

放射電磁波と電磁妨害の双方を考慮した情報セキュリティの研究

氏 名 鍛冶 秀伍

研究室名 情報セキュリティ工学研究室

主指導教員名（論文博士の場合は推薦教員名） 林 優一

内容梗概（1ページ目に収めること）

社会インフラの1つとして情報通信システムは欠かせない存在であり、信頼の基点となるハードウェアに対するセキュリティの確保が課題となっている。特に、情報が機器内部で処理・伝送される際に放射する電磁波の受動的な計測による情報漏えい（電磁情報漏えい）は、攻撃の痕跡が残らないことから深刻な脅威の1つとなっている。電磁情報漏えいにおいて機器から放射される電磁波の強度は、情報を表す電気信号（ソース）の強度とソースを機器外部に放射するアンテナ構造（アンテナ）、そして、ソースとアンテナを接続する電磁的な結合の経路（パス）の周波数特性により決定される。そのため、ソースの信号強度が弱い機器や、各要素の周波数特性による損失が大きい機器は放射される電磁波の強度が弱く脅威の対象外と見なされてきた。

これに対し、本研究では、特定の周波数・強度の電磁波の照射により、電磁波を通じて機器から強制的に情報漏えいが生ずる新たな脅威を示すと共に、故意に照射された電磁波により引き起こされる情報漏えいのメカニズム解明と、メカニズムに基づく脅威に対する耐性の獲得方法に関する知見を与えた。具体的には、ソースは能動素子やそれらを組み合わせた回路の情報に応じた状態変化により生成されることに着目し、（1）ソースの生成回路となるIC内部の出力バッファの入力インピーダンスの変化を照射した電磁波の反射より推定し、従来の電磁情報漏えいの脅威対象外であった機器から強制的な情報漏えいが引き起こされることを示した。また、（2）機器に照射された電磁波の強度に応じて情報漏えいが引き起こされる距離が制御可能であることを示した。（1）、（2）により生ずる情報漏えいは、照射した電磁波の周波数に対するソースの生成回路の応答と伝達特性で決定される。（1）、（2）の脅威では照射電磁波の反射に着目したが、透過に着目すると、機器内部への情報注入の脅威に拡張される可能性がある。そのため、（3）機器の等価回路の一部の意図的な改変により機器内部に電磁波が透過しやすい状況を構築し、機器外部から照射した電磁波による任意の情報が注入可能であることを示した。そして、（4）照射電磁波の反射・透過によるセキュリティ低下メカニズムを解明し、そのメカニズムに基づく対策技術を提案した。