ハードウェアセキュリティ研究の展望

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

略歴

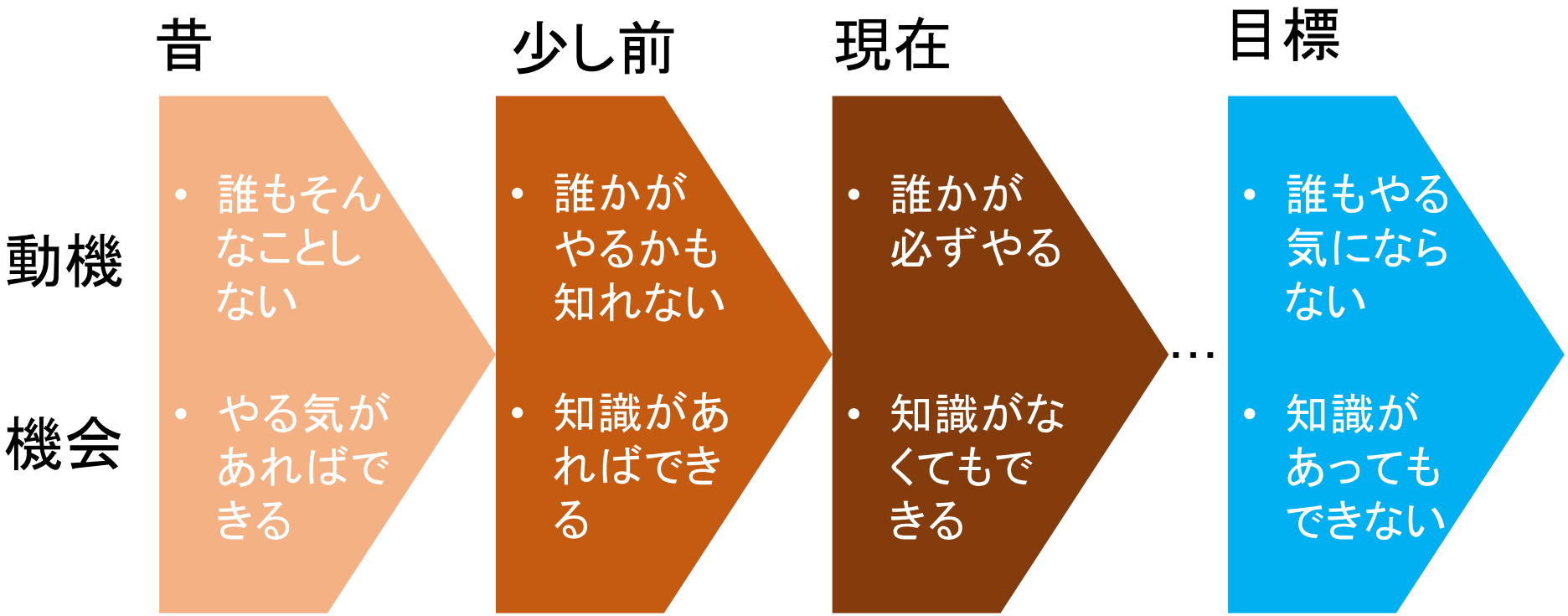
- 85年- （株）東芝 入社　総合研究所（現、研究開発センター）配属
  - ICカードの暗号機能開発、暗号の耐タンパー実装方式の研究などに従事
  - 96年　工学博士
- 09年-11年　産総研　RCIS 副研究センター長　（休職出向）
- 12年-現在　（株）東芝　研究開発センター　技監
- 12年-14年　産総研　RISEC 招聘研究員(兼)
- 18年11月-現在　産総研　CPSEC 副研究センター長　兼ハードウェアセキュリティ研究チーム長

