エッジデバイスのセキュリティを評価認証するための スキームの実現に向けて

国立研究開発法人　産業技術総合研究所
サイバーフィジカルセキュリティ研究センター
セキュリティ保証スキーム研究チーム 研究チーム長
吉田 博隆

IoT向けエッジデバイスの急速な普及

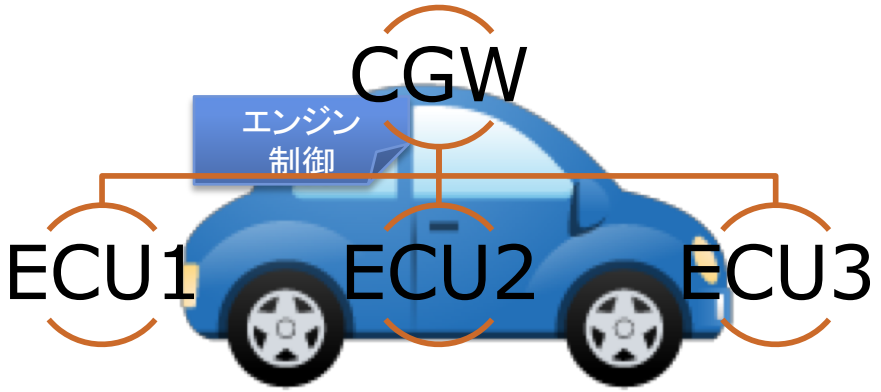
90年代 → 2018年

IT製品・情報機器の普及 → IoT時代

あらゆるモノがネットワークにより繋がることによって新しい価値を創造する情報社会

- パソコン
- ICカード

- 自動車、(ナビ等)
- ロボット
- 医療機器
- 産業制御機器



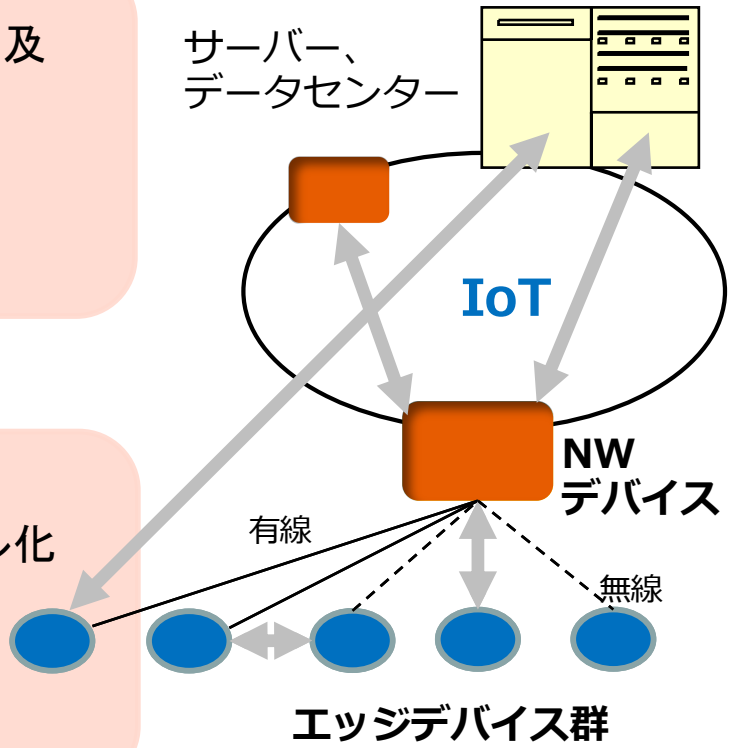
IoTとサプライチェーンにおける脅威

IoT

- 新しいサービス提供が期待されるIoTの急速な普及
- 既存IoT機器の大量マルウェア感染
  - Miraiウイルス
- IoT末端のエッジデバイスがアタックサーフェスに

サプライチェーン

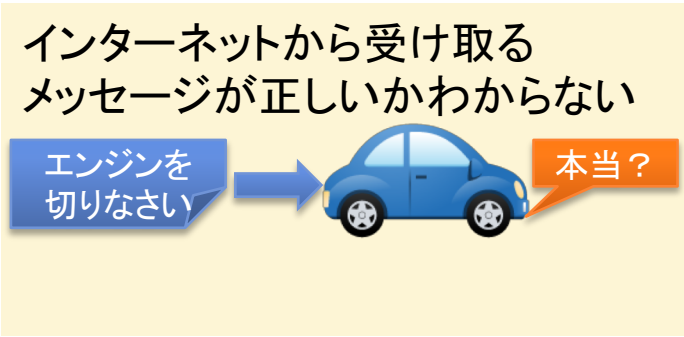
- 多様な事業者や多くのフェーズを含みグローバル化
- モノ自体のすり替えや改ざんがセキュリティ課題
- 不正な半導体部品の潜入等が問題に



