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　６ 年　 ４ 月 １９ 日現在

機関番号：１５５０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2023
課題番号：１９Ｋ１１９６５

研究課題名（和文）IoTマルウェアのサイバー攻撃を防ぐ善玉ボットネットシステムの開発

研究課題名（英文）Development of a White Hat Botnet System for Defending Against IoT Malware Cyberattacks

研究代表者
山口　真悟（Yamaguchi, Shingo）

山口大学・大学院創成科学研究科・教授

研究者番号：００２９４６５３

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：IoTマルウェアのサイバー攻撃に対抗する新たなシステム「ボットネット防衛システム（BDS）」を開発した。BDSは、自ら構築したボットネットによって悪玉ボットネットに対抗するという独自のアプローチを採っており、「毒をもって毒を制す」の原則を体現する。具体的には、まずネットワークを継続的に監視することによって悪玉ボットネットを検出し、その特性に基づいて効果的な駆除戦略を策定する。そして善玉ワームをネットワークに展開することによって善玉ボットネットを構築し、それを指揮統制することによって悪玉ボットネットを駆除する。ローカルな環境での実装と検証により、BDSの有効性を実証した。

研究成果の学術的意義や社会的意義
本研究はボットネットの数理モデルに基づく理論研究とボットネット防衛システムの開発を通して、ボットネット対策における学術研究の進展に大きく貢献するものである。従来の研究では解明できなかったボットネットの複雑な挙動を、独自開発のシミュレータを用いて定量的に解析することに成功した。これは、より効果的な防衛技術を開発するための学術的基盤を築く画期的な成果である。また悪玉ボットネットと戦う善玉ボットネット、その戦いを指揮統制するシステムのアーキテクチャやコンポーネント、戦略等を明らかにし、プロトタイプを実装した。これらは新たな技術開発のインスピレーションを与え、その構築基盤をなすものとして期待される。

研究成果の概要（英文）：This research proposed and implemented a new system to counter IoT malware cyber attacks: the Botnet Defense System (BDS). The BDS continuously monitors the network and detects malicious botnets. Once detecting a botnet, it formulates an effective disinfection strategy based on its characteristics. It then deploys a white hat worm into the network and builds a white hat botnet. It then commands and controlls the white hat botnet to exterminate the malicious botnet. We implementing BDS in a local IoT network and demonstrated its effectiveness. Furthermore, the research results were made publicly available to the world to share findings.

研究分野：システム数理科学

キーワード：ボットネット　セキュリティ　マルウェア　ワーム　マルチエージェント　ペトリネット　IoT　Mirai

様　式　Ｃ－１９，Ｆ－１９－１，Ｚ－１９（共通）

１．研究開始当初の背景

2016 年 9 月，IoT 機器を踏み台にした大規模な分散型サービス妨害（Distributed Denial of Service; DDoS）攻撃が発生した．この攻撃は新種のマルウェアである Mirai ボットネットが引き起こしたとされる．IoT 機器は PC に比べて数が多く，セキュリティが脆弱であることが多い．それゆえ，その攻撃は大規模で破壊的になる傾向があり，その対策は喫緊の課題である．

2016 年 11 月，JPCERT コーディネーションセンタはボットネットによる DDoS 攻撃の脅威に対する対策方法を公開した．ボットはメモリにのみ存在するため，IoT 機器を再起動することで削除できる．2017 年 11 月，報告者らはボットネットの感染現象を表す数理モデルを構築し，再起動による対策の効果をシミュレーションにより定量的に評価した．その結果，再起動による対策は再感染の恐れがあり，根本的な解決にはソフトウェアの設定変更や更新が必要であることが分かった．一方，総務省の平成 30 年版 情報通信白書によると，2017 年時点で IoT 機器は 275 億個あり，2020 年には 400 億個を超えると予測されている．IoT 機器の数は爆発的に増加していることから，人海戦術での対応には限界がある．

２．研究の目的

本研究の目的は，攻撃者がサイバー攻撃にボットネットを使うやり方に倣って，防御者がサイバー攻撃を防御するために善玉ボットネットを使えるようにして防御能力を飛躍的に向上させることである．