RCIS=情報セキュリティ研究センター
RISEC=セキュアシステム研究部門
CPSEC=サイバーフィジカルセキュリティ研究センター

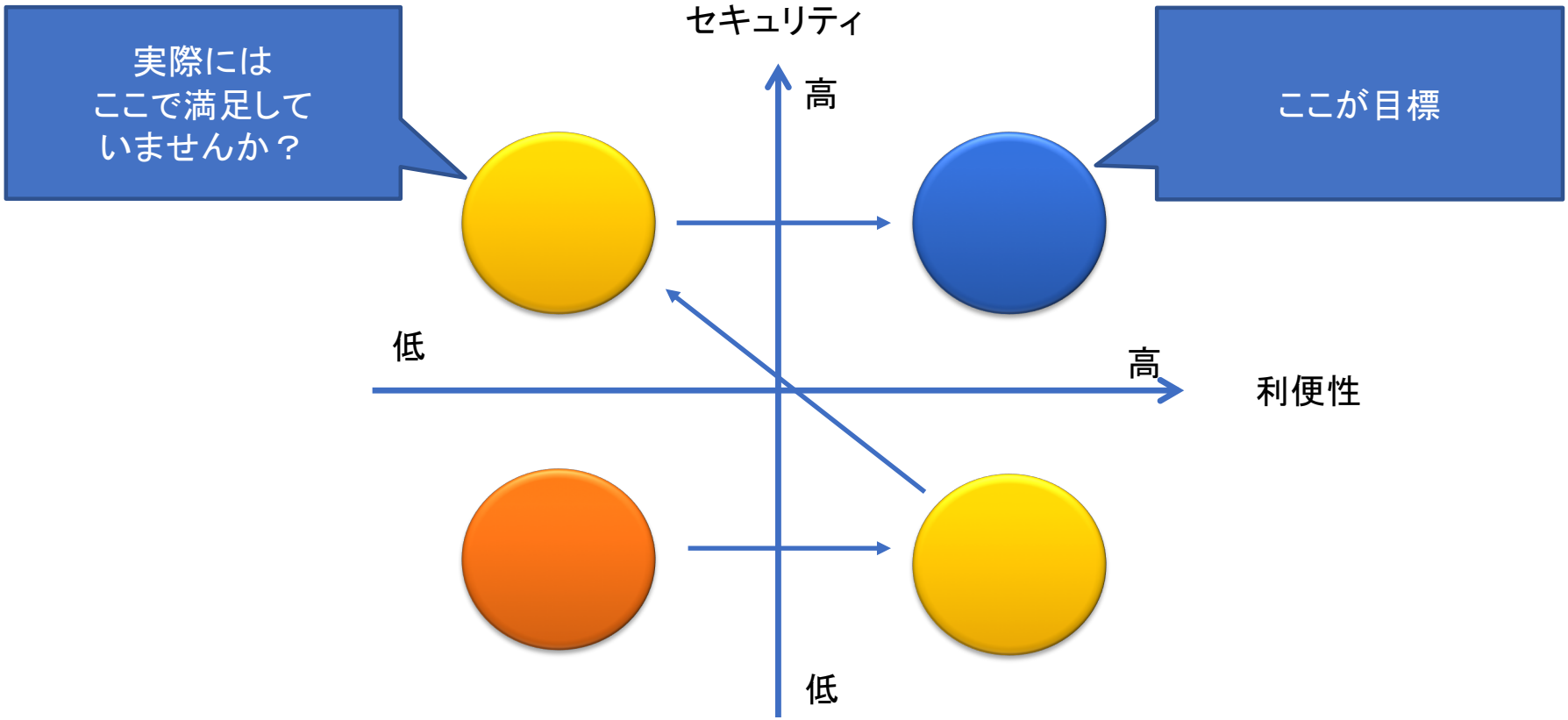
メンバー

川村　信一	研究チーム長(兼務)
坂根　広史	主任研究員
今福　健太郎	主任研究員
堀　洋平	研究チーム付(兼務)
法元　盛久	招聘研究員
永田　真	招聘研究員/神戸大学　教授
林　優一	招聘研究員/奈良先端科学技術大学院大学　教授