IoTエッジデバイスにおけるセキュリティ確保の重要性

IoTエッジデバイス向け軽量暗号の標準化

- 高い安全性をもちつつ、IoTエッジデバイスの低リソース性をクリアする
- 暗号技術対象プラットフォームは、低コストマイコンや組み込みCPU（ARM, H8, H8S, SH-3等）
- 医療機器業界や自動車業界等のニーズを受け、IoTエッジデバイス向けとして、本技術の標準化もアクティブ
  - これらの技術開発と標準化で産総研は主導的立場



軽量暗号技術	用途	最適な実装形態	主な特徴	標準化状況
暗号利用技術 EAMD	データ秘匿・認証	ソフトウェア	低CPU負荷率（従来比: ～1/100）	ITU-T SG17 2017年規格化
ブロック暗号 CLEFIA,PRESENT	データ秘匿	ハードウェア	高速処理性（従来比: 1.5倍速）	ISO/IEC JTC1 SC27 2012年規格化
ストリーム暗号 Enocoro		ハードウェア	低消費電力（従来比: 1/10）	ISO/IEC JTC1 SC27 2013年規格化
ハッシュ関数 Lesamnta-LW	データ認証、乱数生成、署名、相互認証	ソフトウェア（8/16-bit H8（S））	低RAM使用量（従来比: 8割削減）	ISO/IEC JTC1 SC27 2016年規格化
ハッシュ関数 Spongent, Photon		ハードウェア	省回路規模（従来比: 1/10）	
MAC※方式 Chaskey, LightMAC 産総研	データ認証	ソフトウェア（32-bit ARM）	低CPU負荷率（従来比: 1/10）	ISO/IEC JTC1 SC27 2020年規格化予定

最適な実装形態	標準化状況
パスワード認証方式、2017年11月 産総研	ISO/IEC 11770-4 (2nd edition):
産総研の匿名パスワード認証方式、2017年8月 産総研	ISO/IEC 20009-4
産総研の二要素認証方式 産総研	ISO/IEC 11770-4:2017 Amendment 2

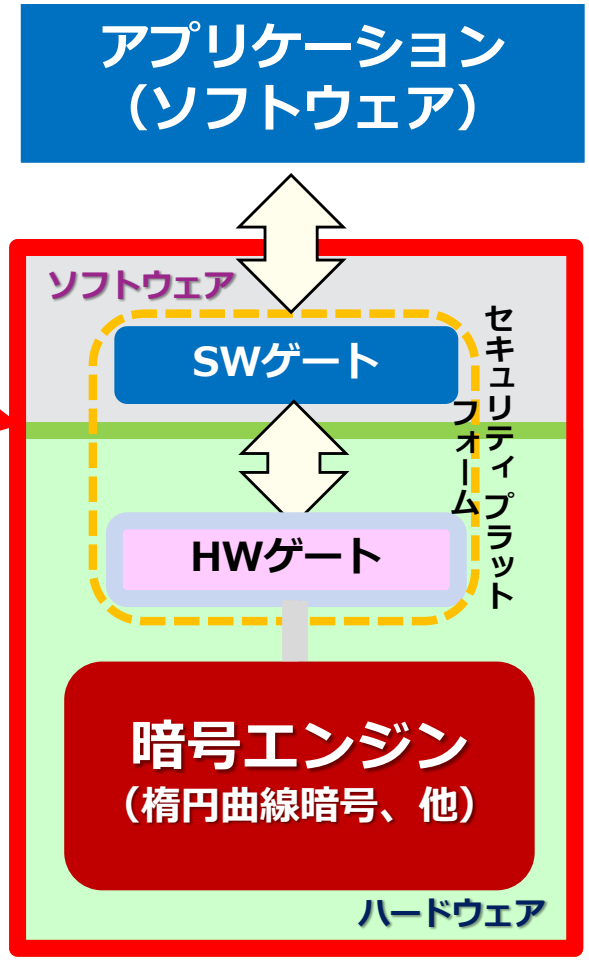
※MAC: メッセージ認証符号。メッセージを認証するための短い情報

最先端暗号実装技術の例*：SCU(Secure Cryptographic Unit)

エッジデバイスのセキュリティ搭載における課題
多様性と省リソース性
・センサorアクチュエータ, マイコンは搭載か
・OSは搭載か, 通信は有線or無線か, 電力供給は安定か

解決策

1. SCU （「軽く、速く、強い」暗号モジュール」）
   末端エッジデバイスで公開鍵暗号にセキュリティ対策を実現
2. 社会実装への導入分析
   モデルシステム（監視カメラシステム）を構築
3. さらに「強い」暗号モジュールのための基礎技術を研究
   ハードウェア上のトロイの木馬に対抗する新技術を提案