３．研究の方法

本研究は，以下のロードマップに従って進めた（図 1 を参照）．

① ボットネットの数理モデルの開発
② ボットネット脅威の定量的な分析
③ 善玉ボットネットの設計
④ ボットネット防衛システムの開発
⑤ 善玉ボットネットの構築・運用法の開発
⑥ 実装とチューニング
⑦ 成果の公開

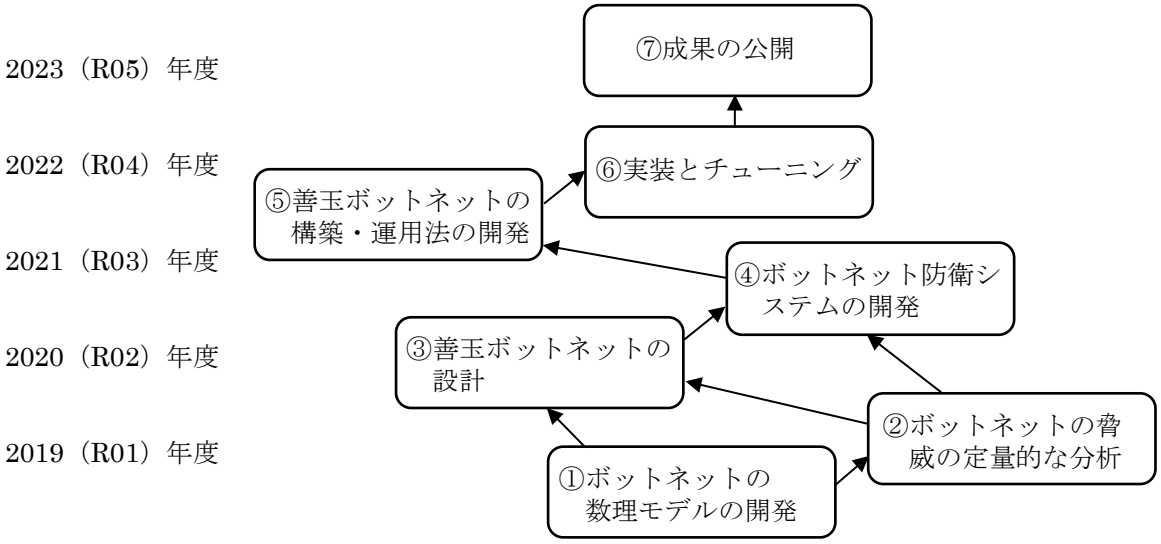


図１：研究ロードマップ

４．研究成果

① ボットネットの数理モデルの開発

悪玉ボットネットと善玉ボットネットの戦いをマルチエージェントシステムとみなし，それをエージェント指向ペトリネット Petri Nets in a Petri Net （PN²）で記述した数理モデルを作成した．

② ボットネット脅威の定量的な分析

PN² モデルのトークンゲームによって，ボットネットの感染拡大やボットネット同士の戦いをシミュレーションし，ボットネットの脅威を定量的に分析した．

③ 善玉ボットネットの設計

②の分析で浮かび上がった課題を解決すべく，善玉ワームの機能として以下を特定した．

・寿命：善玉ワームが存在できる期間．ワームは寿命が尽きると自滅する．ワームがいなくなっても感染した機器はボットのままである．機器が再起動するまでは免疫効果を発揮する．

・二次感染力：悪玉ワームに感染している機器に対して，善玉ワームが重ねて感染できる確率．善玉ワームはその機器から悪玉ワームと悪玉ボットを駆除する．

さらにボットネットとしての組織力を強化すべく，善玉ボットの機能として以下を特定した．

・偵察機能：インターネットはオープンシステムであるため，すべてのノードを観測したり，制御したりできるわけではない．それらのノードに対して，ボットが間接的に観測したり，制御したりする．あるノード n にある善玉ボット w は，n に隣接しているノード n′ にボットがあるかどうかを調べることができる．

・プロキシ機能：Mirai の亜種の一つである OMG のように，善玉ボットはメッセージを中継できる．n′ に善玉ボット w′ がある場合，w は w′ とメッセージを交換できる．これを w は w′ とリンクしているという．なおリンクは推移的な関係である．

