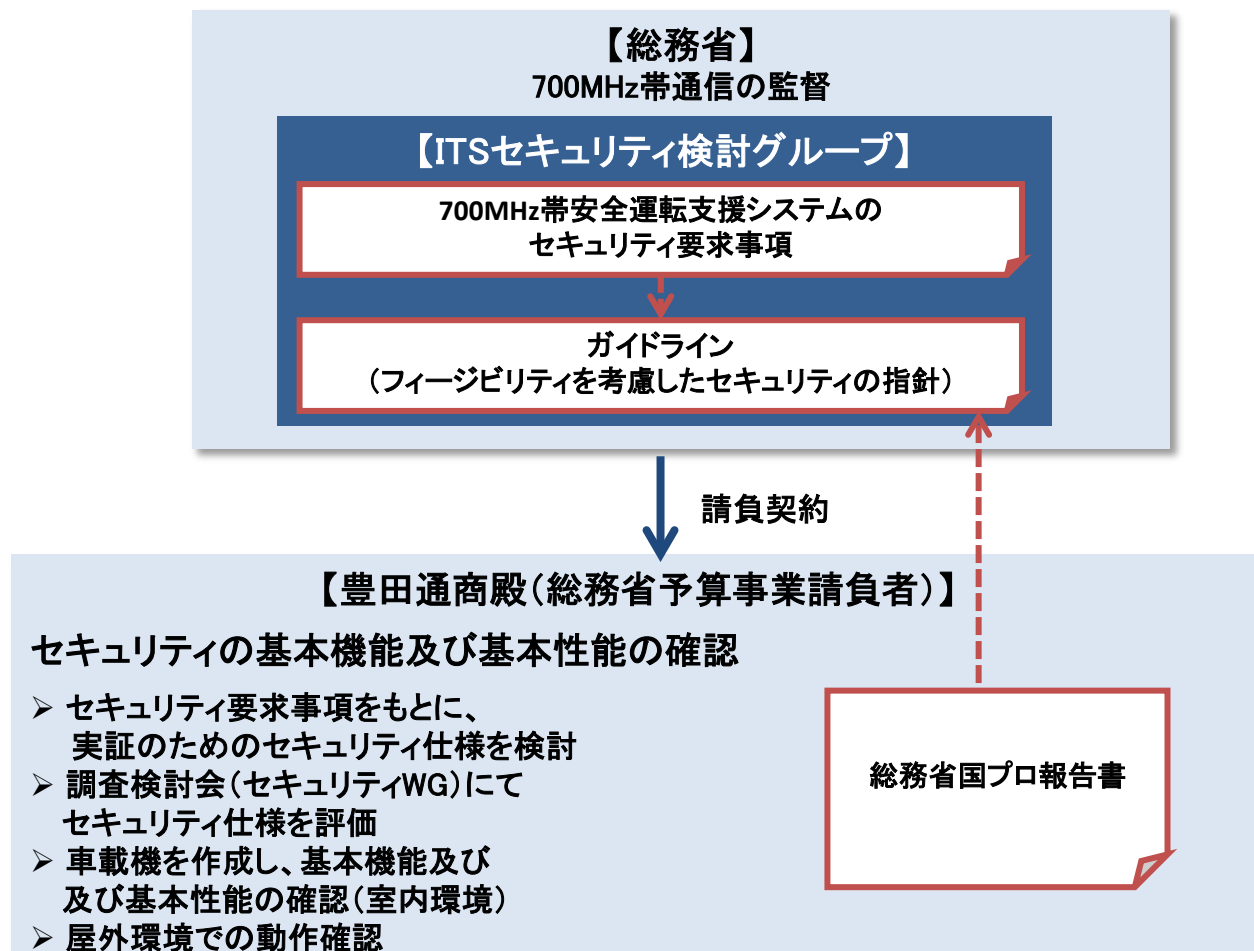


【セキュリティ有識者】
複数の有識者による
セキュリティ仕様の評価



(参考) ガイドライン策定プロセス

ガイドラインは総務省予算事業を踏まえて策定する。



※総務省予算事業で検討したセキュリティ仕様に基づき、SIP予算事業で大規模な実証実験を実施予定。