社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

IPA

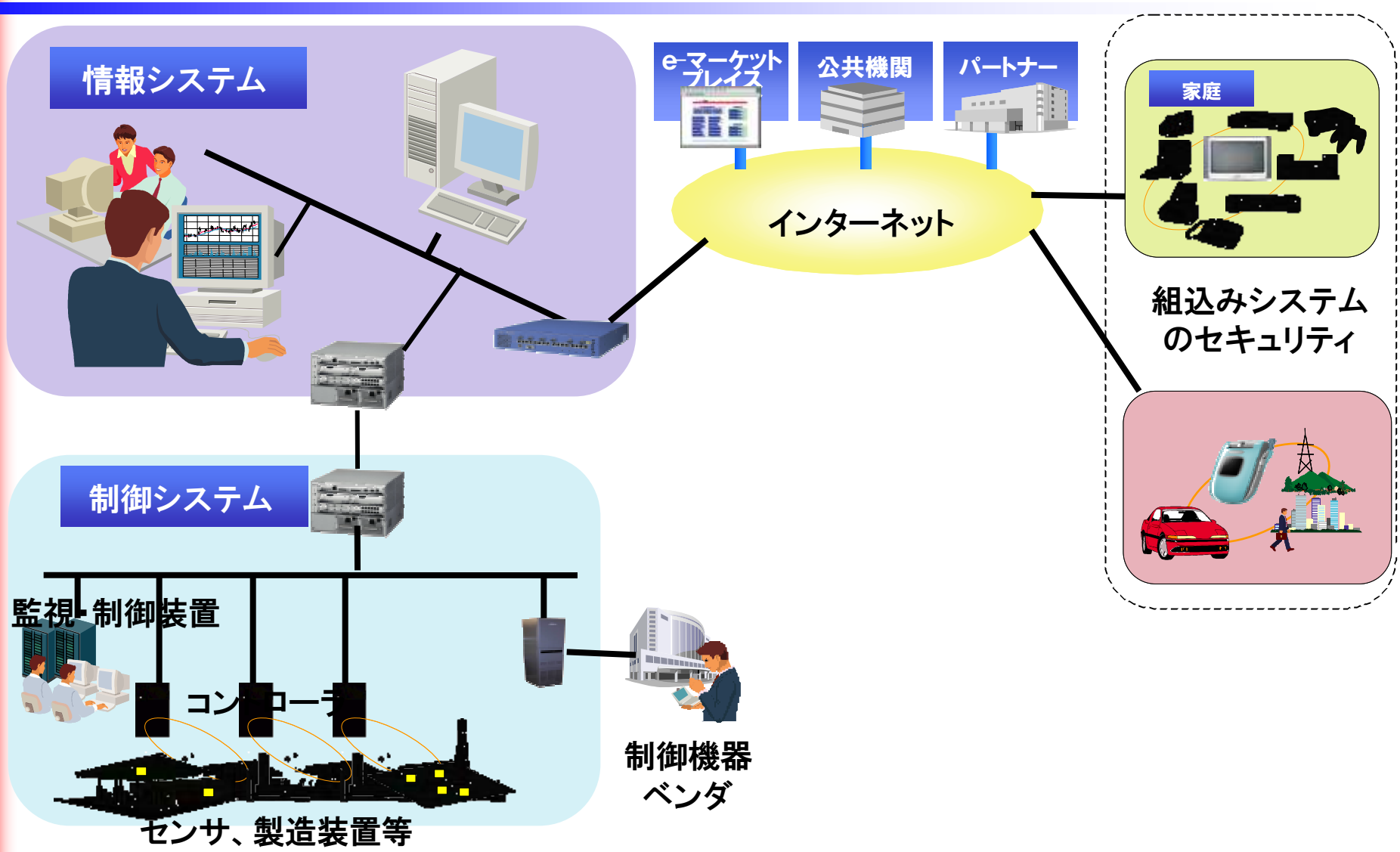
JASAETセミナー

第24回JASA/ETセミナー
自動車等組込みシステムのセキュリティ技術

組込みシステムのセキュリティ調査報告 ～自動車・情報家電・制御システムなど～

2010年10月15日
独立行政法人　情報処理推進機構
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））
mn-naka@ipa.go.jp

様々な組込みシステム



身近な組込みシステム

流通を支える組込みシステム

RFID

識別・認証

カーライフを支える組込みシステム

通信サービス

カーナビ・ETC

安心・便利を支える組込みシステム

ICカード

携帯電話

モバイルを支える
組込みシステム

消費を支える組込みシステム

ATM 金融端末

情報家電

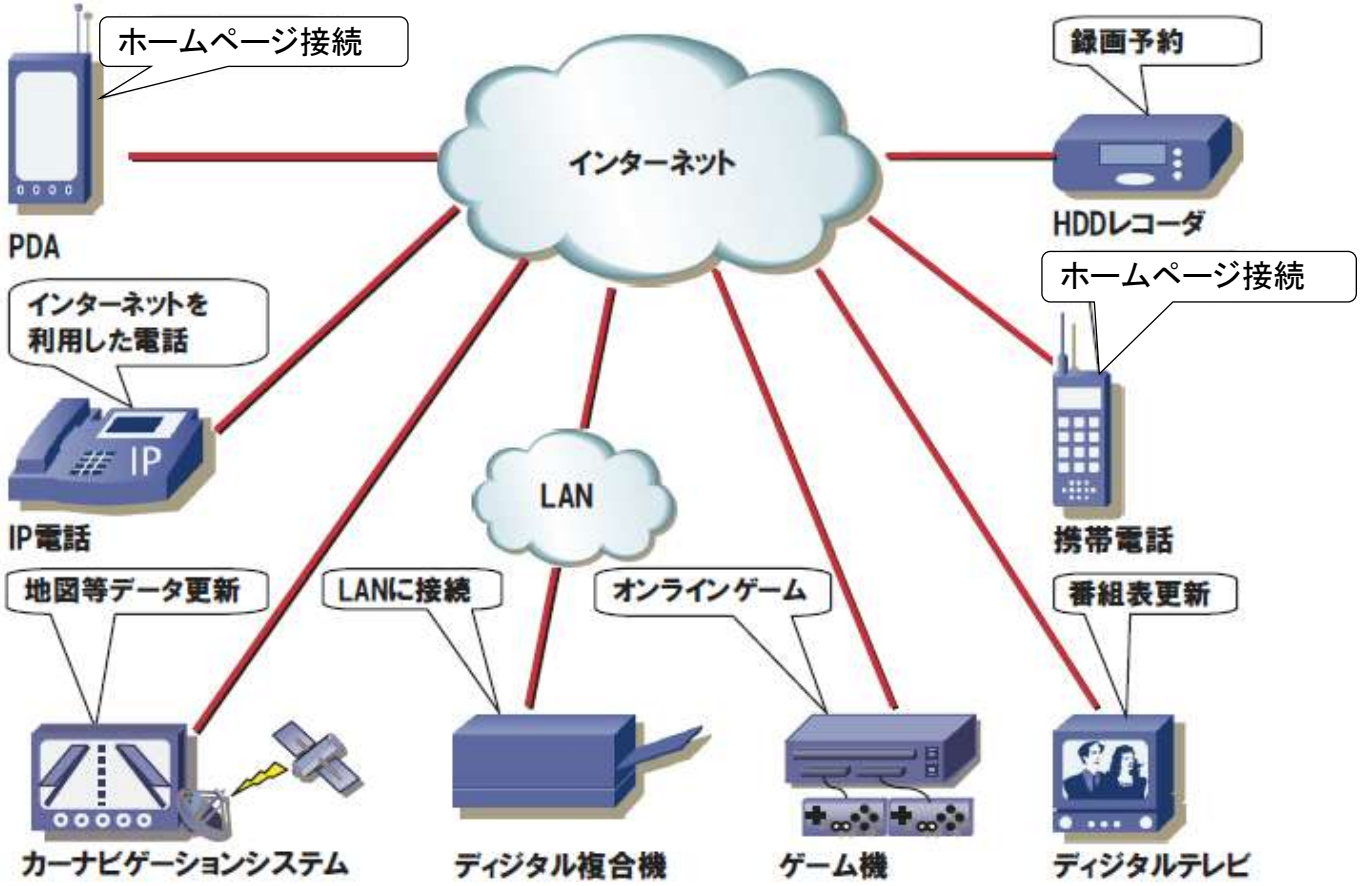
生活を支える組込みシステム

RFID（Radio Frequency IDentification）
ETC（Electronic Toll Collection System）

組込みソフトウェアを用いた機器の現状

ネットワーク機能を備えた組込み機器の例

背景 ： あらゆるものが、ネットワークにつながる



PDA（Personal Digital Assistants）
HDD（Hard Disk Drive）

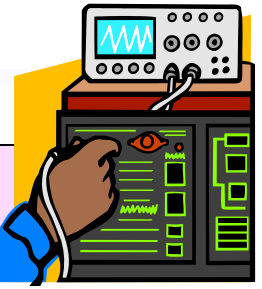
組込みシステムセキュリティの特殊性

- もしパソコンにセキュリティ対策をしていなかったら・・・
  - ウィルス等のマルウェアへの感染
  - 悪意あるユーザの攻撃による被害

- PCの場合の対策例
  - アンチウィルスソフトウェアの導入
  - セキュリティファイアウォールの利用
  - セキュリティパッチのダウンロード・適用

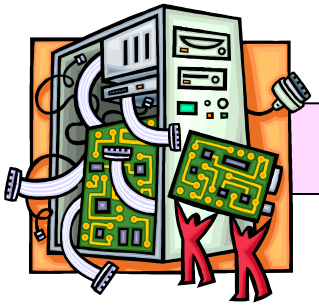
組込みシステムにおいては、開発環境や製品の特徴等の違いから、PCと同じような対策を実施するのは困難。

