

様 式 F - 7 - 2

科学研究費助成事業（学術研究助成基金助成金）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	1 4 6 0 3
研究 代表者	部局	先端科学技術研究科		
	職	助教		
	氏名	藤本 大介		

1．研究種目名 若手研究 2．課題番号 18K18050

3．研究課題名 計測装置におけるセキュリティ要件の解明と対策技術の開発検討

4．補助事業期間 平成30年度～令和元年度

5．研究実績の概要

IoT機器などの普及によりセンサを用いた計測の重要性が高まっている．一方で悪意のある攻撃者が意図的な妨害信号を外部から注入することによるセンサの誤動作が計測セキュリティとして指摘されつつある．距離計、ジャイロなどの様々なセンサに対して攻撃手法が提案される一方で、対策手法については複数のセンサを組み合わせるなどの消極的な手法にとどまっている．本研究では、自律制御システムで外界の情報を取得するセンサデバイスの取得過程におけるセキュリティに関して、センサへの入出力となるアナログ信号に着目し、攻撃可能性の評価、および対策技術の検討を行った．攻撃可能性の評価のために実センサを用いた攻撃再現環境を構築した．環境構築の過程において電磁波を通じたセンサの測定タイミングの可能性を発見し、構築システムにて攻撃可能性の検討を行った．電磁波を通じた攻撃では、センサからの測定信号を直接取得する攻撃に対して、信号を取得可能な範囲が広がる可能性がある．また、電磁波により測定タイミングが漏えいするメカニズムが異なることから、機器内部のケーブルの接触不良により漏えいが増大する可能性を指摘した．攻撃に対する対策技術としてデジタル信号変調がアナログ信号に変換される過程での非線形性を利用することを提案した．これにより、攻撃者が外部でアナログ信号へと変換された測定信号を取得したとしても元のデジタル信号の再現が困難になる可能性を示した．

6．キーワード

ハードウェアセキュリティ センサセキュリティ 計測セキュリティ

7．研究発表

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

1．著者名 FUJIMOTO Daisuke、NARIMATSU Takashi、HAYASHI Yu-ichi	4．巻 E102.C
2．論文標題 Fundamental Study on the Effects of Connector Torque Value on the Change of Inductance at the Contact Boundary	5．発行年 2019年
3．雑誌名 IEICE Transactions on Electronics	6．最初と最後の頁 636～640
掲載論文のDOI（デジタルオブジェクト識別子） <a href="https://doi.org/10.1587/transele.2019EMP0005">https://doi.org/10.1587/transele.2019EMP0005</a>	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 -

2 版

1. 著者名 Masahiro Kinugawa, Daisuke Fujimoto and Yuichi Hayashi	4. 巻 2019
2. 論文標題 Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure	5. 発行年 2019年
3. 雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems	6. 最初と最後の頁 62 -90
掲載論文のDOI (デジタルオブジェクト識別子) <a href="https://doi.org/10.13154/tches.v2019.i4.62-90">https://doi.org/10.13154/tches.v2019.i4.62-90</a>	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7件 (うち招待講演 0件 / うち国際学会 2件)

1. 発表者名 Daisuke Fujimoto, Yuichi Hayashi
2. 発表標題 Study on Estimation of Sensing Timing Based on Observation of EM Radiation from ToF Range Finder
3. 学会等名 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo (国際学会)
4. 発表年 2019年

1. 発表者名 Hikaru Nishiyama, Takumi Okamoto, Kim Young Woo, Daisuke Fujimoto and Yuichi Hayashi
2. 発表標題 Fundamental Study on Influence of Intentional Electromagnetic Interference on IC Communication
3. 学会等名 the 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (国際学会)
4. 発表年 2019年

1. 発表者名 大須賀彩希, 藤本大介, 林 優一
2. 発表標題 TERO-based TRNGの発振回数の変化から推定可能な出力ビットの評価
3. 学会等名 ハードウェアセキュリティフォーラム
4. 発表年 2019年

1. 発表者名 中尾文香, 藤本大介, 林 優一
2. 発表標題 モータ制御通信へのクロックグリッチ注入の影響に関する基礎検討
3. 学会等名 電子情報通信学会ソサイエティ大会
4. 発表年 2019年

1. 発表者名 大須賀 彩希, 藤本 大介, 林 優一
2. 発表標題 単純電磁波解析を用いたTERO-based TRNGの出力ビット推定
3. 学会等名 暗号と情報セキュリティシンポジウム
4. 発表年 2020年

1. 発表者名 藤本 大介, 中尾 文香, 林 優一
2. 発表標題 スマートロックに対する電磁波照射を用いた強制的な開錠の脅威
3. 学会等名 暗号と情報セキュリティシンポジウム
4. 発表年 2020年

1. 発表者名 西山 輝, 岡本 拓実, 藤本 大介, 林 優一
2. 発表標題 意図的な電磁妨害がIC通信に与える影響に関する基礎検討
3. 学会等名 電磁環境両立性研究会
4. 発表年 2019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

8．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）

9．科研費を使用して開催した国際研究集会

計0件

10．本研究に関連して実施した国際共同研究の実施状況

-

11．備考

-