

2023 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	2023 年 4 月 1 日～2024 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**

前年度までに開発した評価方法を用いてメカニズムの解明を進めた。その結果、機器から漏えい情報を含む電磁波は機器内部の幾何構造の非対称性に依存し生ずる寄生結合、ダイポールやモノポールなど同一の幾何構造を有する基板上の金属部位、及び基板上で閉ループを構成する金属部位が電界及び磁界を放射するアンテナとして振る舞うことで生ずることを明らかにした。さらに、これらの要素を考慮した漏えいを事前予測可能なシミュレーションモデルの開発に着手した。

**(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**

意図的電磁妨害による故障発生を引き起こしやすい周波数は、電磁波の相反性から、その伝搬方向を逆向きに捉えることで(1)で明らかにしたメカニズムにより決定されることを明らかにした。また、妨害波印加時に IC で生ずる故障は、組み合わせ回路及び順序回路の双方で発生することも確認した。さらに、シミュレーションモデルに関しても電磁気学の相反性から(1)で開発するシミュレーションモデルを利用可能であることを確認した。

**(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**

前年度で明らかになった HT を実装する際に避けることができない電気的な特性(主に寄生容量)に着目し、この電気特性の変化をモニタリングするために、近年多くの IC に標準的に搭載されている静電容量センサを用いた HT 検出システムの開発を進めた。また、実測をベースにゴールデンモデルを生成することは困難であるため、センシング対象となる機器を等価回路モデルで表現し、その電気応答からゴールデンモデルを抽出し、得られたモデルをリファレンスデータとして HT を検出する試みを開始した。