Vtechの
サイバーセキュリティ
業務について
- ISO/SAE 21434 -

ISO/SAE 21434 対応の必要性

国連法規”UN-R155”への対応でISO/SAE 21434が必要

UN-R155
サイバーセキュリティ法規で、車両のサイバーセキュリティに関する国連規制。
自動車を販売するためにはUN-R155への対応が必要になる。
日本では、下記のように段階的な対応が必要である。

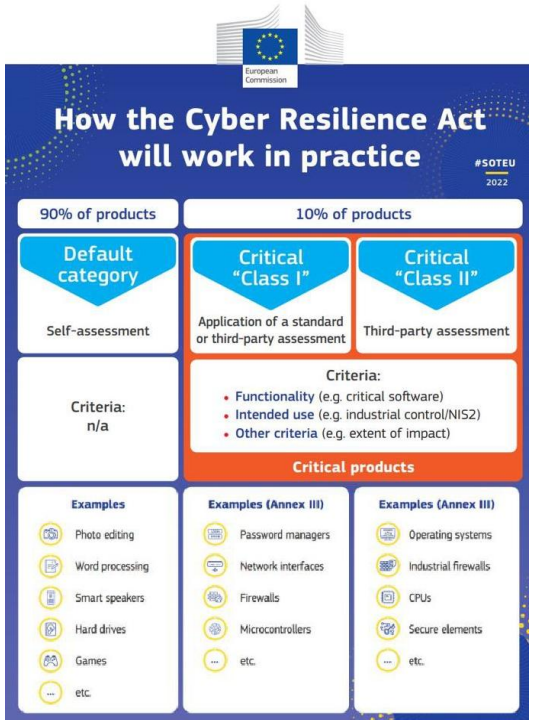
- 適用時期(予定)
  - 無線によるソフトウェアアップデートに対応している車両
    - 新型：令和4年7月1日
    - 継続：令和6年7月1日
  - 無線によるソフトウェアアップデートに対応していない車両
    - 新型：令和6年7月1日
    - 継続：令和8年7月1日

https://www.mlit.go.jp/common/001373651.pdf
国土交通省「4-3. サイバーセキュリティ及びプログラム等改変システムに係る基準（UN-R155 及び UN-R156）」

UN-R155に対応するためには、国際標準規格ISO/SAE 21434に対応しなければならない。

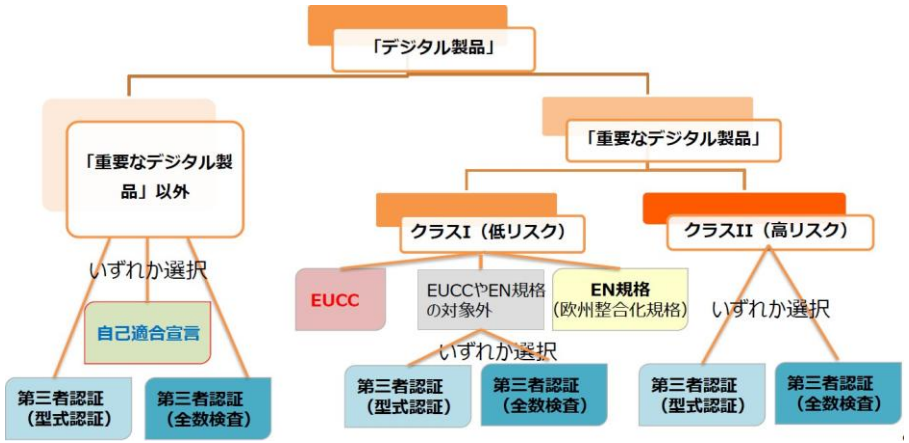
EUサイバーレジリエンス法への対応でISO/SAE 21434が必要(1/2)

サイバーレジリエンス法（CRA：Cyber Resilience Act）
「デジタルの要素を持つ製品」のサイバーセキュリティの欠陥からユーザー・消費者を守ることを目的 とし、サイバー攻撃への対応とデジタル製品への包括的なサイバーセキュリティの要件を規定している。違反した企業には巨額の罰金が科されることがある。対象は、**「 EU域内で販売されるインターネットに接続される全てのデジタル製品」である。**



適合性評価方法　（24条、附属書VI）

- **「重要なデジタル製品」以外**は、**自己適合宣言か第三者認証かを選択**可能。
- **「重要なデジタル製品」**は、**クラスII（高リスク）は第三者認証、クラスI（低リスク）かつ**EUCCやE欧州整合化規格に準拠していない場合は**第三者認証**の取得が必要。



デジタル製品をセキュリティに対する重要度などで３つのカテゴリに分類し、分類によって異なるレベルでのセキュリティへの対応が求められる。
デジタル製品販売業者は、製品がCRAの基準を満たしていることを保証するために、新たなチェックリストやプロセスを導入する必要がある。

https ://www.european-cyber-resilience-act.com/?_fsi=JJJe9Ok8

https://www.meti.go.jp/policy/netsecurity/netsecurity/CRAdraft.pdf

4

EUサイバーレジリエンス法への対応でISO/SAE 21434が必要(2/2)

