CASE時代のコネクティッドカーのサイバーセキュリティの動向と対策

株式会社ユビキタスAIコーポレーション 取締役
一社）組込みシステム技術協会　理事　副会長
一社）セキュアIoTプラットフォーム協議会 理事

佐野　勝大

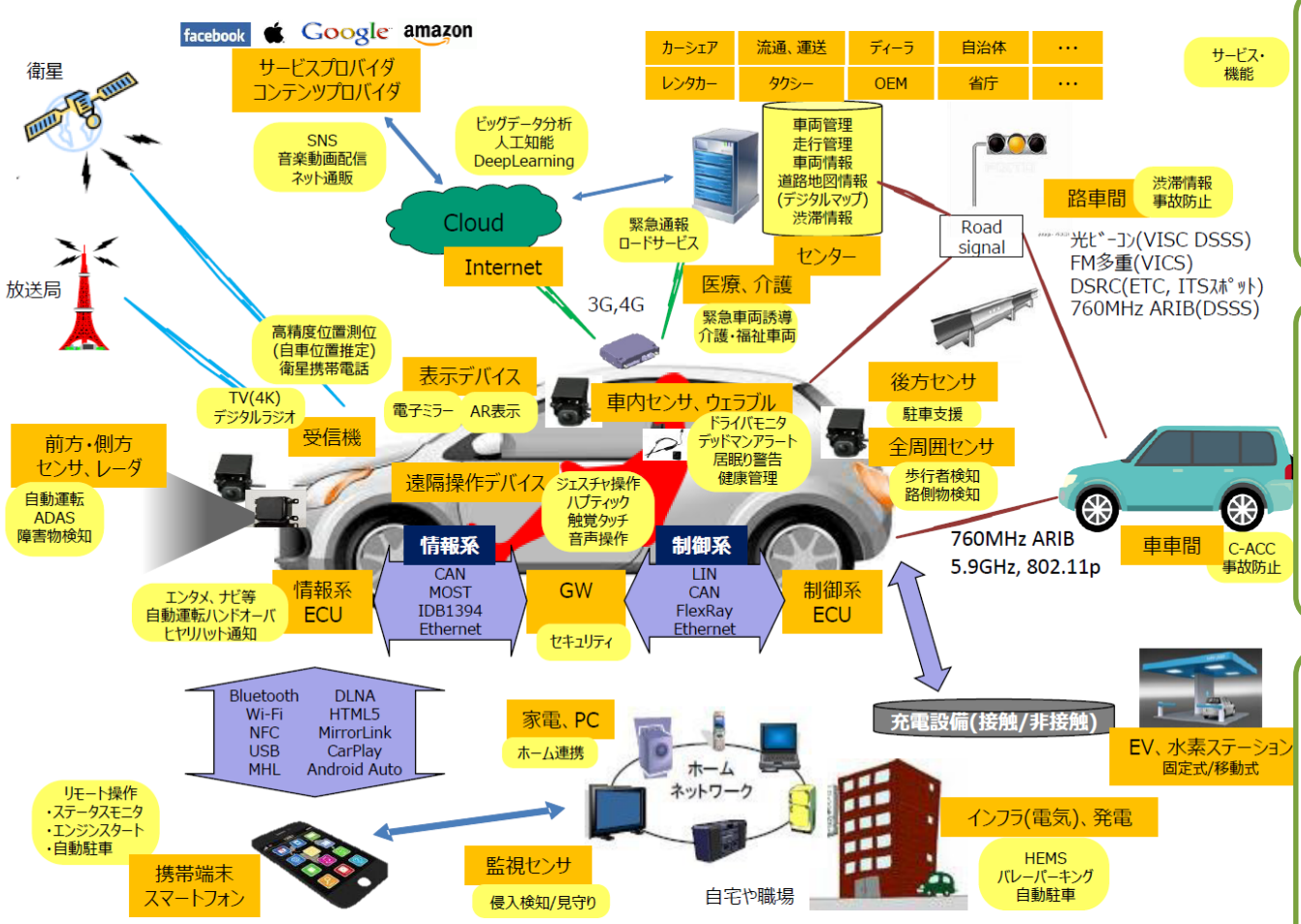
Ubiquitous AI Corporation

本日のアジェンダ

- 会社概要
- 自動車産業でのセキュリティの対応状況
- 複雑化、膨大化する開発工程において自動運転時代の安全を守るソフトウェア品質確保について
- CASE時代のセキュリティ対策について
- まとめ

コネクティッドカーを取り巻くテクノロジー

■ 多様な通信手段によるアクセス – セキュリティの重要性



*JasPar 2017/2/27 活動報告資料より抜粋

サービスとしての自動車への進化

- カーシェアリング・エコドライブなどの新しい利用形態
- 車載ソフトウェアの増加、高度化等の仕組みの変化
- 車載センサーや外部情報を利用したサービスの増加

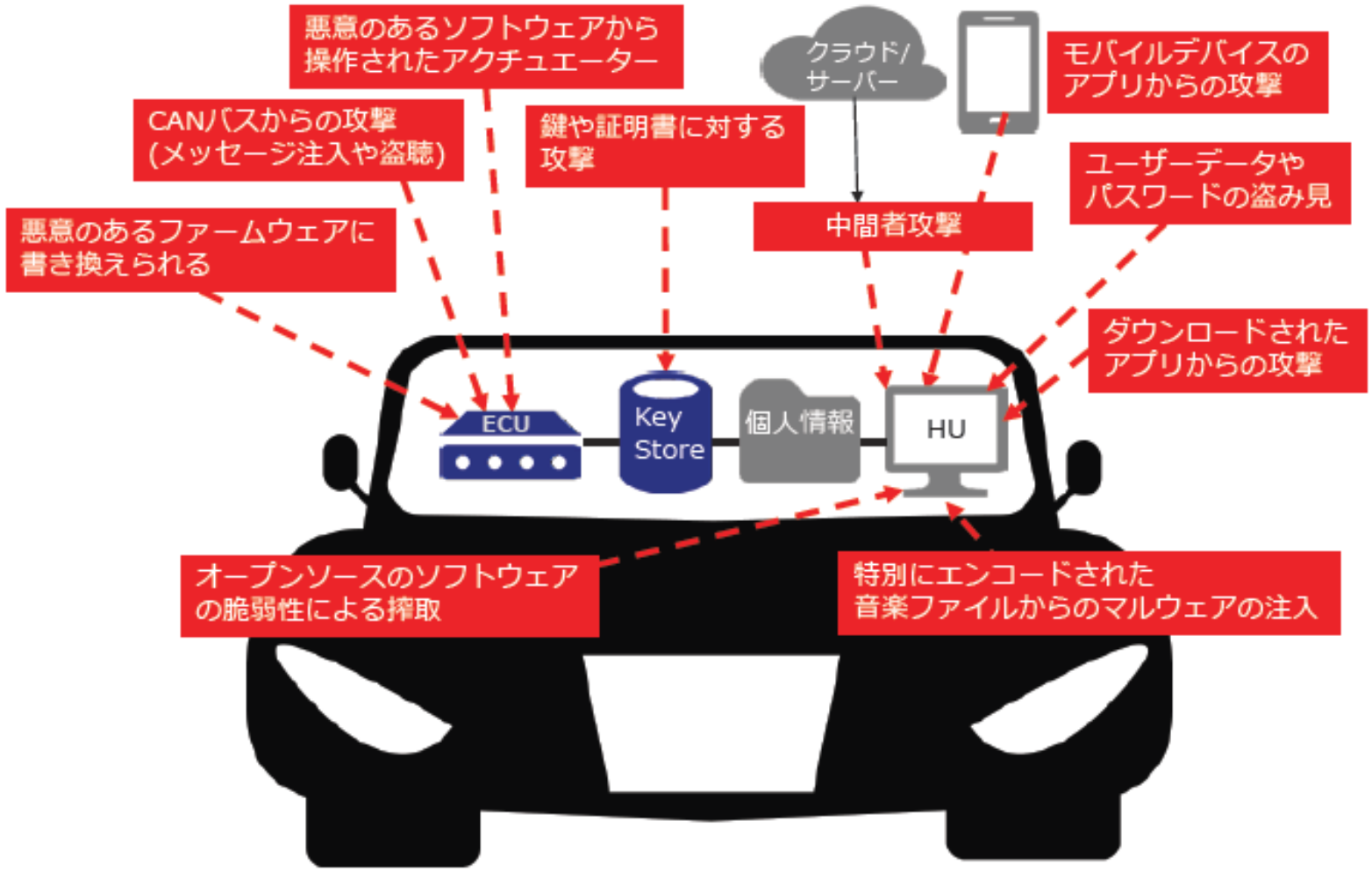
ネットワークへの接続

- 自動車とスマートフォン、サービスとの連携
- V2X(車車間、路車間、人車間）の新しいネットワーク技術とITSネットワークの進化
- 常時接続化するコネクティッドカーと自動運転車への進化（ダイナミックマップ、AI、BigData活用）

汎用プロトコル等の利用

- 車内ネットワークへのEHTERNET, Bluetooth などの活用とTCP/IPなど汎用プロトコルの適用
- 車載システムに対する汎用OSの利用
- 多種多様なセンサーデータのネットワーク転送

自動車のセキュリティの攻撃経路

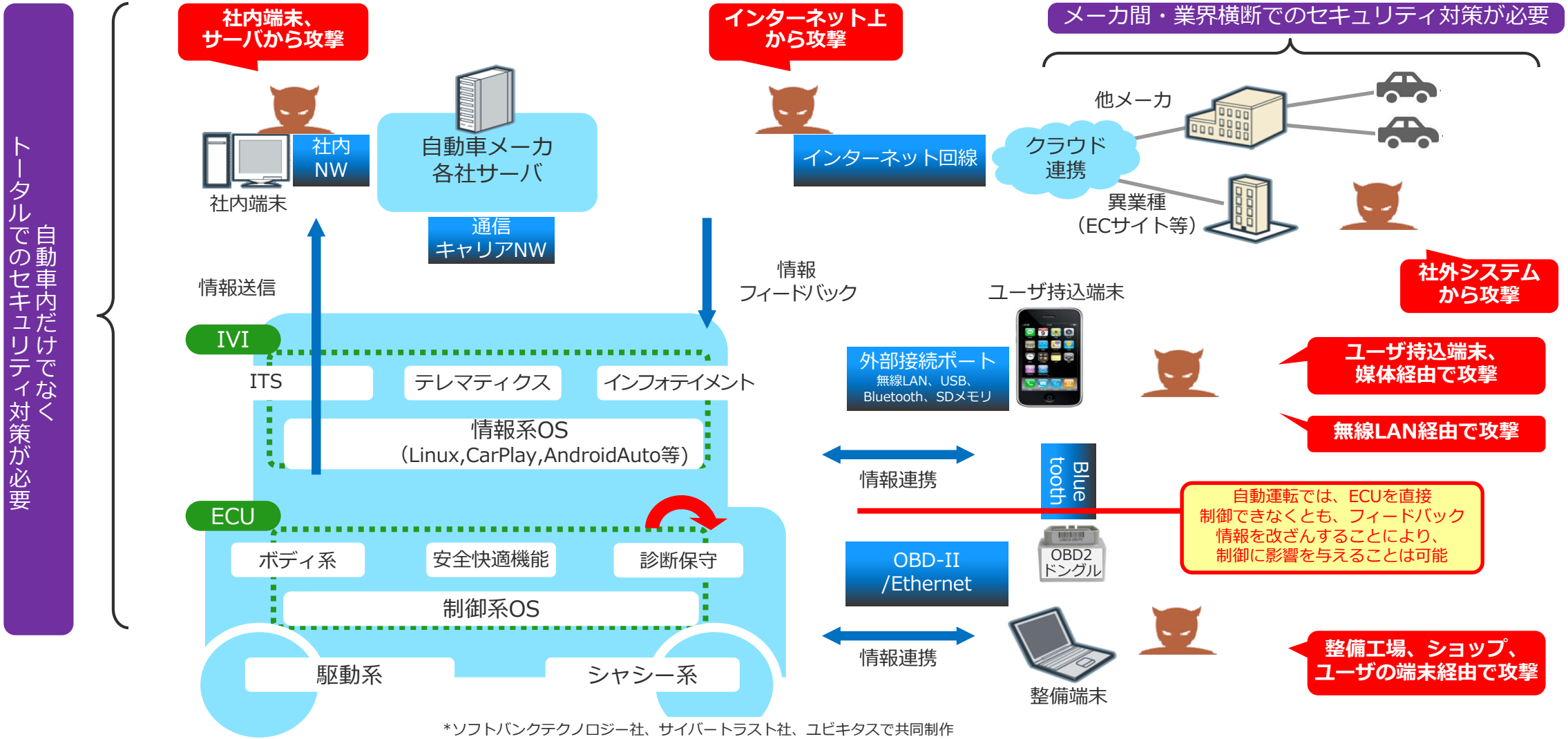


※出典：Banjo, Shelly. “Here are all the ways a hacker can take control of your car”. Quartz. http://qz.com/461576/here-are-all-the-ways-a-hacker-can-take-control-of-your-car/ より改変

出典：情報管理2018 1月号：自動車を取り巻くIoTセキュリティとその課題　倉地　亮

コネクティッドカーで想定されるサイバー攻撃

自動車が、一般の情報システムと同様の機能を持ち繋がることで様々な攻撃に晒される



*ソフトバンクテクノロジー社、サイバートラスト社、ユビキタスで共同制作

車載システムで想定される脅威例

項番	想定脅威	想定被害
1	外部ネットワーク経由で車載ネットワークにDoS攻撃	通信機能を必要とする全サービスの利用停止
2	サーバなりすましによる虚偽メッセージの送信	利用者の混乱など
3	第三者による受信機を用いた通信メッセージの盗聴	運用管理機関の意図しないサービスへの利用
4	第三者によるGPS信号発生器の悪用による、誤った位置を含むメッセージの配信	誤った位置を含むメッセージ配信による混乱の発生
5	利用者による車載器の悪用や第三者による通信機の利用により他の車載器へのなりすまし	誤った情報を含む走行情報配信による混乱
6	利用者による車載器の悪用や第三者の通信機の利用による路側機のなりすまし（路側機なりすまし	誤った情報を含むメッセージ配信による混乱
7	第三者による受信機の利用、利用者による車載器の悪用によって、受信メッセージから個人位置のトレース	個人のプロファイリング
8	3G/LTE回線から第三者が定常運用時に故意に制御ECUの制御機能を停止させる	ECUが正常に動作できなくなり車両機能が動作しない
9	スマートフォンなどのBluetooth機器からディーラ職員がメンテナンス時に車両状態情報を改ざんする	設定が不正に変更されて意図しない性能変更がなされる
10	SDカードインターフェースから第三者が定常運用時に故意にインフォメーションECUのインフォメーション機能の誤作動を誘発する	インフォメーション機能が正常に動作しなくなる

＊重要生活機器連携セキュリティ協議会（CCDS）車載SWG　検討資料より抜粋

自動車のセキュリティの動向

■ECUのハッキング

- 車内（OBDⅡ経由）➡ネット経由（IVI/ナビのWi-Fi、スマフォアプリなど）年々高度化かつ遠隔からの攻撃へ
  - Jeep Uconnect, GM OnStarなど
  - Jeep リコール 140万台　→16年にも走行時車両制御ハッキング
  - 日産 リーフ　→スマートフォンアプリの認証脆弱性　VINの5ケタ判明でネット経由で他車の制御
  - Tesla model S　→　17年遠隔操作で走行中車両の制御ハッキング
  - キーレスエントリ(Door, Engine)のイモビライザーハッキングの高度化

■米国：Auto ISAC設立 2016/01

- NHTSA（米　国家道路交通安全局）
  - 自動運転ガイドライン発行（セキュリティ、プライバシーも評価軸）
  - Cyber-Security Best Practiceガイダンス発行（対応ガイドライン）

■日本：JAMA,JasPar,JSEAなどが業界横断的な標準化推進（日本版Auto ISAC WG設置）

自動車のセキュリティの動向

- 日本：JAMA,JasPar,JSEAなどが業界横断的な標準化推進（日本版Auto ISAC WG設置）
- ISO26262(セーフティ） V.S. SAE J3061(セキュリティ）
  - J3061(SAE)との共同策定 ＝＞ISO/SAE 21434（Automotive Security Engineering)
- TCGでのTPM2.0上でのAutomotive Profileの検討,標準化
  - TNCと合わせたセキュアOTAアップデートへの取り組み
- 情報系でのセキュリティ対策
  - Tesla,GM,Fordなど自動車メーカー主催のハッキングコンテストなどによるコミュニティベースでの脆弱性の発見と対策

CASE時代の自動車開発の主要要素
～ソフトウェア、サービス開発がより重要に

Connected
Autonomous
Sharing & Services
Electric

Security

- CASE実現にセキュリティが必須。レイヤに応じたセキュリティ対策が必要
- 通信暗号セキュリティ、認証、ソフトウェア脆弱性の極小化、進入検知、改ざん防止、データ保護、リモート検証など

Platform

- MaasSビジネスのサービスプラットフォーム（認証、シェアリング、マルチモーダルサービス、、、）
- サービスカー、無人物流、無人小型公共交通などの社会交通インフラプラットフォーム
- 電力グリッドの一部としてのモビリティグリッドプラットフォーム

Autonomous

- センサー技術とAIを活用したダイナミックMAP、高度な自動運転制御技術
- リアルタイムテレメタリングデータを活用したダイナミックMAPとITSインフラ、広域道路交通、気象情報などとの連携

Connectivity

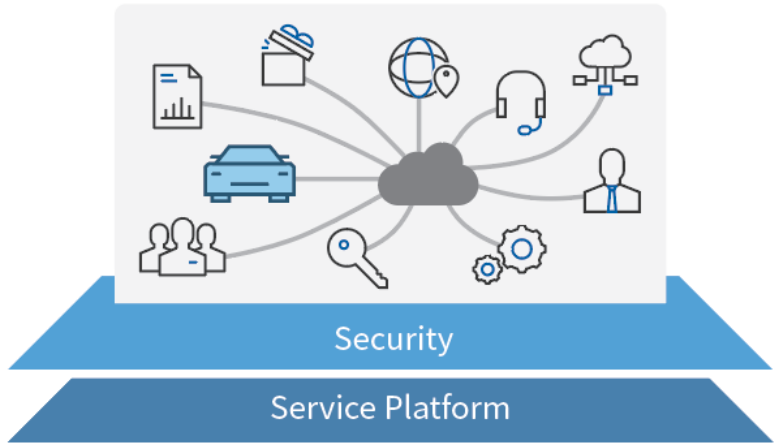
- In-Car, Out-Carを接続するセキュアなV2Xコネクティビティの実現
- V2V, V2I, V2H, V2G, V2M(P), V2N, V2S, V2C

