様式 C - 7 - 1

令和2年度科学研究費助成事業（科学研究費補助金）実績報告書（研究実績報告書）

所属研究機関名称		奈良先端科学技術大学院大学	機関番号	14603
研究代表者	部局	先端科学技術研究科		
	職	教授		
	氏名	林 優一		

1. 研究種目名 基盤研究(A)(一般) 2. 課題番号 19H011043. 研究課題名 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4. 研究期間 令和元年度～令和4年度 5. 領域番号・区分 -

6. 研究実績の概要

本年度は、情報機器からの電磁波を通じた情報漏えいを評価する技術の開発を継続して行うと共に、漏えいメカニズムの解明についても検討を進めた。情報漏えい評価技術に関しては、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、漏えいの担い手となる電磁界を正確に把握することで「漏えい経路」を正確に把握することが可能であることを示し、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、機器の利用環境も漏えいに寄与することを明らかにし、特に機器が設置される素材や機器に接続された給電線が漏えい電磁波の伝搬する範囲に影響を与えることを示した。また、電磁波の相反性に着目し、上記の知見を応用し、機器外部から電磁波を通じた情報漏えいをアクティブにコントロールできる可能性についても引き続き検討を行った。

7. キーワード

電磁情報セキュリティ サイドチャネル攻撃 電磁環境 暗号・認証

8. 現在までの進捗状況

区分 (2) おおむね順調に進展している。

理由
本年度は、評価技術開発を継続すると共に、情報漏えいメカニズムについても検討を進め、当初の計画を達成している。また、対外的な成果の公表としてIEEE Transactions on Electromagnetic Compatibilityに論文が採択されると共に、国際共著論文も採択されている。さらに、本成果のアウトリーチ活動として提案した電磁情報漏えいに関するスペシャルセッションも環境電磁工学分野の主要な国際会議である2020 IEEE International Symposium on EMCに採択された。

2 版

9. 今後の研究の推進方策

今後はこれまでに開発した評価環境、評価手法、シミュレーション手法を用いて情報機器から電磁波を通じた情報漏えいメカニズムの詳細を検討すると共に、メカニズムに基づいた情報漏えい対策手法についても検討・開発を進める。

10. 研究発表（令和2年度の研究成果）

〔雑誌論文〕 計6件（うち査読付論文 6件 / うち国際共著論文 2件 / うちオープンアクセス 0件）

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+SIP1 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

〔学会発表〕 計9件 (うち招待講演 0件 / うち国際学会 1件)

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 製造メーカー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

2 版

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 鍛冶秀伍, 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, 鍛冶秀伍, 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, 鍛冶秀伍, 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

【研究代表者・所属研究機関控】

日本学術振興会に紙媒体で提出する必要はありません。

2版

〔図書〕 計0件

1.1. 研究成果による産業財産権の出願・取得状況

計0件（うち出願0件 / うち取得0件）

1.2. 科研費を使用して開催した国際研究集会

計0件

1.3. 本研究に関連して実施した国際共同研究の実施状況

-

1.4. 備考

-