経済安全保障重要技術育成プログラム／ハイブリッドクラウド利用基盤技術の開発／半導体・電子機器等のハードウェアにおける不正機能排除のための検証基盤の確立
（中間評価）
2023年～2028年　5年間
プロジェクト報告資料

2025年6月2日

国立研究開発法人産業技術総合研究所（代表機関）
株式会社SCU
リンテック株式会社
国立大学法人東京大学
国立大学法人神戸大学

K Program課題概要

経済安全保障重要技術育成プログラム／ハイブリッドクラウド利用基盤技術の開発

別紙2-2

採択テーマ：

半導体・電子機器等のハードウェアにおける不正機能排除のための検証基盤の確立

事業の目的・概要

- 情報システムに用いられる半導体・電子機器などハードウェアの不正機能を排除できる検証技術を確立する。
- 半導体設計時の設計データに不要な機能や、仕様で定められていない部品が混入していないかなどの判定に必要な要素技術の特定と技術開発を行う。また、半導体の設計から組み込みまでの、半導体・電子機器のライフサイクル全体にわたるセキュリティ要求仕様の定義や策定、標準化を目指し、検証とパイロット実証を行う。

実施体制

※太字：代表機関

国立研究開発法人産業技術総合研究所

株式会社ＳＣＵ、リンテック株式会社、

国立大学法人東京大学、

国立大学法人神戸大学

事業期間（予定）

2023年6月~2028年6月

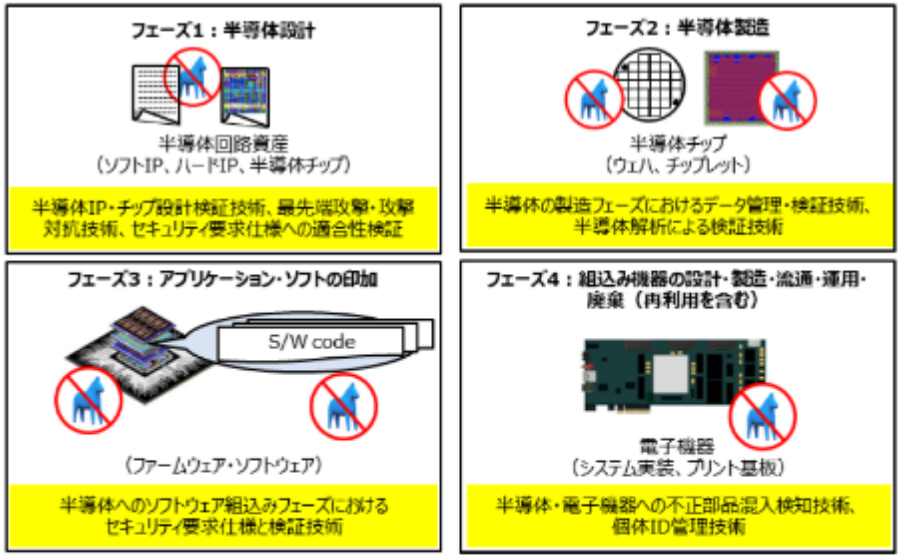
事業規模など

- 事業規模　：　34億円
- 契約形態　：　委託事業

主な研究開発内容

- セキュリティ要求仕様の定義・策定
- セキュリティ要求仕様の標準化
- セキュリティ要求仕様の検証とパイロット実証

事業イメージ（全体像）



出典：内閣府・経済産業省「ハイブリッドクラウド利用基盤技術の開発」に関する研究開発構想概要

https://www.nedo.go.jp/content/100963089.pdf より

＜評価項目１＞研究開発ビジョン及び研究開発構想の実現に向けた研究開発課題の達成目標や内容の妥当性

（１）研究開発課題の達成目標の妥当性
（２）知的財産・標準化戦略

（１）研究開発課題の達成目標の妥当性

1. 不正機能（ハードウェアトロージャン）の排除

- マルウェア対策への関心が高いが、ソフトウェアが動作する基盤であるハードウェアへの不正機能が挿入されいないことをどう担保するも同様に重要な課題である
- 米国・中国などは、学会発表件数等からこの分野への注力が伺える*
- **日本ではこれまでのところ不正機能排除に対する包括的な取り組みはなかった**
- **本プロジェクトでは初めて包括的に不正機能排除に取り組み、可能なアプローチを示すべく取り組んでいる**
- 戦略策定もふくめて、不正機能排除のための検証基盤を確立することが本事業の目標である

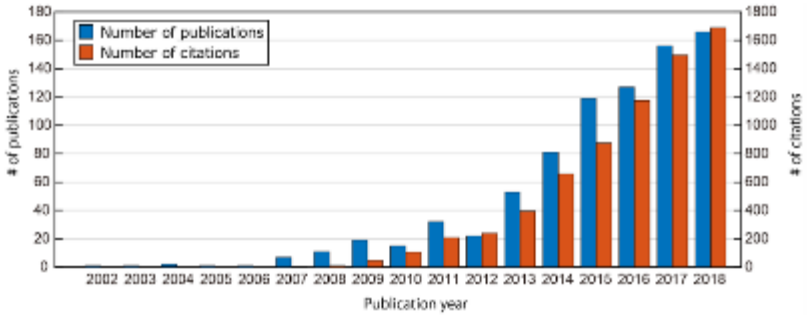
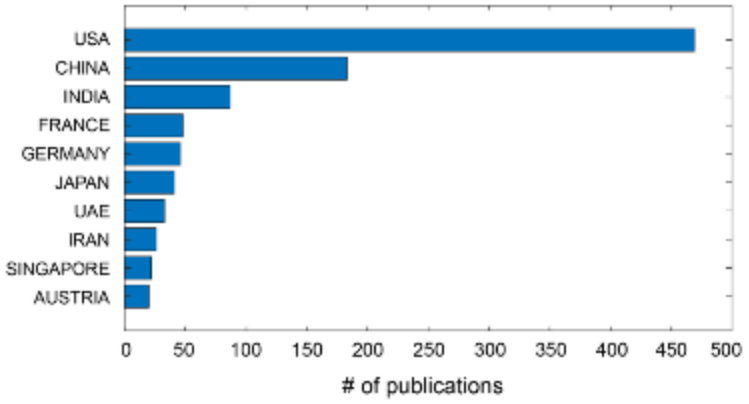


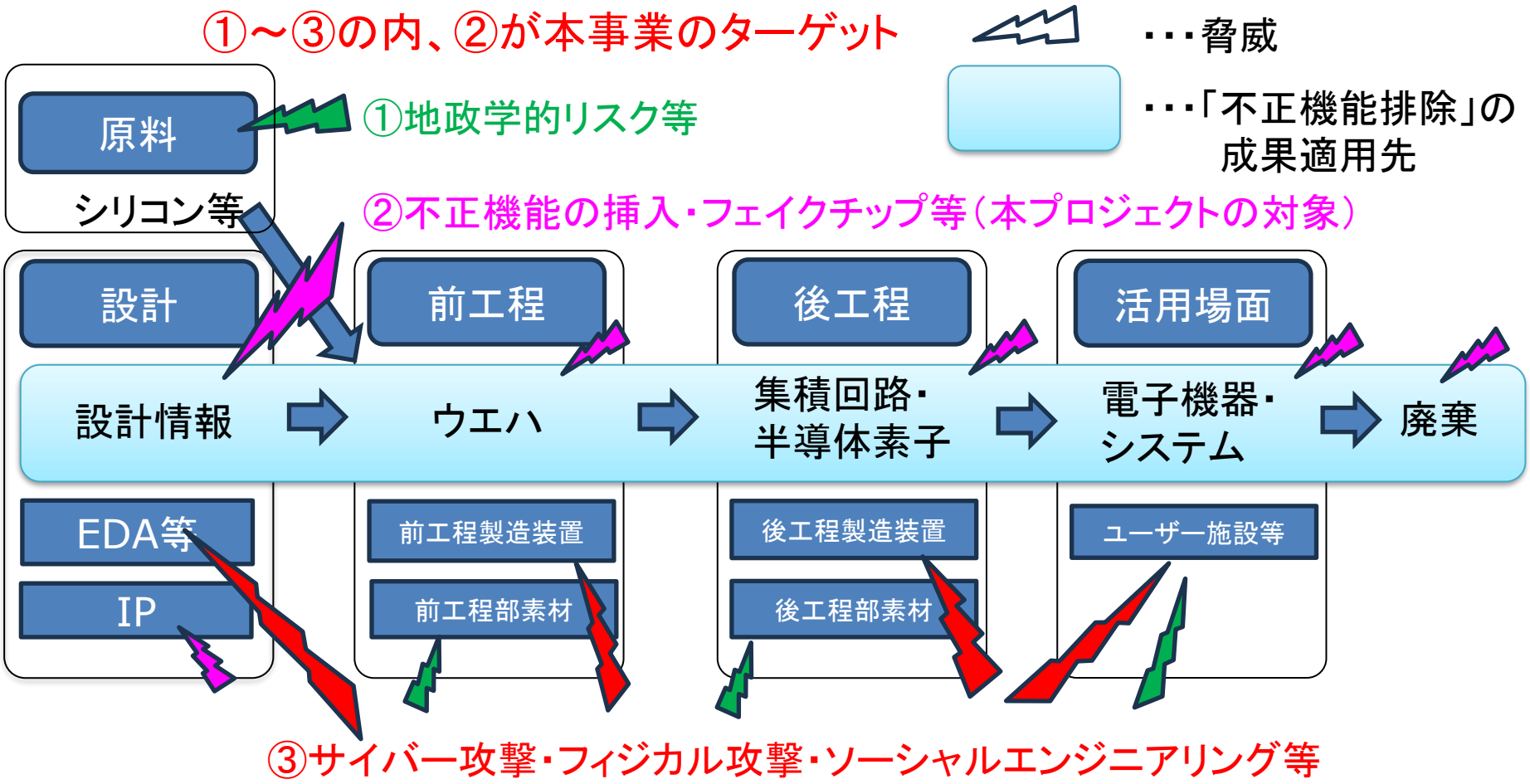
Figure 2: Trends in the number of HT-related papers and citations



*Y. Hayashi and S. Kawamura, "Survey of Hardware Trojan Threats and Detection," 2020 International Symposium on Electromagnetic Compatibility - EMC EUROPE, Rome, Italy, 2020, pp. 1-5, doi: 10.1109/EMCEUROPE48519.2020.9245675.

