IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

CEATEC JAPAN
ソフトウェアマネジメント研究会

～自動車のネットワーク化の将来と課題～
つながる自動車のセキュリティ

2014年10月10日（金）

独立行政法人情報処理推進機構（IPA）
セキュリティセンター
情報セキュリティ技術ラボラトリー 主任
中野 学 （博士（情報学））

IPAの紹介

IPAとは
（Information-technology Promotion Agency, Japan）

未来を拓くIT人材を育てる

◇経済産業省所管の独立行政法人

◇IT産業の健全な発展を推進し、国民すべてに“頼れるIT社会”の実現を目指す

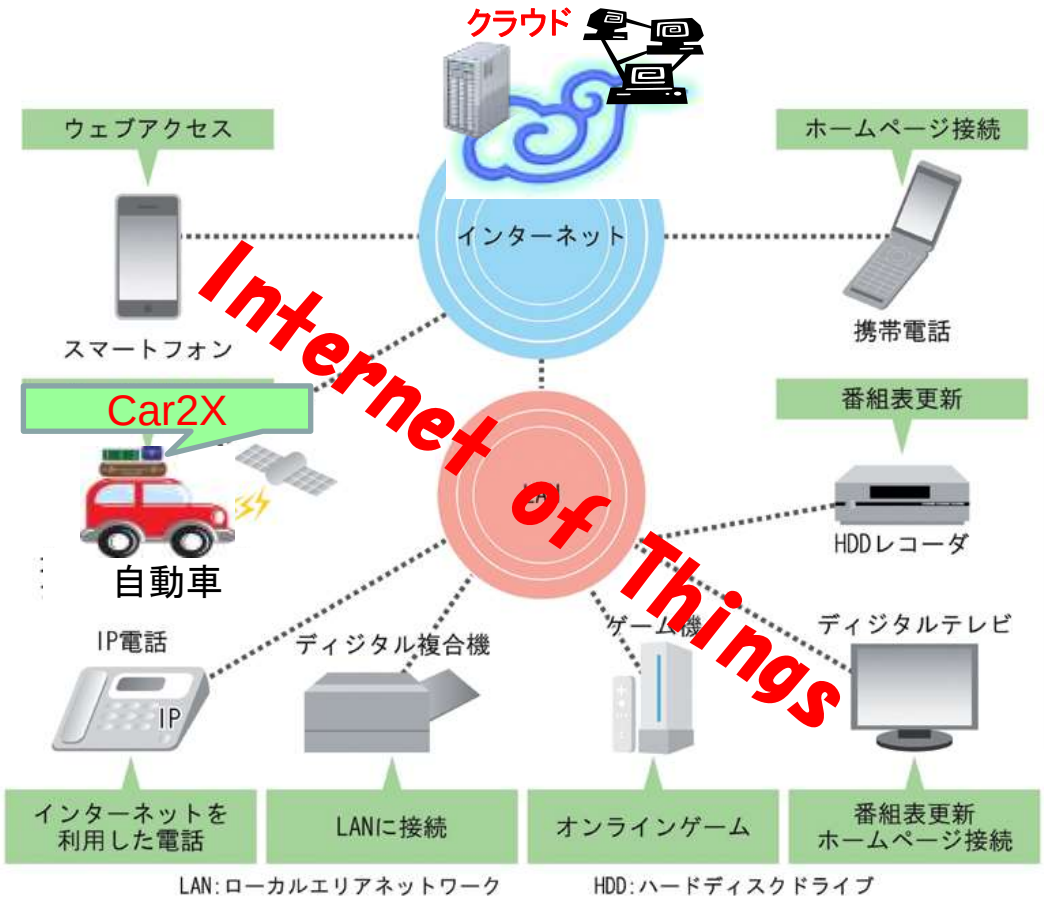
なぜIPAが組込みシステムセキュリティを？

- セキュリティセンター（とりわけ技術ラボ）のミッション
  - 脆弱性関連情報受付機関として
  - 近い将来脅威が発生しそうな社会の先行調査及び脅威分析
  - 組込み機器開発者とセキュリティ専門家の橋渡し

- 具体的な取組み
  - 組込みシステム全般のセキュリティ調査
    - 2006年から開始、毎年報告書を作成・Web公開
    - 調査を行う際には有識者による委員会を併催
    - 自動車に限らず、情報家電や携帯電話等のセキュリティ調査も
  - 組込み機器のセキュリティガイドの作成
  - 組込みセキュリティに関する講演を主とした普及啓発

社会的背景
～情報セキュリティの今・昔～

組込み機器の今昔
～繋がるモノ～



・これまでの組込みシステム

■スタンドアロンで動作

■機械的な制御

・これからの組込みシステム

■インターネットを含めた様々なネットワークと接続して動作。

■そしてクラウドへ。

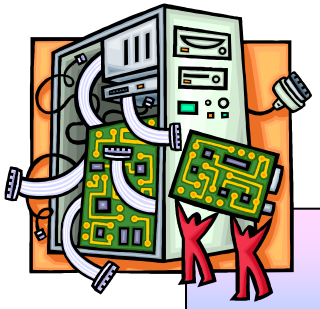
■ソフトウェア制御。

■個人情報や操作情報のような機微な情報を含めた様々な情報（ビッグデータ）を扱う。

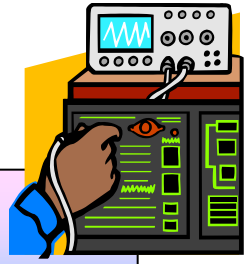
ビックデータの時代へ
～繋がってしまうモノ～

情報の中には、**複数のデータが組み合わさることで個人が特定される情報**や、**人によっては外に出したくない情報**など様々であり、ビックデータの中の情報をどれだけ守れば良いかと定義する事は難しい。利用用途やサービス目的を鑑みつつ、**情報を保護する手段や消去手段**を持つ事が望まれる。また、遠隔操作可能な機能を持つ事で、悪意ある者からの**脆弱性を狙った攻撃**や、**不正利用**が考えられる。**脆弱性を作りこまない開発**や、**攻撃を予防するセキュリティ対策**が必要。

組込みシステムのセキュリティ対策



ライフサイクル全体での対策が必要



限られた資源
↓
セキュリティ技術の軽量化

リバースエンジニアリング
↓
解析に強い耐タンパ技術

ライフサイクル

マネジメント

企画	開発	運用	廃棄

セキュリティガイドライン
↑
タイトなスケジュール

暗号化や認証の利用
↑
第三者からの攻撃

安全な廃棄プロセスの明示
↑
残存情報による情報漏えい

赤字：脅威
青字：対策

三つの進化と、それに伴うセキュリティ

新しいサービスの発達

新しい技術や機器の発展に伴って，様々な新しいサービスが創出される。これにより，組込み業界に様々なプレイヤーが係わり，多様な情報が扱われるようになる。

情報の価値や重要度に応じたセキュリティや情報の取扱いを利用者が理解・選択出来るような仕組みが必要となる。また，新しいサービスの出現伴って，それに適したセキュリティを検討する必要がある。

