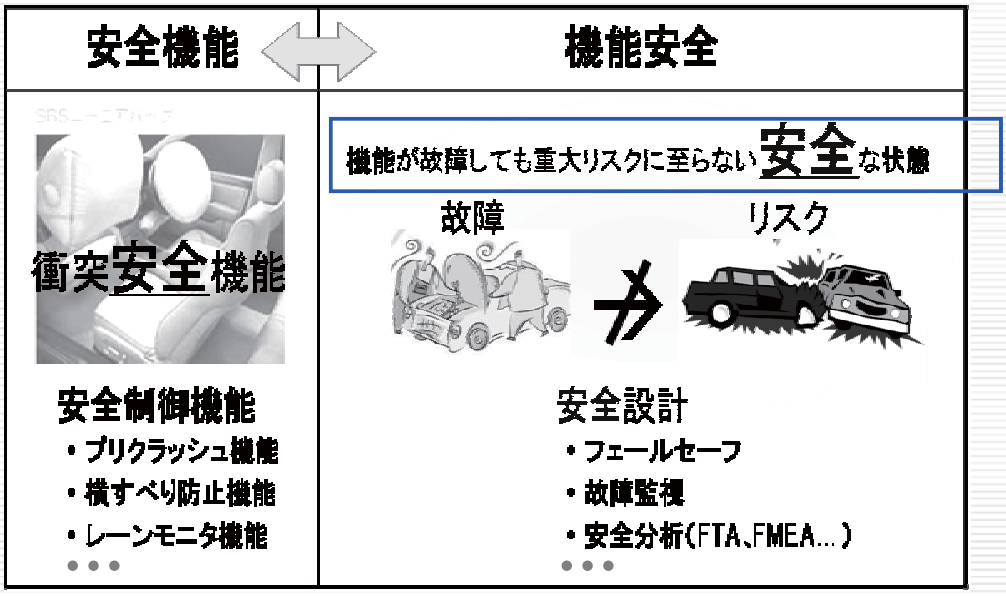
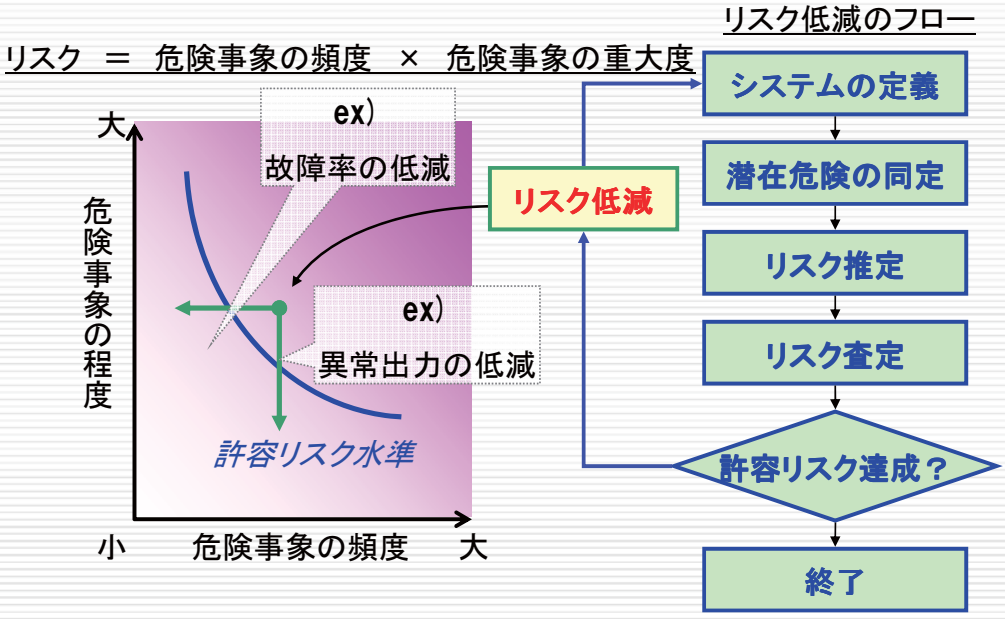
機能安全の意味



故障や異常によるシステムの機能不全を防ぐ/低減する

機能安全の考え方



「リスクベースのアプローチ」が基本の考え方

ISO 26262規格概要

- **名称**
  - Road vehicles — Functional safety —
- **制定**
  - 2011年 11月15日
- **適用**
  - **制定日以降の新規開発車両～**