④ ボットネット防衛システムの開発

ボットネット防衛システム（Botnet Defense System; BDS）のアーキテクチャを設計し，必要な機能を開発した．BDS のコンセプトは「毒を以て毒を制す（Fight Fire with Fire)」である．すなわち，善玉ボットネットを使って悪玉ボットネットを駆除する． BDS はコンポーネントベースのアーキテクチャを採用している． 図２にシステム構成を示す．

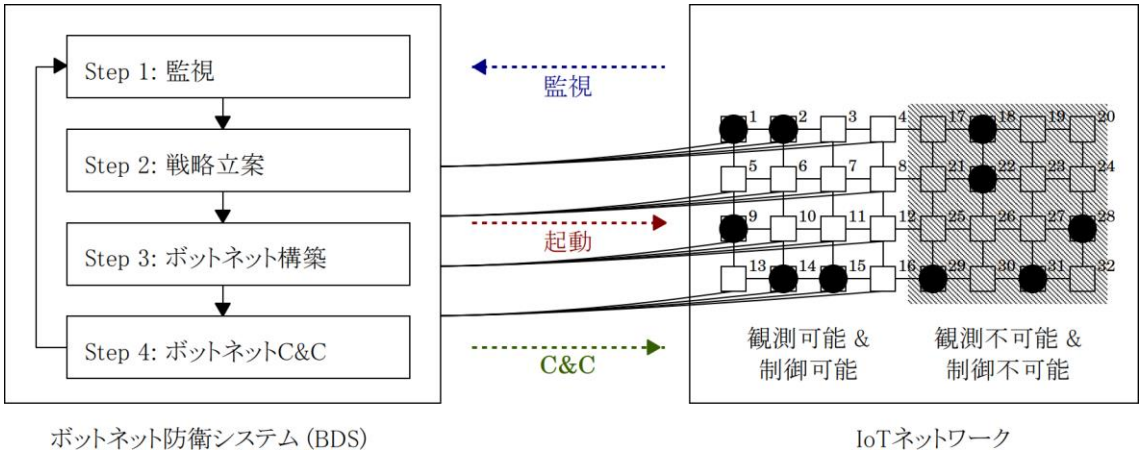
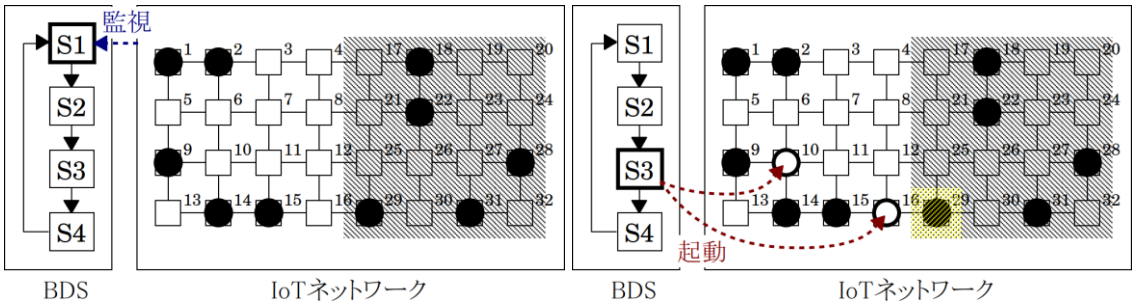
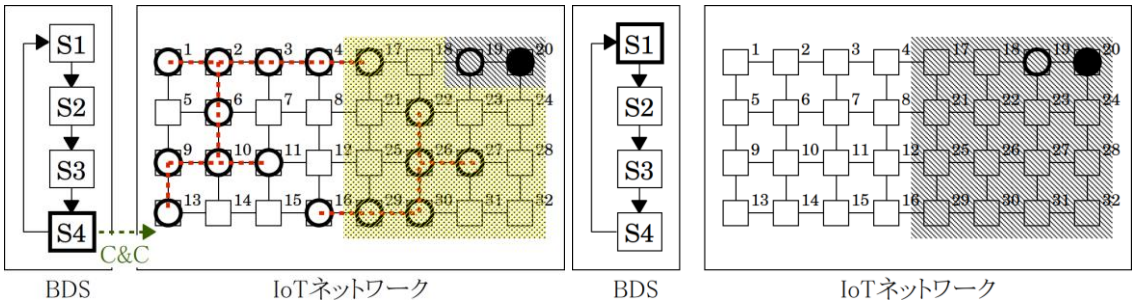


