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　４ 年　 ６ 月 ２０ 日現在

機関番号：３２６８９
研究種目：基盤研究(B)（一般）
研究期間：2019～2021
課題番号：１９Ｈ０４１１１

研究課題名（和文）IoTのアプリ化に向けたコンテキストアウェア・セキュリティ制御技術

研究課題名（英文）Context-aware Approaches for Securing Appified IoT Devices

研究代表者
森　達哉（Mori, Tatsuya）

早稲田大学・理工学術院・教授

研究者番号：６０７０８５５１

交付決定額（研究期間全体）：（直接経費）　　13,460,000円

研究成果の概要（和文）：本研究課題は、IoTプラットフォーム上で動作するアプリケーションのセキュリティ、プライバシーの問題に着目し、アプリケーションが利用されるコンテクスト基づいた挙動の解析手法、ならびに制御手法に取り組んだ。具体的には、(1)「アプリ化されたIoTプラットフォームにおけるセキュリティ脅威・課題の大規模調査」(2)「IoTアプリ動作のコンテキスト検査技術の開発」(3)「IoTプラットフォームにおけるアクセス制御・緊急処理機構の開発」を実施した。

研究成果の学術的意義や社会的意義
アプリ化したIoT に対するセキュリティの確保はサイバー空間で生じる脅威の対策のみならず、我々が生活する実世界空間の安全を守るために、社会的に重要な課題である。IoT に固有な「実世界とのインタラクション」は、個々のインタラクションが適切なものであるか、あるいは検査が必要なものであるかの判断，すなわちコンテキストの理解が必要であることを示唆する。アプリの挙動解析において、コンテキストを理解するという問題は、従来の PC やモバイルプラットフォームのセキュリティでは顕在化してこなかった未解決の問題であり、そのような問題にとりくむことに学術的意義がある。

研究成果の概要（英文）：This research project focused on the security and privacy issues of applications running on IoT platforms, and worked on methods for analyzing and controlling the behavior of applications based on the context in which they are used. Specifically, we conducted (1) a large-scale measurement study of security threats and issues in application-oriented IoT platforms, (2) development of context inspection techniques for IoT application behavior, and (3) development of access control and emergency handling mechanisms for IoT platforms.

研究分野：情報セキュリティ

キーワード：セキュリティ　アプリ　IoT　コンテキスト

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

IoT (Internet of Things) デバイスにおいては、機器の機能を拡張するソフトウェアがアプリとして配布されるプラットフォームが普及している。そのようなモデルは、スマートフォンやタブレット端末で広く採用されている．一方、アプリが中心のプラットフォームが普及することにより アプリの脆弱性をつく攻撃や，悪意のあるアプリ，すなわち マルウェアによる新たな脅威をもたらすリスクを抱えている． また、IoT に対するセキュリティ脅威は従来の PC やスマートフォンを対象とした脅威と比較して，より深刻なものとなる．IoT デバイス，すなわち「モノ」は我々が生きる実世界とのインタラクションを通じて動作するため，IoT デバイスへの攻撃が成立することは我々自身に対する物理的攻撃も可能になることを意味する．IoT デバイスに固有な「実世界とのインタラクション」は，個々のインタラクションが適切なものであるか，あるいは検査が必要なものであるかの判断，すなわちコンテキストの理解が必要不可欠であることを示唆する．こうした問題は従来の PC やモバイルプラットフォームのセキュリティでは顕在化してこなかった．

２．研究の目的

本研究は、以下の学術的問い (Research Question: RQ) に取り組む。

RQ1: アプリ化した IoT に対するセキュリティ脅威とはいかなるものか？

RQ2: 多様な実空間コンテキストを持つ IoT のセキュリティ制御をどのように実現できるか？

RQ1 はこれから普及するアプリ化した IoT プラットフォームに対するセキュリティ脅威を，(1)実機に基づく現状調査，および(2)PC やスマートフォンにおけるマルウェアの事例に基づく実験を通じて明らかにすることを意図している．IoT デバイスは実世界とインタラクションを行うため，動作の自由度が高い．その一方で，「モノ」として期待される動作をポリシーとして規定することは可能である．RQ2 として示した問いの狙いは，実空間において多様なコンテキストをもつ IoT 機器に対し，期待される動作(ポリシー) に反する悪性な挙動を適切に制御する方法を見出すことにある． これら 2 つの学術的問いに答えるために，本研究課題ではアプリ化された IoT プラットフォームに向けた コンテキストアウェア・セキュリティ制御技術の確立を研究目的とする．