自動車業界特有の難しさ
■多様性の考慮が必要（場所・人）
■制約が少ない（一般向け・非管理下）
他…

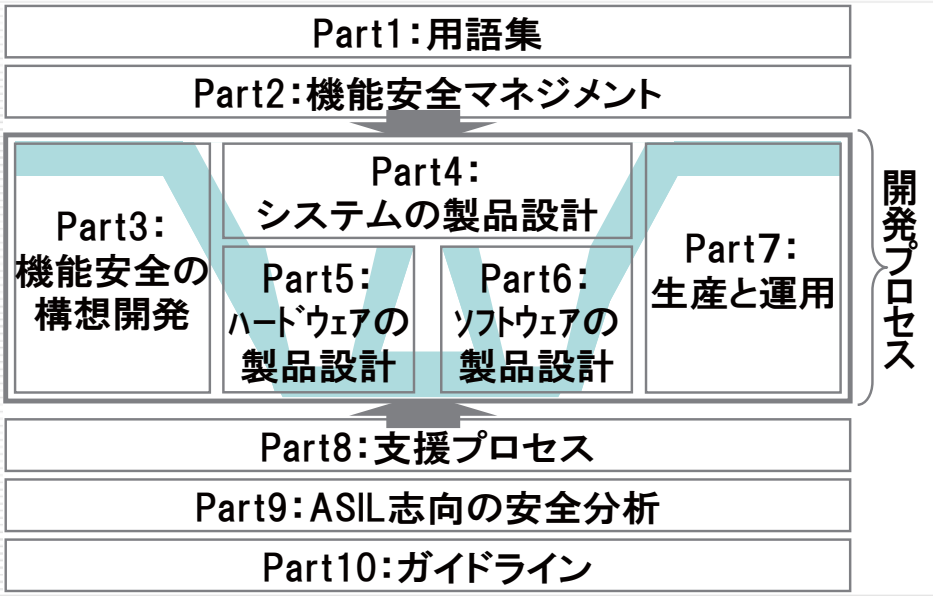
一般消費者向けの量産製品として初めての適用

ISO 26262（規格主旨）

- **自動車分野の安全ライフサイクルの定義と、各フェーズのテーラリングを許容**
- **自動車固有のリスク等級（ASIL）の設定と、リスクベースの手法を提供**
- **残存リスクの許容水準への抑制と、ASILに沿った安全要求の導出**
- **許容水準の抑制の達成を図るための、確認レベルと確認者の独立性に対する規格要件を提供**
- **OEMとサプライヤとの関係に対する規格要件を提供**

考え方～詳細技法の細部までの幅広い観点から規格要件を提供

ISO 26262（Part構成）



V字プロセスモデルと関連するマネジメント･プロセス･技法で構成

ISO 26262（適用範囲）

・対象車両

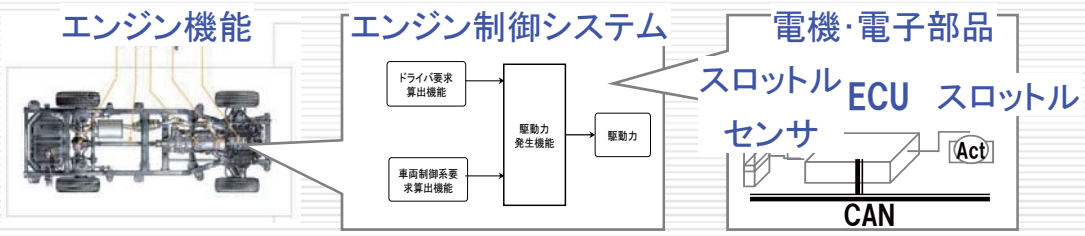
最大総重量 3.5t 以下の乗用車 （通常は、二輪車、大型車、特殊車両は含まない）

・対象システム

「システムの機能失陥 ⇒ 危険な状態」 の可能性がある機能、システム

・対象部品

電機･電子系部品 （通常は、センサやモータのメカ構造部は含まない）



機能失陥が「危険な状態」へ至る可能性があるシステム

機能安全の全社共通基盤

規格と認証の両面から、共通基盤を整備

サイバーセキュリティとは

■ 定義（ISO/IEC 27002）

情報の機密性・完全性・可用性を維持すること

- **機密性**（Confidentiality）
  - 情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること
- **完全性**（Integrity）
  - 情報が破壊、改ざん又は消去されていない状態を確保すること
- **可用性**（Availability）
  - 情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること

＜具体例＞車両盗難

物理的に車に侵入
またはレッカー移動

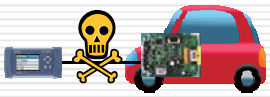
・物理セキュリティ対策
– 侵入検知センサ（振動、傾きなど）
・情報セキュリティ対策
– イモビライザ、GPS追跡