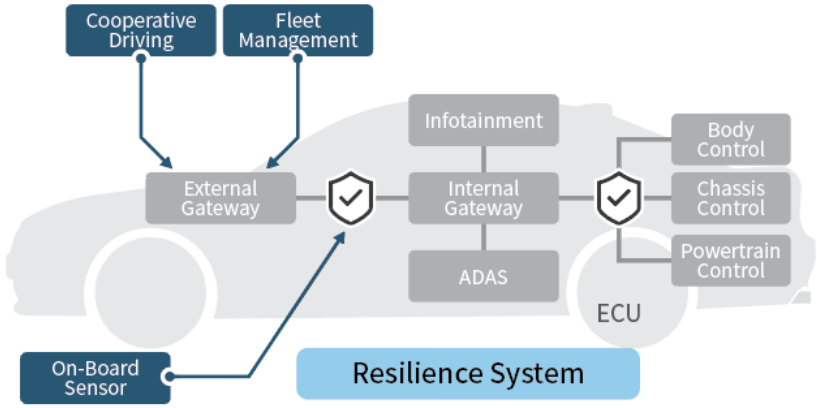
Electrification

- モジュール化された電子プラットフォームとソフトウェアによるコンフィギュアブル、アップデータブルな制御とサービス
- 充電スポットによる新しいサービスの可能性（セキュリティ、認証の確保が課題）

*参考出典:IoT NEWS AMO Labs CEO シン・サンギュ氏提唱　佐野加筆

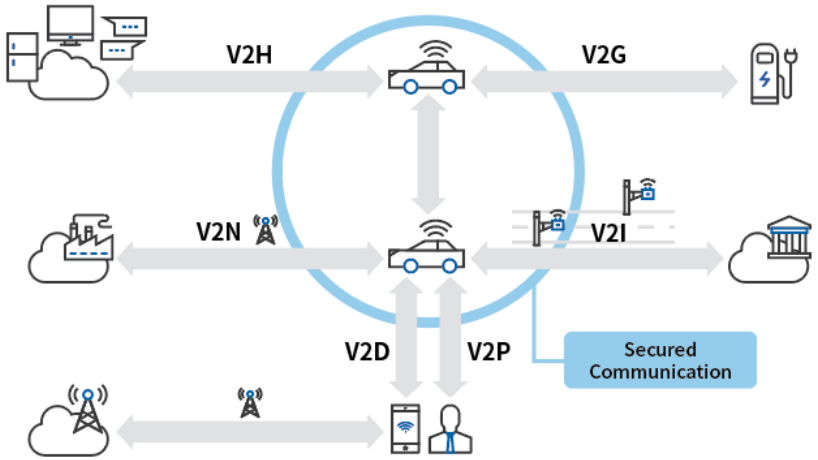
セキュリティの確保がCASE実現への第一歩

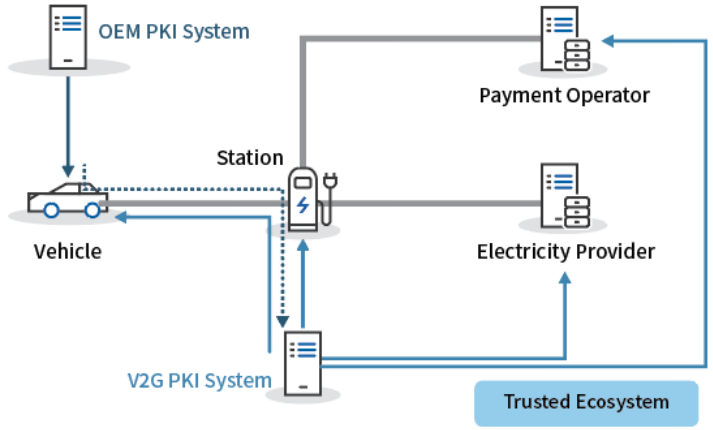




Platform | Autonomous

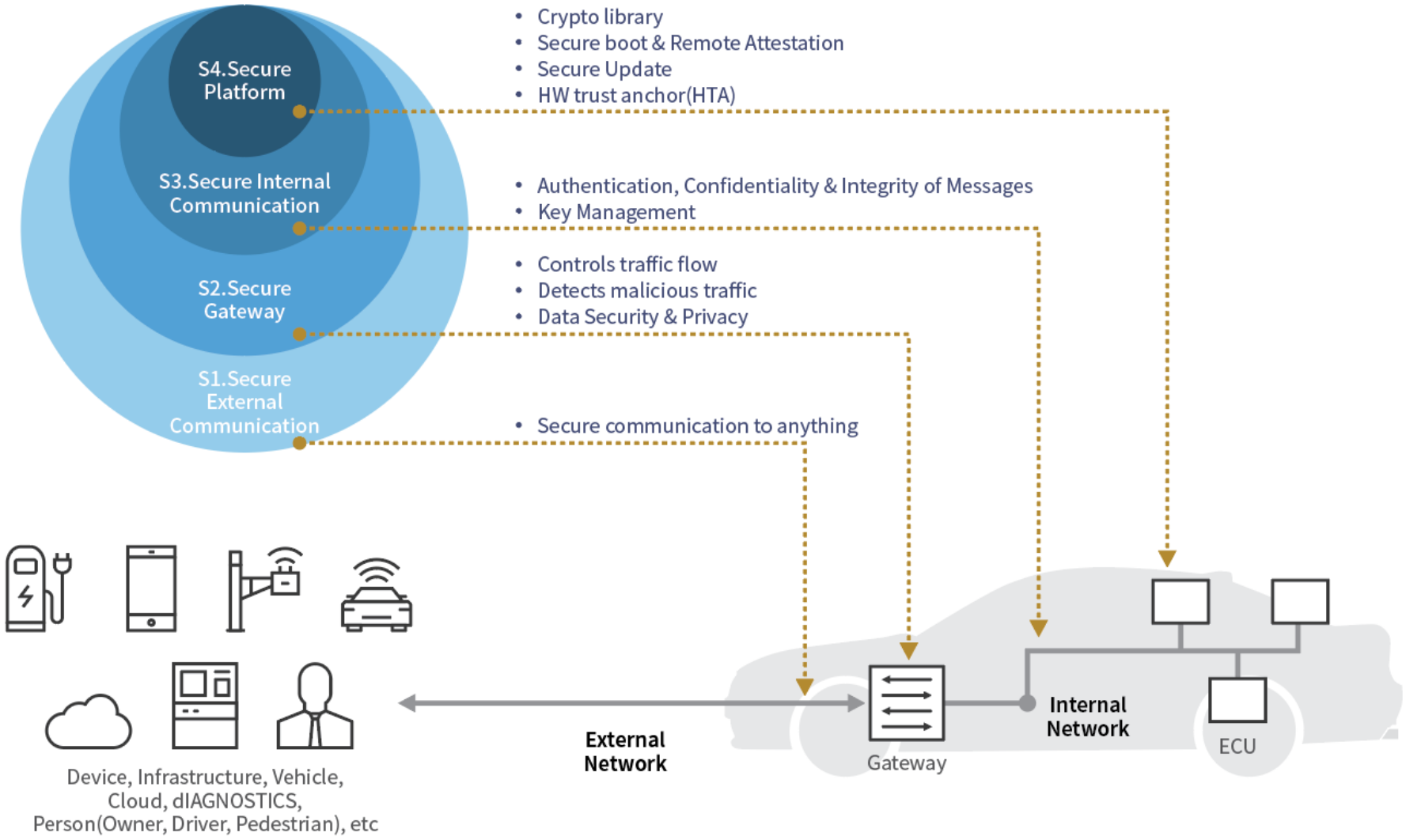
Connectivity | Electrification





*参考出典:IoT NEWS AMO Labs CEO シン・サンギュ氏提唱

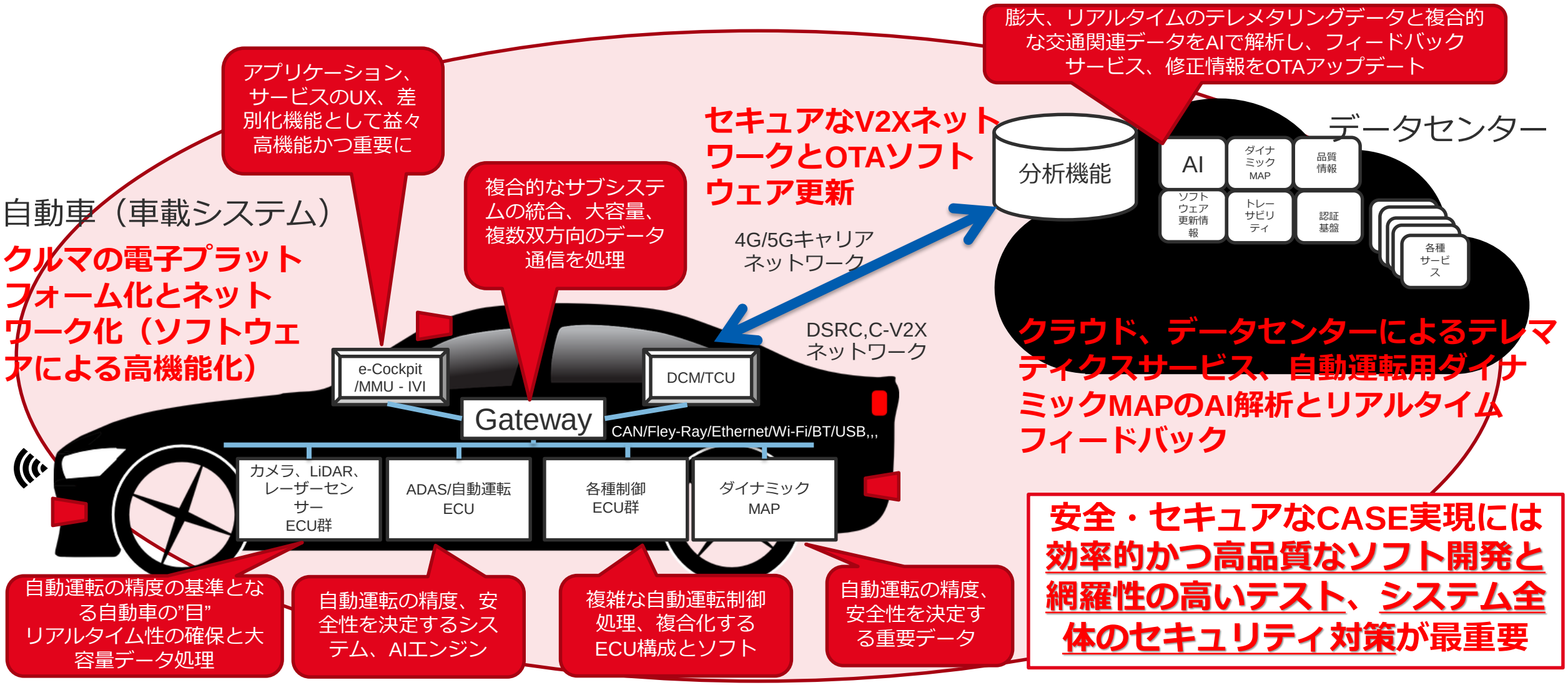
セキュリティの確保がCASE実現への第一歩



*参考出典:IoT NEWS AMO Labs CEO シン・サンギュ氏提唱

次世代自動車のシステム構成要素

～ソフトウェア規模は2億行の未知の世界へ：　ソフトウェアの脆弱性がセーフティとセキュリティに大きく影響



拡大するセキュリティ・プライバシー対応課題

従来のスタンドアロンの自動車からIoTデバイスとしてのコネクティッドカー/自動運転車への進化

考慮すべき要素が拡大

機密性 (Confidentiality) → 完全性 (Integrity) → 可用性 (Availability) → 信頼性 (Reliability) → 責任追跡性 (説明可能性) (Accountability) → 真正性 (認証性) (Authenticity)

セキュリティ設計

- 企画・設計・開発・製造段階でのセキュリティの考慮
- Security by Design
- Privacy by Design

セキュリティ検証

- 自動車・インフラ・サービスまで含めた総合的・複合的な検証
- サイバー攻撃を想定した実地検証

セキュリティ運用

- 自動車のライフサイクルを考慮した継続的に問題を検知し対応する仕組みの確立(リコール対応含む)
- 社会インフラの重要構成要素としてのセキュリティインシデントの共有スキームの確立
- プライバシー確保の仕組み

業界全体で、企画時から一貫したセキュリティ・プライバシー確保のための検討、ポリシー設定の強化が必要

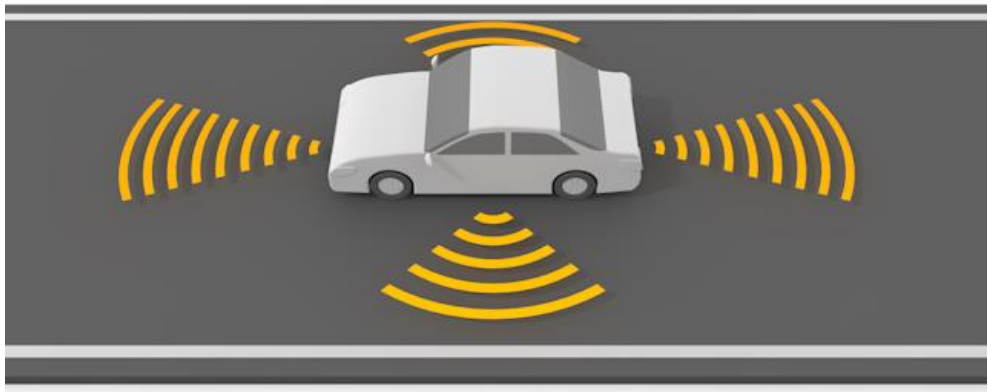
コネクティッドカー時代に向けたセキュリティ対策

Life Cycle Management

Platform Integration

Cryptography Offloading

Audit



Stored Data Protection

Authentication

Boot Process Protection

Secure Communication

Key Management
Crypto Key Establishment and Management

Secure Software Update

- OEMとしてのポリシー設定から、設計ー開発ー製造ー流通ー廃棄(リサイクル)まで一貫した対応が必要
- 行政/業界団体/OEMからサプライヤー、ディーラー、修理工場、流通事業者、サービス事業者まで川上から川下まで連携が必要

自動車分野でのセキュリティ対策におけるFACT

84%

サイバーセキュリティ・プラクティスが**テクノロジーの変化に追いついていない**

- 自企業で開発している車載ソフトウェアが今後12カ月のうちに攻撃を受ける可能性がどれぐらいあると考えるか? => 62%
- サイバーセキュリティにおいて最も大きなリスクとなるものは？ => 自動運転車 58%、テレマティクス 60%、　無線技術（Wi-Fi, BT, HotSpotなど）63%
- ソフトウェアアップデート、セキュリティ脆弱性に迅速に対応できていますか? => いいえ 61%

30%

製品サイバーセキュリティに関する正式なプログラムや**チームを設立していない**

- 製品開発に必要なサイバーセキュリティスキルを備えていますか -> いいえ　62%
- サイバーセキュリティ対策に十分なリソース(予算、人）が割り当てられていますか? => いいえ 51%

63%

全体の半分未満しかハードウェア、ソフトウェア、その他のテクノロジーの**脆弱性テストを実施していない**

- 車載ソフトウェア/テクノロジー/コンポーネントに対して社内または外部で発行されたセキュア・ソフトウェア開発ライフサイクル（SSDLC)プロセルに従っていますか？ => いいえ　36%

出典：SAE InternationalとSynopsys社が車載コンポーネント実装、評価に関わっている593人(サンプル抽出15400人、2018年7月調査）のプロフェッショナルに調査を実施。最先端の自動車セキュリティ：自動車業界のサイバーセキュリティ・プラクティスに関する調査を発行

自動車分野でのセキュリティ対策の困難さ

- 自動車の設計、開発、製造バリューチェインの工程量、複雑さと期間
  - 多層サプライヤとのカスタム品のすり合わせ開発の集大成、メカ、ボディ、部品修理中心のメンテナンスネットワーク
  - 電子化が進む自動車 ECU100個の時代へ – 超高速並列コンピューティング
  - 自動運転化に伴うデータ量と伝送スピード
  - 高度制御と情報化が同時に進行するエッジIoTデバイス、ソフトウェアは２億行超へ　=> 企画から出荷まで3～５年

自動車分野でのセキュリティ対策の困難さ

SafetyとSecurity

- 「走る」「曲がる」「止まる」の生命の保護資産の重要性 => 可能性、完全性が重要
- 性能と安全・安心のバランスポイント => ソフトウェア脆弱性が安全リスクを増大
- 自動運転の安全検証テストは130億キロ相当　－＞人力での限界

自動車分野でのセキュリティ対策の困難さ

- 自動運転、CASE、MaaS時代でのサービスビジネスへのシフト
  - 動的なプライバシー情報の管理
  - シェアリングに向けた情報のライフサイクルマネジメント
  - 無人運転時の補償の責任（物理的な事故へ直結）
  - 異業種のサービス事業者、エンドユーザーも含めた対策が必要（責任の拠り所は誰？）