ネットワークへの接続

通信機能の搭載が容易・必須になりインターネットを含めた公共回線の利用が当然となる。これによって様々なモノが繋がる世界になる。

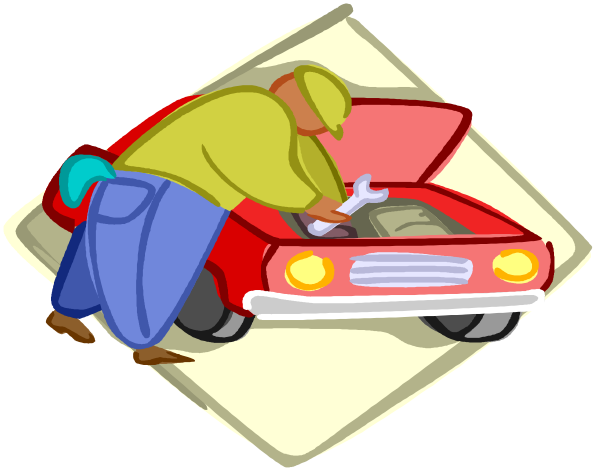
これまでネットワーク経由の攻撃が考慮されてこなかった製品群が，今後は攻撃の対象となるため，製品のセキュリティはもちろん，利用者の教育についても検討する必要がある。

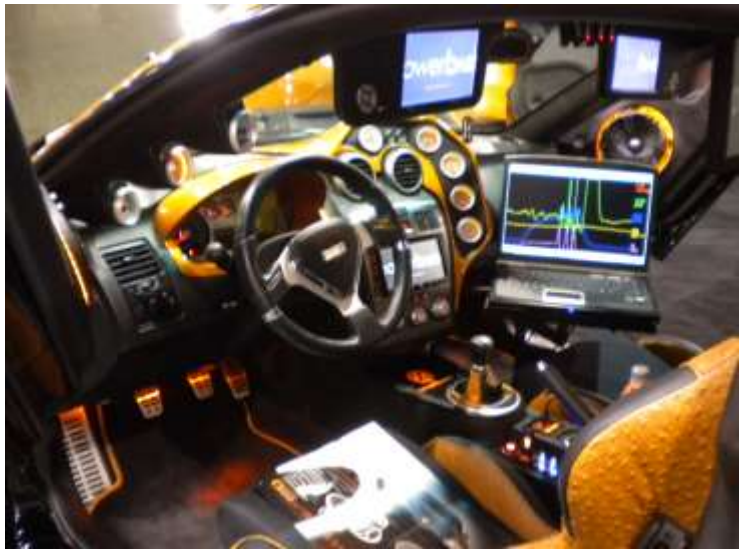
汎用プロトコル等の利用

多種多様な機器を接続するためや，機器のコスト競争等から，例えばTCP/IPなどの汎用プロトコルが利用されるようになる。

これまで利用されてきた独自プロトコルが標準化され，一般的なPCでも利用される汎用プロトコル等が利用されることで，PCと同様の脅威が発生する可能性がある。

自動車に見る情報セキュリティ





自動車の現状

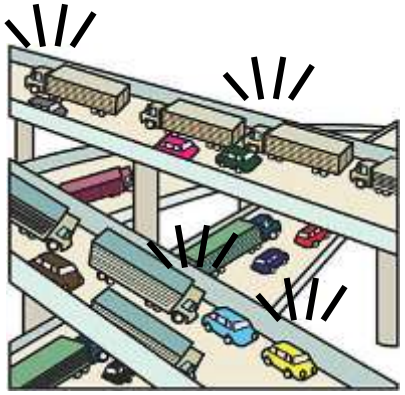
- 新しいサービスの発達
  - カーシェアリング・エコドライブ等の新しい自動車の利用形態
  - 車載ソフトウェアの増加等の、自動車の仕組み変化
  - 車載センサや外部情報を利用したサービスの増加
- ネットワークへの接続
  - 自動車とスマートフォンの連携
  - 路車間・車車間通信等、新しいネットワークも利用される
- 汎用プロトコル等の利用
  - 車内ネットワークへのTCP/IP適用
  - 車載システムに対する汎用OSの利用

自動車における脅威の特徴

- 直接的な攻撃にさらされやすい
  - ・駐車場等での第三者による不正な改造・攻撃
  - ・なりすましたメーカ点検員や利用者自身による不正な改造・攻撃
- 自動車の利用形態ゆえの脅威
  - ・レンタカーやカーシェアリング等における自動車共有による情報漏洩
  - ・移動先で何が繋がり、誰が利用しているか分からない
- 重大かつ広範囲の被害が発生する可能性も
  - ・身体や生命への重大な被害
  - ・社会的混乱を招く可能性

ECUを不正書き換え、
不正なECUを追加

身体への被害
の可能性も



偽の情報で日本中が大渋滞
（「地震が来る」等のデマなど）

自動車の情報セキュリティに関する事例紹介

自動車の情報セキュリティに関連する事例(1/3)
研究としての取組み

【CAN(Controller Area Network):主要な車載LAN方式の一つ】

・2010年ワシントン大学Kohno氏論文「Experimental Security Analysis of a Modern Automobile」にて

CAN本体について;

(1) CAN通信は同一バス上に同報する方式で、**盗聴、解析が容易**

(2) 認証フィールドとは発信元(ソースアドレス)がなく、**なりすましが容易**　など

CANを利用した車載LAN上機器の処理の不足や標準的な処理の不備などについて;

(3) **走行中には無視しなければならないはず**のCANバス全体の通信停止メッセージが、実際には有効

(4) **走行中のECUの書換えは禁止されているはず**であるが、実際には書換えモードに入ることが可能

(5) OBD-IIに接続した実験用のPCから上記のテレマティクス端末のソフトウェアを**認証手順なしで書換え**

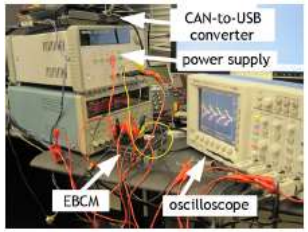


Figure 1. Example bench setup within our lab. The Electronic Brake Control Module (ECBM) is hooked up to a power supply, a CAN-to-USB converter, and an oscilloscope.

Figure 3. To test ECU behavior in a controlled environment, we immobilized the car on jack stands while mounting attacks.

Figure 7. Road testing on a closed course (a de-commissioned airport runway). The experimented-on car, with our driver wearing a helmet, is in the background; the chase car is in the foreground. Photo courtesy of Mike Haslip.

現在は、攻撃を行うための機材とソフトウェアは市販製品では機能不足のため開発が必要で、攻撃の難易度は高い。

ECU単体の解析(左)、静止時の車台上でのECU間解析と試験(中)、走行中の動作試験(右)

自動車の情報セキュリティに関連する事例（２/３）
解析と模倣

【CAN（Controller Area Network）：OBD-IIや直接接続による攻撃事例】

・2013年IOActive社Chris Valasek氏がBlackHatで発表した「Adventures in Automotive Networks and Control Units」にて

(1) OBD-IIへの接続や、CANバスへの直接接続を利用して攻撃

(2) リバースエンジニアリングを利用して通信の解析を行い、インジェクションを利用して命令を注入
　→結果として、ハンドル・アクセルの操作や、ブレーキの無効化が可能に

(3) 今回の攻撃デモでは、クルマの内装とPCをケーブルで直接接続して実施。遠隔操作では無い。
　→自動車に対する攻撃の検討はこれから。サービスの発展に従って攻撃も多様化。

(4) 攻撃手法、攻撃用のコード等は報告書で公開。今回は直接接続が必要で難易度も高いが。
　→攻撃手法は共有されやすい。一方で、セキュリティ対策普及は難しい。

自動車の情報セキュリティに関連する事例（3/3）
ツールの利用

【整備ツール：自動車整備用に製造された市販されていないツール】

- イモビライザーの鍵を消去できる部品の流通
  - 2010年11月、自動車の盗難防止装置である**イモビライザーを解除する器具「イモビカッター」を悪用**し、特定車種の窃盗を繰り返した容疑者グループが逮捕された。
  - ディーラ整備工場には、自動車の電子キーを消去または上書きして新しい電子キーを再登録できる**整備ツールが配備**。
  - 本ツールから電子キーを再登録する機能を抜き出し、OBD-IIに装着するだけで動作する部品を海外で製造