・機密性

通信データを傍受して、
他人になりすます
→ **高速料金のごまかし**

・完全性

ECUリプログラミング



不正なプログラムを
ECUに書き込む
→ 制御異常（最悪事故）

・可用性

Shift-By-Wire

車載LANの通信妨害に
より、シフト制御できず
→ 制御異常（最悪事故）

サイバーセキュリティを取り巻く環境の変化

- 新たなサービスの進展
  - 車外と**ツナガル製品**（例：スマホ連携、V2X、V2G）や**自動運転**に向けた動きが非常に活発な状況

V2X：Vehicle-to-Vehicle and Infrastructure、V2G：Vehicle-to-Grid

出典：ARPEGGiO
http://www.globaldenso.com/en/newsreleases/111208-01.html

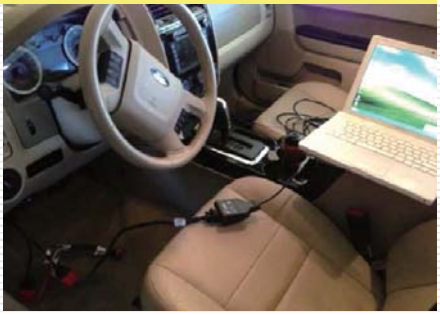
出典：トヨタ 自動運転技術@2013.10.11

- 負の側面（**車の脆弱性の暴露**）

米ハッキング学会：車両制御の乗っ取りデモ

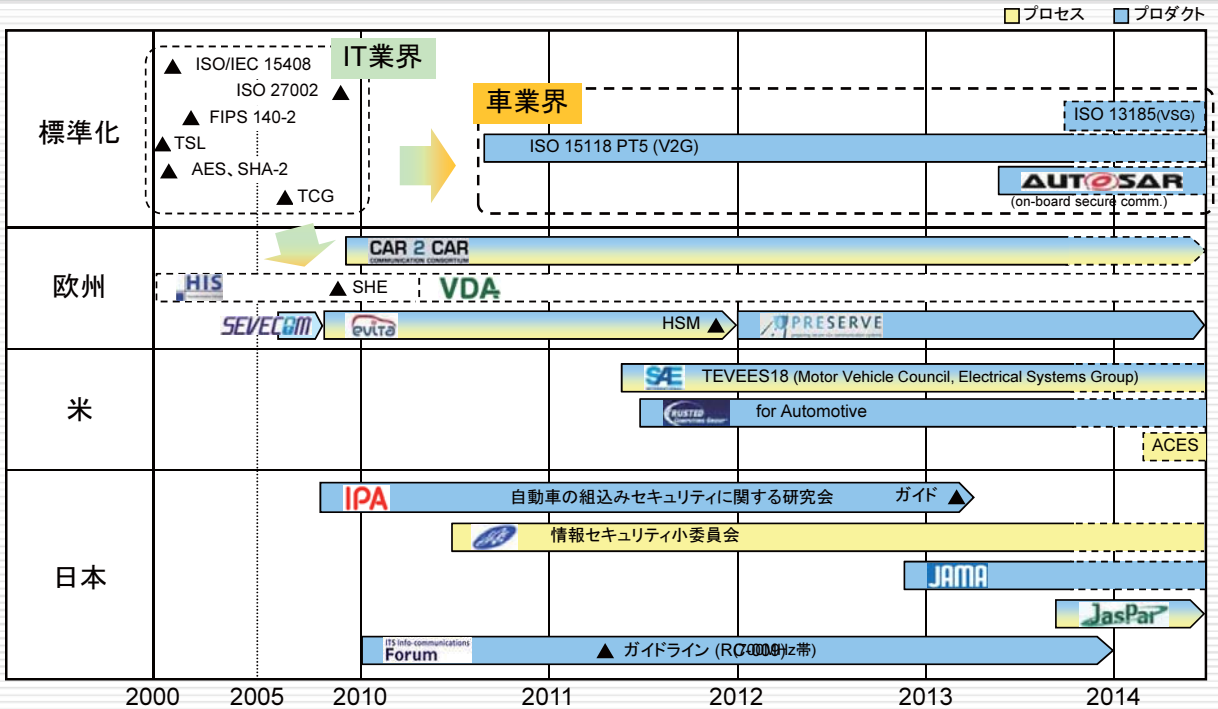
対象箇所	デモ内容
メータ	走行中にスピードメータが100mphなどを示す
ブレーキ	**走行中に勝手に急制動**
ステアリング	**走行中に勝手に蛇行**
エンジン	**走行中に急加速**。エンジンも切れない。
ホーン	走行中に勝手にホーンが鳴る
シートベルト	走行中に運転席のシートベルトが巻き上がる
ガスゲージ	いきなりフルゲージに変更