具体的なセキュリティ課題



利用者(ユーザ)が攻撃者になる

リバースエンジニアリング



リソースの制約

情報資産の改竄・漏洩

組込みシステムのライフサイクル

企画 | 開発 | 運用 | 廃棄

セキュリティ課題の混在

脆(ぜい)弱性の作りこみ

個人情報の漏洩

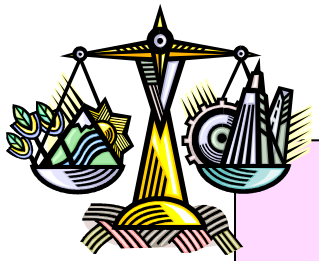
企画書の漏洩

情報漏えいのようなインシデントの発生

リバースエンジニアリング:
機械を分解したり、ソフトウェアを解析するなどして、製品の構造を分析し、そこから製造方法や動作原理、ソースコードなどを調査する事

具体的なセキュリティ対策

耐タンパー性付与等の
システム解析(攻撃)への耐性強化



低リソースで利用できる
セキュリティ技術の普及

暗号・認証の利用

組込みシステムの
ライフサイクル

企画 | 開発 | 運用 | 廃棄

セキュリティ対策
ガイドラインの策定

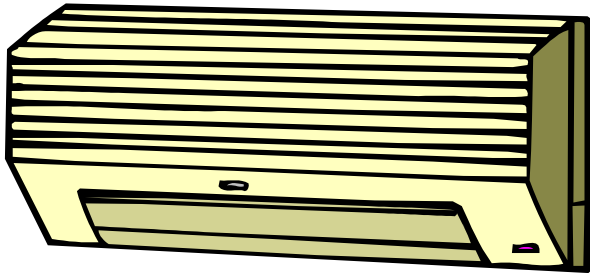
セキュアプログラミング
セキュリティ検証

廃棄方法の周知

一環したセキュリティ対策

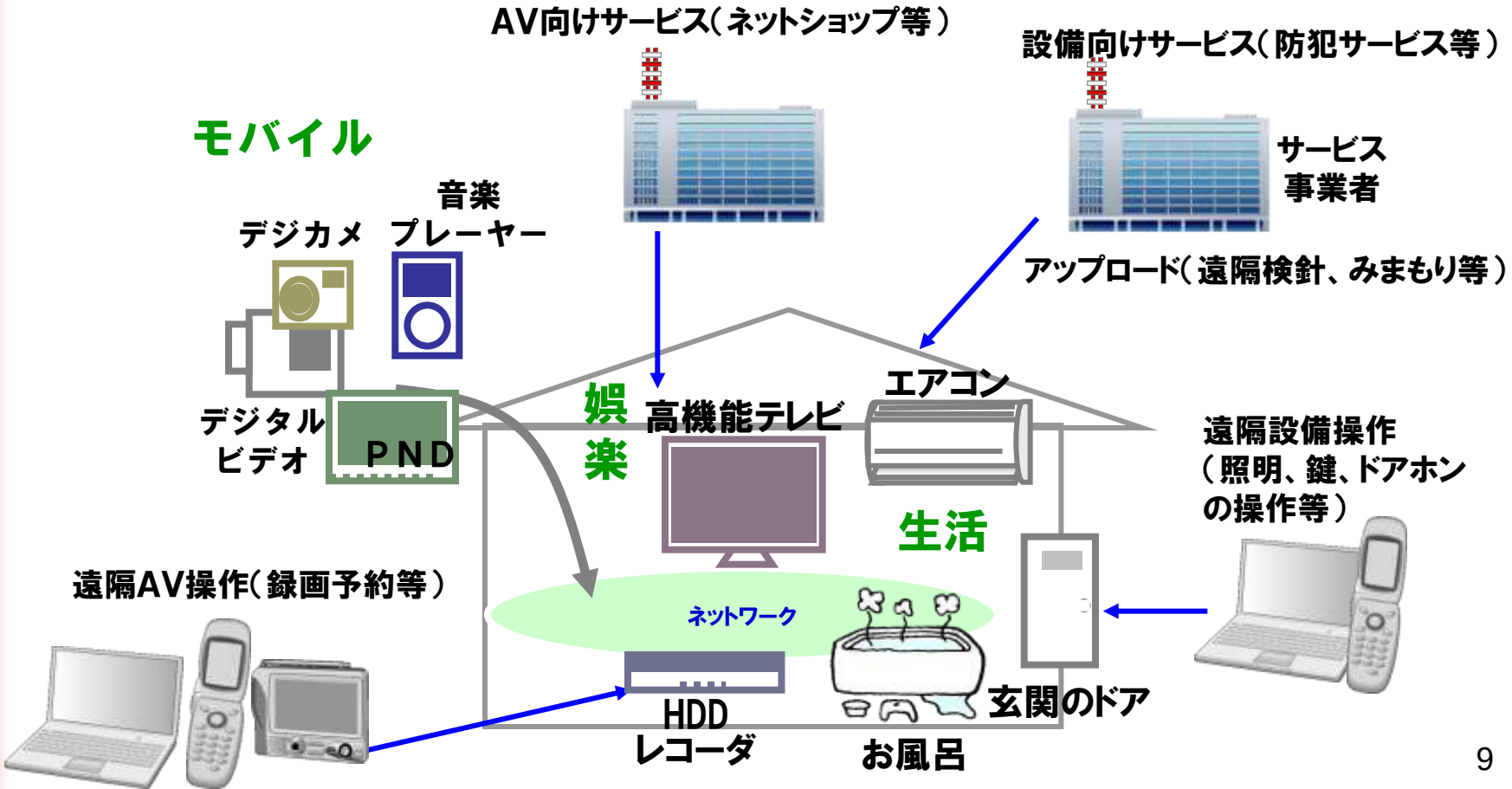
インシデント対応方法体制の確立

情報家電と自動車の情報セキュリティ



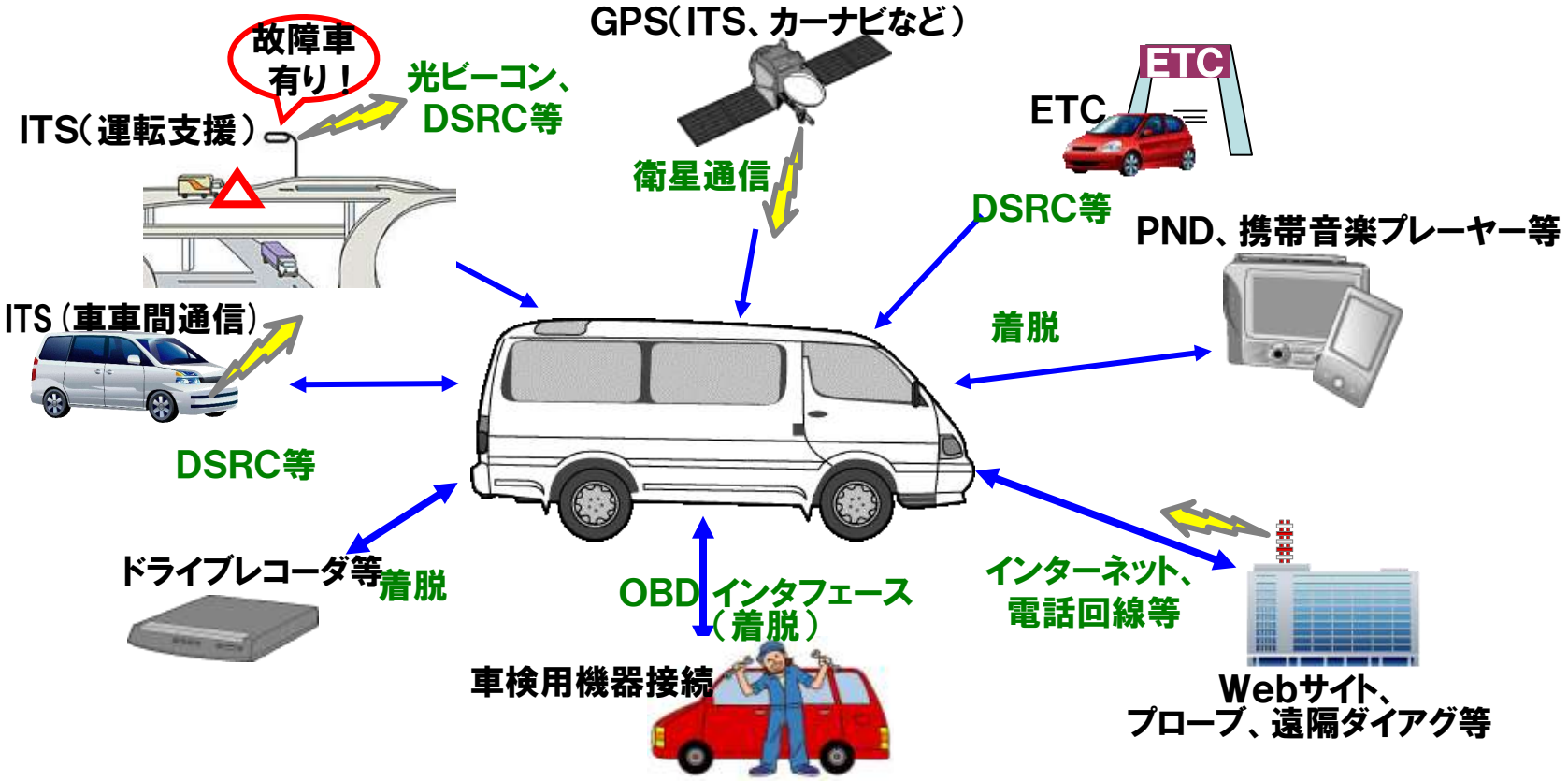
ネットワークで広がる情報家電の世界

- 情報家電の全体像が分からない
  - 何がつながるか、どのような情報が来るか、それらは信頼できるか
  - どのような情報が出て行くか、どのように利用されるか