自動車の情報セキュリティに関連する事例（番外編）

信号機に対するハッキング

- 発生した国
  ◇米国
- 業種
  ◇道路管理
- 原因
  ◇システムが脆弱な状態
- 想定被害
  ◇道路状況の混乱

写真：The Telegraph
http://www.telegraph.co.uk/

2009年1月、米国の複数の州における信号機（交通メッセージ表示）が「ゾンビ注意（ZOMBIES AHEAD）」に変更された。この例はいたずらだが、原因はシステムにおけるパスワードをデフォルトのままにしていたり、本来ロックしておかなければならない機能をロックしていなかったりシステムが脆弱な状態にあったため、いたずらに利用された。

Source: Los Angels Times
http://latimesblogs.latimes.com/lanow/2009/12/engineers-who-hacked-in-la-traffic-signal-computers-jamming-traffic-sentenced.html

最近の発表から：Blackhat USA 2014

- 講演タイトル：A SURVEY OF REMOTE AUTOMOTIVE ATTACK SURFACES
  - 発表者：CHARLIE MILLER（Twitter）、CHRISTOPHER VALASEK（IOActive）
- 講演のキーポイント
  - 今回のメインは自動車に遠隔攻撃をする為の要点の整理
    - 自動車が搭載している（あるいはする予定のある）無線の口について，どの程度の距離まで届くか，機知の攻撃手法，あるいは攻撃の可能性の有無のまとめ
    - 各社の自動車の情報系機能がどのような構造になっているのかをモデル化
  - デモ（動画）はあったものの。。。
    - リモートからBluetoothを利用して，走行中の自動車に対してリモートでブレーキに影響を与えることが可能であろうという動画は発表されたものの，技術的なことについては未公開。

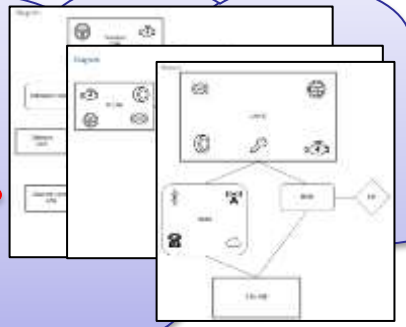
調査の事実も有用だが、アタック手法（攻撃者の視点）の理解を！！

Blackhatの発表から（自動車）

タイヤモニタシステム，Remote Keyless Entry, Bluetooth, Telematics, Internet…
プロトコルに応じて攻撃範囲や手法が変化する。

Attack Surface
攻撃が可能なポート

自動車修理工場用データベース等で手に入れることが可能。総合的にセキュアな設計が必要。



Network Architecture
ネットワーク構成

この三つに「弱点」が存在すると自動車の制御系に攻撃が可能に！

Cyber Physical
ITで操作可能な
物理的機能

セルフパーキング，レーンアシスト，衝突回避システム，自動走行
今後自動車の事故低減や快適性向上のために発展していく。

今後期待される車載セキュリティ
- セキュアゲートウェイ
- 適切なメッセージ暗号化
- セキュアアーキテクチャ
- 攻撃検知
- ログ収集

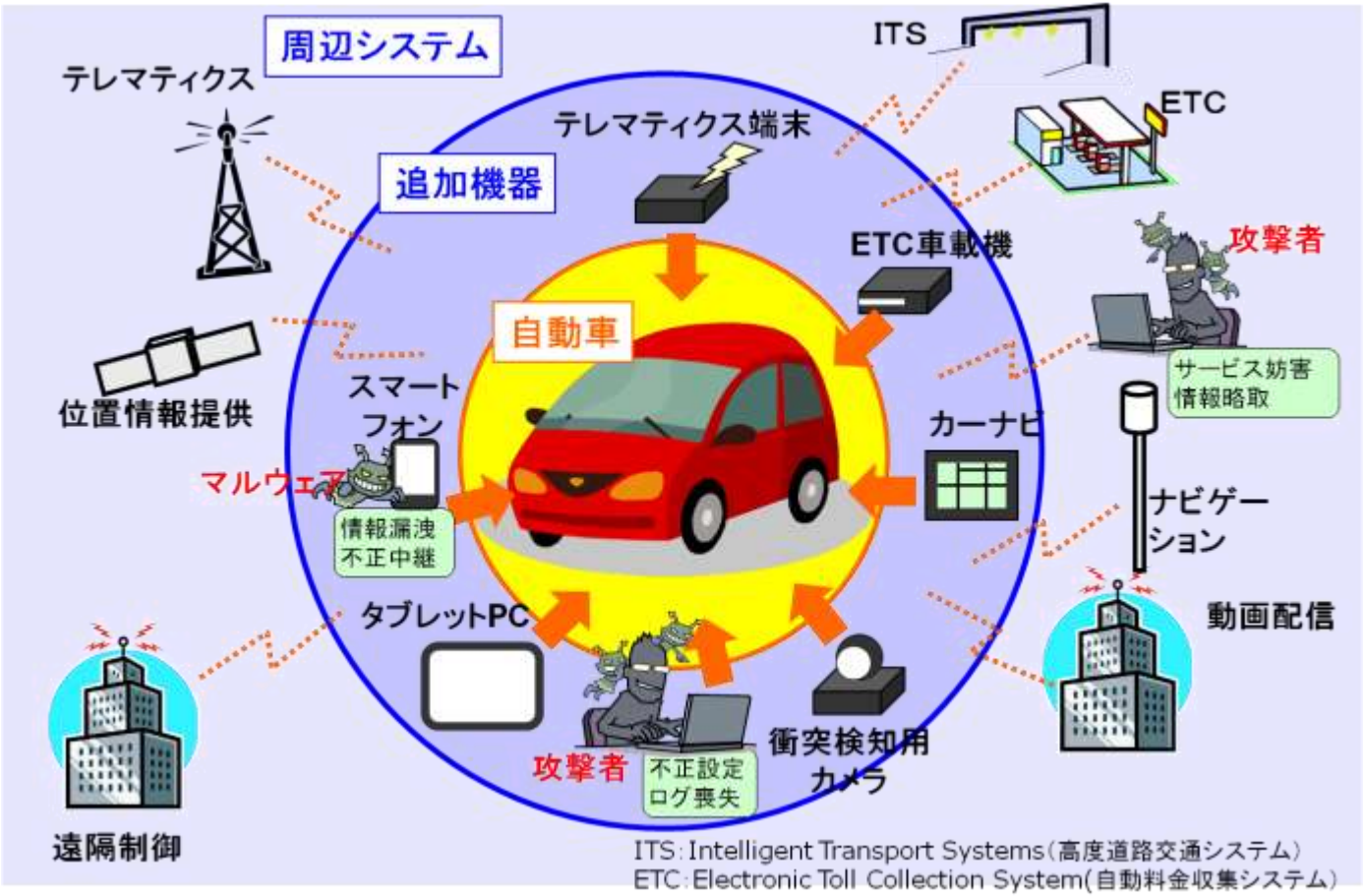
IPAによる自動車の脅威の分析
～自動車の情報セキュリティへの取組みガイド～

自動車キュリティ分析の流れ

- IPAにおける自動車セキュリティ分析の大まかな流れ
  - ネットワークで繋がる自動車を含めた世界を整理
  - 自動車の機能の整理
    - IPAカーという考え方
  - サービス形態や、自動車の持つ情報等資産を整理
  - 自動車における脅威を分析
  - 自動車に利用できると考えられるセキュリティ対策を検討
  - 自動車のライフサイクルにおいて考えられる「セキュリティへの取組み」を検討

