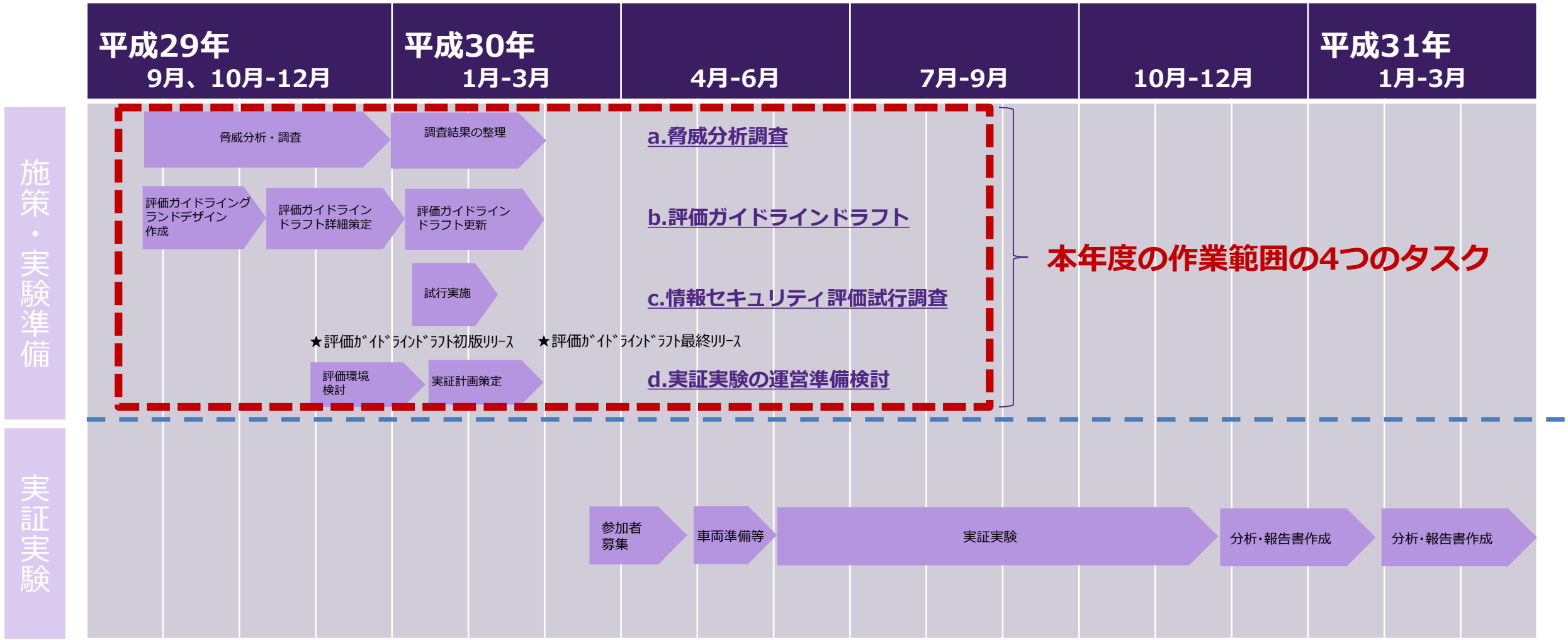
国立研究開発法人新エネルギー・産業技術総合開発機構　御中

「戦略的イノベーション創造プログラム（SIP）自動走行システム／大規模実証実験」のうち「情報セキュリティ実証実験」

業務報告書　概要版

日本シノプシス合同会社
名古屋大学大学院
パナソニック株式会社 製品セキュリティセンター
