IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

第六回
水道分野における
スマートメーターに関する勉強会

『スマートな社会』におけるセキュリティ

2015年3月18日（水）

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
中野 学（博士（情報学））

IPAとは
（Information-technology Promotion Agency, Japan）

IPA

IT社会の
安全・安心を創る

ソフトウェアの
高信頼化を築く

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

IPA/ISEC(セキュリティセンター)の使命と事業の柱

【使命】
経済活動、国民生活を支える情報システムの安全性を確保すること

企画

- セキュリティセンター業務の企画・調整
- 他事業部門、バックオフィスとの連携、調整
- 行政機関、関係機関等との連携、調整

ウイルス・不正アクセス及び脆弱性対策

- ウイルス・不正アクセスの届出・相談受付
- 脆弱性関連情報の届出受付・分析、提供
- 組込み機器(制御システム)等のセキュアな利用に向けた取組み

暗号技術

- 暗号アルゴリズムの安全性監視活動
- 暗号世代交代の普及促進

セキュリティの第三者認証

- ITセキュリティ評価・認証制度(コモンクライテリア)
- 暗号モジュール試験認証制度(JCMVP)

調査・分析

- 情報セキュリティ関連の社会経済的分析
- 情報セキュリティ白書
- 意識調査、被害実態調査

普及啓発・国際連携

- 世界の情報セキュリティ機関との連携
- 情報セキュリティの普及、啓発
- 中小企業のセキュリティ対策向上
- 情報セキュリティ対策ベンチマーク

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
  - 組込みシステムや制御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

