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　Ｆ－７－１

科学研究費助成事業（学術研究助成基金助成金）実施状況報告書（研究実施状況報告書）（令和元年度）

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)(特設分野研究)　　２．課題番号　18KT0050

３．研究課題名　センシング情報の真正性を保証する物理層におけるトラスト基盤の確立

４．補助事業期間　平成３０年度～令和２年度

５．研究実績の概要

センシング情報の真正性を保証する基盤技術開発を開発するために、①環境電磁波を認証情報としたセンサ入力部に対するデータ改ざん検出技術の開発、②機器内部の電磁界分布センシングによるデータ改ざん検出技術の開発、③データ変換時に生ずる電磁的な特徴量を用いたセンサ認証技術の開発を遂行した。
具体的には、センサ入力部に対するデータ改ざん検出に関しては、センサ入力部を情報機器のI/Oで模擬し、複数の情報機器を対象に改ざんを実行し、その際に生ずるデバイス周囲の電磁環境の変化を計測した。そして、機器内外のデータ改ざんを検出するための特徴量について検討を行い、特徴量を用いた改ざん検出手法についてもハードウェアセキュリティ分野や環境電磁工学分野の国際会議及び論文誌で提案を行った。また、機器内部の改ざんにおいてはA/D変換器に着目し、電気的な外乱が機器内部に到達したことを想定し、アナログ信号がディジタル信号に変換される際、値が改ざんされる可能性について検討を行った。
認証技術に関してはデータ入力変換部とそれが実装された基板も含めたシステム全体から生ずる電磁的な特徴量に着目し、フランスTelecom ParisTechのJean-Luc Danger教授の研究グループとの国際連携を通じて開発を進め、当該分野の主要な国際会議に論文を投稿し、採録されている。さらに、機器設計段階におけるセキュリティ評価を行うために、意図的な電気的外乱への耐性を評価可能な基礎的なシミュレーション環境の構築を行った。

６．キーワード

電磁波セキュリティ　計測セキュリティ　真正性保証　故障利用解析

７．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
①環境電磁波を認証情報としたセンサ入力部に対するデータ改ざん検出技術の開発、②機器内部の電磁界分布センシングによるデータ改ざん検出技術の開発、③データ変換時に生ずる電磁的な特徴量を用いたセンサ認証技術の開発のそれぞれについて研究を進めると共に、各知見を有機的に融合させ、本研究課題の達成目標であるセンシング情報の真正性を保証する基盤技術の開発を遂行した。①から③の各研究成果は当該分野の主要な国際会議、論文誌に採択されており、研究は当初の計画通り順調に進展している。

８．今後の研究の推進方策

今後は、今年度までに構築した計測・評価環境、シミュレーション環境を用いて、①環境電磁波を認証情報としたセンサ入力部に対するデータ改ざん検出技術の開発、②機器内部の電磁界分布センシングによるデータ改ざん検出技術の開発、③データ変換時に生ずる電磁的な特徴量を用いたセンサ認証技術の開発を継続すると共に、得られた成果を融合させ、④真正性の保証されたデータを提供するセンシング基盤の構築を行う。

９．次年度使用が生じた理由と使用計画

センサ入力部に対するデータ改ざん検出を行うために評価用基板を作成する予定であったが、この改ざん評価は汎用的な情報機器に搭載されたI/OやADCを用いて同等の評価を行うことができたため、評価用基板として計上していた予算を次年度に繰り越すこととした。また、汎用的な情報機器を用いた高精度な評価には、これまで開発した計測環境の精度向上が必要となるため、繰り越した予算はこれに充てる。

１０．研究発表（令和元年度の研究成果）

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　1件／うちオープンアクセス　1件）

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 (TCHES)	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） 10.13154/tches.v2019.i4.62-90	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 Hikaru Nishiyama, Takumi Okamoto, Kim Young Woo, Daisuke Fujimoto and Yuichi Hayashi	４．巻 2019
２．論文標題 Fundamental Study on Influence of Intentional Electromagnetic Interference on IC Communication	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 201-203
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/EMCCompo.2019.8919838	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 Daisuke FUJIMOTO, Takashi NARIMATSU, Yuichi HAYASHI	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） doi.org/10.1587/transele.2019EMP0005	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 Shugo Kaji, Masahiro Kinugawa, Daisuke Fujimoto, Laurent Sauvage, Jean-Luc Danger, Yuichi Hayashi	4．巻 2019
2．論文標題 Method for Identifying Individual Electronic Devices Focusing on Differences in Spectrum Emissions	5．発行年 2019年
3．雑誌名 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility	6．最初と最後の頁 670-670
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13件（うち招待講演　1件／うち国際学会　1件）

1．発表者名 川上 莉穂，鍛治 秀伍，衣川 昌宏，藤本 大介，林 優一
2．発表標題 電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波の抑制に関する基礎検討
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 2019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 電子情報通信学会・環境電磁工学研究会
4．発表年 2019年

1．発表者名
鍛治 秀伍，衣川 昌宏，藤本 大介，林 優一

2．発表標題
電磁的情報漏えいを強制的に誘発する照射周波数推定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
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に対する周波数注入攻撃時の出力ビット推定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
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
川上莉穂，藤本大介，林 優一

2．発表標題
複数の信号を含む漏えい電磁波からのターゲット信号の抽出に関する検討

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

日本学術振興会に紙媒体で提出する必要はありません。

1．発表者名
川上 莉穂，鍛治 秀伍，衣川 昌宏，藤本 大介，林 優一

2．発表標題
複数のデータ伝送路を有するICから強制的に引き起こされる電磁的情報漏えいに関する検討

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
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
鍛治 秀伍，藤本 大介，衣川 昌宏，林 優一

2．発表標題
電子機器への連続波注入による強制的な電磁情報漏えい誘発に関する基礎検討

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 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 岡本拓実，藤本大介，崎山一男，李　陽，林　優一
2．発表標題 順序回路への故障注入に起因した不均一な頻度分布を持つ誤り出力を用いた故障利用解析
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 2020年

1．発表者名 Yuichi Hayashi
2．発表標題 EM Information Leakage Threat Caused by Low-power IEMI and Hardware Trojan
3．学会等名 The 2019 IEEE International Symposium on EMC+SIPI（招待講演）（国際学会）
4．発表年 2019年

〔図書〕　計0件

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）

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

―