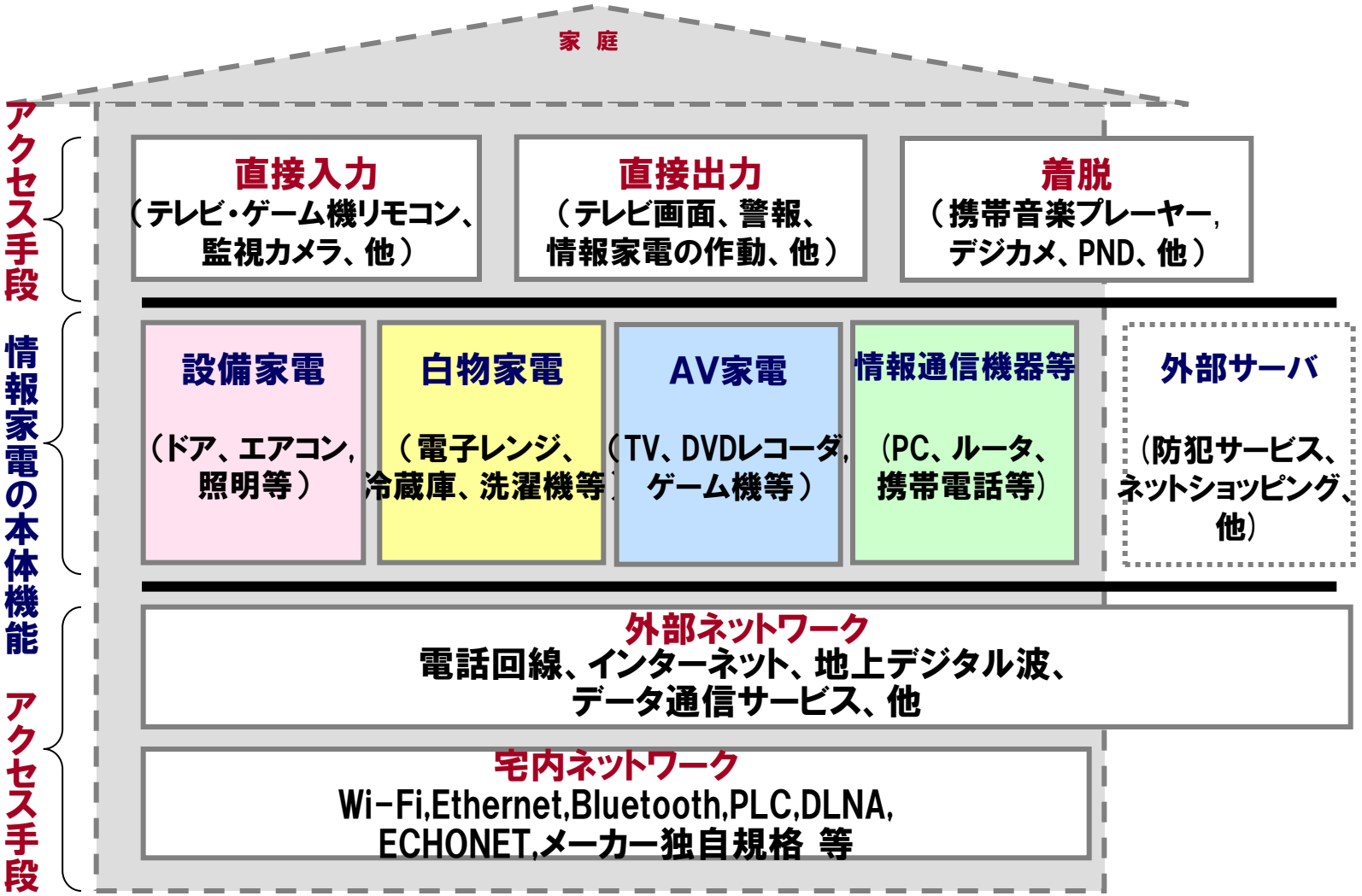
ネットワークで広がる自動車の世界

- 自動車の全体像が分からない
  - 何がつながるか、どのような情報が来るか、それらは信頼できるか
  - どのような情報が出て行くか、どのように利用されるか



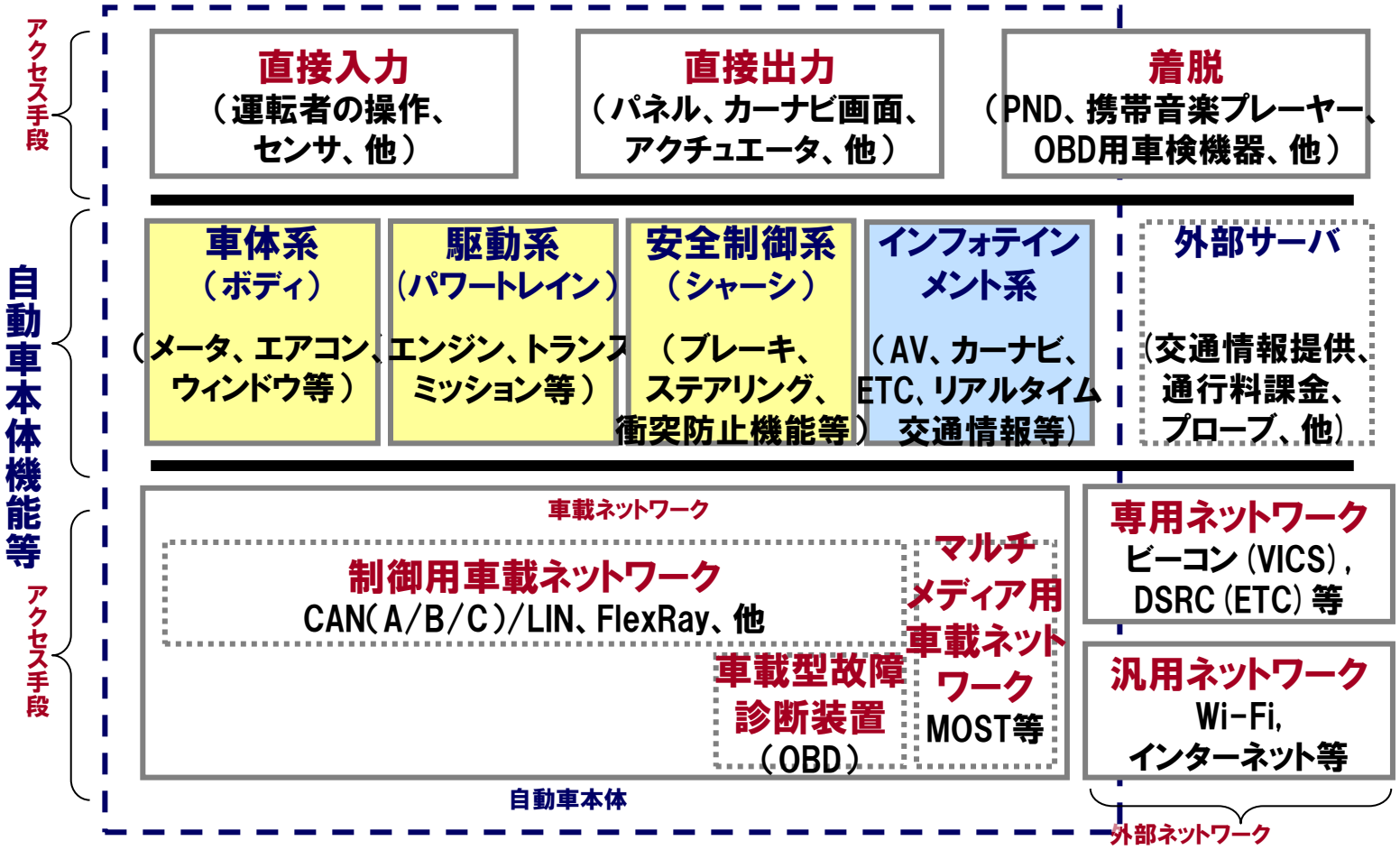
情報家電の全体像（フレームワーク）

- 委員へのヒアリング、研究会での審議等により、全体像を策定



自動車の全体像（フレームワーク）

- 委員へのヒアリング、研究会での審議等により、全体像を策定



守るべき対象（情報等資産）

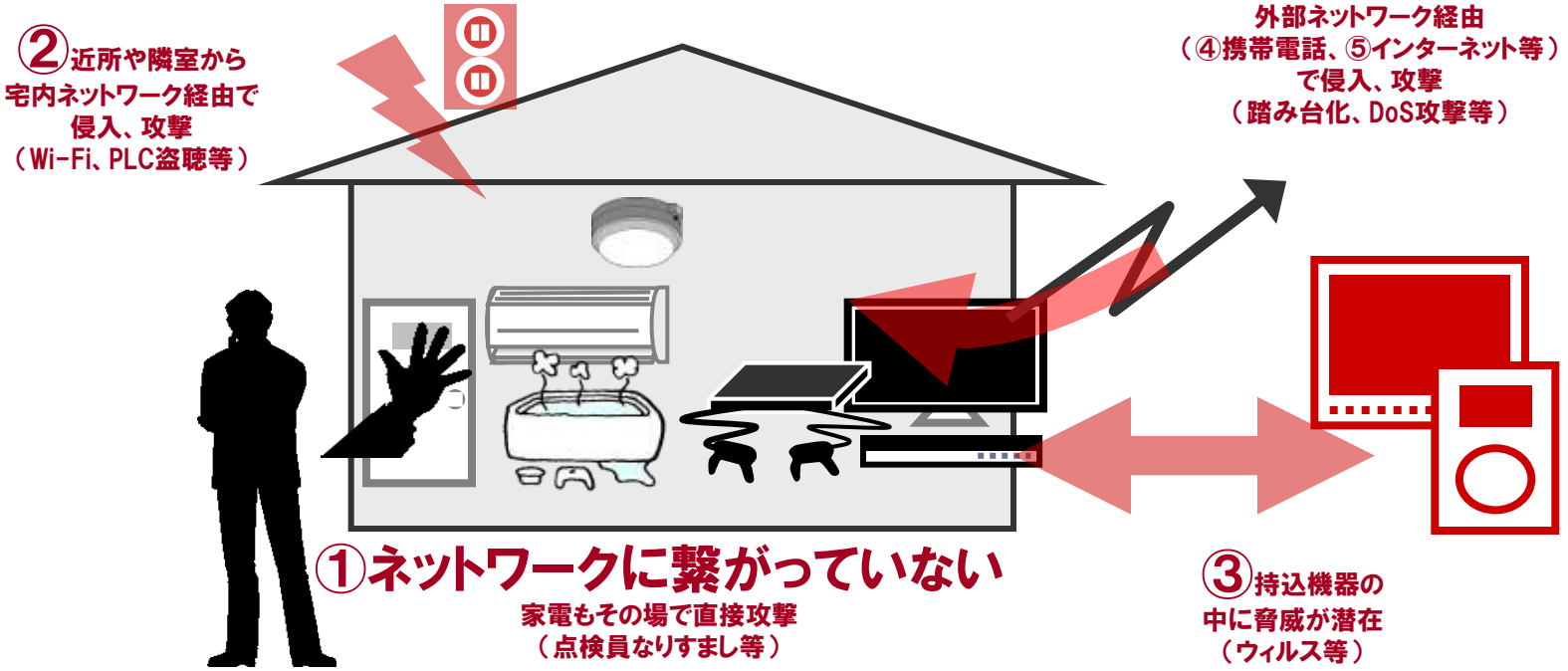
- 従来の情報資産の定義：情報システム、ハードウェア、ソフトウェア、データ、ノウハウ・社会的信用（IPA　Webページより）