スマートメーター単体は組込みシステム
スマートメーターを利用した社会システムは大きな制御システム

情報セキュリティの現状

脅威の現状

インターネットの環境は大きく変化している
攻撃(悪意)の動機も変化している

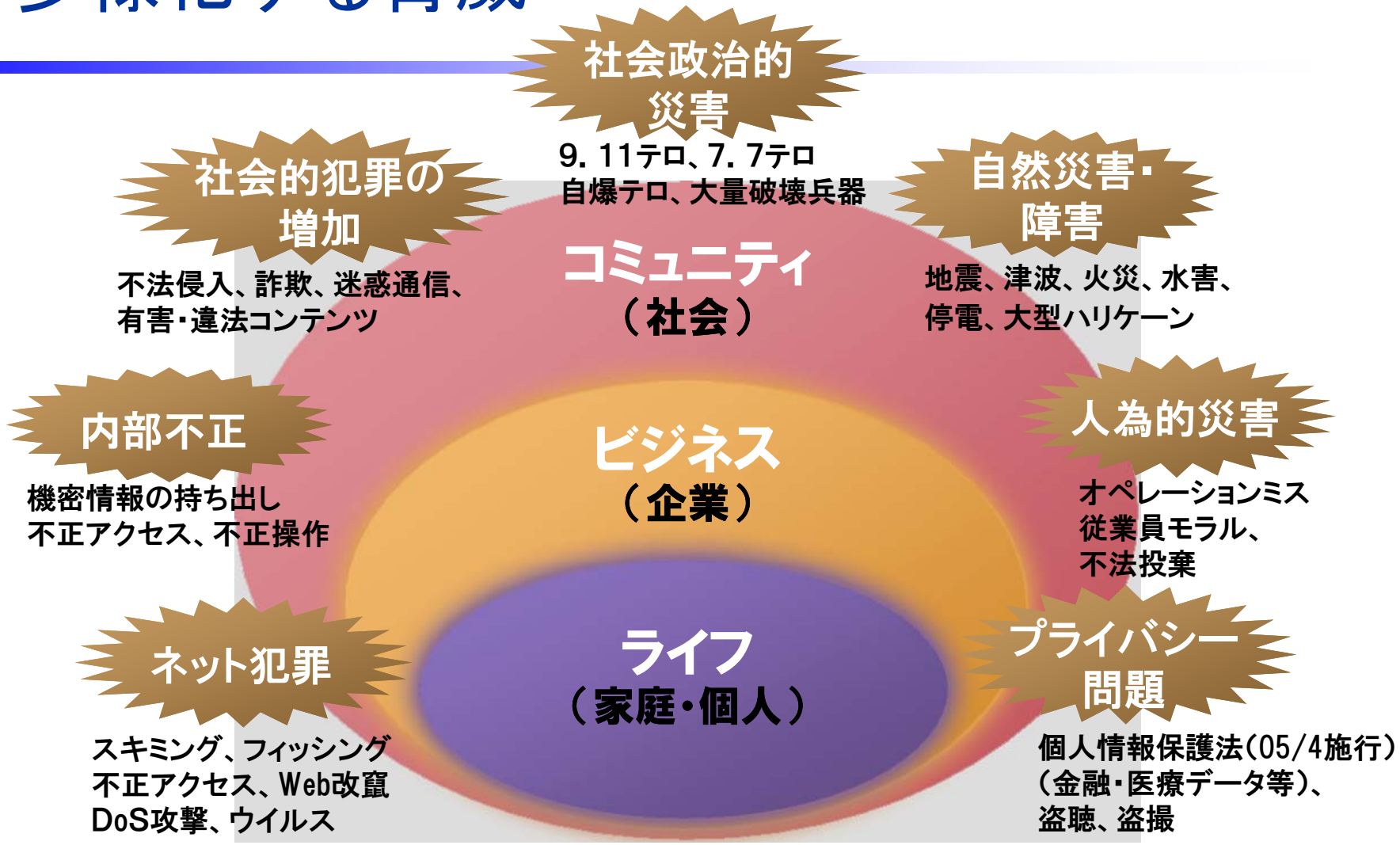
＜初めの頃は＞

いたずら

＜現在、これから？＞

金銭・犯罪・テロ・情報戦

多様化する脅威



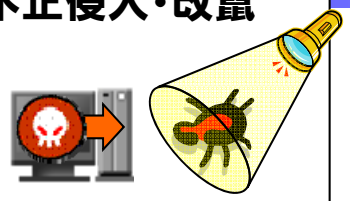
「不安解消」、「安心・安全の確保」に対する社会的ニーズ増大

サイバー攻撃の変容

IPA

2000

不正侵入・改竄



1脆弱性＝1攻撃の時代

PCとホームページ改竄がターゲット

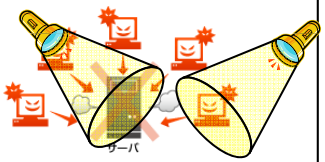
攻撃者ひとり

PCの破壊・HP改竄

対象：PC、サーバ

2004～

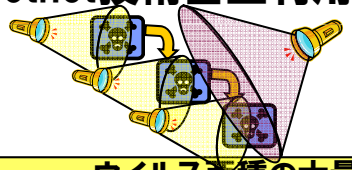
体系化（Botnet）



攻撃組織基盤化

2006～

多段化
（Botnet技術基盤利用）



2009～

正規サービスの
攻撃基盤利用

正規サイト・サービス利用

ウイルス亜種の大量出現
シーケンシャルマルウエア（多段型攻撃）
0-Day脆弱性利用
toolによるウイルス生産
情報システムがターゲット

攻撃組織間連携

戦術的攻撃

多様な意図性（情報搾取攻撃）

影響（業務インパクト）の変化

情報搾取等
e-マーケットビジネス、決済等への影響
決済関連情報搾取等、サプライチェーン
危機管理

対象：情報システム（組織・ビジネス）

セキュリティ製品でカバー（製品の出現）
製品を置く設計思想

？
設計思想を変化させないと…

脅威全貌とポイントが見えにくい時代
一定の情報運用で守る時代（情報連携）
皮を切られても肉まで切られない発想設計
システム・ネットワークトポロジ設計で防御

出展：亀山社中

スマートシティセキュリティ

スマートシティ

IPA

IPAの検討範囲

地域の連携（スマートコミュニティ）

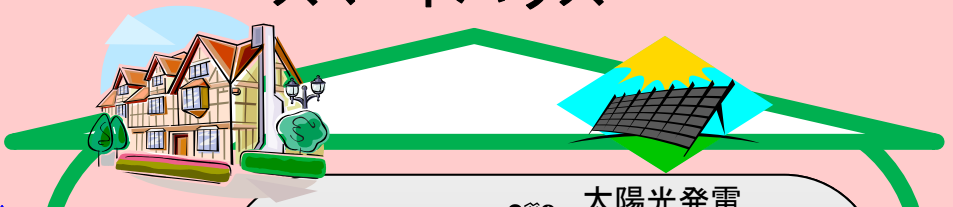
情報やエネルギー等の交換・共有

サービス
ゲートウェイ

スマートメータ

双方向の
情報の流れ

スマートハウス



太陽光発電

蓄電池

情報家電

白物家電
スマート家電

ルータ等

ゲーム機

家庭用PC

電話・スマートフォン

電気自動車

家庭における管理システム

家庭エネルギー
管理システム
（HEMS）

水道・サービス会社との連携

サービス系

水道利用
管理
サービス等

水道制御系

水道関連情報系

料金等基本
データベース

スマートシティが目指すもの

「繋がる」事でスマートシティが目指す世界

・水道利用の見える化　　・水道管理サービスによる、エコ化
・情報サービスとの連携、外部からの制御　・料金徴収コスト等の削減

この実現にはIT技術やネットワークの利用が必須

スマートハウスにおけるセキュリティの課題

・多種多様なサービスや機器との連携により、制御や情報保護が複雑に
・これまでのPCセキュリティ以上に、可用性を重視したセキュリティ設計が必要
・サイバー攻撃によって資産だけでは無く、人体への被害の可能性もある

