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　３ 年　 ５ 月 ２５ 日現在

機関番号：１４６０３
研究種目：基盤研究(B)（特設分野研究）
研究期間：2018～2020
課題番号：１８ＫＴ００５０

研究課題名（和文）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

研究課題名（英文）Establishment of a Trusted Platform at the Physical Layer to Guarantee the Authenticity of Sensing Information

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）　　14,200,000円

研究成果の概要（和文）：本研究では、実世界センシングにより得られる情報の真正性を保証するために（１）センサ入力部におけるデータの改ざんに対抗するためにセンサ周囲の電磁界を認証情報として用い、データの真正性を保証する技術を開発すると共に（２）センサ内部及びデータ伝送時の改ざんに対抗するため、機器内部の電磁界分布をモニタリングすることで改ざんの予兆を検出すると共にデータの真正性を保証する技術を開発した。また、（３）センサを搭載したデバイス自体を置き換えて値を改ざんする脅威に対し、センシングデバイスが有する物理特性を認証情報として用い、デバイスの真正性を保証する技術の開発を行った。

研究成果の学術的意義や社会的意義
センシングを行う過程で得られる値の真正性については十分な議論がなされておらず、意図的な妨害波などを通じてセンシング過程において情報改ざんが行われた場合、上位レイヤにおける情報保護技術による検出は困難であり、センシング情報を基に創出されるサービス全ての信頼性を著しく低下させる新たな脅威となり得る。
本研究では、センシング情報の改ざんを行いIoTシステム全体のセキュリティを低下させる脅威に対抗するために、情報セキュリティ、環境電磁工学、集積回路工学の3分野の知見を併せ、ハードウェアレベルで真正性の保証されたセンシング情報を提供する技術開発を行った。

研究成果の概要（英文）：In this research, we have developed fundamental technologies to guarantee the authenticity of information obtained through real-world sensing, which is the key to creating services in the IoT era. The following technologies were developed to achieve the above goals. (1) Technology guarantees the authenticity of data by using environmental electromagnetic waves distributed around the sensor as authentication information to resist data tampering at the sensor input. (2) Technology to detect signs of tampering and guarantee data integrity by monitoring the distribution of the electromagnetic field inside the device in real-time to counter tampering inside the sensor and during data transmission. (3) Technology to guarantee the device's authenticity by using the physical characteristics of the sensing device as authentication information against the threat of tampering with values by replacing the device itself equipped with the sensor.

研究分野：情報セキュリティ

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

１．研究開始当初の背景

エッジノードなどからネットワークを介して大量のセンシング情報が生成され、これらがリアルタイムに処理系に伝送されて活用されると共に、ビッグデータとしてクラウドなどのサイバー空間に蓄積されるようになっている。実空間の人やモノがそれらを複合的に活用することで、人々の日常生活、社会経済活動、教育研究活動、行政活動などに資する新たなサービスが創出され、多数の人々がそれらを社会インフラとして利用する新しい情報社会が到来しつつある。この様にして創出されるサービスは、コンピュータやセンサなどからネットワークを介して大量に収集されたセンシング情報が正しいという前提で提供される。

一方、近年の検討では、数 V 程度の妨害波により、機器内部で処理される値を非侵襲に改ざんし、出力に僅かなビット誤りを生じさせ、それを統計的に解析することで暗号化に用いる秘密鍵の取得に成功したという報告もなされており、こうした値の改ざんは暗号機器に限らず、IoT 時代のサービス創出の要となる実世界センシングにより得られる情報の改ざんにも繋がる可能性がある。そのため、上位のアプリケーションがサービスを提供する際、誤った情報の提示や誤った判断の導出に繋がり、サービスのトラストを大幅に低下させる可能性がある。

すなわち、上述の検討では「収集されたデータは信頼できるのか？」という問を投げかけており、センシング情報の真正性が保証されない場合、それらの情報を利活用する全てのサービスアプリケーションの信頼性が損なわれることを示唆しており、これまで上位のレイヤで検討されてきた高機能な暗号アルゴリズムや高度なデータ構造などを用いたセキュリティの確保とは異なる対策が求められる。

２．研究の目的

これまでセンシングを行う過程で得られる値の真正性については十分な議論がなされておらず、意図的な妨害波などを通じてセンシング過程において情報改ざんが行われた場合、上位レイヤにおける情報保護技術による検出は困難であり、センシング情報を基に創出されるサービス全ての信頼性を著しく低下させる新たな脅威となり得る。

本研究では、センシング情報の改ざんを行い、IoT システム全体のセキュリティを低下させる脅威に対抗するために、情報セキュリティ、環境電磁工学、集積回路工学の 3 分野の知見を併せ、ハードウェアレベルで真正性の保証されたセンシング情報を提供する技術開発を行うと共に、セキュアなセンシング環境を構築するためのフレームワーク及び機器設計指針を提供する。

