資料2

700MHz帯安全運転支援システムの
セキュリティ仕様検討のためのガイドライン等について

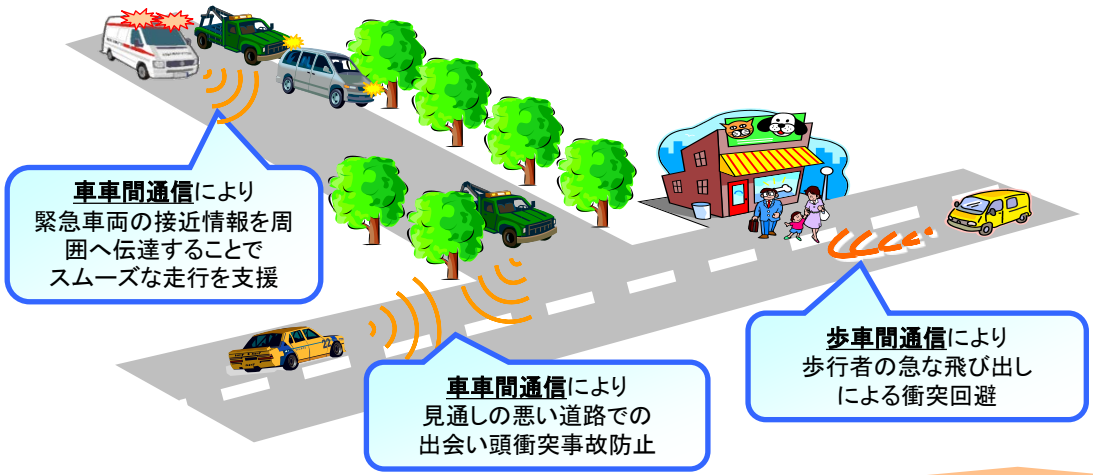
事務局

700MHz帯安全運転支援システムのセキュリティ要求事項の策定

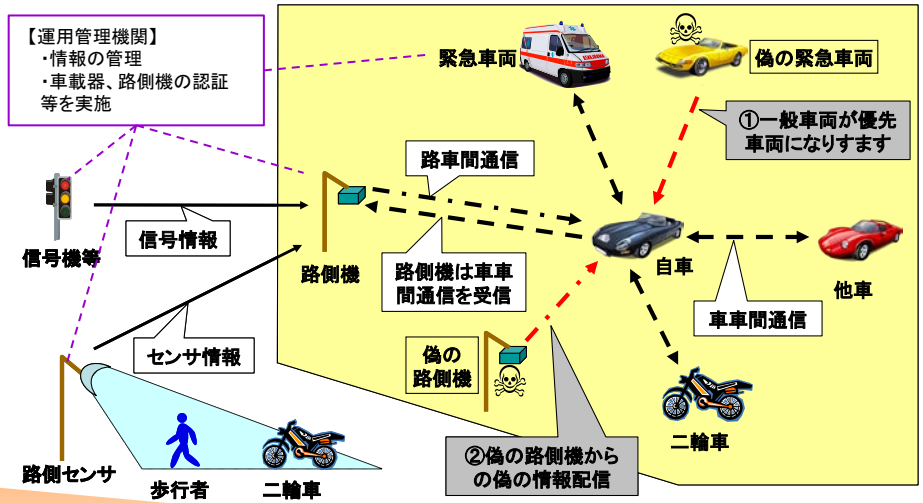
【背景】交通事故による死傷者数は、近年減少傾向にあるものの、依然として深刻な状態。安全・安心で快適な交通社会を実現するためには、既存技術を更に高度化して事故を防ぐこと等が必須であり、従来の自動車単体での運転支援に加え、車と車、車と人等をつなぐ高度な無線通信技術を活用した安全運転支援システムの早期実用化が必要。

しかしながら、適切なセキュリティ対策が実施されなければ、偽情報の配信や、緊急車両へのなりすまし等により、安全運転支援システムの信頼性が失われてしまい、事故の防止に繋がらないといった問題がある。