自動車のSafetyとSecurity

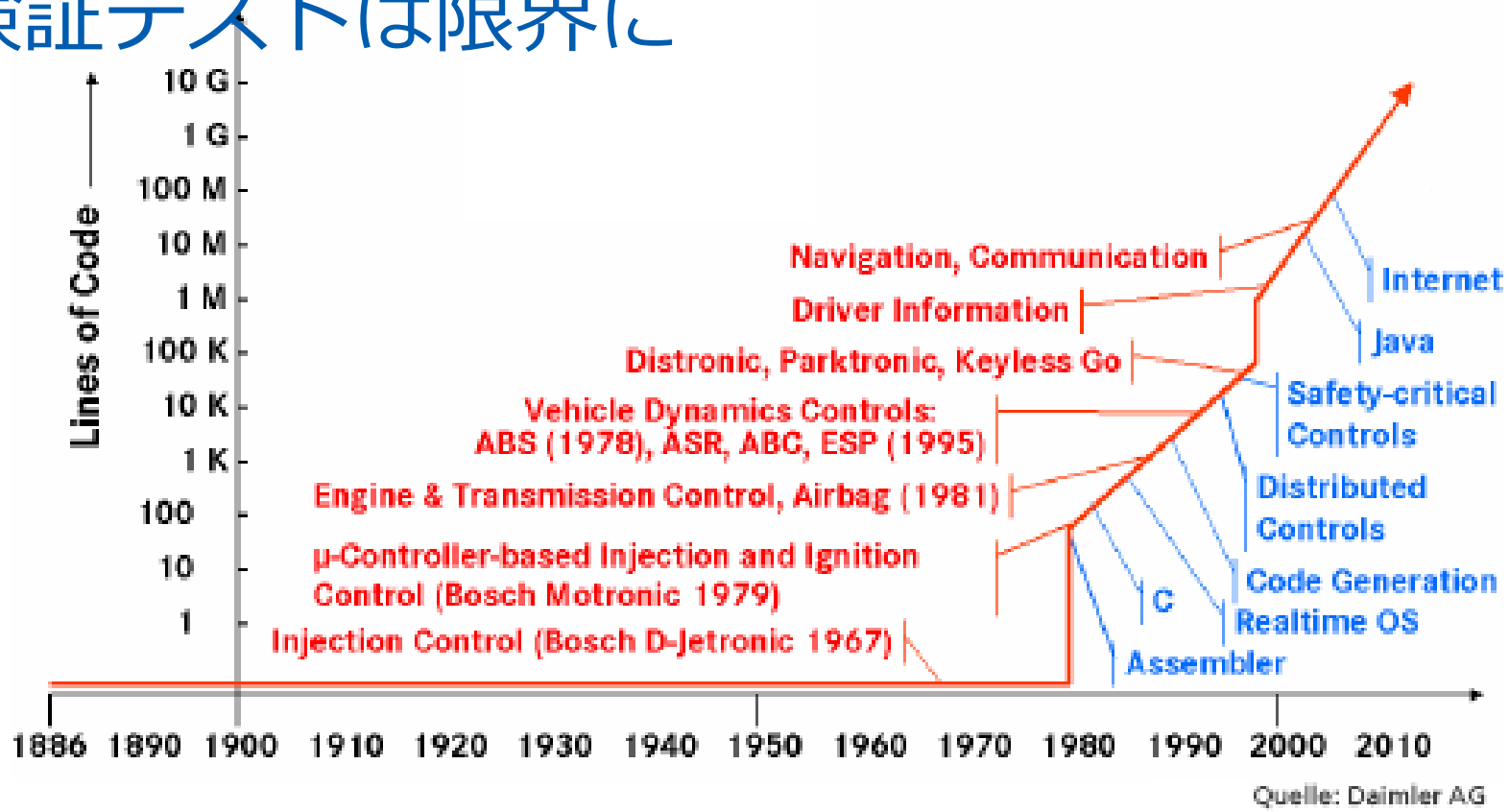
- 機能安全（ISO26262)に対応していることが大前提
  - 安全 >> セキュリティであるが、セキュリティを突破されることで発生する安全面の危険性も存在
- 保護すべき資産の明確化
  - 自動車の利用シーンによって、生命（資産）、物理資産と情報資産の重要性と攻撃、奪取される目的が異なる
- 安全関連の危害
  - 攻撃手段の難易度によって、実現のコストとリソースのバランスの考慮の必要性
  - 自動運転車はソフトウェアの脆弱性に起因する安全性の低下のリスクが増大

複雑化、膨大化する開発工程において
自動運転時代の安全を守る
ソフトウェア品質確保に向けて

Ubiquitous AI Corporation

自動車向けソフト開発の現状

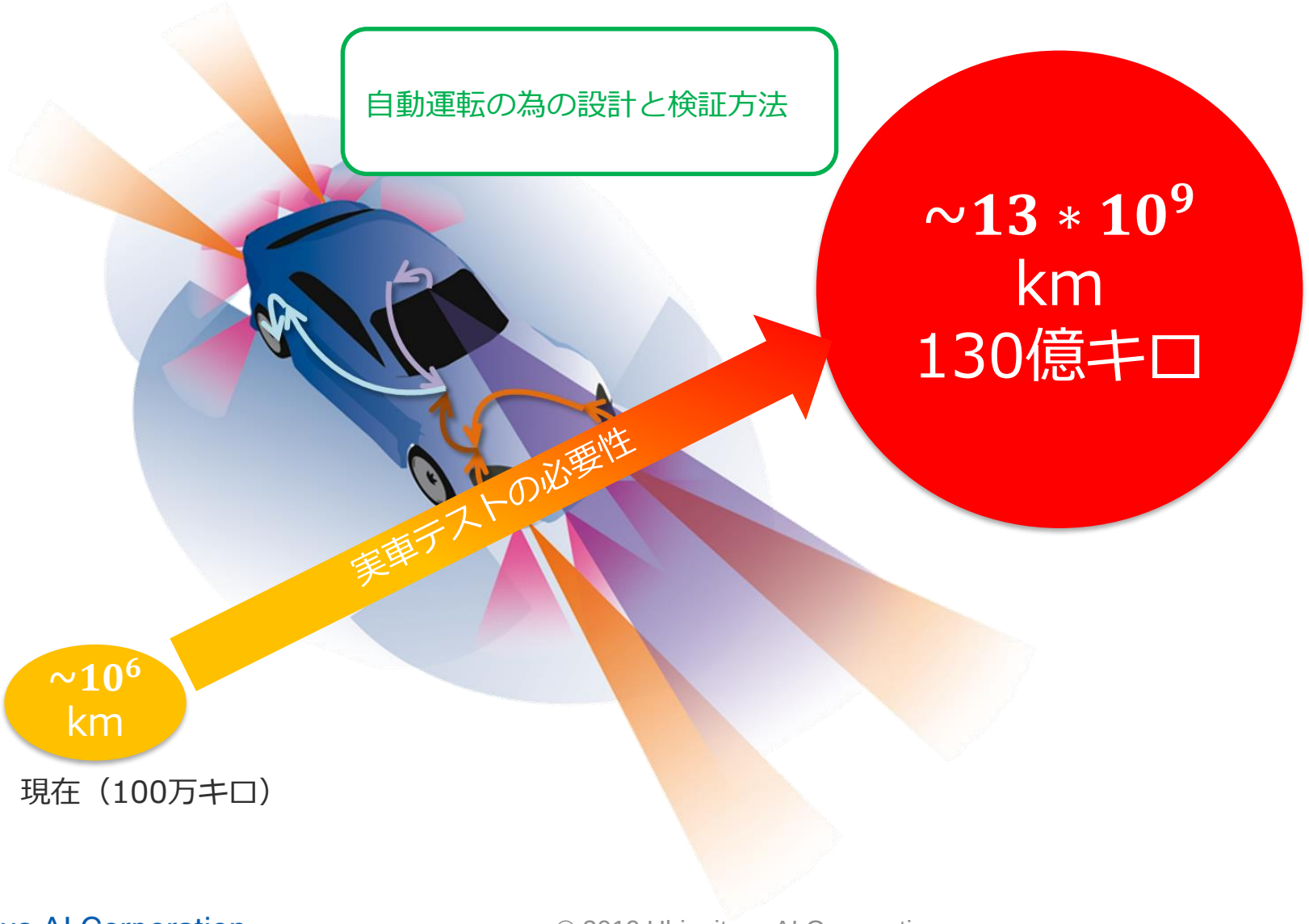
- 複雑な仕様、膨大なコード
- 車載ソフト、特に自動運転では、絶対的な信頼性が必要
- 人手で検証テストは限界に



Quelle: Daimler AG

車載ECUに求められる信頼性

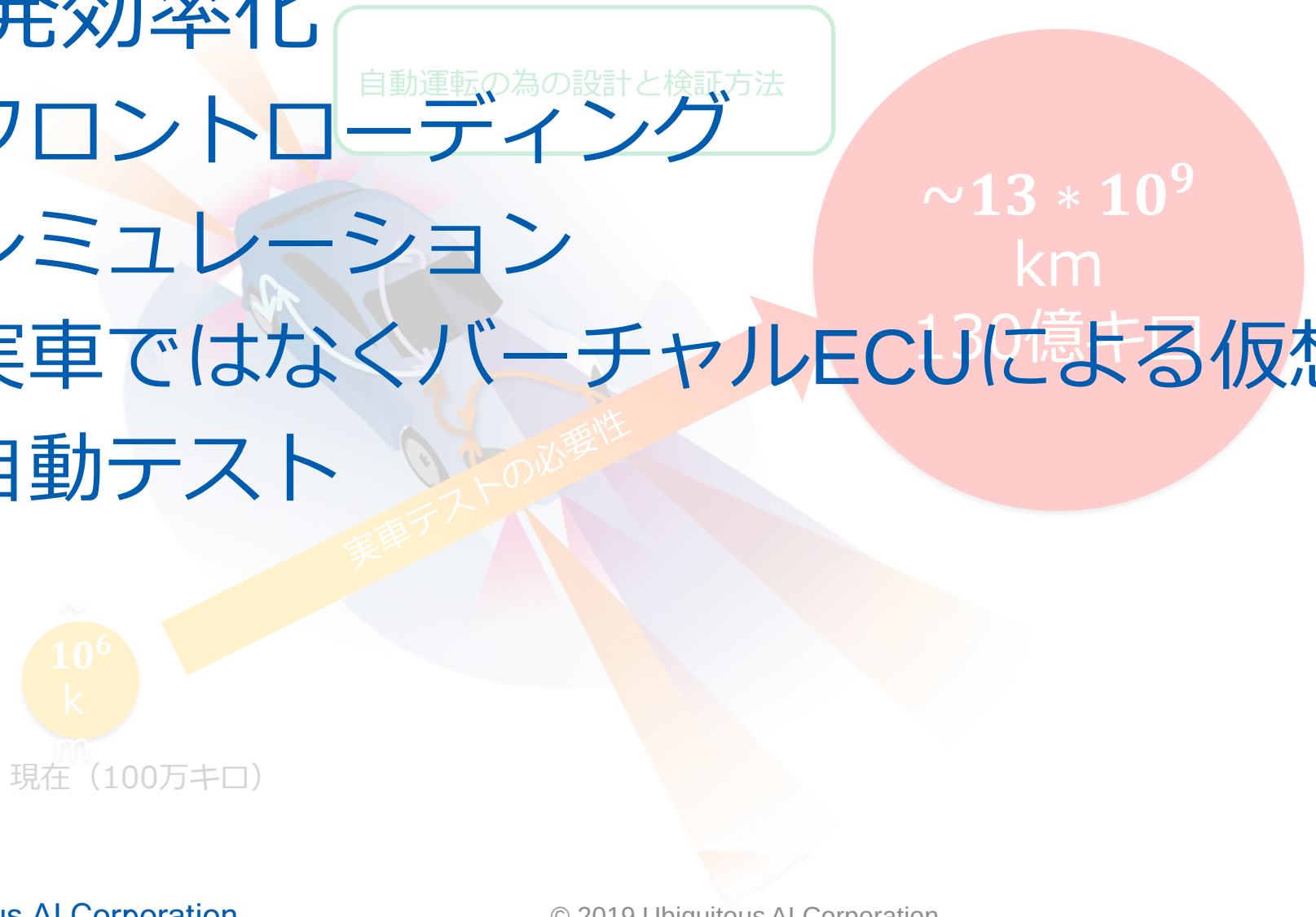
Estimated effort for high automated driving
Prof. Hermann Winner, TU Darmstadt



車載ECUに求められる信頼性

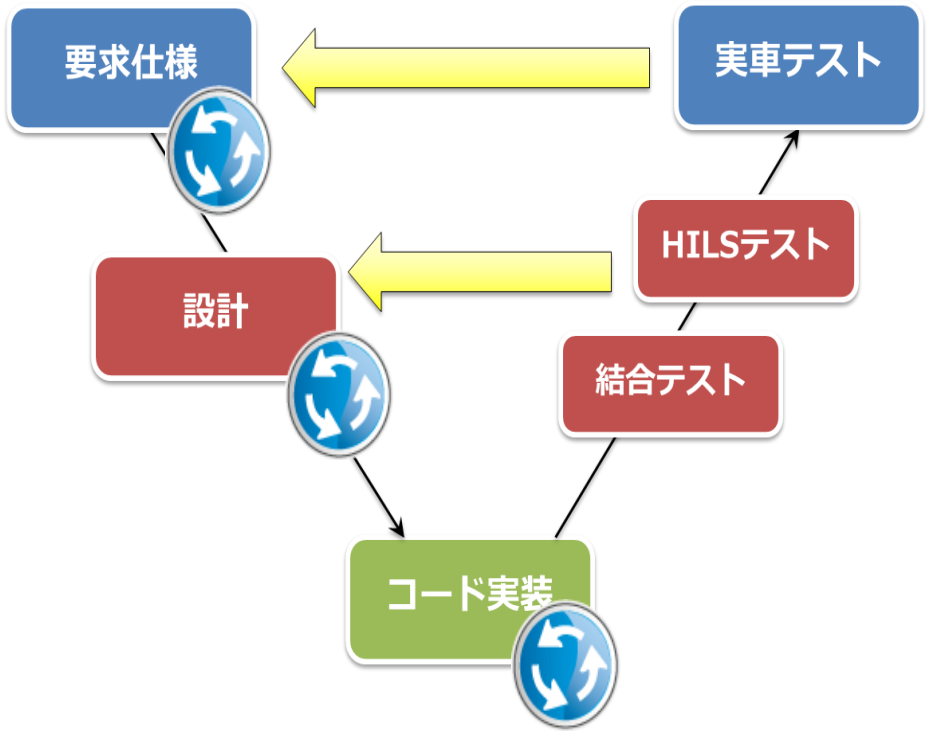
Estimated effort for high automated driving
Prof. Hermann Winner, TU Darmstadt

- 開発効率化
  - フロントローディング
  - シミュレーション
  - 実車ではなくバーチャルECUによる仮想検証
  - 自動テスト



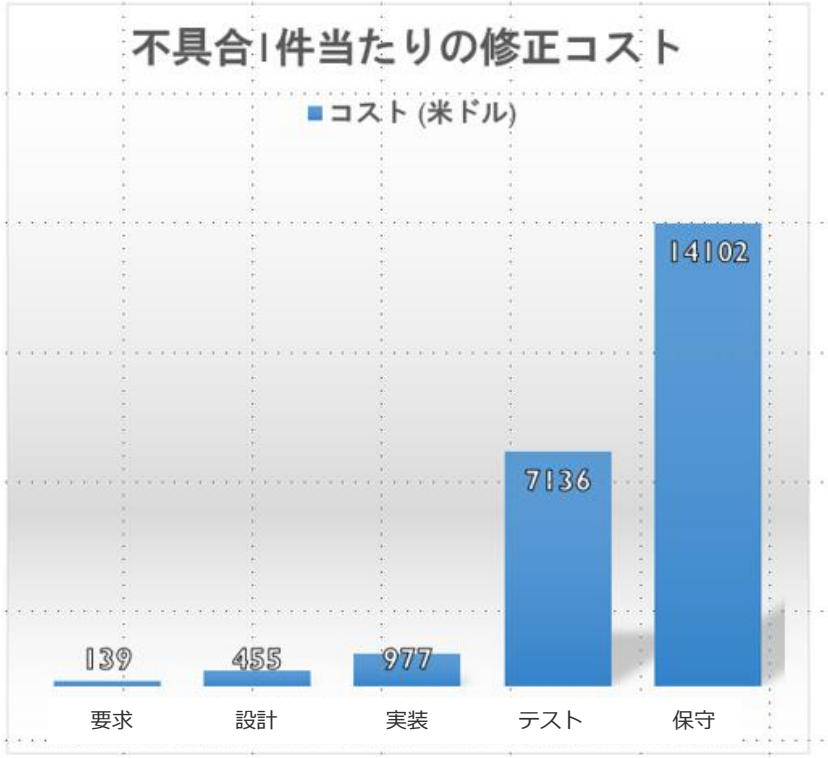
フロントローディングの利点

- 開発プロセスのやり直し



テスト ➡ 不具合再現 ➡ デバッグ ➡ 仕様再検討 再設計 ➡ 実装 ➡ リグレッションテスト

- 手戻りによるコスト、開発遅延



出典: IBM Systems Sciences Institute

フロントローディングの実践

■要求仕様のシミュレーションによる検証

- –要求仕様の不具合は物ができないと実行、検証ができない
  - 手戻り工数が非常に大きい
  - 形式検証
    - スケーラビリティ、実装の検証ができない。⇒．．．

