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 ２３ 日現在

機関番号：１４６０３
研究種目：基盤研究(A)（一般）
研究期間：2019～2022
課題番号：１９Ｈ０１１０４

研究課題名（和文）情報漏えいを引き起こす電磁波の計測困難化を実現する機器設計手法の開拓

研究課題名（英文）Advancing Device Design Techniques to Obfuscate the Measurement of Electromagnetic Information Leakage

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）　　34,500,000円

研究成果の概要（和文）：本研究では、情報漏えいを引き起こす電磁波の計測困難化を実現するための評価技術・メカニズム解明・対策技術の開発に取り組んだ。まず、(1) 漏えいモデルに基づき、完全な情報の復元を必要としない高速な漏えい評価技術を開発し、その評価技術を用いて、(2) デバイスからの漏えい電磁界の伝搬を時間領域において高分解能で可視化することにより、漏えいメカニズムを解明した。次にメカニズムに基づき、(3) 機器設計時に情報漏えいを予測可能なシミュレーションモデルを構築した。さらに、(4) メカニズムに基づき、上位レイヤで処理される情報に依存しない漏えい情報計測を困難化する対策手法を開発した。

研究成果の学術的意義や社会的意義
本研究では、漏えい電磁波による情報漏えいの脅威を「漏えい電磁情報の計測」と「計測された情報の解析」の2つのフェーズからなる攻撃と捉え、前段の「計測」に着目し、これを困難化することで、後段の「解析」も無効化する新たなアプローチを用いた対策手法の開拓に学術的意義な意義がある。開発した対策手法は上位レイヤのプロトコルやアプリケーションに依存しないため、機器設計時に多種多様な入出力機器に統一的に適用できることから、その社会的意義は少なくない。

研究成果の概要（英文）：This research developed evaluation techniques, mechanism clarification, and countermeasure techniques to make measuring electromagnetic waves that cause information leakage difficult. First, (1) we developed a rapid leakage evaluation technique that does not require complete information restoration based on a leakage model, and (2) we clarified the leakage mechanism by high-resolution visualization of the propagation of leaking electromagnetic fields from devices in the time domain. Following this mechanism-based approach, (3) a simulation model was constructed to predict information leakage during equipment design. Furthermore, (4) a design methodology was given that makes the measurement of leakage information independent of the information processed at upper layers more difficult, again based on the identified mechanism.

研究分野：ハードウェアセキュリティ

キーワード：電磁情報セキュリティ　サイドチャネル攻撃　環境電磁工学　暗号・認証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

電磁波を通じた情報漏えいの脅威に対する評価・対策技術の従来検討では、攻撃対象となる機器は主に据え置き型であり、機器から放射される漏えい電磁波強度も一定で、攻撃者は専門的な知識を有する攻撃者が据え置き型の計測器を屋内や車内に設置した上で、十分な時間をかけて攻撃を実行するという前提の下で議論が行われており、機器から漏えいする電磁波が攻撃者の計測装置に到達する前に信号レベルを背景雑音以下に減衰させるゾーニングという概念の下に対策がとられてきた。

これに対し、近年ではプロファイリングと信号処理を用いることにより、ポータブルなセットアップを用いて専門的な知識を有していない攻撃者が移動しながらリアルタイムに漏えい電磁波を通じて情報を取得出来る可能性が示されており、こうした新たな脅威は、これまでの前提条件を覆すものであり、ゾーニングに基づいた既存の対策手法を直ちに適用することは難しい。そのため、新たなシナリオの下で攻撃が実行された場合、これまでの攻撃シナリオにおいては脅威の対象外であった機器も脅威の対象となる可能性があり、セキュリティを確保するためには、従来とは異なる評価法・対策法が求められる。

２．研究の目的

本研究は、情報漏えいを引き起こす電磁波の計測困難化を実現するための評価技術・メカニズム解明・対策技術の開発を目指す。まず、(1) 漏えいモデルに基づき、高速かつ完全な情報の復元を必要としない漏えい評価技術を開発し、その評価技術を用いて、(2) デバイスからの漏えい電磁界の伝搬を時間領域において高分解能で可視化することにより、漏えいメカニズムを解明する。次にメカニズムに基づき、(3) 漏えいに深く関わる設計パターンを特定し、設計情報からそれらの構造を抽出し、機器設計時に情報漏えいを予測可能なシミュレーションモデルを構築する。さらに、(4) メカニズムに基づき、漏えいを抑止する配線パターンや電気素子などを効果的に組み合わせ、逐次シミュレーション上で評価しながら、上位レイヤで処理される情報に依存しない漏えい情報計測を困難化する機器設計手法を開発する。