安全運転支援システムの実現イメージ



想定される脅威



車両メーカ、機器メーカ、運用管理機関等が遵守しなければならないセキュリティ対策について取りまとめ

700MHz帯安全運転支援システムのセキュリティ要求事項

【対策の例】

○車両メーカ
- ・マルウェア（不正なソフトウェア）を検知できるようにする
- ・異常な情報を検知できるようにする　等

○車載器メーカ、路側機メーカ
- ・機器のソフトウェア等を解析できないようにする
- ・セキュリティ情報は適切な鍵長で暗号化する　等

○運用管理機関
- ・情報の発信元の確認や盗聴を防ぐ等のために適切な鍵長により通信情報を暗号化する
- ・セキュリティ情報が漏洩した場合、セキュリティ情報を更新できるようにする
- ・問題が発生した場合に備え、車両メーカ、機器メーカ等との連絡体制、手順を明確にする
- ・セキュリティ情報を管理する区域では入退室の認証をする
- ・セキュリティ機器の認定装置は外部ネットワークと接続しない　等

700MHz帯安全運転支援システムのセキュリティ要求事項の概要

概要

- 高度道路情報システム（ITS）の情報セキュリティ上の要件について検討することを目的として、平成26年2月より「情報セキュリティアドバイザリーボード ITSセキュリティ検討グループ」（主査：松本勉 横浜国立大学大学院教授）を開催。
- 検討グループでの議論を踏まえて、700MHz帯安全運転支援システムにおいて関係者が遵守すべき情報セキュリティ上の基本方針及び要求事項を取りまとめ。具体的には、車車間通信及び路車間通信の情報セキュリティの確保に必要となる要件及び関係者が鍵・電子証明書等のセキュリティ情報を管理・運用する際に必要となる情報セキュリティ上の要件について記載。

具体的内容

第１章　一般事項

本要求事項において対象となる700MHz帯安全運転支援システム及びセキュリティ情報運用管理システムの概要について記載。

第２章　700MHz帯安全運転支援システムにおけるセキュリティ要求事項

システムを用いて提供されるサービス（左折時衝突防止、緊急車両情報提供等の安全運転支援サービス）において、「通信ヘッダ情報」及び「ペイロード情報（インフラ情報、車両情報、汎用情報）」を保護資産として定義し、保護資産を守るために関係者（運用管理機関や車載器メーカ等）が遵守すべき基本方針とセキュリティ要求事項を規定。

【基本方針】

- セキュリティ管理体制を構築し、セキュリティの維持・向上に努めること。
- 保護資産である通信情報に対して、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こと。
- セキュリティに関するインシデントが発生した場合は、関係者が連携し、適切な対策を速やかに行うこと。

【セキュリティ要求事項】

- ✓ **発信元の真正性確認**：第三者によるなりすましを防ぐために、通信情報の発信元及び受信先において、セキュリティ情報を用いて発信元が正しく本人であることを確認できること。
- ✓ **通信情報の完全性確認**：通信情報の改ざんを防ぐために、通信情報の発信元及び受信先において、セキュリティ情報を用いて情報が改ざんされていないことを確認できること。
- ✓ **通信情報の機密性維持**：第三者による盗聴を防ぐために、発信元においてセキュリティ情報を用いて通信情報を暗号化し、受信先において暗号化された情報を復号できること。
- ✓ 上記3要件の実現方法として、通信規格の制約（通信データ量等）や車載器・路側機の処理能力（処理台数、コスト）を考慮した適切な暗号アルゴリズムと鍵長を用いること。
- ✓ 運用管理機関において、要求事項を実現するためのセキュリティ仕様書及び運用管理規定を作成すること。

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

700MHz帯安全運転支援システムにおける情報セキュリティを確保するために重要となる「セキュリティ情報」を保護資産として定義し、その管理・運用（セキュリティ情報の生成、配布、保管、格納等）に当たって、関係者（運用管理機関や車載器メーカ等）が遵守すべき基本方針とセキュリティ要求事項を規定。

【基本方針】

- セキュリティ管理体制を構築し、セキュリティの維持・向上に努めること。
- 保護資産であるセキュリティ情報に対して、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こと。
- セキュリティに関するインシデントが発生した場合は、関係者が連携し、適切な対策を速やかに行うこと。