出典： DEF CON 21@2013.8
Adventures in Automotive Networks and Control Units



サイバーセキュリティの重要性が高まってきた

標準化動向

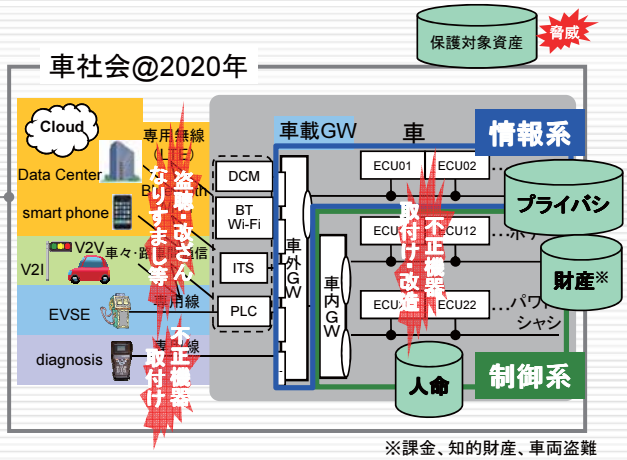


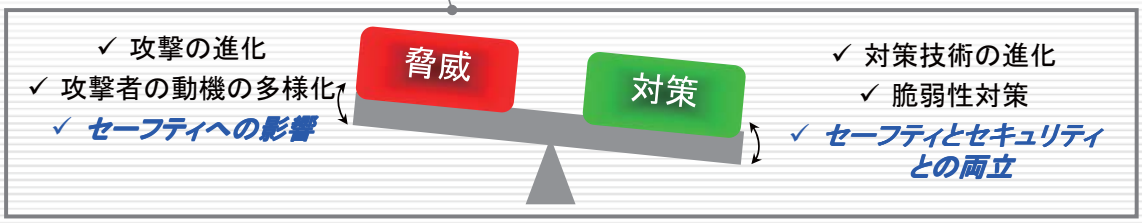
IT業界の知見をベースに、各国で標準化活動中

車におけるセキュリティの課題

車の難しさ

- 保護対象資産が多岐に渡る（人命、プライバシ、財産）
- イタチごっこの世界
- 脅威と対策との適正なバランス（セーフティも含む）

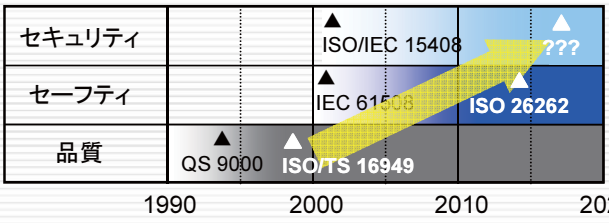


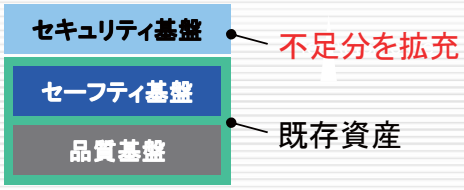


業界レベルでの相場作りが必要である

セキュリティ対応の考え方

- これまでの活動

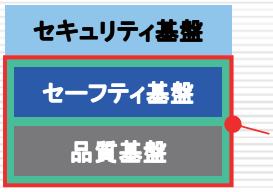




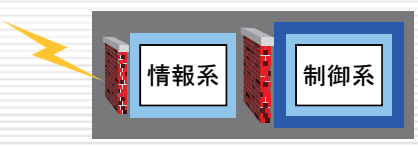
品質をベースにセーフティを拡充してきた → セキュリティも同様

- 考え方

①既存資産の脆弱性対策



②アーキテクチャレベルから検討



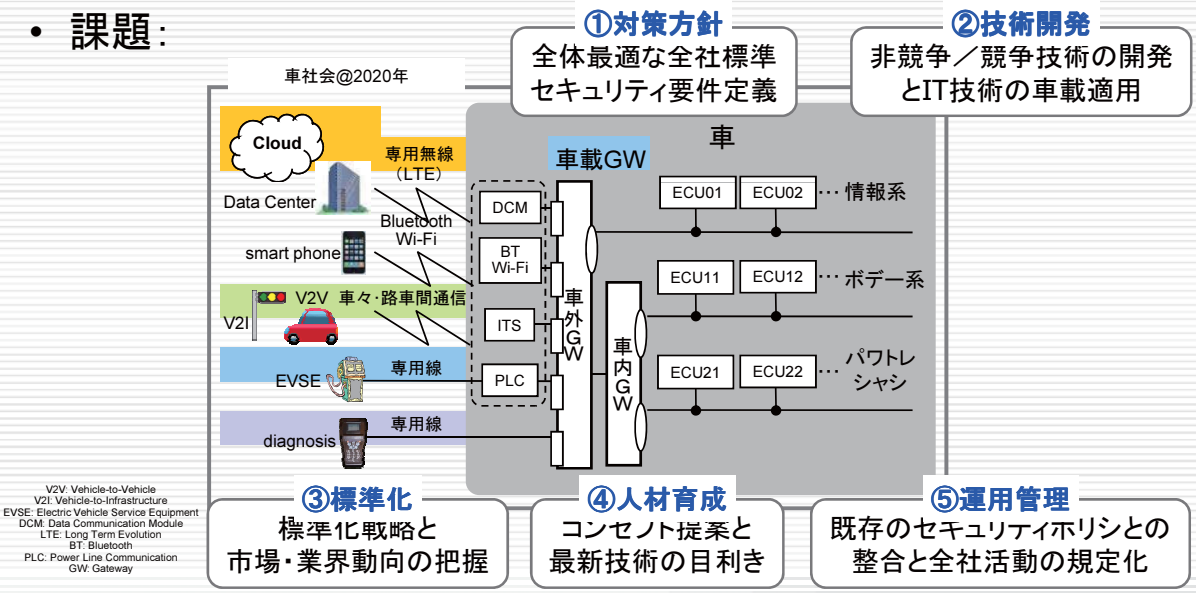
IT技術を流用 セーフティも考慮した対策

※リスクベースのstate of the art

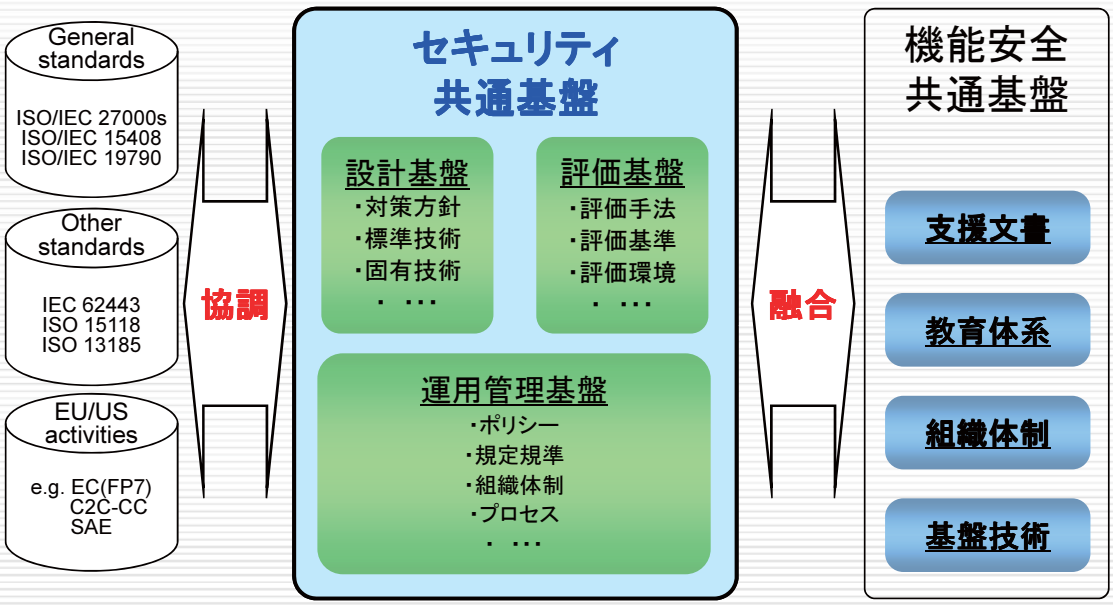
セキュアな既存資産に対して、アーキテクチャから適切な対策※をする

セキュリティ対応の活動概要

- 目標：車のサイバーセキュリティの全社仕組みを確立
- 活動方針：車社会@2020年における“セキュリティ要件・技術・管理”を速く策定し、実製品でブラシアップする
- 課題：