３．研究の方法

本研究では、上述の研究目的を達成するために、(1) 情報機器から電磁波を通じた漏えいを高精度に短時間で評価する技術の開発を行う。さらに、(2) 機器から漏えいする電磁波を高時間分解能で計測し、それらを時系列で可視化することで漏えい源・伝搬経路・アンテナ要素を特定し、漏えいメカニズムの解明を行う。(3) 漏えい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、漏えいを事前予測可能なシミュレーションモデルを構築する。続いて、(4) メカニズムに基づき、漏えいの抑制及び攻撃を検知する対策技術を開発し、漏えい電磁波計測を困難化する機器設計手法を確立する。

４．研究成果

情報機器からの電磁波を通じた情報漏えいを評価する手法として、電磁波を通じた情報漏えいモデルを機器内部で繰り返し実行される処理に着目して構築し、情報端末から放射される周波数毎に復調処理を施し、復調された信号に含まれる周波数を識別子として、漏えいチャネルを特定する手法を開発した。本手法は従来の評価手法に比べ、評価時間を 1/100 程

度に短縮した。

さらに、評価対象となる機器内部の「漏えい源」から「計測位置」までの伝達関数に着目し、機器内部に漏えい源が複数ある場合に関しても、観測する周波数・観測場所を変化させることで高精度に情報を復元し、評価できることを示した。

漏えいメカニズムの解明に関しては、評価手法を用いて情報を含む漏えい電磁波の伝搬経路を正確に把握し、漏えいを引き起こす基板上の経路に寄与する設計パターンや素子配置などを明らかにした。こうしたメカニズムの解明には、情報機器をモデル化した情報漏えい評価基板とそれに対応したシミュレーション手法の双方を活用した。また、メカニズムから、漏えいモデルを生成し、従来、電磁的情報漏えいの評価が行われていなかったデバイスについてもモデルを用いて漏えいを予測可能にすると共に、実計測を用いてその予測が正しいことを実証した。また、本予測は、漏えいモデルに基づき、機器に実装された素子などの部分的な情報のみを用いて行ったが、配線や基板素材などの詳細な機器設計情報が入手できた場合、高精度な漏えい評価が可能になることについても示した。

さらに、メカニズムと漏えいモデルに基づき、情報機器の周囲の電磁環境が電磁波を通じた情報の漏えいに影響を与えることを示した。また、安価で既存機器にも実装可能な対策技術に関しては、上記で得られた電磁環境が電磁波を通じた情報の漏えいに影響に関する知見を応用し、情報機器が設置される環境、接続されるペリフェラルの数やケーブル長などを変化させることで、機器が有する電磁波の放射特性を変化させ、電磁的情報漏えいを抑止可能であることを明らかにした。また、攻撃検知技術としては、電磁情報計測を困難化するため、「電磁情報のプロービング時に情報機器周辺で観測される電磁環境の変化」を計測可能なセンサをディジタル回路のみで構成し、評価用機器を用いた実験によりその有効性を示した。また、開発した対策手法は上位レイヤのプロトコルやアプリケーションに依存しないため、機器設計時に多種多様な入出力機器に統一的に適用することが可能であることについても示した。