* www.nedo.go.jp/content/100863674.pdf

セキュリティの保証と評価の重要性

- 前掲の先端技術のアプリ・製品展開においては、IoTセキュリティ全体の取り組みが重要
  - 全体を見てレベル、バランス、漏れのなさを評価
- セキュリテイ保証とセキュリティ評価
  - セキュリティ保証：セキュリティ機能が間違いなく動作
  - セキュリティ評価：セキュリティ保証を確認
- セキュリティ機能を実装後、評価の主体は第三者であることが必要
  - 自己評価（対策の実施者や計画者）ではない
  - ミスや勘違いの防止、意図的な弱点の検出
- システム調達・構築する場合、採用ベンダー未定、複数ベンダーの可能性
  - セキュリティの仕様の記述に、普遍性・共通性・容易性が要求
  - 国際的な調達、セキュリティレベルの国境を超えた比較→国際規格の策定

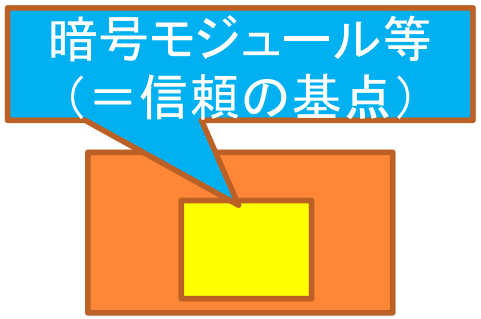
HWセキュリティ標準の類型

評価基準ISO/IEC 15408 CC(Common Criteria)が策定

- 暗号実装に着目した標準（CMVP=ISO/19790）
- 製品仕様に着目した標準（例：TPM，EMV・・）

エッジデバイスのセキュリティの評価認証に向けて

- 課題1：組込製品用チップの脆弱性分析技術の集約
- 課題2：暗号モジュール等のアプリケーション分野別セキュリティ要求のまとめ
- 課題3：セキュリティ保証スキーム運用の技術的支援と対象暗号モジュールの認定