他の指令・規制との関係

- 既に他のEU規則においてセキュリティ要件が課されている対象製品は適用除外となる。（第2条）
- 現在、法案策定中の「一般製品安全規則」及び「AI規則」についての関係性も整理されている。
- また、EU適合宣言（CEマーク）に関する記述も引用されている。

第2条：以下の規則の対象製品は適用除外
・「医療機器規則」　（EU 2017/745）
・「体外診断用医療機器規則」（EU 2017/746）
・「民間航空機規則」　（EU 2019/2144）
・「自動車の型式承認規則」（EU 2018/1139）
・他の規制によっても適用除外となる場合もある。

これらの規制を満たせば、EUサイバーレジリエンス法への対応不要となる。
→　自動車の場合は、UN-R155への対応が必須
→よってISO/SAE21434への対応が必須

第７条：「一般製品安全規則（法案策定中）」における製造者の義務などはこの規制ではカバーされていない安全上のリスクに関して、この規制の対象製品にも適用される。

第８条：「AI規則（法案策定中）」におけるサイバーセキュリティ要件について、この規則で遵守していることをもって、AI規則上の要件も満たしているものとする。

11
https://www.meti.go.jp/policy/netsecurity/netsecurity/CRAdraft.pdf

2024年3月12日 - 欧州議会はサイバーレジリエンス法を承認した。

5

国際標準規格
”ISO/SAE 21434”とは？

国際標準規格”ISO/SAE 21434”とは？

規格名称：Road vehicles-Cybersecurity engineering
自動車ーサイバーセキュリティエンジアリング
リリース：2021年8月31日

自動車技術の発展に伴い、電動車、自動運転などカーエレクトロニクス(電子化)の役割はますます重要になってきている。

そのため、セキュリティのリスクが上がり、**車両外部からのサイバー攻撃(ハッキング等)へのセキュリティ対策**が重要な課題である。

このような中、ISO とSAE がジョイントビジネスとして定めた自動車のライフサイクル全般にわたるサイバーセキュリティ対策を定めた国際規格が**ISO/SAE 21434**である。

ISO: International Organization for Standardization（国際標準化機構）の略称。国際的に通用する規格を制定す活動をしており、ISOが制定した規格がISO規格である。
SAE:SAE International（SAEインターナショナル）の略称。モビリティ専門家を会員とする米国の非営利団体。SAEが制定した規格がSAE規格である。