（１）研究開発課題の達成目標の妥当性

2．半導体サプライチェーンの脅威



内閣府公開資料「特定重要物資の指定について」2022/11
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai4/siryou1.pdf
の半導体サプライチェーン（SC）マップを参考にした

（1）研究開発課題の達成目標の妥当性

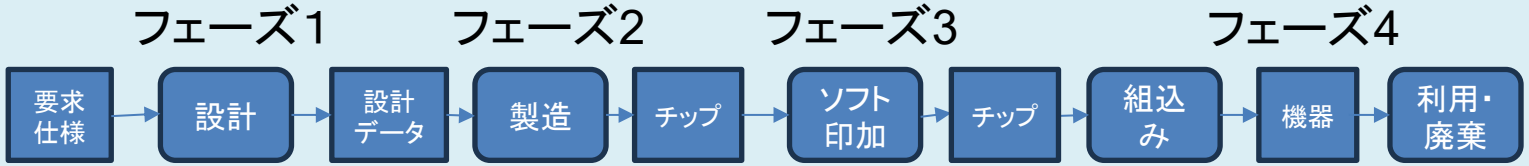
3. 想定する脅威と対応する実施項目

フェーズ	半導体ライフサイクルで想定される不正機能混入の脅威	該当実施項目
1	仕様に不正機能を挿入	対象外
	第3者IPに仕様以外の機能が挿入	〔1－1〕
	（内部の）設計者が仕様にない不正機能を挿入	〔1－1〕〔1－2〕
	外乱等に対する脆弱性の混入	〔1－3〕
	具備すべきセキュリティ機能が仕様に備わっていないこと	〔1－4〕
2	マスク製造工程までの不正機能の挿入	〔2－1〕
	ウエハ製造工程までの不正機能の挿入	〔2－1〕
	チップ製造工程までの不正機能の挿入	〔2－2〕
	パッケージング工程での不正機能の挿入	該当項目無し 一部〔4－1〕
3	ソフトウェア初期書込み工程での不正機能の挿入	〔3－1〕
	ソフトウェア更新工程での不正機能の挿入	〔3－1〕
	書き込まれたソフトウェアの不正な書き換え	〔3－1〕
4	チップ搭載電子機器における不正機能の挿入	〔4－1〕
	流通段階での不正チップ（フェイクチップ）の混入	〔4－2〕

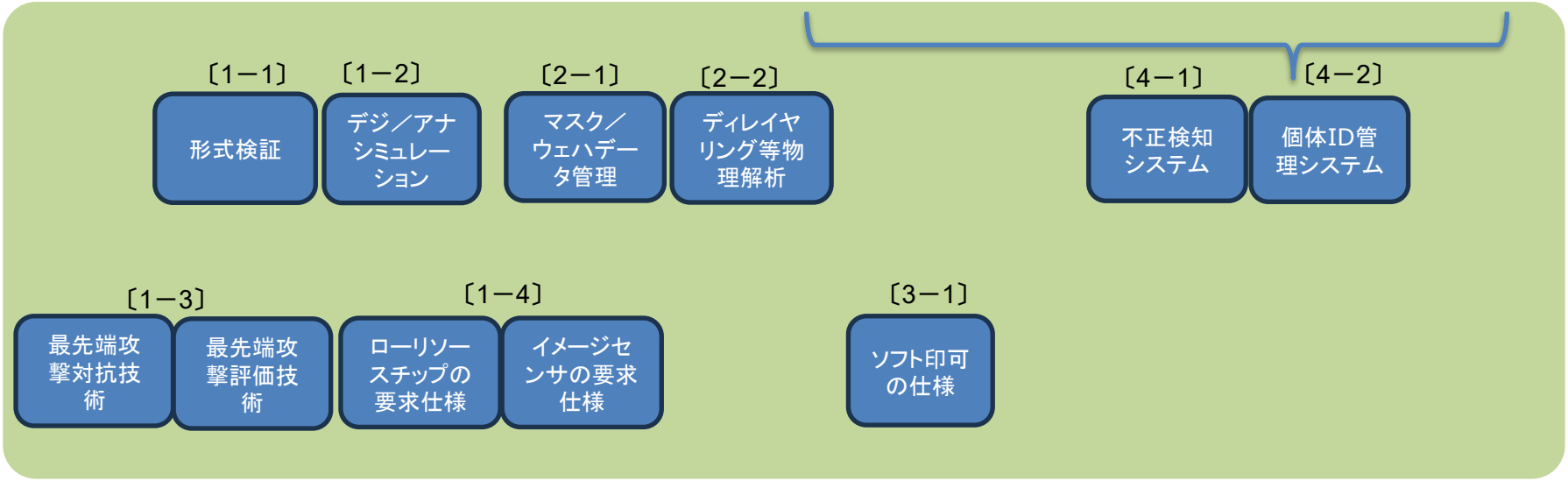
（1）研究開発課題の達成目標の妥当性

4. フェーズと対応する予定成果

半導体ライフサイクル



実施項目の予定成果



（2）知的財産・標準化戦略

■ 知的財産の取扱い方針

- 経済安全保障上、取り扱いに注意すべきと各受託者が判断した成果については秘匿化や共有範囲を限定することによりその内容が拡散することがないようにする。
- 経済安全保障上の懸念がないと各受託者が判断した成果については、学会発表や広報、半導体ベンダーや評価機関、ユーザへの開示などにより積極的に普及を図る。また、特許提案により権利を確保して参加者による製品適用や、第三者へのライセンス等による活用を目指す。

■ 標準化の取組状況

- ISO/IEC15408をベースとするセキュリティ要求仕様の策定や評価手順の策定などを進め、国際的な展開を視野にいれた活動を推進する。
- 人工物メトリクスに関する日本工業規格（JIS X 22387）のJIS化プロセスを進めた結果、2024年11月20日にJISが制定・発行・公示された。

＜評価項目２＞研究開発課題の達成目標に向けた進捗状況

（1）研究開発課題の達成目標に向けた進捗状況（国内外との比較を含む）
（2） 今後の見通し（多様な分野における実現可能性含む）

（１）研究開発の進捗状況・成果

全ての研究開発項目において、予定通りの進捗が得られている。具体的な成果は以下の通り。

①半導体設計フェーズにおける検証

〔１－１〕 ガロア体乗算器やAES※等を対象とした検証技術の検証適用範囲をさらに拡張することに成功した。 また、形式検証ツールの開発を行い、2025年5月に形式検証ツールver.1.0を完成し、評価を開始した。2025年9月までにver1.0の評価を完了予定。
研究成果を国際会議ULSIWで発表し、Student Presentation Awardを受賞。
※AES:Advanced Encryption Standard

〔１－２〕 要求外の機能が混入されてないことの確認手法を以下の方針で探求している：
【デジタル】機能検証の手段であるテストカバレージの概念を活用すること。
【アナログ】物理設計データに基づく回路物理特性量について、統計分布に系統的でない異常な振る舞いがないか探索すること。

〔１－３〕 技術調査を行い、６種類の最先端攻撃を抽出し、手順を定めて追試と脅威の分析、対策の検討を行っている。エミッション顕微鏡（PHEMOS X）の設置が完了し稼働（25年02月）。ICシステムセキュリティ協会/CC認証部会の関連WGに参加し、関連企業との検討体制を立ち上げた。

〔１－４〕 イメージセンサーを想定して、最小限のセキュリティ要求仕様の骨格を固め、素案作成。攻撃パスの調査を通し評価の観点で検討中。ICシステムセキュリティ協会/CC認証部会が有する欧州のEUCC/ISACへのパイプを活用し、要求仕様文書化の道を探索中。

（１）研究開発の進捗状況・成果

②半導体製造フェーズにおける検証

〔２－１〕 設計者による論理設計検証終了以降のチップ実装工程について調査実施。ISO/IEC JTC1/SC27/TR6114に加えて、半導体製造業界規格であるSEMI-E187,E188を調査し両者の比較を行った。

〔２－２〕 評価ターゲットとするハードウェアトロ―ジャン（HT）入りLSIを開発すると共に、侵襲・非侵襲の評価環境を構築。市販チップに対してリバースエンジニアリングを試行し、設計データを抽出し、その手順・観察結果等を文書化。要求外の機能の混入を光学顕微鏡画像によりスクリーニングする手法を構築し、国際会議PAINEにて発表した。

③ソフトウェア印加フェーズにおける検証

〔３－１〕 有識者ヒアリング等に基づき、ソフトウェア印加のセキュリティ要求仕様書の第０版を作成。評価観点の追記に向け、脅威の実現方法を整理した攻撃パスDBを整備中。ICシステムセキュリティ協会内に、本課題に資する新たな部会を設置することを検討中。

（１）研究開発の進捗状況・成果

④電子機器設計・製造・運用フェーズにおける検証

〔４－１〕 電気特性、電磁特性の電位変化を計測する技術を開発、PoCによるデモシステムを構築した。試験対象の個体差や計測環境によって、ゴールデンデータと計測結果に乖離がみられることから、機械学習により計測データを処理し、不正な改竄等を判定するアプローチに切り替え、改竄検知の手法を開発した。セキュアパッケージング手法開発中。

〔４－２〕 インクジェット印刷利用人工物メトリクス技術とシリコン表面にランダムな凹凸を形成するナノ人工物メトリクス技術の双方において、個別性と読取り安定性を十分に備えた製造・計測・照合技術を開発し、耐クローン性を評価する技術の開発を進めている。また、ブロックチェーン技術と暗号技術に基づく個体ID管理システムの設計を行った。人工物メトリクスに基づき個体ID管理を行うシステムのパイロット実証に向けて既に制定したJIS規格を含むプロセスの検討を進めている。

（２）今後の見通し

■ アウトプット目標の達成見込み

〔１－１〕～〔４－２〕の９つの実施項目において、実施計画において設定した目標を達成する見込み。

■ アウトカム目標達成の見通し／多様な分野における研究成果活用の状況

- 人工物メトリクスを利用する際の妥当性確認手順のJIS規格（本プロジェクトの成果であるJIS X22387）を活用した人工物メトリクスの普及
- CC等既存の国際的セキュリティ保証制度に適合したセキュリティ要求仕様文書や新たな脆弱性評価手法の開発により、半導体・電子機器の不正機能の排除およびセキュリティの向上
- ICシステムセキュリティ協会および同CC認証部会への参画企業、JEITA参画企業等での不正機能排除の手法等成果の活用
- JC-STAR等新しいセキュリティ検証制度への展開可能性の検討

（2）今後の見通し

今後に向けて

- 中間目標の到達見通し・・・計画通りの進捗
- ステージゲート以降の進め方
  - 技術開発の継続
  - パイロット実証を進める
    - 開発した技術を、より実際的な対象・状況に適用する
  - 標準化や外部組織との連携等では、状況に応じて柔軟に対応する

〔１－１〕半導体設計IP検証

形式検証の概念

仕様

計算しやすい

回路機能を表す方程式

$Z = AB$

$A = a_0 + a_1\alpha$
$B = b_0 + b_1\alpha$
$Z = z_0 + z_1\alpha$

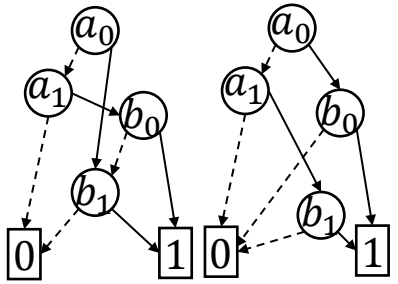
＋

回路動作の形式表現

$\mathrm{RSTn} = 0 \rightarrow Z = \mathbf{X}^3 D$

変換

仕様グラフ(一意)