新IoTアプリ
（監視カメラシステム等）

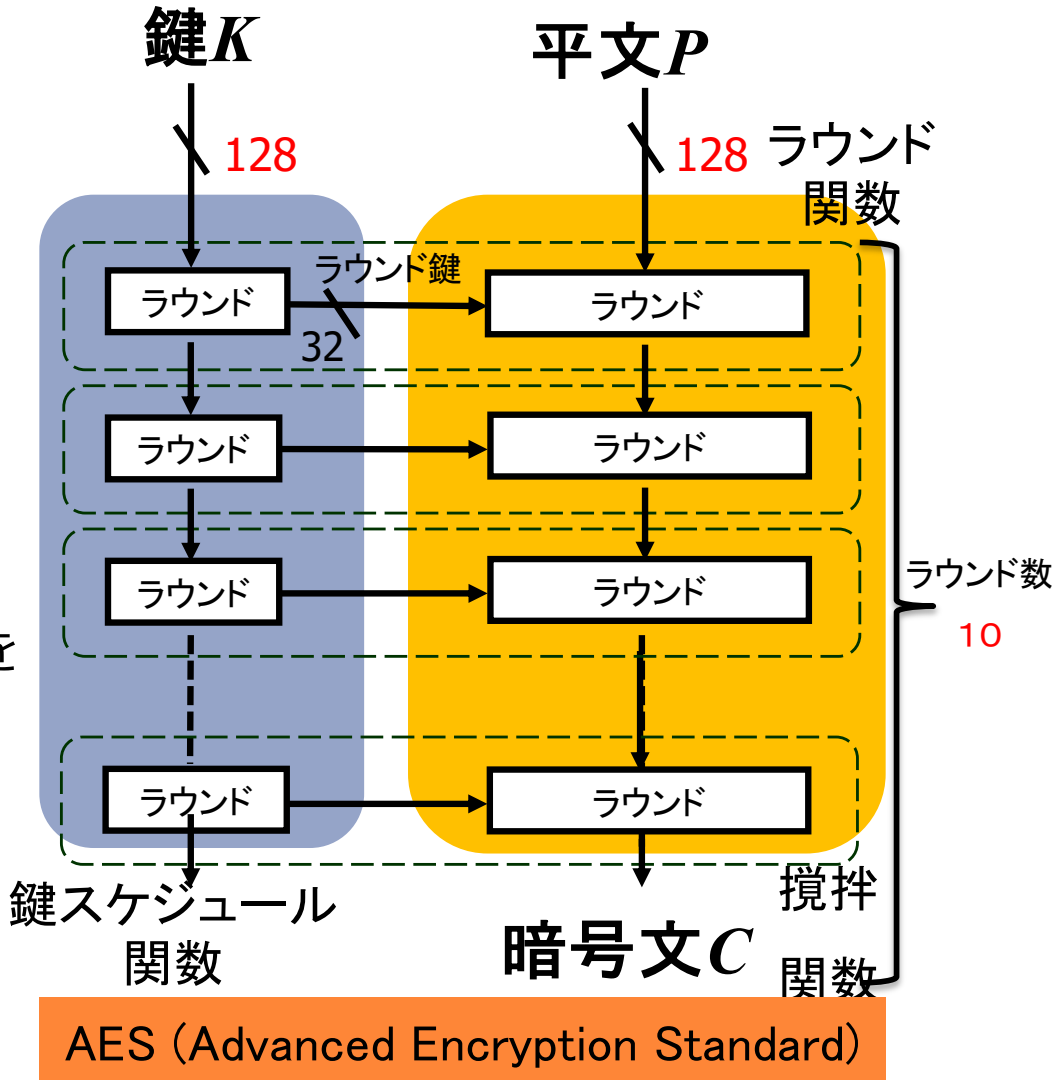
課題1:組込製品用チップの脆弱性評価技術の集約

- ICへの新たな攻撃の動向調査
  - 脆弱性評価に関する国内外学会の論文
    - ハードウェアセキュリティ研究会 (HWS) [1]
    - CHES [2], CARDISなど
  - JIL(Joint Interpretation Library)文書
    - SOGIS(欧州のCC認証機関連合体)のJIWG[3] によって作成

[1] https://www.ieice.org/ess/hws/
[2] https://ches.iacr.org/
[3] https://www.sogis.org/uk/detail_operation_en.html

ハードウェア脆弱性評価の事例(CHES2015)