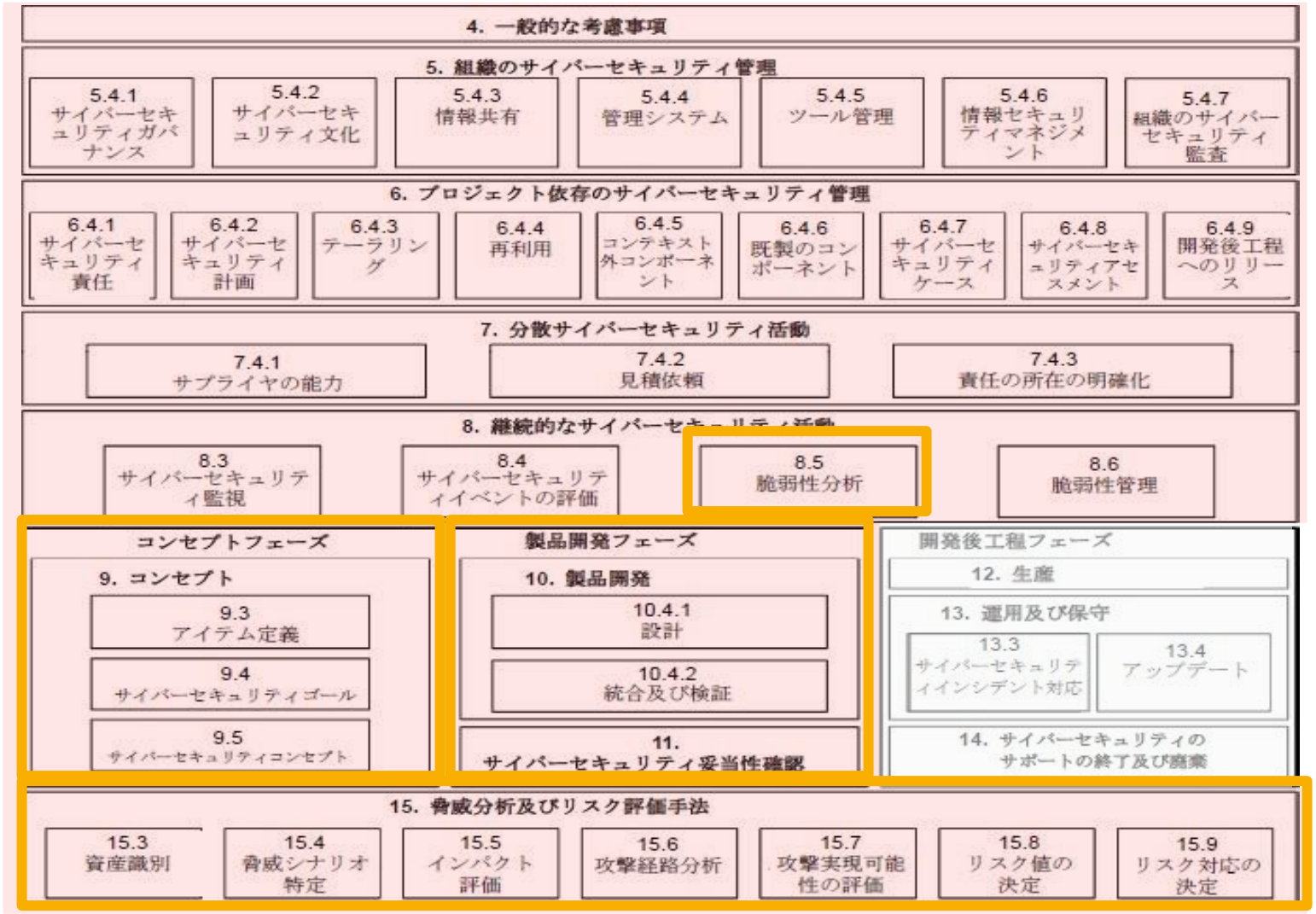
ISO/SAE 21434の特徴

- 車載システム開発（自動車メーカや電子システムのサプライヤなどの分散開発）に沿った**電気電子システムの開発プロセスに適用**できる。
- セキュリティの防御技術は日進月歩であること、また攻撃者にヒントを与えることから**具体的な方法論は記載していない。**
- 車載器以外の外部セキュリティに関しては、リスクを想定する際に考慮するが、**適用の範囲は車両内**である。
- 車載システムとその周辺のセキュリティリスクを考え、**具体的なプロセスに落とし込むためのエンジニアリングの規格**である。
- **国連WP 29のプロセス認証の法規部分**（UN-R155）に親和性のある規格である。

