様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 ２２ 日現在

機関番号：１４６０３
研究種目：挑戦的研究（萌芽）
研究期間：2021～2022
課題番号：２１Ｋ１９７７２

研究課題名（和文）機器への故意な電磁波照射による情報漏えいへの耐性獲得

研究課題名（英文）Acquiring Resistance against Threats of Information Leakage due to Intentional Electromagnetic Irradiation Exposure to Electronic Devices

研究代表者
林　優一（Hayashi, Yuichi）

奈良先端科学技術大学院大学・先端科学技術研究科・教授

研究者番号：６０５５１９１８

交付決定額（研究期間全体）：（直接経費）　　5,000,000円

研究成果の概要（和文）：本研究では、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を高精度かつ短時間に計測可能な評価システムを開発し、脅威の対象となるデバイスの判定を可能とした。さらに、漏えい源・伝搬経路・電磁波を受信/送信するアンテナ要素を特定し、情報漏えいのメカニズムの解明を行うと共に、情報漏えいに関わる物理構造を明らかにした。また、これらの知見に基づき、漏えいモデルを構築し、機器の設計段階で漏えいの事前予測を可能とした。さらに、機器周囲の電磁環境を変化させることで、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脅威に対し、耐性を獲得可能であることを示した。

研究成果の学術的意義や社会的意義
研究代表者らが新たに発見した脅威は、「ICを搭載する機器に特定の振幅、周波数の電磁波を故意に照射することでICの入出力情報を強制的に漏えいさせる新たな脆弱性」であり、多くの情報機器のセキュリティがハードウェアレベルで低下する恐れがある。こうした脅威に対し、本研究では、潜在的に耐性を有するデバイスの特徴を明らかにし、その知見を元に対策技術の基礎を導いた。こうした成果は多くの情報機器のセキュリティを確保するものであり、社会に与えるインパクトは少なくない。また、本研究の遂行において環境電磁工学及び情報セキュリティの融合領域を新たに開拓しており、この点において学術的意義が認められると考えられる。

研究成果の概要（英文）：This study developed a fast, accurate method to measure information leakage from intentionally emitted electromagnetic waves, identifying threat-targeted devices. By tracking and visualizing high-resolution time series of leaked waves, we determined leakage sources, propagation paths, and participating antenna elements, thus elucidating leakage mechanisms and involved physical structures. This knowledge informed a leakage model for advanced leakage prediction during design stages. Moreover, altering the equipment's electromagnetic environment via EMC countermeasures and environment control demonstrated the feasibility of resisting information leak threats by intentional electromagnetic interference.

研究分野：ハードウェアセキュリティ

キーワード：ハードウェアセキュリティ　電磁的情報漏えい　意図的電磁妨害　サイドチャネル攻撃

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

情報機器の内部で処理を実行する際、電流や電圧などの電磁信号の時間変化が必ず発生し、その時間変化に伴い生ずる電磁波が機器から放射される。こうした放射電磁波には機器内部の処理情報が含まれ機密情報が漏えいする可能性がある。特に人間を対象とした情報機器からの入出力信号に関しては、暗号化処理などが施されていないため、攻撃者がそれらを取得することで即座に機密情報を把握される危険性がある。

上述の脅威から情報機器のセキュリティを確保するため、機器評価法や対策法が議論され、規格化などがこれまで進められている。一方、電磁波を通じた情報漏えいの脅威は全ての情報機器が対象となるわけではなく、機器から放射される電磁波が弱く、潜在的に脅威に対する耐性を獲得している機器もあり、こうした機器は脅威の対象外とされてきた。

２．研究の目的

研究代表者らは基礎実験により、特定の周波数・強度の電磁波を情報機器に対して故意に照射することにより、電磁波を通じて機器から強制的に情報漏えいが生ずる現象を発見した。研究代表者らが明らかにした新たな脅威は、入出力情報を処理する多くの機器が電磁波を通じた情報漏えいの脅威の対象になることを示唆している。そこで、本研究では、情報機器のセキュリティを確保するために、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の基礎を開拓する。

３．研究の方法

本研究では、まず、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を高精度に短時間で計測可能な評価システムを開発し、脅威の対象となるデバイスを判定する。さらに、高時間分解能で情報を含む漏えい電磁波を計測し、時系列で可視化することで、漏えい源・伝搬経路・電磁波を受信/送信するアンテナ要素を特定し、情報漏えいのメカニズム解明を行う。