図２：BDS のシステム構成



(a) 初期状態．BDS は観測可能な 5 つのノードに悪玉ボット（●）を発見することによって悪玉ボットネットを検出した．

(b) 善玉ボットネット構築時の状態．BDS は善玉ボットネットを構築するために，2 つの善玉ワーム(○)を送信した．



(c) 善玉ボットネットが拡散し，悪玉ボットネットを撃退した状態．BDS は撤退を命じた．

(d) 撤退命令を受けた善玉ボットがすべて自滅した後の状態．制御不可能な領域に 2 つのボット（悪玉ボット 1 つと善玉ボット 1 つ）が残った．

図 3 ：BDS と IoT ネットワークの状態遷移

BDS の仕組みを図 3 に示す状態遷移の例を用いて説明しよう．図 3 (a)は初期状態を示している．IoT ネットワークを構成する 32 個のノードのうち 10 個が悪玉ボットになっている．ステップ 1 として，BDS は IoT ネットワークを監視する．その結果，観測可能な 5 個のノード n1，n2，n9，n14，n15 に悪玉ボットがあることを発見し，IoT ネットワークが悪玉ボットネットに感染していることを検知した．しかし，10 個の悪玉ボットのうち残り 5 個は観測不可能なノード n18，n22，n28，n29，n31 にあるため，BDS はそれらを発見できていない．その後，ステップ 2 として，BDS は悪玉ボットネットを撃退するための戦略を立てる．この例では，BDS は悪玉ボットネットを撃退するのに十分な能力を有する善玉ワームを保有していたため，少数精鋭戦略を採用した．次に，ステップ 3 として，BDS はその戦略に基づいて善玉ワームを起動し，善玉ボットネットを構築する．図 3 (b)は善玉ボットネット構築時の状態を示している．BDS は少数精鋭戦略に従って，善玉ワームを 2 つの観測可能なノード n10，n16 へ送り込み，それらの機器に感染させることによって，2 つのボットからなる善玉ボットネットを構築した．BDS は観測不可能なノード n29 を直接的に観測することはできないが，観測可能なノード n16 の善玉ボットを通して間接的に観測することができる．BDS が間接的に観測可能なノードは黄色で網掛けしている．善玉ボットネットは悪玉ボットネットを撃退しながら，自律的にネットワーク全体へ広がっていく．図 3 (c)は善玉ボットネットがノード n20 にある 1 つを除くほぼ全ての悪玉ボットを駆除した状態を示している．その後，ステップ 4 として，BDS は善玉ボットネットを指揮統制する．この例では，BDS は撃退が十分であると判断して撤退戦略を採用し，善玉ボットネットに撤退を命令した．この撤退命令はリンクで接続されている全ての善玉ボットに伝達

される．リンクは赤い破線で図示されている．図 3 (d)は撤退命令を受信した全ての善玉ボットが自滅した後の状態を示している．1 つの善玉ボットと 1 つの悪玉ボットが，それぞれ観測不能なノード n19 と n20 に残った．

⑤ 善玉ボットネットの構築・運用法の開発

BDS は悪玉ボットネットを撃退するために，悪玉ボットネットより優勢となるように善玉ボットネットを構築し，運用しなければならない．一方，善玉ボットネットは，いわゆる両刃の剣である．悪玉ボットネットから IoT ネットワークを守るが，システムのリソースを浪費することになる．そのため，BDS は必要最小限の数の善玉ボットネットを使用し，悪玉ボットネットを駆除した後には善玉ボットはネットワークに残るべきではない．

自律的に動く善玉ワームを束ねて組織的に運用するには，大局的な視点から見た戦略が重要となる．BDS の戦略は大きく 2 つに分けられる．

・構築戦略：善玉ワームを送り込み，そのボットネットを構築する方法を定める．
　具体的な構築戦略として，総力（All-Out）戦略，少数精鋭（Few-Elite）戦略，環境適応型（Environment-Adaptive）戦略を提案した．
・運用戦略：構築した善玉ボットネットを指揮統制する方法を定める．
　具体的な運用戦略として，撤収（Pull-Out）戦略を提案した．