スマートハウスを構成する機器やシステムでは、稼働条件や取り扱う情報を明確にした上で、設計・開発段階から適切なセキュリティ対策を選択する事が必要となる。

三つの進化と、それに伴うセキュリティ

IPA

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。

スマートシティの未来

- 新しいサービスの発達
  - より「便利」な社会インフラ確立に向けたサービスの充実
  - 「エコ」なビジネスモデルの確立
- ネットワークへの接続
  - 遠隔地・僻地等のインフラ管理
  - エネルギー・資源管理会社と各家庭・都市の連携
- 汎用プロトコル等の利用
  - コストダウンのための汎用OSの利用
  - 機器連携やネットワーク利用に向けた汎用プロトコルの利用

（スマートメーターに関連のありそうな）脅威の事例

スマートメーターを組込み機器と見立てたときの関連事例

スマートメーターへの攻撃可能性の報告
→セキュリティ関係者もスマートメーターに興味を

【スペインの電力会社で利用されているスマートメータへの攻撃】

・2014年10月、オランダで開催されたBlack Hat Europe 2014において、スペインの電力会社で利用されているスマートメーターの**入手・分解・解析**を行うことで、スマートメータの持つ暗号鍵の解析に成功。欧州で利用されている特定のベンダ（非公表）の製品は、**スマートメータの暗号鍵が同じに設定**されているため、それを利用して他のスマートメータを攻撃することが可能。

考えられる脅威

- 電力の**遮断**
- メーターの**改ざん**（料金徴収への不正行為）
- **社会インフラに対する攻撃**

無線利用時の設計に関連する事例
→セキュリティ仕様を検討することの重要性

IPA

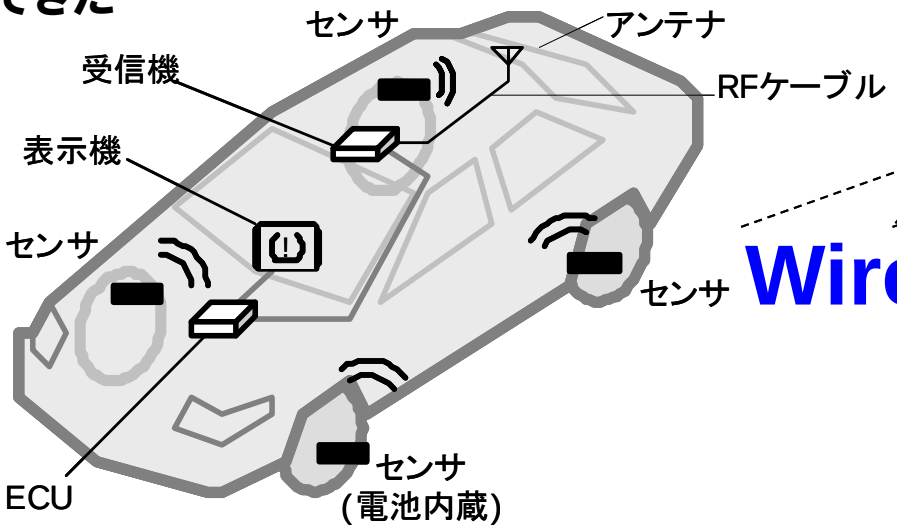
【TPMS (Tire Pressure Monitoring System) :タイヤの空気圧を常時監視するシステム】

・TPMSの脆弱性を指摘する論文(2010年8月コンピュータソフトウェア関連学会USENIX)にて TPMSが使用する二つの無線周波数について、ソフトウェアで無線周波数をデジタル処理するソフトウェアラジオの手法を使い、TPMSの無線通信方式そのものを解析。

(1) TPMSでは**通信メッセージは暗号化**されていない

(2) タイヤのバルブに装着した空気圧測定装置は32bitの固有のIDを持つとともに、**自動車本体から40m離れても無線通信**が可能であった。このことから路肩や高架橋などで測定すれば、特定の自動車がいつ通過したかを記録することができる。

(3) **TPMSの空気圧報告メッセージになりすますことができ、いつでも警告灯を点灯させることができた**



Wireless

遠隔からの攻撃

物理システムがIT化されることによる事例
→「ツール利用」による攻撃難易度低下

IPA

【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

ITやネットワークを活用したサービスにおける事例 →サービス運用を行う上での内部不正等への対処

【遠隔イモビライザー：イモビライザー（電子キーを利用した自動車盗難防止機能）を遠隔から操作できるシステム】

- 2010年3月、米国テキサス州オースチンで、突然100台以上の自動車のエンジンがかからなくなったり、警告ホーンが鳴り続け止められなくなる事件が発生。
- ある自動車販売店がローンで販売した自動車には、返済が滞った場合に停止させるための遠隔イモビライザーが装着されていたが、**解雇された従業員が不正操作**。
- 自動車のキーを持っていても警告ホーンの鳴動を止められず、エンジンをスタートできないため整備工場にも持ち込めず。

（スマートメーターと繋がる管理設備等に関連のありそうな）脅威の事例

工場等の制御システム側の関連事例

実在する制御システムの被害事例 (1/3)

