# ③ 安価なIoT機器に組込めるSCUを対象としたセキュリティ保証スキームの開発

A
創出・証明

電子商取引安全技術研究組合、 産業技術総合研究所

網羅的な脅威分析で、セキュリティ要件を明確化し、セキュリティ評価の厳密さと開発工数のバランスを確保

## 技術の特長

■ セキュリティのレベル分け

IoTの安価な末端ノードに対し、セキュリティ実装の確からしさのレベルの分け方とセキュリティの示し方の妥当性を確保

■ セキュリティ保証スキーム

信頼の基点となるハードウェアを組込む機器に最適なセキュリティ保証スキーム(セキュリティ評価技術と認証の仕組み)を構築

## SCU搭載IoT機器のセキュリティ保証

信頼の基点と　なる暗号ハードウェアを組込む1チップマイコン等を軸とした、**高信頼**な機器を**妥当なコスト**で開発する基盤を構築

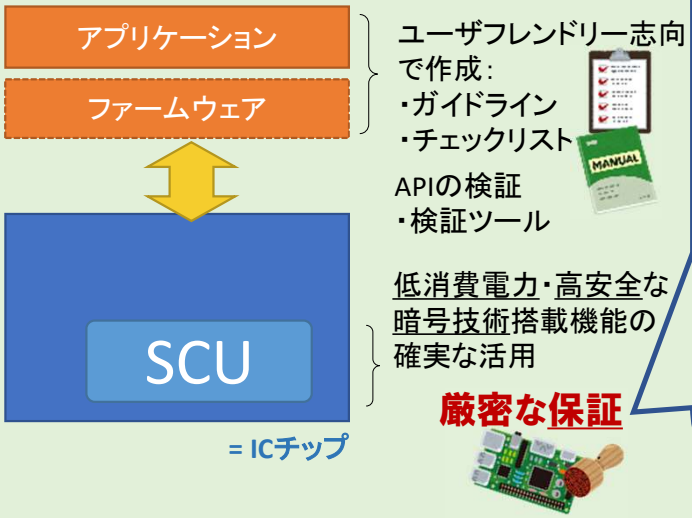

## IoT機器の脆弱性評価/攻撃手法の集約

主要国際会議の論文を調査し、**脆弱性DB**として集約


- Physical Attacks
- Overcoming sensors and filters
- Perturbation Attacks
- Retrieving keys with DFA
- Side-channel Attacks
- Exploitation of Test features
- Attacks on RNG
- Java Card applications
- Software Attacks

## 信頼の基点に対するセキュリティ保証スキームの整備/構築

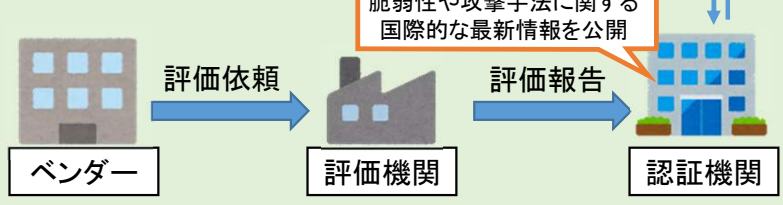
### SCUを信頼の基点として用いたIoT機器のセキュリティ確保




### SCUに対するセキュリティ保証スキーム

対象IoT機器に組込まれる暗号モジュールが**確かにSCU**であることを認定


**SOGIS**[*1]における脆弱性評定(AVA_VAN)や**評価保証レベルEAL**[*2]等の議論動向を踏まえ、SCU搭載機器のセキュリティ保証のあり方を検討




*1 Senior Officials Group Information Systems Security
*2(Evaluation Assurance Level)

⇨ 製品を認証

November 2020