フロントローディングの実践

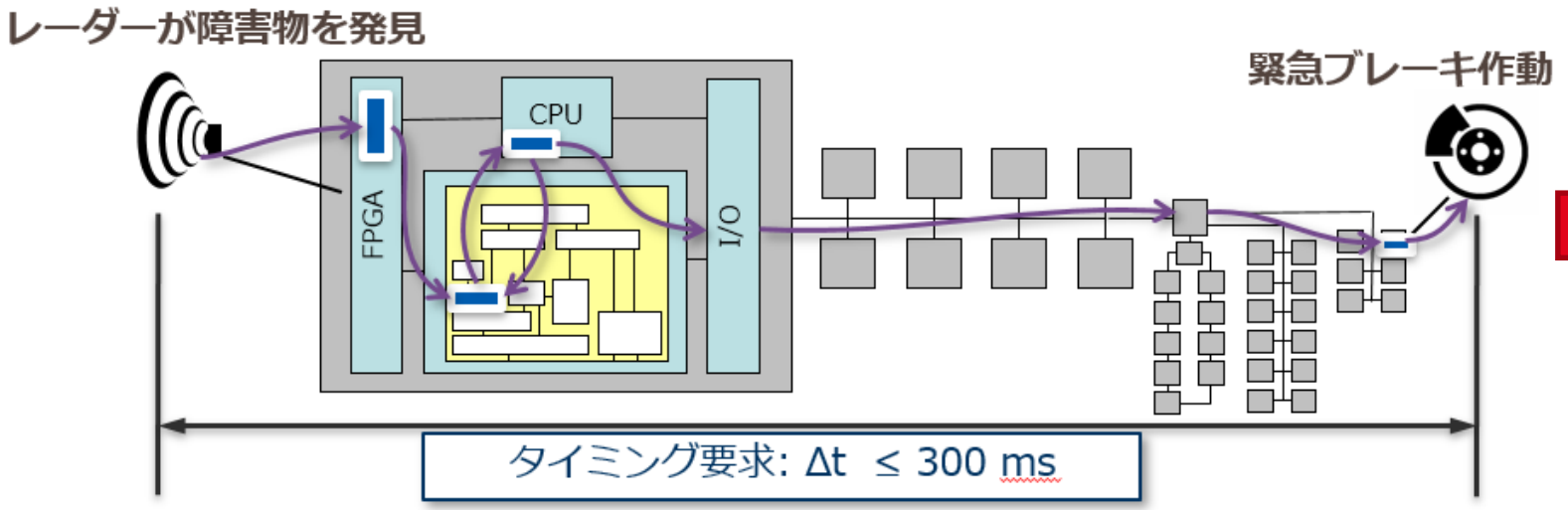
■静的解析

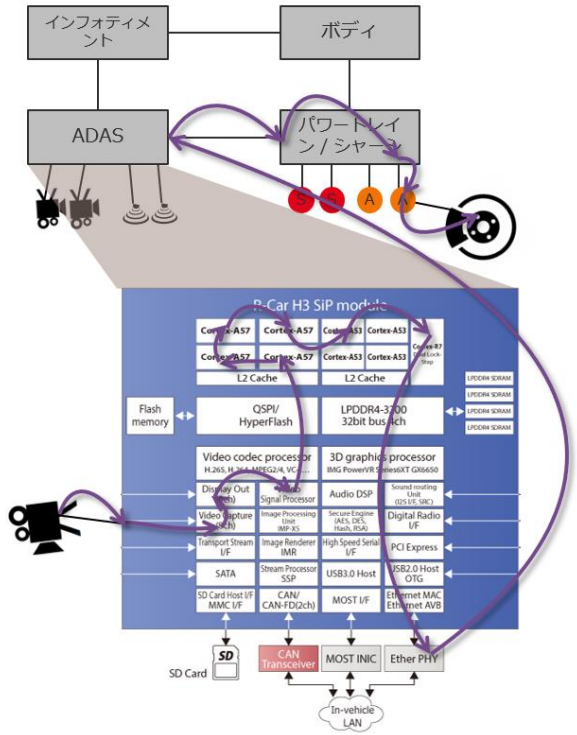
- ソースコードを解析
- テスト実行前に、テスト無しで不具合を検出
- デバッグ不用
- コーディングルールのみでなく、実行時エラー検出可能が重要（まれにしか起きないケース）
- 脆弱性の検出可能（CERT、CWE）

フロントローディングの実践

タイミングのシミュレーションによる検証

- 自動運転では、複数のECUが通信を行う
  - タイミング要求の検証は難しい
- ECUができてからの検証では遅すぎる
- シミュレーションであれば、問題発見⇒設計変更⇒確認のループは直ぐに終了
- まれに起きるタイミング要求不具合を見つけるのは難しい



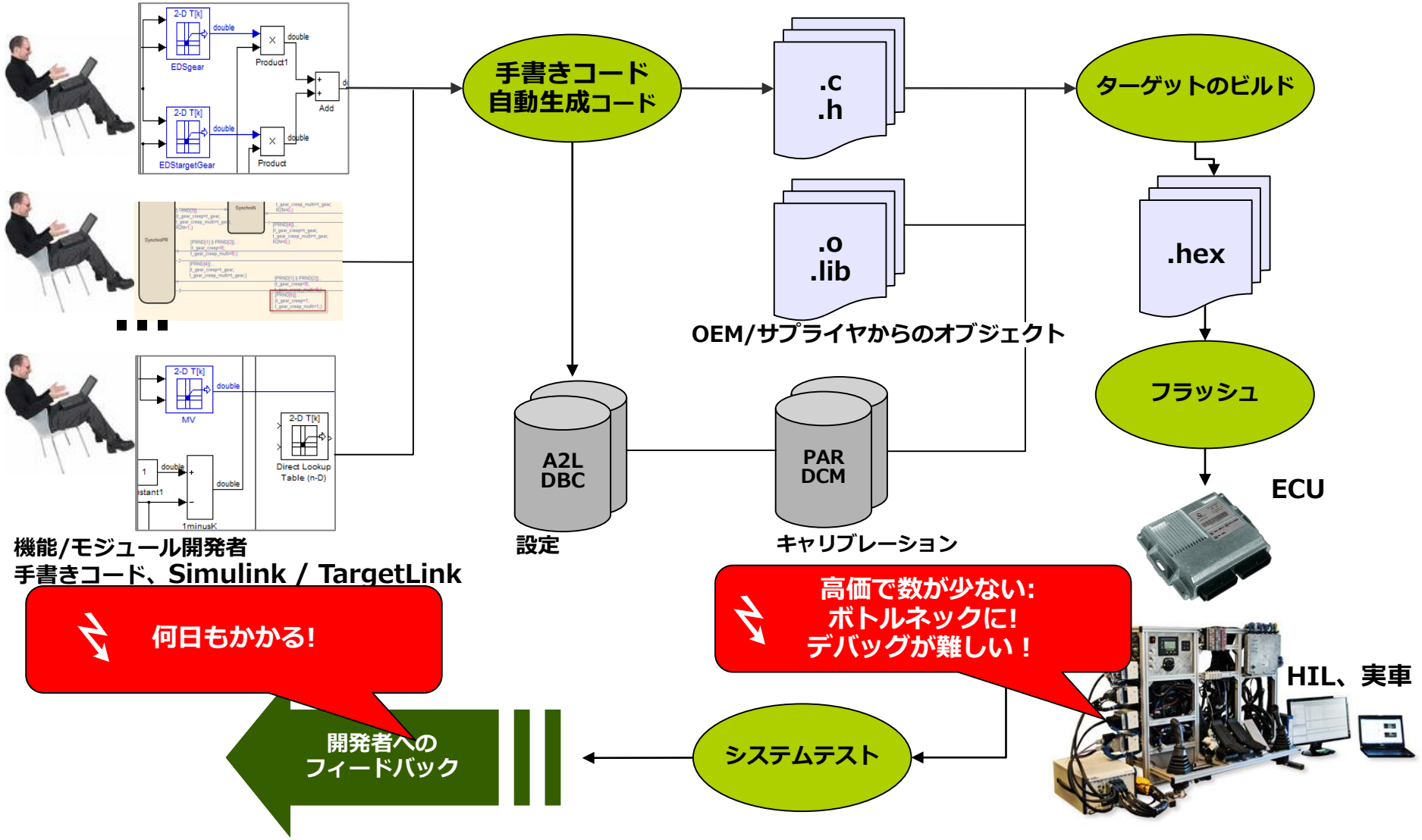


ヴァーチャルECUによる仮想検証

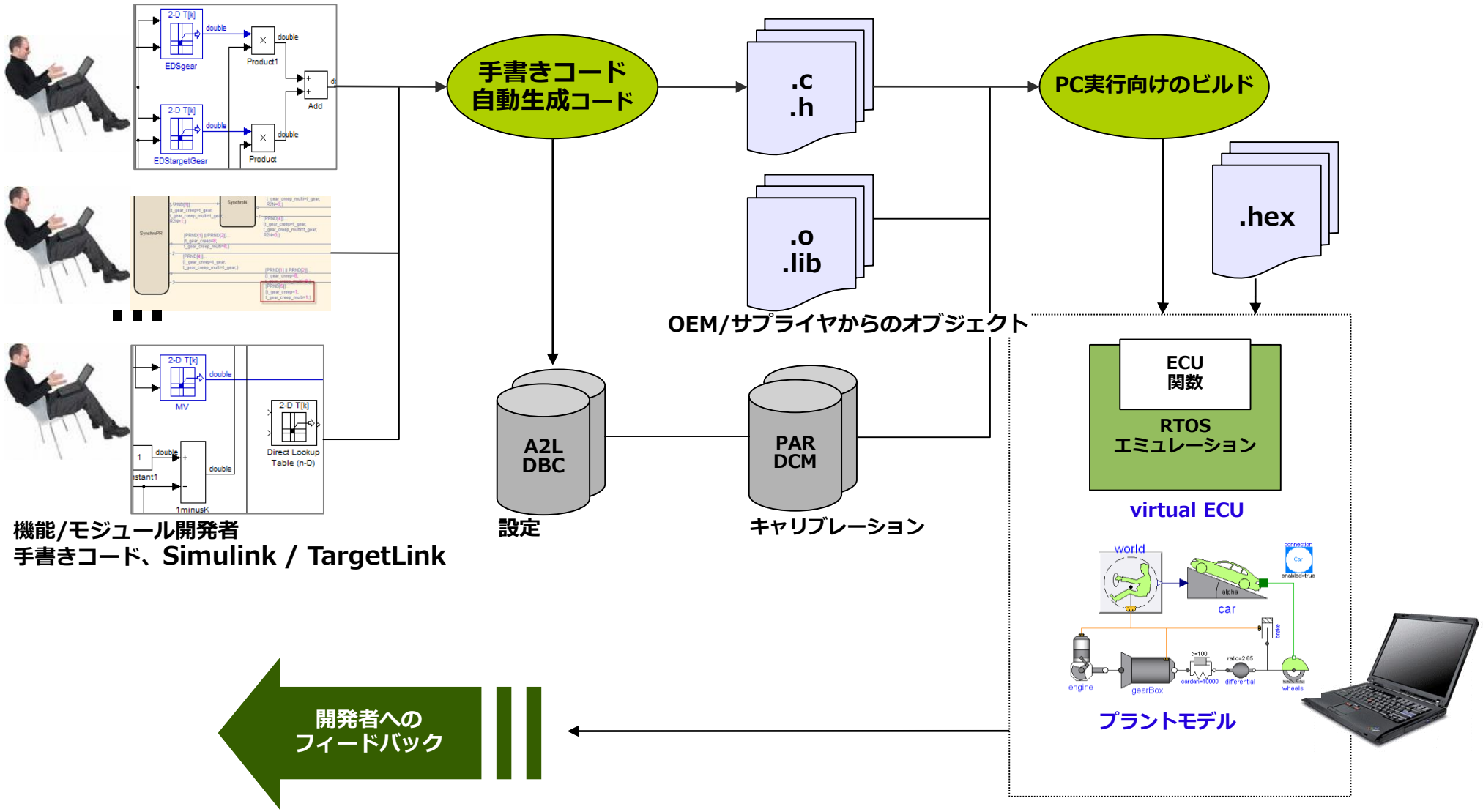
■実車、HILSではなく、PC上でソフト実行

- –安価に環境構築可能
  - • 全ての機能開発者が使用可能
- –自動テストが可能に
  - • 自動テストツールへの連携が容易
- –不具合の再現、デバッグが容易
  - • 実車やHILSでは、例えば例外が起きて、CPUリセットしても、原因を探るのは難しい
  - • ⇒Visual Studio等のIDEを使用して、ブレークポイント、ステップ実行

今のECUソフトウェア開発プロセス



ヴァーチャルECUによる仮想検証



自動テストによる検証

今までのテスト

- 実車、テストスクリプトの作成。網羅性が低く、信頼性の検証ができない。

自動テスト

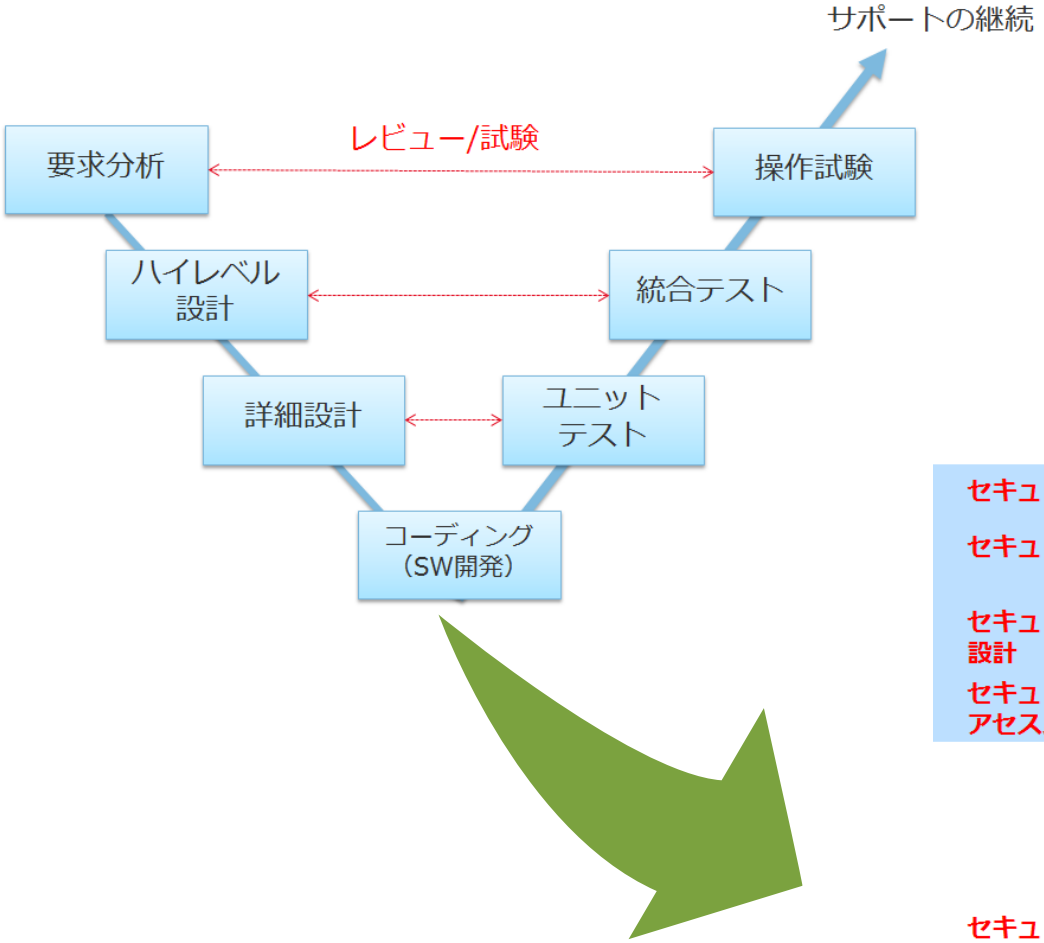
- 非常に多くのテストによる網羅率向上
  - 信頼性の大幅な向上が可能に
    - 実車テストや手書きのテストスクリプトでは、まれに起こる不具合は中々検出できない
    - 不具合が起きても再現できない
  - 脆弱性のもととなる実行時エラーの自動検出
  - 要求仕様を満たしているかどうかを自動でテスト
  - 実際にネットワークに自動で膨大なパターンのテストシナリオを流して、脆弱性を検出（ファジングツール）