- 実際に制御システムでウイルス感染や不正アクセス等のサイバー攻撃により多くの被害が発生しています。

生産ラインが停止する被害が発生しています

事例1　自動車工場

被害:　自動車生産50 分間停止等、
約1,400万ドル（約17億円）の損害

被害企業：ダイムラー・クライスラー（現ダイムラー）

原因:　ウイルス感染。外部から持ち込まれて接続されたノートPCの可能性が指摘されている

概要:　2005年8月18日、13の自動車工場がウイルス感染により操業停止となった。ウイルス感染により、各工場のシステムはオフラインになり、組み立てラインで働く50,000 人の労働者は作業を中断し、生産が50 分間停止した。部品サプライヤへの感染も疑われ部品供給の懸念も生じ、およそ1,400 万ドルの損害をもたらした。

出所：情報処理推進機構「重要インフラの制御システムセキュリティとIT サービス継続に関する調査」, 2009.3, pp.23-24
http://www.ipa.go.jp/files/000013981.pdf

実在する制御システムの被害事例 (2/3)

石油パイプラインの爆発や製鉄所の操業停止といった事態が発生しています。

事例2　石油パイプライン

被害:　　トルコの石油パイプラインの爆発

被害企業:BP（British Petroleum、運営主体）

原因:パイプラインに設置されている監視カメラの通信ソフトの脆弱性を利用して内部ネットワークに侵入。不正に動作制御系にアクセスし、管内の圧力を異常に高めて爆発を引き起こした。
その際、攻撃者は警報装置の動作を止め、通信を遮断するなどの操作も実施。

出所:Bloomberg, “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar Era,” 2014.12.10
http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html

事例3　製鉄所

被害:　　ドイツの製鉄所の操業停止

被害企業:ドイツの製鉄所

原因:　　電子メールに添付したマルウェアを使って、ネットワークにアクセスするためのユーザーIDとパスワードを入手し、内部システムに不正アクセス。
溶鉱炉を正常に停止できず、生産設備が損傷する大きな被害を受けた。

出所:BSI（ドイツ連邦情報セキュリティ庁）, “Die Lage der IT-Sicherheit in Deutschland 2014（2014年版サイバー犯罪白書）”
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

実在する制御システムの被害事例 (3/3)

事例4　国内　自動車工場

報道こそほとんどされていないものの、国内でも多数の被害が発生しています。

被害:　　自動車の生産ラインの処理能力低下

被害企業:国内自動車メーカー

原因:　　業者による端末入れ替え時にウイルスが混入し、システム内のパソコン約50台がウイルス感染し、処理能力が低下。

出所:毎日新聞「サイバー攻撃:車工場ウイルス感染　制御システム、処理能力低下――08年、西日本で」, 2011.11.27

事例5　国内　半導体工場

被害:　　生産ライン停止

被害企業:国内大手半導体メーカー

原因:　　品質検査を行う検査装置へのウイルス感染による生産ライン停止、USBメモリ経由での感染。

出所:MONOist「産業制御システムのセキュリティ(5):事例から見る、製造現場でのセキュリティ導入のツボ」
http://monoist.atmarkit.co.jp/mn/articles/1402/12/news082.html