- 守るべき対象は、情報家電や自動車上の情報資産だけでなく、組込み機器から外部に出て行く情報、ネットワークを介したサービス、さらには組込み機器本体までを含める。

- これらを総括して、「情報等資産」と呼ぶ。

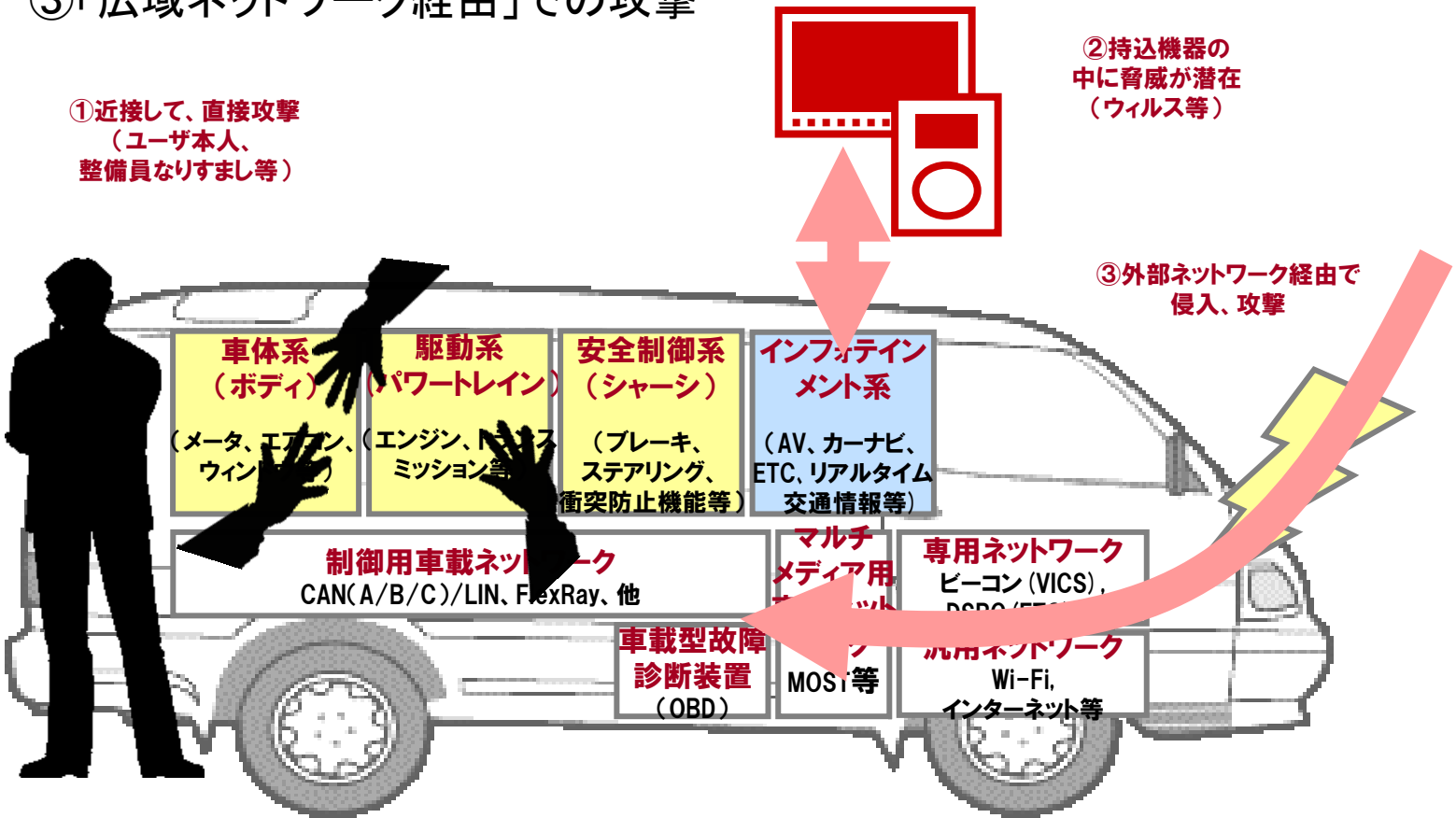
情報家電に対する脅威（情報家電周辺）

- 情報家電本体に対する攻撃を、以下の5パターンに分類
  - ①「直接、入出力」により攻撃
  - ②「宅内ネットワーク経由」での攻撃
  - ③「持込機器経由」での攻撃
  - ④「広域ネットワーク（電話回線）経由」での攻撃
  - ⑤「広域ネットワーク（インターネット）経由」での攻撃



自動車に対する脅威（自動車周辺）

- 自動車本体に対する攻撃を、以下の3パターンに分類
  - ①「近接」での攻撃
  - ②「中間（持込機器着脱等）」での攻撃
  - ③「広域ネットワーク経由」での攻撃



情報家電に対する脅威の例（情報家電周辺）

IPA®

情報家電分類 / アクセス経路	設備系	白物系	AV系
直接、入出力	・居住者なりすましによる攻撃（ドア錠等） ・点検員なりすましによる外部アクセス用設定情報の詐取（ホームゲートウェイ）	研究会では特に重要な脅威が挙げられていない	・家電店員による外部アクセス用設定情報の漏えい（Webカメラ等）
無線LANやPLC等で宅内で繋がる	・宅内ネットワーク経由で侵入、乗っ取り（ホームゲートウェイ） ・盗聴による個人情報漏洩（宅内ネットワーク上）	・宅内ネットワーク経由で侵入しOS・アプリケーションを改ざん ・盗聴による個人情報漏洩（宅内ネットワーク上） ・中古家電でウィルス感染（同）	・宅内ネットワーク経由で侵入しOS・アプリケーションを改ざん ・盗聴による個人情報漏洩（宅内ネットワーク上） ・中古家電でウィルス感染（同）
家庭に持ち込んでPCと繋がる	現状では対象が少ない		・着脱機器によるウイルス感染 ・持ち出した家電の盗難、情報漏洩（着脱機器上） ・コンテンツの違法コピー（同）
電話回線で外部と繋がる	研究会では特に重要な脅威が挙げられていない		
インターネットで外部と繋がる	・乗っ取り、踏み台 ・通信機能の停止（DoS） ・OS・アプリケーション改ざん（情報家電）	・乗っ取り、踏み台 ・通信機能の停止（DoS） ・OS・アプリケーション改ざん（情報家電）	・乗っ取り、踏み台 ・通信機能の停止（DoS） ・OS・アプリケーション改ざん（情報家電）

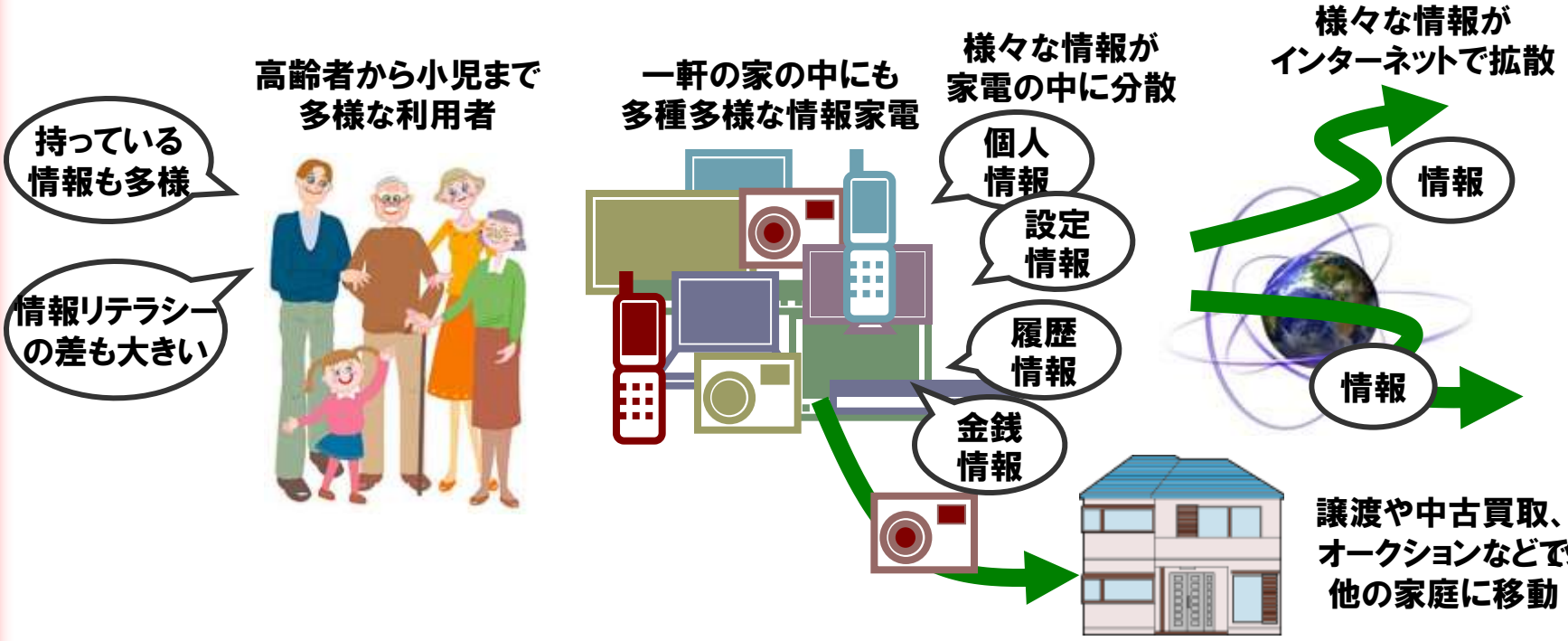
自動車に対する脅威の例（自動車周辺）

自動車機能分類 ＼ アクセス経路		制御	インフォテインメント
		セーフティ上クリティカル ⟷ セーフティ上影響小	損害大（金銭、個人情報等） ⟷ 損害小
近接		不正ECU取付け パラメータ改ざん プログラム改ざん （駆動系ECU） 他人のETCカードに成りすまし	個人情報の吸い出し、 プロファイリング、 プログラム改ざん （エンタメ系ECU）
中間（持込機器着脱等）		運転情報の破壊、改ざん、漏洩 （ドライブレコーダ）	・持込機器からエンタメ系ECUへのDoS攻撃、無線へのDoS攻撃 持込機器からウィルス感染
広域ネットワーク経由	専用	サーバなりすましによる 虚偽メッセージの表示 （車車間（路車間）通信）	エンタメ系ECU・ 車載ネットワーク へのDoS攻撃
	汎用	研究会では 特に重要な脅威が 挙げられていない	決済情報フィッシング・盗聴 虚偽情報の表示、ウィルス感染、インフォテインメント系ECUや通信機能へのDoS攻撃

情報家電と自動車の
セキュリティ対策の方向性

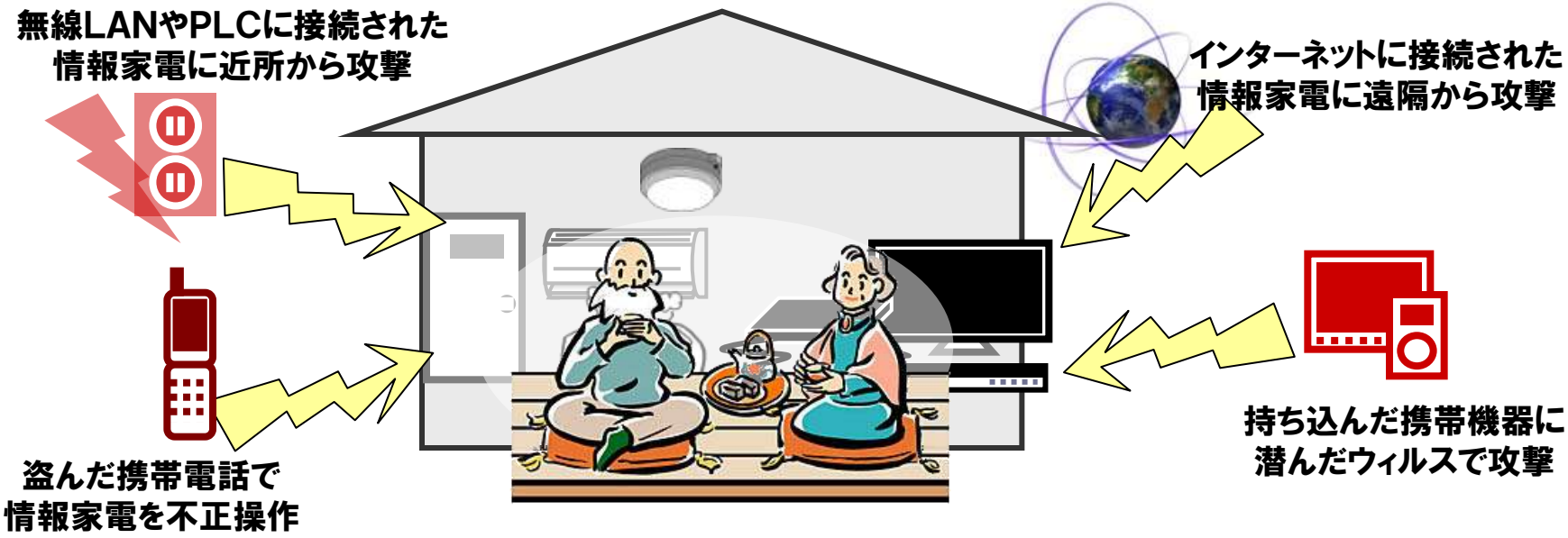
情報家電における脅威の特徴（1）

- 情報家電の脅威が拡大する可能性
  - a）情報リテラシーが充分でない利用者が存在する可能性
  - b）情報等資産の多種多様化、範囲拡大の可能性
  - c）オークションや譲渡による情報の漏洩の可能性
  - d）セキュリティ対策が不十分な情報家電が混在する可能性
  - e）何が繋がり、誰が利用しているか、把握できなくなる可能性