8

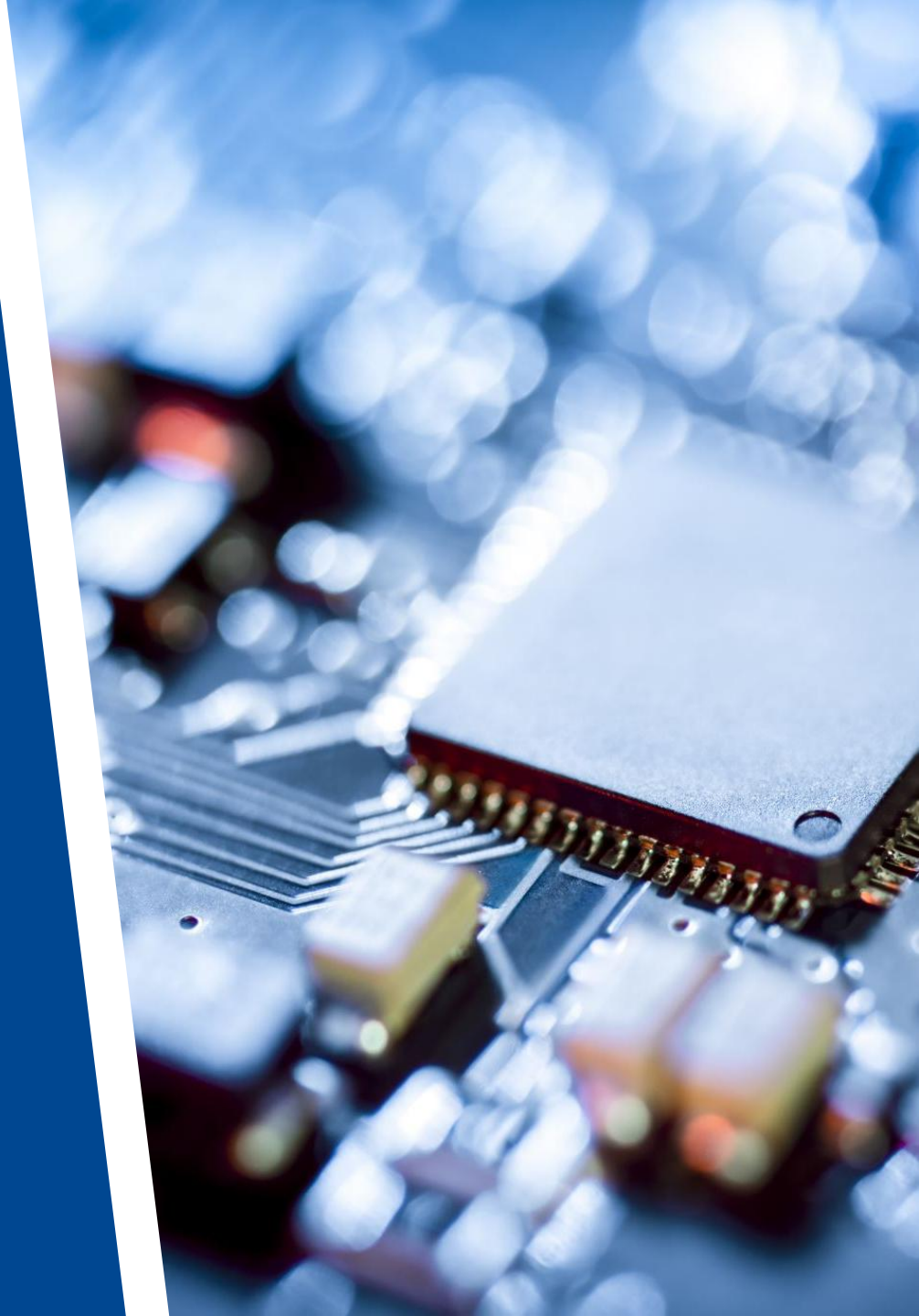
ISO/SAE 21434規格構成図

ISO/SAE 21434規格構成図及び当社が関わる主たるプロセス



9

Vtechのサービス



サービス一覧

- セキュリティの導入支援
  - ISO/SAE21434セミナ(基礎編、エンジニアリング編、管理者編)
- 脅威分析・リスクアセスメント(TARA)
- 脆弱性評価/脆弱性診断
- 脆弱性評価結果を用いた脆弱性対策のエンジニアリング支援
  - 対策方法の検討、対策機構の仕様策定、対策機構の実装仕様の提案等
- セキュリティ(+機能安全)に対応したプロセス構築支援
  - GAP分析、プロセス構築支援
- セキュリティ(+機能安全)開発支援、請負

セキュリティの導入支援

サイバーセキュリティ(ISO/SAE 21434)に対応するには、規格の内容を理解する事が重要です。Vtechは、サイバーセキュリティに対応したセミナを用意しており、導入の支援を行う事で、作業者の立ち上げ、スキルの底上げに貢献します。

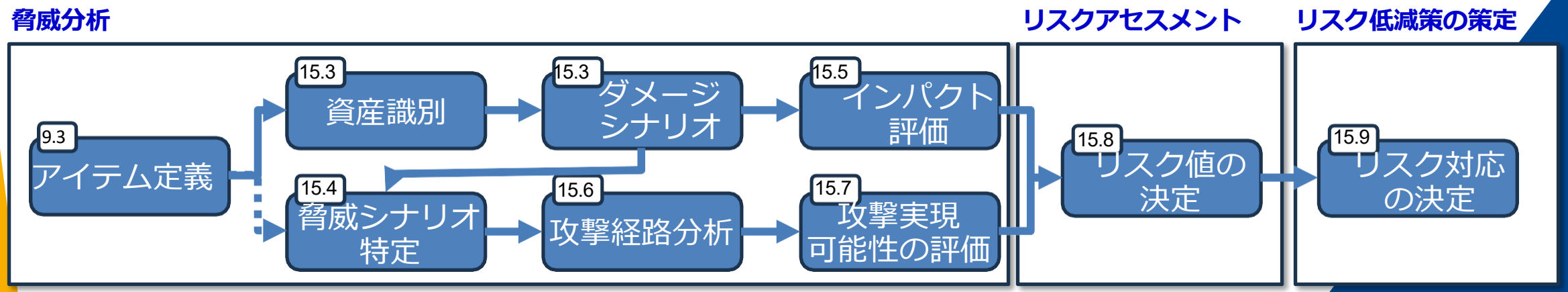
名称	概要	対象
基礎編	ISO/SAE 21434の基礎知識とISO/SAE 21434の実施フロー、必要な組織及びサイバーセキュリティ活動の実施概要の説明	サイバーセキュリティ業務に携わる全ての方
エンジニアリング編	ISO/SAE　21434におけるLSI開発に関わる実施フローと実施事項の説明、サイバーセキュリティ機構の要求仕様作成及び事例紹介	(上記、基礎編を受講された方で) • プロジェクトの業務・サイバーセキュリティ管理業務に携わる方とサイバーセキュリティ業務に携わるエンジニア • プロジェクト外においてサイバーセキュリティの品質管理に携わる方
サイバーセキュリティ管理編	ISO/SAE 21434におけるサイバーセキュリティ管理・確証方策の内容/実施事項とサイバーセキュリティ管理業務の説明	(上記2編を受講された方で) • プロジェクトの業務・サイバーセキュリティ管理業務に携わる方 • プロジェクト外においてサイバーセキュリティの品質管理に携わる方