５．主な発表論文等

〔雑誌論文〕　計22件（うち査読付論文　22件／うち国際共著　4件／うちオープンアクセス　7件）

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 －

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 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 Kim Youngwoo、Fujimoto Daisuke、Hayashi Yuichi	４．巻 11
２．論文標題 Simultaneous Security and EMC Evaluations Based on Measuring Electromagnetic Field Distribution on PCBs	５．発行年 2022年
３．雑誌名 IEEE Electromagnetic Compatibility Magazine	６．最初と最後の頁 84～92
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/MEMC.2022.9982569	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 Kitazawa Taiki、Arai Kimihiro、Kim Youngwoo、Fujimoto Daisuke、Hayashi Yuichi	４．巻 64
２．論文標題 A Novel Remote Visualization of Screen Images Against High-Resolution Display With Divided Screens Focusing on the Difference of Transfer Function of Multiple Emanations	５．発行年 2022年
３．雑誌名 IEEE Transactions on Electromagnetic Compatibility	６．最初と最後の頁 1941～1948
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2022.3204357	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 Osuka Saki、Fujimoto Daisuke、Kawamura Shinichi、Hayashi Yuichi	４．巻 64
２．論文標題 Electromagnetic Side-Channel Analysis Against TERO-Based TRNG	５．発行年 2022年
３．雑誌名 IEEE Transactions on Electromagnetic Compatibility	６．最初と最後の頁 1288～1295
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2022.3189372	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 Kitazawa Taiki、Kubo Hiroyuki、Hayashi Yuichi	４．巻 2023
２．論文標題 A Method for Extracting Plausible Images From EM Leakage Measured at Low Sampling Rates	５．発行年 2023年
３．雑誌名 2023 IEEE 7th Global Electromagnetic Compatibility Conference	６．最初と最後の頁 34-34
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/GEMCCON57842.2023.10078185	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 Haga Rikuo、Toyoda Kodai、Shinoda Yuto、Miyahara Daiki、Shinagawa Kazumasa、Hayashi Yuichi、Mizuki Takaaki	４．巻 2022
２．論文標題 Card-Based Secure Sorting Protocol	５．発行年 2022年
３．雑誌名 Advances in Information and Computer Security	６．最初と最後の頁 224～240
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-15255-9_12	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 Haga Rikuo、Hayashi Yuichi、Miyahara Daiki、Mizuki Takaaki	４．巻 2022
２．論文標題 Card-Minimal Protocols for?Three-Input Functions with?Standard Playing Cards	５．発行年 2022年
３．雑誌名 The International Conference on Cryptography Africacrypt2022	６．最初と最後の頁 448～468
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-17433-9_19	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 Kitazawa Taiki、Hayashi Yuichi、Fukawa Yoshi、Kim Yougwoo	４．巻 2022
２．論文標題 Analysis of the PDN Induced Crosstalk Impacts on the High-Speed Signaling in Ultra- Thin and High Permittivity Substrates	５．発行年 2022年
３．雑誌名 2022 International Symposium on Electromagnetic Compatibility EMC Europe	６．最初と最後の頁 84～89
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/EMCEurope51680.2022.9900949	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 Hayashi Yuichi	４．巻 25
２．論文標題 Issue of Information Security Degradation Caused by Electromagnetic Emissions and Its Countermeasures	５．発行年 2022年
３．雑誌名 Journal of The Japan Institute of Electronics Packaging	６．最初と最後の頁 314～320
掲載論文のDOI（デジタルオブジェクト識別子） 10.5104/jiep.25.314	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 Kitazawa Taiki、Kitahara Ren、Yamagiwa Taiki、Chakarothai Jerdvisanop、Hayashi Yuichi、Kasuga Takashi	４．巻 2021
２．論文標題 Basic Study on a Novel FDTD Method Implemented Frequecy Dispersion of PCB	５．発行年 2021年
３．雑誌名 2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium	６．最初と最後の頁 580-580
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/EMC/SI/PI/EMCEurope52599.2021.9559370	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 Kaji Shugo、Fujimoto Daisuke、Kim Youngwoo、Hayashi Yuichi	4．巻 2021
2．論文標題 A Fundamental Evaluation of EM Information Leakage Induced by IEMI for a Device with Differential Signaling	5．発行年 2021年
3．雑誌名 2021Asia-Pacific International Symposium on Electromagnetic Compatibility	6．最初と最後の頁 SS-02-7
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/APEMC49932.2021.9597081	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 Wada Shinpei、Hayashi Yuichi、Fujimoto Daisuke、Homma Naofumi、Kim Youngwoo	4．巻 2021
2．論文標題 Measurement and Analysis of Electromagnetic Information Leakage From Printed Circuit Board Power Delivery Network of Cryptographic Devices	5．発行年 2021年
3．雑誌名 IEEE Transactions on Electromagnetic Compatibility	6．最初と最後の頁 1～11
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2021.3062417	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 Utsumi Kohei、Hayashi Yu-ichi、Mizuki Takaaki、Sone Hideaki	4．巻 2020
2．論文標題 Experimental Study on Measurement Resolution of Side Channel Waveform in Correlation Power Analysis	5．発行年 2020年
3．雑誌名 2020 International Symposium on Electromagnetic Compatibility - EMC EUROPE	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） 10.1109/EMCEUROPE48519.2020.9245659	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 Birukawa Ryota、Nagata Daiya、Hayashi Yu-ichi、Mizuki Takaaki、Sone Hideaki	4．巻 2020
2．論文標題 The Source Estimation of Electromagnetic Information Leakage from Information Devices	5．発行年 2020年
3．雑誌名 2020 International Symposium on Electromagnetic Compatibility - EMC EUROPE	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/URSIGASS49373.2020.9231979	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 D. Nagata, R. Birukawa, Y. Hayashi, T. Mizuki, H. Sone	4．巻 2
2．論文標題 Design of Suitable Controlled Image for Evaluation of EM Information Leakage	5．発行年 2021年
3．雑誌名 URSI Radio Science Letters	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） 10.46620/20-0054	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 Kundrata Jurica、Fujimoto Daisuke、Hayashi Yuichi、Baric Adrijan	4．巻 2020
2．論文標題 Comparison of Pearson correlation coefficient and distance correlation in Correlation Power Analysis on Digital Multiplier	5．発行年 2020年
3．雑誌名 2020 43rd International Convention on Information, Communication and Electronic Technology	6．最初と最後の頁 146-151
掲載論文のDOI（デジタルオブジェクト識別子） 10.23919/MIPRO48935.2020.9245325	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 該当する