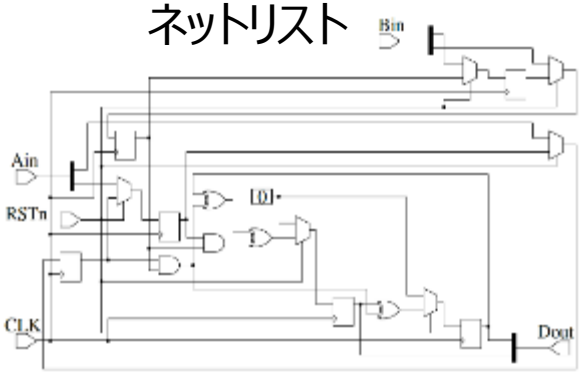


等価？

等価！

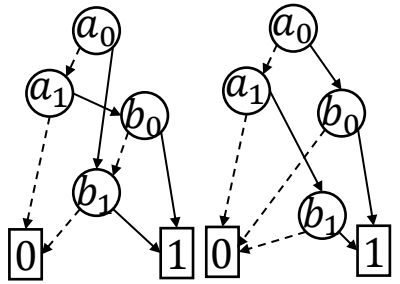
実装

ネットリスト



回路動作の
記号実行

回路機能グラフ
(一意)



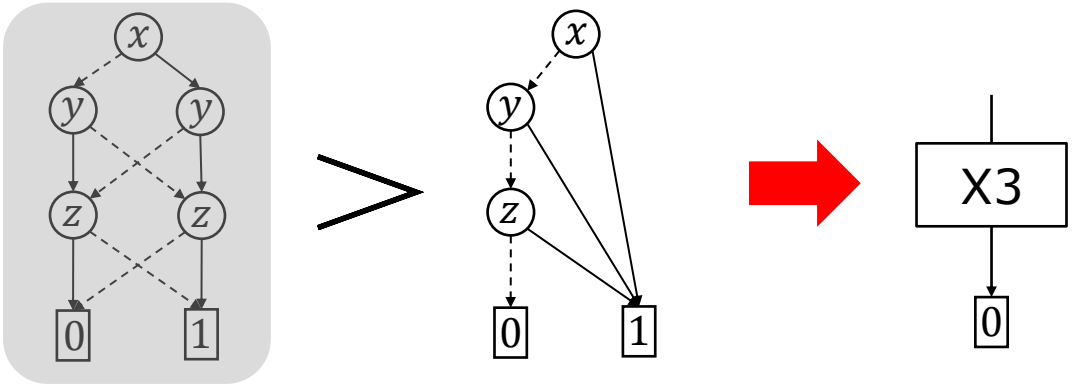
AESのIPをターゲットとした形式検証の効率化チャレンジ

1. 順序回路の仕様記述を形式化するために線形時相論理（LTL）を採用し、順序回路の形式仕様と回路ネットリストに対する等価性検証手法を開発した。
2. AESの仕様記述と回路ネットリストの等価性検証を実現するため、従来手法で用いられるZDDより効率的な表現と演算が可能な決定グラフの開発を行い、**現在評価中**。

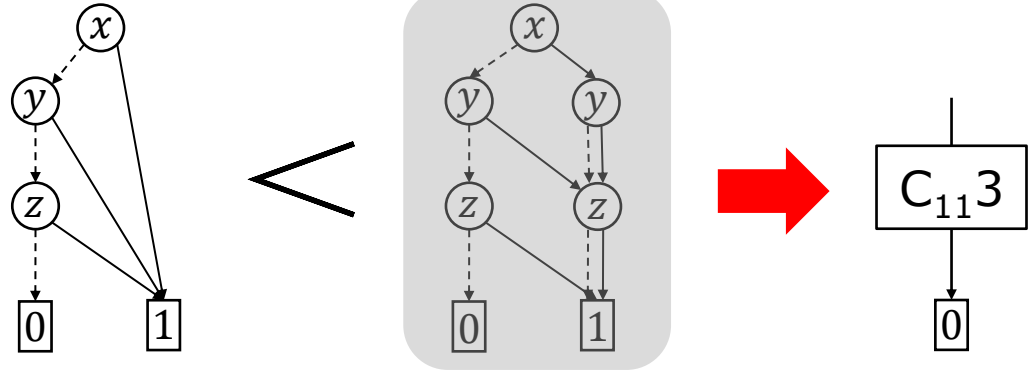
BDDとZDDのハイブリッドによるさらなるサイズ圧縮

BDD　　ZDD　　ハイブリッド

$x \oplus y \oplus z$



$x \vee \neg xy \vee \neg x\neg yz$



〔１－２〕チップ設計検証

実施項目〔1-2-A（デジタル）〕の内容

【取組状況】RTL/ネットリストシミュレーションからテストカバレージ（ハードウエア・データカバレージ）を抽出し、要求外の機能の混入を検出する

- ✓ RTLシミュレーションのテストベンチ記述において、よりテストカバレジの高いテストベンチ生成手法の検討→記述&テストステップ数とテストカバレジの相関を求めることでよりカバレジの高いテストベンチ生成の実現を目指す：**実施中**
- ✓ 論理合成後/配置配線後のネットリストシミュレーションにおいて、よりテストカバレジの高いテストベンチ生成手法の検討→記述&テストステップ数とテストカバレジの相関を求めることでよりカバレジの高いテストベンチ生成の実現を目指す：**実施中**
- ✓ より上位の記述言語（ソフトウエア）とRTLの協調検証環境の構築→テストカバレジを抽出し、よりテストカバレジの高いソフトウエア記述の実現を目指す：**今後実施予定**
- ✓ 最終目標：仕様外の動作箇所の抽出を目指す
- ✓ 現状の具体的な検証対象
  - 楕円曲線暗号・ペアリングエンジン
  - 耐量子計算暗号
  - RISC-Vプロセッサ＋AXI-BUS

実施項目〔1-2-B（アナログ）〕の内容

実施内容①：アナログやメモリの半導体チップにおいて統計分布に系統的でない異常な振る舞いがないか探索し、要求外の機能に紐づけられる回路特性量が無いことを確認する手法の開拓

実施内容②：アナログやメモリについて物理設計データの改竄に対して感度を持つ複数の回路物理特性量を選定し、その統計量を効率的に評価するシミュレーション手法の開拓

★アナログやメモリの物理特性量として「伝搬遅延」と「消費電力」を選定、物理シミュレーションによる抽出

★回路物理特性量の統計的な変化を利用して、「要求外の機能」の検知および「回路の改竄」を検定

一般性の高い半導体設計(EDA)ツールである高速回路シミュレータを利用して計算機上で検証する手法を開拓・試行（中間目標）

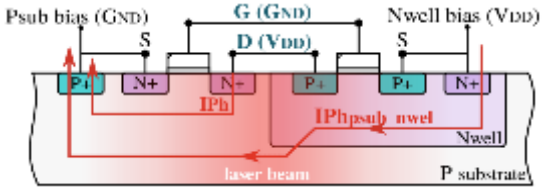
〔１－３〕最先端攻撃・攻撃対抗技術

1．レーザー攻撃センサ

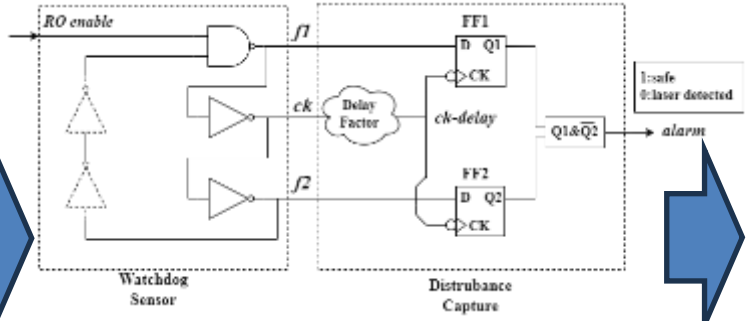
※1:Time-to-Digital Converter

- レーザー照射によるフォールト攻撃を検知するデジタル回路で構成可能なセンサの開発

[1]より引用

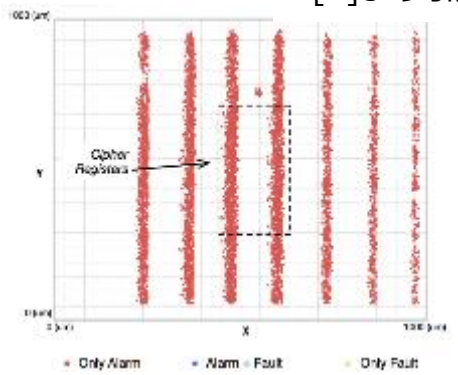


レーザーフォールト攻撃はIR-Dropを発生させ回路の信号遅延を増加[1]
⇒**レーザーによるフォールト攻撃の検知に利用できる**



既存研究[2]ではリングオシレータを用いて信号遅延の異常な変動から攻撃を検知するセンサを提案

[2]より引用



FPGA上での実験では既存のセンサにレーザーへの感度が悪い領域が存在
⇒検知されずに攻撃される可能性

- 研究計画

既存センサの評価
既存のリングオシレータベースのセンサをFPGA上で評価

センサ基礎設計の検討
センサの検知性能を改善する提案を国際会議で発表[3]

実証実験
暗号回路を保護するシナリオにおいて提案手法を評価した結果を国内会議で発表[4]

[1] Viera, Raphael A. Camponogara, et al. "Simulation and experimental demonstration of the importance of IR-drops during laser fault injection." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 39.6 (2019): 1231-1244.
[2] He, Wei, Jakub Breier, and Shivam Bhasin. "Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks." International Conference on Security, Privacy, and Applied Cryptography Engineering. Cham: Springer International Publishing, 2016.
[3] Hayashi, S., Sakamoto, J., Chikano, M., & Matsumoto, T. (2023, November). Effective Layout Design for Laser Fault Sensor on FPGA. In Proceedings of the 2023 Workshop on Attacks and Solutions in Hardware Security (pp. 103-112).
[4]林　俊吾, 坂本純一, 松本　勉, “FPGAにおけるリングオシレータ利用レーザー検知センサのAES回路への適用“, HWS研究会, 2024年4月

2．DL-SCAの設計へのフィードバック

①サイドチャネル攻撃の評価
目的：最新攻撃の性質評価

DL技術の台頭によって，サイドチャネル攻撃の高度化 (DL-SCA)

DL-SCA関連の論文を網羅するリストを作成し(図1)，代表論文や今後の展望、評価との関連を報告書として整理.

