資料3

研究開発戦略専門調査会
2022-02-22

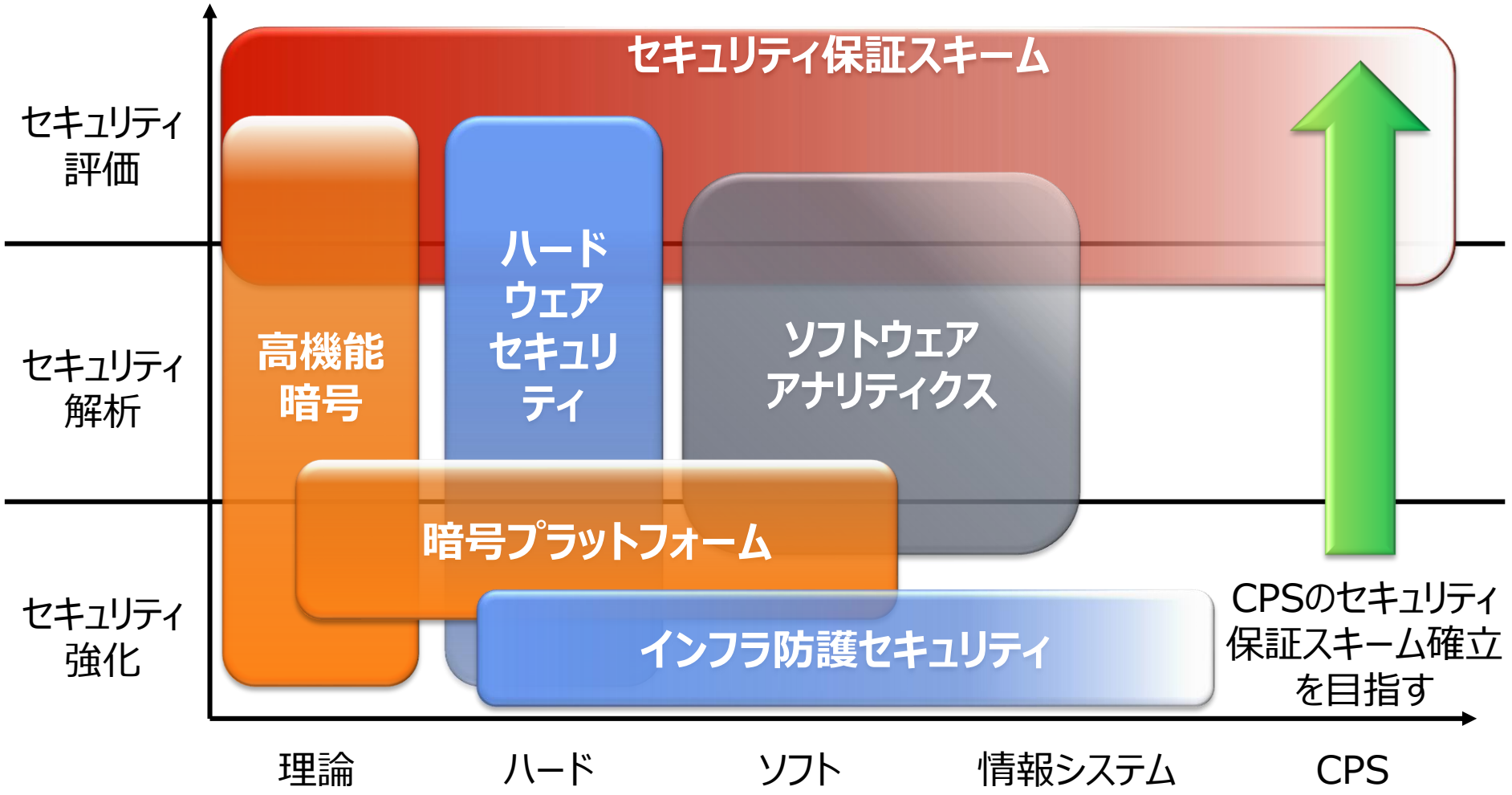
# ハードウェアセキュリティ実現に向けた種々の課題

（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（CPSEC）
副研究センター長／ハードウェアセキュリティ研究チーム長
川村　信一

**サイバーフィジカルセキュリティ研究センター (CPSEC)**
**2018年11月発足**
**（国立研究開発法人）産業技術総合研究所（AIST)**
**情報・人間工学領域（７領域のひとつ）に設置**

チーム数：6　連携研究室：1　総勢：124名（2021年12月1日現在）
研究拠点：
臨海副都心センター、つくばセンター、関西センター
研究目標：
サイバー／フィジカル空間が高度に融合した社会の
セキュリティを実現する強化技術や保証スキーム等の研究を
推進し、経済発展や社会課題解決の実現に貢献する。