３．研究の方法

前述した目的を達成するために本研究では以下 3 つのワークパッケージ (WP)に取り組む．

WP1:アプリ化された IoT プラットフォームにおけるセキュリティ脅威・課題の大規模調査

WP1 は RQ1 に直接アプローチすることを狙いとし，IoT アプリのセキュリティ評価環境構築、IoT アプリの攻撃可否・耐性評価に取り組む。

WP2:IoT アプリ動作のコンテキスト検査技術の開発

WP2 は RQ2 の前段として，アプリが関与する入出力の関係をもとに，アプリ動作のコンテキストを検査し，個々のアクションの正当性を判定することを狙いとしインタラクションの計測技術の開発、コンテキスト検査技術の開発に取り組む。

WP3:IoT プラットフォームにおけるアクセス制御・緊急処理機構の開発

P3 は RQ2 の後段として，WP2 の開発技術で得るコンテキスト検査結果をもとに，セキュリティ上の脅威や，故障などの誤動作に対して，被害を最小とするためのセキュリティ制御技術の実現に取り組む

４．研究成果

以下では、各 WP において得られた研究成果概略を報告する。

WP1:アプリ化された IoT プラットフォームにおけるセキュリティ脅威・課題の大規模調査

WP1 として、IoT アプリ[2,7,8,9,10]および Android アプリ[1,2,3,4,5,6]の大規模な調査を実施し、それぞれのプラットフォームに特有なセキュリティリスクや脅威を明らかにした。これらの研究においては、独自のデータ収集方法を開発し、実アプリの計測と分析を行った点に特徴がある。また、[9]では今日の代表的な IoT アプリ・プラットフォームである、Voice Assistant(VA)のアプリを対象として、アプリの挙動に関する情報を大規模に調査した結果を報告した（右表)。この結果、音声対話および陽には表示されないメタデータの通信を通じて、ユーザのプライバシ情報を収集する VA アプリが無視できない数存在することを明らかにした。なお、この計測調査を実施する上では、WP2 で開発したコンテキスト検査技術を活用している。

個人情報別取得方法及び VA アプリ数

個人情報	取得方法	個数
生年月日等	対話	16
名前	対話	2
	Google Sign-In	10
	Helpers インテント	1
メールアドレス	対話	1
	Google Sign-In	10
プロフィール写真	Google Sign-In	10
現在地	Helpers インテント	10
住所等	対話	7
年齢	対話	2
血液型	対話	2
電話番号	対話	1
性別	対話	1

WP2:IoT アプリ動作のコンテキスト検査技術の開発

WP では、代表的な IoT アプリ・プラットフォームとして、Voice Assistant プラットフォームを対象とし、人間の認識と機械の認識に存在するギャップやコンテキストの違いに着目し、そのようなコンテキストの違いによって生じるセキュリティ課題を評価する方法を開発した[11,12]。[12]では、Voice Assistant プラットフォームにおいて、アプリの挙動を、自然言語処理技術を利用して動的解析するシステムを開発した。このシステムは VA の発話内容に対して自然言語処理によるセンテンス解析を行い、コンテキストを把握した上で、適切な応答を生成することを狙いとしている。