同様の分析手法はこれまで「情報家電（主にデジタルテレビ）」においても実施成果有。

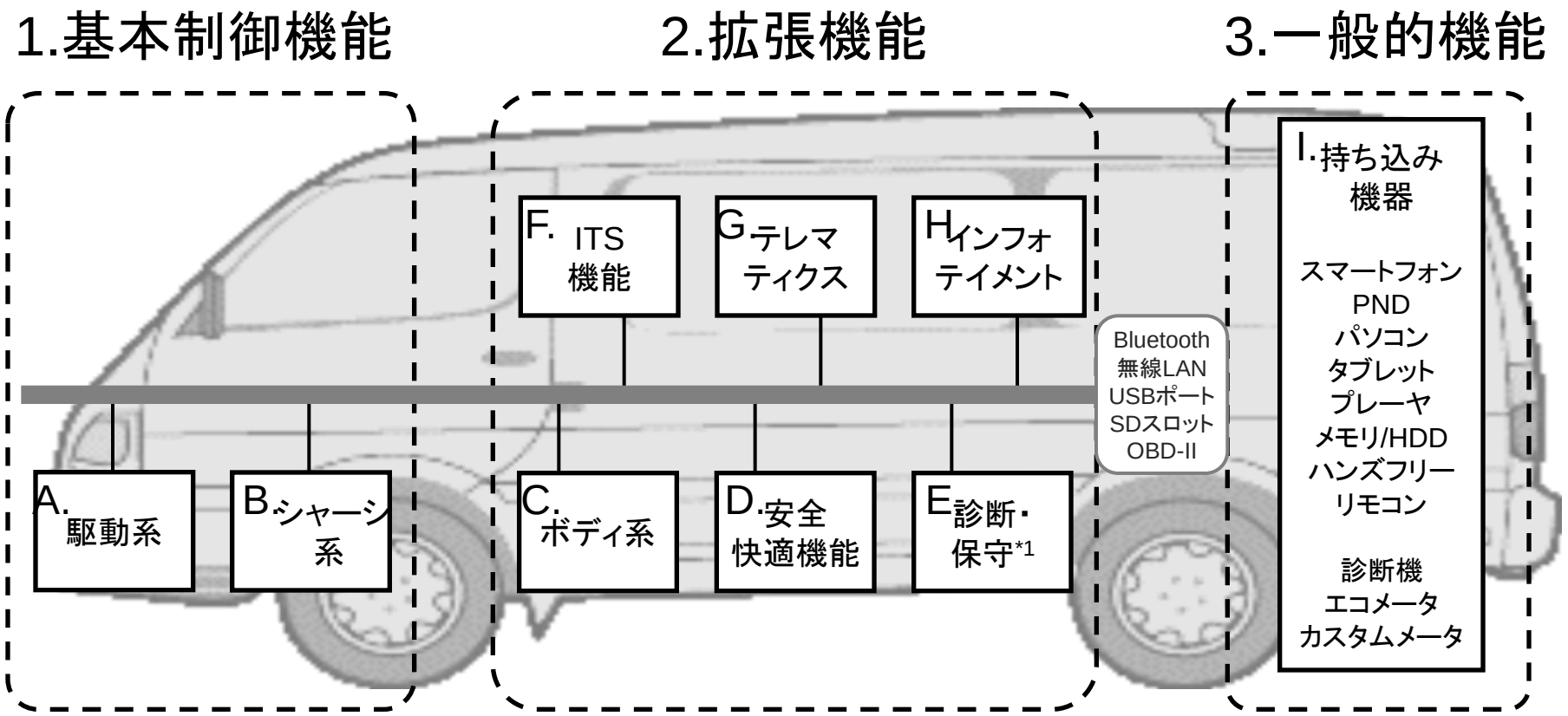
自動車システムの整理



最初に自動車がどのようなものと繋がる可能性があるのか、整理する必要がある。自動車が様々な機器やサービスに繋がると、それに従って色んな場所に攻撃者が現れる可能性がある。また、今後技術の発展によって、現時点では想定しえないものと繋がる可能性もある。

IPAによる自動車の脅威分析(1/6)

自動車の脅威を考える為に、自動車の機能を整理する必要がある。
しかし、自動車メーカや車種等によって、機能の整理手法は様々。
→IPAでは自動車の機能を整理した「IPAカー」をモデルとし、脅威を分析した

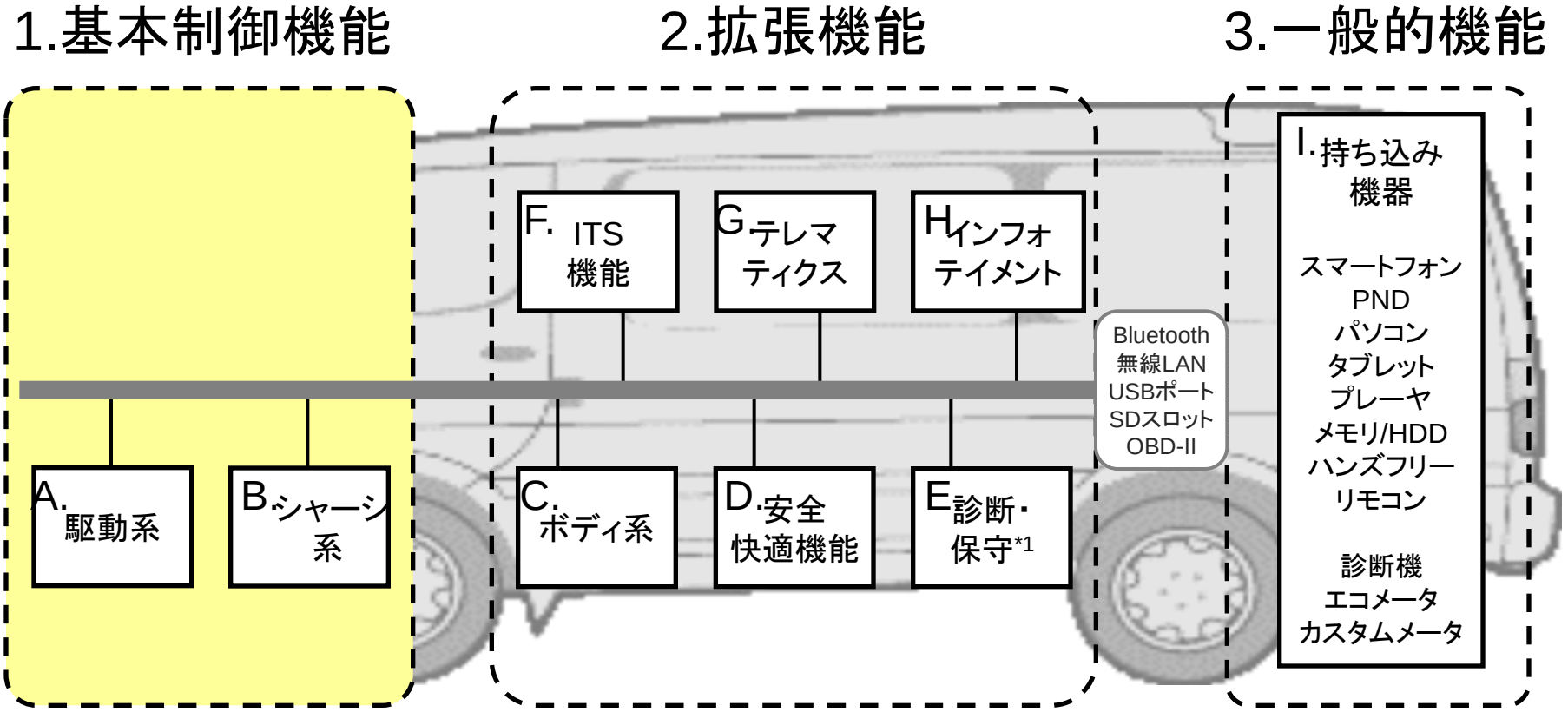


*1 診断・保守: 診断・保守は個々のECUなどに搭載されている場合がある

IPAによる自動車の脅威分析(2/6)