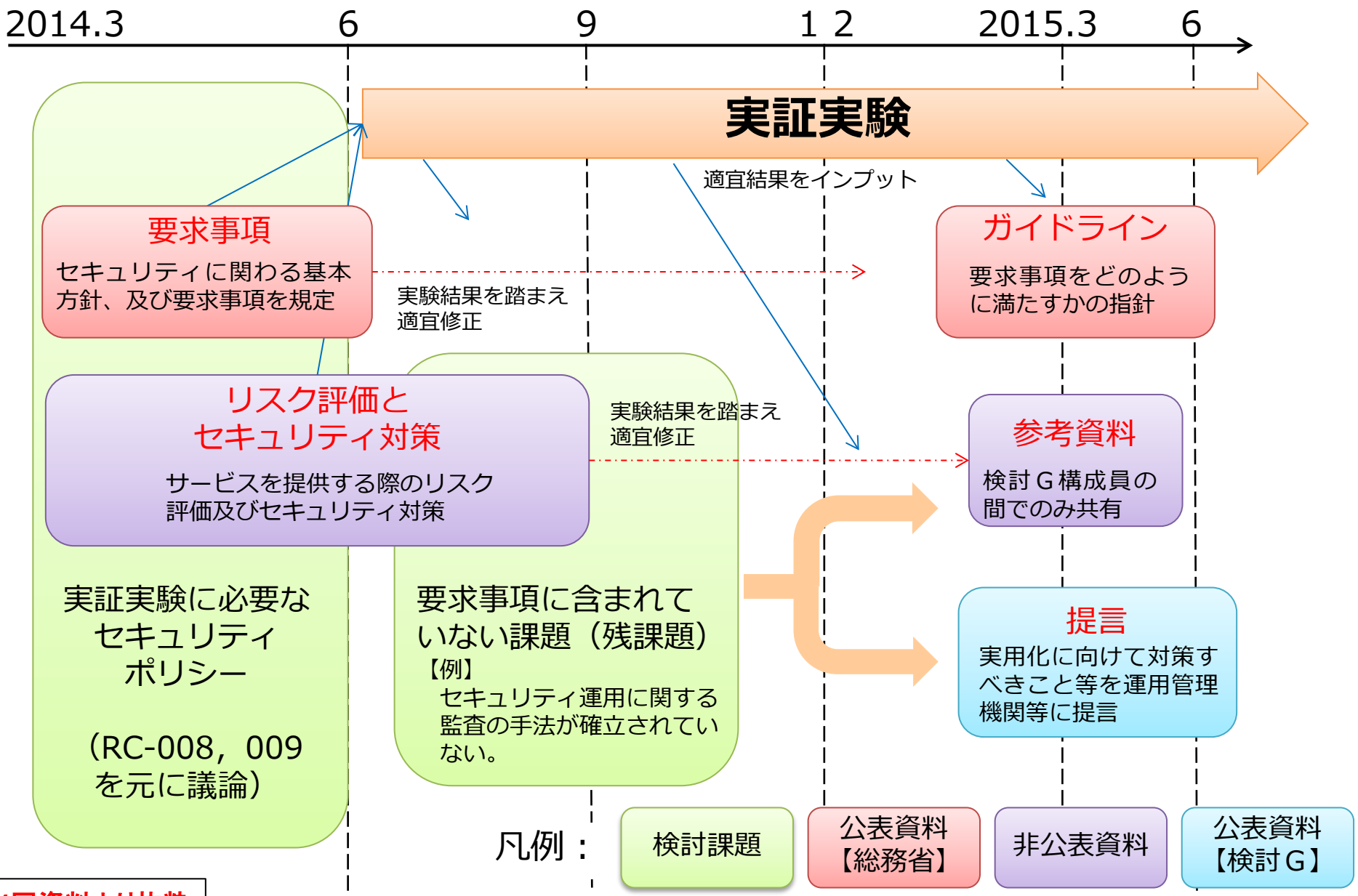
【セキュリティ要求事項】

- ✓ 入退室管理や端末のユーザ認証等により、許可のない者がシステムを扱うことができないようにすること。
- ✓ 端末からセキュリティ情報を生成、出力、配布等を行う際には適切な暗号アルゴリズムと鍵長で暗号化し、セキュリティ情報の真正性・完全性・機密性を確保すること。
- ✓ 各端末は外部ネットワークに接続しないようにし、また、USBメモリ等を接続する際にはマルウェア感染等に気をつけること。