総計448件検索によって該当した論文のうち，関連する総計306個の論文を抽出した．抽出した全論文について従来SCAの評価指標に合わせて分類したデータベースの作成を行い，そのうち15個の重要XAI論文について，論文を精査

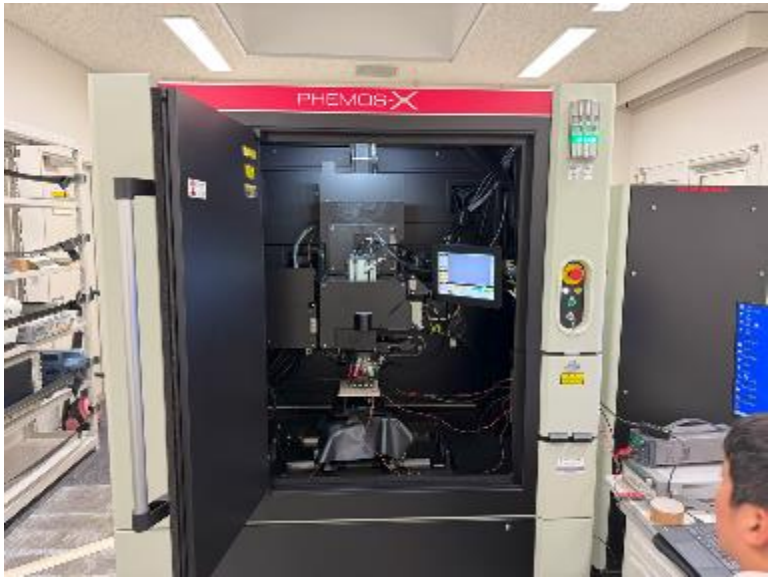
② リーク検知
目的：設計者へフィードバック

攻撃の高度化に合わせて，検知手法を更新する必要がある

説明可能AI（XAI)が有益であると判断し，関連研究のデータベース化・文書化を実施.
XAIを用いた評価手法、およびツールについて国内会議にて発表.

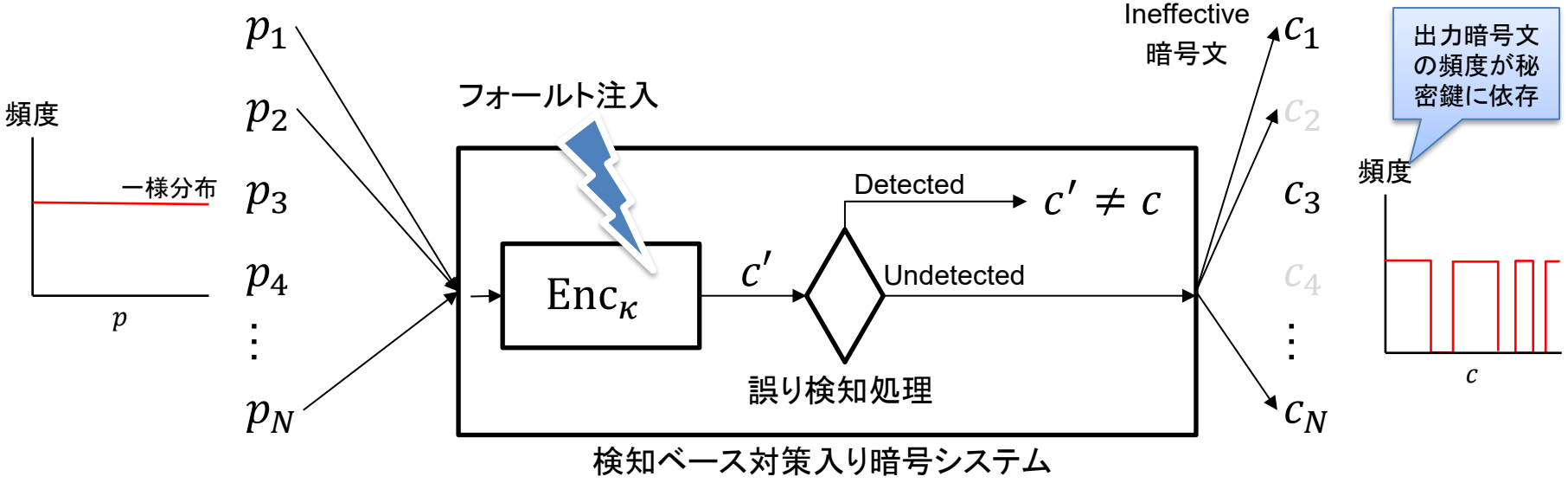
3．エミッション攻撃

- 発光顕微鏡や電気光学プロービングを用いたサイドチャネル攻撃（以下「エミッション攻撃」）への耐性検証技術の開発に向け、FPGAボードのサンプルを準備し、ボード制御プログラムおよび測定環境・制御スクリプトを構築し、発光・電気光学プロービングの基本測定を確認した。
- 測定装置：



4．SIFA（統計的無効フォールト攻撃）

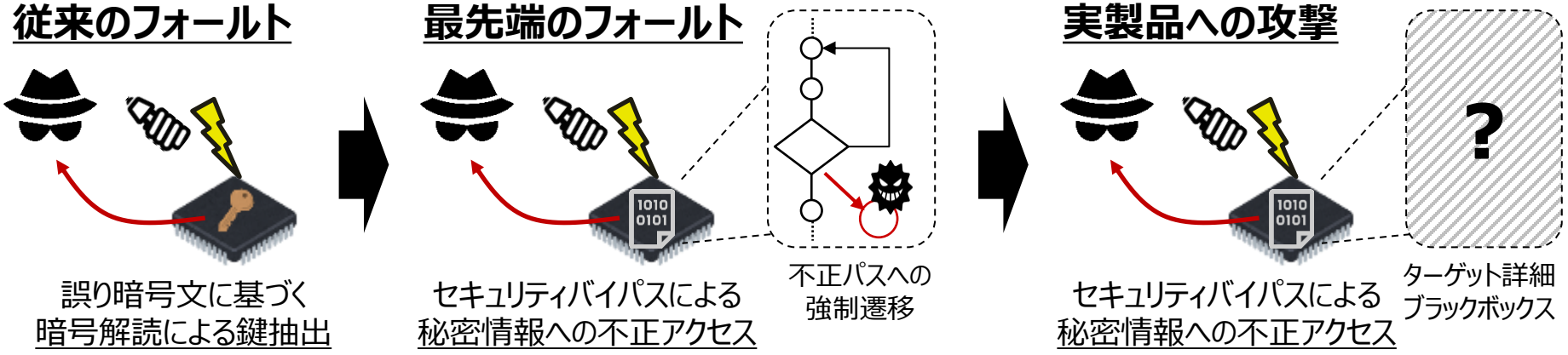
- 誤り暗号文を必要としないフォールト攻撃をIneffective（無効）Fault Analysisと呼ぶ
- 特に出力暗号文の分布から統計的に解析を行うStatistical IFAが着目されている.
  - IFA系の攻撃へアルゴリズムレベルで対策することは難しい
  - 誤りの注入とタンパーリアクションを無関係にする必要がある->フォールトセンサが有効



- これまでの成果：SIFA解析の効率化手法を国内研究会で2件発表
- 今後の予定：SIFA解析手法のさらなる効率化、および既存のSIFA対策の解析を行う

5．TEEへのフォールト攻撃

- セキュリティ機構TEE*を狙ったフォールト攻撃に対する耐タンパー性検証技術、 対抗する半導体実装技術 （*Trusted Execution Environment）



最先端のセキュリティバイパス フォールト攻撃に対する3つの研究成果

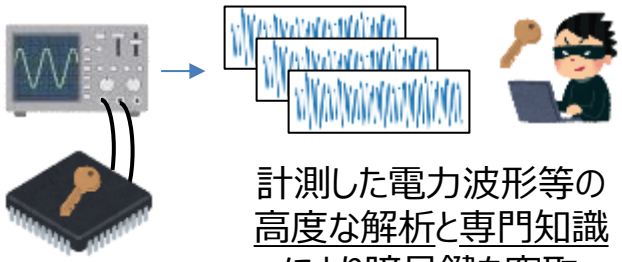
① 最先端攻撃の検証技術	② 最先端攻撃対抗の半導体実装技術	③ 実製品レベルの攻撃評価技術
• 最先端攻撃の調査 • 検証環境の構築	• 対策技術の実装 • 対策の網羅評価	• 製品攻撃事例の調査 • ブラックボックス攻撃技術開発

2025年9月SG時点の成果予定

6．PQCへのDL-SCAの適用

- DL-SCAに対する耐タンパー性検証技術、対抗する半導体実装技術

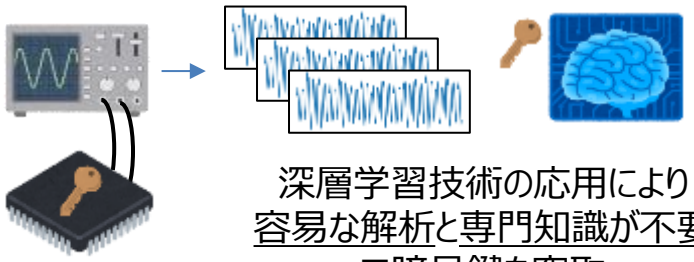
従来のSCA



暗号IC

計測した電力波形等の
高度な解析と専門知識
により暗号鍵を窃取

最先端のDL-SCA



暗号IC

深層学習技術の応用により
容易な解析と専門知識が不要
で暗号鍵を窃取

(SCA対策が施されていても対策の
傾向を学習し、暗号鍵の窃取可能)

最先端のDL-SCAに対する3つの研究成果

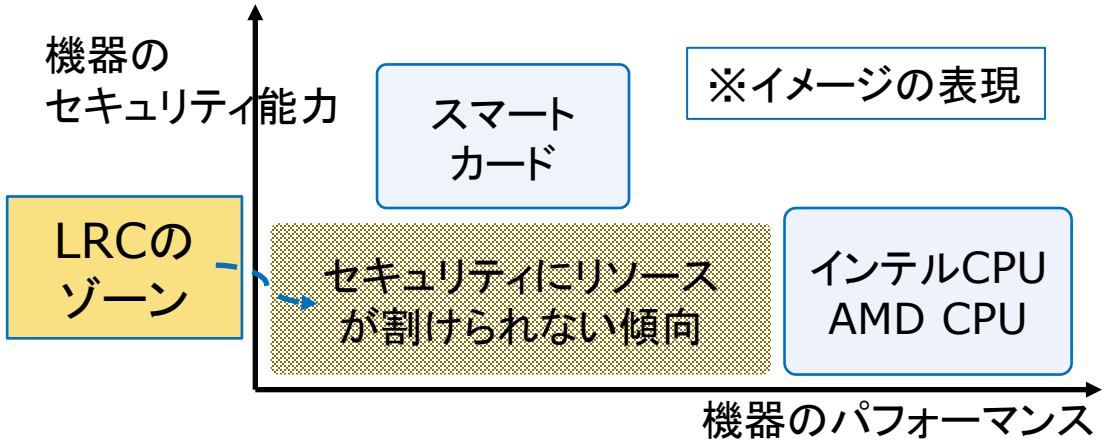
① 最先端攻撃の検証技術	② 耐量子計算機暗号の攻撃評価技術	③ 最先端攻撃対抗の半導体実装技術
• 最先端攻撃の調査 • 検証環境の構築・手順整備	• NIST標準の耐量子計算機暗号向け検証環境の構築	• 対抗技術の実装・評価 • 脆弱な対抗技術の整理