基本制御機能：

- **自動車の基本的な機能である「走る・曲がる・止まる」を制御する基本的な機能。**
- **この機能が攻撃を受ける車両事故に直結する為、高いセキュリティが必要。**
- **「拡張機能」が不安定な時は、他の機能を遮断してでも守る必要がある。**



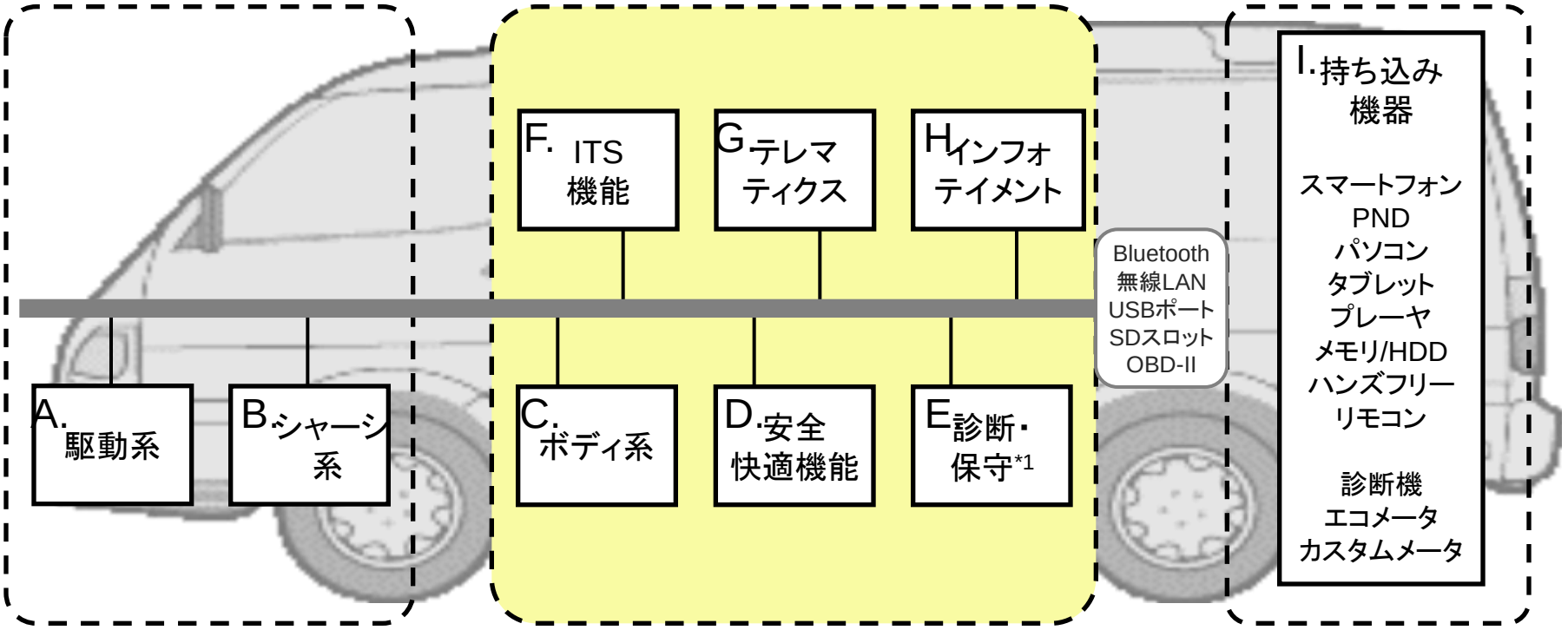
*1 診断・保守: 診断・保守は個々のECUなどに搭載されている場合がある

IPAによる自動車の脅威分析(3/6)

拡張機能：

- **自動車の快適な運転や、運転のサポートを担う機能**
- **機能の性質上、外部との通信機能を持つ事も多く、また車内での連携機能も多い。**
- **今後も機能向上が見込まれ、それに伴ったセキュリティ対策が必要になっていく。**

1.基本制御機能　2.拡張機能　3.一般的機能



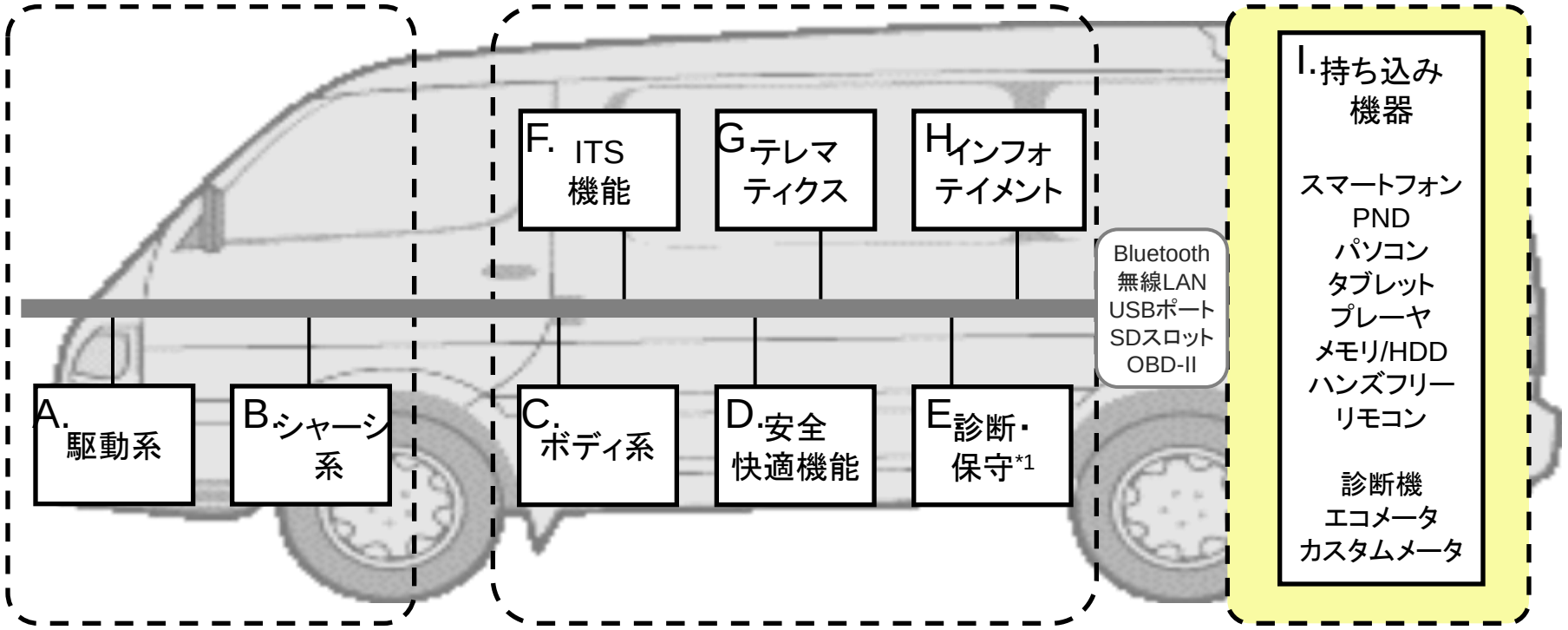
*1 診断・保守: 診断・保守は個々のECUなどに搭載されている場合がある

IPAによる自動車の脅威分析(4/6)