⑥ 実装とチューニング

善玉ボットネットと悪玉ボットネットをローカルな IoT ネットワークに実装した. IoT 機器の OS にはルーターなどで広く使われている OpenWrt を採用した．善玉ボットネットと悪玉ボットネットの実装には Mirai のソースコードを直接利用した．善玉ボットの実装には，二次感染力と寿命の機能を実現する必要がある．二次感染力を実現するために，感染に使うポートを開いたままにし，善玉ワームの感染対象がすでに悪玉ボットになっている場合は，そのプロセスを停止するようにした. また寿命を実現するため, 感染してから寿命が過ぎると自滅するようにした. 本実装では，Mirai のソースコードを流用することにより，開発にかかる時間や手間を削減すると共に，ボットネットの動作を忠実に再現することができた．

本実装を 65,536 個の IP アドレスからなるローカルネットワークに適用し，その感染状況を観察する実験を行った．その結果，善玉ボットネットが十分な能力を有していれば，5 分程度で悪玉ボットネットを駆除できることを確認した．悪玉ボットネットを駆除するには，善玉ワームの感染力と寿命が重要である．本実験では毎回感染を試みる IP アドレスの数を 100 以上，寿命を 180 秒以上とすることが必要であることが分かった．

⑦ 成果の公開

研究で得られた成果を世界に向けて公開するためウェブサイトを構築し，知見を共有した．

＜ウェブサイト＞

Botnet Defense System, https://ds0n.cc.yamaguchi-u.ac.jp/~shingo/BDS/

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　7件／うち国際共著　0件／うちオープンアクセス　5件）

１．著者名 Pan Xiangnan、Yamaguchi Shingo	４．巻 22
２．論文標題 Machine Learning White-Hat Worm Launcher for Tactical Response by Zoning in Botnet Defense System	５．発行年 2022年
３．雑誌名 Sensors	６．最初と最後の頁 4666～4666
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/s22134666	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 Yamaguchi Shingo	４．巻 22
２．論文標題 Botnet Defense System: Observability, Controllability, and Basic Command and Control Strategy	５．発行年 2022年
３．雑誌名 Sensors	６．最初と最後の頁 9423～9423
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/s22239423	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 Bin Ahmadon Mohd Anuaruddin、Yamaguchi Shingo	４．巻 23
２．論文標題 Diffusion of White-Hat Botnet Using Lifespan with Controllable Ripple Effect for Malware Removal in IoT Networks	５．発行年 2023年
３．雑誌名 Sensors	６．最初と最後の頁 1018～1018
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/s23021018	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 Xiangnan Pan, Shingo Yamaguchi, Taku Kageyama, Mohd Hafizuddin Bin Kamilin	４．巻 14(1)
２．論文標題 Machine-Learning-Based White-Hat Worm Launcher in Botnet Defense	５．発行年 2022年
３．雑誌名 International Journal of Software Science and Computational Intelligence	６．最初と最後の頁 1~14
掲載論文のDOI（デジタルオブジェクト識別子） 10.4018/IJSSCI.291713	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 Yamaguchi Shingo	4．巻 11
2．論文標題 Botnet Defense System: Concept, Design, and Basic Strategy	5．発行年 2020年
3．雑誌名 Information	6．最初と最後の頁 516～516
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/info11110516	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 Shingo Yamaguchi, Hiroaki Tanaka, Mohd Anuaruddin Bin Ahmadon	4．巻 -
2．論文標題 Modeling and Evaluation of Mitigation Methods against IoT Malware Mirai with Agent-Oriented Petri Net PN2	5．発行年 2019年
3．雑誌名 International Journal of Internet of Things and Cyber-Assurance	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1504/IJITCA.2019.10021463	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 Shingo Yamaguchi	4．巻 20(2)
2．論文標題 White-Hat Worm to Fight Malware and Its Evaluation by Agent-Oriented Petri Nets	5．発行年 2020年
3．雑誌名 Sensors	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/s20020556	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34件（うち招待講演　2件／うち国際学会　29件）