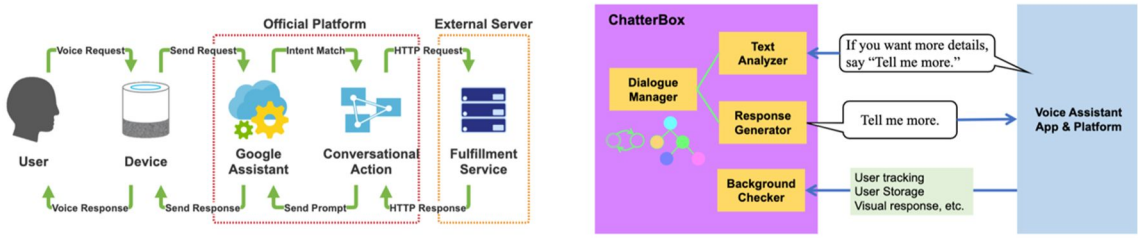
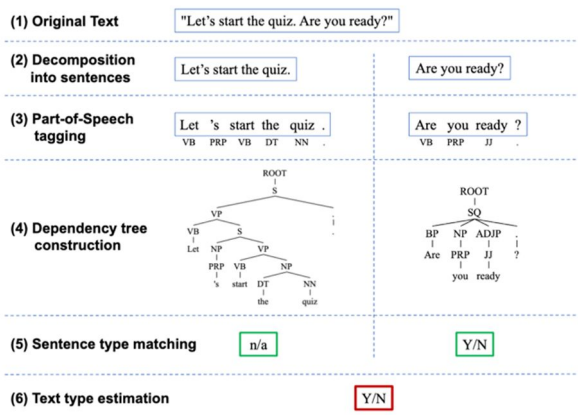


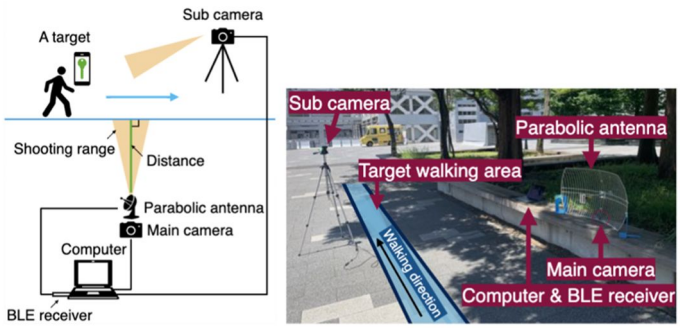
Table 1: Types of text speech generated by VA apps.

Type	Description
Y/N	A question sentence that can be answered with "yes" or "no."
Noun	A question sentence that can be answered with a noun.
Instruction	An instruction sentence that gives the user an example of a request and instructs them to make the request.
Selection	An instruction sentence that instructs the user to select the behavior of the VA application from a set of options.
Multiple	Text that is a mixture of multiple types.



英語版、日本語版の VA アプリを調査した結果，リスクにつながる可能性がある VA アプリが全体の 30-35%存在していることが明らかとなった。リスクを持つ VA アプリの例として，ユーザトラッキングやユーザ情報収集を行うアプリ，VA アプリで固有に保持されるストレージをユーザに対して無断利用するアプリ，明確な理由なくユーザ識別子を保存・利用するアプリが存在することを示した。

[13]では、コロナ接触確認アプリのような、BLE による無線通信を用いた常時通信を行うモバイル OS アプリを対象に、物理空間を移動するユーザが、自身が気付かない内に追跡されてしまうセキュリティリスクを実システムで評価した（下図）。

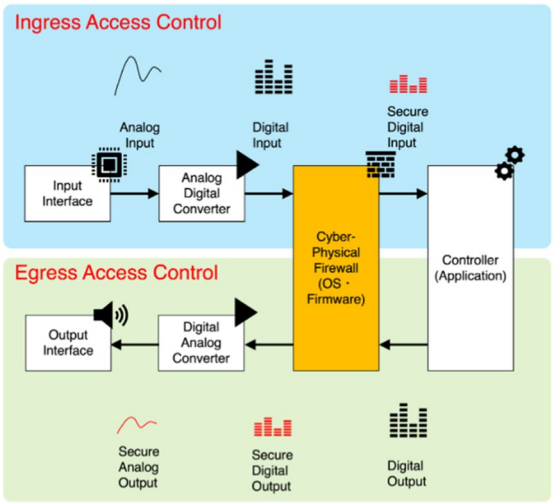


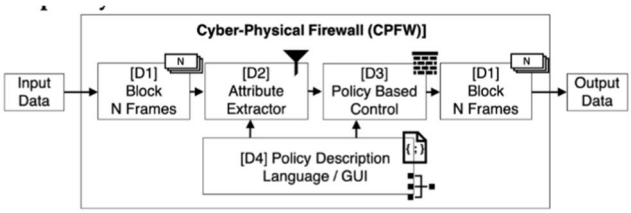
スマートフォン端末を用いたフィールド実験を通じ、攻撃謝が指向性アンテナを用いることにより、高精度にリンキング攻撃を成立させられることを明らかにした。また、様々な BLE 送信電力プロファイルを持つスマートフォンを用いた実験では、比較的弱い送信電力のスマートフォ

