2021 年度

創発的研究支援事業　年次報告書

研究担当者	林 優一
研究機関名	奈良先端科学技術大学院大学
所属部署名	先端科学技術研究科
役職名	教授
研究課題名	物理法則上回避不可能なハードウェアセキュリティ対策手法の開拓
研究実施期間	2021 年 4 月 1 日～2022 年 3 月 31 日

研究成果の概要

物理法則上回避不可能なハードウェアセキュリティ対策手法を開発するために、(1) 漏えい電磁情報によるセキュリティ低下、(2) 電磁的な外乱によるセキュリティ低下、(3) 回路の意図的な改変によるセキュリティ低下に関するそれぞれの課題に取り組み、以下の成果を得た。

（１）情報機器から生ずる電磁波を通じた情報漏えい評価技術の開発

情報機器からの電磁波を通じた情報の漏えいは特定の周波数帯（漏えいチャネル）で発生しており、こうした周波数帯において観測される放射電磁波に対し、信号処理を施すことで情報取得の有無が評価可能となる。本年度は、情報機器から電磁波を通じて情報が漏えいするモデル（漏えいモデル）を構築し、情報端末から放射される周波数を高速にスキャンし、漏えいパターンにマッチする周波数を探索し、漏えいチャネルを特定する手法を開発した。また、開発した評価技術を用いて、情報機器からの電磁波を通じた情報漏えいメカニズムの解明に着手した。

（２）IC 内部への妨害電磁波伝搬計測のための評価環境の構築

故障を容易に検出可能な回路の実装及び故障発生時にチップ内の電気的変動をモニタリングできる環境の構築を行った。故障としては、オーバークロック、IR ドロップ、メモリビットビットフリップなどを想定し、これらの発生を検出するために IC 内部にモニタ回路を配置すると共に、故障時に生ずるサイドチャネル情報も計測可能な評価環境の構築も行った。評価環境では、印可する電磁波として連続正弦波を用い、その振幅、周波数、位相を制御することで故障の誘発を制御可能な評価環境を実現した。

（３）ハードウェアトロージャンによるセキュリティ低下の脅威分類

本年度は、民生品に現実的なコストで実装可能なハードウェアトロージャンについての調査を行った。これまでハードウェアトロージャンは軍事・外交レベルの視点から多くの検討がなされており、本脅威が民生品に及ぶ場合の要件などが十分明らかになっていない。そこで、本年度は、費用、実装対象、実装範囲、実装に要する時間、サプライチェーン内外で実装が行われるタイミングなどの軸から脅威を分類し、商用製品に現実的なコストで実装可能なハードウェアトロージャンについて絞り込みを行った。