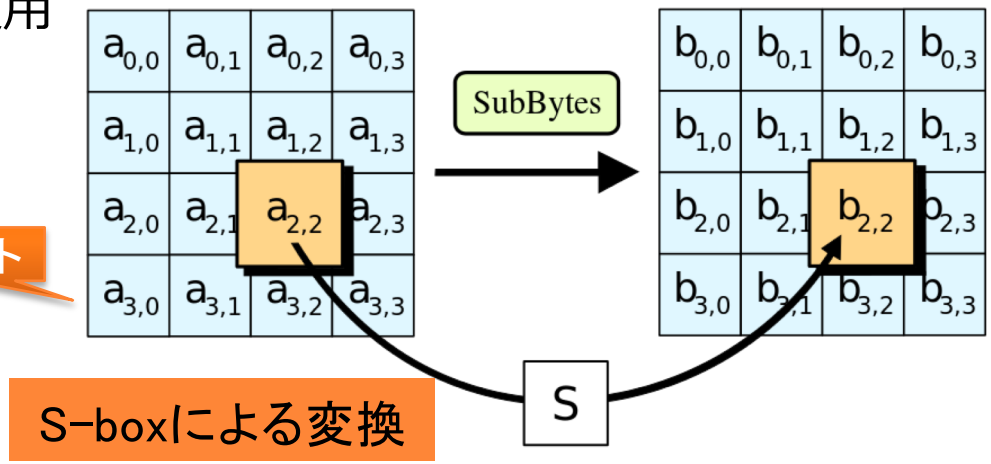
- 論文名：
  DPA, Bitslicing and Masking at 1 Gthz
- 著者: J. Balasch他
- HW: Texas Instruments Sitara SOC
- Processor: ARM Cortex-A8
- 評価対象：共通鍵AES暗号の実装
- 評価項目：電力解析攻撃手法:
  消費電力の変化に着目して鍵や処理内容を解析
  電力差分解析: DPA
  (Differential Power Analysis:)



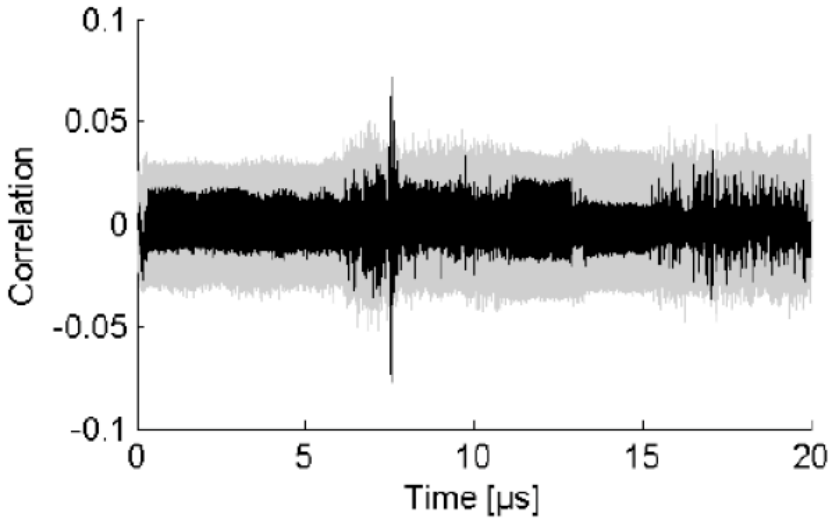
AESのBitSlise実装への電力解析攻撃

- AES:S-box(8ビット入出力の置換表)を使用
- AESのビットスライス実装
  ①ソフトウェアで高速（ CPUに依存）
  - 長いレジスタを利用し、並列実装可能
    （SIMD命令利用可能）