ンであってもリンキング攻撃が成功することを示した。さらに、ターゲットと攻撃デバイスの距離が　7 m 離れていても攻撃が成立すること、スマートフォンをポケットに入れたり、かばんにいれたときでも攻撃が成功することを示した。

WP3:IoT プラットフォームにおけるアクセス制御・緊急処理機構の開発

WP3 では、IoT アプリのアクセス制御を実現する技術として、システムコール解析技術[14]、SELinux を用いた適切なポリシ制御管理手法[15]、ならびに IoT デバイスが外部に送信するアナログ信号に対してポリシ制御を実現する機構の開発[16]を実施した。[16] では、IoT に特徴的な、各種センサが計測したアナログ信号が、予め定めたポリシーにマッチしているかを検査し、ポリシー違反とみなされた信号に制御をかける機構（サイバーフィジカル・ファイアウォール）を開発・実装し、その有効性を明らかにした。





[1] Shuichi Ichioka, Estelle Pouget, Takao Mimura, Jun Nakajima, Toshihiro Yamauchi, “Analysis of Android Applications Shared on Twitter Focusing on Accessibility Services,” Journal of Information Processing, Vol.30, 2022 年 9 月. (掲載決定)

[2] 藤田彬，楊志勇，熊佳，鉄穎，楊笛，江澤優太，中山颯，田宮和樹，西田慎，吉岡克成，松本勉，“実攻撃の観測と疑似攻撃の試行に基づくホームネットワークセキュリティの検証,” 情報処理学会論文誌, Vol. 61, No. 3, 2020.

[3] Mitsuhiro HATADA, Tatsuya MORI, “CLAP: Classification of Android PUAs by Similarity of DNS Queries,” IEICE TRANSACTIONS on Information and Systems, Vol. 103-D, No. 2, pp. 265-275, January 2020

[4] Takuya WATANABE, Mitsuaki AKIYAMA, Fumihiro KANEI, Eitaro SHIOJI, Yuta TAKATA, Bo SUN, Yuta ISHII, Toshiki SHIBAHARA, Takeshi YAGI, Tatsuya MORI, “Study on the Vulnerabilities of Free and Paid Mobile Apps Associated with Software Library,” IEICE TRANSACTIONS on Information and Systems, Vol. 103-D, No. 2, pp. 276-291, January 2020

[5] 福田泰平，鄭俊俊，瀧本栄二，齋藤彰一，毛利公一，Android における端末識別情報送信検出のための動的解析システム，情報処理学会論文誌 Vol. 60, No. 2, pp. 2259-2268, 2019 年 12 月

[6] Kanae Yoshida, Hironori Imai, Nana Serizawa, Tatsuya Mori, Akira Kanaoka, “Understanding the Origin of Weak Cryptographic Algorithms Used for Signing Android Apps,” Journal of Information Processing, Vol. 27, pp. 593-602, September 2019

[7] Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, Jakob Bleier, Katsunari Yoshioka, Martina Lindorfer, Michel van Eeten, Carlos H. Ganan, “No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis,” The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), 2022.

[8] Takayuki Sasaki, Akira Fujita, Carlos Hernandez Ganan, Michel van Eeten, Katsunari Yoshioka, Tsutomu Matsumoto, “Exposed Infrastructures: Discovery, Attacks and Remediation of Insecure ICS Remote Management Devices,” Proc. 43rd IEEE Symposium on Security and Privacy (IEEE S&P), 2022

[9] Toshihiro Yamauchi, Ryota Yoshimoto, Takahiro Baba, Katsunari Yoshioka, “Analysis of commands of Telnet logs illegally connected to IoT devices,” 12th International Conference on E-Service and Knowledge Management (ESKM 2021), poster, Proceedings of