1．著者名 Yuichi Hayashi , William A. Radasky	4．巻 2020
2．論文標題 Introduction to Measurement Methods for Electromagnetic Information Security	5．発行年 2020年
3．雑誌名 IEEE EMC+SIPI 2020	6．最初と最後の頁 1-1
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 該当する

1．著者名 林優一	4．巻 13
2．論文標題 ハードウェアに潜む電磁波セキュリティの脅威とその対策	5．発行年 2019年
3．雑誌名 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review	6．最初と最後の頁 28-37
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/essfr.13.1_28	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 Young Woo Kim, Daisuke Fujimoto, Hikaru Nishiyama, Daehwan Lho, Hyunwook Park, Joungho Kim and Yuichi Hayashi	4．巻 2019
2．論文標題 Statistical Analysis of Simultaneous Switching Output (SSO) Impacts on Steady State Output Responses and Signal Integrity	5．発行年 2019年
3．雑誌名 2019 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo)	6．最初と最後の頁 138-140
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/EMCCompo.2019.8919652	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 該当する

1．著者名 Youngwoo Kim , Daisuke Fujimoto, Shugo Kaji, Shinpei Wada, HyunwookPark, Daehwan Lho, Joungho Kim, and Yuichi Hayashi	4．巻 2020
2．論文標題 Statistical Eye-Diagram Estimation Method Considering Power/Ground Noise Induced by Simultaneous Switching Output (SSO) Buffers	5．発行年 2020年
3．雑誌名 IEEE Transactions on Electromagnetic Compatibility	6．最初と最後の頁 1-11
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2020.2975202	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 該当する

〔学会発表〕　計33件（うち招待講演　7件／うち国際学会　6件）

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 北澤太基，キムヨンウ，藤本大介，林優一
2．発表標題 薄膜高誘電率基板を用いた低インピーダンスPDNによるクロストーク抑制効果の解析
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
鍛治秀伍，太刀掛彩希，藤本大介，林優一

２．発表標題
静電容量センサの出力分布に着目したID生成手法に関する基礎検討

３．学会等名
電子情報通信学会 ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
北村圭輝，北澤太基，藤本大介，林優一

２．発表標題
利用環境を考慮したディスプレイからの電磁的漏えい強度の評価

３．学会等名
電子情報通信学会 ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
和田慎平，藤本大介，林優一，キムヨンウ

２．発表標題
暗号機器のプリント基板上の電源供給ネットワークにおける電磁的情報漏えい抑制に関する基礎検討

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
芳賀陸雄，林優一，宮原大輝，水木敬明

２．発表標題
ランダムカット1回の6枚XORプロトコルの不可能性について

３．学会等名
情報処理学会 コンピュータセキュリティ研究会

４．発表年
2022年

１．発表者名
北澤太基，久保尋之，林優一

２．発表標題
映像機器の電磁情報漏えい評価のための漏えい源モデルの検討

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
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
ERO-TRNGに対する振幅確率分布を用いた乱数性評価に関する基礎検討

３．学会等名
電子情報通信学会 ハードウェアセキュリティ研究会

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
北澤太基，高野誠也，林優一

２．発表標題
複数の復調方式を用いた漏えい電磁波からの音情報復元に関する基礎検討

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
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
高野誠也，林優一

２．発表標題
意図的電磁照射によるスピーカーフォンからの電磁情報漏えいの脅威と対策時に求められる指標の提案

３．学会等名
電子情報通信学会 ハードウェアセキュリティ研究会

４．発表年
2023年

１．発表者名
林優一

２．発表標題
高速信号伝送と電磁波セキュリティ

３．学会等名
高速信号伝送研究会（招待講演）

４．発表年
2022年

１．発表者名
橋本 律紀，藤本 大介，林 優一

２．発表標題
周波数注入攻撃に対するROベースのTRNG耐性評価に関する検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2021年