  ②タイミング攻撃に対して安全



- ARMコアのサイドチャネル攻撃
  - 情報の測定
  - 非接触電力測定
- 結果：
  - 1GHzのクロック周波数で
    動作する複雑なプロセッサ
    上での攻撃、10000波形で成功



https://www.cryptoexperts.com/ches2015/slides/day3/session3/talk1.pdf

進化する攻撃への対応 (スマートカードと組み込み機器のギャップ分析)

検討項目：組込機器用ICへの攻撃類型

	スマートカードへの攻撃類型* (Hardware AVA_VLA)の技術内容
4.1	Physical Attacks
4.2	Overcoming sensors and filters
4.3	Perturbation Attacks
4.4	Retrieving keys with DFA
4.5	Side-channel Attacks – Non-invasive retrieving of secret data
4.6	Exploitation of Test features
4.7	Attacks on RNG
4.8	Ill-formed Java Card applications
4.9	Software Attacks
4.10	Applet isolation

左記に追加が必要な新たな攻撃はないか

攻撃技術が進歩中
定義を超越するほど新規か？

HWのリバースエンジニアリング**
・電位コントラスト
・フォトンエミッション
・一層ごとに剥ぐ
・熱放出

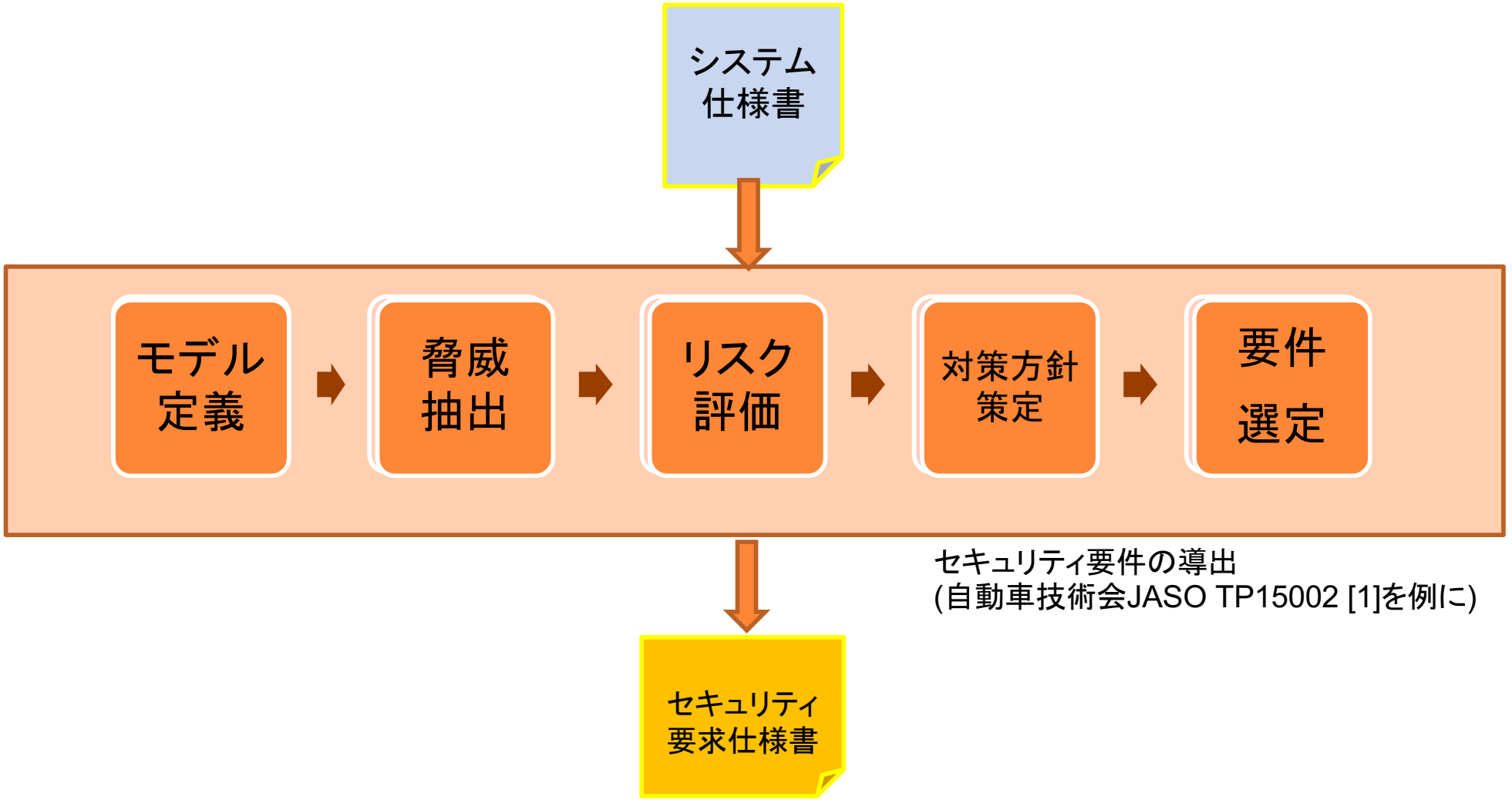
IC回路のSWダウンロード時のアクセス侵害は？

暗号鍵管理や市場における無効ICの扱いは？

* ＜CC Supporting Document CCDB-2013-05-002 Version 2.9 Application of Attack Potential to Smartcards＞

**ハードウェアの脆弱性評価の最新技術動向に関するセミナー IPA
https://www.ipa.go.jp/security/jisec/seminar/documents/hw_semi_20151203.pdf

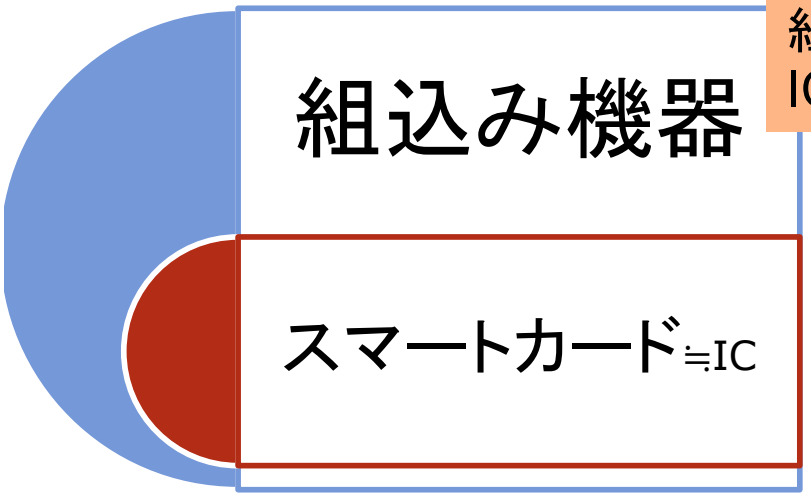
課題2:アプリにおけるセキュリティ要求のまとめ



セキュリティ要件の導出
(自動車技術会JASO TP15002 [1]を例に)