国立開発法人 産業技術総合研究所

本年度の業務範囲



SYNOPSYS®

a.脅威分析調査

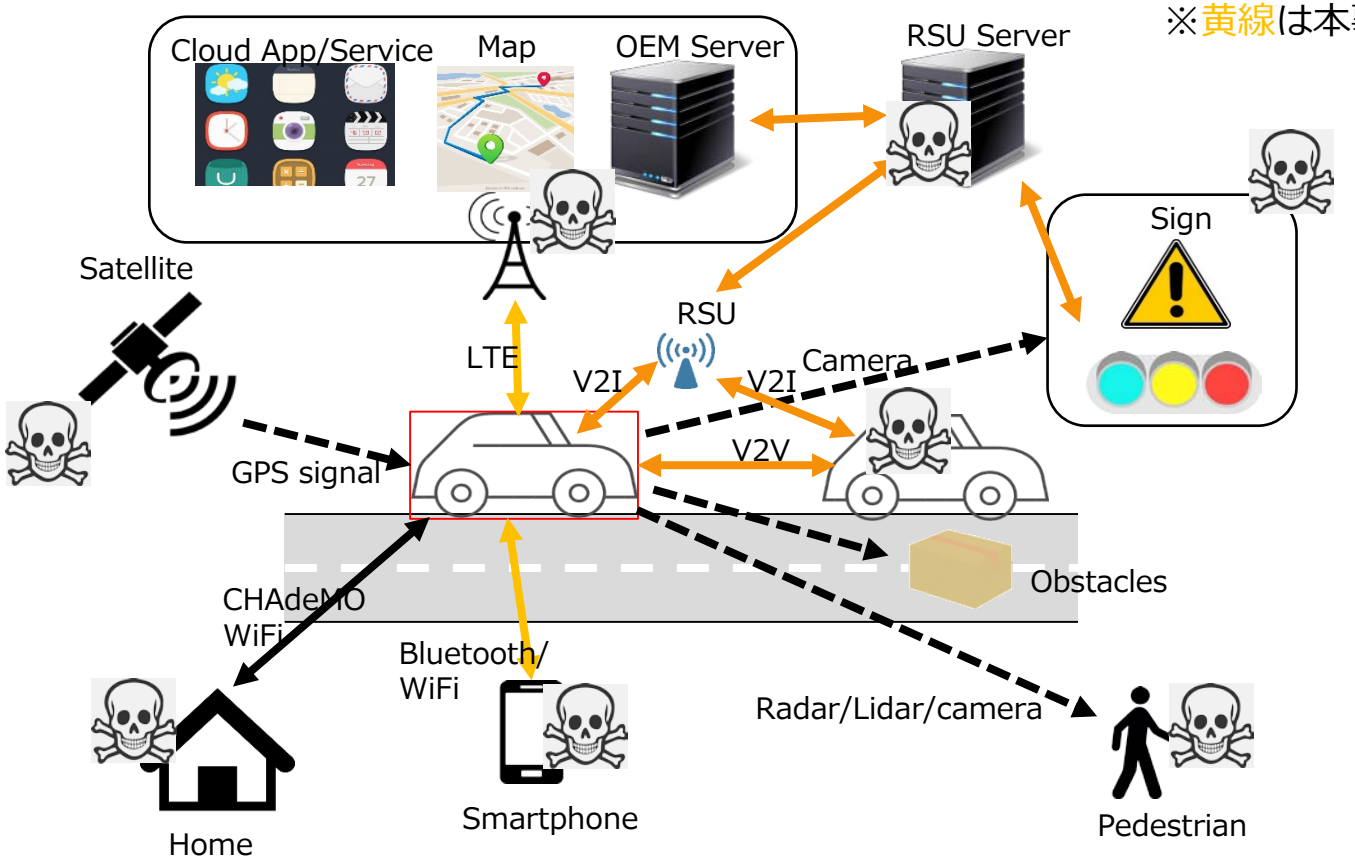
SYNOPSYS®

脅威の全体像

- 接続機器が増えるとセキュリティ観点で以下の2点が重要になる
  - –1) 通信する相手に騙されない
  - –2) 車両内の情報の改ざんや乗っ取りなどへの対抗