セーフティとセキュリティの共通基盤



グローバル標準と協調し、機能安全とセキュリティの共通基盤を融合する

本日の講演内容

1. 車載電子システムの動向と課題

2. 機能安全と情報セキュリティ

3. モデルベース開発

モデルベース開発とは？

モデルベース開発 (MBD: Model Based Development)

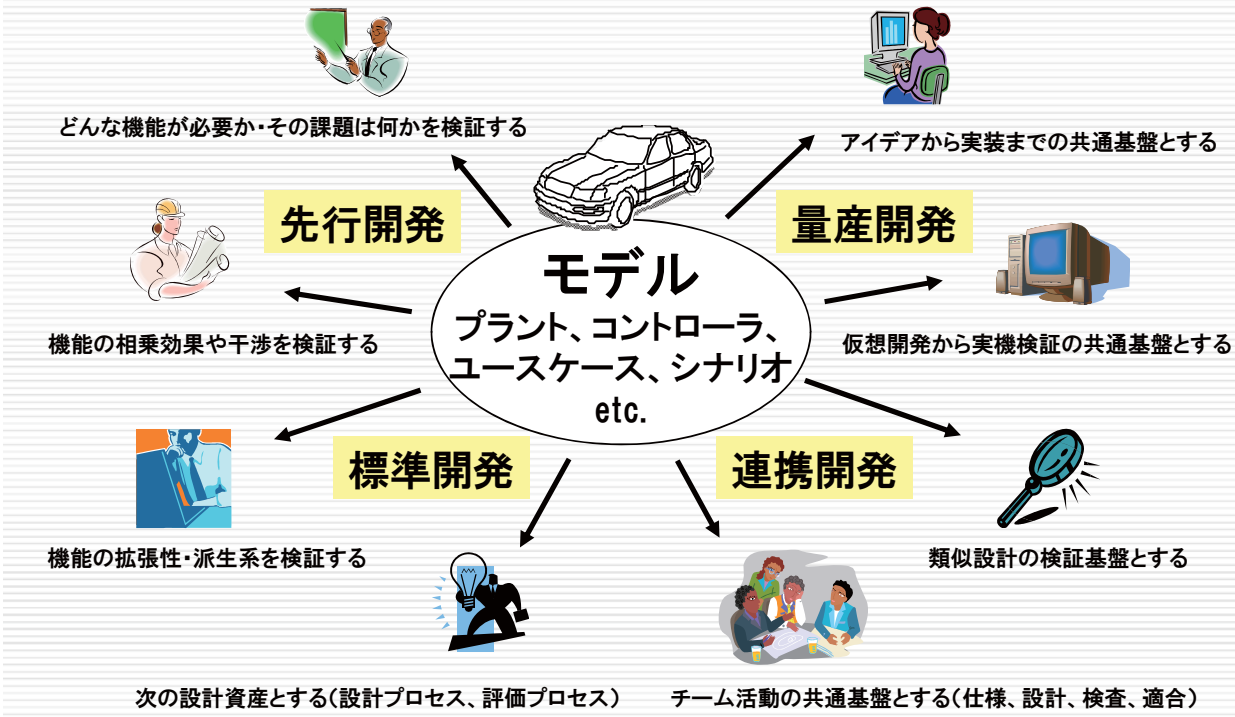
従来のソフトウェア開発のようなソースコードによる開発とは異なり、**開発の初期段階で実現すべき機能を設計図・モデルで作成**し、開発の**上流工程から下流工程**において、これを検証しながら開発プロセスを進めていく開発手法のこと。

実際にソースコードを書きはじめる前に、目的の機能をシミュレートできるため、仕様や機能の不具合を初期段階で発見でき、**開発効率の向上やコスト削減**にも効果があるとされている。

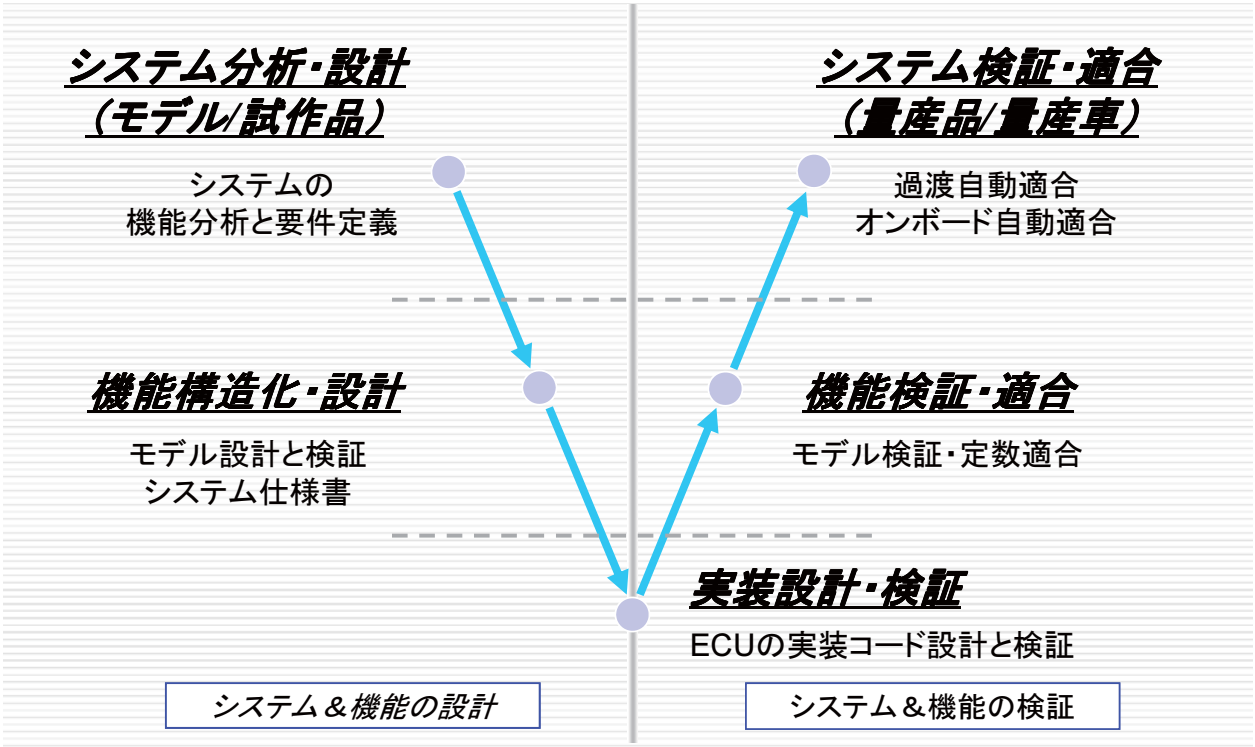
また、ソフトウェアで実装したい機能を抽象度の高いモデルとして可視化することで、ソフトウェア資産の再利用性を高めることができる。さらに、大規模なソフトウェア開発の場合、そのソースコードを一から読んで仕様を理解するよりも、モデルから仕様を把握する方がはるかに容易であるため、複数の開発メンバーでの開発にも適している。