CASE時代のセキュリティ対策について

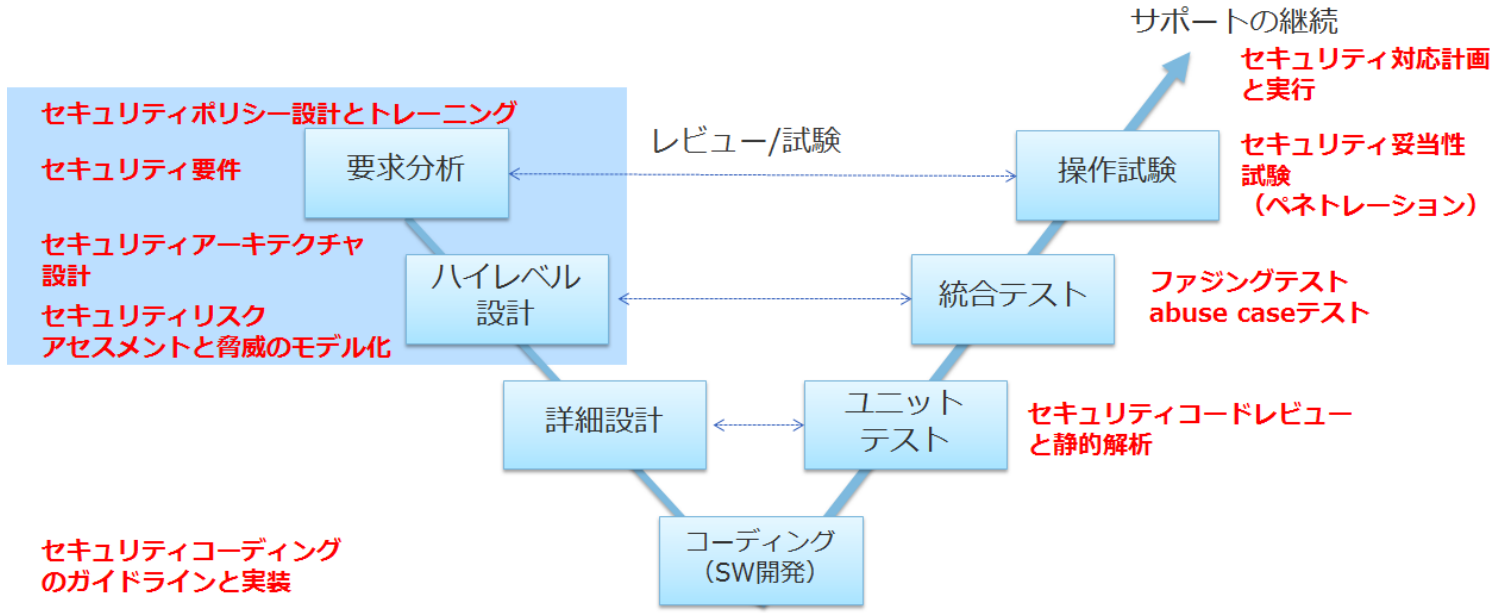
Ubiquitous AI Corporation

Security Development Lifecycleへ

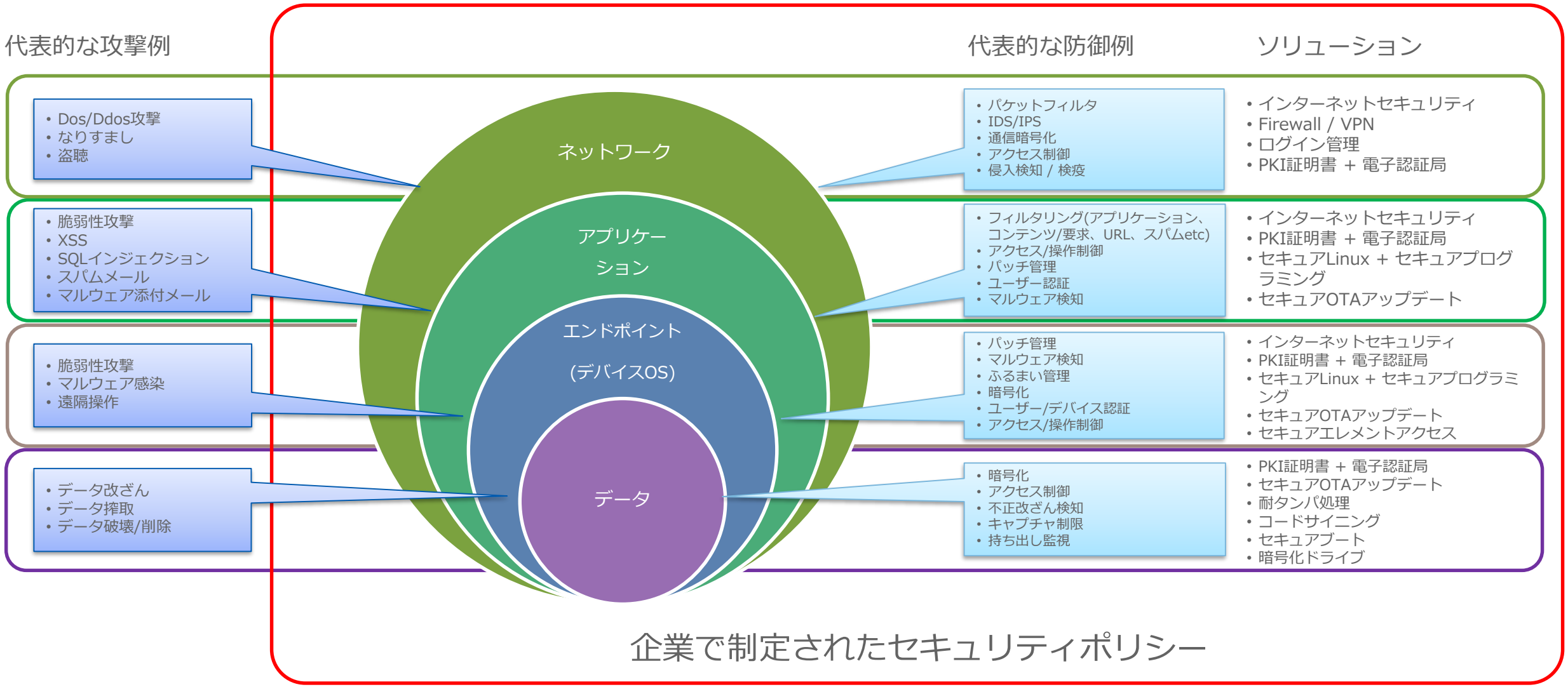
- これまでの自動車のV字開発プロセス



- 次世代自動車の新しいV字開発プロセス（Security Development Lifecycle）の導入

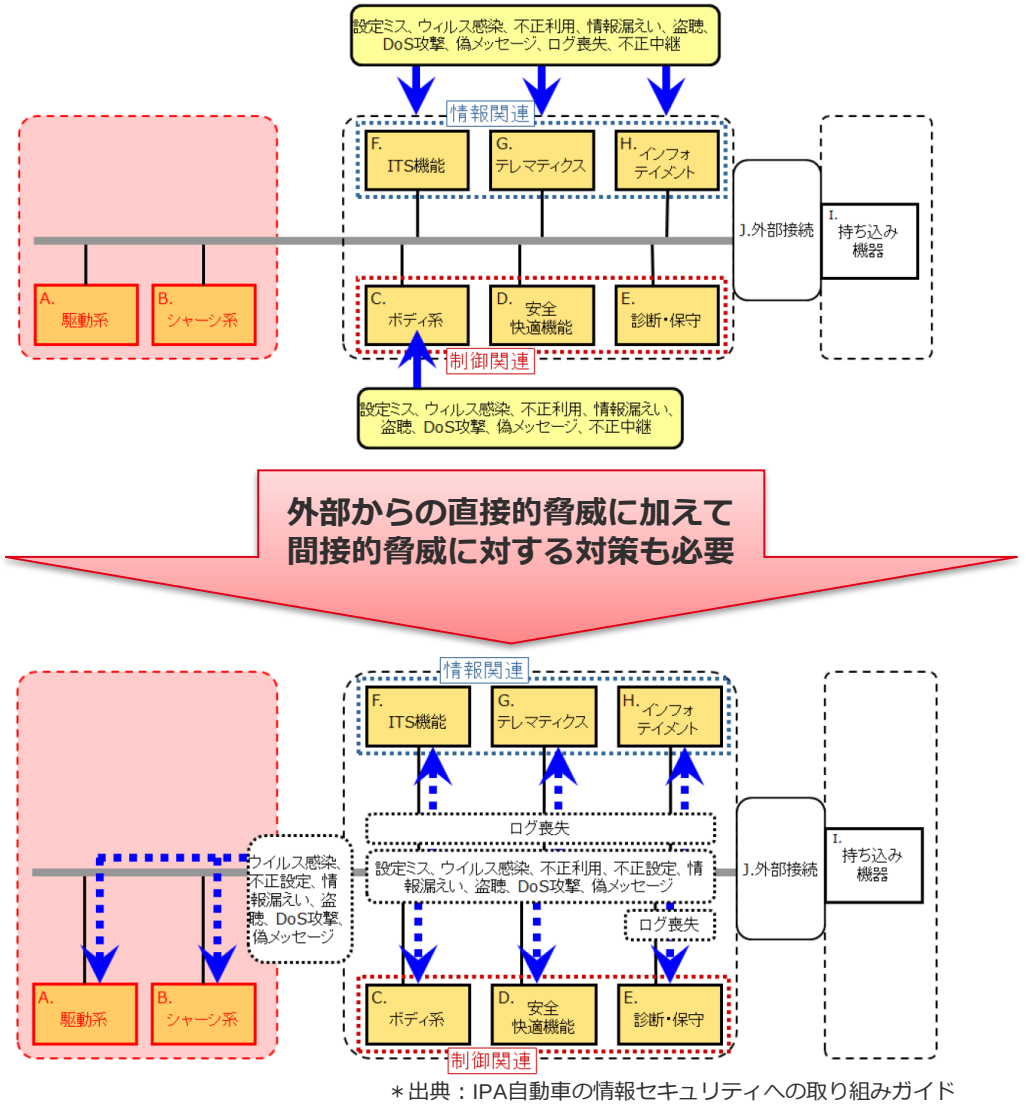


サイバー攻撃への備え　多重防御の考え方



サイバー攻撃への備え　多重防御の必要性

- レイヤに応じたセキュリティ対策が重要
  - クラウド、インターネット
  - 接続インターフェース
  - アプリケーション
  - OS/ファーム、ソフトウェアプラットフォーム
  - データ、秘匿データ（秘密鍵/証明書など）
- レベルに応じたセキュリティポリシー
  - 情報系：なりすまし、プログラム/データの改ざん、プライバシー情報の盗窃
  - 制御系：制御乗っ取り、無効化
  - 情報系と制御系のゲートウェイ(セントラルゲートウェイ、DCU/TCUなどの通信ブリッジ)

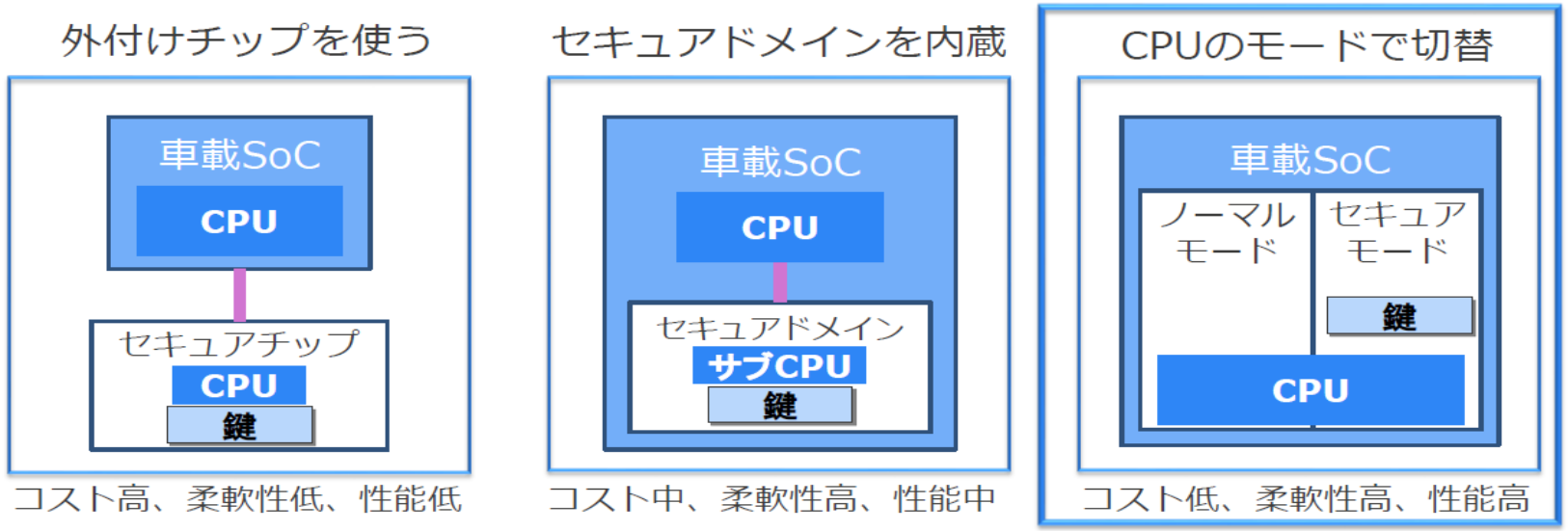


＊出典：IPA自動車の情報セキュリティへの取り組みガイド

車載コンピュータのセキュリティの技術動向

セキュリティを担保するための重要技術要素

- セキュアドメイン：ノンセキュアソフトから介入できない領域の確保
- 鍵管理ソフト：改ざんされていないかチェックが必要
- 鍵：鍵が流出しない仕組みが必要
- 守るべきものの重要度と脅威分析から実装レベルを決定（実装コストと性能のバランスが重要）
- セキュリティのアップデートプロセス(PDCA)



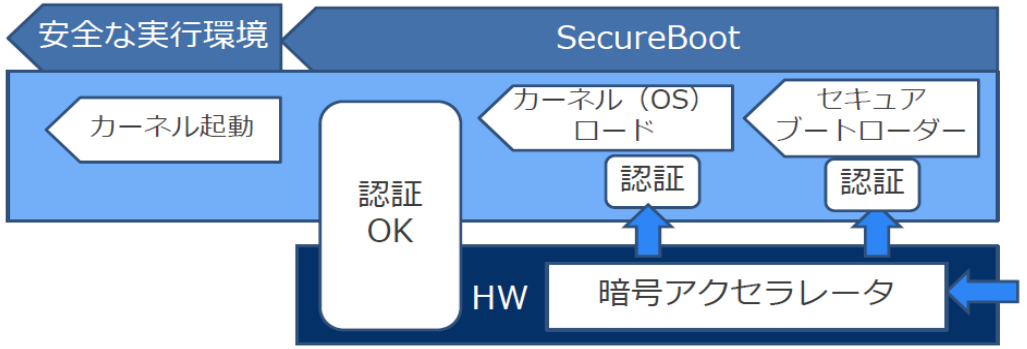
*ルネサスDevCon2017資料から抜粋

車載コンピュータのセキュリティの技術動向

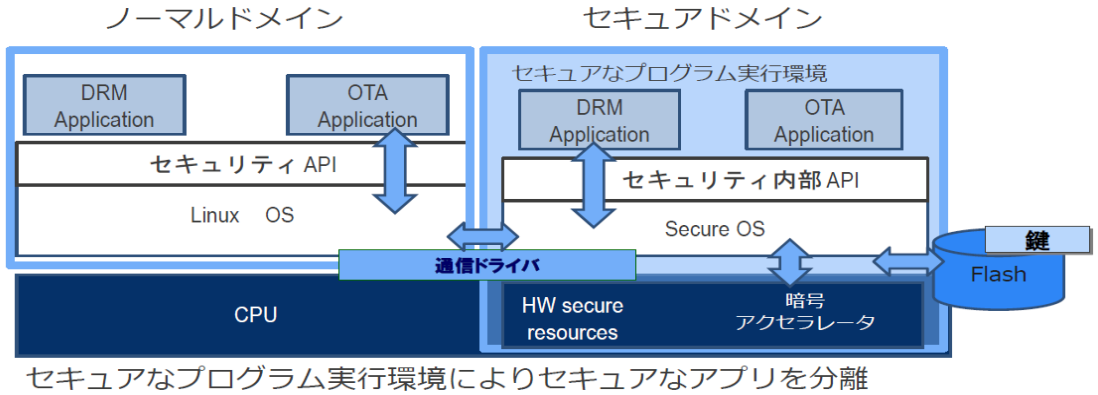
セキュアドメイン、HMSなどを利用し耐タンパ性の高いセキュア環境を確保し、実行環境を保護、改ざん防止

- SecureBoot
  - OS、SWなどの不正改ざんのチェック後、安全なアプリケーション実行環境を起動

- セキュアなプログラム実行環境
  - セキュアドメインを利用し秘匿性が必要なアプリケーションを分離



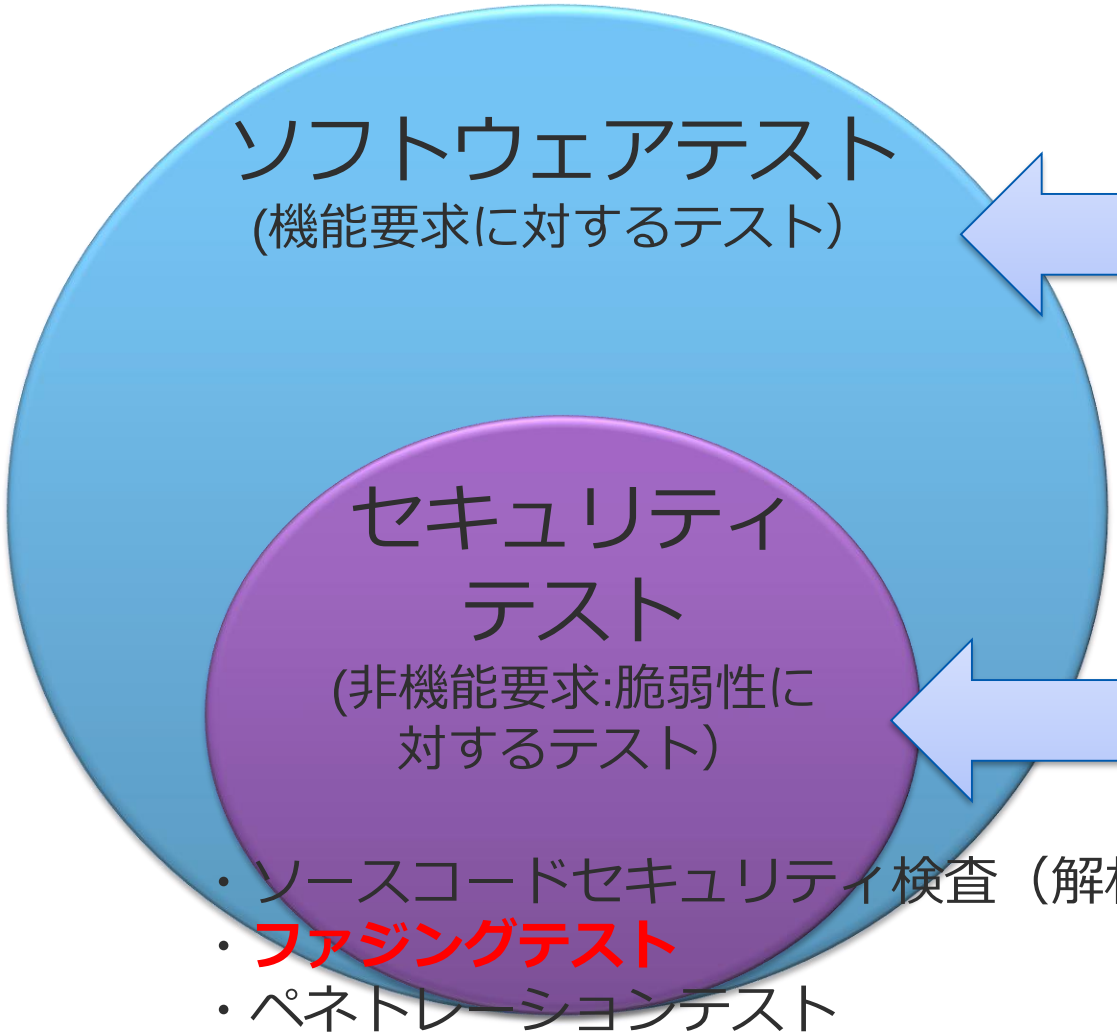
■ ハードウェアで実現　⇒　セキュリティアンカーかつ高速実行
■ SWの不正改ざん、マルウェアの混入防止
■ 起動部分のデータ漏えい防止