セキュリティの脅威：動機＆機会

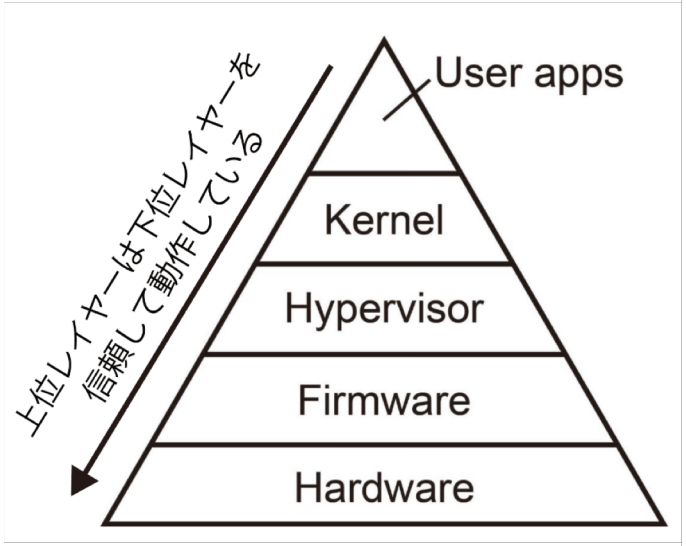


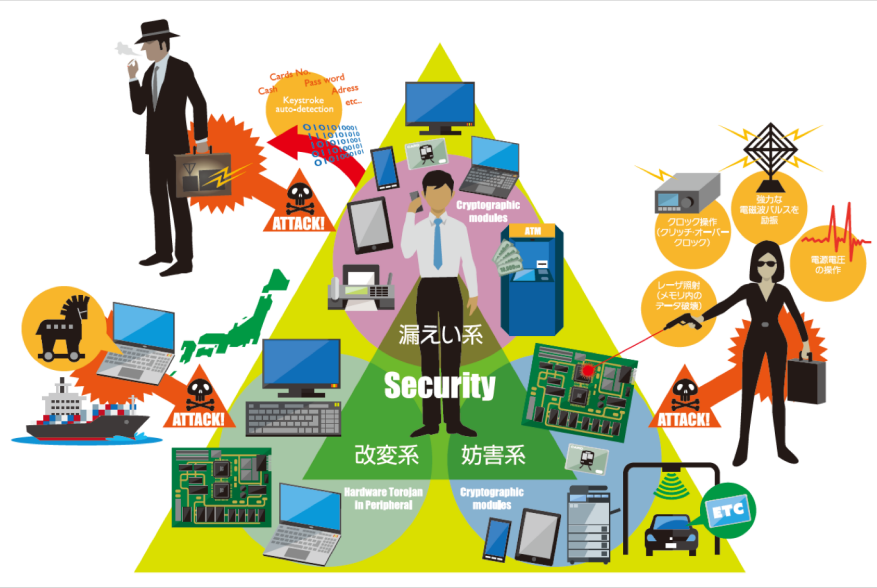
セキュリティvs利便性



ハードウェアセキュリティはすべての信頼の起点（Root of trust/Trust anchor）

- CPS、特にエッジデバイスの安全性向上がメインのターゲット





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

チームミッション：ハードウェアセキュリティについて、以下の取り組みを推進する

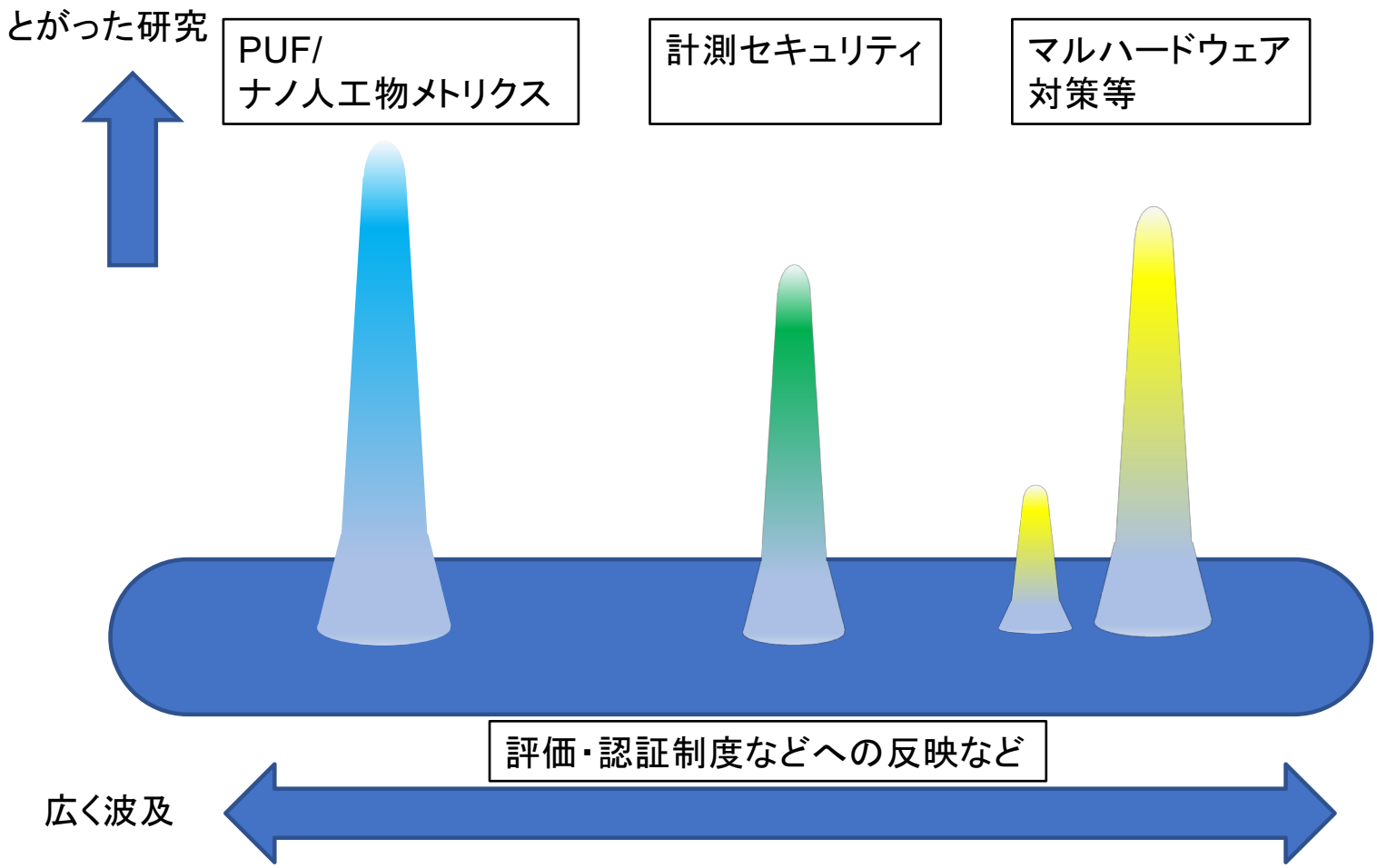
1. 先端課題の解決
   大学・企業との緊密な連携

2. 研究成果の実用化
   関係企業・業界との協調

3. 次世代人材の育成
   所外との人材交流

4. セキュリティ保証スキームへの寄与
   実験施設・開発装置の活用

アプローチ

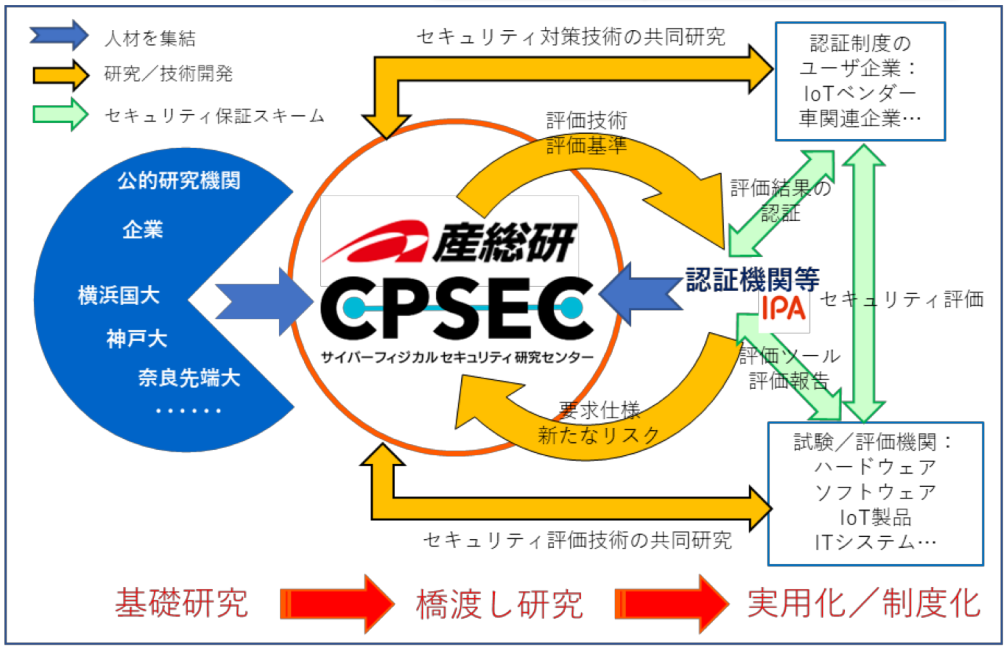

とがった研究
PUF/
ナノ人工物メトリクス
計測セキュリティ
マルハードウェア
対策等
評価・認証制度などへの反映など
広く波及

取り組みの全体像

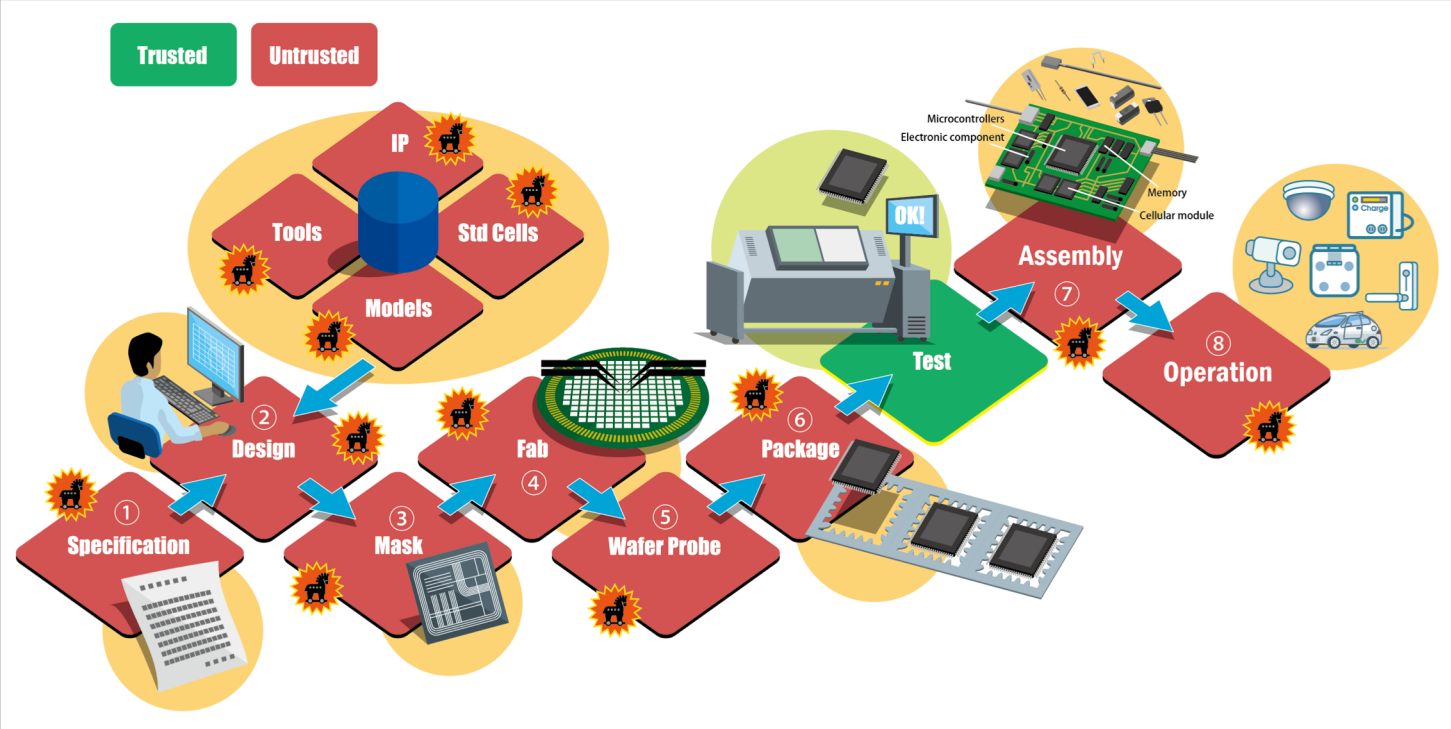
ハードウェアや物理特性の観点からセキュリティの強化と評価 に貢献
得られた研究成果を対策基準、評価・認証制度などへ反映