- セキュリティ保証スキームの確立（セキュリティを測定可能に）
  - 理論→ハード／ソフト→情報システム→CPSに展開

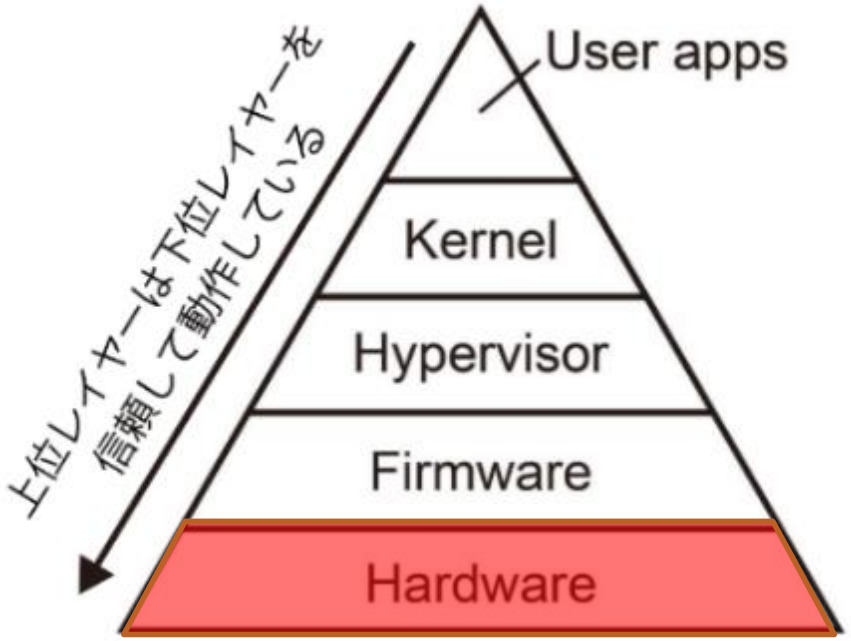


# 目次

- 信頼の基点
- サイドチャネル攻撃
- ハードウェアトロージャン（不正機能の挿入）
- リバースエンジニアリング
- サプライチェーン
- まとめ

# 様々なシステムの動作は、ICチップのハードウェアの安全性に依拠

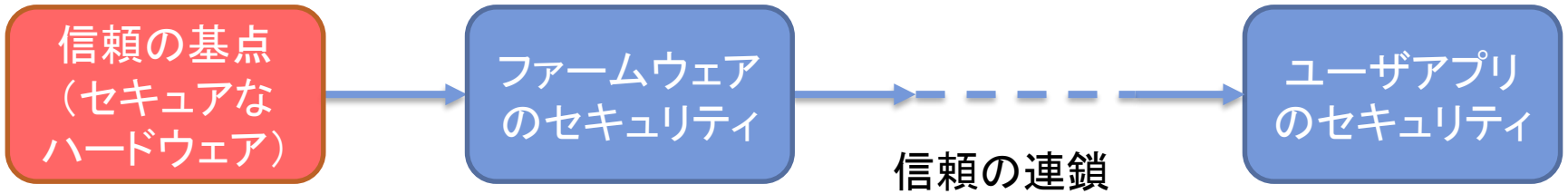
# 様々なシステムの信頼の基点はハードウェア





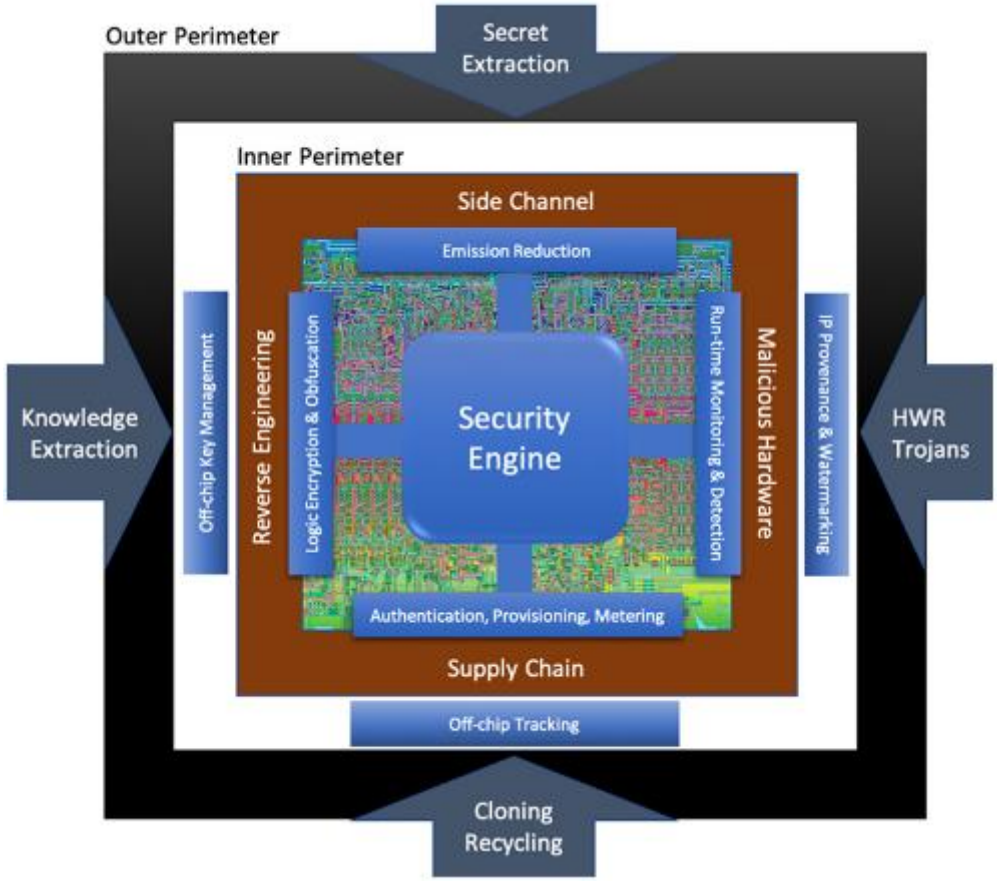
©Y. Hayashi, NAIST

最終的に情報を処理しているのはハードウェア（物理層）であり、その信頼性が低下した場合、システム全体のセキュリティが低下する恐れがある



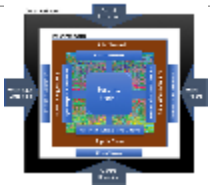
# 同分野のDARPAの取り組み

- Defense Advanced Research Projects Agency (DARPA) project called Automated Implementation of Secure Silicon (AISS) での攻撃Surface
  - サイドチャネル
  - マリシャスハードウェア（ハードウェアトロージャン等）
  - リバースエンジニアリング
  - サプライチェーンセキュリティ
- この４つの切り口について一般的な考察を試みる