情報家電における脅威の特徴（2）

- ネットワーク経由による脅威の可能性
  - f）着脱機器やテレメトリングによる情報の拡散の可能性
  - g）偽のダウンロードパッチを受け入れてしまう可能性
  - h）情報家電経由でインターネットの不正サイトにアクセスしてしまう可能性
  - i）宅内ネットワークのセキュリティ設定が行われていない可能性



気がつかないうちに、様々な脅威の可能性

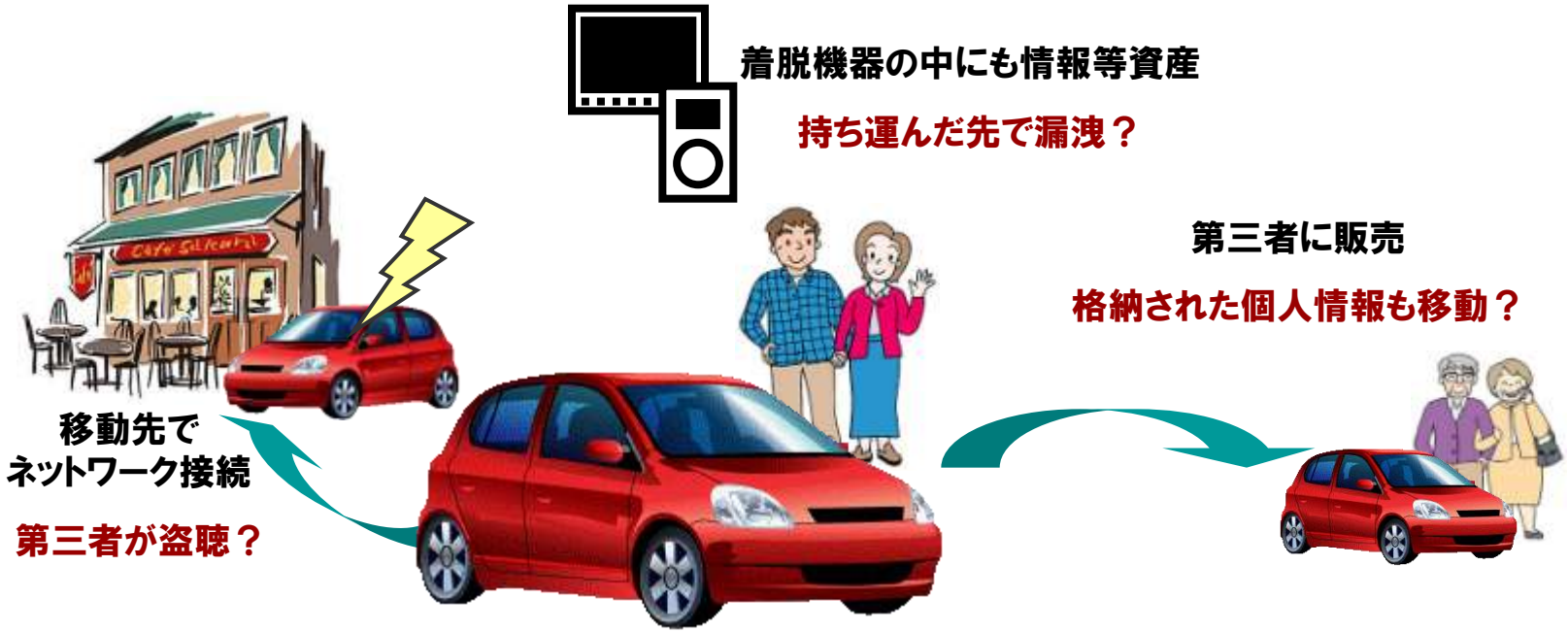
情報家電における脅威の特徴(3)

- 直接的な攻撃の可能性
  - j)第三者の侵入による不正な設定変更の可能性
  - k)メーカ点検員になりすました第三者による不正な設定変更の可能性
  - l)利用者自身による改造の可能性
- 重大な被害が減少しない可能性
  - m)重大な被害が減少しない可能性

家の中に入り込むのは、意外に簡単？

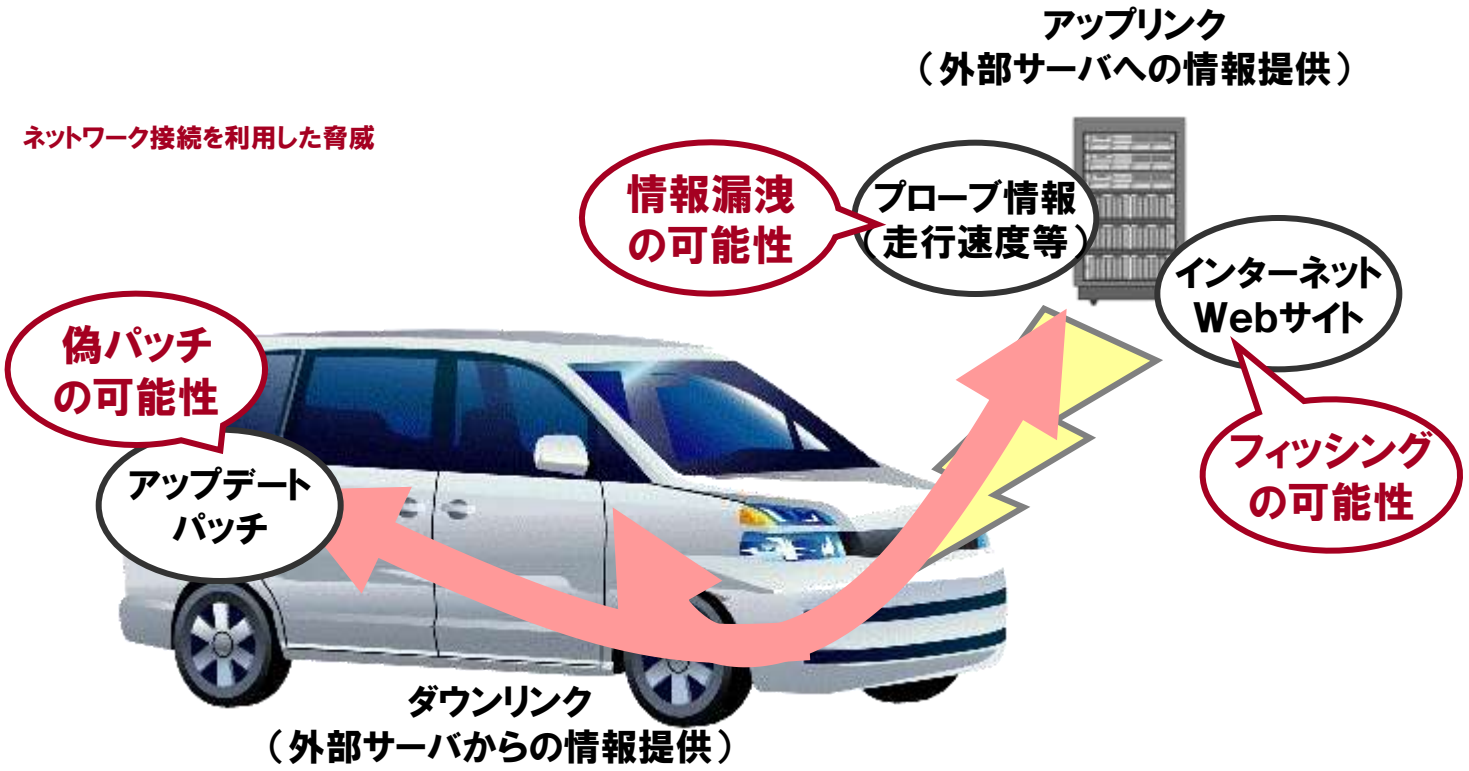
自動車における脅威の特徴（1）

- 自動車の脅威が拡大する可能性
  - a）情報等資産の多種多様化、範囲拡大の可能性
  - b）オークションやレンタルによる情報の漏洩等の可能性
  - c）セキュリティレベルが低い組込み機器が混在する可能性
  - d）移動先で何が繋がり、誰が利用しているか分からない可能性



自動車における脅威の特徴（2）

- ネットワーク経由による脅威の可能性
  - e）着脱機器やプローブによる情報等資産の拡散の可能性
  - f）偽のダウンロードパッチを受け入れてしまう可能性
  - g）カーナビ経由でインターネットの不正サイトにアクセスしてしまう可能性



自動車における脅威の特徴（3）

- 直接的な攻撃の可能性
  - h）駐車場等での第三者による不正な改造の可能性
  - i）メーカ点検員になりすました第三者による不正な改造の可能性
  - j）利用者自身による改造の可能性