連携先 評価機関（電子商取引安全技術研究組合, みずほ情報総研など）、認証機関（IPAなど）

攻撃可能性などの検証 → 対策技術/対策基準などの策定 → 評価・認証パイロット実証 → 評価・認証のスキーム化については、セキュリティ保証スキーム研究チームと連携



成果の適用対象例：ハードウェアトロイの場合
IC及び機器の製造過程における意図的な回路改変の脅威分析とその対策



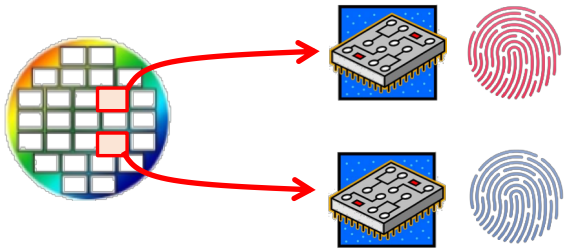
ICを製造する過程・ICを機器に搭載・機器を運用する過程（①から⑧）のそれぞれでハードウェアトロイが仕掛けられる可能性があり、特に⑦、⑧における脅威の分析と対策を行っている

具体的研究課題(As is)

- PUFの標準化および実用化
- ナノ人工物メトリクス
- ハードウェアセキュリティを担うアナログ技術
- 電磁波等を利用した攻撃と対策技術
- 量子アニーリングなど先端コンピューティング

Physically Unclonable Function (PUF)

- **PUF ≒ ICチップの「指紋」**
  - 設計データ上は同じ回路だが、半導体の「**ばらつき**」によって異なる値を出す

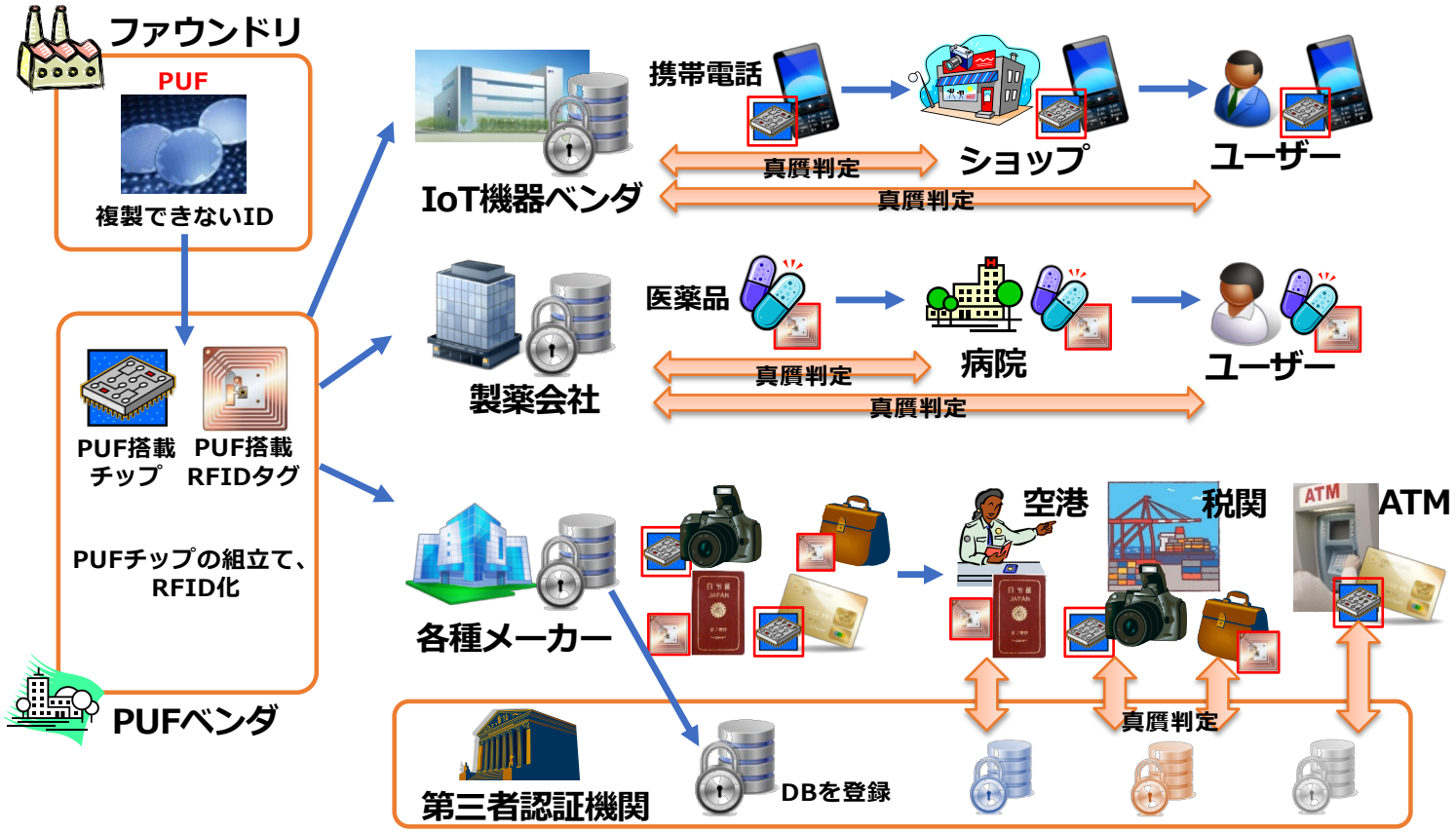


ばらつきは制御できないので、同じ指紋を
出力するPUFを製造することはできない
（複製不可能）

設計図が盗まれて回路が複製されても、「指紋」は複製できない	主体認証や真贋判定が可能	認証・識別
固有の「指紋」から鍵を生成して暗号化、データに署名	機密保護や改ざん検知	鍵生成
停止時はチップ内に秘密情報が存在せず動作する瞬間のみ秘密情報が現れる	高度な物理解析に対しても安全	耐物理解析