※青線はSIP-V2Xで検討

※黄線は本事業で検討



SYNOPSYS®

脅威分析の流れ

- 以下の4手順で分析

① 調査と類型化

–車両システムや機能を調査し類型化を実施

② 脅威分析

–脅威分析方法の検討

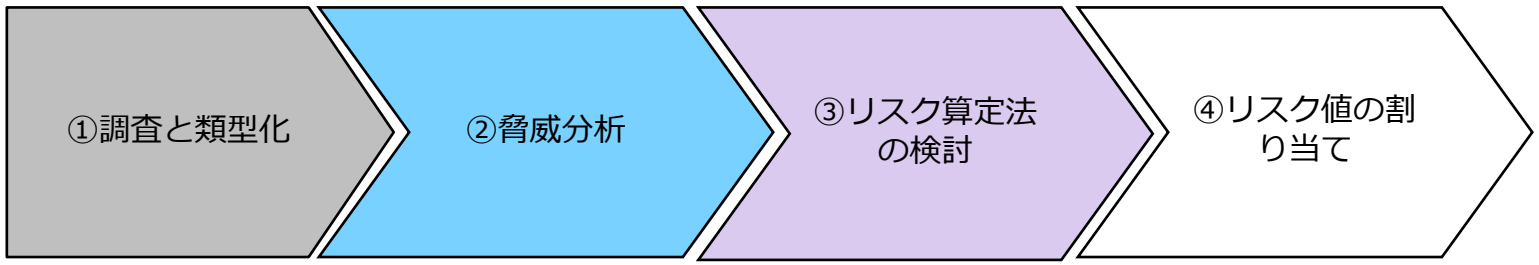
–類型化された車両システムと機能/サービスの脅威分析を実施

③ リスク算定法の検討

–リスク値算定のメトリクスの検討

④ リスク値を割り当て

–脅威分析結果より，導出された脅威にランク付けを実施