窓を割ってPNDを盗む

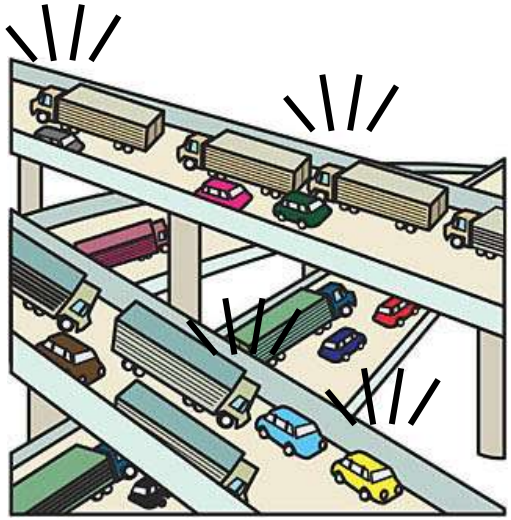
ECUを不正書き換え、
不正なECUを追加

屋外に置かれていると攻撃しやすい

自動車における脅威の特徴（4）

- 重大かつ広範囲の被害の可能性
  - k）重大な被害の可能性
  - l）社会的混乱を招く可能性

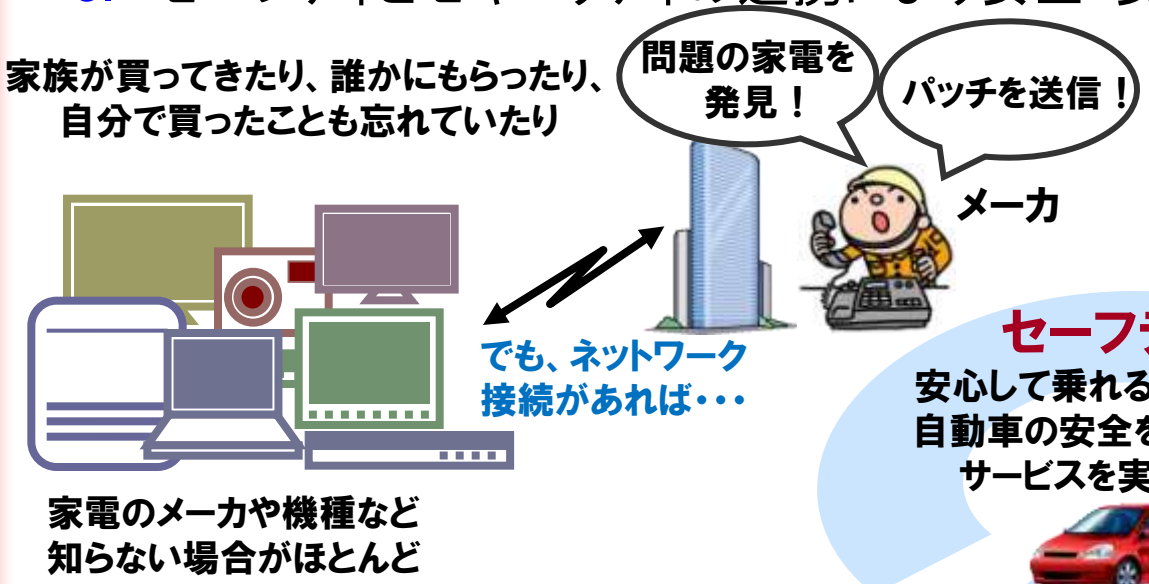
身体への被害の可能性も



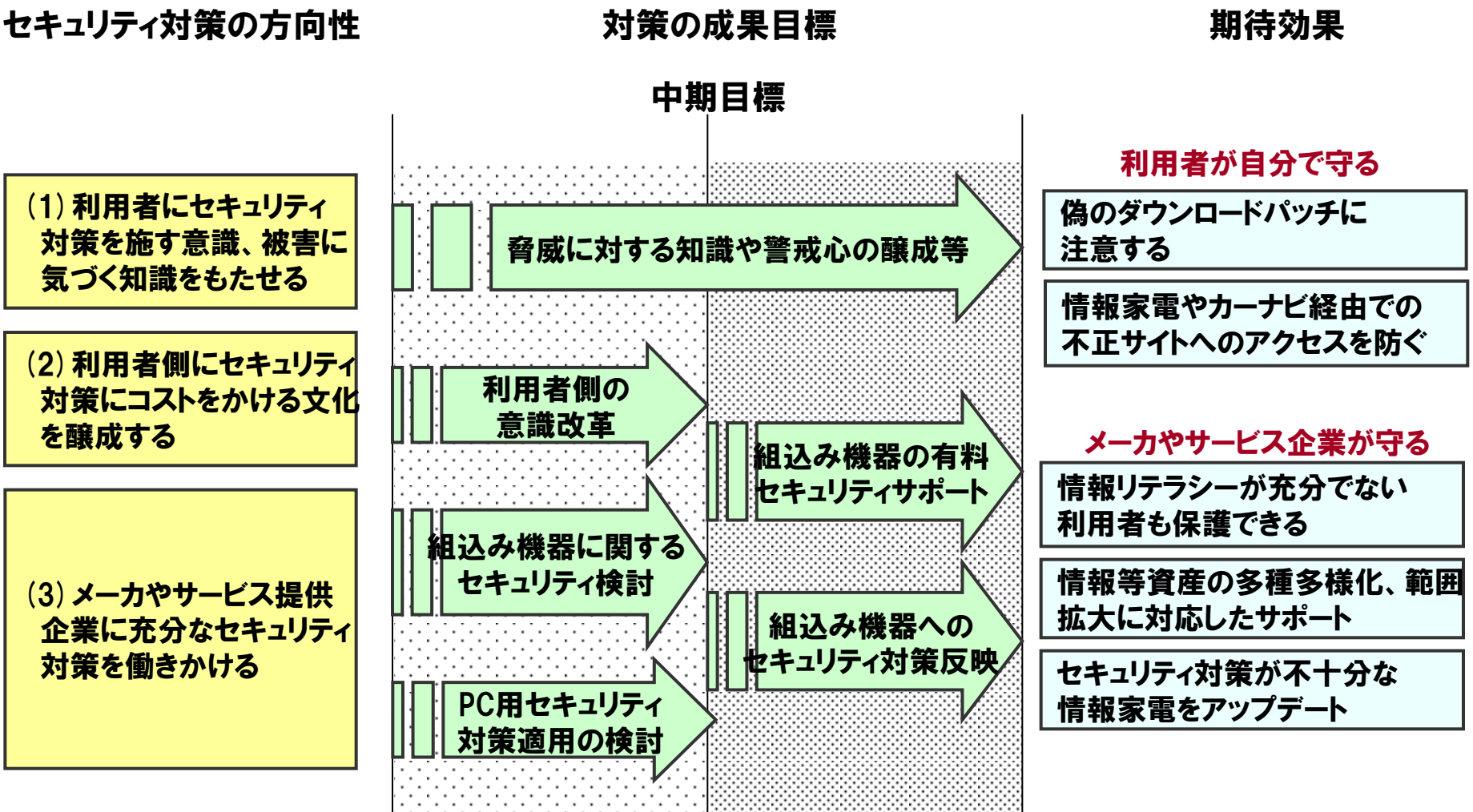
偽の情報で日本中が大渋滞
（「地震が来る」等のデマなど）

情報家電と自動車のセキュリティ対策の方向性

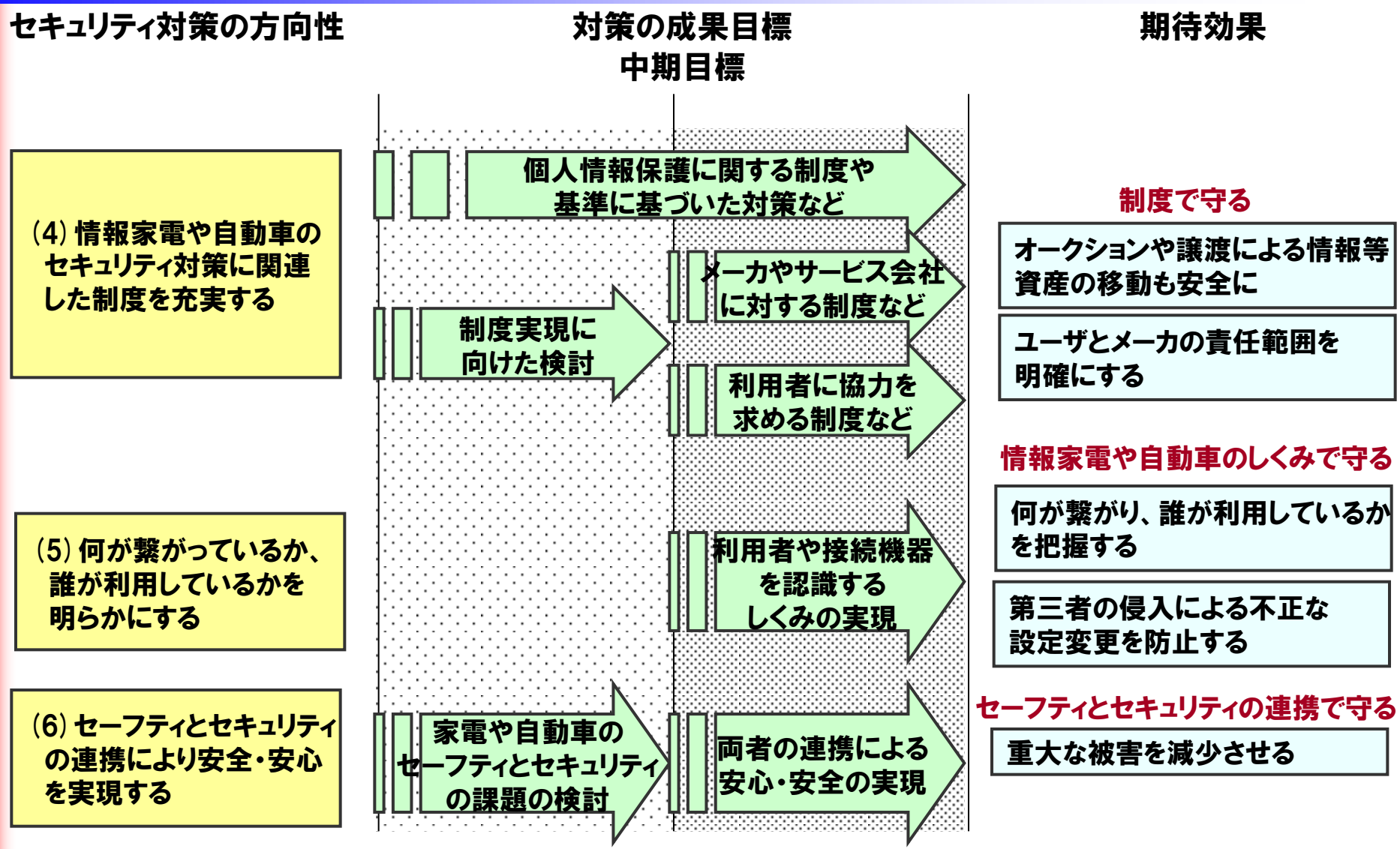
1. 利用者にセキュリティ対策を施す意識、被害に気づく知識をもたせる
2. 利用者側にセキュリティ対策にコストをかける文化を醸成する
3. メーカやサービス提供企業に充分なセキュリティ対策を働きかける
4. 情報家電のセキュリティ対策に関連した制度やしくみを充実する
5. 何が繋がっているか、誰が利用しているかを明らかにする
6. セーフティとセキュリティの連携により安全・安心を実現する



情報家電や自動車のセキュリティ対策の方向性(1/2)



情報家電や自動車のセキュリティ対策の方向性(2/2)



