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２９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	情報科学研究科
	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

今年度は、機器から放射される情報漏えい周波数において、描画情報の色が変化する際、放射電磁波の振幅に差が生ずることに着目し、ディスプレイに表示する情報を選択することで、機器から放射された電磁波スペクトルの中で、情報を含む周波数か否かを簡単に判定出来る評価手法を提案した。本手法により、従来法に比べ、簡便な処理によって評価が実現可能となったことから、スマートデバイス内外の漏えい情報を含む電磁界伝搬を高速に計測することが可能となった。また、上記の計測により、情報の漏えいは画面描画に関わるデータをシリアルに処理するIC及びケーブルを漏えい源とし、それらの信号が伝送される際、屈曲部などを有する部分から寄生結合を通じて周囲の導体に信号が漏えいすることにより生ずることを明らかにした。

また、上記のメカニズムにより、情報を含む電磁放射は機器を構成する基板のサイズや信号を伝送するケーブル長などの物理構造により引き起こされると予想されることから、設計データからこうした物理構造のみを抽出した簡易的なシミュレーションモデルを構築した。

さらに、情報漏えいに関し、機器内部の電気回路を意図的に改造し、情報漏えいを意図的に誘発する脅威が近年指摘されており、これまで検討をおこなってきた「機器から非意図的な電磁放射により引き起こされる脅威」に加えて、これらの脅威についても基礎的な評価法・対策法の検討に着手した。

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　(2) おおむね順調に進展している。

理由

今年度はメカニズムの解明とシミュレーションモデルの構築を目標に掲げ研究を遂行し、予定通りの結果を得ている。また、メカニズムを解明するために必要となる電磁波伝搬計測・評価手法については従来の評価法に比べ1/10から1/100程度の時間で評価を可能にする評価法を新たに開発することに成功している。今年度のターゲットはタブレットやスマートフォンなどのタッチスクリーンデバイスであったが、開発した評価方法は情報機器全般に汎用的に適用できる可能性がある。

９．今後の研究の推進方策

今後は、これまでに開発を行った評価システム及びシミュレーションモデルを用いてスマートデバイス内外の電磁界伝搬を高時間・高空間分解能で観測し、電磁波可視化技術を用いて時系列で可視化することにより、漏えいの詳細なメカニズムを解明すると共に評価法を確立する。さらに、得られたメカニズムを基に、配線パターンなどの幾何的な形状及び、環境電磁工学分野で開発されたノイズ抑制素子、これまでに開発した電磁界センサなどを効果的に組み合わせ、それを逐次シミュレーション上で評価しながら、幅広い機器に適用可能な対策技術を開発する。さらに、情報の漏えいを意図的に誘発するハードウェアトロージャンによる脅威についても検討を進める予定である。

１０．研究発表（平成２９年度の研究成果）

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著論文　1件／うちオープンアクセス　0件）

１．著者名 Ko Nakamura, Yuichi Hayashi, Takaaki Mizuki, Hideaki Sone	４．巻 印刷中
２．論文標題 Information Leakage Threats for Cryptographic Devices Using IEMI and EM Emission	５．発行年 2017年
３．雑誌名 IEEE Transactions on Electromagnetic Compatibility	６．最初と最後の頁 1～8
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 －

１．著者名 Yuichi Hayashi, Jong-Gwan Yook, William A. Radasky	４．巻 -
２．論文標題 Hardware Security for Information/Communication Devices	５．発行年 2017年
３．雑誌名 2017 Asia-Pacific International Symposium on Electromagnetic Compatibility	６．最初と最後の頁 92-92
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8件（うち招待講演　2件／うち国際学会　1件）

１．発表者名 杉本藍莉，林優一，水木敬明，曽根秀昭
２．発表標題 暗号機器からの電磁情報漏えいにおける周波数特性に関する研究
３．学会等名 EMC仙台ゼミナール
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。

1．発表者名 林優一，水木敬明，曽根秀昭
2．発表標題 描画情報の選択を用いた電磁情報漏えいの評価に関する研究
3．学会等名 EMC仙台ゼミナール・IEEE EMC-S Sendai-Ch学生発表会
4．発表年 2018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 HTを用いて局所的にイミュニティを低下させた電子機器へのデータ注入攻撃
3．学会等名 2018年暗号と情報セキュリティシンポジウム
4．発表年 2017年

1．発表者名 田辺弦太郎，林優一，水木敬明，曽根秀昭
2．発表標題 描画情報の制御時における放射電磁波の特徴量に着目した情報漏えい評価
3．学会等名 IEEE Instrumentation & Measurement Society Japan Chapter 2017年度 第2回学生研究発表会
4．発表年 2017年

1．発表者名 杉本藍莉，藤本大介，林 優一，水木敬明，曽根秀昭
2．発表標題 周波数選択による暗号機器の情報漏えい評価の効率化に関する検討
3．学会等名 環境電磁工学研究会
4．発表年 2017年

1．発表者名 田辺弦太郎，林 優一，水木敬明，曽根秀昭
2．発表標題 表示画像の選択を用いた電磁情報漏えい評価手法に関する検討
3．学会等名 環境電磁工学研究会
4．発表年 2017年

1．発表者名 Yuichi Hayashi
2．発表標題 EM Information Security Threats and Its Countermeasures
3．学会等名 EMC Beijing 2017（招待講演）（国際学会）
4．発表年 2017年

1．発表者名 林 優一
2．発表標題 次世代ワイヤレス通信に求められるハードウエアセキュリティ
3．学会等名 次世代ワイヤレス技術講座 - KEC関西電子工業振興センター（招待講演）
4．発表年 2017年

〔図書〕　計1件

1．著者名 瀬戸信二，富永哲欣，秋山佳春，市川紀充，井上慎，上田芳信、内山一雄，國分誠，小林正明，栄千治，崎山一男，島田一夫，高谷和宏，竹谷晋一，立松明芳，徳田正満，服部光男，峯松育弥，関口秀紀，林優一	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）

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

―