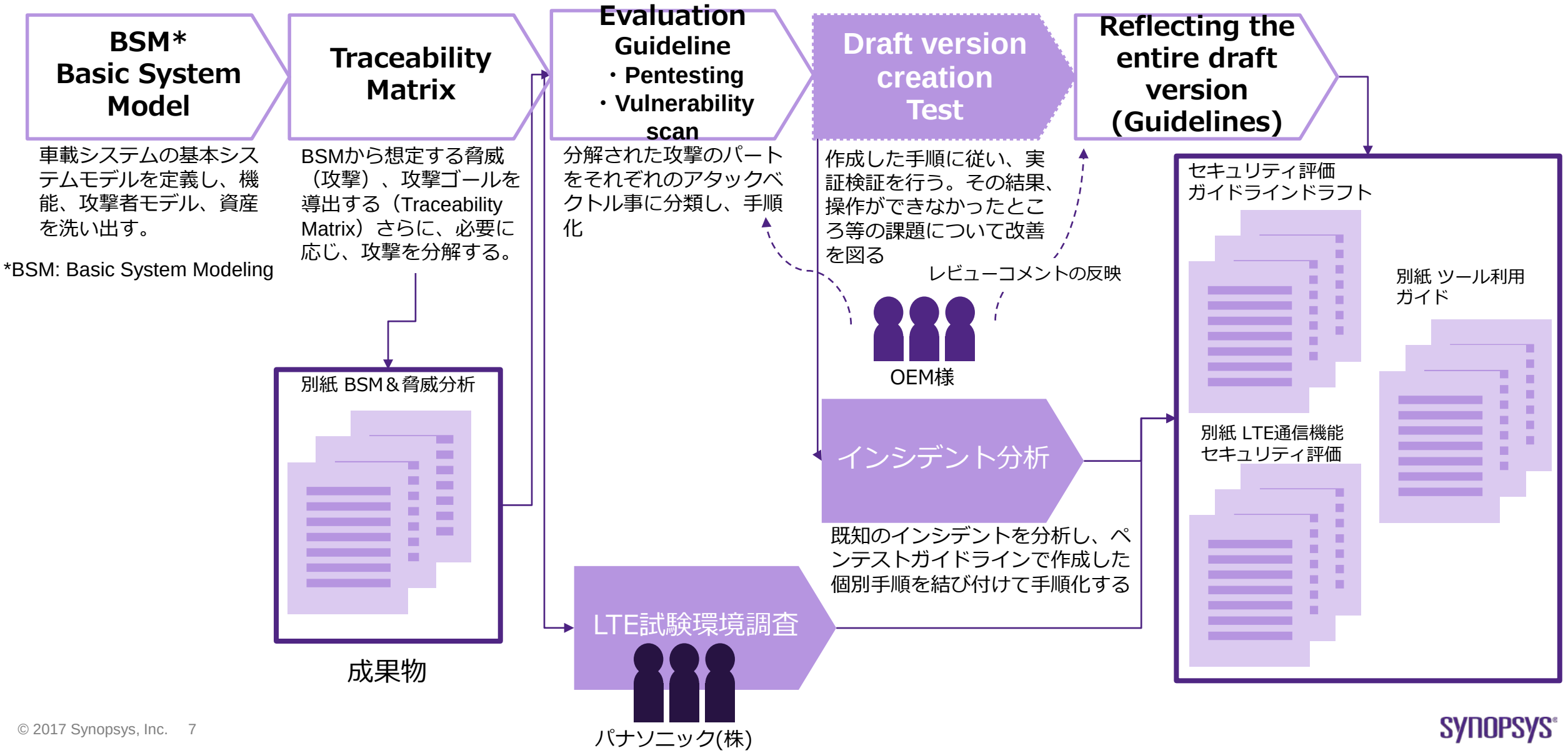


SYNOPSYS®

b.情報セキュリティ評価ガイドラインドラフトの作成

SYNOPSYS®

セキュリティ評価ガイドライン策定フローと成果物



SYNOPSYS®

BSM＆脅威分析の概要

①車両システムの脅威分析のために、自動走行車両のシステムコンポーネントを配置（下図）

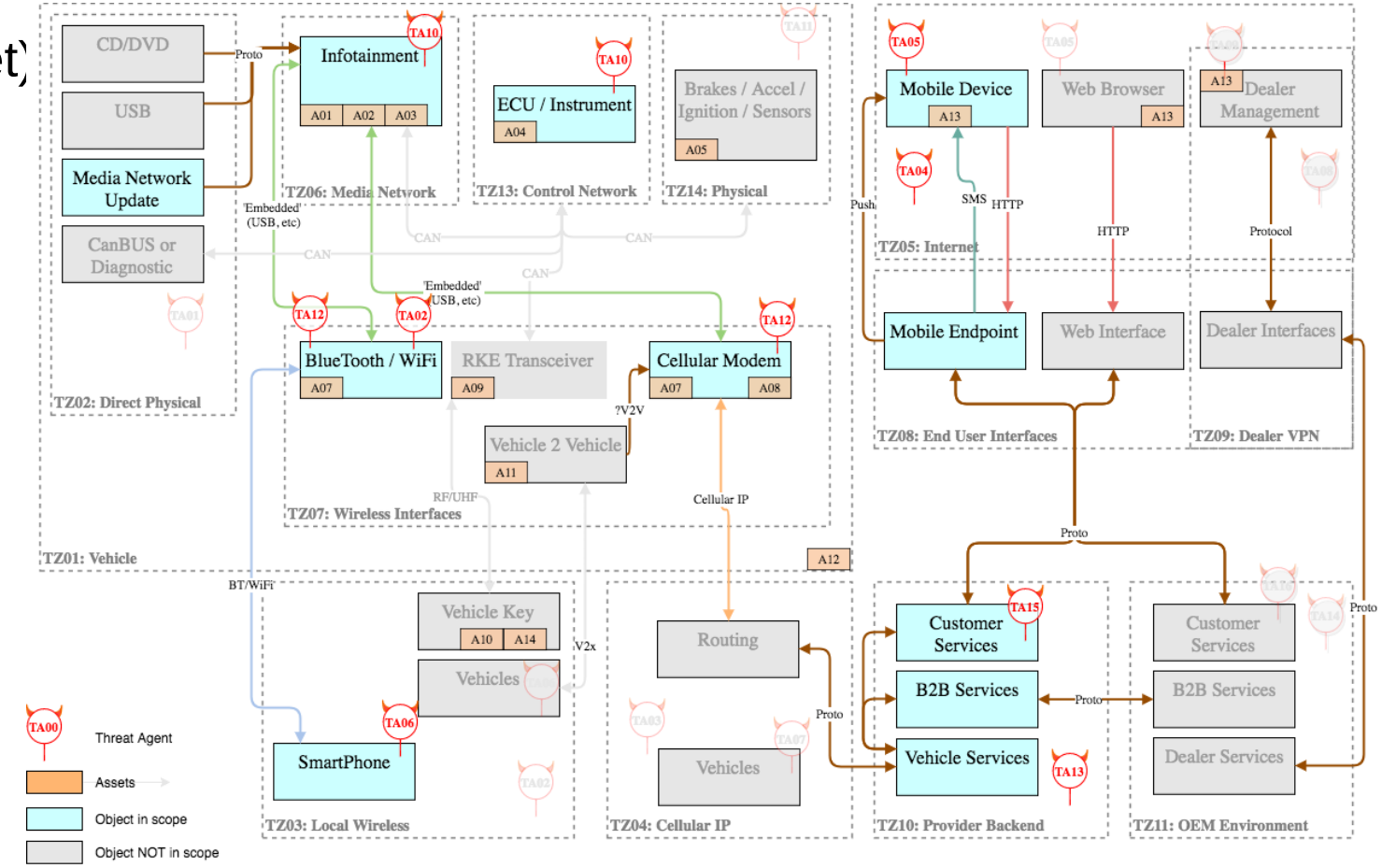
②車両システムの資産の洗い出し(Asset)