続いて、得られたメカニズムに基づき、情報機器の設計情報から漏えいに関わる物理構造及び信号パターンなどを抽出し、脅威に対する耐性を事前予測可能な情報漏えいモデルを構築する。さらに、メカニズムを基に、情報漏えいを抑止するための機器設計の基礎を与え、脅威への耐性獲得を目指す。

４．研究成果

まず、電磁波を用いた能動的なセンシングにより生ずる信号を介した情報漏えいの脅威について複数の実デバイスを用いて検討し、(1)電磁波を用いて情報が処理される過程の電気的な特徴量の変化を能動的にセンシングすることにより、機器内部の情報を取得可能であることを示すと共に、(2)能動的なセンシングに用いる電磁波の照射強度に応じて、情報を取得可能な範囲が制御可能であることを示した。さらに、(3)漏えい電磁波の放射強度が弱いため従来の電磁情報漏えい手法の脅威対象外となっていた機器に対する能動的なセンシングにより、情報が取得可能であることを示し、脅威の一般性を導いた。

これらの成果に基づき、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を高精度に短時間で計測可能な評価システムを開発し、脅威の対象となるデバイスの判定を可能とした。特に、高精度計測部分に関しては、電磁波印加時に生じた自己干渉による漏えい信号の劣化を抑制し、漏えい信号の取得を可能とした。

また、高時間分解能で情報を含む漏えい電磁波を計測し、時間及び周波数領域で可視化するこ

とで、情報漏えいのメカニズム解明を行うと共に、情報漏えいに関わる物理構造を明らかにした。具体的には、能動的なセンシングによる機器から生ずる反射波は、機器外部から照射された電磁波を受信する機器の非意図的なアンテナと機器内部に伝搬した信号を反射・吸収する回路構造により生ずることを明らかにした。機器外部で照射された電磁波は、機器に接続されたケーブル等のアンテナ構造より機器内部に伝搬し、「情報漏えいのターゲットとなる情報を処理する回路（ターゲット回路）」まで到達する。続いて、ターゲット回路まで伝搬した電磁波は、処理する情報に依存して時間的に変化するターゲット回路の入力インピーダンスの値に応じて、その一部は回路内に伝搬し、一部が反射する。そして、反射した電磁波は、入射した時と逆向きの経路を辿り、機器外部に反射波として再放射される。このとき反射波は、ターゲット回路の入力インピーダンスの時間変化に伴いその振幅が変化する。そのため、こうして得られた反射波は、照射した電磁波を搬送波とし、ターゲット回路の出力信号を被変調波とする振幅変調波として捉えることができる。以上より、ターゲット回路の出力信号の状態は反射波を介して取得でき、これに基づき入出力情報の推定が可能となる。さらに、再放射される電磁波の強度は能動的なセンシングに使用する電磁波の照射強度に依存する。そのため、I/O 回路の出力バッファを構成する回路が動作可能な範囲で照射強度を増強することにより、反射波の放射強度を制御することが可能となることも明らかにした。

これらの知見に基づき、漏えいモデルを構築し、機器の設計段階で漏えいの事前予測を可能とした。さらに、EMC 対策技術や、機器が設置される環境をコントロールすることにより、機器周囲の電磁環境を変化させることで、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脅威に対し、耐性を獲得可能であることを示した。また、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にはターゲット回路まで電磁波を伝搬させる必要があり、攻撃者は機器周辺の背景雑音以上の強度で電磁波を照射し、機器で生成された反射波を計測する。そのため、照射された電磁波の検知による対策、ターゲット回路に伝搬する電磁波を減衰させる対策、機器で生成された反射波の放射強度を減衰させる対策が有効であることも示した。

さらに、照射電磁波の検知に着目し、照射された電磁波により変動する IC 内部の電源電圧の計測やリファレンス CLK と IC 内部の CLK との位相・周波数の同期ずれの検出、伝送信号への干渉により生じるビットエラーレートの解析などを用いた検知手法も対策として有効であることを示した。これらの技術を用いることで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前段である電磁波照射を検知し、処理中の情報の伝送を中断することで攻撃者による反射波の取得を困難化できる可能性を示唆した。