@IT MONOist　組み込み用語辞典より引用

共通基盤として必要となるモデル



車両電子制御システムの開発プロセス(一般的)



車載電子システムのモデルベース開発

電子システムの構成

制御対象

クルマ

実物(Real)

制御装置

ECU

実物(Real)

“制御対象” と “制御装置” から成る

車載電子システムのモデルベース開発

電子システムの構成 → モデル化

制御対象モデル

機能(振る舞い)を図示

走る、
曲がる、
止まる、
空調する、
守る、
などなど

アクチュエータ
モデル

センサ
モデル

モデル(Virtual)

制御装置モデル

機能(処理)を図示

出力回路
モデル

入力回路
モデル

制御
ロジック
(～させる)

モデル(Virtual)

“制御対象” と “制御装置” の機能を仮想定義したものがモデル

車載電子システムのモデルベース開発

電子システムの構成 → 大規模・複雑化

制御対象

クルマの構成要素

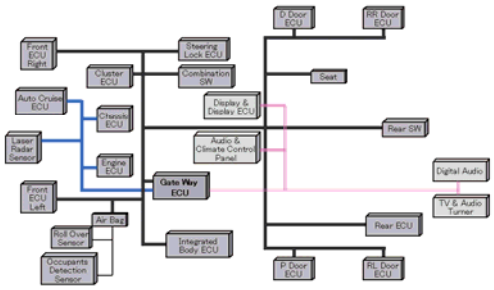




実物(Real)

制御装置

ネットワーク接続されたECU



実物(Real)

“全部そろってから”の評価・検証では、開発期間が増大

車載電子システムのモデルベース開発

電子システムの構成 → 大規模・複雑化

制御対象モデル

クルマの構成要素

モデル(Virtual)

