

論文内容の要旨

博士論文題目

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

Electromagnetic Information Security Focusing on the Physical Phenomenon of both Emission and Interference

氏名 鍛治 秀伍

(論文内容の要旨)

情報通信システムは欠かせない社会インフラの一つであり、その信頼の基点となるハードウェアのセキュリティ確保が課題となっている。中でも電磁波を介したセキュリティ（電磁波セキュリティ）の脅威は、攻撃の痕跡が残らないことから深刻な問題となっている。電磁波セキュリティの脅威は、電磁波を介した情報漏えい（電磁情報漏えい）と意図的に発生させた電磁波による機器の動作妨害（意図的な電磁妨害）に分類され、その脅威の対象となるか否かは、機器からの不要放射の強度（エミッション）と電磁妨害波に対する耐性（イミュニティ）により決定される。これまで、機器のエミッションやイミュニティに基づいた電磁波セキュリティの脅威や対策技術が検討されてきたが、機器のエミッションやイミュニティが攻撃者によって制御可能な場合、これまで脅威の対象外とされていた機器にも脅威が拡大し、従来の対策技術が無効化される恐れがある。

上述の背景に基づき、本研究では、機器のエミッションとイミュニティの制御により引き起こされる電磁波セキュリティの脅威を示すと共に、セキュリティ低下のメカニズムに基づいた対策技術について示した。具体的には、従来の脅威の対象外とされてきた機器に電磁波を照射し、その反射波から機器内部で電気信号として表現される情報信号が取得可能であることを示した。また、電磁波の照射強度に応じてエミッションが制御され、電磁情報漏えいが引き起こされる範囲を制御可能であることを示した。続いて、機器の等価回路網の一部を意図的に改変することによりイミュニティが制御され、機器内部に任意の電気信号を誘導し、機器の動作を改変可能であることを示した。さらに、エミッションとイミュニティの制御によりセキュリティが低下するメカニズムを明らかにし、そのメカニズムに基づいた脅威の検知・対策技術を提案した。

以上の結果より、本研究は環境電磁工学の知見を情報セキュリティに応用し、潜在的に電磁波セキュリティの脅威に耐性を有していた機器に対しても脅威が及ぶ可能性について検討を行うと共に、新たな脅威に対しても、電気信号として表現される情報信号の取得と誘導の困難化に着目することでそれらを抑止できることを示した。

(論文審査結果の要旨)

本論文では、環境電磁工学の視点から電磁波セキュリティを、エミッションとイミュニティに関わる脅威として再定義すると共に、エミッション及びイミュニティが攻撃者により制御可能という新たな脅威シナリオを導入することで、電磁波セキュリティの対象外とされてきた機器にも脅威が及ぶことを示し、電気信号として表現される情報信号の取得と誘導の困難化の視点に基づき、新たな脅威への対策技術を提案した。

本論文の主な成果は以下に要約される。

1. 機器外部からの電磁波の照射により生じた反射波から機器内部の電気信号として表現される情報信号が取得可能であることを示すと共に、電磁波の照射強度に応じて機器のエミッションが制御され、電磁情報漏えいが生ずる範囲を制御可能であることを示した。
2. 等価回路網を意図的に改変することで機器のイミュニティが変化し、任意の電気信号を機器内部に誘導でき、機器の動作を改変可能であることを示した。
3. 機器のエミッションとイミュニティの制御により拡大した電磁波セキュリティの脅威に対し、提案手法のメカニズムに基づいた対策技術を提案した。

以上のように、本論文は環境電磁工学と情報セキュリティの知見を融合させ、電磁波セキュリティの新たな脅威の発見と、脅威によるセキュリティ低下のメカニズムに基づく対策手法を提案しており、環境電磁工学及び情報セキュリティ双方の分野に与える学術的インパクトは少なくない。よって本論文は、博士(工学)の学位論文としての価値があるものと認める。