一般的機能：

- **スマートフォンやPCに代表されるような、ユーザが外から持ち込んで使う機器。**
- **サービスも多様で、様々な情報を扱う為、攻撃者に最も狙われやすい部分。**
- **既存のセキュリティ技術の適用が可能であり，対策の実施にはユーザの協力が必要。**

1.基本制御機能　　2.拡張機能　　3.一般的機能



*1 診断・保守: 診断・保守は個々のECUなどに搭載されている場合がある

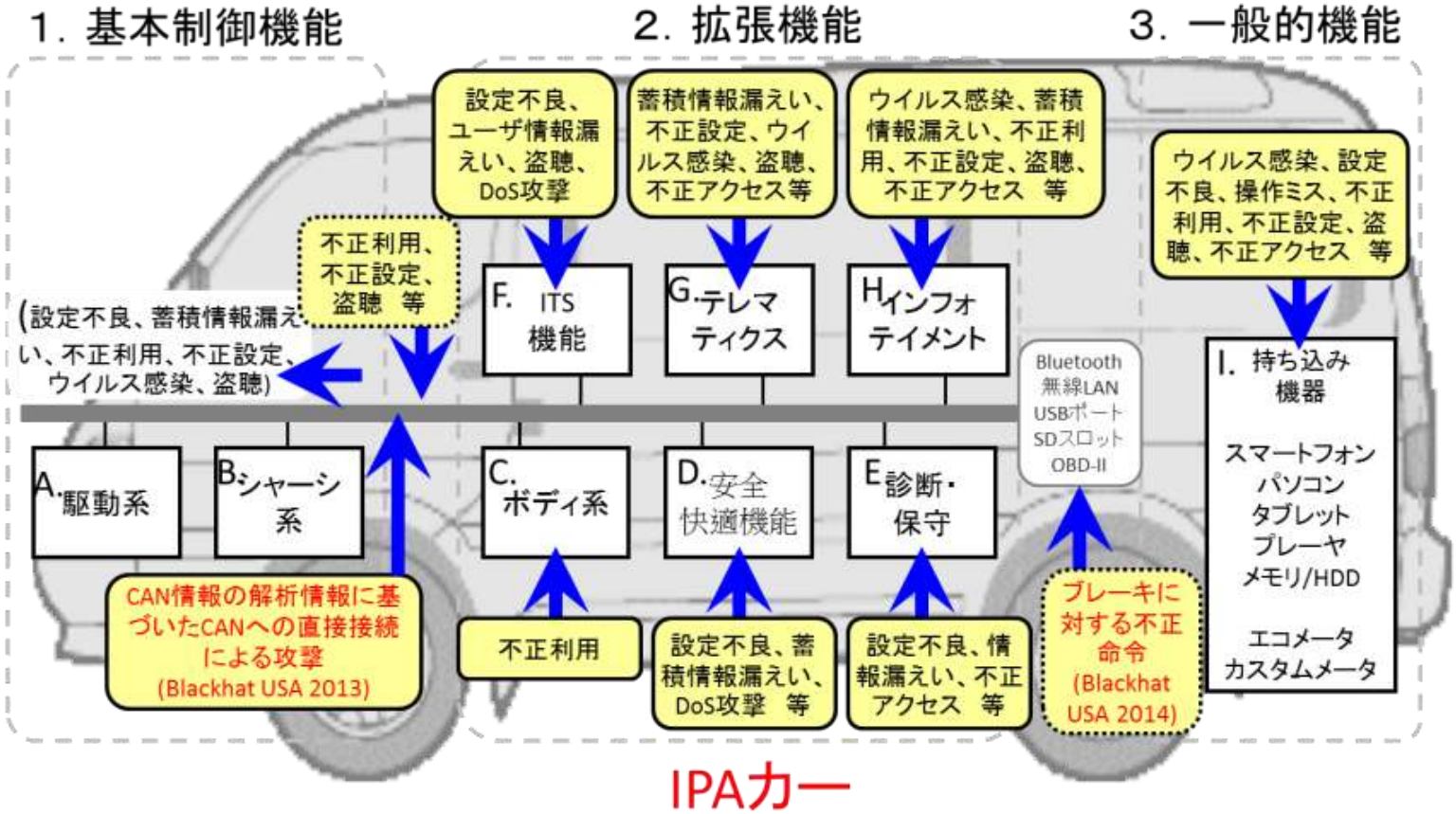
IPAによる自動車の脅威分析(5/6)

- 守るべき対象を明確にする
  - 「攻撃者から何を守りたいのか」を明確にすることがセキュリティの第一歩
  - 守りたい対象の価値がセキュリティ対策のコストに繋がる。
  - サービスの拡大によって、保護対象は広がっていく。
- 情報システムと組込みシステムの違い
  - 情報の保護以上に、車両事故の回避が重要な場面も
  - 機密性より可用性を重要視した作りになることも。

保護すべき対象区分	説明
基本制御機能の動作	基本制御機能の一貫性と可用性、基本制御機能の実行環境や、動作のための通信
自動車固有情報	自動車車体に固有の情報（車両ID・機器ID等）、走行・動作履歴等蓄積情報
自動車状態情報	自動車の状態を表すデータ、位置、車速、目的地等
ユーザ情報	運転者・搭乗者の個人情報、認証情報、課金情報、利用履歴・操作履歴等
ソフトウェア	ECU（Electronic Control Unit）のファームウェア等自動車の基本制御機能・拡張機能に関わるソフトウェア
コンテンツ	ビデオ、音楽、地図等のアプリケーション用データ
設定情報	ハードウェア・ソフトウェア等の動作設定データ

IPAによる自動車の脅威分析(6/6)

外部から、情報の入出力が出来るポートを持つ機能についてはPCと同様の脅威がある。
一方で、制御系を外部から直接攻撃する手段に関しても、模索され始めてきた。



海外の研究発表の事例にもあるように、自動車制御に直接攻撃を仕掛けるのではなく、脆弱なシステムを踏み台にして、自動車制御に影響を与える危険性がある

セキュリティ対策の考え方

- どのようにセキュリティ対策を実装していくか？
  - 完全にいつまでもセキュアなシステムは至難
    - そもそも完全にセキュアなシステムは困難
    - 時間経過による脅威。攻撃者の成長，技術革新，暗号の危殆化など
    - 最低限のセキュリティレベルを統一するのは有効
      →それでも最後は各自のリスク判断
  - 情報システムにおける一般的なセキュリティ技術の利活用
    - 情報システムセキュリティの知見を利用しないのは損。
    - 技術は「必要性」が存在することで磨かれる。
    - これまでに日の目を見なかった技術や研究が輝く･･･かも。
  - 自動車に特化したセキュリティの検討も必要
    - 自動車独自のプロトコルに適したセキュリティ対策も
      →裏を返せば、**自動車だけが抱える脅威**も？
    - 情報システムのセキュリティ対策では対応しきれない部分も