セキュアなプログラム実行環境によりセキュアなアプリを分離

*ルネサスDevCon2017資料から抜粋

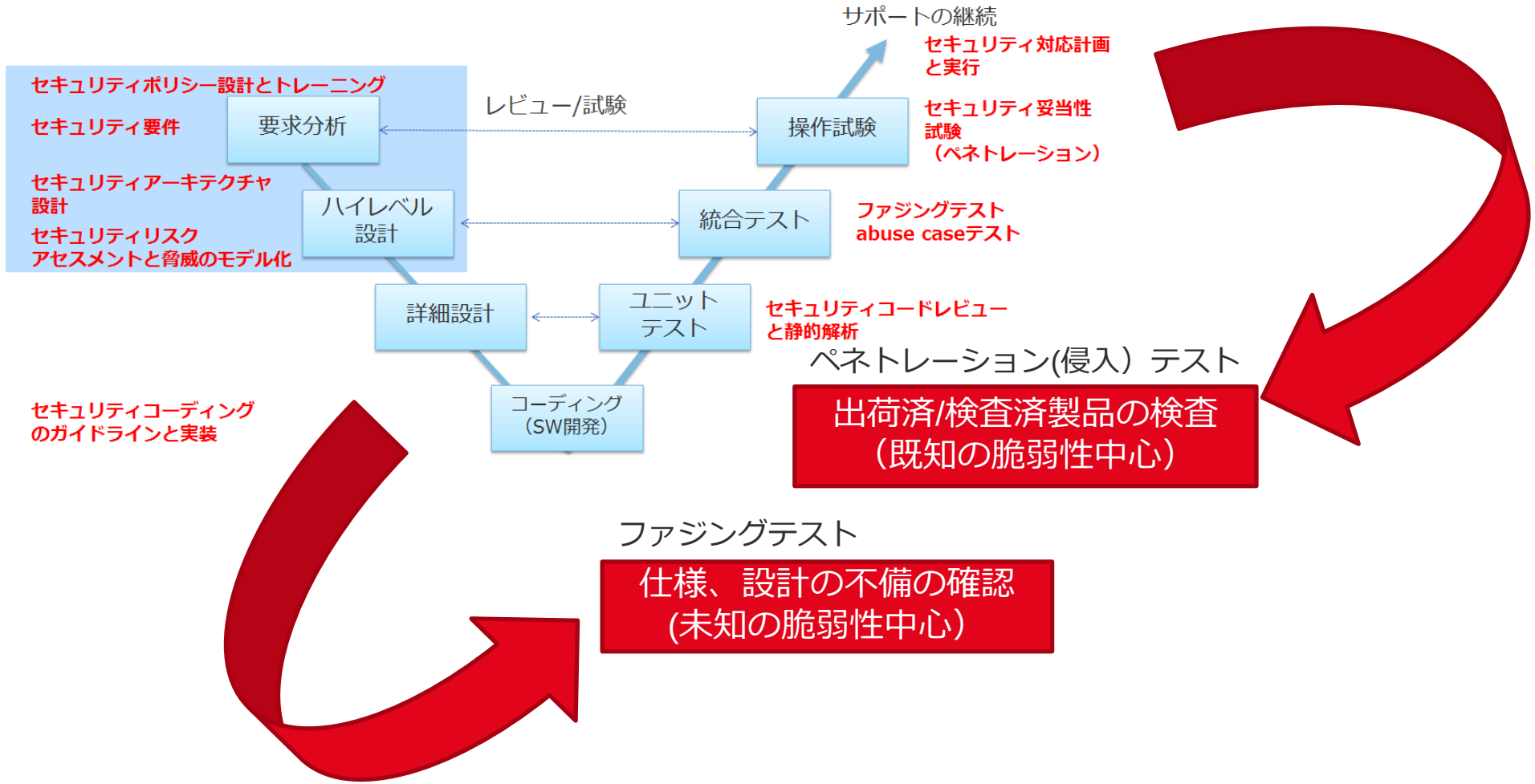
ソフトウェア品質とセキュリティテスト



製品に対する機能、性能、処理能力を満たしているか？

脆弱性による機能の不具合、停止,
暴走などが発生しないか？

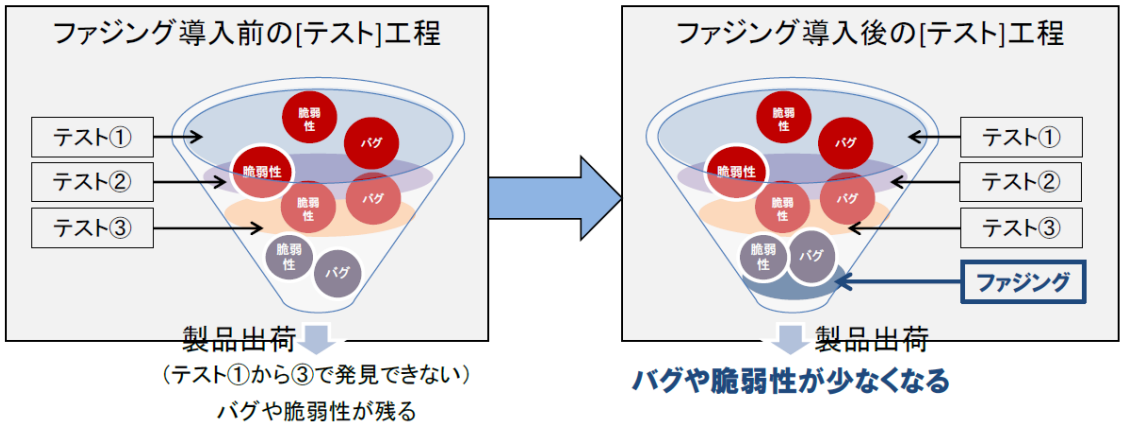
ホワイトボックス / ブラックボックスアプローチ



ファジングによるリスク低減

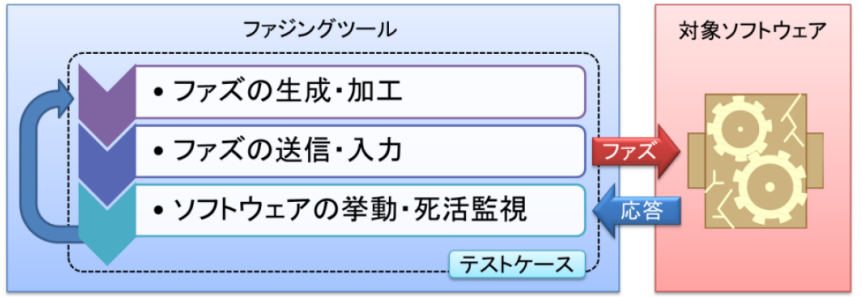
- 検査対象のソフトウェア製品、通信プロトコルなどに、機能に問題を引き起こしそうな無作為のデータ、ファイルなどを大量に送付し、その応答や挙動を監視することでソフトウェアの脆弱性を検出する手法、異常動作や終了、再起動、無応答などが発生した場合は、問題があると判断
- ファズ（プロトコルヘッダーや、ボディへの不正文字列や制御コード、異常コードファイルなど）を大量送付し、異常動作を誘発させたり、既知の脆弱性を有無をテスト
- テスト工程前半での効果的な活用により、バグや脆弱性の補修コスト、期間の低減が期待
- ツールを活用することによりテストの自動化・効率化が期待できる
- 製品の内部構造を考慮せず、ブラックボックス検査が可能

ファジングの効果



ファジングの概念

ファジングツールの動作イメージ



セキュア開発ライフサイクルにおけるファジングの重要性

- SDL(Security Development Lifecycle)により開発プロセスにセキュリティとプライバシーの概念を取り入れソフトウェアの脆弱性発見とリスクを極小化するアプローチ
- ファジングはセキュリティ強度検証のフェーズで重要な手段

図 3: セキュリティ開発ライフサイクル (SDL) プロセスを定義するプラクティス

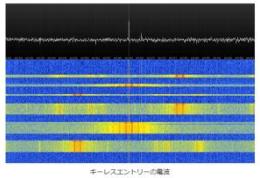
*出典：米Microsoft CorporationによるSDLレポート

脆弱性検証の実例

■車載関連の脆弱性検証の一例

- 診断用ポートから車載バスへのメッセージ送信
- カーナビのUSB, Bluetooth, 光学ディスクを経由した車載機器への攻撃試行
- イモビライザーの突破試行
- GPSからの位置偽装
- ECU間の認証機構の突破試行
- ECUのdiag機能を悪用した設定フラッシュ読み出し・解析・書き換え
- 秘密情報(ECU間の認証用秘密鍵等)の読み出し・改ざん試行
- カーナビのシリアルやJTAGからのフラッシュ読み出し・解析・書き換え
- 公衆網からのTCUへの攻撃
- ECUのシリアルやJTAGからのフラッシュ読み出し・解析・書き換え

ペネトレーションテストの進め方



テスト準備

- インテリジェンスギャザリング(機能調査)
- シナリオドラフト作成
- テスト計画・項目作成
- テストツールの決定、調達、セットアップ

テスト実施

- 対象車両、部品のファームウェア解析
- マルウェア準備
- テスト実行

テスト結果検証

- テスト結果の評価(リスク係数の評価)
- 報告書作成
- 報告会

ペネトレーションテストの攻撃シナリオ設定例

1.攻撃対象として**ADAS及びIVI**にフォーカス
2.攻撃者として**特定組織に属さない悪意を持った第三者**＊1を想定
3.攻撃のゴールを「**ドライバーの健全な運転を脅かす**＊2」ことに設定
4.手段として以下２つを選定

①サービス停止
［説明］ ドライバーが意図したタイミングで必要なサービスが機能**しない**状態をつくる
［手段］ DoS攻撃、マルウェア（ランサム）、不正なCANパケット

②不正な挙動
［説明］ ・偽メッセージ等でドライバーの誤判断を誘発する ・ドライバーが意図しないタイミングで意図しないサービスを機能させる
［手段］ 内部・外部からの不正なCANパケット

除外条件：
*1 今後のシナリオ拡張を想定し、1st stepである今回は攻撃に特殊なツールや回線を利用する可能性のある保険業者やディーラー等に限定しない。
　攻撃者の行動理念は「いたずら」「嫌がらせ」とする。
*2 健全な運転＝ドライバー自身が運転によって身体的、金銭的、精神的被害を受けない状態
　以下はスコープ外とする
　・営業妨害目的（情報窃取、車両追跡、等）
　・政治的目的（車両追跡、盗聴、等）
　・攻撃者の金銭目的（窃盗、等）

参考：リスク評価例

■自動車関連での車載関係のリスク評価手法として有効な評価手法を検討、
■例：重要生活機器連携セキュリティ協議会（CCDS）車載SWGでの評価例

脅威事例			リスク特性							リスク値の比較			
事例	想定脅威	想定被害	対象機器	分野固有・共通	脅威の分類	接続I/F（侵入ルート）	who 誰がつなげたか	whom 何が危害をうけたか	where どこで発生したか	ETSIの改良方式	CRSS（CVSSの応用）	RSMA方式	CCDS改良方式
1	外部ネットワーク経由で車載ネットワークにDoS攻撃。	通信機能を必要とする全サービスの利用停止	車載器	共通	DoS攻撃	3G/GSM	攻撃者	IoT機能	通常使用I/F	Critical（6）	レベルⅡ（警告）	H	Must
2	サーバなりすましによる虚偽メッセージの送信。	利用者の混乱など	車載器	共通	偽メッセージ	3G/GSM	ユーザー（誤接続）	IoT機能	通常使用I/F	Major（4）	レベルⅡ（警告）	M	High
3	ブラウザのバグを利用したストリーミングコンテンツによるシステムのフリーズ。	インフォテインメント系サービスの利用停止	車載器	共通	偽メッセージ	3G/GSM	ユーザー（意図的）	IoT機能	通常使用I/F	Major（4）	レベルⅡ（警告）	M	High
4	第三者による受信機を用いた通信メッセージの盗聴。	運用管理機関の意図しないサービスへの利用	車載器	共通	盗聴	Wi-Fi	攻撃者	情報	通常使用I/F	Minor（3）	レベルⅠ（注意）	L	Low
5	第三者によるGPS信号発生器の悪用による、誤った位置を含むメッセージの配信。	誤った位置を含むメッセージ配信による混乱の発生	車載器	共通	不正中継	GPS	攻撃者	本来機能	通常使用I/F	Major（4）	レベルⅡ（警告）	H	Middle
6	利用者による車載器の悪用や第三者による通信機の利用により他の車載器へのなりすまし。	誤った情報を含む走行情報配信による混乱	車載器	共通	不正利用	3G/GSM	ユーザー（意図的）	情報	通常使用I/F	Major（4）	レベルⅡ（警告）	M	Middle
7	第三者による受信機の利用、利用者による車載器の悪用によって、受信メッセージから個人位置のトレース。	個人のプロファイリング	車載器	分野固有	情報漏えい	Wi-Fi	攻撃者	情報	通常使用I/F	Minor（3）	レベルⅠ（注意）	L	Low
8	3G/LTE回線から第三者が定常運用時に故意に制御ECUの制御機能を停止させる。	ECUが正常に動作出来なくなり車両機能が動作しない	ECU	分野固有	不正利用	3G/GSM	攻撃者	本来機能	通常使用I/F	Critical（6）	レベルⅢ（危険）	H	Must
9	スマートフォンなどのBluetooth機器からディーラ職員がメンテナンス時に車両状態情報を改ざんする。	設定が不正に変更されて意図しない性能変更がされる	車載器	分野固有	不正設定	Bluetooth	サービス事業者	情報	通常使用I/F	Major（4）	レベルⅡ（警告）	M	High
10	SDカードインターフェースから第三者が定常運用時に故意にインフォメーションECUのインフォメーション機能の誤動作を誘発する。	インフォメーション機能が正常に動作しなくなる	ECU	分野固有	不正利用	SD	攻撃者	本来機能	通常使用I/F	Minor（3）	レベルⅠ（注意）	L	Middle

1）ETSIの改良方式
ETSI（European Telecommunications Standard Institute、欧州電気通信標準化協会）のリス ク評価は、「発生可能性」と「影響」に分け、それぞれ3段階で評価した値の積で、リスク値のク ラス分けを行う手法

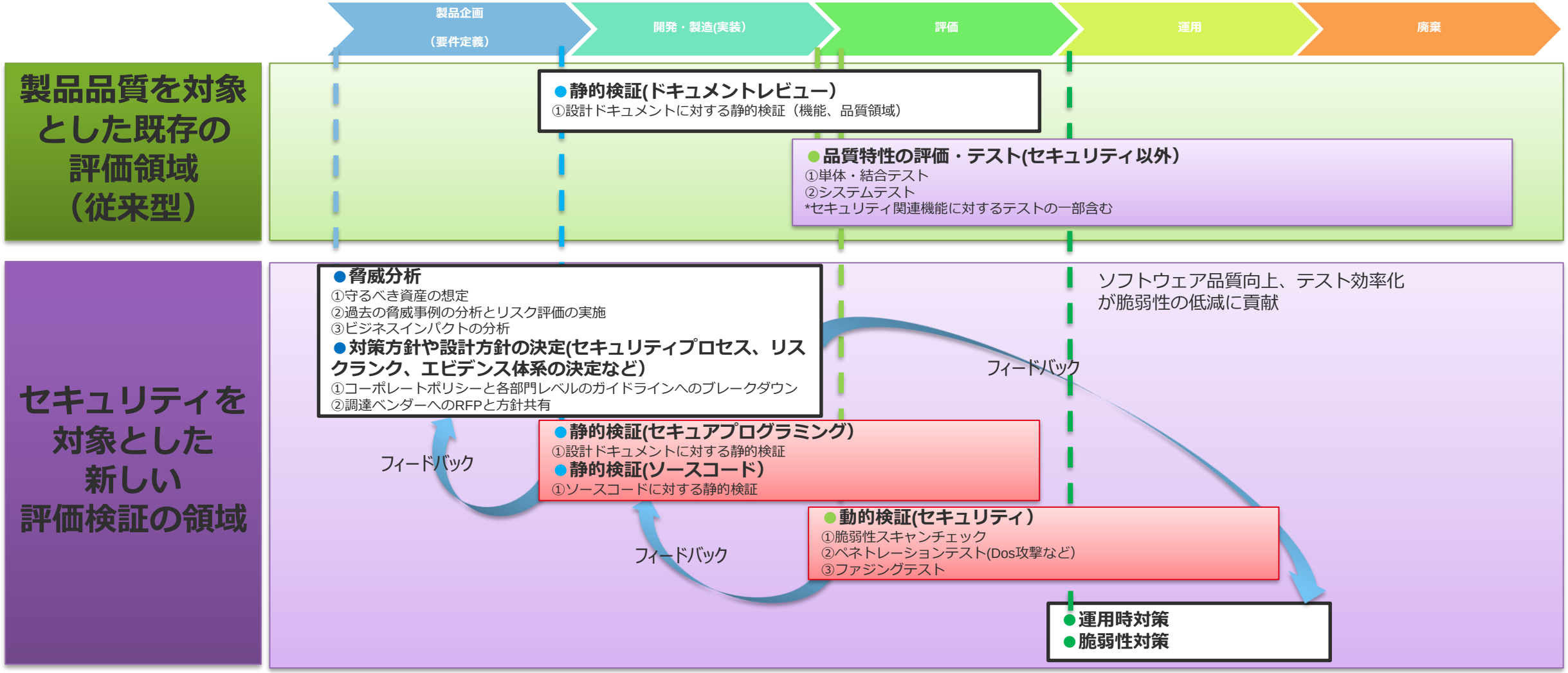
2）CRSS方式（CVSSの応用方式）
CRSS (CVSS based Risk Scoring System)は、情報システム・装置に対する脆弱性評価で実績の あるリスク評価手法である共通脆弱性評価システムCVSS（Common Vulnerability Scoring System) を応用したリスク評価手法である。 脅威事例のリスク評価を行うにあたり、自動車関係の参考文献から車載関係のリスク評価手法とし てどのようなものがあるのかを調査

3）RSMA方式
RSMA（Risk Scoring Methodology for Automotive system）方式では「リスク値」を「影響度」と 「発生可能性」のリスクレベル判定表によって決定する方式である。「影響度」は“セーフティ”、 “個人情報／プライバシ”、“財産／企業価値”の3種類の被害分類に分けた上でレベルを決定する。

