日本学術振興会に紙媒体で提出する必要はありません。

様　式　Ｃ－７－１

平成３０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）

		機関番号	１４６０３
所属研究機関名称		奈良先端科学技術大学院大学	
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(B)(一般)　　２．課題番号　16H02831

３．研究課題名　公共空間におけるスマートデバイスに対する物理攻撃への対策スイートの研究開発

４．研究期間　平成２８年度～平成３０年度　　５．領域番号・区分　－

６．研究実績の概要

本年度は、これまで得られたメカニズムを基に漏えい源から攻撃者が所有する受信アンテナまでの伝搬経路上の漏えい電磁波レベルを大幅に低減することで、漏えい電磁波を通じた情報取得の脅威に対抗する手法を開発した。伝搬経路には漏えい源からアンテナまで電磁信号を誘導するカップリングパス、機器を構成するプリント基板上の配線パターンや接続線路など機器の幾何的構造により構成されるアンテナ及び、電磁波が放射されてから受信されるまでの空間が含まれるため、これらに対し、漏えい源近傍にデカップリング回路を形成する手法や機器の筐体やケーブルから漏えいを抑制する電磁シールド手法などを適用し、これまで開発を行ったシミュレーション技術を用いて評価を行いながら、スマートデバイスに共通して適用可能な対策技術の開発を行った。さらに、これまで検討を行ってきた漏えい電磁波によるセキュリティ低下の脅威に関して、電磁波の伝搬を逆向きに考えることで、これまで得られた知見を妨害電磁波によるセキュリティ低下の脅威にも応用できる可能性についても基礎的な実験を通じて明らかにした。

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　情報システム　ディスプレイ　スマートデバイス　電磁環境

８．現在までの進捗状況

区分

理由

平成30年度が最終年度であるため、記入しない。

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

９．今後の研究の推進方策

平成30年度が最終年度であるため、記入しない。

１０．研究発表（平成３０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　1件／うちオープンアクセス　1件）

１．著者名 Y. Hayashi, N. Homma	４．巻 1
２．論文標題 Introduction to Electromagnetic Information Security	５．発行年 2019年
３．雑誌名 IEICE Transactions on Communications	６．最初と最後の頁 40-50
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transcom.2018EBI0001	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 S. Kaji, M. Kinugawa, D. Fujimoto, and Y. Hayashi	４．巻 99
２．論文標題 Data Injection Attack Against Electronic Devices With Locally Weakened Immunity Using a Hardware Trojan	５．発行年 2018年
３．雑誌名 IEEE Transactions on Electromagnetic Compatibility	６．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2018.2849105	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 S. Osuka, D. Fujimoto, Y. Hayashi, N. Homma, A. Beckers, J. Balasch, B. Gierlichs and I. Verbauwhede	４．巻 99
２．論文標題 EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakage	５．発行年 2018年
３．雑誌名 IEEE Transactions on Electromagnetic Compatibility	６．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2018.2844027	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 藤本大介，林優一	4．巻 138
2．論文標題 実環境で動的構成可能なデジタル回路を用いたIC 内部に伝導するノイズの測定法	5．発行年 2018年
3．雑誌名 電気学会論文誌A	6．最初と最後の頁 335-340
掲載論文のDOI（デジタルオブジェクト識別子） 10.1541/ieejfms.138.335	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 中村 紘，林優一	4．巻 138
2．論文標題 タイミング違反の検出に基づくIC内部の処理に過渡電磁界の与える影響評価	5．発行年 2018年
3．雑誌名 電気学会論文誌A	6．最初と最後の頁 302-308
掲載論文のDOI（デジタルオブジェクト識別子） 10.1541/ieejfms.138.309	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 K. Nakamura, Y. Hayashi, T. Mizuki, and H. Sone	4．巻 60
2．論文標題 Information leakage threats for cryptographic devices using IEMI and EM emission	5．発行年 2018年
3．雑誌名 IEEE Transactions on Electromagnetic Compatibility	6．最初と最後の頁 1340-1347
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2017.2766139	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 －

〔学会発表〕　計16件（うち招待講演　9件／うち国際学会　4件）

1．発表者名 S. Kaji, M. Kinugawa, D. Fujimoto, and Y. Hayashi
2．発表標題 Data Injection Attacks Using a Hardware Trojan on a Transmission Line
3．学会等名 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility（国際学会）
4．発表年 2018年