2021 10th International Congress on Advanced Applied Informatics (IIAI-AAI 2021), pp.913-915, 2021年7月.
[10] Atsuko Natatsuka, Ryo Iijima, Takuya Watanabe, Mitsuaki Akiyama, Tetsuya Sakai, and Tatsuya Mori,“A First Look at the Privacy Risks of Voice Assistant Apps,” (poster presentation), Proc. of ACM Conference on Computer and Communications Security (CCS 2019)
[11] R. Iijima, S. Minami, Y. Zhou, T. Takehisa, T. Takahashi, Y. Oikawa, and T. Mori, “Audio Hotspot Attack: An Attack on Voice Assistance Systems Using Directional Sound Beams and its Feasibility,” IEEE Transactions on Emerging Topics in Computing PP(99):1-1 · November 2019
[12] Atsuko Natatsuka, Ryo Iijima, Takuya Watanabe, Mitsuaki Akiyama, Tetsuya Sakai, Tatsuya Mori, “Understanding the Behavior Transparency of Voice Assistant Applications Using the ChatterBox Framework,” Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022), October 2022
[13] Kazuki Nomoto , Mitsuaki Akiyama, Masashi Eto, Atsuo Inomata, and Tatsuya Mori, “On the Feasibility of Linking Attack to Google/Apple Exposure Notification Framework,” Proceedings of the 22nd Privacy Enhancing Technologies Symposium (PETS 2022), July 2022
[14] Yuki Kajiwara, Junjun Zheng, and Koichi Mouri, Performance Comparison of Training Datasets for System Call-Based Malware Detection with Thread Information, IEICE Transactions on Information and Systems, Vol. E104-D, No. 12, pp. 2173-2183, December 2021
[15] 齋藤凌也, 山内利宏,”SELinux CILを利用した不要なセキュリティポリシ削減手法,” 情報処理学会論文誌, Vol.61, No.9, pp.1519-1530, 2020年9月.
[16] Ryo Iijima, Tatsuya Takehisa and Tatsuya Mori, “Cyber-Physical Firewall: Monitoring and Controlling the Threats Caused by Malicious Analog Signals,” Proceedings of the 19th ACM International Conference on Computing Frontiers (CF ’22), pp. 296-304, Turin, Piedmont, Italy, May 2022

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　8件／うち国際共著　0件／うちオープンアクセス　6件）

１．著者名 齋藤 凌也, 山内 利宏	４．巻 61
２．論文標題 SELinux CILを利用した不要なセキュリティポリシ削減手法	５．発行年 2020年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1519-1530
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 －

１．著者名 藤田 彬, 楊 志勇, 熊 佳, 鉄 穎, 楊 笛, 江澤優太, 中山 颯, 田宮和樹, 西田 慎, 吉岡克成, 松本 勉	４．巻 61
２．論文標題 実攻撃の観測と疑似攻撃の試行に基づくホームネット ワークセキュリティの検証	５．発行年 2020年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 567-580
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 －

１．著者名 WATANABE Takuya、AKIYAMA Mitsuaki、KANEI Fumihiro、SHIOJI Eitaro、TAKATA Yuta、SUN Bo、ISHII Yuta、SHIBAHARA Toshiki、YAGI Takeshi、MORI Tatsuya	４．巻 E103.D
２．論文標題 Study on the Vulnerabilities of Free and Paid Mobile Apps Associated with Software Library	５．発行年 2020年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 276～291
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019INP0011	査読の有無 無
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 HATADA Mitsuhiro、MORI Tatsuya	４．巻 E103.D
２．論文標題 CLAP: Classification of Android PUAs by Similarity of DNS Queries	５．発行年 2020年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 265～275
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019INP0003	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 齋藤凌也，山内利宏	4．巻 61
2．論文標題 SELinux CILを利用した不要なセキュリティポリシ削減手法	5．発行年 2020年
3．雑誌名 情報処理学会論文誌	6．最初と最後の頁 1519-1530
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 オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Iijima Ryo、Minami Shota、Zhou Yunao、Takehisa Tatsuya、Takahashi Takeshi、Oikawa Yasuhiro、Mori Tatsuya	4．巻 9
2．論文標題 Audio Hotspot Attack: An Attack on Voice Assistance Systems Using Directional Sound Beams and its Feasibility	5．発行年 2021年
3．雑誌名 IEEE Transactions on Emerging Topics in Computing	6．最初と最後の頁 2004～2018
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TETC.2019.2953041	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 Natatsuka Atsuko、Iijima Ryo、Watanabe Takuya、Akiyama Mitsuaki、Sakai Tetsuya、Mori Tatsuya	4．巻 1
2．論文標題 Poster: A First Look at the Privacy Risks of Voice Assistant Apps	5．発行年 2019年
3．雑誌名 Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security	6．最初と最後の頁 2633-2635
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3319535.3363274	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 Yoshida Kanae、Imai Hironori、Serizawa Nana、Mori Tatsuya、Kanaoka Akira	4．巻 27
2．論文標題 Understanding the Origins of Weak Cryptographic Algorithms Used for Signing Android Apps	5．発行年 2019年
3．雑誌名 Journal of Information Processing	6．最初と最後の頁 593～602
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.27.593	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 福田泰平，鄭俊俊，瀧本栄二，齋藤彰一，毛利公一	４．巻 60
２．論文標題 Androidにおける端末識別情報送信検出のための動的解析システム	５．発行年 2019年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 2259-2268
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 オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計29件（うち招待講演　1件／うち国際学会　8件）