１．発表者名
太刀掛彩希，鍛治秀伍，藤本大介，林優一

２．発表標題
静電容量センサを用いたプリント基板の個体差の検出に関する基礎検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2021年

１．発表者名
西鳥羽陽，鍛治秀伍，衣川昌宏，藤本大介，林優一

２．発表標題
オンチップセンサを用いた線路上のハードウェアトロージャン検知に関する基礎検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
湯川 大雅，鍛治 秀伍，藤本 大介，林 優一

２．発表標題
通信線路上のハードウェアトロイによる電磁情報漏えい評価法の検討 ～変調度と放射強度に着目した評価 ～

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
Yuichi Hayashi

２．発表標題
Electromagnetic Security for Perceptual Information to Protect Digital Privacy

３．学会等名
IEEE Digital Privacy Workshop（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
上田浩行，藤本大介，キム・ヨンウ，北澤太基，春日貴志，林優一

２．発表標題
製造メーカの異なるコネクタの相互接続時に生ずる接触境界部の高周波特性の基礎評価

３．学会等名
電気情報通信学会ソサイエティ大会

４．発表年
2020年

１．発表者名
荒井公寛，藤本大介，林優一

２．発表標題
漏えい経路の伝達特性の差異に着目した高解像度ディスプレイに対する電磁的情報漏えい評価

３．学会等名
2021年暗号と情報セキュリティシンポジウム

４．発表年
2021年

１．発表者名
鍛治秀伍，藤本大介，林優一

２．発表標題
複数の周波数印加による電磁的情報漏えい誘発に関する検討

３．学会等名
2021年暗号と情報セキュリティシンポジウム

４．発表年
2021年

１．発表者名
福嶋章悟，藤本大介，林優一

２．発表標題
リモートワーク環境におけるスピーカーフォンからの電磁波を通じた情報漏えい評価

３．学会等名
2021年暗号と情報セキュリティシンポジウム

４．発表年
2021年

１．発表者名
福嶋章悟，藤本大介，林優一

２．発表標題
設置環境の異なるスマートスピーカーからの電磁的情報漏えい評価と対策

３．学会等名
電子情報通信学会・ハードウェアセキュリティ研究会

４．発表年
2021年

１．発表者名
荒井公寛，藤本大介，林優一

２．発表標題
複数の漏えい周波数に着目した高解像度ディスプレイからの画面情報復元に関する検討

３．学会等名
電子情報通信学会・ハードウェアセキュリティ研究会

４．発表年
2021年

１．発表者名
福嶋章悟，藤本大介，林優一

２．発表標題
利用環境を考慮したラップトップからの電磁的情報漏えい評価

３．学会等名
2021年電子情報通信学会総合大会

４．発表年
2021年

１．発表者名
上田浩行，鍛治秀伍，藤本大介，キムヨンウ，林優一

２．発表標題
接触境界の表面粗さとトルク値がコネクタ高周波特性に与える影響に関する基礎検討

３．学会等名
電子情報通信学会・機構デバイス研究会

４．発表年
2021年

１．発表者名
上田浩行， 鍛治秀伍， 藤本大介， 北澤太基， 春日貴志， 林優一

２．発表標題
Fundamental Evaluation of Impedance Variations in the Connector Caused by High-Frequency Noise Propagation

３．学会等名
International Session on Electro-Mechanical Devices（国際学会）

４．発表年
2020年

１．発表者名
Y.Hayashi

２．発表標題
Introduction to Electromagnetic Information Security

３．学会等名
2019 Symposia on VLSI Technology and Circuits（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
林優一

２．発表標題
IoT時代に求められるハードウェアセキュリティ

３．学会等名
EMC Sapporo & APEMC 2019 市民セミナー（招待講演）

４．発表年
2019年

１．発表者名
林優一

２．発表標題
EMCとセキュリティ ~電磁波によるセキュリティ低下の問題とその対策~

３．学会等名
EMCユーザ会議 2019（招待講演）

４．発表年
2019年

１．発表者名
Y.Hayashi

２．発表標題
Introduction：Application of EMC Methodology to Information Security Evaluations/Countermeasures/Education

３．学会等名
2019 IEEE International Symposium on EMC+SIPI（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Youngwoo Kim , Yu-ichi Hayashi, Fujimoto Daisuke, Hyunwook Park,and Joungho Kim

２．発表標題
Statistical Signal/Power Integrity Analysis of High-BandwidthMemory (HBM) Interposer Channel considering SSO Noise and Data Coding

３．学会等名
DesignCon 2020（国際学会）

４．発表年
2020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	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)	

６．研究組織（つづき）

	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)	

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	KAIST		
ベルギー	KU Leuven			