「自動車のセキュリティへの取組みガイド」
もう一つのアプローチ：セキュリティを考慮すべき15項目

マネジメント（セキュリティ関連商品でなくても、メーカとして常に行うべき事柄）

- **セキュリティルールの策定、セキュリティ教育の実施、セキュリティ情報の収集と展開**

企画（ライフサイクル全体の計画を行うフェーズ）

- **セキュリティに配慮した要件定義の策定、セキュリティ関連予算の確保、開発外部委託におけるセキュリティへの配慮、新技術に関連する脅威への対応**

開発（システムの開発を行うフェーズ）

- **設計、実装時のセキュリティ対策、セキュリティ評価・デバッグ、利用者等への情報提供用コンテンツ等の準備**

運用（組込みシステムがユーザの手に渡った後、製品として利用されるフェーズ）

- **セキュリティ上の問題への対処、利用者や自動車関係者への情報提供、脆弱性関連情報の活用**

廃棄（買い替え、故障などで組込みシステムが廃棄、リサイクルされるフェーズ）

- **廃棄方法の策定と周知**

詳しくはIPAの公開している

「自動車の情報セキュリティへの取組みガイド」で

http://www.ipa.go.jp/security/index.html

情報システムにおける セキュリティ対策の有効利用(1/4)

■ 脆弱性情報データベース　JVN iPedia

URL:http://jvndb.jvn.jp/

国内外の脆弱性対策情報を収集したディクショナリデータベース

- IPAが運営するサイト
- 国内ベンダーと連携をし、脆弱性対策情報を公開
- 海外の脆弱性DB(NVD)の情報を日本語翻訳して公開
- 約42,000件の脆弱性対策情報を登録

情報システムにおける セキュリティ対策の有効利用(2/4)

- セキュリティ上の弱点(脆弱性)を作りこまないための教育
  - 学習によって脆弱性に対する理解を深める
  - サンプルアプリで実際に手を動かして脆弱性を知る
  - 「よくある脆弱性」に対するチェックを行う

学習の流れ

学習テーマ選択後の流れ

脆弱性 原理解説 ▶ 演習 ▶ 影響解説 ▶ 対策方法 解説 ▶ 脆弱性 修正 ▶ 解答・修正 例確認

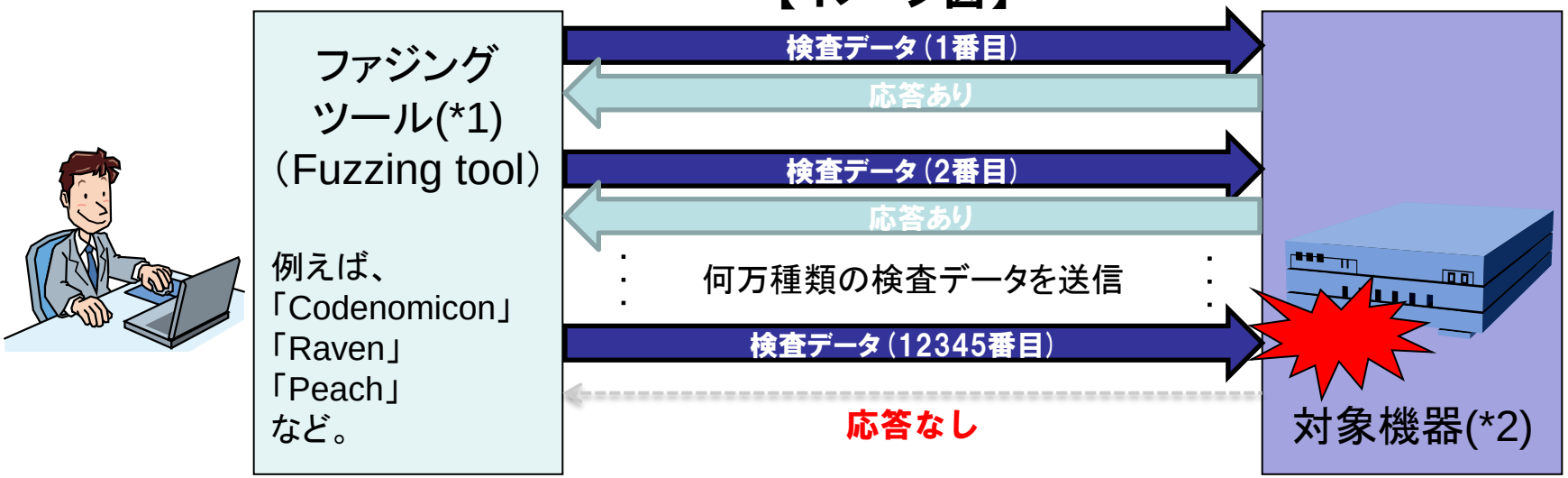
ウェブアプリの脆弱性体験学習ツール
AppGoat

Androidアプリの脆弱性体験学習ツール
AnCole

情報システムにおける セキュリティ対策の有効利用(3/4)

- ファジング(英名:Fuzzing)の利用
  - 何万種類もの問題を起こしそうなデータ(例:極端に長い文字列)を送り込み、対象製品の動作状態(例:製品が異常終了する)から脆弱性を発見する技術

【イメージ図】



IPAが実施したファジングでは、ルータの脆弱性を発見。他の組込み機器に対しても調査中。
IPAではこの調査結果や、ファジングの利用ガイド等も随時公開。

(*1): ファジングツールは、商用製品だけではなく、オープンソースソフトウェア、フリーソフトウェアも存在します。
(*2): この図では組込み機器を示していますが、ソフトウェア製品でも同様です。

情報システムにおける セキュリティ対策の有効利用(4/4)

ソフトウェアの脆弱性を評価するシステム、『共通脆弱性評価システム（CVSS：Common Vulnerability Scoring System）』を利用して、自動車システムにおける脆弱性の深刻度の評価を試行。セキュリティ対策の優先度を決める上で非常に重要となる。

	脆弱性	OBD-II経由で認証なしでECUのファームウェアを書き換えられる	何も対応せず、脆弱性が深刻化する例
	被害	走行中のブレーキ操作不能	
基本評価基準	攻撃元区分	ローカルでのみ攻撃可能	ネットワークから攻撃可能
	攻撃条件の複雑さ	高	低
	攻撃前の認証要否	認証操作が不要	認証操作が不要
	機密性への影響	影響なし	影響なし
	完全性への影響	全面的	全面的
	可用性への影響	全面的	全面的
現状評価基準	攻撃される可能性	実証可能	容易に攻撃可能
	利用可能な対策のレベル	非公式な解決法	非公式な解決法
	脆弱性情報の信頼性	未確認の情報源のみ	開発者が情報を確認済み
環境評価基準	二次的被害の可能性	重大な被害や損失	壊滅的
	影響を受ける対象システムの範囲	中規模	大規模
	機密性の要求度	低	低
	完全性の要求度	高	高
	可用性の要求度	高	高
	基本値 / 現状値 / 環境値	5.6 / 4.3 / 5.2	9.4 / 8.9 / 9.8
	全体的評価値	5.2 (最大10点)	9.8 (最大10点)
	深刻度	レベルII（警告）	レベルIII（危険）

同じ脆弱性でも攻撃手法が洗練されたり、簡易攻撃ツールが出回る事で深刻化
そうなる前に、脆弱性をきちんと評価し、対応する事が必要

既存制度の利用

- 自動車は他の機器に比べ制度的に優れている？
  - 免許の取得・更新
    - 利用者にセキュリティ教育を施す機会
    - 公的機関によるものなので，足並みを揃えるのが容易
  - 車検
    - 数年に一度とはいえ，必ずメンテナンスできる機会
    - 被害事例やパッチ適用率等も調査可能？
  - ガソリンスタンドという情報ステーション
    - 「自動車利用者なら必ず訪れる場所」が存在

