ハードウェアトロージャン(HT)対策技術

奈良先端科学技術大学院大学(NAIST)
・神戸大学・東北大・横浜国立大学・電子商取引安全技術研究組合

情報システムの信頼の起点となるハードウェアのセキュリティを確保し、社会基盤を支える情報システムの信頼性を飛躍的に高めます

適用領域

半導体・実装 | IoT | ICTベンダー | 製造 | インフラ | 流通

技術の特長

■ ハードウェアトロージャン検知技術

機器の製造過程及び出荷後に機器を構成する基板上に実装される可能性のあるハードウェアトロージャンを検出し、信頼の起点となるハードウェアのセキュリティを確保

■ LSI設計IPのHT形式検証技術

ハードウェアIPコアの論理記述検証とソフトウェアのセキュリティ検証に用いられる形式検証を統合し、ハードウェア・トロージャンフリーなIC設計を保証する技術に関する基礎理論を構築

導入効果・ユースケース・技術内容

■ 導入効果

「サプライチェーン・リスクへ対応するためのオールジャパンの技術検証体制の整備」に求められる”チップの設計回路解析や各種システム・サービスの挙動・動作観測を通じた悪性機能を検出する技術”に対応

■ ユースケース

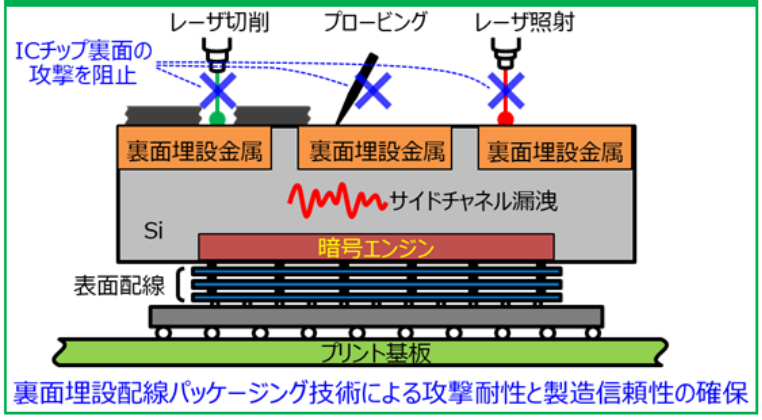
SCU搭載を搭載した機器において本技術を適用することで基板レベルでのハードウェアトロージャン脅威への耐性を獲得可能

■ 技術内容

SCU搭載機器のサイドチャネル攻撃耐性を獲得し、SCU搭載機器の開発・製造・出荷の各過程でハードウェアに組込まれる恐れのある悪意の機能を検出・排除することで、信頼の基点となるハードウェアのセキュリティを確保

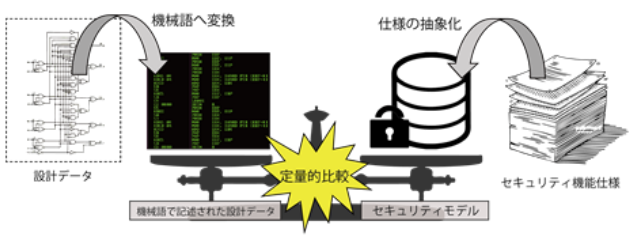
ハードウェアトロージャン(HT)の混入を防ぐ・見つける

セキュアパッケージング技術



裏面埋設配線パッケージング技術による攻撃耐性と製造信頼性の確保

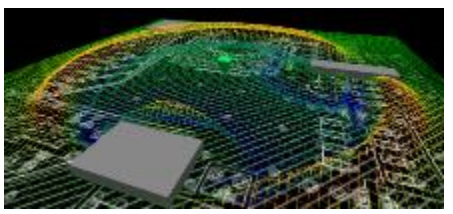
LSI設計IPのHT形式検証技術



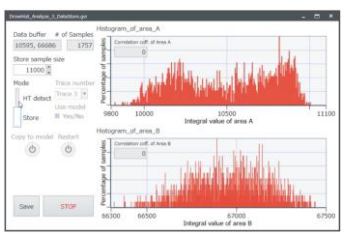
半導体チップ設計の際に第三者から購入する設計IPにHTが混入している場合を想定し、形式検証技術で設計IP内のHTを検知する方法を基礎理論として開発し、実証

ICチップにおけるHT検知技術

HT検知シミュレーション



センサを用いたHT検出



SCUに搭載したアクティブセンサを用いて周囲をセンシングしIC及び周囲の電気的な変化を計測することでHTの実装された位置を検出・動作を抑止

問い合わせ先:　奈良先端科学技術大学院大学　先端科学技術研究科　情報科学領域　yu-ichi@is.naist.jp