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

1．発表者名 S. Osuka, D. Fujimoto, Y. Hayashi, N. Homma, A. Beckers, J. Balasch, B. Gierlichs and I. Verbauwhede
2．発表標題 Fundamental Study on Non-invasive Frequency Injection Attack against RO-based TRNG
3．学会等名 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility（国際学会）
4．発表年 2018年

1．発表者名 林優一
2．発表標題 漏えい・妨害電磁波によるセキュリティ低下の脅威と対策
3．学会等名 IEEE SSCS Kansai Chapter Technical Seminar（招待講演）
4．発表年 2018年

1．発表者名 林優一
2．発表標題 情報機器に求められる電磁波セキュリティ
3．学会等名 第４回 極限環境電磁波センシング研究施設ワークショップ（招待講演）
4．発表年 2018年

1．発表者名 林優一
2．発表標題 情報セキュリティとEMC
3．学会等名 第19回EMCシンポジウムIIDA2018（招待講演）
4．発表年 2018年

１．発表者名
林優一

２．発表標題
電磁波による情報漏えいの脅威とその対策

３．学会等名
奈良先端科学技術大学院大学公開講座2018（招待講演）

４．発表年
2018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関西2018（招待講演）

４．発表年
2018年

１．発表者名
Y.Hayashi

２．発表標題
EM Information Leakage Threat Caused by Low-power IEMI and Hardware Trojan

３．学会等名
AMEREM（招待講演）

４．発表年
2018年

１．発表者名
林優一

２．発表標題
IoT時代の電磁波セキュリティ～痕跡を残さない攻撃とその対策～

３．学会等名
IoTセキュリティフォーラム2018（招待講演）

４．発表年
2018年

1．発表者名 林優一
2．発表標題 融合領域におけるEMC 分野の役割と人材育成
3．学会等名 次世代のEMC 研究者・技術者を交えたワークショップ, NICT/EMC-net 将来課題研究会（招待講演）
4．発表年 2018年

1．発表者名 Y.Hayashi
2．発表標題 EMC from hardware security perspective
3．学会等名 The 1st Croatia-Japan EMC Workshop（招待講演）
4．発表年 2018年

1．発表者名 D. Fujimoto, T. Narimatsu, Y. HAYASHI
2．発表標題 Fundamental Study on the Effect of Torque Value at Connector on Equivalent Circuit of Contact Boundary
3．学会等名 国際セッションIS-EMD2018（国際学会）
4．発表年 2018年

1．発表者名 R. Birukawa, G. Tanabe, Y. Hayashi, T. Mizuki, and H. Sone
2．発表標題 A Study on an Evaluation Method for EM Information Leakage Utilizing Controlled Image Displaying
3．学会等名 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility（国際学会）
4．発表年 2018年

1．発表者名 硲マーティン，衣川昌宏，藤本大介，林優一
2．発表標題 意図的な電磁波注入による漏えい情報の制御に関する基礎検討
3．学会等名 2018年電子情報通信学会ソサイエティ大会
4．発表年 2018年

1．発表者名 仁科泉美，藤本大介，衣川昌宏，林優一
2．発表標題 スマートデバイスからの電磁情報漏えい源特定に関する基礎検討
3．学会等名 ハードウェアセキュリティ研究会
4．発表年 2018年

1．発表者名 岡本拓実，藤本大介，林優一，本間尚文，Arthur Beckers，Josep Balasch，Benedikt Gierlichs，Ingrid Verbauwhede
2．発表標題 ガウス雑音を用いた暗号機器への意図的な電磁妨害に対する耐性評価手法
3．学会等名 ハードウェアセキュリティ研究会
4．発表年 2018年

〔図書〕　計1件

1．著者名 一般社団法人　電気学会　電気システムセキュリティ特別技術委員会 スマートグリッドにおける電磁的セキュリティ特別調査専門委員会	4．発行年 2018年
2．出版社 科学情報出版	5．総ページ数 345
3．書名 IoT時代の電磁波セキュリティ　～21世紀の社会インフラを電磁波攻撃から守るには～	

１１．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）

日本学術振興会に紙媒体で提出する必要はありません。

１２．科研費を使用して開催した国際研究集会

計0件

１３．本研究に関連して実施した国際共同研究の実施状況

―

１４．備考

―