③脅威エージェント(TAxx)

④アタックサーフェス（攻撃口）

⑤トレーサビリティマトリクス

セキュリティテスト評価ガイドライン策定へ



SYNOPSYS®

c.情報セキュリティ評価の試行調査

SYNOPSYS®

セキュリティ評価ガイドラインの試行概要

BSM*
基本システム
モデル

Traceability
Matrix

評価ガイドライン
・ペンテスティング
・脆弱性スキャン

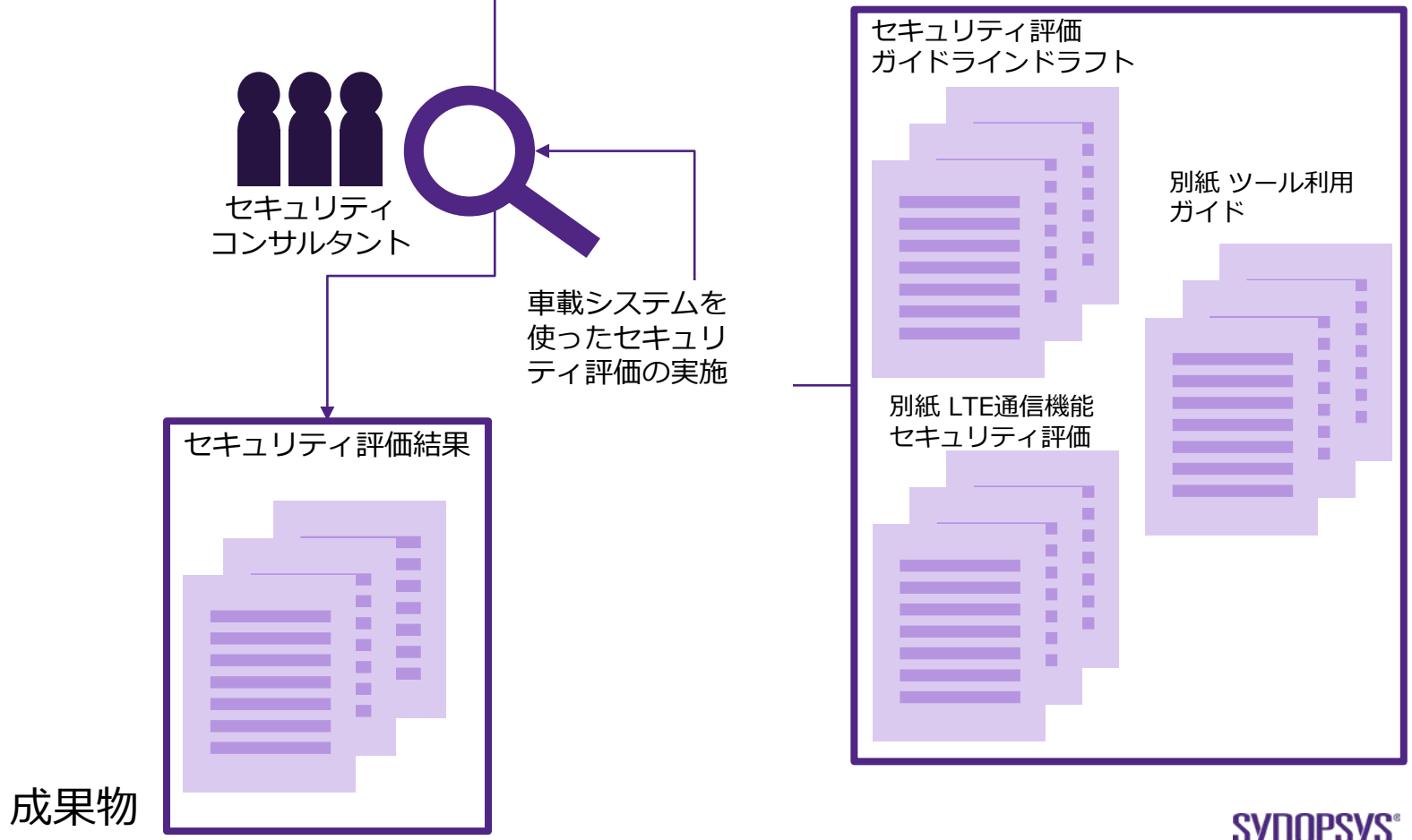
ドラフト版
実証検証

ドラフト版の全体
反映
(ガイドライン化)

・対象となったテストケースリスト

・ガイドライン策定の中で、テストケースの作業時間を見積。　テストに要した時間を記録。同様の試験を実施する際のテスト計画に活用可能

・



成果物

SYNOPSYS®

d.来期実証実験の運営準備

SYNOPSYS®

実証実験概要

自動走行システムの社会実装に向けて、攻撃者視点で車両レベルでのセキュリティ評価ガイドラインを策定しました（STEP1）。そして、実証実験として複数車両等を用いてSTEP1で作成したガイドラインを検証し、セキュリティ評価ガイドラインを確立します。（STEP２）

SYNOPSYS®

実証実験の進め方

A.実証実験への参加募集と選定	B.提供車両および業務契約等の締結	C.セキュリティ評価（約2か月間/車両を想定）	D.クロージング
・国内OEMを対象として、車両システムのセキュリティ評価実証実験参加者の募集を行います。 ・実証実験の実施概要を参照いただきます。 ・希望者は、参加要領にご記入いただき応募いただきます。	・提供車両に係る諸条件について2社間での合意形成を調整します。 ・提供車両の実装状況と準備等から業務契約書を作成します。 ①無線通信実装状況 ②車両準備状況 ③評価範囲の定義 ④体制と運営方法 ⑤スケジュール	次の順に作業を実施します。 ①開始時ミーティング ②環境構築 ③車両システム分析 ④評価開始 ⑤評価結果情報整理 ⑥レポート作成 ⑦報告会開催 ⑧評価終了	契約内容に基づきて、検収を行います。 また、2社間で、次の内容を確認します。 ・借用物の返却 ・取得情報の破棄 サインオフをして終了します。

SYNOPSYS®