https://www.darpa.mil/news-events/2019-03-25 より引用

# DARPA AISSプロジェクトのシンボルを再配置



Secret Extraction

HWR Trojan

Knowledge Extraction

Cloning Recycling

Outer Perimeter

IP Provenance & Watermarking

Off-chip Key Management

Off-chip Tracking

Inner Perimeter

Side Channel

Malicious Hardware

Reverse Engineering

Supply Chain

Emission Reduction

Runtime Monitoring & Detection

Logic Encryption & Obfuscation

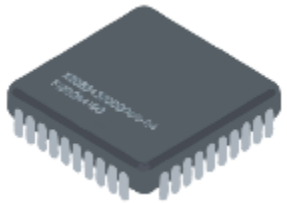
Authentication, Provisioning, Metering

Security Engine

# サイドチャネル攻撃

# 内部情報を盗む例・・・サイドチャネル攻撃

装置内部を直接解析することなしに、装置の処理時間や消費電力や放射電磁界等を用いて、内部の秘密情報（例えば暗号の鍵やAIの学習パラメータ）を推定する攻撃手法

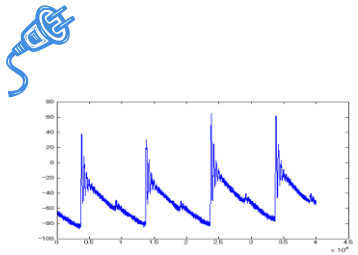


装置（ICチップ等）

理論や単純な実装では想定していなかった種々の漏洩チャネルが存在

（何れもイメージ）

タイミング

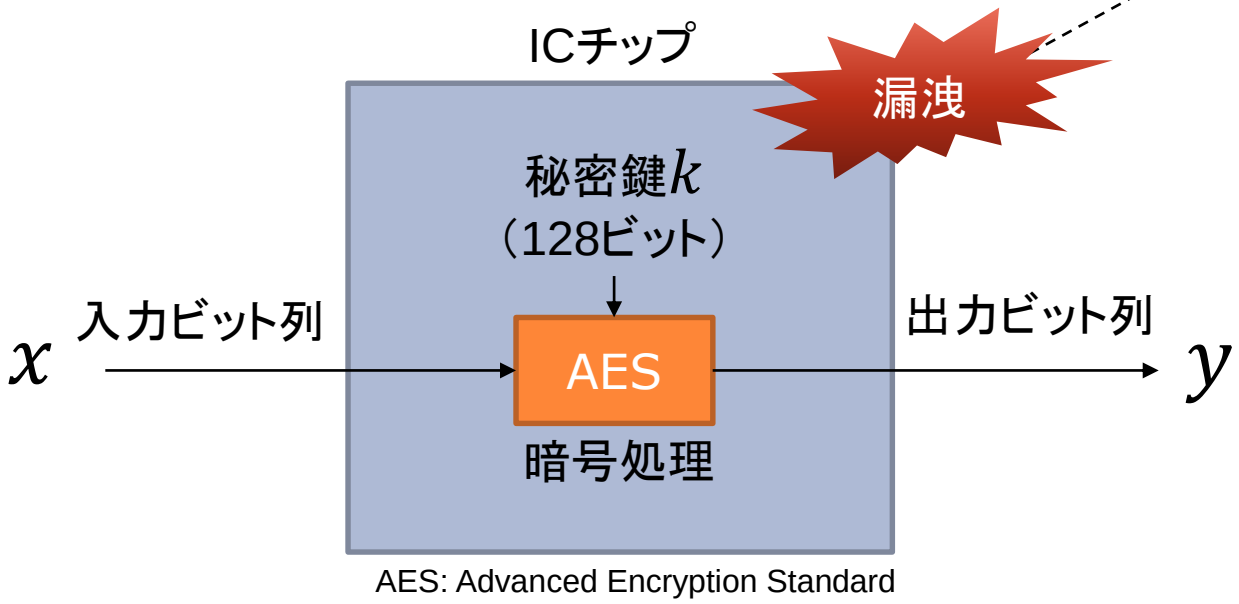


消費電力

放射電磁界

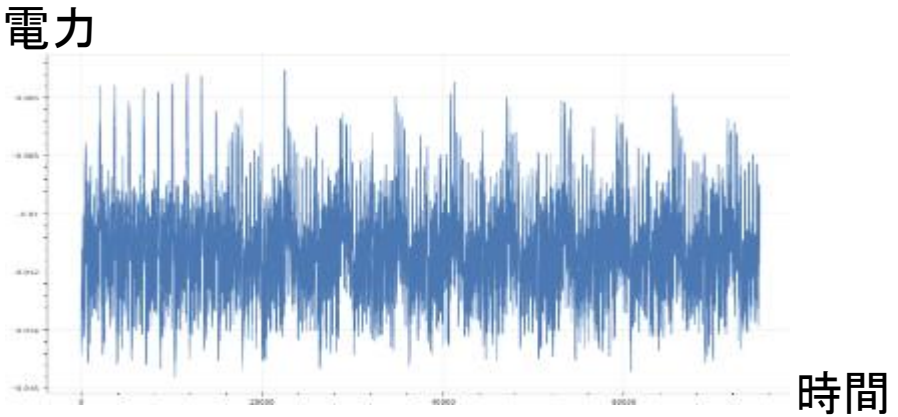
・・・・・

# サイドチャネル攻撃




AES: Advanced Encryption Standard

サイドチャネル情報
- 消費電力波形
- 漏洩電磁波
- 無線信号の変動、温度、光など様々




暗号処理時の消費電力波形

対策
- マスク対策（鍵一定でも処理が変化）
- ジッター（時間的変動）
- 閾値実装（複数ビットで1ビットを表現）

# サイドチャネル攻撃の整理

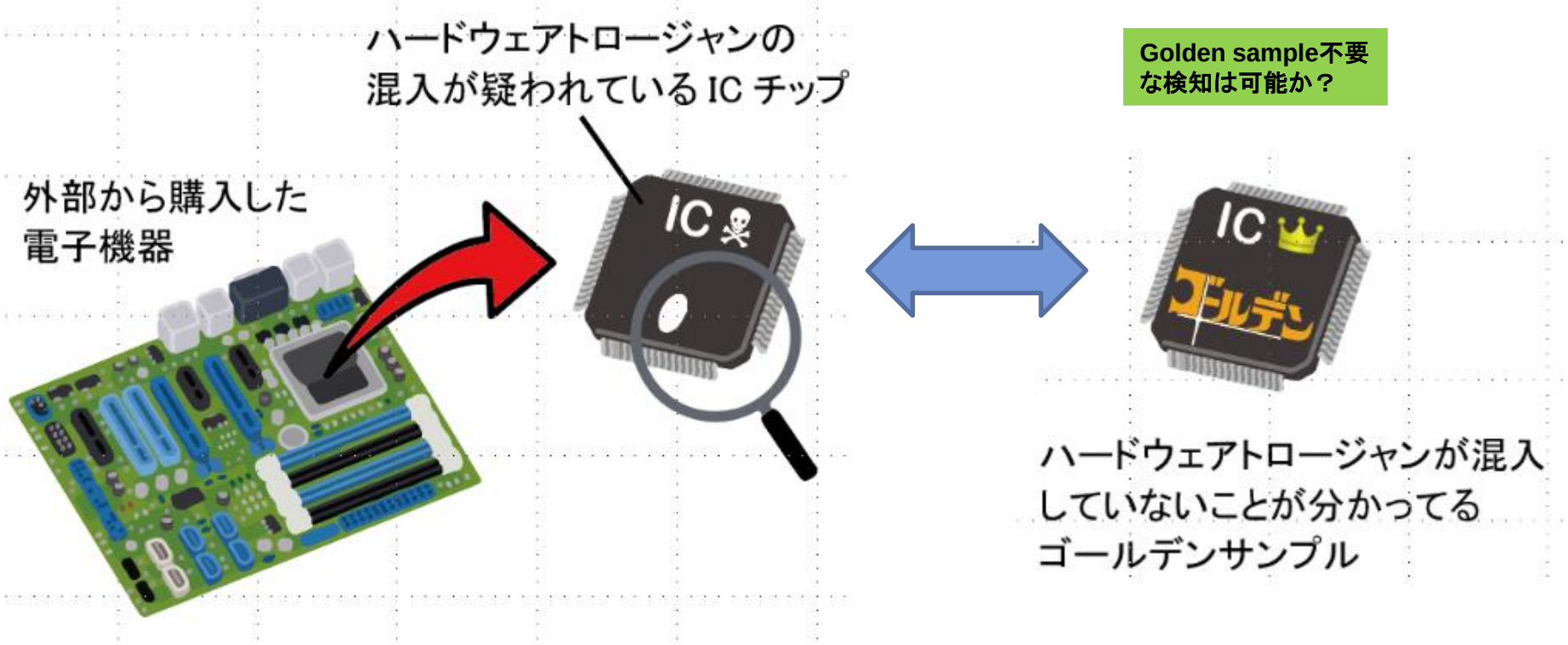
- ICチップ内の暗号鍵への攻撃として出現
- フォールト攻撃（故障利用攻撃）なども同様
- 金融系等のスマートカード（ICカード）の侵入試験では重要な評価項目
- セキュリティ保証スキームなど検討するうえで分かり易いモデルを提供
- 対策や制度が成熟しつつあるが、異分野では顧慮されていない現実も