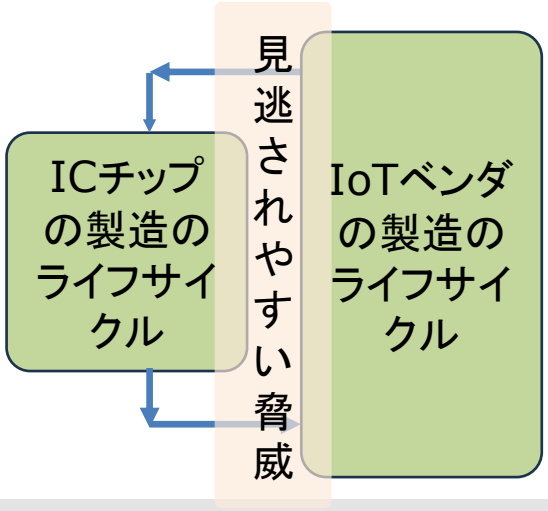
2025年9月SG時点の成果予定

〔１－４〕セキュリティ仕様への適合性検証

LRC(ローリソースチップ)の最小限のセキュリティ要求仕様

- 評価対象の絞り込み：
  - 既に普及しているSESIPのLevel 1～3に対する整合性を重視
  - スマートカードより弱い防御、Intelチップより低い能力のゾーン内のIoT用ICチップ
- 資産の絞り込み：
  - 全てのICチップが必ず保護しなければならない資産
  - 各ICチップの特徴的な資産（製品固有のオプション）
- 脅威の絞り込み：
  - ICチップベンダーとIoTデバイスベンダーの狭間で見逃されやすい製造過程の脅威
  - 標準的なICチップの脅威

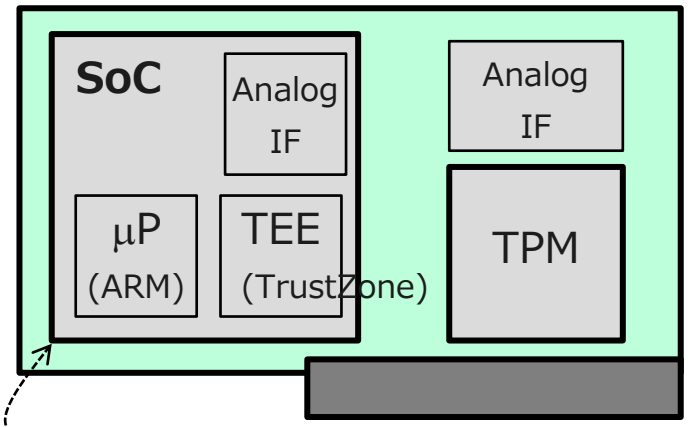




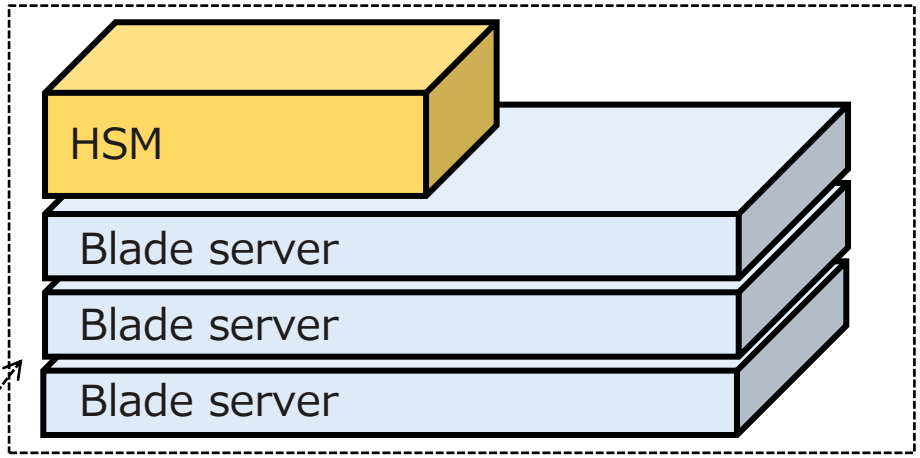
〔２－１〕半導体設計データ管理

JEITA/ICSS-JCのチップレットHWS-WGにおける検討課題

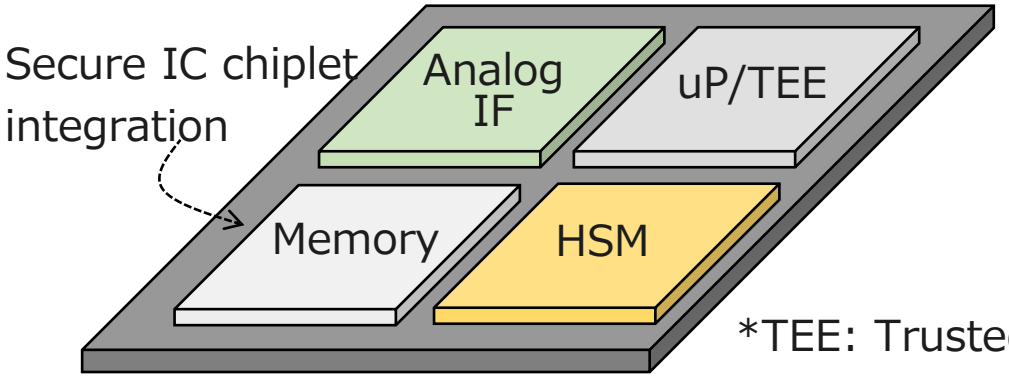
従来構成：ボードレベル



従来構成：ラックマウント



検討対象：パッケージレベル



- ✓ Root of Trustの主体
- ✓ セキュリティ機能の選択・分担・実装方法
- ✓ 設計自由度の確保（非固定化）

*TEE: Trusted execution environment
TPM: Trusted platform module
HSM: Hardware security module

〔２－２〕半導体解析による検証

1．評価ターゲットとしてHT入り評価チップ開発

- 不正回路排除技術の研究開発プラットフォーム TACTICS の開発
  - TACTICS (Trojan Analysis and Countermeasures toward Trusted Integrated CircuitS)
    - TEGチップ (TACTICS-Chip130/065)
      - 物理設計・製造
      - 動作確認 (FY2025 Q1)
    - 評価ボード (TACTICS-Board)
      - 通常動作の確認用
      - エミッション観察用（FY2025 Q1-Q2）
    - 評価プログラム (TACTICS-SW)
      - TEGチップの制御、動作確認用ソフトウェア (FY2025 Q1)

成果	TEGチップを作製
成果見込	TEGチップの動作を確認

成果	評価ボードを作製
成果見込	エミッション用評価ボードを作製

成果見込	TEGチップの制御・動作確認用ソフトウェアを作製

TEGチップ

評価ボード

評価プログラム

2．半導体解析としてディレイヤリング技術の適用

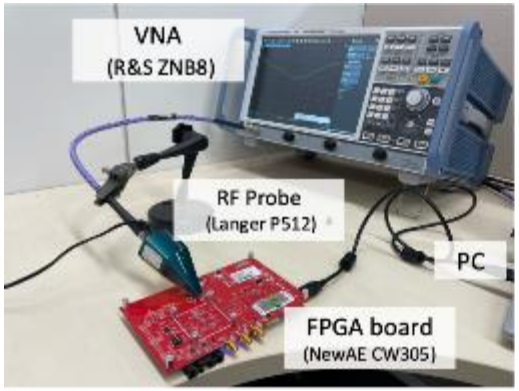
- 不正回路検出技術の開発に向け、設計ルール90nmおよび16nm相当の対象LSIについて、配線層・接続層・ポリゲートを含むSEM画像を取得（成果見込）。取得した画像から回路構造を抽出し、レイアウト対回路図（Layout Versus Schematics：LVS）を実施。これにより、SEM画像を用いた不正回路検出技術の利点と課題を整理（成果見込）。

（イメージ）

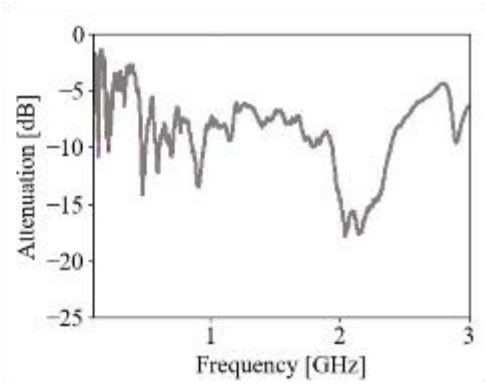
- 技術調査
  - 不正半導体製品およびHWSインシデント
  - 欧米における類似国家プロジェクトの調査

3．EMインジェクション応答を利用した解析技術の適用

- **ステージゲートまでの成果**
  - ICチップレベルの改ざん検出手法に関する文献調査とそれに基づく研究課題の整理
  - 環境構築（FPGA評価ボード上のHT実装およびその検知環境の構築）



構築した実験系の外観



取得した応答波形の例

- **ステージゲート後の予定、主な成果、パイロット実証のシナリオ。**
  - **前年度で検討した研究方針に従って、実用的なHT検知手法の提案・実証**
    - 研究レベルと実システム間でのHT検知技術に関する乖離を減らす。
      - RFプローブおよびVNAを用いた非侵襲なHT検知に必要な物理量の抽出
      - 製造ばらつきと改ざんの切り分けが可能な後処理手法
  - **パイロット実証：**既存手法より高精度かつ汎用的に改ざん検知ができることを実証する。
    - 計測ポートなし、クロック&I/O配線あり、その他モジュールが実装された機器
    - 製品出荷後でも検知可能、追加実装が不要、最小限の計測時間コスト等