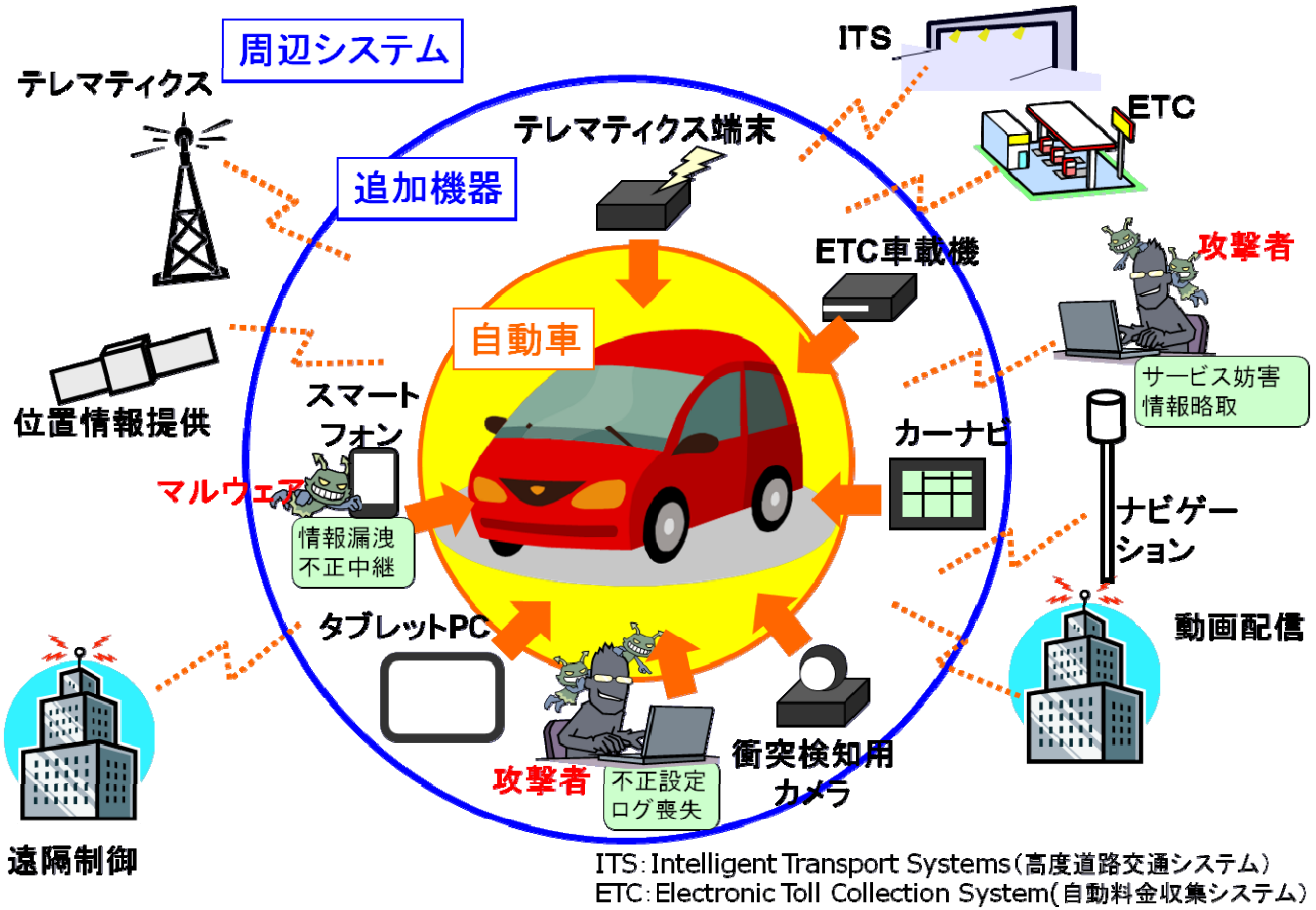
セキュリティの考え方の一例
～IPAにおける自動車の脅威分析例～

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

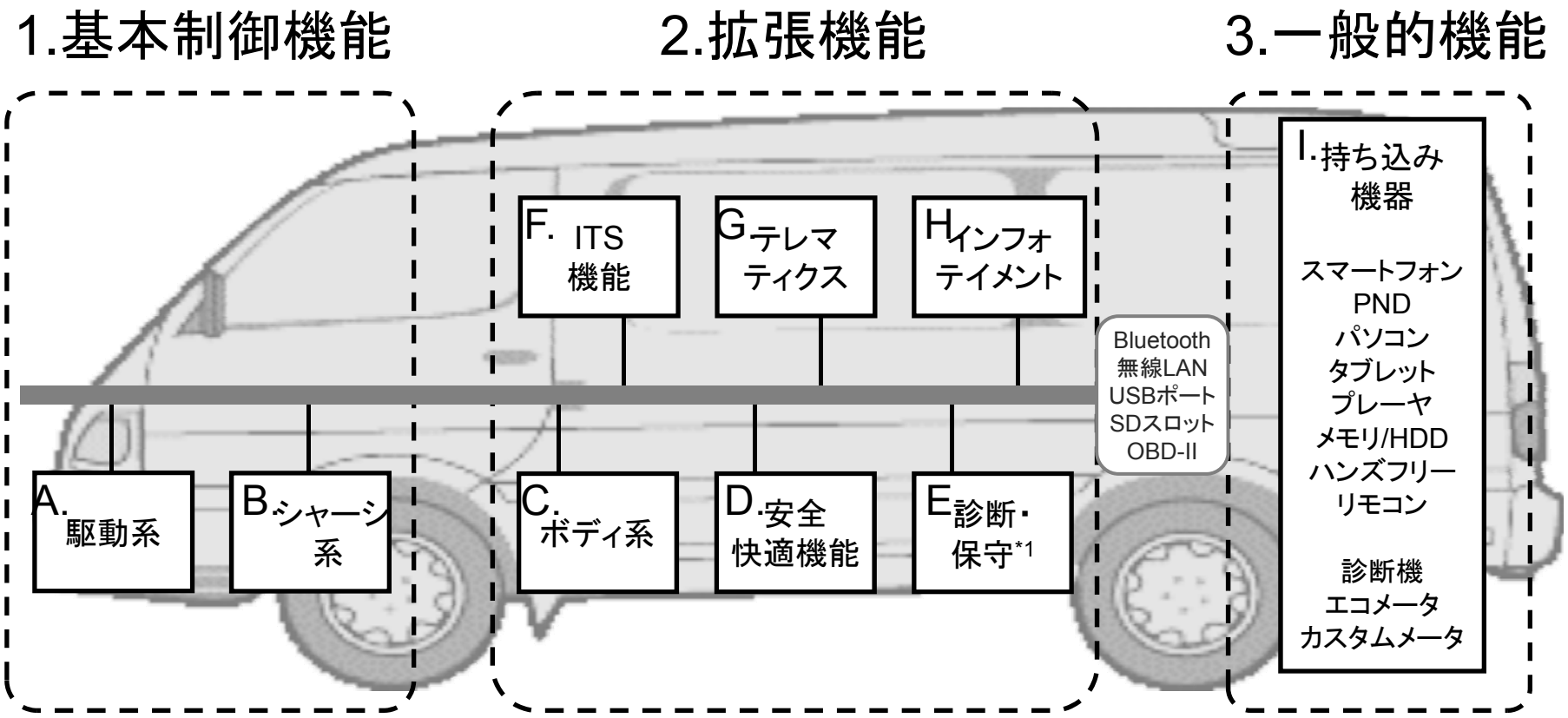


ITS：Intelligent Transport Systems（高度道路交通システム）
ETC：Electronic Toll Collection System（自動料金収集システム）