# ハードウェアトロージャン

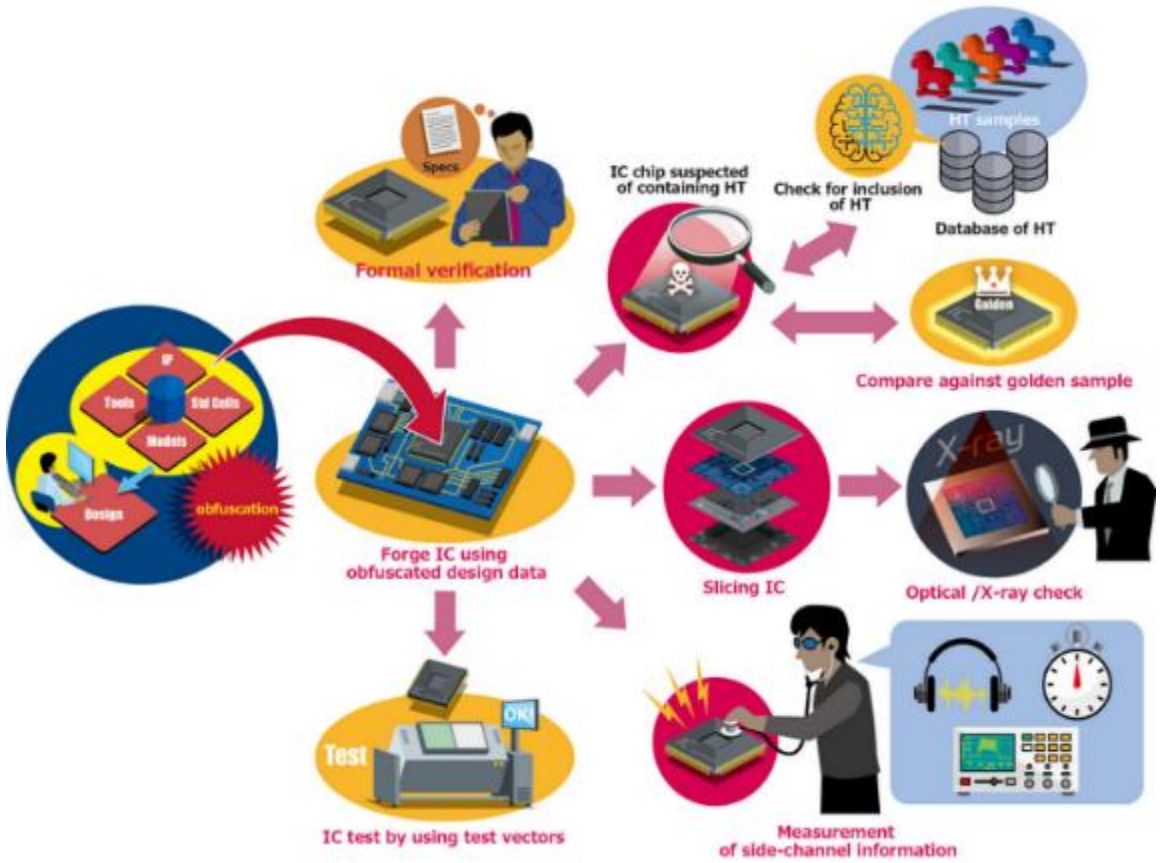
# ハードウェアトロージャン（HT)とは？

ICチップや基盤上に密かに挿入された不正回路

- HTによる異常動作はデジタル社会にとって重大な脅威
- 米・中は多数研究助成（2018年までで米国147件、中国80件）
- Golden sample（GS）不要な対策の開発は挑戦的課題



# HT 実装の検出と実装困難化




HTの実装を検知するための様々なアプローチ


検出や実装困難化技術群とその相互関係

2002年—2018年のHT関連論文約800件を調査し引用関係から注目課題を抽出 (林・川村:”ハードウェアトロージャンの脅威と検出“,情報処理 Vol.61 No.6 June 2020)

# ハードウェアトロージャンの整理

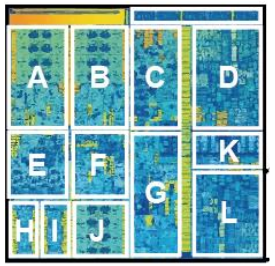
- チップやボード、あるいはシステムに混入された不正機能全般
- ICチップでは国際分業などで挿入機会は増大
- 信頼の基点としてのICチップにとって重大な脅威
- 対応の方法論は十分には確立していないが戦略的取組が必要
- 米中は積極的に取組んでいる

