2022 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	2022 年 4 月 1 日～2023 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、３つの課題に取り組み、以下の成果を得た。

（１）漏えい電磁情報によるセキュリティ低下に対する対策技術

前年度に開発した情報機器から生ずる電磁波を通じた情報漏えい評価手法の高速化を進めると共に、近傍界評価においては電界・磁界双方に着目した計測を行い高精度な評価を可能とする手法を開発した。さらに、情報漏えい源が複数あり、それらが隣接して存在する場合にも漏えいを評価可能な手法についても開発を行った。開発を行った評価手法を用いて、機器の内外の電磁界伝搬を計測することで、情報漏えいメカニズムの解明を進めた。

（２）電磁的な外乱によるセキュリティ低下に対する対策技術

意図的な電磁妨害による故障発生の有無は注入周波数に大きく依存する。そのため、伝導及び放射雑音をカバーする連続波及びパルス波を IC に印加し、機器への妨害電磁波の注入効率を決定するパラメタを抽出した。また、IC 内部において引き起こされる故障は、時間変化する機器内部の処理に依存して変化することから、周波数領域に加え、時間領域における妨害波の伝搬についても計測を行うと共に、意図的な電磁妨害より生ずる IC 内部の評価回路からの故障を示すデータ出力を解析することで、故障の発生しやすい妨害波の印加タイミングを明らかにした。

（３）意図的な改変によるセキュリティ低下に対する対策技術

具体的な脅威を評価可能なプラットフォームを構築し、その上に脅威対象となるハードウェアトロージャン（HT）を実装し、動作時の電気特性計測を実施することで、回路や基板の電気的な特性を変更することなく HT を実装することは困難であることを確認した。さらに、基板上の電気特性を持続的にモニタリングことにより、HT 実装を検知する技術を開発すると共に、シミュレーションを用いたゴールデンモデルの構築にも着手した。