脅威分析・リスクアセスメント(TARA)

対応すべき「サイバーセキュリティ目標」を決定するには、

- 脅威分析とリスクアセスメント（TARA)
- リスク低減策の決定

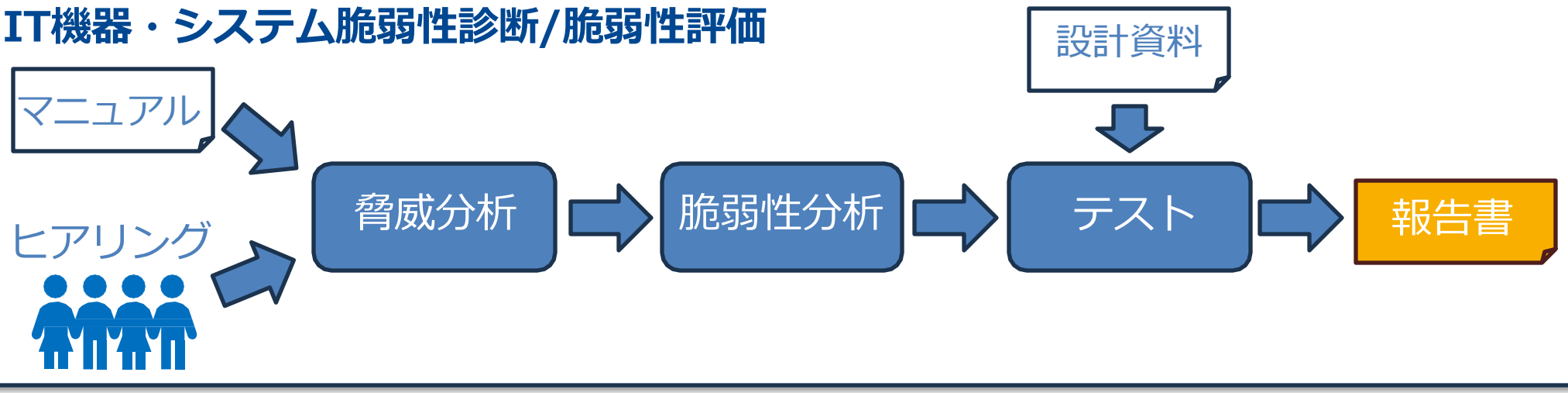
が必要です。これらのステップを各資産ごとに繰り返し、評価、対策を決定していくことが規格対応に必要です。
Vtechは、この一連のステップの作業の進め方、成果物の内容に対するサポート、アドバイスを行う事で、御社の作業者のスキルの底上げ、作業効率向上に貢献します。



脆弱性診断/脆弱性評価(1/2)

開発製品を、利用を想定する環境で脆弱性診断を実施し、その結果を使って脆弱性評価する。これにより、対策すべき機能やブロックの明確化に貢献する。
この脆弱性診断/脆弱性評価はISO/SAE 21434の認証を取るためにも必須な作業である

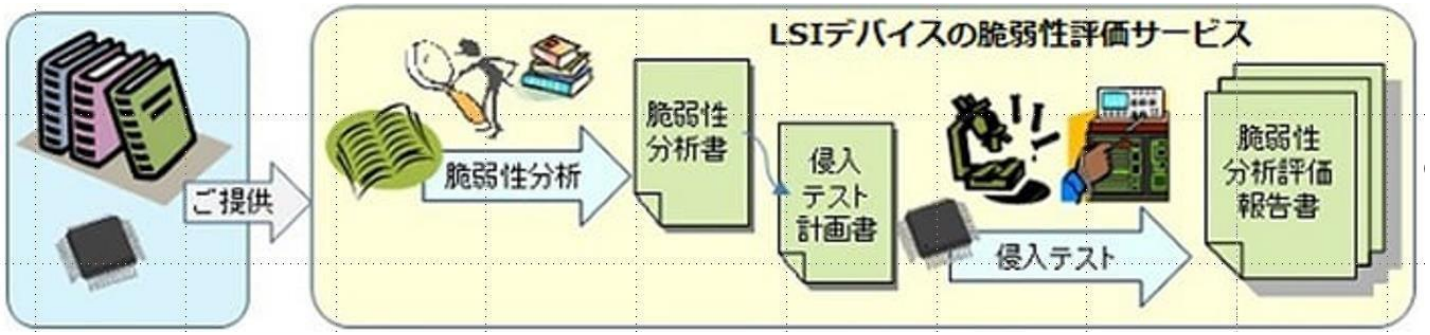
- **◆IT機器・システム脆弱性診断/脆弱性評価**

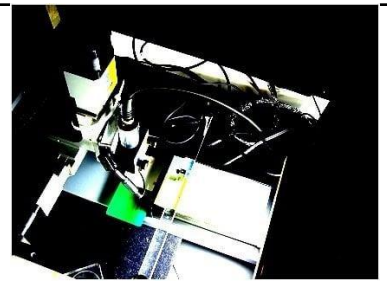
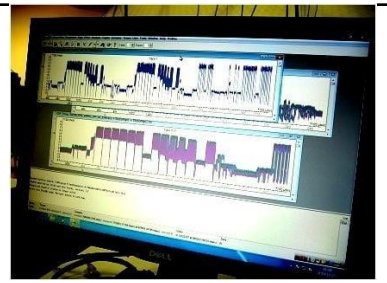