[1] 自動車ー情報セキュリティ分析ガイド

モデル定義と脅威抽出（SCと組込み機器の比較）



組込機器はより複雑なシステムで、
ICより上位のレイヤー

スマートカード
日欧で発達したセキュリティ文化、HWセキュリティの原型

攻撃者の視点のアドバンテージ：

- サンプルの入手容易性
- 物理インターフェイスも使用可
- リーダライタを使用する環境は非保護
- 製造過程でも攻撃

組込機器

攻撃者の視点のアドバンテージ：

- ICへの脅威はすべて脅威
- IC以外の部分への脅威も問題

インターフェースからのアプローチ

- 種類や型式により異なり、モデル化難
- デバッグ用のインターフェース有り

ユースケース

・リモートSW(OTA)更新ダウンロード：
NW経由でダウンロード、更新を常に実施

ライフサイクル定義

- インターフェース：組込機器用ICの場合、
- 運用が未確立

リスク評価と対策立案

リスク評価

- 脅威の優先付け
- 多様な方法が提案
  CRSS, RSMA@JASO TP15002

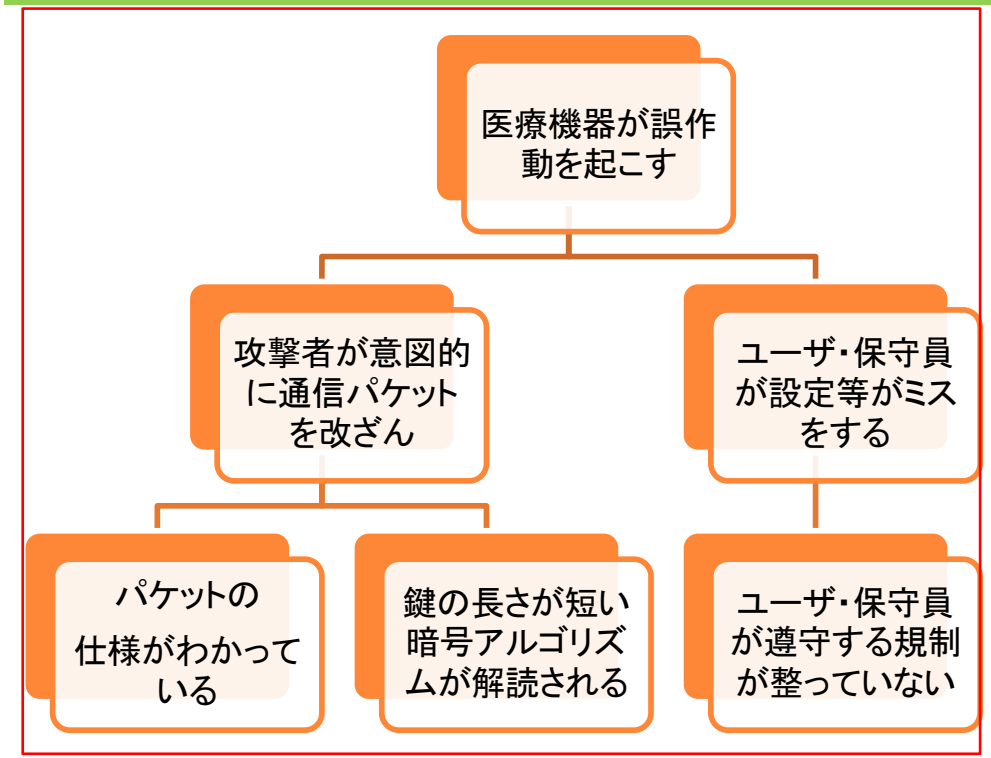
対策立案

- 評価対象(ToE)のIT対策、環境IT対策等を策定

組込機器用ICの耐タンパー対策の課題:
セキュリティ対策の実装が制限される可能性あり
リソースが極端に乏しい場合があり(対スマートカード)

産総研の貢献

成果種別	タイトル
ITU-T X.1373 国際規格	ITU-T X.1373 "Secure software update capability for intelligent transportation system communication devices"
国際論文	A Study on Quantitative Risk Assessment Methods in Security Design for Industrial Control Systems. DASC/PiCom/DataCom/CyberSciTech 2018: 62-69
国際論文	Detailed Analysis of Security Evaluation of Automotive Systems Based on JASO TP15002. SAFECOMP Workshops 2017: 211-224



Attack Tree による原因分析

課題3: セキュリティ保証スキームの構築と運用

アプリの評価：信頼基点（SCU等の暗号モジュール）を用いたアプリが要求水準を満たしているか
信頼基点の認定：対象機器に組み込まれた信頼基点が正真正銘のものであるか