一般利用者にセキュリティ意識を持って頂く事はなかなかに難しい事
自動車はパソコンやスマートフォン、情報家電等の情報関連機器に比べ、
利用者教育及び機器の一元管理がやりやすい状況にある。

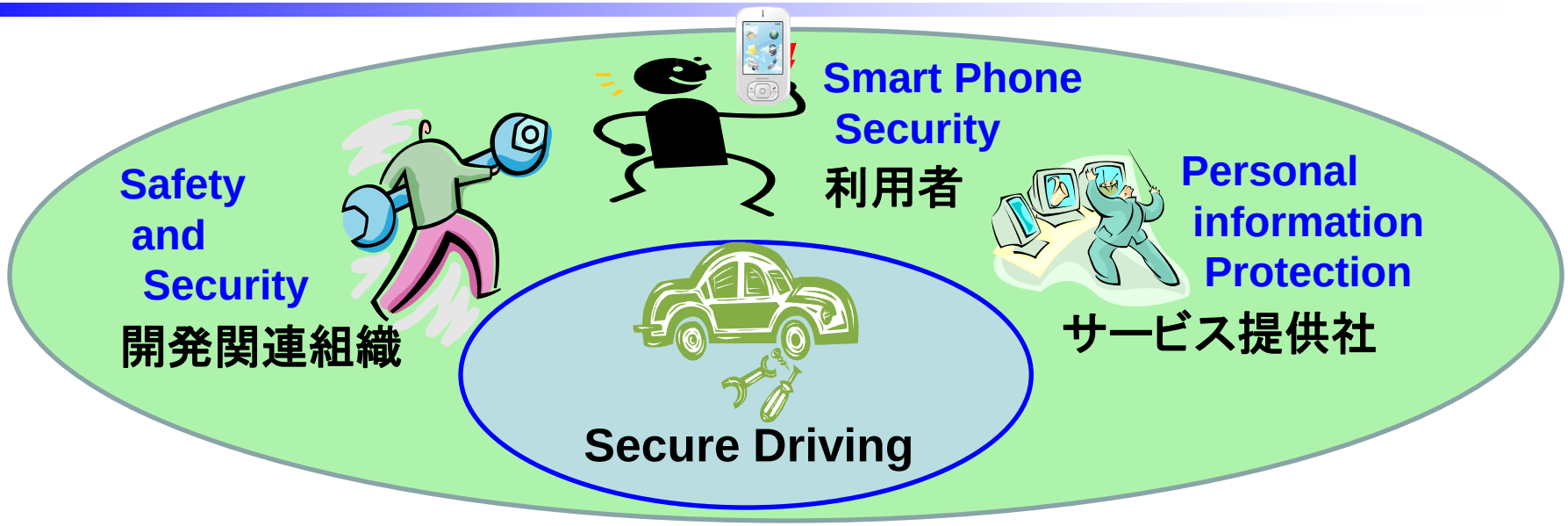
まとめ

「繋がる」情報・機能をどう扱うか

情報・機能を利用する際にインターネットを利用するのであれば、そこには**漏えい**・**改ざん**・**奪取**・**破壊**等のリスクがある。またそれに伴う機能については**遠隔地からの攻撃**や**不正利用**のリスクが常に考えられる。

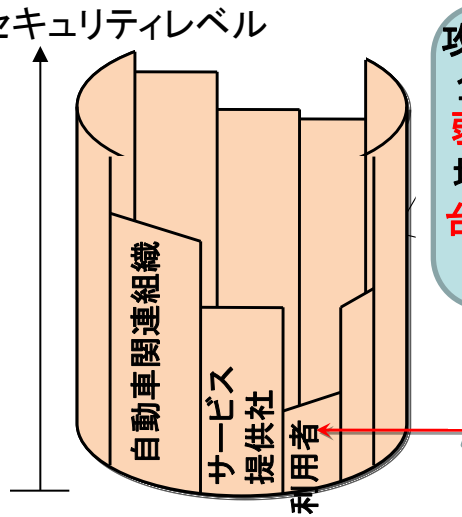
機器の企画・開発段階から、利用用途やサービス等を踏まえた**セキュリティリスク分析・検討**が必要。

総合的＆継続的なセキュリティ対策を



樽の理論

何本もの樽材で組み合わせ、タガを締めた樽には、一番短い樽材の位置までしか水は入らない。それより長い樽材をどれほど高級なものにしたとしても、この結果は変わらない。



攻撃者はサービス・システム全体を分析した上で、一番弱点となっている所を狙う。場合によってはそれを踏み台としてさらに内部に攻撃をしかける事も。

効果的なセキュリティ対策を実施するためには、組込み機器の開発関連組織のみならず、それに関わる組織・人の連携が必要

最後に:
安全でセキュアな社会に向けて

組込みセキュリティに関連する IPA セキュリティセンターの活動

2011年5月9日公開
2010年度 制御システムの情報セキュリティ動向に関する調査
2013年3月6日公開
2012年度 制御システムの情報セキュリティ動向に関する調査

2011年4月26日公開
2010年度 自動車の情報セキュリティ動向に関する調査
2012年5月31日公開
2011年度 自動車の情報セキュリティ動向に関する調査
2013年3月25日公開
2012年度 自動車の情報セキュリティ動向に関する調査

2009年6月24日公開
組込みシステムのセキュリティへの取組みガイド
2009年11月25日公開
上下水道分野用のSCADAセキュリティ グッド・プラクティス
2013年3月25日公開
自動車のセキュリティへの取組みガイド

組込みシステムのライフサイクル

企画	開発	運用	廃棄

2011年1月27日公開
脆弱性体験学習ツール AppGoat
2012年3月27日公開
ファジングに関する手引き・レポート等
2014年4月11日公開
Androidアプリの脆弱性の学習・点検ツール AnCoLe

2007年4月25日から実施
組込みシステムを含んだソフトウェアの脆弱性関連情報の受付・蓄積・公開

2007年9月26日公開
セキュア・プログラミング講座

ご清聴ありがとうございました！

本成果はIPAのWebサイトでダウンロードする事ができます。
http://www.ipa.go.jp/security/index.html

Contact：
IPA（独立行政法人 情報処理推進機構）
技術本部　セキュリティセンター
情報セキュリティ技術ラボラトリー
TEL 03（5978）7527
FAX 03（5978）7518
電子メール　vuln-inq@ipa.go.jp

Windows Server 2003のサポート終了に伴う注意喚起

Windows Server 2003のサポートが、2015年7月15日に終了します。

サポート終了後は修正プログラムが提供されなくなり、脆弱性を悪用した攻撃が成功する可能性が高まります。

サポートが継続しているOSへの移行検討とOS移行に伴う周辺ソフトウェアの影響調査や改修等について計画的に迅速な対応をお願いします。

- 業務システム・サービスの停止・破壊
- 重要な情報の漏えい
- データ消去
- ホームページの改ざん
- 他のシステムへの攻撃に悪用

会社の事業に悪影響を及ぼす被害を受ける可能性があります

詳しくは　IPA　win2003　検索

企業・社員の情報セキュリティ対策、コンプライアンス向上に！！

ITパスポート試験　（iパス）

IPA

ITを利活用する<u>すべての社会人・学生</u>のための<u>国家試験</u>

iパス公式キャラクター
上峰　亜衣

情報セキュリティ対策の重要性の高まりを踏まえ、<u>情報セキュリティの出題を強化！</u>

i パス　　検 索