作業項目	概要
脅威分析	マニュアル、ヒアリング等で入手した情報を基に、製品に想定される脅威分析を実施。
脆弱性分析	脅威分析結果を用いて脆弱性分析を実施。
テスト	対象の機器・システムに対して、分析結果から作成したテストを実施し、問題の有無を検証。
報告書作成	分析結果より報告書を作成して、提供。

脆弱性診断/脆弱性評価(2/2)

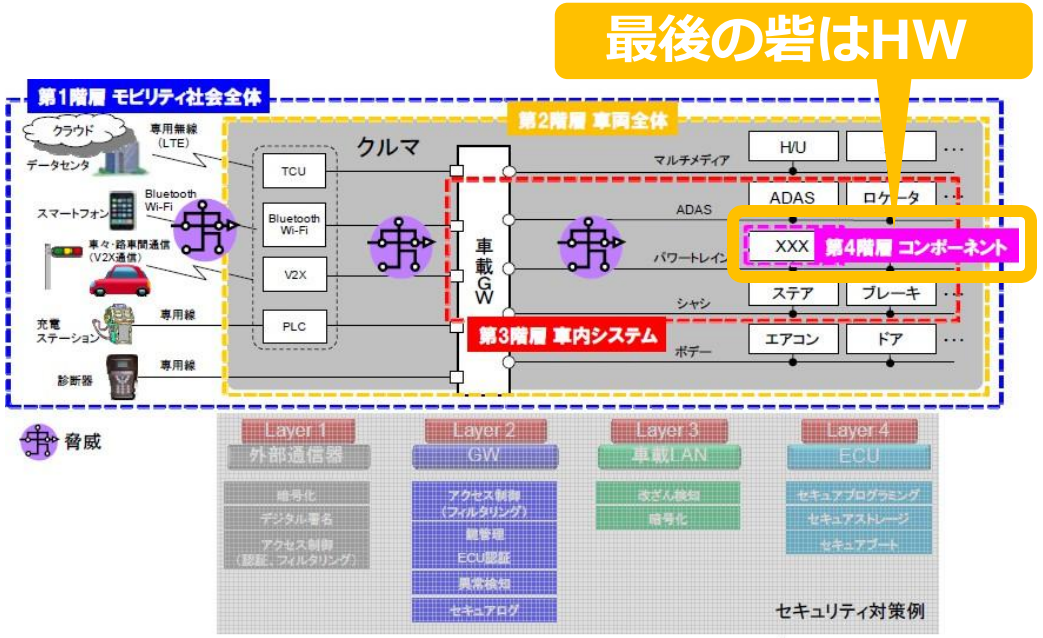
◆システムLSIを対象とした脆弱性診断/脆弱性評価



			
物理的な攻撃	**かく乱攻撃**	**サイドチャネル攻撃**	**ソフトウェア攻撃**
集積回路内部にプロービングして、メモリから機密データを読み出す。 集積回路内部の配線に変更を加えて、セキュリティ機能を無 効化することで信号を取り出す。	動作中のLSI上にレーザー光を照射、又は電源やクロックラインにパルスを印加することによりLSIの動作をかく乱させて、プログラムの流れや処理データを変更させる。	LSI動作時の消費電力や放射電磁波の波形を採取して採取波形の特徴を分析し、多数の波形の統計処理を行うことにより内部の秘密情報を抽出する。	未定義コマンドや想定外のパラメータをLSIに与えることで、想　定外のふるまいやレスポンスを行わせて内部情報を抽出する。