4）CCDS改良方式
CCDSでは、「リスク値」を攻撃の「難易度」とユーザへの「影響度」についてランク付けして 判定する方式を用いている。評価項目については、「共通脆弱性評価システムCVSS概説」の情報 を参考とし、初動段階において早期評価および開発を行う事を目的として、基本軸を「難易度」と「影響度」としている

*出典：CCDS(重要生活機器連携セキュリティ協議会）：国内外230件の発表文献から脅威事例を収集しリスク評価

開発サイクルにおけるセキュリティ対策



参考：フェーズ毎の取り組み例

セキュリティの全社基本方針の策定
①経営層への理解と教育
②脅威の変化に応じた基本方針の策定、アップデート
③対応レベルの指針の検討と決定
体制
①統括責任者と部門責任者の決定
②取り組みの継続的運用のサイクル化
③インシデントレスポンスセンターの設置（単なる製品不具合とは別）
④インシデントの報告体制、共有体制の構築（DB化とナレッジ化）
⑤セキュリティ専門家、資格化
教育
①基本方針の定期メンテナンスと従業員への定期教育
②実務レベルに応じた情報セキュリティ教育
③倫理教育、重要情報の取扱者の極小化、誓約書,NDAなどでの信頼関係の醸成

企画

製品のコンセプト、予算、要件定義の策定など

評価対象モデルの構築
①対応システムモデルの記述
②想定接続先・接続口の定義
③隠れているI/Fの網羅
④網羅的な脅威候補の列挙

脅威分析の実施
①複数の評価手法での脅威分析の実施
②攻撃者のモチベーションや過去事例の有無をリスク評価に反映
③対策案の検討と仮説決定後、再度脅威分析を実施し、対策の効果を検証
④インシデントによる企業リスクの評価実施
⑤守るべき資産の明確化と、脅威分析の再実施

対策の検討
①対策案の列挙
②対策が破られる前提で検討
③鍵、証明書管理の手法、責任の所在
④進入経路としてサーバー側への出口も検討（踏み台の可能性）
⑤接続機器やアプリソフトの正当性の確認（なりすましによるリスク）
⑥非正規のI/F経由によるリスク対策
⑦リスク重要度、優先順位、対策コスト、機能仕様への影響などを考慮して設計に落とし込む
⑧OEM側より全体システムとセキュリティの実装レベルのガイドライン化し、サプライヤの役割分担に見合う条件設定の上、もれのない役割設定を行うことが重要
⑨各レイヤ毎のリスクと対策案の列挙
⑩コストや仕様の制限で十分な対策が実施できない場合、システム全体や上位コンポーネントとの連携での対策も検討

開発

企画フェーズの要件定義を受けて、設計、実装/テスト、製造の実施

エビデンス
①脅威に対するリスク分析と対策の検討結果、その有効性や選択した理由をドキュメントに記録
②インシデント発生時のトレーサビリティの確保

評価・検証
①ファジングツールなどを使用したテスト実施
②自己評価時の第三者チェック
③第三者によるリスク評価およびセキュリティ検証の実施

未知の脅威に対する対応
①ペネトレーションテストの定期実施
②進入検知や異常挙動の監視機能の実行
③ログの蓄積と解析
④定期的なセキュリティ評価・検証とガイドラインの更新

運用

ディーラーから所有者（利用者）に販売、利用者が使用している期間にインシデントへの対応、整備、サービスを実施

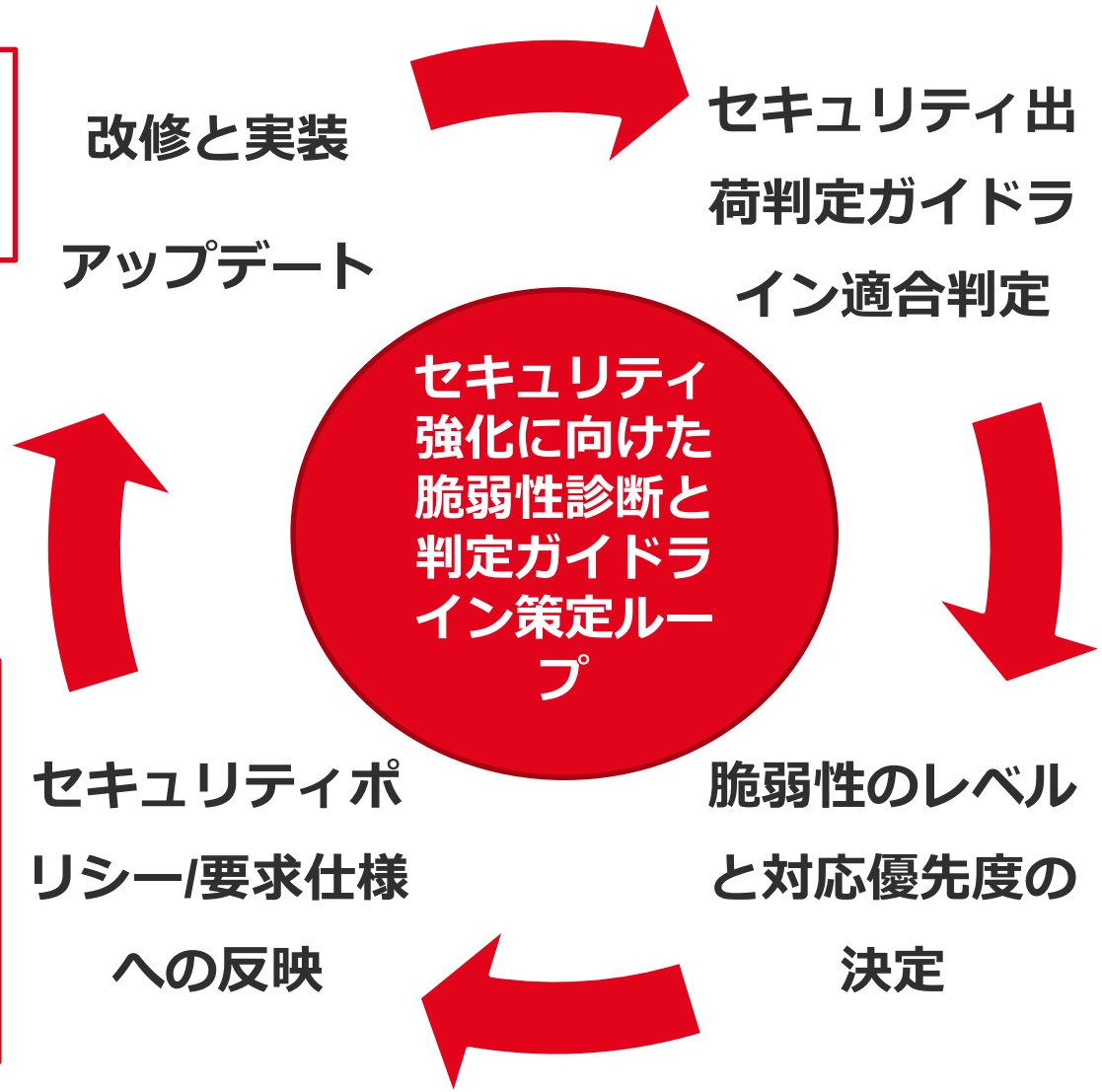
取扱説明書
①免責事項などの明記
②販売時にセキュリティ対応に考慮した製品になっていることを表示
運用時の利用定義
①使用範囲や制限、前提条件などを運用社に通知
利用者への注意喚起
①意図しない機器の接続や機器の予期しない挙動時に注意を喚起する表示、仕組みを提供
②設定ミスのまま利用されないブロック機能などの実装(デフォルトセキュリティの状態などでの不備防止)
アップデート
①セキュアにフォームウェアをアップデートできる仕組みの構築（信頼できるサーバーからセキュアブートの鍵付きでDLして改竄チェックできる仕組み）
②OTAなどリモートアップデート機能
運用関係者
①保守マニュアルの流出などの対策
②運用スタッフの内部悪用などの対策
③関係者のレベルに応じた情報共有、システム運用レベルの設定
インシデント情報の共有
①インシデント情報を社内関係者、事業者で共有する仕組み作り
②業界横断のインシデント共有（Auto ISAC)

廃棄

所有者が中古車として売却または廃車手続きを行う

難解析化
①廃棄された自動車、基盤を解析されても解析が困難な仕組みの実装
初期リセット
①初期状態にリセットできる機能の実装
②証明書ベースでの運用による無効化

サイバーセキュリティ脅威への対応ループ



- 守るべき資産、評価するシステムモデルの想定
- ペネトレーション/ファジングテストによる脆弱性解析とリスク評価
- セキュリティ出荷判定ガイドラインの作成
- PDCAで常時ガイドラインをアップデート

- 優先度別に各種ツールによる脆弱性箇所の特定と影響度のとりまとめ
- 対応レベル案とレポーティング

- 優先度に応じてセキュリティポリシーの策定、改定
- 要求仕様/設計/実装仕様案の策定

- 脆弱性箇所の改修
- 要求仕様/設計仕様に応じたテストシナリオ策定

会社概要

- 会社名　株式会社ユビキタスAIコーポレーション（UAC）
- 所在地　＜本社＞　〒160-0023 東京都新宿区西新宿 1-21-1 明宝ビル６Ｆ
  ＜事業所＞五反田　＜営業所＞大阪、名古屋
- 沿革
  - 2001年　5月　元マイクロソフトのエンジニアを中心に株式会社ユビキタスを創業、組込みソフトウェア事業開始
  - 2005年　大手ゲームメーカーに組込みネットワーク製品が採用
  - 2007年　11月　JASDAQ NEO市場に上場　（現在はJASDAQ上場）
  - 2010年　3月　Ubiquitous QuickBootを発売開始
  - 2012年　12月　株式会社村田製作所と資本・業務提携締結
  - 2016年　4月　株式会社エイムを子会社化
  - 2017年　4月　株式会社エーアイコーポレーションを子会社化
  - 2018年　7月　株式会社エーアイコーポレーションを吸収合併
    商号を株式会社ユビキタスAIコーポレーションに変更
- 資本金　14億7,098万円（2018年3月31日現在）
- 代表取締役社長　長谷川 聡
- 事業内容　組込み機器関連ソフトウェア開発・輸入・販売
- URL　https://www.ubiquitous-ai.com/
- グループ企業　株式会社エイム　http://www.aim-inc.co.jp

Connecting the Future

Ubiquitous AI Corporation

会社概要

多種多彩なソフトウェア製品と技術開発力により
お客様の開発を協力にサポートいたします

Connecting the Future

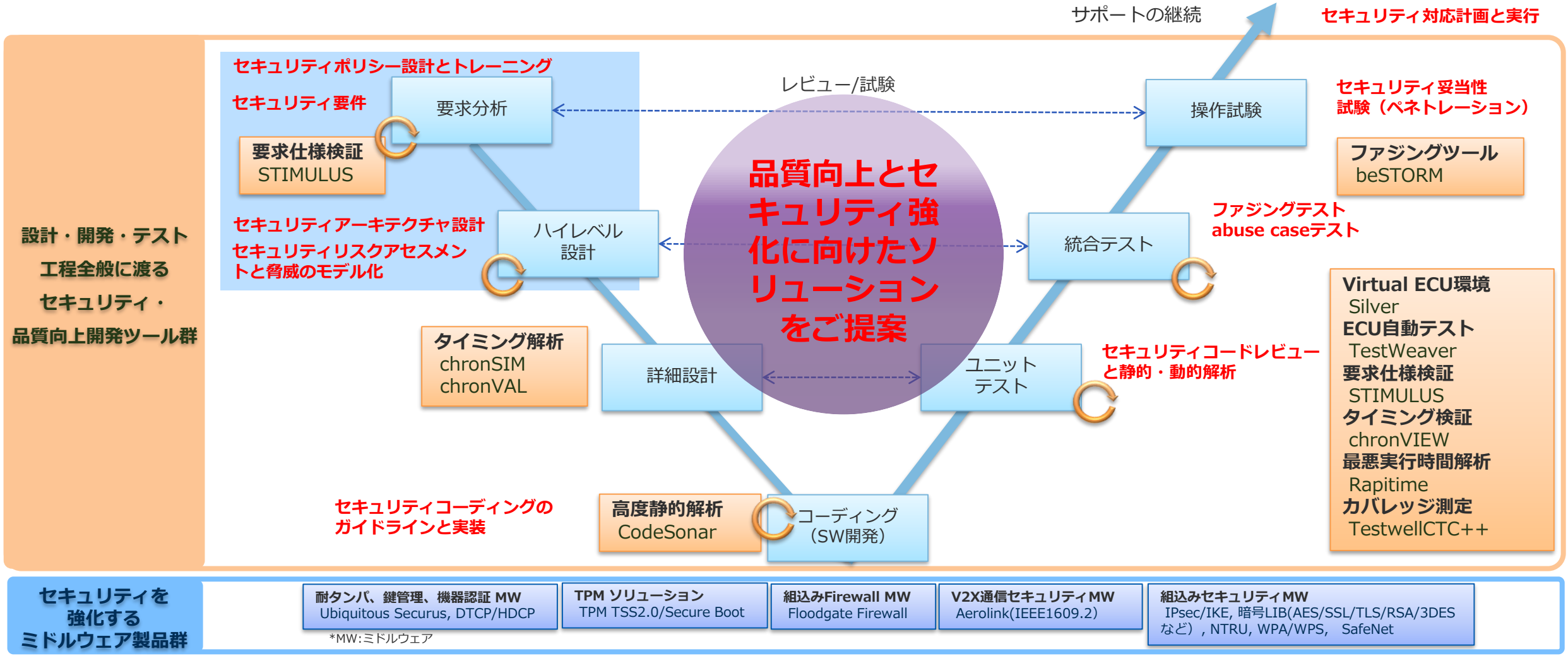
Ubiquitous AI Corporation

テクノロジーを通じて
「お客様」、「社会」、「社員」の、みらいをつなぐ

- セキュリティ
- 品質向上支援ツール
- 車載機器開発・テストツール
- 脆弱性・セキュリティ検証
- ネットワーク
- コネクティビティ
- ワイヤレス
- OS/BIOS
- ストレージ/データマネージメント
- キャリアグレード
- 音声・動画・UIソリューション
- 開発ツール/ユーティリティ

ユビキタス AIコーポレーション **セキュリティ/品質向上支援ツール群**

■ コネクティッドカーのセキュアかつ高品質な開発プロセスを支援



セキュリティを強化するミドルウェア製品群

耐タンパ、鍵管理、機器認証 MW	TPM ソリューション	組込みFirewall MW	V2X通信セキュリティMW	組込みセキュリティMW
Ubiquitous Securus, DTCP/HDCP	TPM TSS2.0/Secure Boot	Floodgate Firewall	Aerolink(IEEE1609.2)	IPsec/IKE, 暗号LIB(AES/SSL/TLS/RSA/3DESなど）, NTRU, WPA/WPS, SafeNet

*MW:ミドルウェア

UACグループの車載分野向けの取り組み

インフォテインメント/情報系ソフトウェア開発

コネクティビティ
- Ubiquitous Wi-Fi SDK
- Bluetooth SDK(BlueSDK)
- ASIL-B対応TCP-IPスタック
- UBSスタック
- NFC Stack / FeliCa

OTAアップデート
- OMA-DM, LWM2M クライアント

スマフォミラーリング
- Ubiquitous Miracast SDK
- Mirroring SDK

高速起動
- Ubiquitous QuickBoot

ストレージ
- Ubiquitous DeviceSQL
- 電断対応ファイルシステム（Reliance Nitro/FlashFX)
- SD/SDIOドライバー

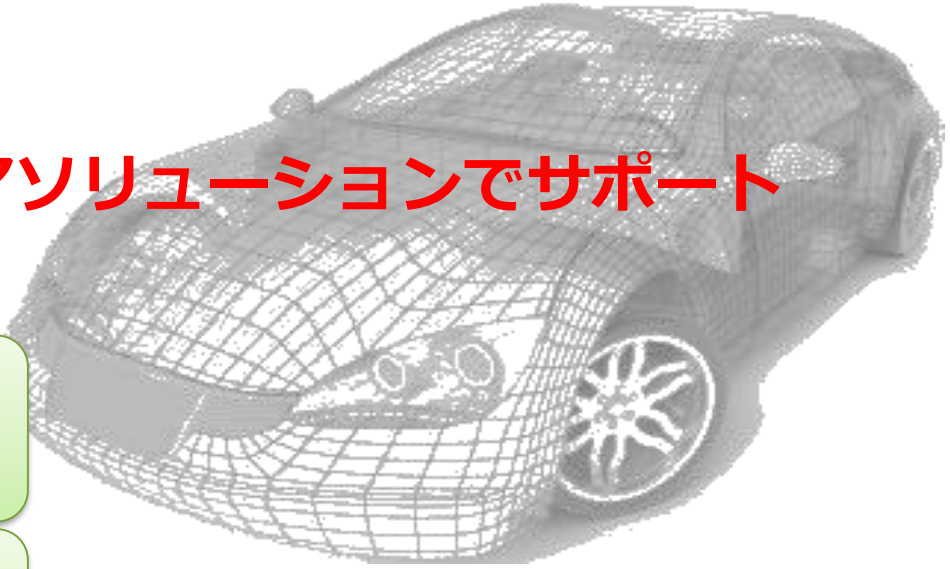
仮想化/ブートローダー
- SafeG / µLoad

ドライバモニタリング
- CoDriver

インフォテインメント
- Gracenote CDDBポーティングサービス
- YOMIデータコンテンツライセンス

セキュリティ/暗号ライブラリー
- Ubiquitous Securus
- Ubiquitous DTCP / HDCP
- Ubiquitous TPM Security
- Embedded Firewall
- Crypto and Codec Libraries

コネクティッドカーへの進化を幅広いソフトウェアソリューションでサポート



ECU/制御系ソフトウェア開発

品質向上支援ツール
- 要求仕様検証（STIMULUS)
- ランタイムエラー静的検出ツール（CodeSonar)
- マルチECUタイミング解析（INCHRON TS)
- カバレッジ測定（TestWell CTC++)
- Virtural ECU(Silver)
- ECUテストシナリオ自動生成ツール（TestWeaver)
- 脆弱性・セキュリティ検証フレームワーク(beSTORM)