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(1/3)

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

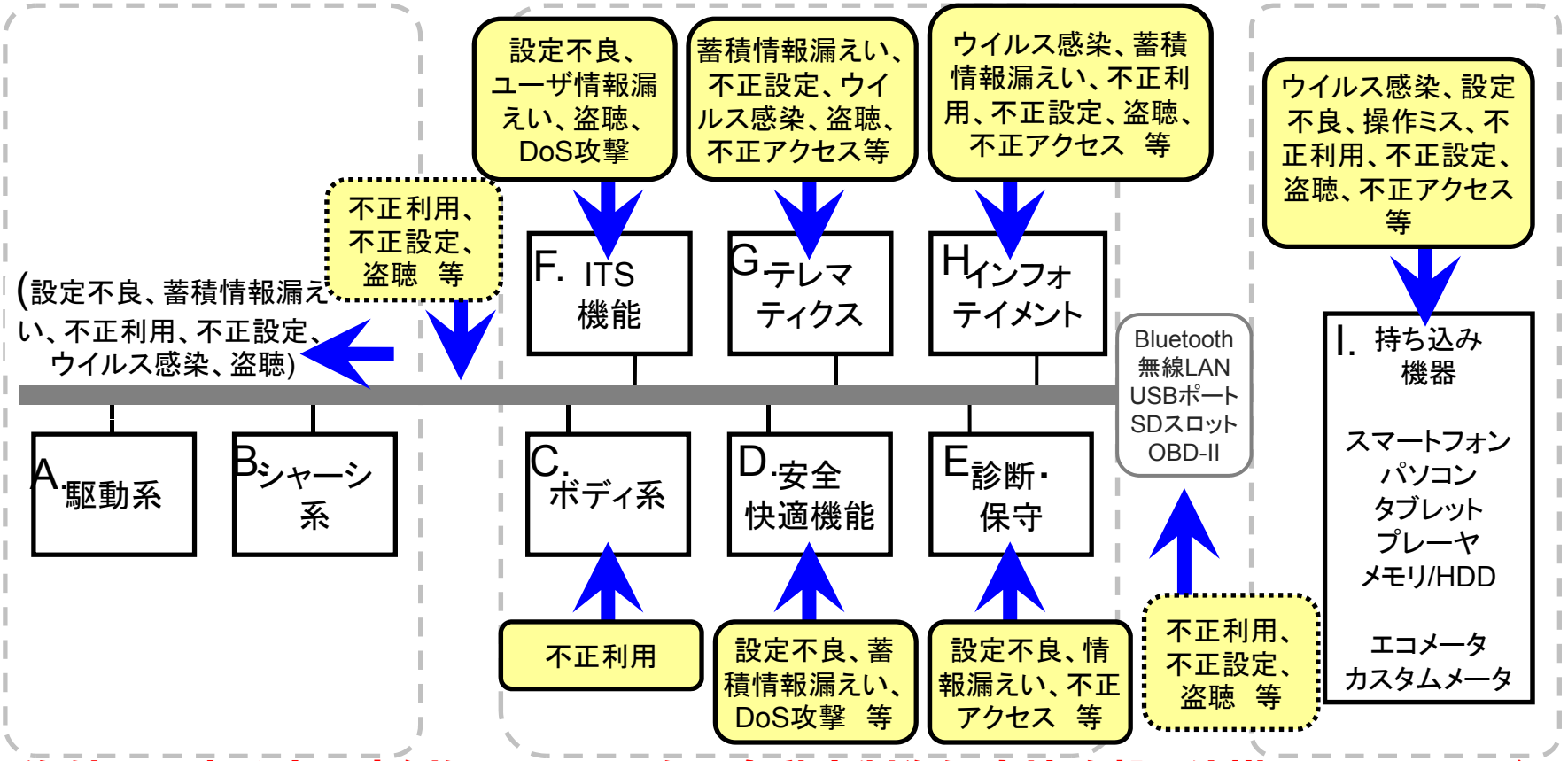
IPAによる自動車の脅威分析(2/3)

- 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(3/3)