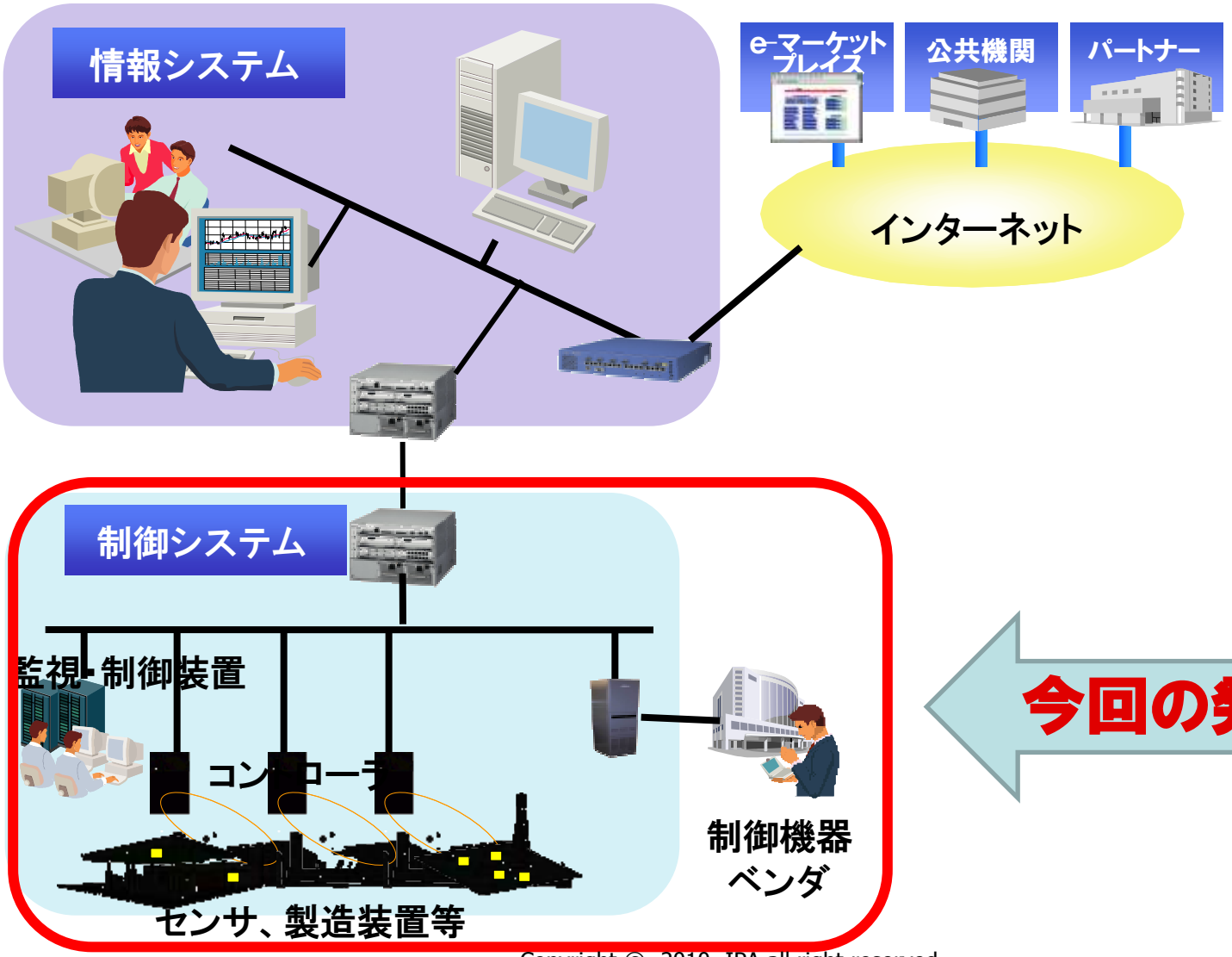
セキュリティに関する取り組み状況の比較

- 自動車、情報家電ともセキュリティに関する取組みはこれから

	オフィスの情報機器	自動車	情報家電
セキュリティやセーフティを保つための仕組みや制度	セキュリティポリシーや社内規則に基づき、情報システム部門の管理担当者が、チェック。	車検（道路運送車両法）等で定期的な検査が義務付けられている。	特になし。ただし2009年4月より「長期使用製品安全点検制度」が施行。
セキュリティやセーフティに料金を支払う慣習	情報システム管理や、セキュリティ・ソフトウェアにコストが必要であることは一般的。	車検、点検等に費用がかかることは、自動車の所有者には認知されている。	特になし。
利用者教育の仕組み	社員は業務の一環としてセキュリティ対策に必要な知識を学習することが一般的。	運転免許取得時時に、知識および技術の習得が義務付けられている（道路交通法）。	特になし。
個人的な改造に対する制限	会社の物品であり、個人的な改造は許可されないことが一般的。	合格基準を満たさない改造を行うと、車検は通らない。	所有物については自由（保証を受けられなくなる場合はある）

制御システムセキュリティ

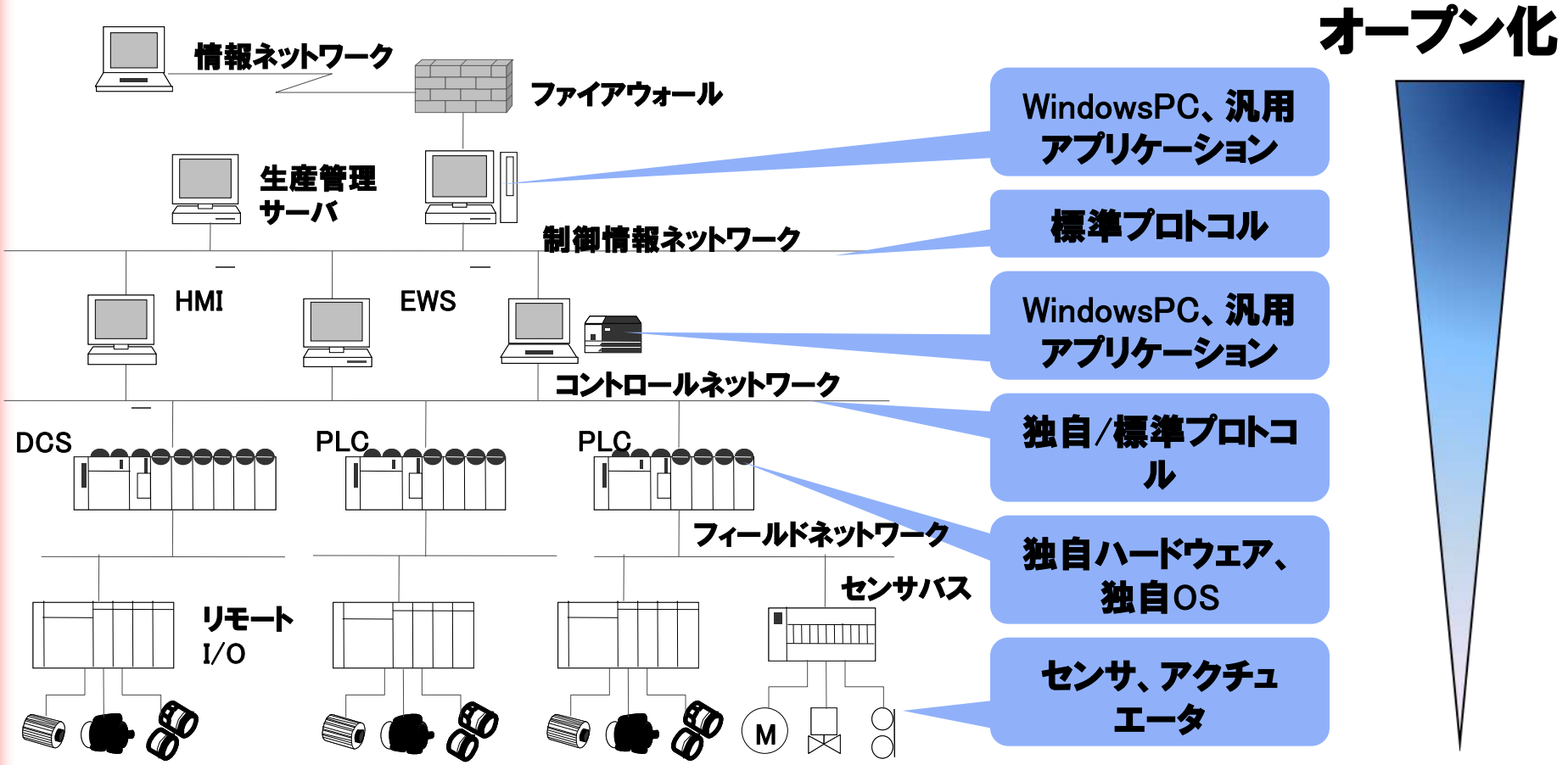
2009年度
制御システムのセキュリティ調査



今回の発表内容

制御システムの現状

「オープン化」:汎用製品＋標準プロトコル



制御システムのセキュリティ課題

【課題１：オープン化に伴う脆弱性リスクの混入】

- **汎用製品、標準プロトコルネットワーク採用により、脆弱性リスク、ワームなどのウイルスの侵入や、機密情報漏えいのおそれ**

【課題２：製品の長期利用に伴うセキュリティ対策技術の陳腐化】

- **制御システムは通常10～20年使用。セキュリティ対策も最新ではない可能性**

【課題３：可用性重視に伴うセキュリティ機能の絞込み】

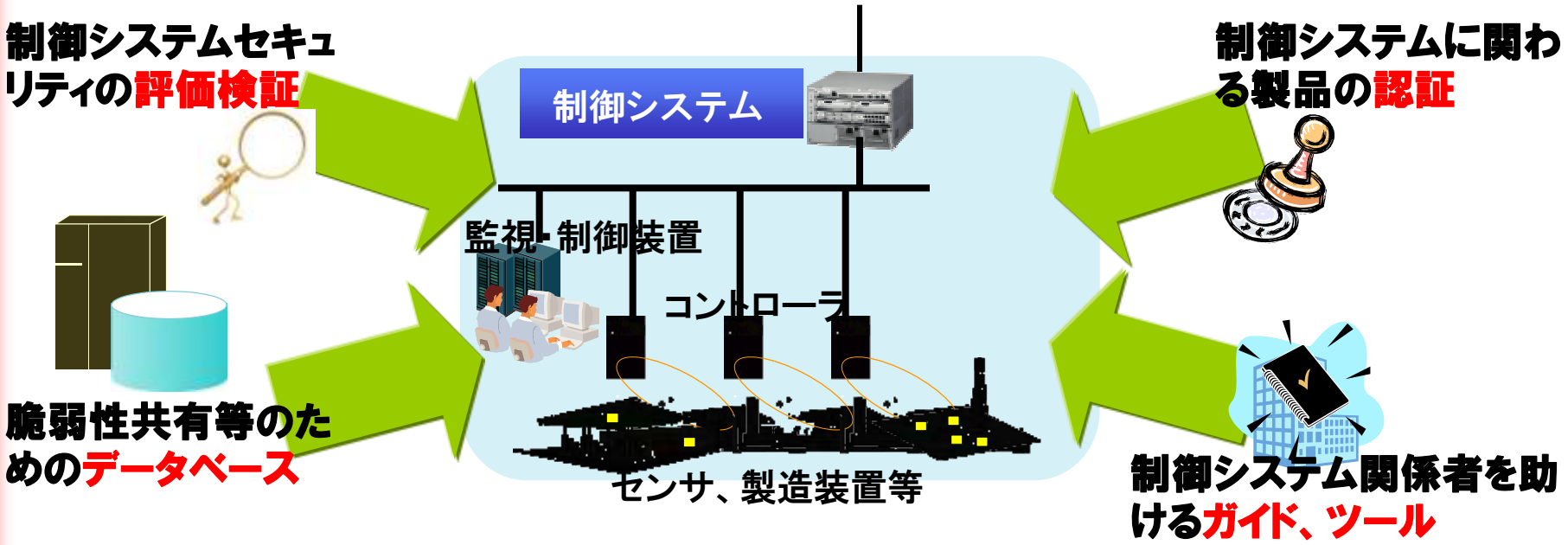
- **可用性重視の観点から、一般的に、システム上の負荷となるウイルス監視やチェックプログラムの自動更新せず**