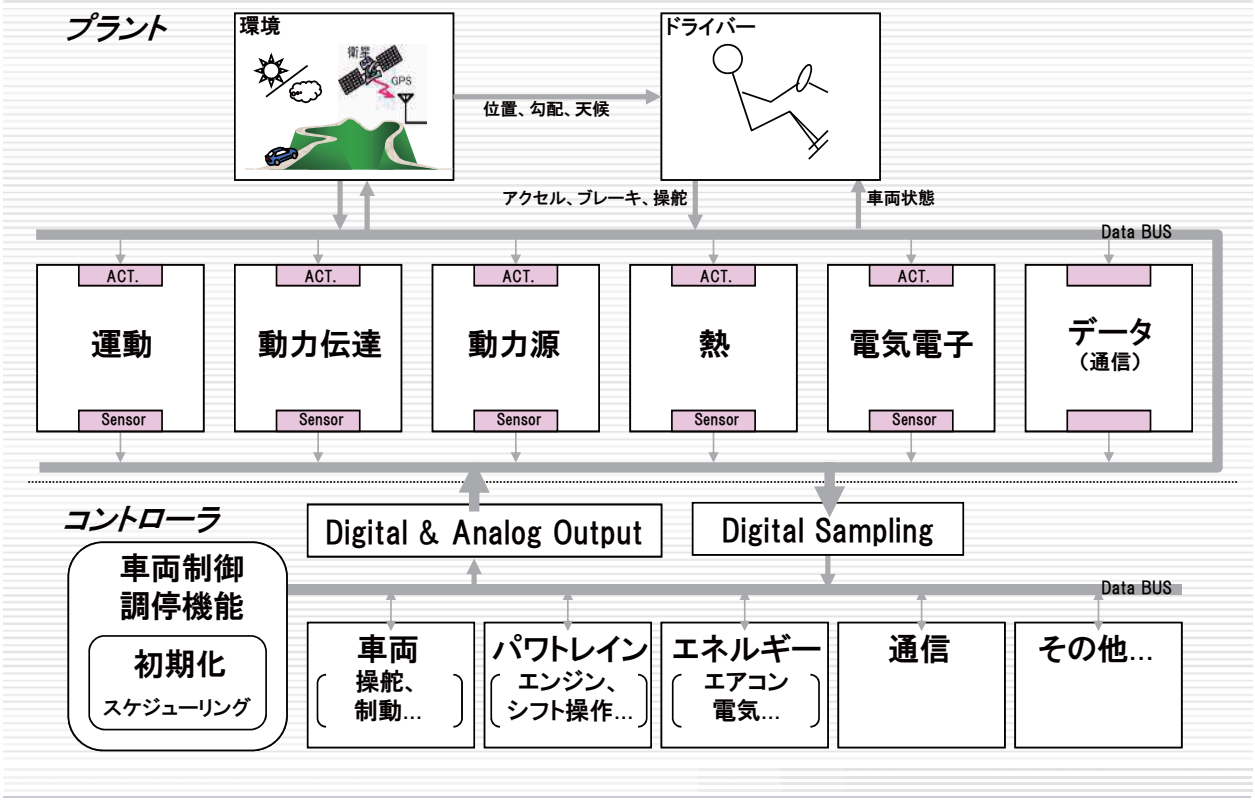
制御装置モデル

ネットワーク接続されたECU

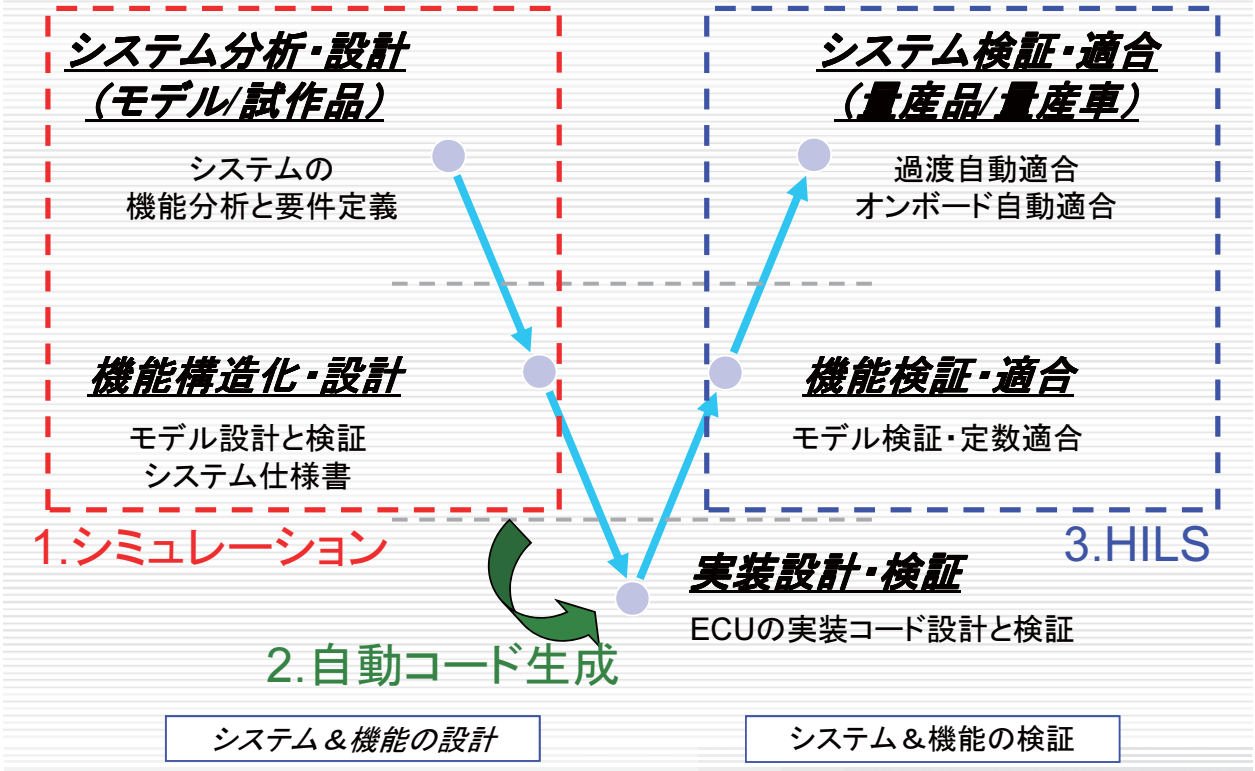
モデル(Virtual)

個々の製品レベルから車両全体まで、様々な粒度のモデルを活用

共通基盤としてのモデル ： 車両システム構造の一例

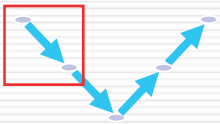


ツールを用いた、モデルベース開発の効率化



シミュレーション

目的：仮想環境におけるシステム設計およびテスト



制御対象モデル

機能（振る舞い）を図示

走る、
曲がる、
止まる、
空調する、
守る、
などなど

アクチュエータ
モデル

センサ
モデル

モデル(Virtual)

制御装置モデル

機能（処理）を図示

出力回路
モデル

入力回路
モデル

制御
ロジック
（～させる）

モデル(Virtual)