# リバースエンジニアリング

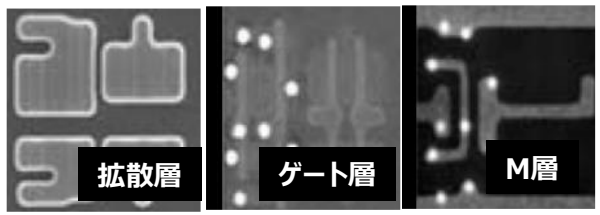
# ICチップのディレイヤリングから設計情報の再生まで

**イメージデータから回路機能や特性を含むデータ生成する流れ**

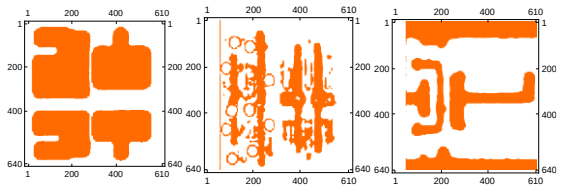
着目する部分の選択
事前知識の利用



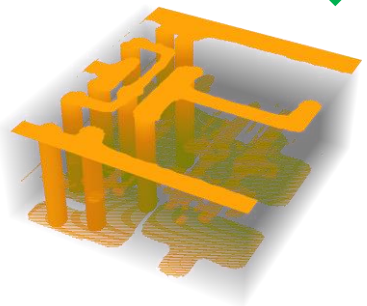

画像データの取得（注）
（不完全な部分を含む）イメージデータ



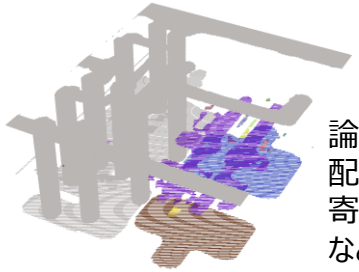

画像認識
含む推定や補完技術



3 D構造の再構成
逆レンダリング技術



回路要素の認識
推定と連結ラベリング技術



論理ゲート抽出
配線トレース
寄生成分抽出
など

各種EDAツールの利用
静的／動的シミュレーション

近年、画像認識には深層学習技術が適用されている

理想的には、プレシリコンの問題に還元される

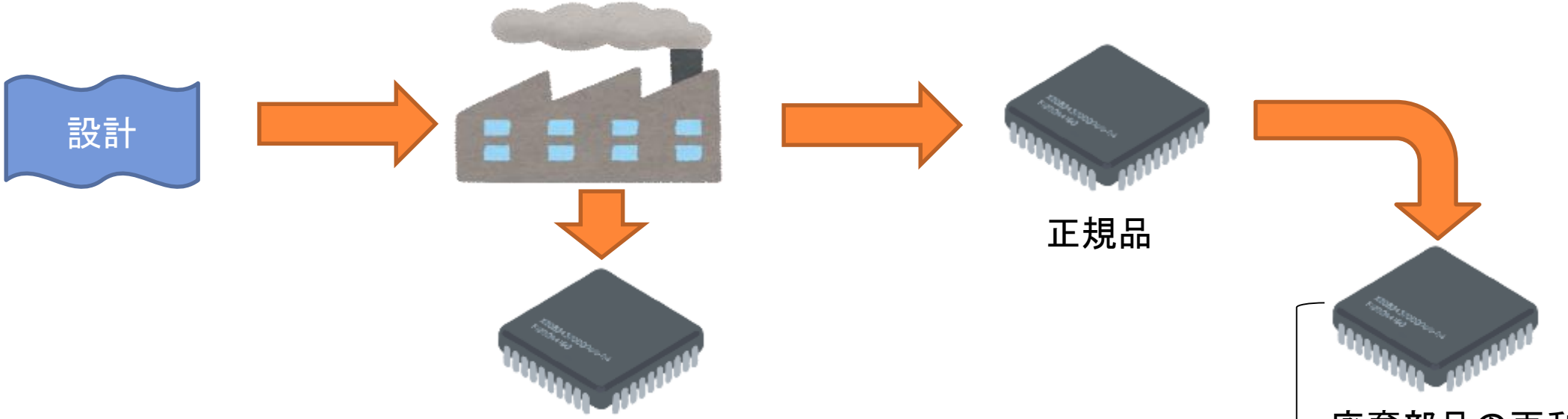
注）中島蕃，"LSIの総合的な解析技術について", 2008年度OKIエンジニアリング技術論文，(https://www.oeg.co.jp/thesis/index.html#a2008)より