	制御システム	情報システム
セキュリティ優先順位	A.I.C（可用性重視）	C.I.A（機密性重視）
セキュリティの対象	モノ（設備、製品） サービス（連続稼動）	情報

資料：IPA「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」より抜粋

2009年度
制御システムのセキュリティに関わる取組みのポイント

欧州や米国の制御システムセキュリティについて、四つの視点から調査を行い、日本の制御システムに必要とされる施策について提言。



取組み状況調査結果のまとめ

● 日米欧の取組み状況比較（１／２）

施策	欧州	米国	日本
ガイド・ツール	・推奨されるプラクティス集（Good Practice）を公開（英国CPNI、オランダTNO水セクター向け） ・セキュリティ基準を策定（ドイツBSI standard 100-1～4） ・自己評価ツールを配布（英国CPNIのSSAT） ・情報共有の仕組みを整備（欧州のE-SCSIE、英国CPNIのSCSIE、スウェーデンSEMAのFIDI-SC）	・推奨されるプラクティス集（Good Practice）を公開（DHS/CSSP） ・セキュリティ基準を策定中（NISTのSP800-82およびISAのISA99 100、NERCのCIP002～008） ・自己評価ツールを配布（DHS/CSSPのCS2SATおよびその後継のCSET） ・情報共有の仕組みを整備（2008年までPCSF、2009年よりICSJWG）	・「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定に当たっての指針」（2007年6月　情報セキュリティ政策会議）などに基づき分野ごとに安全基準を設定 ・独自のツール類は少ない
評価・検証	・ヨーロピアンテストベッド取組みの一部としてIPSCではSCADAテストベッドを開設しセキュリティ検証を実施	・DOEがSCADAテストベッドを開設しセキュリティ技術の開発、検証を実施	・電力中央研究所で制御システムセキュリティの評価・検証を行っているが、事業者または制御機器ベンダー内で共通的に利用可能なセキュリティテスト環境等は少ない

取組み状況調査結果のまとめ

● 日米欧の取組み状況比較（2／2）

施策	欧州	米国	日本
データベース	・CPNIが制御システムセキュリティプログラムのひとつであるSCSIEを運営しており、インフラ運用者間での脆弱性情報共有カンファレンスを定期的に実施 ・制御機器ベンダーが脆弱性関連情報をユーザグループに直接通知、対策し、ユーザグループ内での解決を図る ・TNOがインシデント情報のデータベースを構築	・US-CERTが制御システムの脆弱性関連情報のデータベースを持つが15～20件と少数 ・RISIが制御システムのセキュリティ事象データベースを運用 ・制御機器ベンダーが脆弱性関連情報をユーザグループに直接通知、対策し、ユーザグループ内での解決を図る	・JPCERT/CCが制御システムの脆弱性関連情報の収集、公開を実施。但し件数は少ない ・IPAが脆弱性対策情報DB（JVN iPedia）を運用
認証	・TUViTが複数の基準を顧客要件により組み合わせ、制御システムの監査・認証を実施	・製品認証機関による認証製品を利用することで、一定のセキュリティレベルが担保されていることを確認、保証可能	ー

調査分析結果を踏まえて（1/2）

● 欧米で脆弱性対策への取組みが拡大中

- ガイド・ツールに関しては、セキュリティ基準の策定、推奨プラクティス集の公開、自己評価ツールの配布を実施
- 評価・検証に関しては、SCADAテストベッドの開設によるセキュリティ検証を実施
- データベースに関しては、制御システムのインシデント情報のデータベース構築・公開を開始
- 認証に関しては、民間主導によるセキュリティ監査・認証サービスが行われており、ISA ISCIによる標準化が進展中
- 制御システムセキュリティ強化に向けた認識向上や関係者間の信頼関係構築により施策の普及を促進させるための、情報共有コミュニティを設置し運用

調査分析結果を踏まえて(2/2)

● 日本としても具体的な対策を進める必要性あり

- 日本独自のガイド・ツール類の提供はまだ少なく、テスト環境も一部セクターのみ。脆弱性対策情報(JVN iPediaなど)のデータベースはあるがインシデンツを含む幅広い制御システムセキュリティの情報収集はこれから
- 制御システムのセキュリティ対策のあり方は日本と欧米とで必ずしも同一ではなく、日本の重要インフラにとっての優先度を判別した上で、最も効果のある課題から始めていくことが必要
- セキュリティ規格標準化の動向に関しては、産業の国際競争力強化の観点からも日本独自の規格ではなく、国際標準への対応を念頭に推進することが重要
- 欧米での制御システムセキュリティへの取組みも、まさに現在進行形であり、今後の動向を注視しながらアジアの展開も視野に幅広く対応
- 制御システムセキュリティの脆弱性対策においては、関係者の認識改善と対策の実効性向上の観点からも、官民連携による情報共有の仕組みづくりが鍵

まとめ

全体まとめ　その1(1/2)

制御システムと自動車システムの課題

オープン化の方向にある制御システムと自動車システムで検討されたセキュリティ課題についてのまとめ

	制御システム	自動車システム
課題1	**オープン化に伴う脆弱性リスクの混入** ・汎用製品、標準プロトコル採用により、脆弱性リスク、ワームなどのウィルス進入、機密情報朗詠の恐れ	○同じ課題が当てはまる ・ウィルス進入や個人情報漏洩の脅威は昨年指摘されている
課題2	**製品長期利用に伴うセキュリティ対策陳腐化** ・制御システムは通常 10-20年使用。セキュリティ対策も最新ではない可能性	○同じ課題が当てはまる ・自動車のライフサイクルは、およそ 10年前後。常に最新の対策を施しておくことは困難な可能性
課題3	**可用性重視に伴うセキュリティ機能絞込み** ・可用性重視の観点から、一般的にシステム上の負荷となるウィルス監視やチェックプログラムの自動更新せず	○同じ課題が当てはまる ・機能安全性(可用性、完全性)と低コスト重視の観点から、ウィルス監視機能などは搭載機能順位が低くなる

制御システムのセキュリティ課題と類似性は高い。
制御システムにおけるセキュリティ対策の取り組みは、
自動車業界での取り組みの参考になると考える

全体まとめ　その２（2/2）

特徴比較

- **制御システムと自動車システムの特徴と位置づけ**

セキュリティ上、必要となる要件	情報システム	制御システム	自動車システム
技術のサポート期間	3-5年	20年以上	一般的に10年前後
パッチ提供サイクル	頻繁・定期的	ベンダごとに不定期、長期間隔で実施（公表値なし）	法廷点検、定期点検時などで実施可能（実施状況は不明）
システム上流れるデータの処理速度	データ受け取り遅延が致命的な被害となるケースは少ない	システム／機器制御にはリアルタイムのデータ受け取りが不可欠	稼働中のシステム／機器制御にはリアルタイムなデータ受け取りが不可欠
可用性（Availability）	再起動は許容可能	24時間365日の安定稼動が不可欠（再起動不可）	一旦停止しエンジン再始動は可能
セキュリティに関する意識	民間企業、公的機関との意識行き渡り、対策が定義されている	発展途上にあり未成熟。情報システム技術の適用で対策するケースもある	開発メーカー、利用者とも未成熟。対策への取り組みも顕在化していない
被害の結果	金銭的損失、プライバシー被害	人命損失の可能性	金銭的損失、プライバシー被害、人命損失の可能性

自動車システムの特徴は制御システムにより近い。
したがって、制御システムにおけるセキュリティ対策の取り組みは、
自動車業界での取り組みの参考になる

今後の検討課題

- **利用者、メーカ、サービス事業者等の情報リテラシー向上**
  - 利用者の情報セキュリティのリテラシー向上、対策コストの必要性の理解促進。
  - リテラシー向上が難しい利用者を誰がどのように保護するかの方策検討。
  - 自動車関係企業に対するガイドライン、利用者向け説明資料の整備、配布。
- **状況の可視化と役割分担の明確化**
  - 不正な機器の接続や不正利用の発見・対策を行う可視化のしくみの実現。
  - セキュリティ上の脅威に対する役割分担や、自動車や家の「物理的なバリア」と「ネットワーク上のバリア」のあり方の明確化。
- **ライフサイクルを通じた検討**
  - 設計段階からのセキュリティ検討、廃棄時の個人情報やセキュリティ機能の適切な消去などライフサイクルを通じた検討。
- **協力および提言の場の確立**
  - 利用者、メーカ、サービス事業者、セキュリティ技術者が協力し、セキュリティ対策を検討するとともに、法制度の整備について国に提言していく場の設置。
- **ネットワークの両側でのセキュリティ対策の実施**
  - 機器側（メーカ側）とサービス側（サービス提供企業側）の双方でのセキュリティ対策による、より確実な脅威の解消。

安全な組込みシステム社会にむけて

- 課題解決に向けた提案
  - 組込みシステムの特徴（省電力、低リソース、等）を考慮した上で、従来の情報システムのセキュリティインシデントやその対策についてのセキュリティに関する考察
  - 組込みシステム間の相互接続や融合時の複合的な環境でのセキュリティに関する考察
  - 利用者の個人情報、金銭被害に繋がる情報、さらに人命に繋がる情報等、取扱う情報資源の特徴の観点を考慮に入れた考察
  - 組込みシステム開発者・技術者のセキュリティを含めた意識共有の為の活動

様々な観点から課題を検討し、組込み開発者やユーザ、事業者、セキュリティ研究者といった組込みシステムに係る方々の連携で、課題の解決に向けて取り組む必要がある。

組込みセキュリティに対するIPAの活動

2007年5月10日公開
組込みシステムの脅威と対策に関する
セキュリティ技術マップの調査

2008年1月29日公開
複数の組込み機器の組み合わせに
関するセキュリティ調査

2009年3月10日公開
自動車と情報家電の組込みシステムの
セキュリティに関する調査

2010年4月15日公開
国内外の自動車の情報セキュリティ動向と
意識向上策に関する調査

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

2009年3月30日公開
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年3月30日公開
制御システムセキュリティの信頼性と
推進施策に関する調査

**組込みシステムの
ライフサイクル**

企画	開発	運用	廃棄

2006年5月19日公開
現場技術者向け「40のポイント集」
経営者向け「組込みセキュリティ資料」

報告書（第四版）、検証ツール：2009年1月8日公開
TCP/IPに係る既知の脆弱性検証ツール
報告書、検証ツール：2009年4月23日公開
SIPに係る既知の脆弱性検証ツール

2007年4月25日公開
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）
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
（担当：小林・董島・中野・長谷川）