３．研究の方法

本研究では、IoT 時代のサービス創出の要となる実世界センシングにより得られる情報の真正性を保証する基盤技術の開発を行う。

具体的には、（１）センサ入力部におけるデータの改ざんに対抗するためにセンサ周囲に分布する環境電磁波を認証情報として用い、データの真正性を保証する技術を開発すると共に（２）センサ内部及びデータ伝送時の改ざんに対抗するため、機器内部の電磁界分布をリアルタイムモニタリングすることで改ざんの予兆を検出すると共にデータの真正性を保証する技術を開発する。また、（３）センサを搭載したデバイス自体を置き換えて値を改ざんする脅威に対し、センシングデバイスが有する物理特性を認証情報として用い、デバイスの真正性を保証する技術を開発する。

４．研究成果

（１）センサ入力部におけるデータの改ざんに対抗するためにセンサ周囲に分布する環境電磁波を認証情報として用い、データの真正性を保証する技術の開発に関しては、攻撃が実行される際に生ずるセンサ入力部と攻撃セットアップとの電磁界結合に着目し、電磁界結合の強さを周波数領域で観測することにより改ざんの有無を検出する手法を開発した。また、着目する界としては電界に着目し、センサ入力部が実装される基板上の導体部分と攻撃セットアップを構成する導体部分の結合により生ずるセンサ周囲に分布する電界の乱れの有無を認証情報として用いた。

（２）センサ内部及びデータ伝送時の改ざんに対抗するため、機器内部の電磁界分布をリアルタイムモニタリングすることで改ざんの予兆を検出すると共にデータの真正性を保証する技術の開発に関しては、データ改ざんを発生させる要因として考えられるオーバークロック、IR ドロップ、グリッジ挿入をリアルタイムにモニタリング可能で機器内部に容易に実装可能なフルディジタルで構成されたセンサを開発し、前述した要因により生ずる機器内部の電磁界の乱れをセンシングし、攻撃の予兆を検出する技術を開発した。

（３）センサを搭載したデバイス自体を置き換えて値を改ざんする脅威に対し、センシングデバイスが有する物理特性を認証情報として用い、デバイスの真正性を保証する技術の開発に関し

ては、基板上に実装される素子の実装ばらつきによる機器の電気特性の変化に着目し、この変化に起因して変化する機器からの放射電磁波のスペクトルの変化、放射電磁波のスペクトルが弱い場合には意図的に電磁波を照射することで再放射される電磁波を認証情報として用いることで、デバイス自体を置き換える攻撃への対策とした。

さらに、機器設計段階において攻撃への耐性を評価可能で、膨大な計算資源を必要としないシミュレーション技術についても HSPICE ベースで開発した。

また、得られた成果の一部は、フランス Telecom ParisTech の Jean-Luc Danger 教授の研究グループ及びベルギーKU Leuven の Ingrid Verbauwhede 教授のグループとの国際連携を通じて得られたものであり、本研究課題を通じて国際連携が加速した。

本プロジェクトの成果と関連する分野の研究成果からなるスペシャルセッションを環境電磁工学分野の主要な国際会議である、IEEE EMC Society International Symposium on EMC+SIPI 及び The Asia-Pacific International Symposium on Electromagnetic Compatibility に提案し、これが採択された。

５．主な発表論文等

〔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） 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21件（うち招待講演　1件／うち国際学会　1件）

1．発表者名
鍛治秀伍，藤本大介，林優一

2．発表標題
意図的な電磁妨害時に生ずる情報漏えいの基礎評価

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
2020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
意図的に引き起こされる電磁的情報漏えい評価法の検討 ～ デジタル出力回路のインピーダンス変化に着目した評価 ～

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
2020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(SCIS2021)

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
2020年

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

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

１．発表者名
和田 慎平, 藤本 大介, 林 優一

２．発表標題
IC周囲に分布する電磁雑音を用いた電磁波解析攻撃検知手法の検討

３．学会等名
電子情報通信学会・環境電磁工学研究会(EMCJ)

４．発表年
2018年

１．発表者名
鍛治秀伍, 衣川昌宏, 藤本大介, Laurent Sauvage, Jean-Luc Danger, 林優一

２．発表標題
製造・実装ばらつきに起因する放射スペクトルの違いを用いた電子機器の個体識別手法に関する基礎検討

３．学会等名
電子情報通信学会・HWS・VLD合同研究会

４．発表年
2018年

１．発表者名
成松貴,藤本大介,林優一

２．発表標題
締め付けトルクの減少が接触境界の高周波素子に与える影響に関する検討

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
2018年

１．発表者名 Shinpei WADA, Daisuke FUJIMOTO, Yuichi HAYASHI
２．発表標題 Detecting Electromagnetic Analysis Attacks Using the Distribution of Electromagnetic Noise
３．学会等名 EMC Joint Workshop 2018 Daejeon
４．発表年 2018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)	

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			
フランス	Telecom ParisTech			
ベルギー	KU Leuven			