モデルを用い様々な状況のテストを実施し、システム構成を最適化

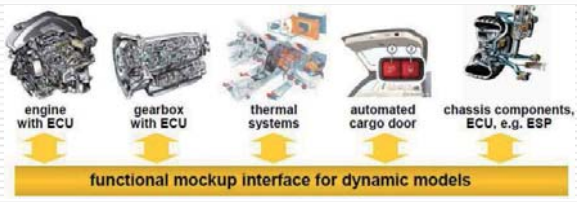
シミュレーション環境の標準化動向

欧州ではソフトが異なるモデルを接続／計算させるための標準化が進行

団体名：Modelisar
創設：2008年
メンバー：欧州の主要な車両メーカと
シミュレーションソフト会社

FMI（Functional Mockup Interface）

各社が開発したモデルを簡単につなげて
シミュレーションさせるためのインタフェース



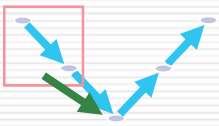
対応可能なシミュレーションソフト

- AMESim（LMS）
- Dymola（DASSAULT SYSTEMS）
- SimulationX（ITI）
- SIMPACK（ SIMPACK ）

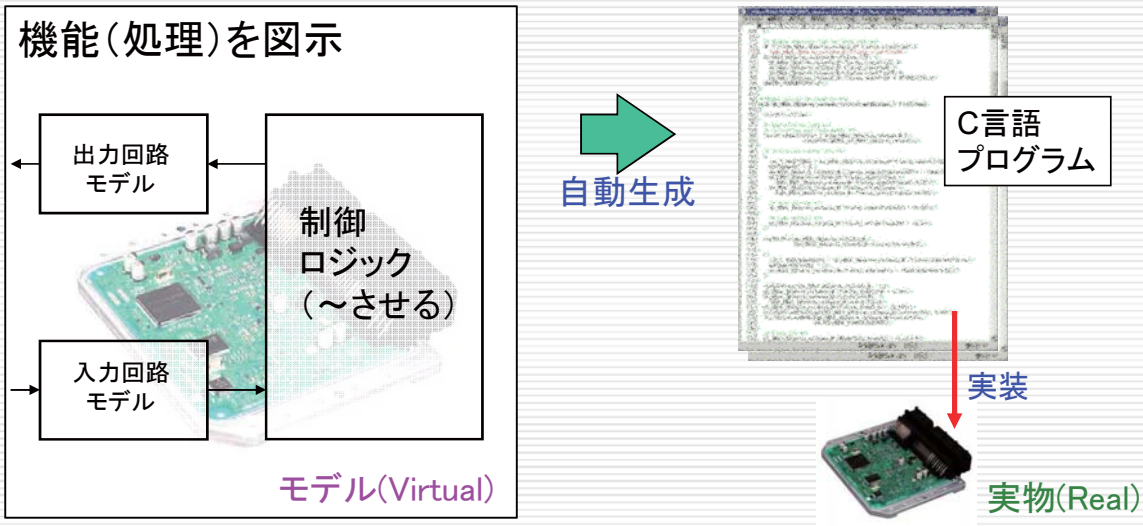
2010年に機能限定のFMI Ver1.0の規約が発行され、Ver2.0が策定中

自動コード生成(Auto Code Generation)

目的:制御装置モデルからECUのソフトウェア自動生成



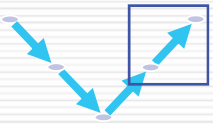
制御装置モデル



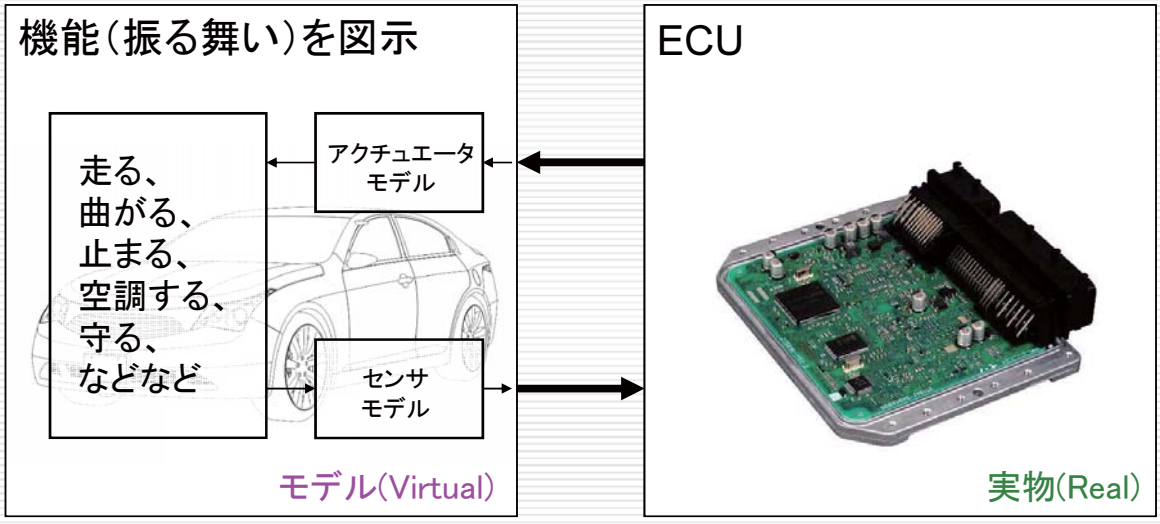
制御モデルからプログラムコードを実ECUに組込み

HILS (Hardware In the Loop Simulation)

目的:仮想環境におけるシステム設計およびテスト



制御対象モデル　　制御装置



モデルを用い様々な状況のテストを実施し、システム構成を最適化

まとめ

ニーズの進化に伴い、車載電子システムの大規模・複雑化はいっそう進む。限られた開発期間の中で、効率的に機能や品質を作りこむことが必要で、そのためには共通基盤に基づく開発が有効。

機能安全と情報セキュリティ

ISO26262対応と、サイバーセキュリティ攻撃の対応は、車載電子システム開発に対する2大インパクト

モデルベース開発

「システムをどうとらえるか」をモデルとして定義、それを拠り所として開発をする手法（シミュレーション、自動コード生成、HILS）