PP*: Protection Profile
セキュリティ要求仕様書

調達側が、IT製品への適切な機能（使用環境や対抗する脅威、対応するセキュリティ機能）と保証すべきレベルをCC従った方法で指定

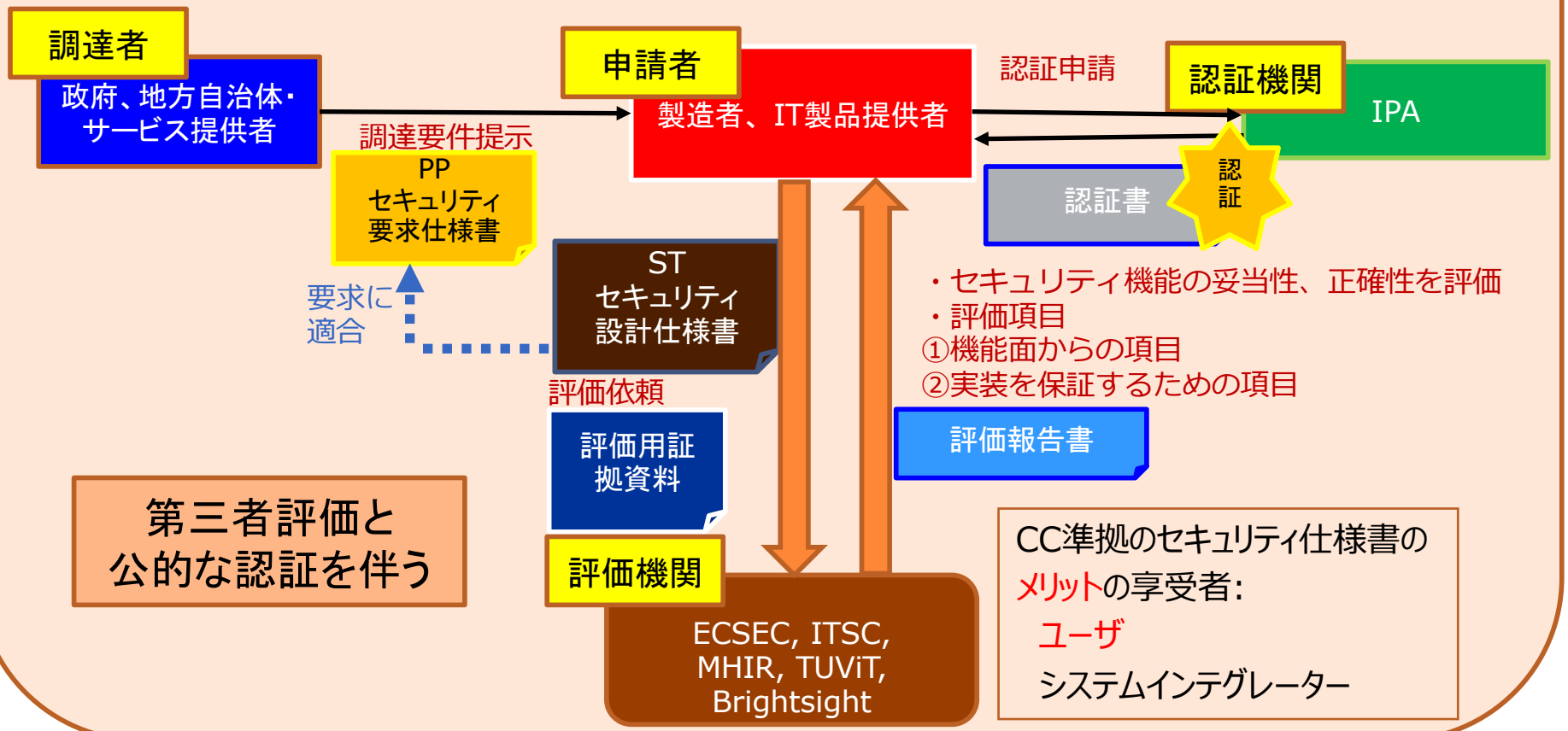
ST: Security Target
セキュリティ設計仕様書

IT製品提供者が、IT製品のセキュリティ要件が調達要件を満たすことを（PP適合）を宣言

* ITセキュリティ評価及び認証制度に関する説明会 2017年3月17日
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

セキュリティ評価と認証のスキームの例

JISEC (Japan Information Security Evaluation and Certification Scheme)*
評価基準ISO/IEC 15408(Common Criteria: CC)に基づきIT製品を認証する制度
CC: Common Criteria for Information Technology Security Evaluation
(情報技術(製品)セキュリティ評価のための共通基準)



* ITセキュリティ評価及び認証制度に関する説明会 2017年3月17日 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

エッジデバイス向けセキュリティ保証スキーム構築に向けて

CCの問題点

- システムセキュリティの保証が困難
  情報システムではない、あくまでも要素としての情報技術製品
- バージョンの更新やパッチに対応できない
- 対象製品の「セキュリティの程度」を測る直接的基準ではない
  セキュリティそのものの標準ではない,あくまでも評価の方法を定めたもの
- コストと時間がかかる
  CC評価の論理的厳密さ

エッジデバイスへの適用に向けた検討項目(案)

- 社会全体でどのような基盤が必要かを検討し、以下の軸で方向を提案

  例1：各産業におけるCCベースの脆弱性分析の適用
  セキュアペイメント：EMV*型式認定
  産業機器:IEC 62443
  自動車:ISO/SAE 21434

  例2：評価技術（脆弱性データベースや試験ツール等）の整備

  例3：セキュリティ保証の対象の明確化

EMV仕様: Europay International、MasterCard International、Visa Internationalの共同制定による金融取引用ICカード関連仕様

まとめ

現況
機器・システムのサプライチェーンは多様な事業者や多くのフェーズを含み、グローバル化
新しいサービス提供が期待されるIoTの急速な普及
不正な半導体部品の潜入等によるモノ自体のすり替えや改ざん等がセキュリティ課題

セキュリティ保証スキーム研究の目標
関係機関と連携しながら、セキュリティ保証の技術基盤を整備し、評価認証と国際標準化につなげる
新セキュリティ技術を迅速かつ確実に製品・システムに搭載すること

今後の取り組み
①多様な論理・物理インターフェースを高度に利用する攻撃者の観点から、脆弱性を網羅的に分析・評定することにより、攻撃類型を集約
②製造者が満たすべきセキュリティ要件の導出方法及び評価機関が実施する脆弱性評価方法のそれぞれに関し、技術的および手続き的に検討
③チップベンダからアプリケーション供給者まで複数のレイヤーが関与する様々なIoT分野に適したセキュリティ保証スキームの研究開発