付録　インシデント対応

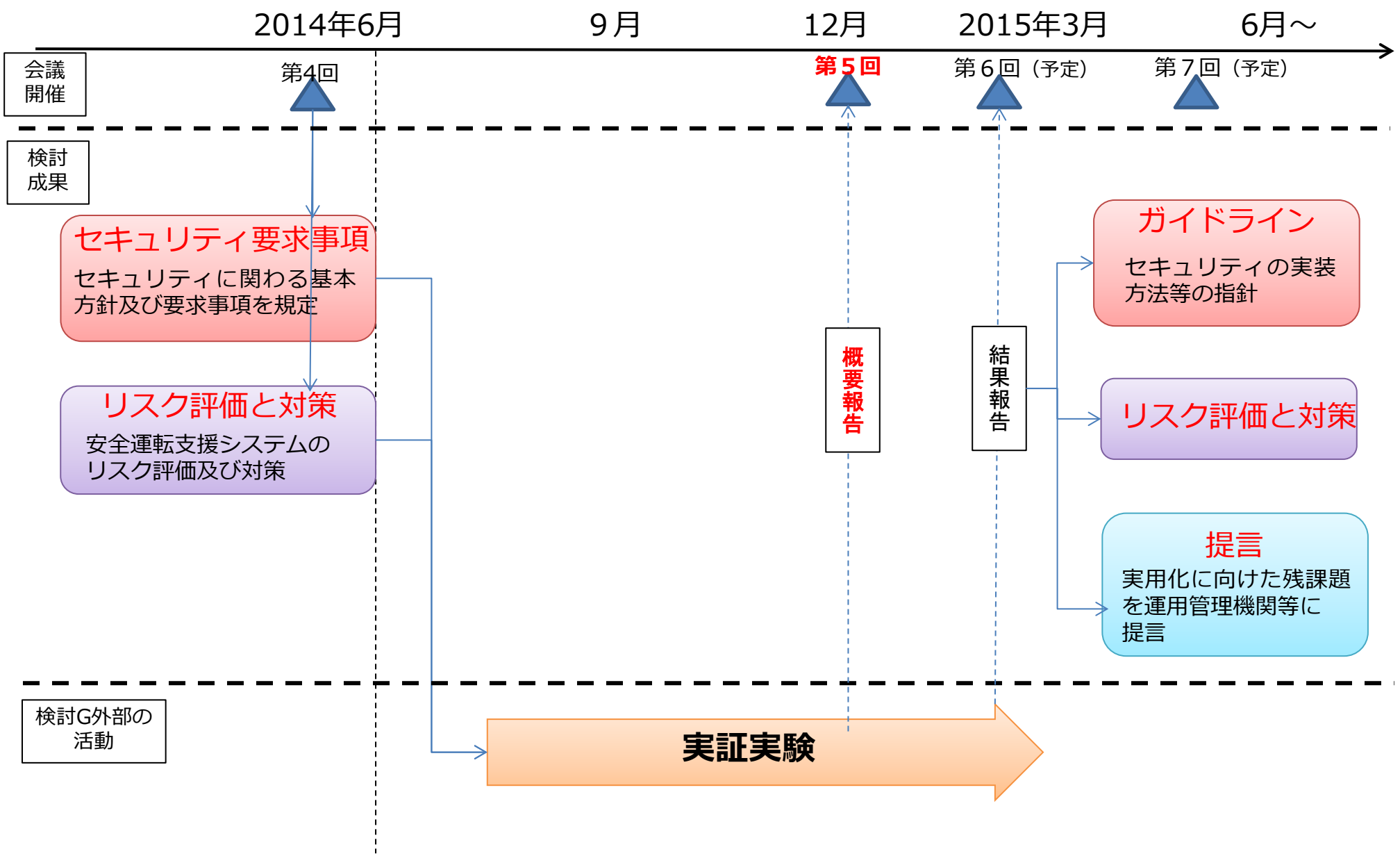
本要求事項において想定されるインシデント例、インシデント対応における関係者、インシデント対応フローについて記載