車載ネットワーク
- ASIL-B対応TCP-IP
- 暗号ライブラリ
- IPSec

V2X通信ソフト
- IEEE1609.2通信スタック（Aerolink)
- IEEE1609.2通信テストツール

まとめ

- 自動運転、CASE実現には、ハードウェアとソフトウェア開発の両輪
  - SPACE : セキュリティ、プラットフォーム、自動運転制御、コネクティビティ、電子化がキーテクノロジー
- ソフトウェア、サービス開発が益々重要に
- 自動車の安全、品質の確保に向けたソフトウェア開発プロセスの進化：モデルベース開発、シミュレーション、セキュア開発、自動テスト、脆弱性検証などのツール活用によりフロントローディング、シミュレーション、テスト自動化を駆使した開発モデルが必須
- 複合システム（車体、通信インフラ、クラウドサービス）である次世代自動車はプラットフォーム横断でセキュリティ対応プロセスの確保が最重要
  - 開発プロセスに機能品質とセキュリティ品質の両方が必要
  - バリューチェイン、ライフサイクルを横断、一貫したセキュリティポリシーと対策が重要

おまけ：これからの自動車産業

- 中国の自動車産業
- インターネットプラットフォーマーの動き
- オーナーカーとサービスカー
- トヨタのMaaS戦略

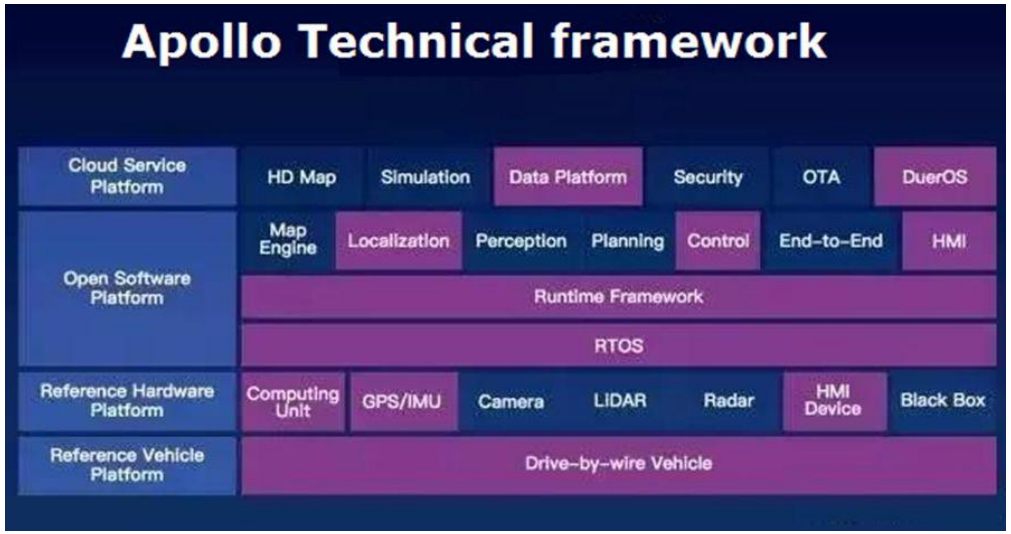
中国の自動車産業の中長期発展計画

- 2020年までに世界に通用する「中国ブランド」の確立
  - 10年後には世界の自動車「強国」へ　:世界のトップ10に入る自動車メーカー、電池・センサー・電気制御システムなどの部品メーカーを育成
  - NEV(新エネルギー車）・コネクティッドカー・省エネ車の強化
  - 自動車サービス産業の創出：R&D,製造、物流、販売、アフターサービスのサプライチェイン化
  - EV化推進：NEVポイントとバッテリー「ホワイトリスト」登録企業調達
  - BYD社,FMC社の新興EVメーカーの台頭
  - 吉利自動車(Geely Auto)の世界戦略:リンクアンドカンパニー コンパクトモジュラアーキテクチャの採用、CASEモデル、カーシェアリング企業の設立
- 「AI産業 X 自動車産業」政策
  - 次世代人工知能発展計画：2020年までにAIの産業化、16兆円市場へ
  - 各産業への応用で160兆円の市場形成
  - 次世代人工知能の解放・革新プラットフォーム、4つの重点テーマを民間に委託
    - 「都市計画」：アリババ
    - 「医療映像」：テンセント
    - 「音声認識」：アイフライテック
    - 「自動運転」：バイドゥ（百度）　–　自動運転プラットフォーム「アポロ計画」

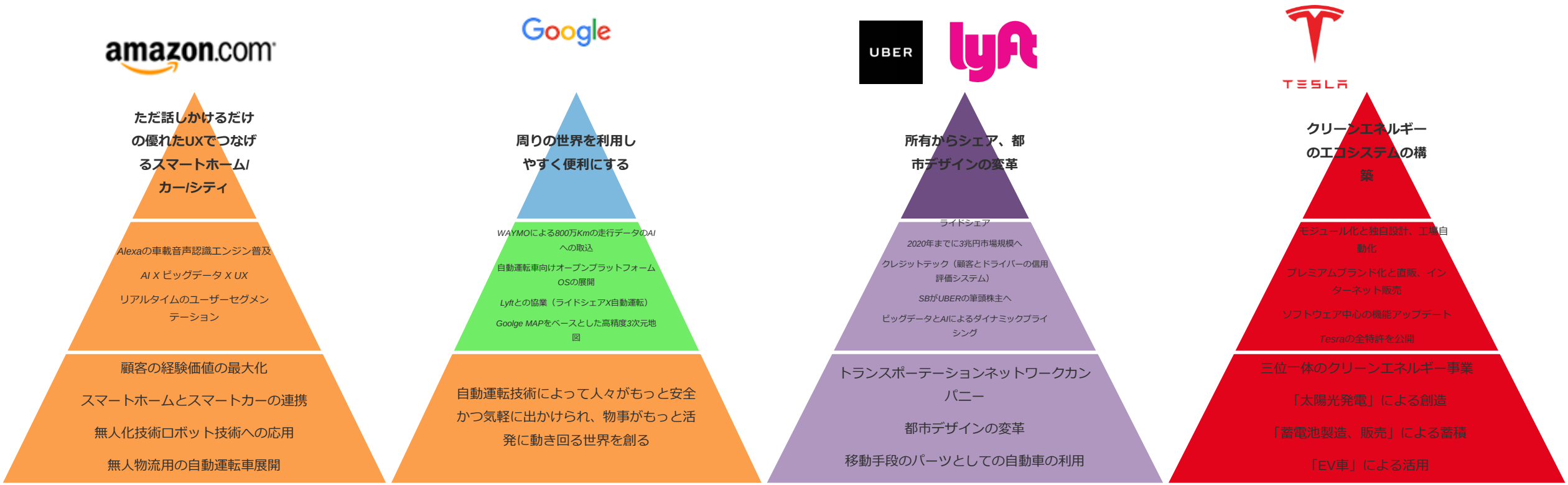
バイドゥの「アポロ計画」

- 2020年12月に完全自動運転の実現を目指して発表された計画
- バイドゥが持つAI技術、ビッグデータ、自動運転技術をパートナーにオープンにし、相互共有することにより短期間で独自の自動運転システムを構築することを可能にする
- 国際的なエコシステムの構築
- 自動運転プラットフォーム「アポロ」
- 「百度大脳：AI開放プラットフォーム」（音声認識/合成、文字認識、画像認識、顔認識、画像検索、言語処理、機械翻訳など）
- 「デュアーOS」(AIアシスタント用基本ソフト、認証、セキュリティその他UXフロントエンジンとしての基本機能網羅）
- 高精度3次元地図
- アポロコンピューティングユニット（ACU)アポロプラットフォームを統合した自動運転用ハードウェアユニットによる囲い込み
- アポロ計画参画の中国自動車OEM、第一汽車、東風汽車、長安汽車の戦略提携の将来的な影響（3社で1000万台）

自動車	米フォード、独ダイムラー、韓ヒュンダイ、日ホンダ
	第一汽車、北京汽車、長城汽車、東風汽車、奇瑞汽車、江淮汽車、長安汽車、金龍客車 BYD,CHJ, NIO, Weltmeister
自動車 部品	米デルファイ、独コンチネンタル、独ボッシュ、独ＺＦ
ＩＴ、通信	米エヌビディア、米インテル、米マイクロソフト、中興通訊、紫光展鋭、蘭NXP、日ルネサス、中ファーウェイ



次世代自動車産業を取り巻くテクノロジー企業のビジョンとCASE



Connected

Autonomous

Sharing & Services

Electric

CASEに向けた自動車産業の課題

- スマートライフも含めた一気通貫プラットフォームの主導権
- UXとAIプラットフォーム（音声認識、VR/AR、ジェスチャー、センシング）
- ビッグデータの蓄積量とスピード
- 5G NWの普及とセキュリティ・認証基盤

- 完全セルフドライビングカーの実現
- AI用半導体と膨大な走行データ、高精度3次元地図、高度なセンサー群
- 統合された車載ソフトウェアプラットフォーム
- 垂直統合から水平分業モデルへの転換（レイヤ構造）

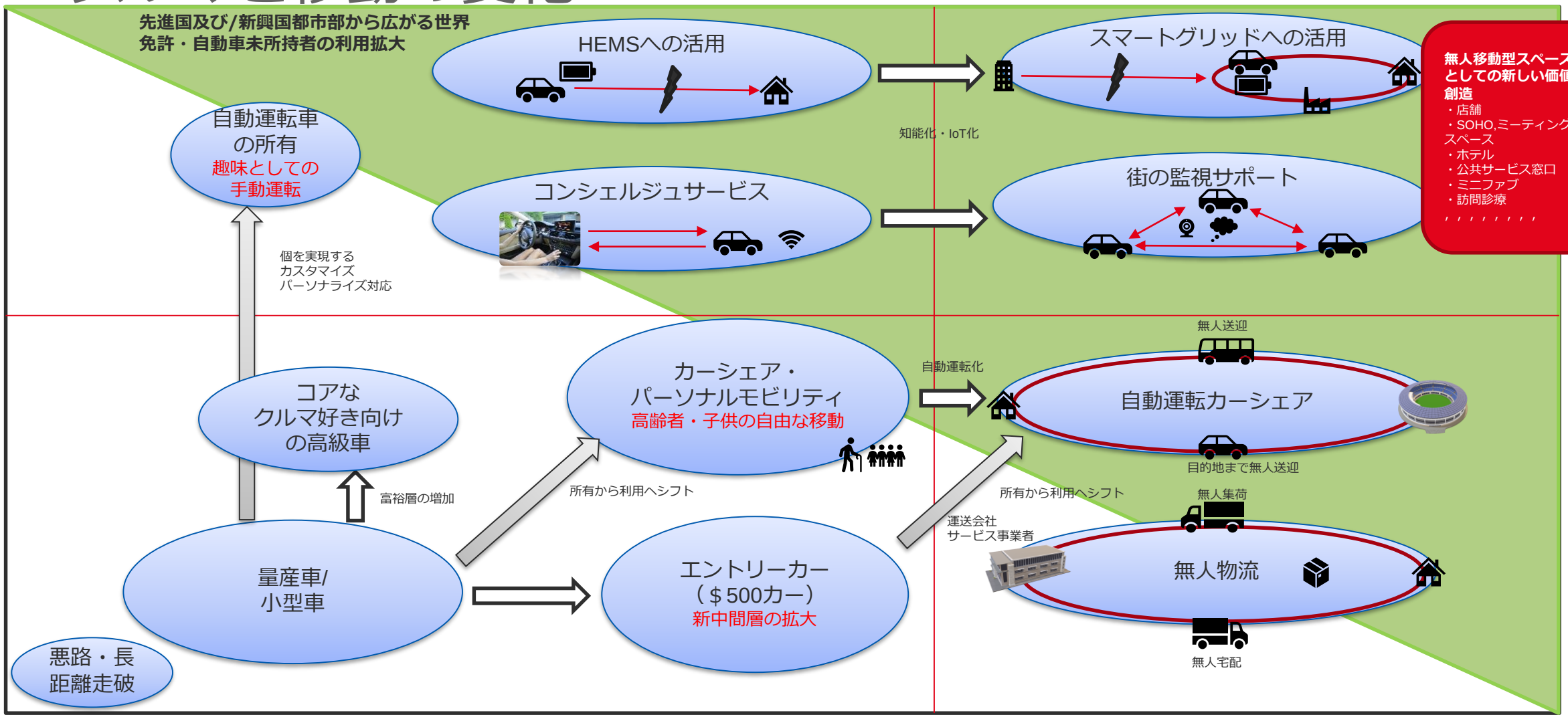
- シェアリングサービスビジネスモデル（サブスクリプションできる継続可能なビジネス）
- オーナーカーとサービスカーのすみ分け
- MaaS（ヒトを中心とした総合移動サービス）ビジネスモデルの創造

- 電池の量産コストの低減、収益化の確保
- 産業構造の再定義（水平分業によるレイヤ化 or 垂直統合によるプラットフォーマーか）
- 充電スポットのマイクログリッド化などによる停車時の用途の創造(シェア、蓄電、複合サービス利用など)
- ゼロエミッション、再生可能エネルギーの限界利益化

MaaSプロバイダーへの進化（都市移動基盤、サービス）

*参考出典:PHPビジネス新書「2022年の次世代自動車産業」、佐野加筆

2030年のモビリティ社会の世界観
～クルマと移動の変化～



*参考出典:日経ＢＰ社「モビリティ革命 2030」、佐野加筆

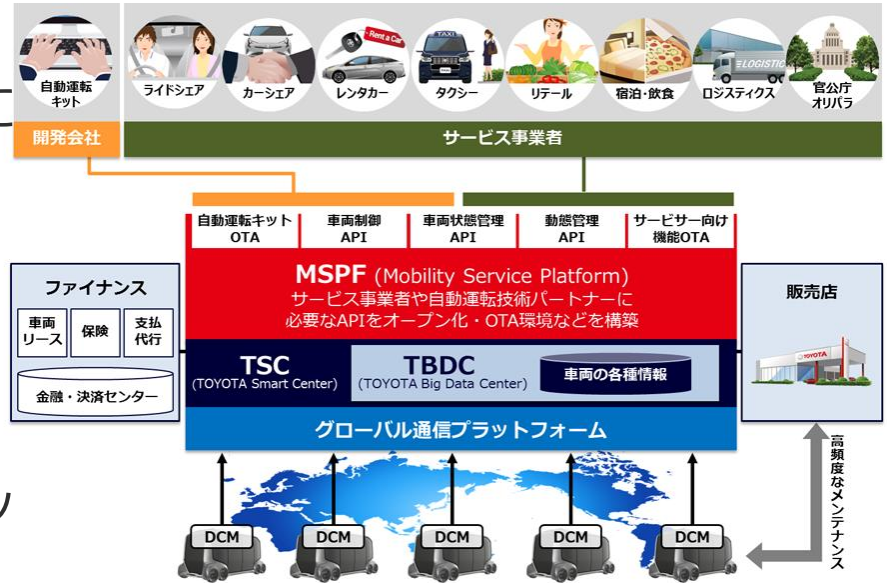
MaaSへの産業シフト

- シェアリングへの移行とマルチモーダルサービス産業へ
  - 自動車はユーザーの移動体験の中での一部の機能
  - サービスとの連携、サービス自体の提供が価値へ
- ユーザーの特定(誰が?、いつ?、どこに？、何のために？）、サービスを跨いだ認証がキー

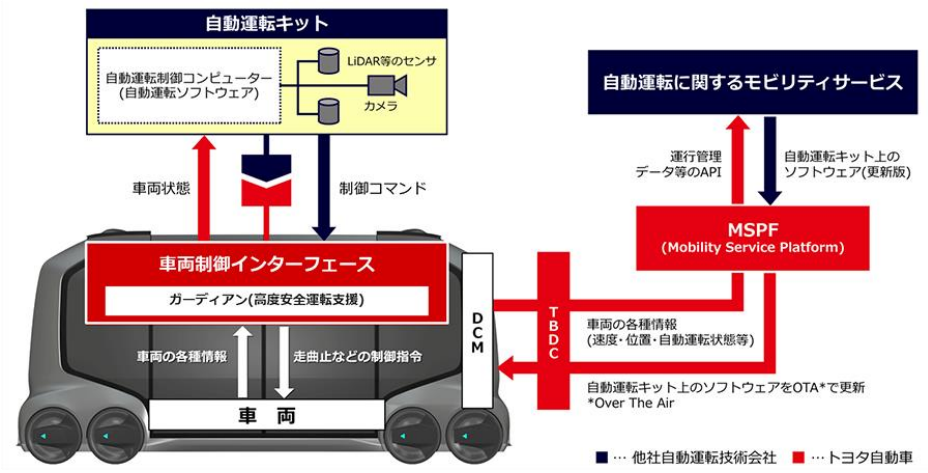
*日経テクノロジーオンライン記事から転載

トヨタ自動車のMobility Service Platform

- TOYOTA Mobility Server Platform(MSPF)
  - 車両情報をTBDC(TOYOTA Big Data Center)へ蓄積、APIによるデータ、API提供
  - 様々なサービス事業者との提携、モビリティサービスの創出に貢献



- ePallet用 車両制御インターフェースの公開
  - 車両状態や車両制御が可能なAPIをMSPF上で自動運転キット開発会社に公開
  - セキュアなOTAアップデートによる更新



- Monet Technologies
  - MaaS事業化に向けソフトバンクと合弁

TOYOTA connected

MONET TECHNOLOGIES INC.

Ubiquitous AI Corporation

*トヨタ自動車発表資料より転載

Connecting the Future

Ubiquitous AI Corporation

株式会社ユビキタスAIコーポレーション

本社　：新宿区西新宿1-21-1 明宝ビル 6F
五反田事業所　：品川区西五反田2-25-2 飯嶋ビル 2F&3F
大阪営業所　：大阪市淀川区西中島6-2-3 1205
名古屋営業所　：名古屋市中区栄5-19-31 T&Mビル 3F-F
五反田ウェストヒル事業所　：品川区西五反田2-24-4 WEST HILL 2F

sales@ubiquitous-ai.com　https://www.ubiquitous-ai.com