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は、現状では見つからない。



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？
  - 序段としては、情報システムにおける一般的なセキュリティ技術を検討してはどうか
    - 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。
  - システムに特化したセキュリティの検討も必要
    - システム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、**スマートメーターだけが抱える脅威**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

具体的な情報セキュリティ対策
（参考例）

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

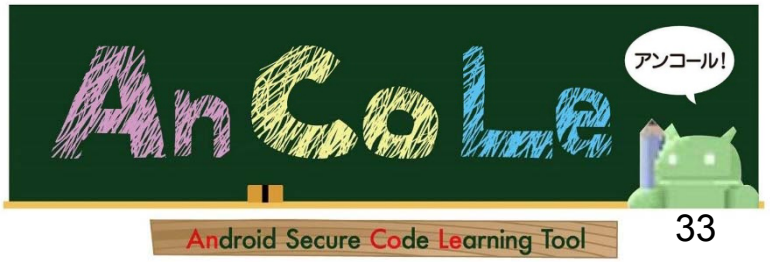
学習の流れ

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

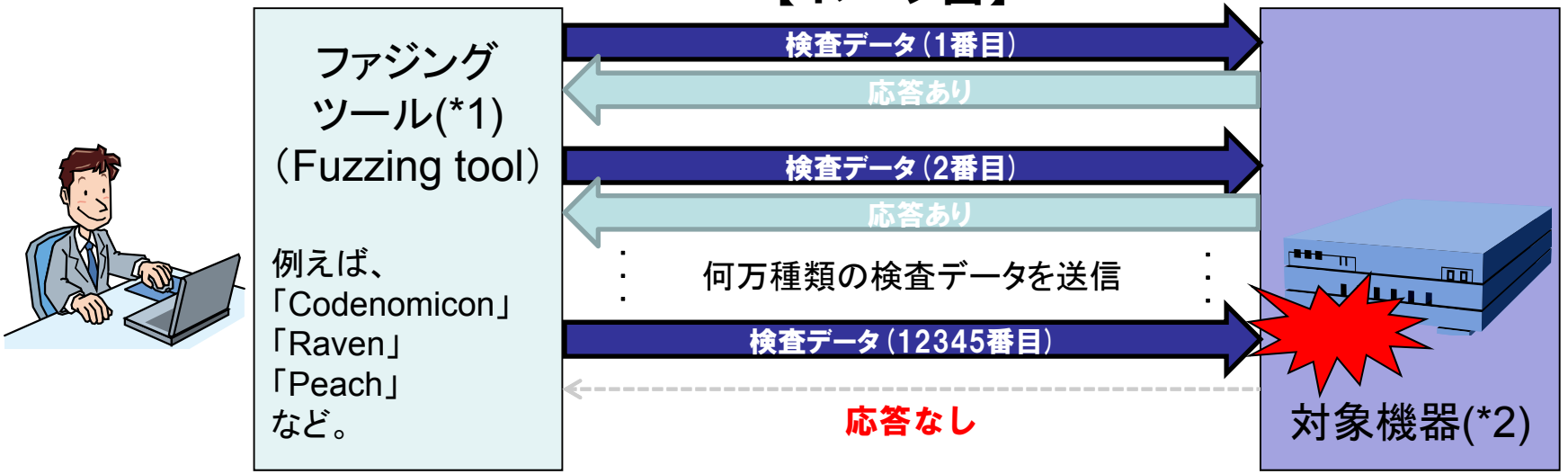
Androidアプリの脆弱性体験学習ツール AnCole



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

スマートシティのセキュリティを考えるために

組込み・制御システムセキュリティから見た スマートシティセキュリティ

IPA

(1) 脆弱性の顕在化

・情報システムを利用する以上**脆弱性は出てくるもの。脆弱性弱性を作らない開発**と共に、**運用面で脆弱性に対策**することが必要。
また、「**誰がどこまで対応するのか？**」という事も考える必要がある。

(2) 外部との多様な（ネットワーク）接続の拡大

・スマートシティの中では多種多様なネットワークが利用される。
どのネットワークが、**何と繋がり、どのような情報を交換しているか**を把握した上で、適切なセキュリティ対策を実施する必要がある。