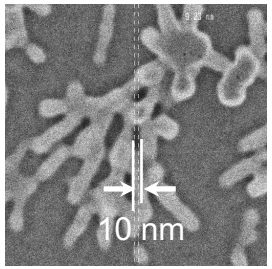
IoT機器のセキュリティを実現する **Trust Anchor（信頼点）** として最適

PUFの利用イメージ

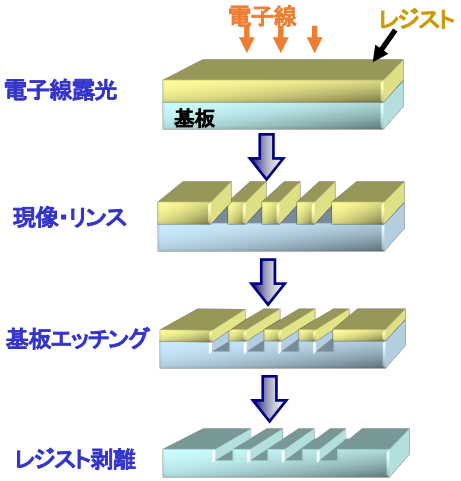

ファウンドリ
PUF
複製できないID
PUF搭載 チップ
PUF搭載 RFIDタグ
PUFチップの組立て、RFID化
PUFベンダ
IoT機器ベンダ
携帯電話
真贋判定
ショップ
ユーザー
真贋判定
製薬会社
医薬品
真贋判定
病院
ユーザー
真贋判定
各種メーカー
空港
税関
ATM
ATM
真贋判定
第三者認証機関
DBを登録

ナノ人工物メトリクス

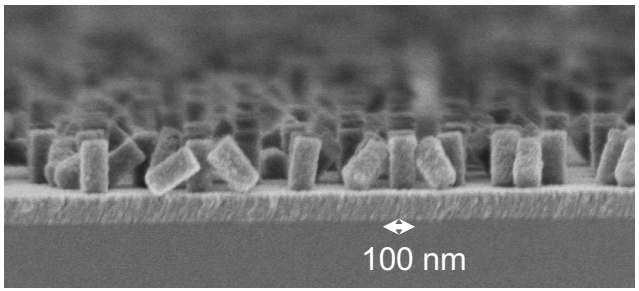
- 個体に固有のナノスケールのランダムな3次元物体形状をIDとして利用する技術。
  - ✓ 究極の耐クローン性（偽造不能性）を有する頑健なID技術
- 電子線リソグラフィ工程におけるレジスト倒壊現象を意図的に利用して、ナノスケールのランダムな表面3次元形状を、シリコン、石英、樹脂フィルム等の表面に形成し、光学的手段あるいはFETを形成することで電気的手段で読み取る。
- AIエッジデバイスの個体管理用として開発中。