〔３－１〕ソフトウェア組込み段階でのセキュリティ要求仕様と検証技術

ソフトウェア印加・更新のセキュリティ要求仕様書第0版作成

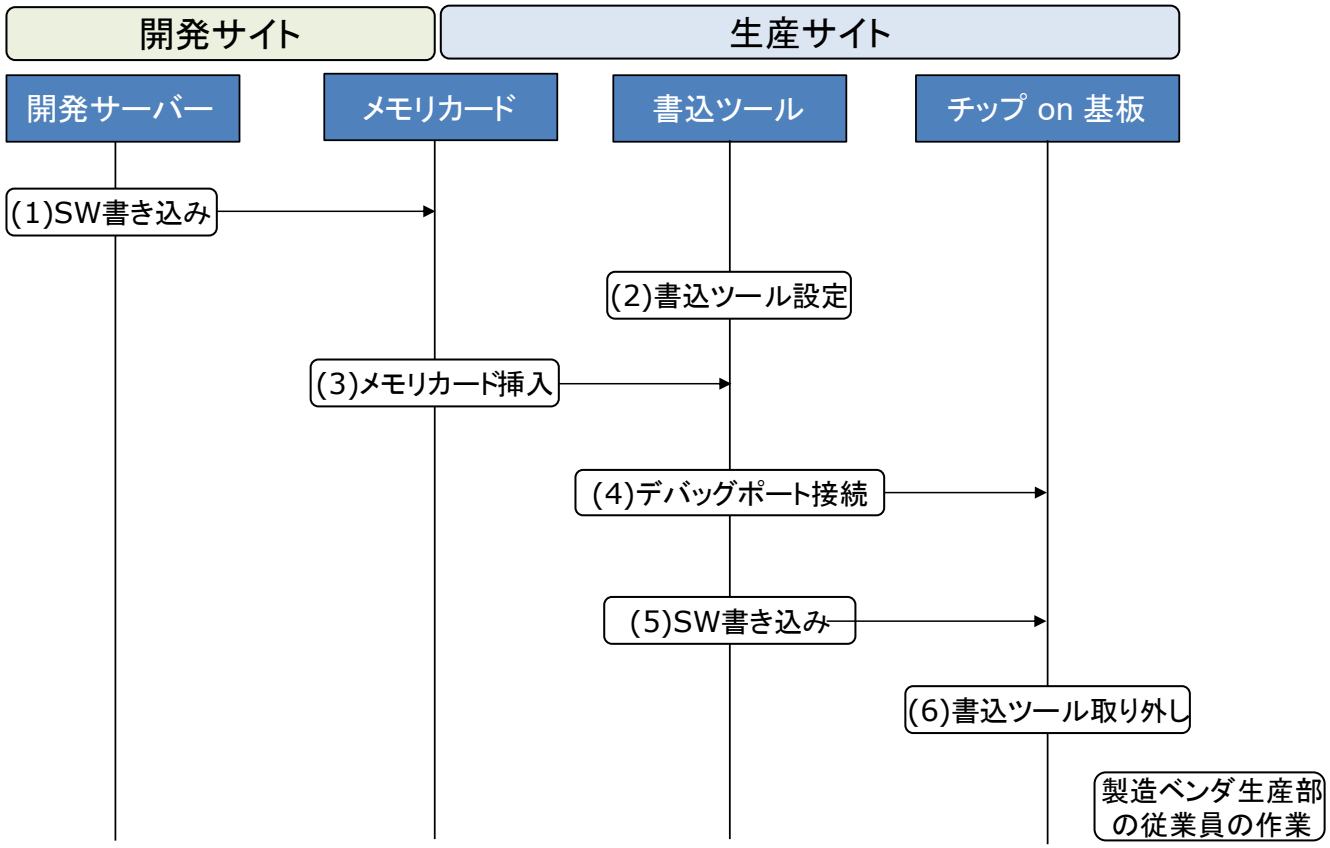
調査・検討結果をもとに、セキュリティ要求仕様書第0版を作成

目次

1. TOE概要
   - 調査結果に基づき、ソフトウェア印加に関わるライフサイクルと資産を記載
   - 廉価なIoT機器へのソフトウェア印加を対象としたTOE構成を作成。
2. セキュリティ課題定義
   - 5W法による分析、および、文献調査により抽出した脅威を記載。類似する脅威についてはグルーピング済み。
   - 脅威を実現するための攻撃方法を攻撃パスとして整理。
3. セキュリティ要件
   - 脅威および攻撃パスに対抗するためのセキュリティ機能を記載。
   - SESIP のセキュリティ機能要件との関係について記載。

ツールベンダへのヒアリングとソフトウェア印加のシーケンスの作成

機器ベンダにおける詳細な印加プロセスのシーケンス



5W法を用いた脅威分析

- 5W法を用いて洗い出した、ソフトウェア印加に想定される脅威例

#	資産	Where	When	Who	Why	What
1	書き込み対象のSW	開発サーバー	(1) SW書き込み	第三者	故意	改ざんされたSWをメモリカードに書き込む
2	書き込み対象のSW	開発サーバー	(1) SW書き込み	第三者	故意	SWデータを詐取
3	書込ツール設定情報	書込みツール	(2) 書込ツール設定	第三者	故意	不正な書き込みがされるように設定を改ざん
4	書き込み対象のSW	メモリカード	(3) メモリカード挿入	第三者	故意	不正なSWが保存されたメモリカードを挿入
5	書き込み対象のSW	メモリカード	(3) メモリカード挿入	第三者	故意	メモリカード上のデータを詐取する
6	書き込み対象のSW	書込みツール	(4) デバッグポート接続	第三者	故意	不正なSWの書かれたメモリカードが挿入された不正な書込みツールを接続する
7	書き込み対象のSW	書込みツール	(4) デバッグポート接続	第三者	故意	非正規のチップに書込みツールを接続する
8	書き込み対象のSW	書込みツール	(5) SW書き込み	第三者	故意	SWを書き込まない

ソフトウェア印加における攻撃パス

- ソフトウェア印加に対する脅威について、攻撃パスを用いて詳細に分析
  - 攻撃パス: 脅威について攻撃目標、攻撃者のモデル、攻撃対象、攻撃の手順を列挙したもの

#	資産	Where	When	Who	Why	What
4	書き込み対象のSW	メモリカード	(3) メモリカード挿入	第三者	故意	不正なSWが保存されたメモリカードを挿入

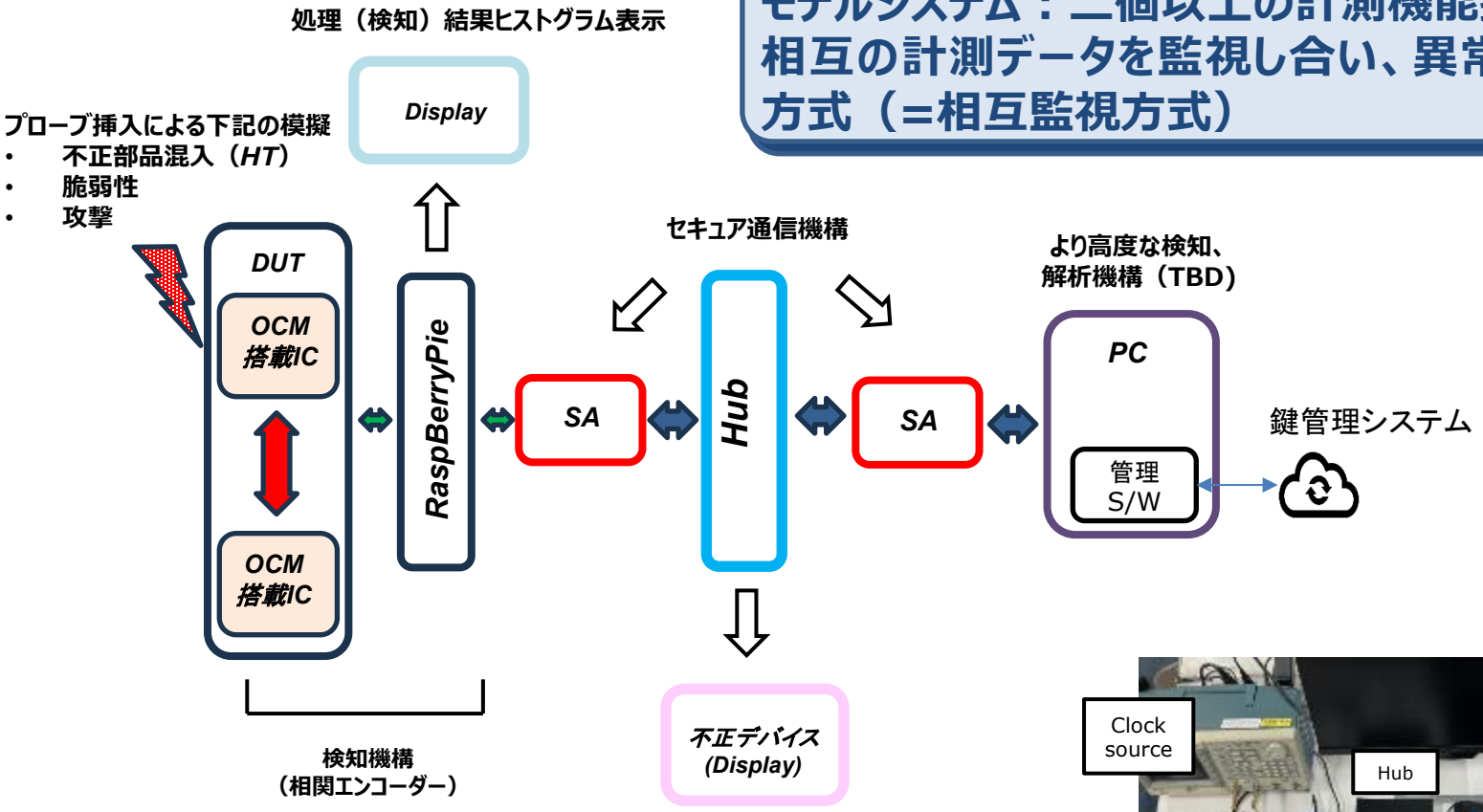
4番目の脅威について想定される攻撃パス

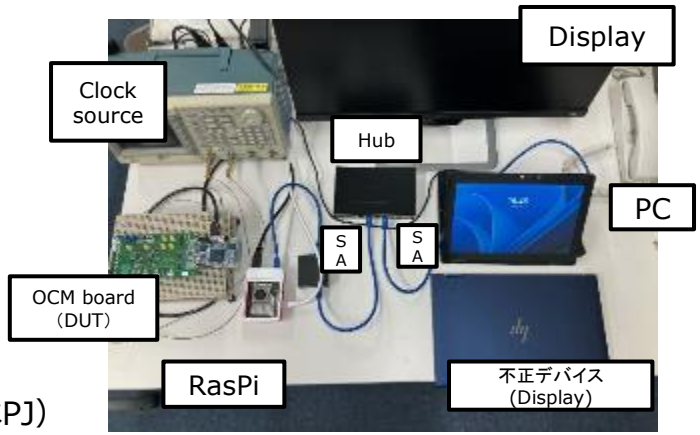
攻撃目標	印加されるソフトウェアの完全性を侵害
攻撃者のモデル	• 不正なソフトウェアを開発できる • 生産サイトに侵入し、メモリカードへアクセスできる
攻撃対象	デバッグインターフェースからの書き込みへのセキュリティ保護機構を持たない組み込み機器
攻撃手順	1. 攻撃者が不正なソフトウェアを開発する。 2. 攻撃者は不正なソフトウェアをメモリカードへ書き込む。 3. 攻撃者が生産サイトの正規のメモリカードと不正なソフトウェアを書き込んだメモリカードを入れ替える。 4. 正規の生産者が入れ替えられたメモリカードを印加ツールへ挿入する。 5. 正規の生産者が印加ツールを機器へ接続し、機器へソフトウェアを印加する。