# リバースエンジニアリングの整理

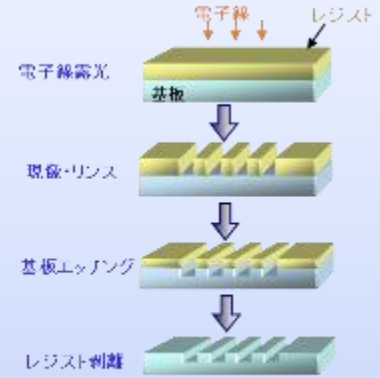
- 故障解析やセキュリティ分析で必要となる基礎的技術
- ICチップの知財の流用を見つけるための解析でも利用される
- DARPAの図では脅威の位置づけだが、基礎技術としての掘り下げも重要
- 対策として論理回路の難読化や暗号化も研究されている

# サプライチェーン

# デバイスの不正流通と対策技術

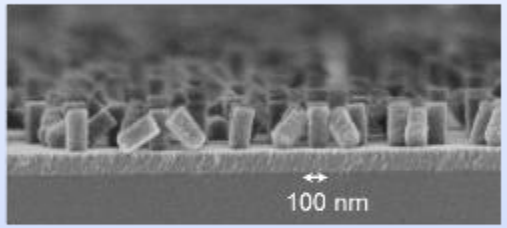



物理的に複製できない固有のID（NAM）を開発中




電子線リソグラフィの基本プロセスフロー

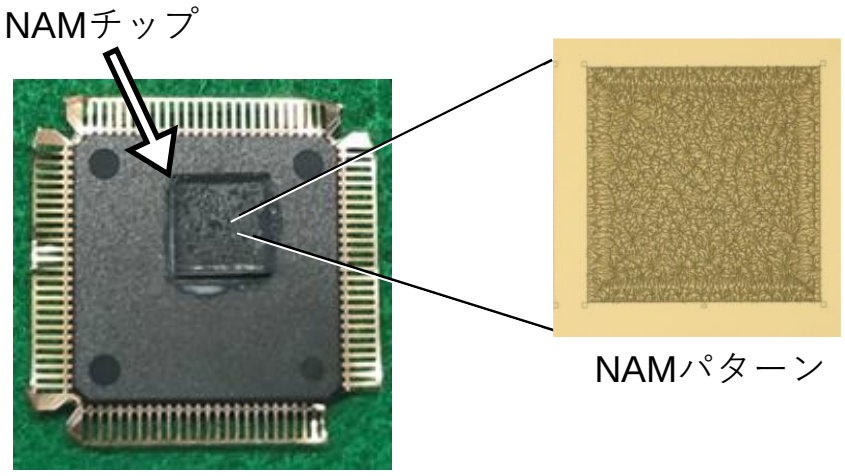
Nano-artifact metrics




現像・リンス後の倒壊したレジストパターンのSEM画像

# ナノ人工物メトリクス(NAM)

- 用途： 付加価値の高い製品や部品の真贋判定に使用
  - 現在はNEDO-PJで、ALエッジデバイスの個体認証実用化の研究開発を実施
- 優位点： 物理的な複製困難性を実現
  - 半導体製造工程でのバラツキに起因するプロセスを用いて、ナノスケールのランダムなパターンを形成しているので、複製は困難
- 特徴： チップ形状であり、各種の製品・部品への実装が容易
  - シリコンあるいは石英であり、非常に安定した材料で形成されている