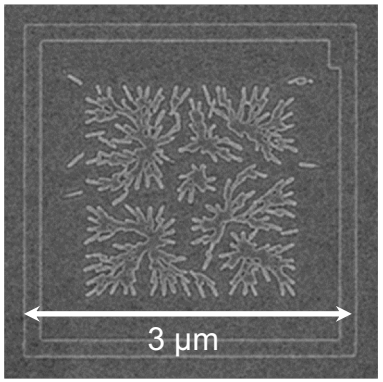
レジスト倒壊を用いたランダムパターン形成の説明



電子線リソグラフィの基本プロセスフロー



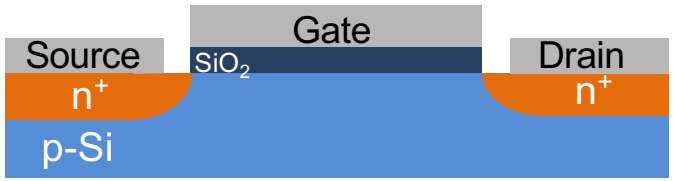
現像・リンス後の倒壊したレジストパターンのSEM画像

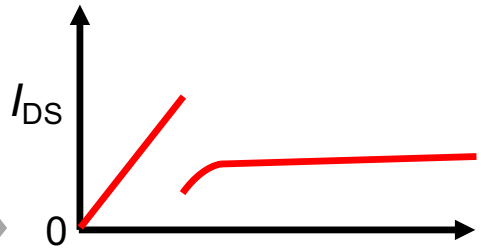


エッチング後のシリコンパターンのSEM画像

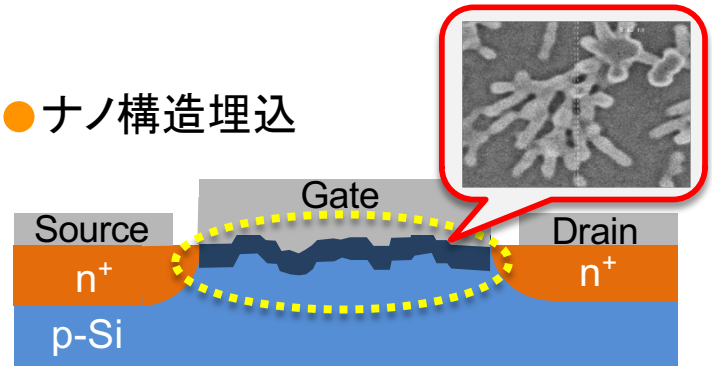
FET形成による電気的読出し方式の開発も着手

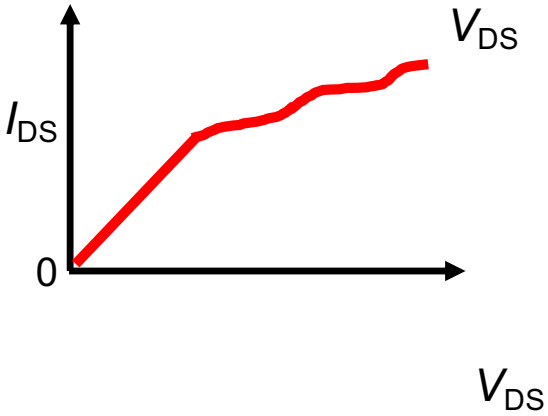
● 通常のMOSFET

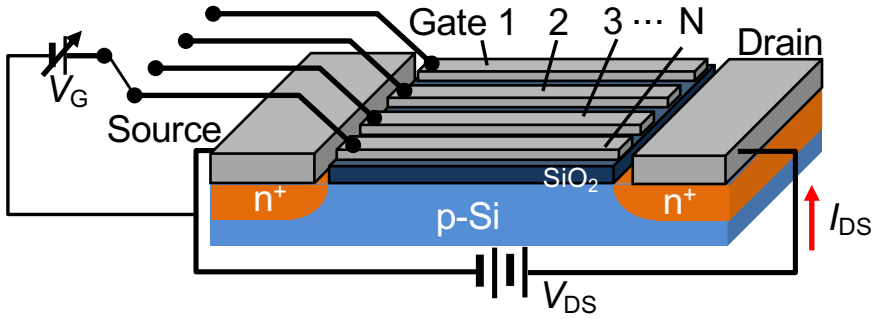




● ナノ構造埋込



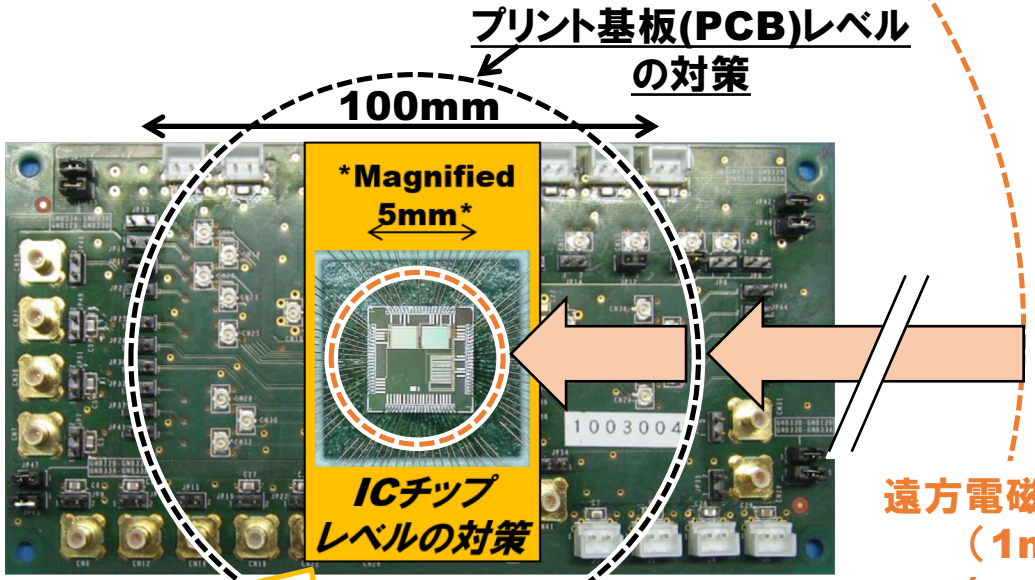




ナノ構造をMOSFETゲート部に埋込み、幾何構造を電子密度分布に反映させ、ドレイン電流を介して読み出す

特願2016-234745、出願日：2017. 12. 2.
特許権者：DNP, 北大, 横浜国大, NICT, 九大
発明者：法元, 有塚, 大八木, 葛西, 松本, 成瀬, 竪