〔４－１〕不正部品混入検知

2024.11　EdgeTech展POCデモンストレーション

モデルシステム：二個以上の計測機能搭載チップが相互の計測データを監視し合い、異常を検知する方式（=相互監視方式）



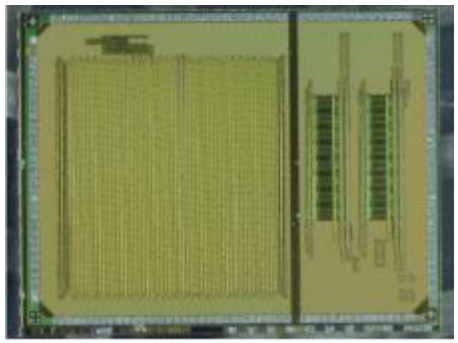


★関連特許（出願済み）の技術デモンストレーションに成功

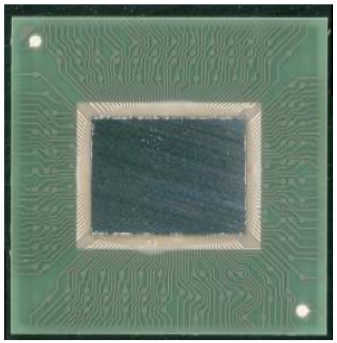
特願2021-157183「改竄検知回路及び改竄検知方法」（特許査定、登録済み）
特願2024-201299「異常検知装置、異常検知方法及び異常検知プログラム」（本PJ）

セキュアパッケージング技術の開発

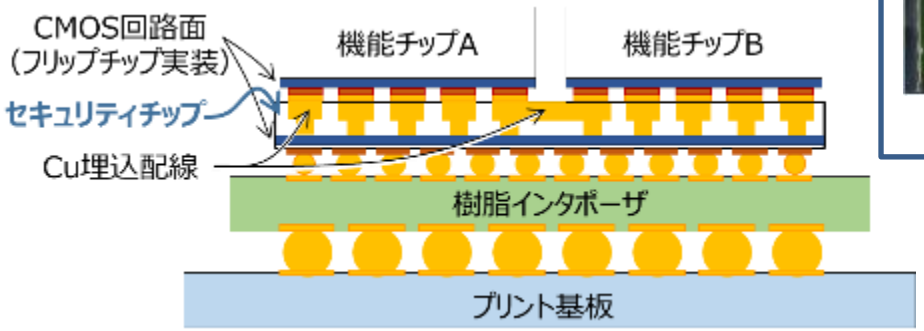
貼り合せ技法によるセキュアパッケージングの構造と製造工程の開発を継続



CMOSチップ（回路面）



FCパッケージ（シリコン裏面）



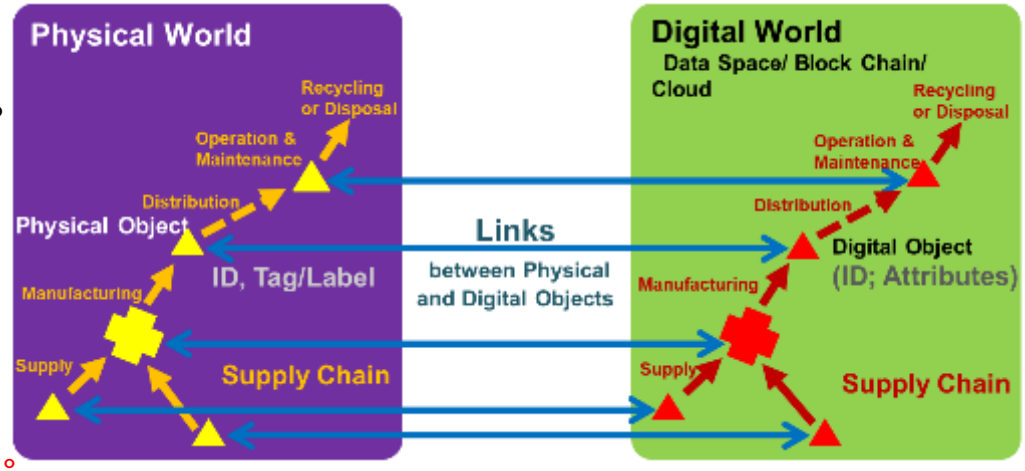
★関連特許（出願済み）の製法を開発、製造工程を具体化

特願2017-241052「半導体装置」（特許査定・登録済み）
特願2021-163849「積層半導体パッケージ」（先行PJ）

〔４－２〕個体ID管理

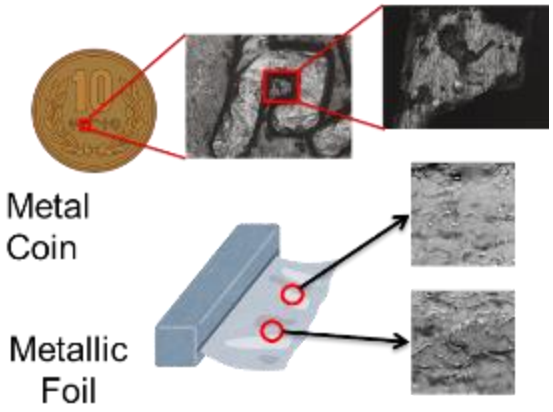
実施項目〔４－２〕個体ID管理の内容

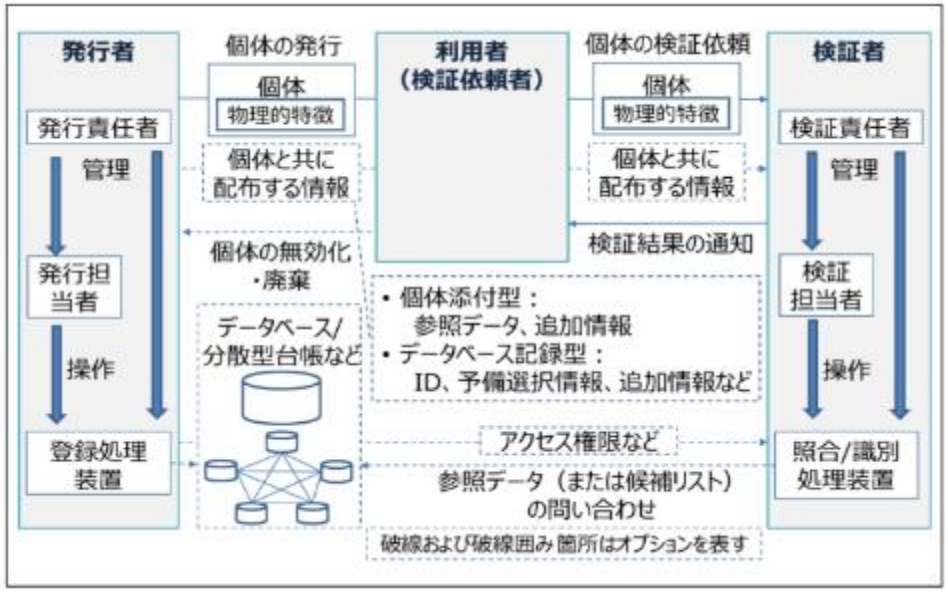
- サプライチェーンにおいては、半導体や電子機器の、IDによる個体管理が重要である。
- IDによる半導体や電子機器の個体管理は、悪意をもった攻撃者が個体とそのIDとの対応関係を偽装できると根底から崩れる。



Cf) 欧州を中心に導入が進むDPP (Digital Product Passport)では、典型的にはQRコード等が想定されている。

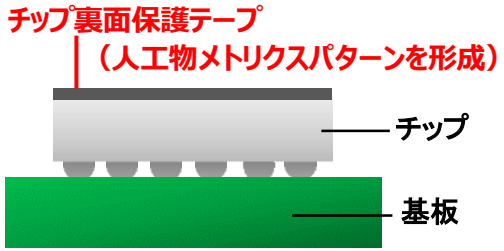
- **人工物メトリクス(物体に固有のパターン)と暗号技術でこの問題を抜本的に解決する。**





人工物メトリックシステムを利用した個体管理の一般的な運用モデル
人工物メトリクスを用いた個体管理技術ガイダンス 初版, 産業技術総合研究所CPSEC テクニカルレポート CPSEC-TR-2022001 (2022年1月)

〔4－2〕研究開発内容　A）



個体IDと
人工物メトリクスパターン
との対応関係を証明する
個体ID証明書
（暗号技術を活用）

- IDによる半導体や電子機器の個体管理は、悪意をもった攻撃者が個体とそのIDとの対応関係を偽装できると根底から崩れる。
- 人工物メトリクス(物体に固有のパターン)と暗号技術でこの問題を抜本的に解決する。

A）人工物メトリクスを用いた個体ID付与・活用技術の研究開発

産業技術総合研究所、横浜国立大学、九州大学の保有技術と知見をベースとする

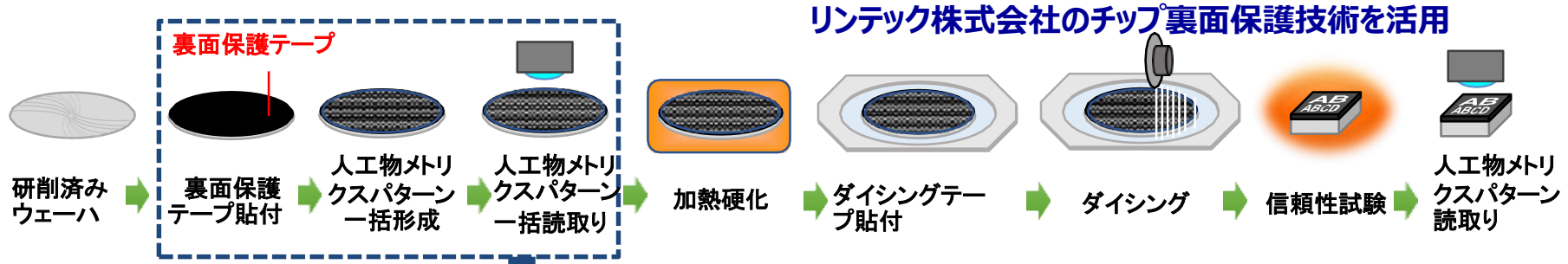
1. 個体とそのIDの対応関係が偽装できない個体ID付与技術を、人工物メトリクス技術（材料、パターン形成、パターン読取り、パターンデータ形成、パターンデータ照合）と、暗号応用技術（パターンデータとIDとの結合・登録・検証）から研究開発する。
2. 材料やメディアの違いによらない基盤技術をまとめ、コンセンサス形成を図る。

- 半導体ウェーハ裏面保護テープへのインクジェット印字に基づく人工物メトリックシステムを開発中
- 電子線リソグラフィにおける電子線レジスト倒壊現象を活用してシリコン表面に形成されるナノメータスケール3次元構造NAMを用いた人工物メトリックシステムの照合精度と耐クローン性（精巧な贋物を拒否する能力）の評価方法の検討
- 1億個の個体を正確に区別できることを実証
- モノの署名技術（暗号理論）の個体ID管理への応用方法の検討
- JIS X 22387 策定・発行済

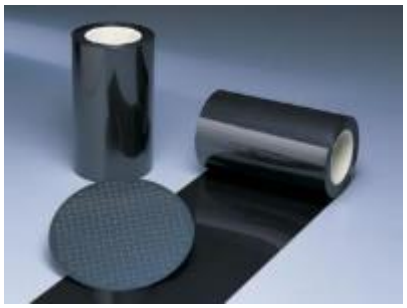
- ナノ人工物メトリクス基本文献 Matsumoto,T., et al. Nano-artifact metrics based on random collapse of resist. Sci Rep 4, 6142 (2014).