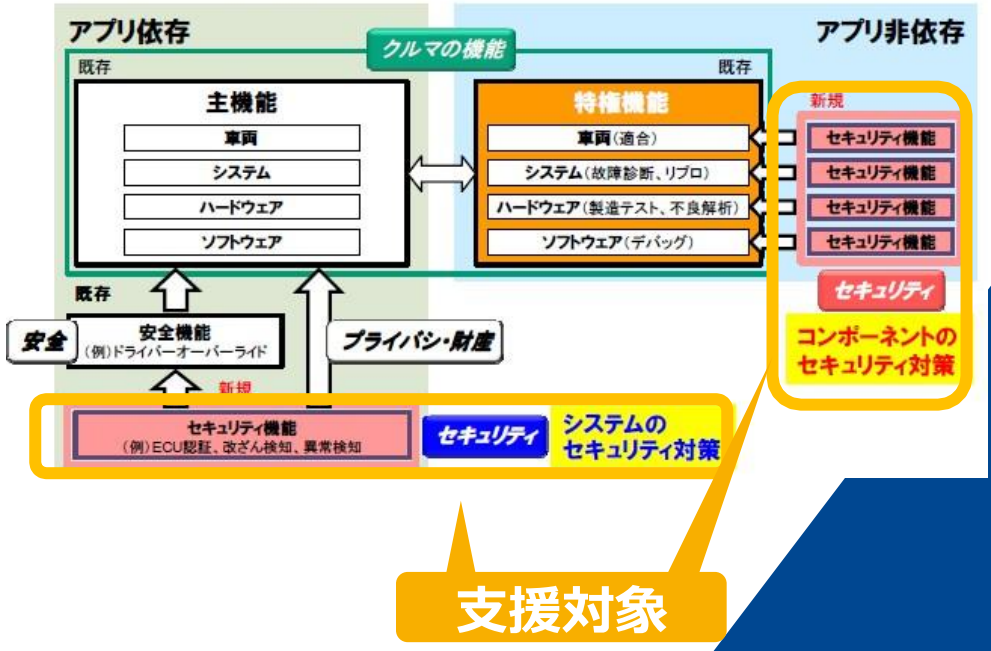
脆弱性評価結果を用いた脆弱性対策のエンジニアリング支援

脆弱性評価/脆弱性診断にて明らかになった脆弱性に対するセキュリティ対策のエンジニアリング支援を提供します。
対策方法の検討、対策機構の仕様策定、対策機構の実装仕様の提案等を行う事で、ISO/SAE 21434に沿ったセキュリティに強い製品開発に貢献します。



TCU: Telematics Communication Unit, PLC: Power Line Communication,
GW: Gateway, H/U: Head Unit,
ADAS: Advanced Driver Assistance Systems,

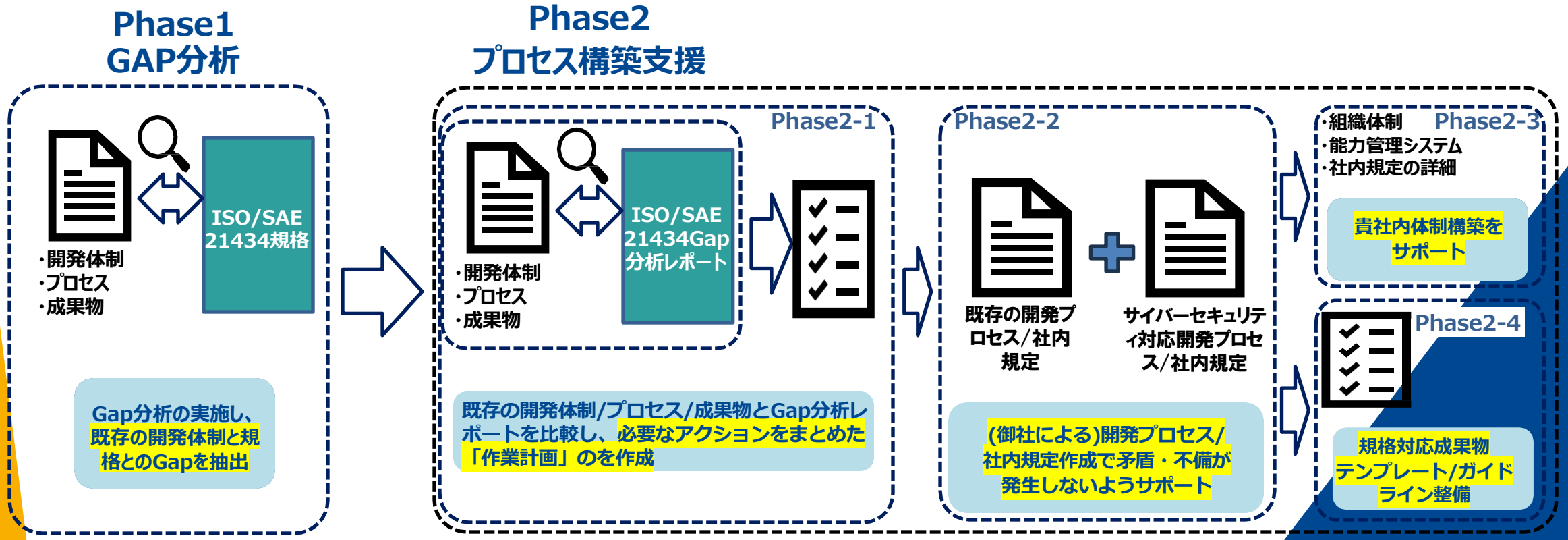
項目	定義	例	分類
主機能	自動車オーナが活用する機能	走曲止、高度運転支援	アプリ依存
特権機能	品質保証や機能確証に必要な機能	デバッグ、リプロ	アプリ非依存