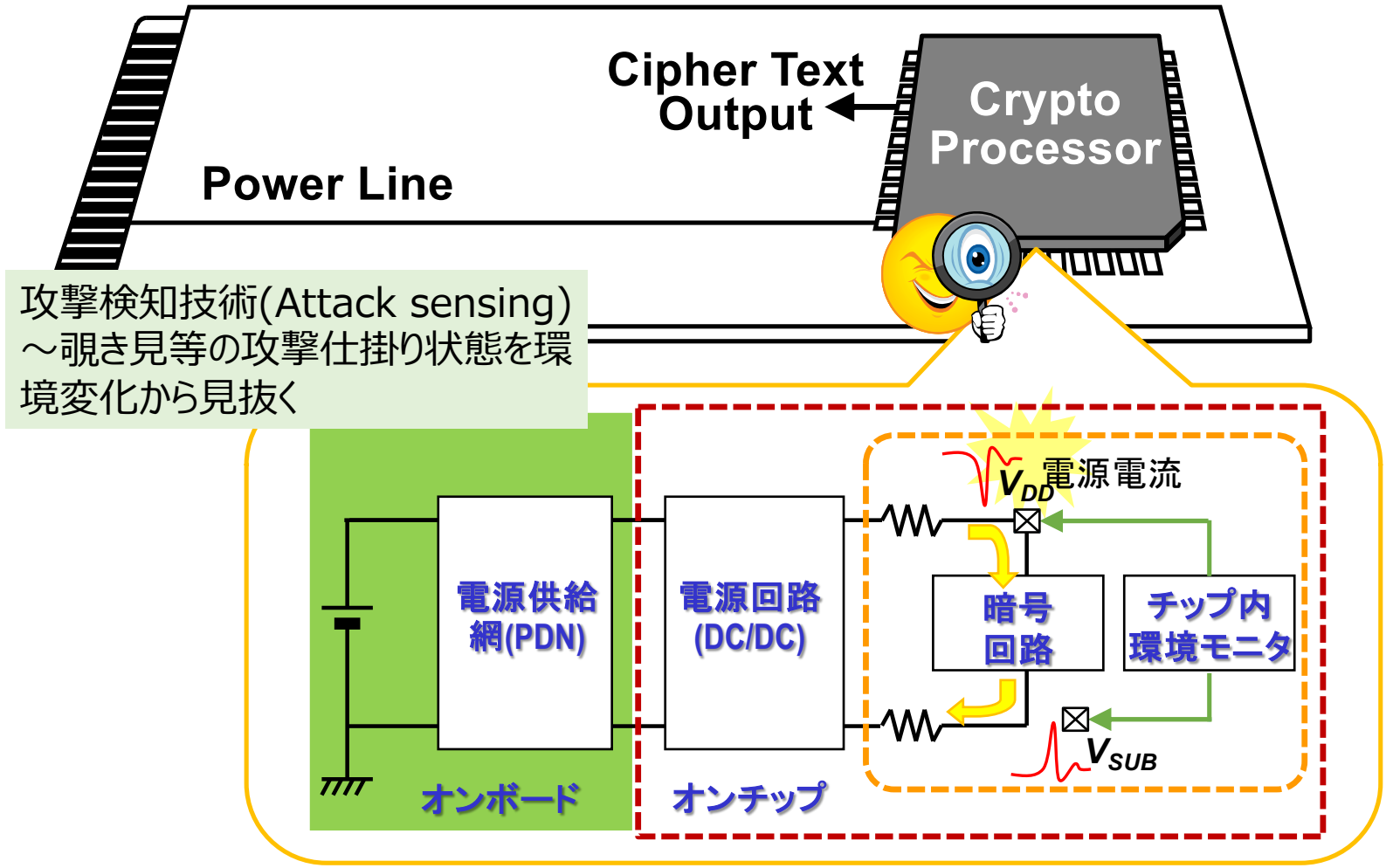
ハードウェアセキュリティを担うアナログ技術



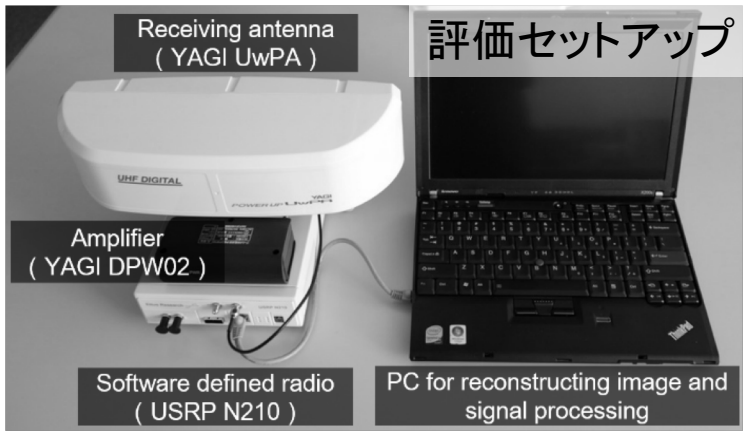
HWSのアナログ・サポート

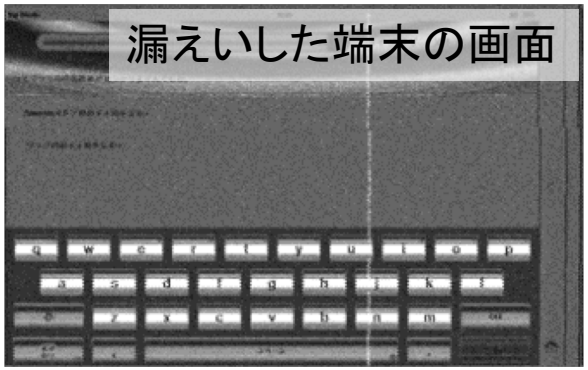
1. セキュリティ機能の物理範囲（回路の素子・信号経路・電源供給）を限定する
2. セキュリティ機能の実行中における「通常でない動作環境の変化」を検知する
3. セキュリティシステムにおけるアナログ機能への脅威を緩和する

怪しい環境変化の検知



タッチスクリーンデバイスから漏えいする電磁波を用いた情報取得の脅威

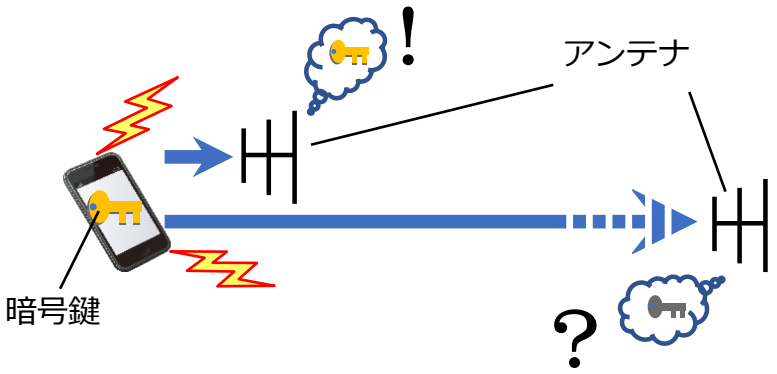




電磁界/電磁波を利用したサイドチャネル攻撃

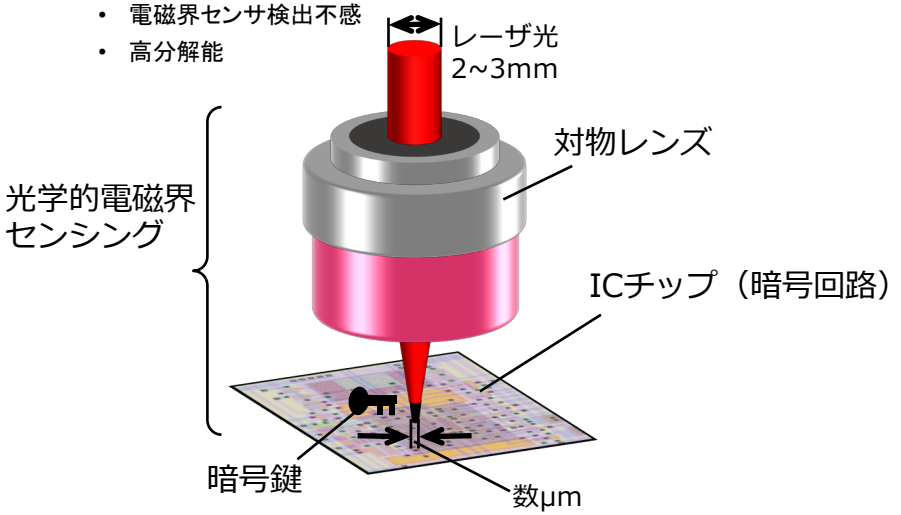
❑ 遠方電磁界（電磁波）

- 電磁波＝電界と磁界が交互に発生し**遠方**へ伝搬
- チップ近傍の電界や磁界が電磁波となって空間に放射される際の効率が著しく低い。
  → サイドチャネル攻撃は困難
  → 検出感度を高めれば可能？
- **ソフトウェア無線技術と信号処理による感度向上**



❑ 近傍電磁界

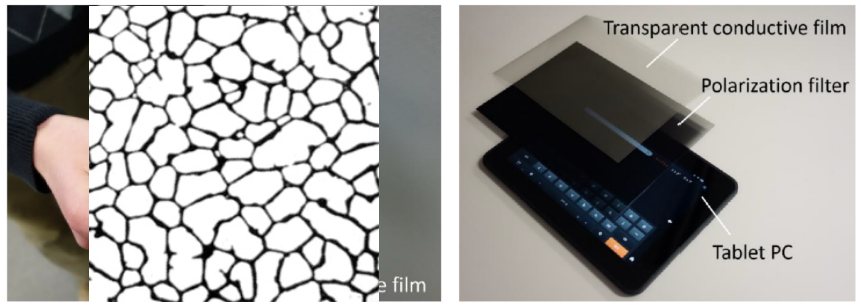
- 電子回路の動作がチップ近傍の電界や磁界に影響を与える（動作情報が漏洩）
  - 距離が離れるに従い急激に減少
  - チップ近傍ではサイドチャネル攻撃可能な強度
- 攻撃対策
  - 電磁界センサの接近検出（→回路動作を停止）
- 攻撃対策の回避策（＝さらなる攻撃技術）
  - **光学的センサの使用**
    - 電磁界センサ検出不感
    - 高分解能