ITSセキュリティ検討グループの今後の進め方 H26.5.30



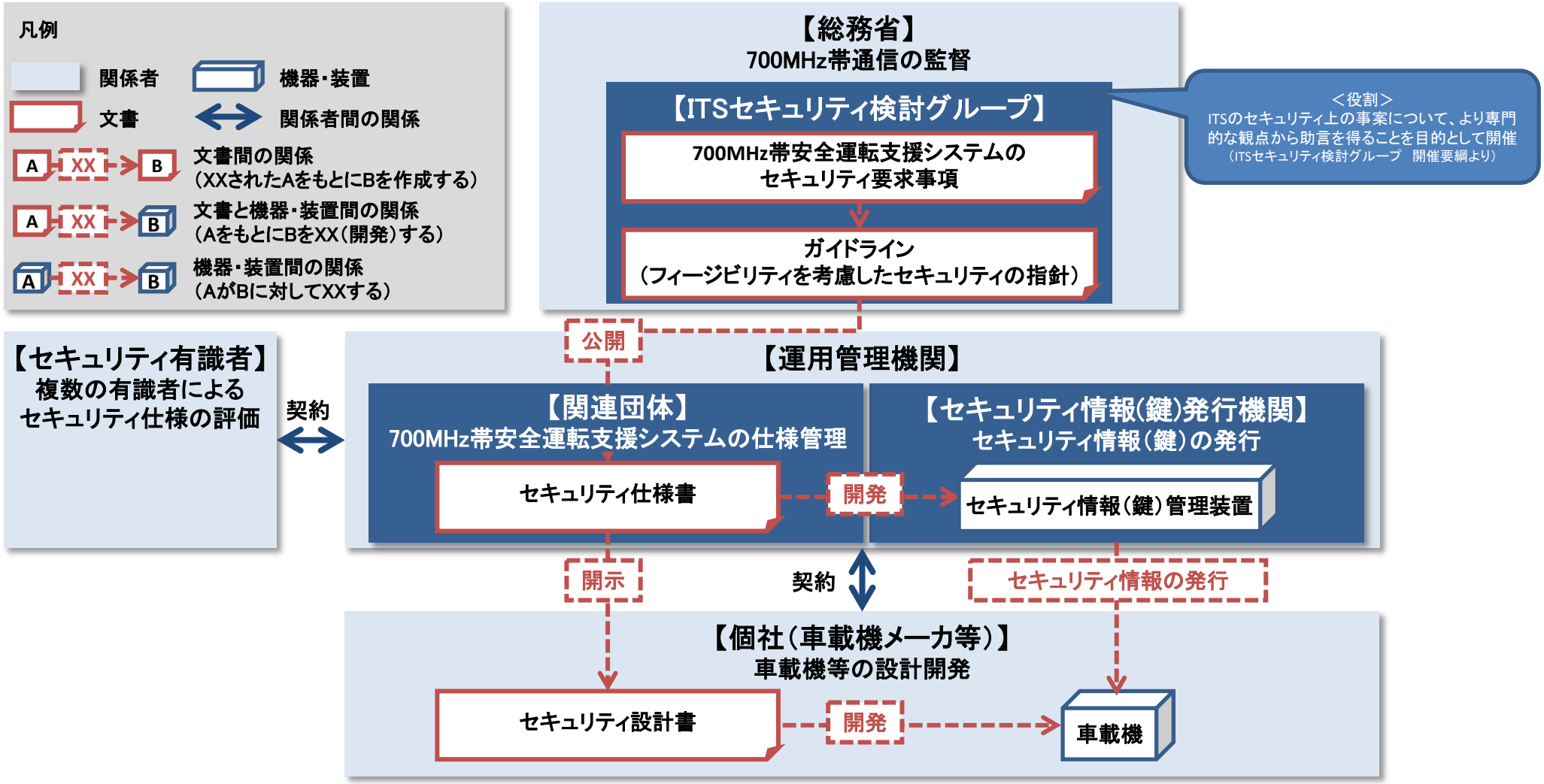
第4回資料より抜粋

ITSセキュリティ検討グループの今後の進め方の方針（案）



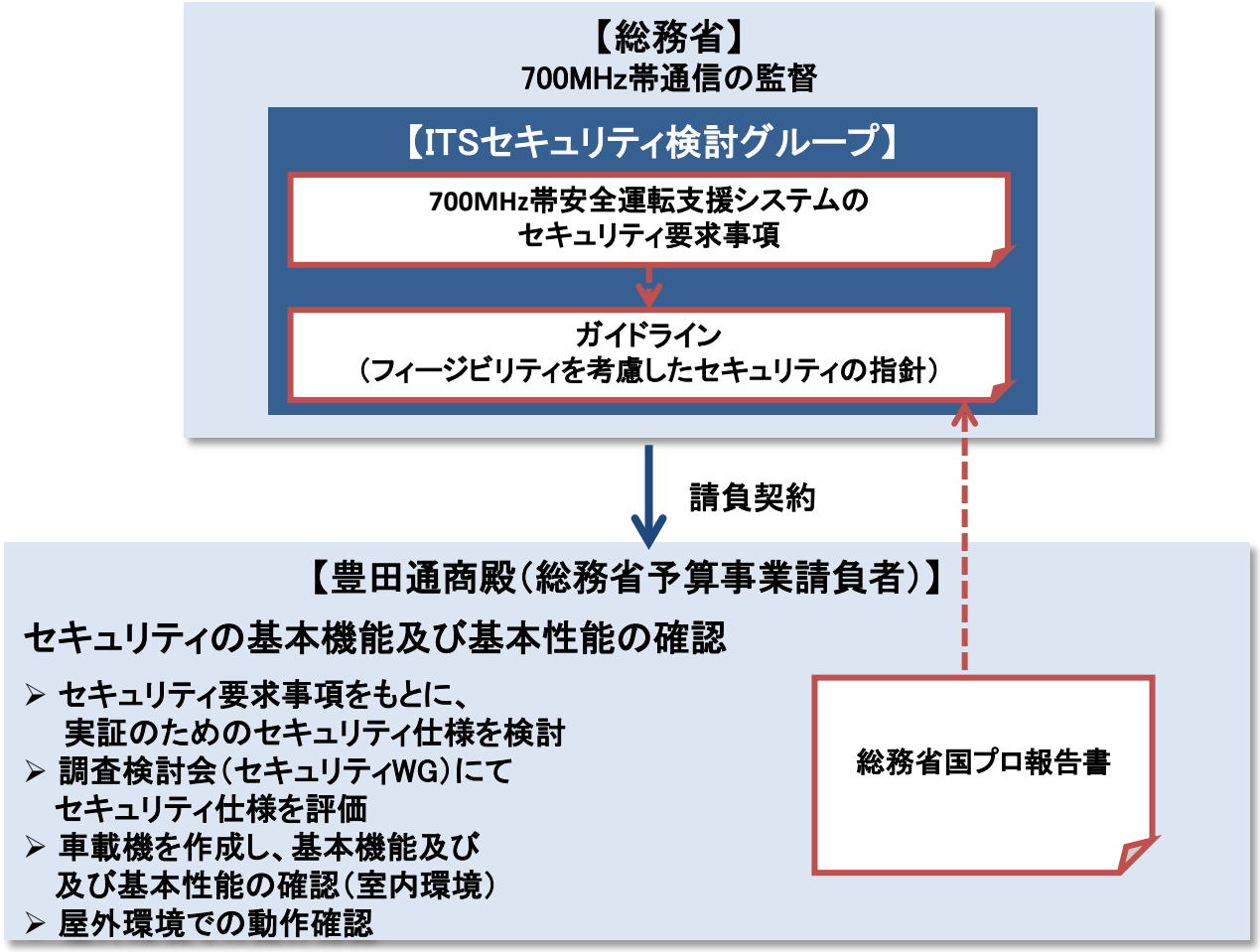
ITSセキュリティ検討グループの役割

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。



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。