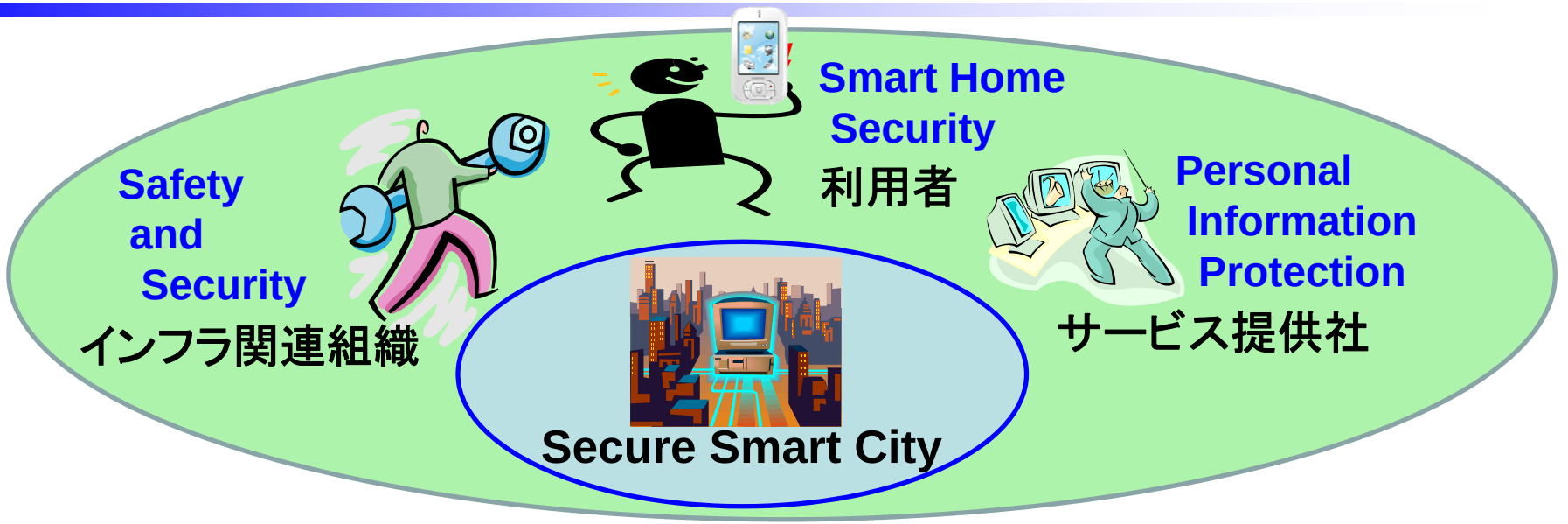
(3) スマートシティ内での『区切り』をつける

・スマートシティ内では、街やビル、家など様々な機能群がある。
全ての情報を安易に共有するのではなく、それぞれの機能群を重要度や利用者をもとに、**ゲートウェイ等で『区切る』**ことが重要となる。

(4) EVでの新しい脅威

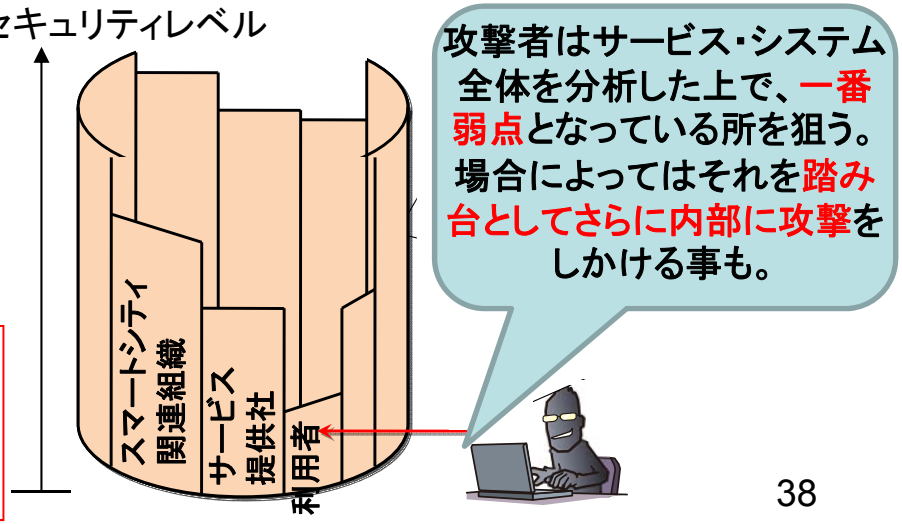
・スマートシティの発展と共に、今後新しいサービスや機能が展開される。
新しい事が新しい脅威に繋がらないよう、セキュリティ面での検討が必要。

まとめ：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。



効果的なセキュリティ対策を実施するためには、自動車本体の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:
安全でセキュアなスマートシティに向けて

セキュアなスマートシティの実現を

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

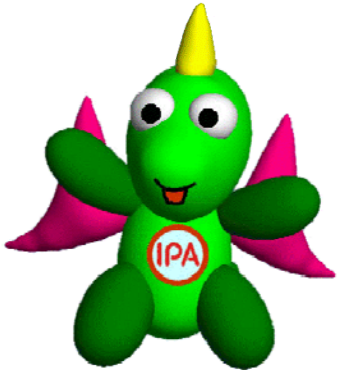
企画	開発	運用	廃棄

2014年4月16日公開
医療機器における情報セキュリティに関する調査

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

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

IPA

ITパスポート試験

ITパスポート公式キャラクター
上峰亜衣（うえみねあい）

【プロフィール：マンガ】 https://www3.jitec.ipa.go.jp/JitesCbt/html/uemine/profile.html

「iパス」は、ITを利活用するすべての社会人・学生が備えておくべき
ITに関する基礎的な知識が証明できる国家試験です。