〔4－2〕研究開発内容　B）

B）半導体チップへの一括個体ID付与技術の研究開発



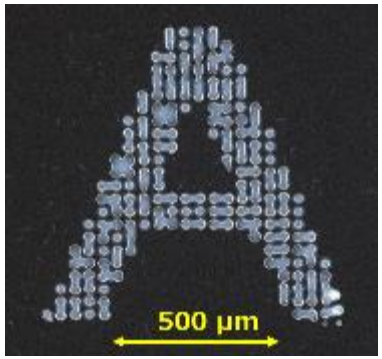
裏面保護テープ貼付装置に
人工物メトリクスパターン形成・
読取り機構を追加



- A)の技術と、B)の技術を合わせて実装する装置技術を開発する。
- 開発された技術のパイロット実証を、C)のシステムとも接続して実施。

2つのアプローチで研究開発実施中

- 「チップ裏面保護テープ」上に複製困難な特殊インクジェット印刷を施し得られる固有の特徴を用いるインクジェット印刷利用人工物メトリクスに基づく方式



- 電子線リソグラフィにおける電子線レジスト倒壊現象を活用してシリコン表面に形成されるナノメータスケール3次元構造を「チップ裏面保護テープ」と一体化したナノ人工物メトリクスに基づく方式

〔4－2〕研究開発内容　C）

C）IDに対応する個体の属性を照会・検証するシステムの研究開発

目標：

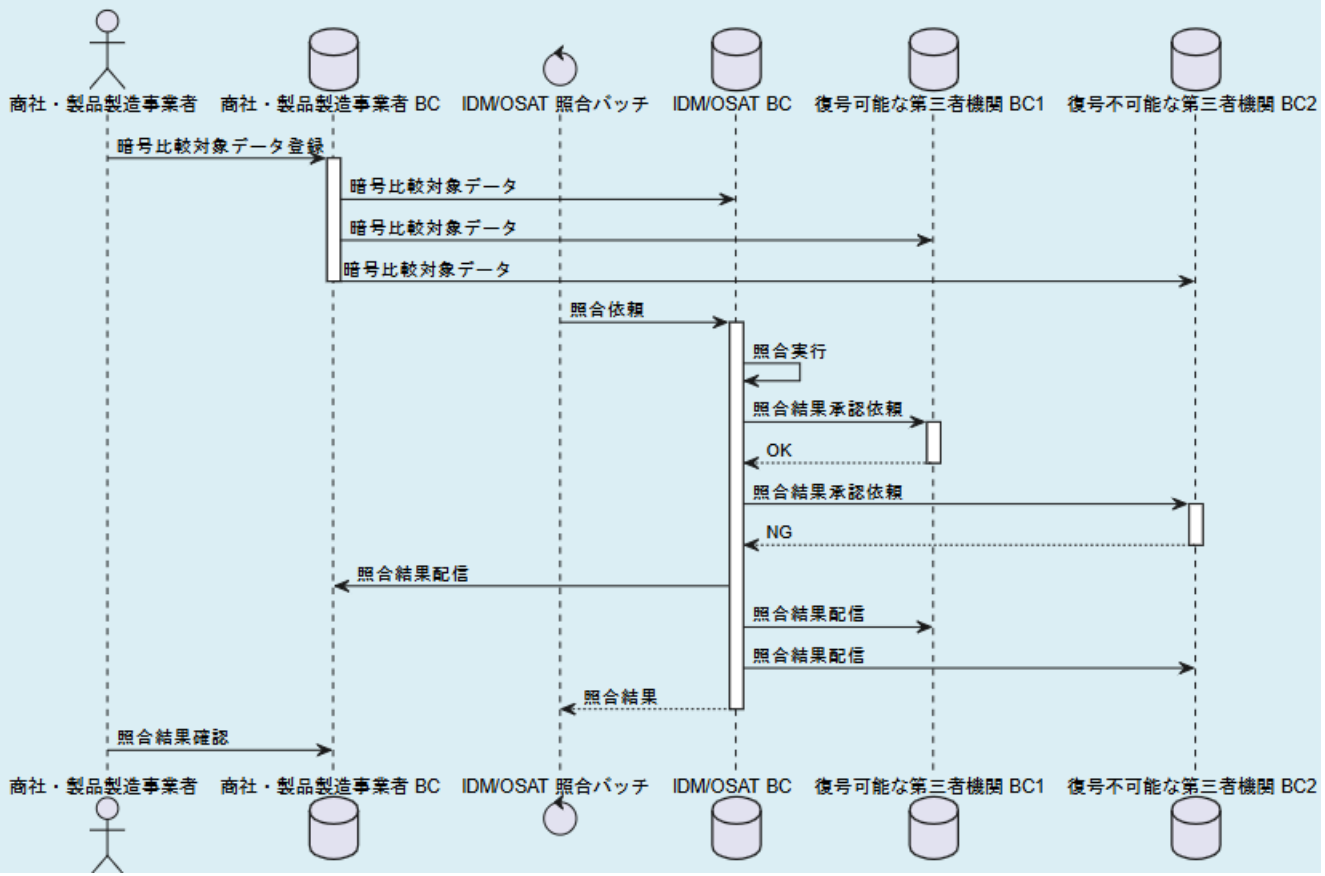
三菱電機株式会社のブロックチェーン活用データ共有・管理技術をベースとする

複数ステークホルダー間でデータをセキュアに管理しながら透明性の高いトレーサビリティを実現するシステムを開発する。

進捗状況：

要件定義のため、データ連携関連の各種調査を行い、個体管理と人工物メトリクスの管理を疎結合とするシステムを開発する方針を定めた。

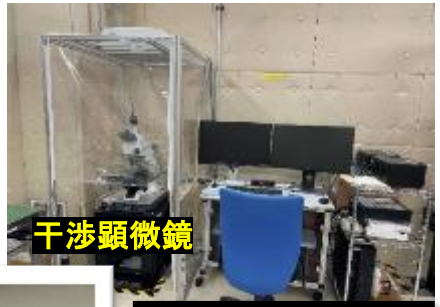
当該システムの基本設計を実施し、試作・評価に備えている。



評価装置等の整備


電子顕微鏡

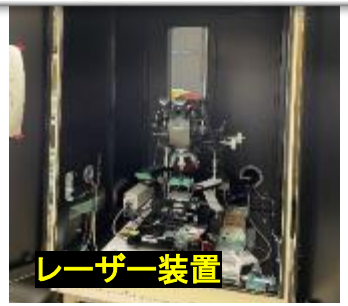

ナノフレーザ
（走査型プローブリソグラフィ）


干渉顕微鏡


エミッション顕微鏡


サイドチャネル評価


オープンクリーン装置


レーザー装置


実験室（写真は1スパン）
→ 4 スパン に拡張（24年）
→ 7 スパン に（25年～）

NAM研究設備（左・上）と半導体の脆弱性評価設備（右・下）

＜評価項目３＞マネジメント

（1）実施体制
（2）研究資金の効果的、効率的な活用
（3）国民との科学・技術対話に関する取組

（1）実施体制

研究開発機関

	機関名
代表提案者	産業技術総合研究所
共同提案者	株式会社SCU
	リンテック株式会社
	東京大学
	神戸大学
再委託先	三菱電機株式会社
	横浜国立大学
	九州大学
	東北大学
	奈良先端大
	ソニーセミコンダクタソリューションズ

（1）実施体制

実施項目と担当組織

		産総研	横国大	九州大	SCU	三菱電機	ソニーSS	東北大	奈良先端大	リンテック	東京大学	神戸大学
〔1〕半導体設計フェーズにおける検証	〔1-1〕半導体設計IP検証	－	－	－	●	－	－	●	－	－	－	－
	〔1-2〕チップ設計検証	－	－	－	－	－	－	－	－	－	●	●
	〔1-3〕最先端攻撃・攻撃対抗技術	●	－	－	●	●	－	－	－	－	－	－
	〔1-4〕セキュリティ仕様への適合性検証	●	－	－	●	－	●	－	－	－	－	－
〔2〕半導体製造フェーズにおける検証	〔2-1〕半導体設計データ管理	－	－	－	●	－	－	－	－	－	●	●
	〔2-2〕半導体解析による検証	●	－	－	－	－	－	－	－	－	－	－
〔3〕ソフトウェア印加フェーズにおける検証	〔3-1〕ソフトウェア組込み段階でのセキュリティ要求仕様と検証技術	●	－	－	●	－	－	－	－	－	－	－
〔4〕電子機器設計・製造・運用フェーズにおける	〔4-1〕不正部品混入検知	－	－	－	●	－	－	－	●	－	－	●
	〔4-2〕個体ID管理	●	●	●	●	●	－	－	－	●	－	－

●：各実施項目のリーダー所属組織　　ソニーSS：ソニーセミコンダクタソリューションズ

（２）研究資金の効果的、効率的な活用

NEDO委託業務 事務処理手続き、経費計上の手引きに従い適切に計上をしている。

年度初めに予算計画を実施して、毎月管理している。

また、その他経費、機械設備費等 検収毎に、エビデンスをまとめ、毎月経理部門の確認を実施している。

2023年度中間検査（中間）、（年度末）、2024年度中間検査（中間）を受けて、経費が正しく計上されていることをNEDOに監査していただき、合格している。

（３）国民との科学・技術対話に関する取組

外部発表等成果

本資料作成時点（2025年5月8日）迄の成果の登録状況は以下の通り。
[]内は、23年度から現在までの年度毎の件数。

（1）研究発表・講演	57件	[13件、39件、5件]
（2）論文	2件	[0件、2件、0件]
（3）受賞実績	3件	[1件、2件、0件]
（4）成果普及の努力（プレス発表等）	8件	[4件、3件、1件]
（5）特許等（知財）	7件	[3件、4件、0件]

※9/15までに、
・英文論文誌（採録決定）、HWS研究会（7月）、
IoTセキュリティフォーラム、などでの発表も計画中。

ハードウェアセキュリティ啓発書の出版(2025.03)