NAMチップを表面実装した
半導体パッケージの写真

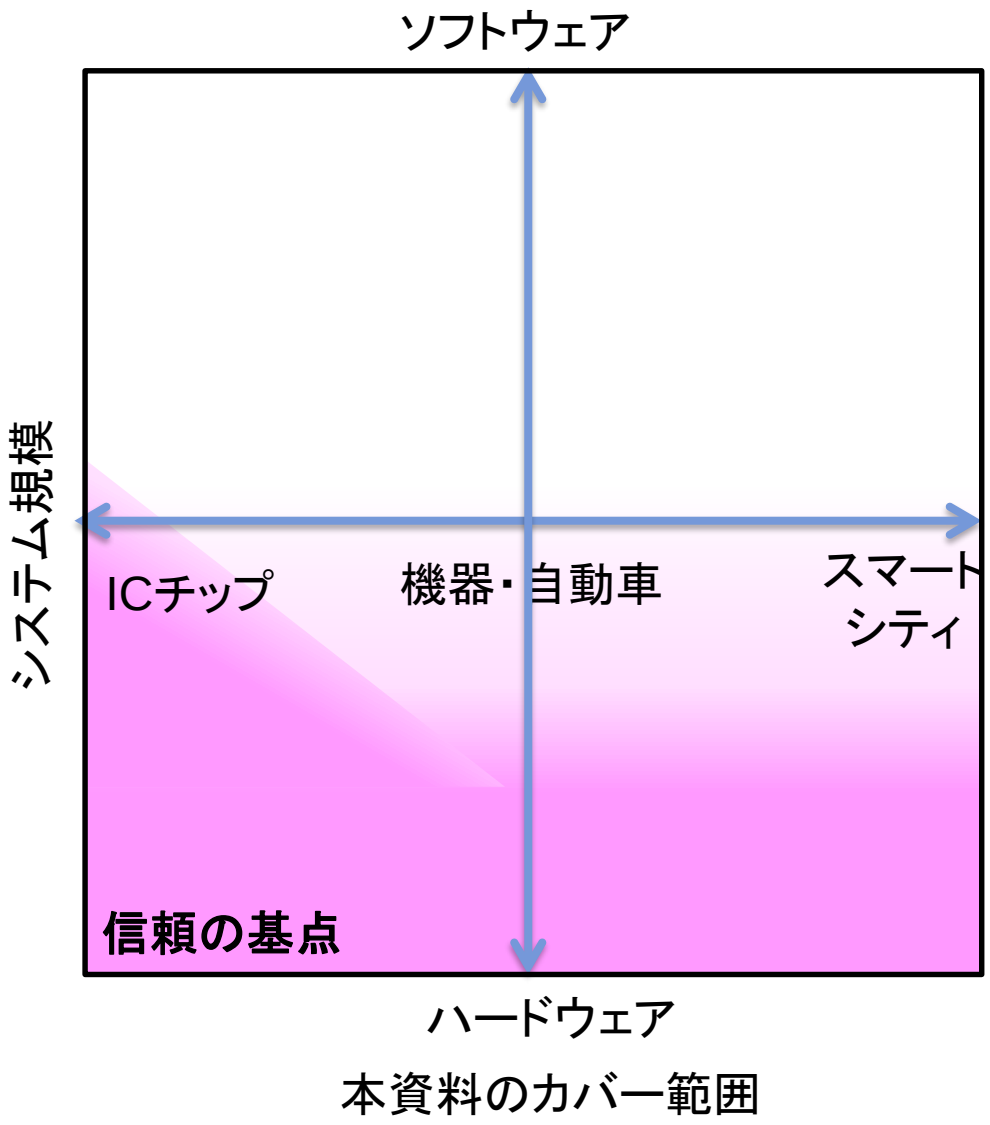
◆ NEDO-PJ での取組み
- 産総研： 全体取り纏め
  NAMパターン形成技術
  干渉画像取得技術
- 横浜国大： 照合技術
- 九州大： 画像取得技術（小型化、他）
- 早稲田大： 表面実装技術
- 北海道大： 電気的読出し技術

# サプライチェーンの整理

- ICチップに限らず守るべき対象としての認識が高まっている
- 偽物対策としては個体識別と個体のトラッキングが解決手段の一つ
- 正常なICチップの流通のためには他の３つのアプローチの確立も前提となる

# まとめ

- デジタル社会のセキュリティを守る
  - ハードウェアが信頼の基点
  - 各種攻撃技術と対策技術の研究振興が必要
    - サイドチャネル
    - ハードウェアトロージャン
    - リバースエンジニアリング
    - サプライチェーン




本資料のカバー範囲

# ご清聴ありがとうございました