１．発表者名 Atsuko Natatsuka, Ryo Iijima, Takuya Watanabe, Mitsuaki Akiyama, Tetsuya Sakai, Tatsuya Mori
２．発表標題 Understanding the Behavior Transparency of Voice Assistant Applications Using the ChatterBox Framework
３．学会等名 International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022)（国際学会）
４．発表年 2022年

１．発表者名 Kazuki Nomoto , Mitsuaki Akiyama, Masashi Eto, Atsuo Inomata, and Tatsuya Mori
２．発表標題 On the Feasibility of Linking Attack to Google/Apple Exposure Notification Framework
３．学会等名 Privacy Enhancing Technologies Symposium (PETS 2022)（国際学会）
４．発表年 2022年

１．発表者名 Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, Jakob Bleier, Katsunari Yoshioka, Martina Lindorfer, Michel van Eeten, Carlos H. Ganan
２．発表標題 No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis
３．学会等名 ACM ASIACCS 2022（国際学会）
４．発表年 2022年

１．発表者名
Takayuki Sasaki, Akira Fujita, Carlos Hernandez Ganan, Michel van Eeten, Katsunari Yoshioka, Tsutomu Matsumoto

２．発表標題
Exposed Infrastructures: Discovery, Attacks and Remediation of Insecure ICS Remote Management Devices

３．学会等名
IEEE Symposium on Security and Privacy (IEEE S&P)（国際学会）

４．発表年
2022年

１．発表者名
Ryo Iijima, Tatsuya Takehisa and Tatsuya Mori

２．発表標題
Cyber-Physical Firewall: Monitoring and Controlling the Threats Caused by Malicious Analog Signals

３．学会等名
ACM International Conference on Computing Frontiers (CF ' 22)（国際学会）

４．発表年
2022年

１．発表者名
Toshihiro Yamauchi, Ryota Yoshimoto, Takahiro Baba, Katsunari Yoshioka

２．発表標題
Analysis of commands of Telnet logs illegally connected to IoT devices

３．学会等名
International Conference on E-Service and Knowledge Management (ESKM 2021)（国際学会）

４．発表年
2021年

１．発表者名
Atsuko Natatsuka, Ryo Iijima, Takuya Watanabe, Mitsuaki Akiyama, Tetsuya Sakai, and Tatsuya Mori

２．発表標題
A First Look at the Privacy Risks of Voice Assistant Apps

３．学会等名
ACM Conference on Computer and Communications Security (CCS 2019)（国際学会）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

プロジェクト業績リスト（完全版） - https://nsl.cs.waseda.ac.jp/iotb/ Survey of cryptographic APIs in Android (Kanaoka Lab) - https://github.com/kanaoka-laboratory/CryptAPISurvey_inAndroidA IP Address Hard Coding Survey (Kanaoka Lab) - https://github.com/kanaoka-laboratory/IPaddrHardCodingSurvey

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	金岡　晃 (Akira Kanaoka) (00455924)	東邦大学・理学部・准教授 (32661)	
研究分担者	吉岡　克成 (Katsunari Yoshioka) (60415841)	横浜国立大学・大学院環境情報研究院・准教授 (12701)	
研究分担者	山内　利宏 (Toshihiro Yamauchi) (80359942)	岡山大学・自然科学学域・教授 (15301)	
研究分担者	毛利　公一 (Koichi Mouri) (90313296)	立命館大学・情報理工学部・教授 (34315)	

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