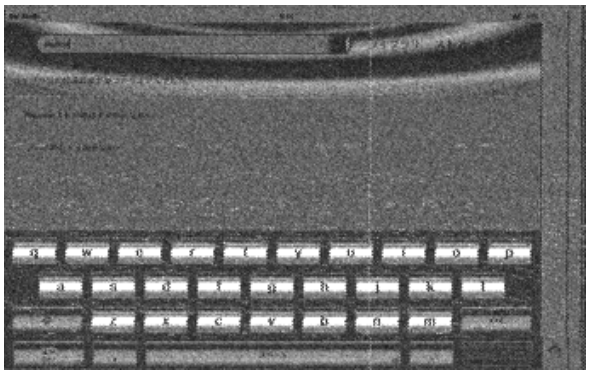
漏えいメカニズムに基づく情報漏えい対策

本検討ではデバイスの製造後に適用可能な電磁波シールドベースの対策を採用

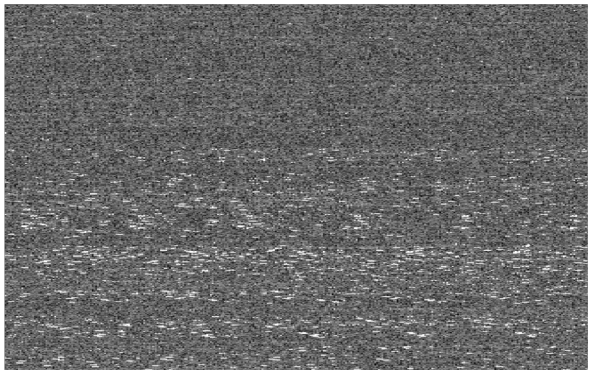
シールドにはランダムなメッシュ構造有する透明導電膜を使用



タッチスクリーンへのデータの入力を可能にするために、一定の厚さの偏光フィルタをモニタとシールドの間に挿入



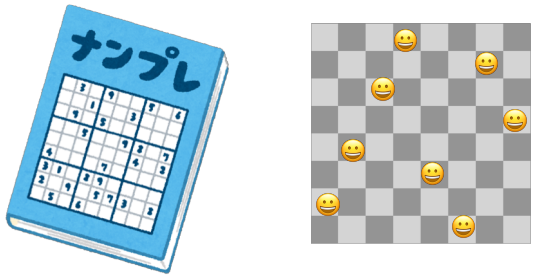
対策前（アンテナ-タブレット:50 cm）

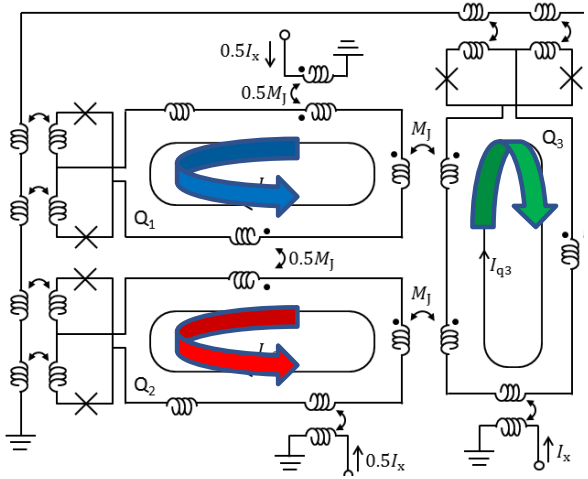


対策後（アンテナ-タブレット:50 cm）

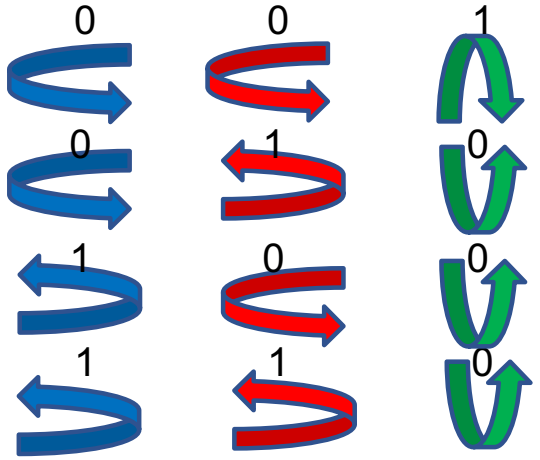
超電導量子アニーリングコンピュータ

- ナノエレクトロニクス研究部門との協業開発
- （アルゴリズム的にではなく）物理法則に基づいた制約充足問題ソルバー
  - 制約充足問題
    - ✓ 数独、クイーン配置問題など
- セキュリティ技術の中の制約充足問題
  - （一方向性）関数の原像を求める問題
  - システム検証用テストベクタの設計など

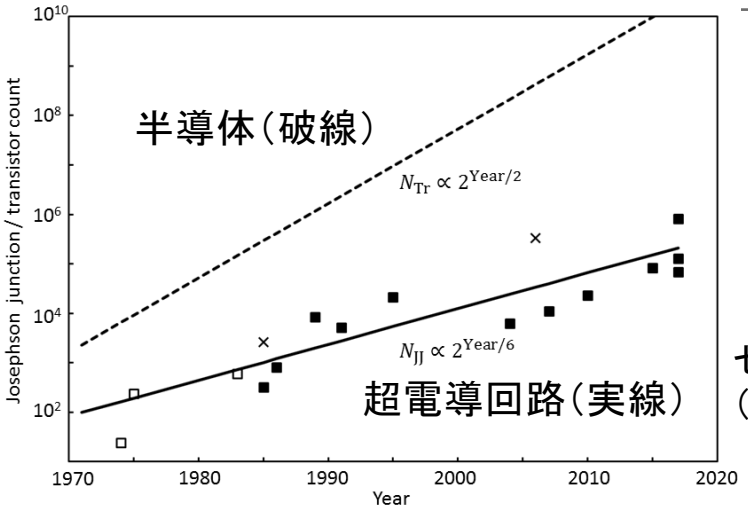




NORと整合的な安定状態だけを持つ超電導回路
arXiv:1809.01425 [quant-ph] より



NORの真理値表と対応する4つの安定状態
（青と赤のNORが緑）



超電導回路版ムーアの法則　arXiv:1809.01425 [quant-ph] より

発展途上の技術だが既にある程度の規模のものは
市販されている（カナダ D-Wave Inc, など）
＋
半導体（破線）に比べて穏やかだが確実な大規模化も
見込まれている

セキュリティ技術に対するインパクトは今後増大
（その他の量子情報技術も含めて）影響は多角的に

関連の深まりが想定されるセキュリティ技術

むすび

- 安全で安心できる社会の実現を目指してハードウェアセキュリティの研究に取り組みます。
- 体制の拡充、研究環境の整備のために、多方面との連携や支援をいただけるよう努めてゆきます。
- 多くの方からのご意見、ご助言を期待しています。

ご清聴ありがとうございました