② SCU搭載チップ自身のセキュリティ強化 & SCU搭載チップによるシステムのセキュリティ強化

A
創出・証明

SCU：Secure Cryptographic Unit（セキュア暗号ユニット）

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

技術開発の効用のポイント：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する。

技術の特長

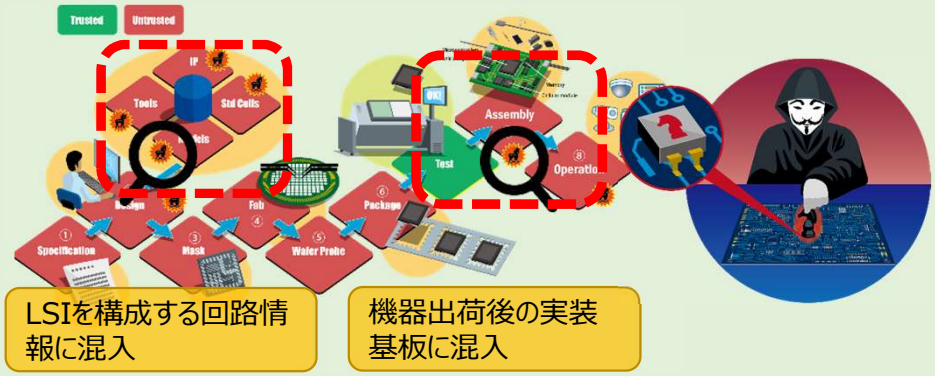
■ ハードウェアトロージャン（HT）検知技術

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

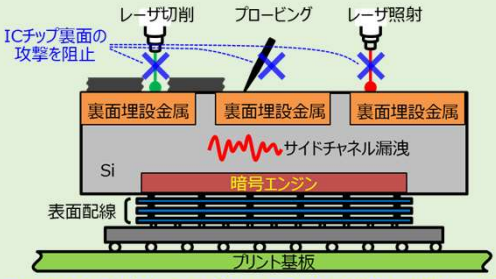
HTの混入を防ぐ・見つける



LSIを構成する回路情報に混入

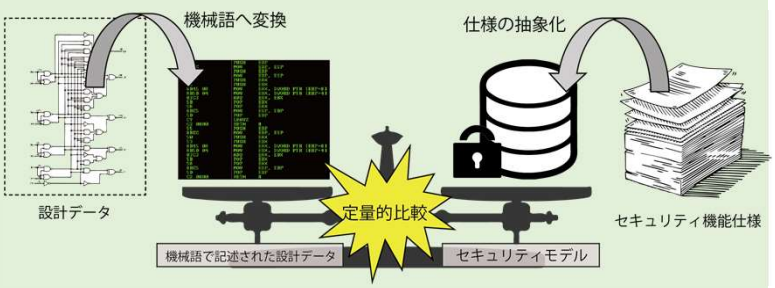
機器出荷後の実装基板に混入

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

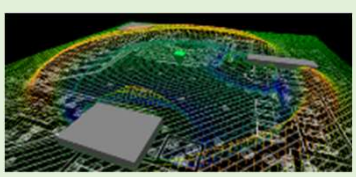
LSI設計IPのHT形式検証技術



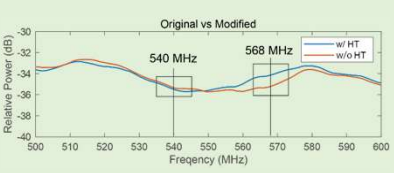
半導体チップ設計の際に第三者から購入する設計IPにHTが混入している場合を想定し、形式検証技術で設計IP内のHTを検知する方法を基礎理論として開発し、実証

ICチップにおけるHT検知技術

時間領域計測による検知



周波数領域計測による検知



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

November 2020