https://testjp.sip-adus.jp/wp/wp-content/uploads/meti_2015_meti6-5_doc1.pdf

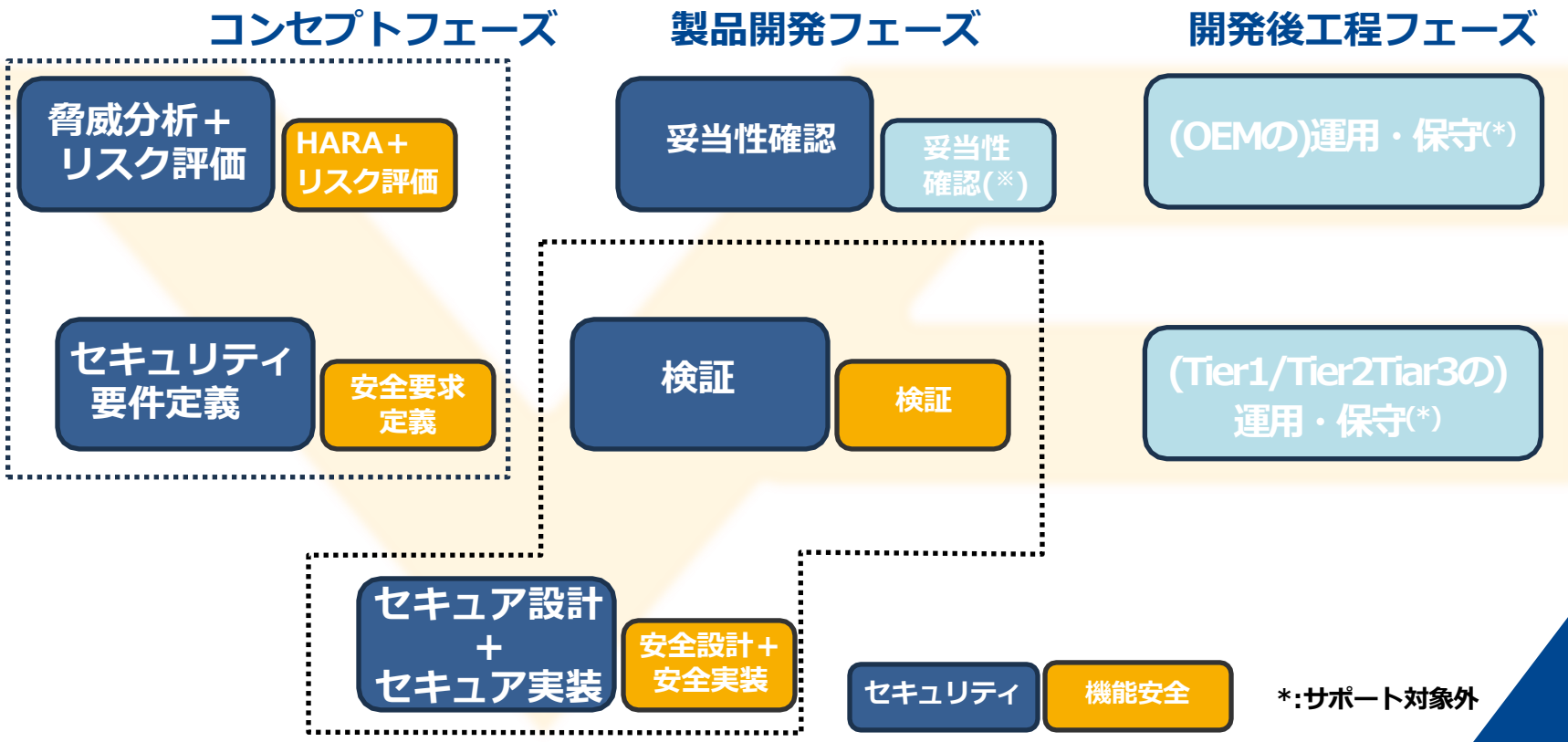
セキュリティ(+機能安全)に対応したプロセス構築支援

既存のQMS（品質マネジメントシステム）に対して、セキュリティ(ISO/SAE 21434)に対応した開発プロセスを構築するための支援を行います。
また、これまでVtechが蓄積してきた機能安全 (ISO26262) の知見も活かし、セキュリティとセーフティが両立できる開発プロセスを構築するための支援も行います。



セキュリティ(+機能安全)開発支援、請負

構築したセキュリティ(ISO/SAE 21434)や機能安全(ISO26262)に対応した御社の規程に従った製品開発がスムーズに行えるように、上流設計(セキュリティ機構仕様の策定)から、HWの設計/検証及びSWのコーディング/検証を支援します。また実作業の請負も行います。これらによって、お客様の開発の加速に貢献いたします。



Thank you!