また、ターゲット回路までの電磁波伝搬や機器から放射される反射波の計測に着目すると、機器のイミュニティの向上や放射電磁波の抑制が対策となる可能性があり、こうした対策をターゲットとなる機器に適用することで、機器から放射される反射波の振幅を背景雑音レベル以下に抑制し、攻撃者による情報の復元が困難となる可能性を示した。また、従来の電磁情報漏えい対策技術として検討されてきた筐体や建物、接続線路へのシールディング、ゾーニング、ノイズを用いたジャミングなども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対策として適用できる可能性を示した。

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　3件）

１．著者名 Kitazawa Taiki、Kitamura Yoshiki、Kim Yougwoo、Fujimoto Daisuke、Sone Hideaki、Hayashi Yuichi	４．巻 2022
２．論文標題 TEMPEST attack against high-resolution displays using differences in the transfer function of EM waves	５．発行年 2022年
３．雑誌名 2022 3rd URSI Atlantic and Asia Pacific Radio Science Meeting	６．最初と最後の頁 1-4
掲載論文のDOI（デジタルオブジェクト識別子） 10.23919/AT-AP-RASC54737.2022.9814293	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Fujimoto Daisuke、Okamoto Takumi、Li Yang、Kim Youngwoo、Hayashi Yuichi	４．巻 65
２．論文標題 Evaluation of Statistical Fault Analysis Using Input Timing Violation of Sequential Circuit on Cryptographic Module Under IEMI	５．発行年 2023年
３．雑誌名 IEEE Transactions on Electromagnetic Compatibility	６．最初と最後の頁 51～57
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2022.3215583	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Kaji Shugo、Fujimoto Daisuke、Kinugawa Masahiro、Hayashi Yuichi	４．巻 2023
２．論文標題 Echo TEMPEST: EM Information Leakage Induced by IEMI for Electronic Devices	５．発行年 2023年
３．雑誌名 IEEE Transactions on Electromagnetic Compatibility	６．最初と最後の頁 1～12
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2023.3252636	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Nishiyama Hikaru、Fujimoto Daisuke、Sone Hideaki、Hayashi Yuichi	４．巻 2023
２．論文標題 Efficient Noninvasive Fault Injection Method Utilizing Intentional Electromagnetic Interference	５．発行年 2023年
３．雑誌名 IEEE Transactions on Electromagnetic Compatibility	６．最初と最後の頁 1～9
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2023.3264586	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計6件（うち招待講演　2件／うち国際学会　1件）

１．発表者名
高野誠也，鍛治秀伍，衣川昌宏，藤本大介，林優一

２．発表標題
意図的な電磁妨害により生ずる情報漏えいのモデル化に向けた評価環境の構築

３．学会等名
電子情報通信学会 環境電磁工学研究会

４．発表年
2022年

１．発表者名
尾崎慧一，藤本大介，大須賀彩希，川村信一，林優一

２．発表標題
ROベースのTRNGに対する振幅確率分布を用いた乱数性評価手法

３．学会等名
2023年 暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
西山輝，藤本大介，林優一

２．発表標題
漏えいと妨害電磁波を用いた暗号モジュールに対する統計故障解析

３．学会等名
2023年 暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
林優一

２．発表標題
スマートシステムにおけるハードウェアセキュリティ

３．学会等名
第28回 EMC環境フォーラム（招待講演）

４．発表年
2022年

１．発表者名 Yuichi Hayashi
２．発表標題 Recent Trends and Future Prospects in Electromagnetic Information Security
３．学会等名 EMSEC Workshop 2022（招待講演）（国際学会）
４．発表年 2022年

１．発表者名 鍛治秀伍，藤本大介，林優一
２．発表標題 位相限定相関法を用いた意図的な電磁情報漏えい耐性評価法
３．学会等名 電子情報通信学会総合大会
４．発表年 2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	Ｋｉｍ　ＹｏｕｎｇＷｏｏ (Kim YoungWoo) (30862403)	奈良先端科学技術大学院大学・先端科学技術研究科・助教 (14603)	
研究分担者	藤本　大介 (Fujimoto Daisuke) (60732336)	奈良先端科学技術大学院大学・先端科学技術研究科・助教 (14603)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
韓国	YONSEI University			