1．発表者名 Yuji Katsura, Shingo Yamaguchi
2．発表標題 On Countermeasure Against Repeatedly Occurring Botnets by Collective Reboot
3．学会等名 ITC-CSCC 2023（国際学会）
4．発表年 2023年

１．発表者名
Shingo Yamaguchi, Ryutaro Matsumoto

２．発表標題
Smallest Botnet Firewall Building Problem and a Girvan-Newman Algorithm-Based Heuristic Solution

３．学会等名
IEEE ICCE-TW 2023（国際学会）

４．発表年
2023年

１．発表者名
Ryo Yamashita, Shingo Yamaguchi

２．発表標題
Estimating the Infection Spread Rate of Malicious Botnets Using Reconnaissance Worms in Botnet Defense System

３．学会等名
IEEE ICCE-Asia 2023（国際学会）

４．発表年
2023年

１．発表者名
Shingo Yamaguchi

２．発表標題
Mesa-Based Simulator of Botnet Defense System and Impact Evaluation of Botnet Infection Rates

３．学会等名
ICEIC 2024（国際学会）

４．発表年
2024年

１．発表者名
Aoi Fukushima, Yudai Yamamoto, Shingo Yamaguchi

２．発表標題
Implementation of Infection Environment for White-hat Worm and Malicious Botnet Using Mirai Source Code

３．学会等名
ICIET 2024（国際学会）

４．発表年
2024年

１．発表者名
Ryutaro Matsumoto, Shingo Yamaguchi

２．発表標題
On Building a Firewall with White Hat Bots in the Neighborhood of Malicious Bots in Large-Scale Networks

３．学会等名
ETTIS 2024（国際学会）

４．発表年
2024年

１．発表者名
Shingo Yamaguchi, Daisuke Makihara

２．発表標題
On Resident Strategy for White-Hat Botnet in Botnet Defense System

３．学会等名
IEEE ICCE-TW 2022（国際学会）

４．発表年
2022年

１．発表者名
Yudai Yamamoto, Shingo Yamaguchi

２．発表標題
A Method to Prevent Known Attacks and Their Variants by Combining Honeypots and IPS

３．学会等名
IEEE GCCE 2022（国際学会）

４．発表年
2022年

１．発表者名
Kazuki Ohsaki, Shingo Yamaguchi

２．発表標題
On Directional Spread of White-hat Botnet by Heterogeneous Use in Botnet Defence System

３．学会等名
IEEE ICCE-Asia 2022（国際学会）

４．発表年
2022年

１．発表者名
Gaku Tatebatake, Shingo Yamaguchi

２．発表標題
Mathematical Modeling and Analysis of the Dictionary Attack Mechanism in IoT Malware Mirai

３．学会等名
IEEE ICCE-Asia 2022（国際学会）

４．発表年
2022年

１．発表者名
Ryutaro Matsumoto, Shingo Yamaguchi

２．発表標題
On Building Firewall with White-Hat Bots to Prevent the Infection Spread of Malicious Botnets

３．学会等名
ICIET 2023（国際学会）

４．発表年
2023年

１．発表者名
松本 隆太郎, 山口 真悟

２．発表標題
善玉ボットによる悪玉ボットネットの感染拡大防止について

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2022年

１．発表者名
桂 雄治, 山口 真悟

２．発表標題
領域リブートによるボットネット対策について

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2023年

１．発表者名
山下 諒・山口 真悟

２．発表標題
Botnet Defense Systemにおける善玉ワームによる悪玉ボットネットの探索について

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2023年

１．発表者名
Yamaguchi Shingo

２．発表標題
Research and Development of Botnet Defense System

３．学会等名
HCII 2022（国際学会）

４．発表年
2022年

１．発表者名
Shingo Yamaguchi

２．発表標題
On Application of Botnet Defense System to IoT Systems Including Private Networks

３．学会等名
IEEE ICCE-TW 2021（国際学会）

４．発表年
2021年

１．発表者名
山口 真悟

２．発表標題
ボットネット防衛システムの研究開発

３．学会等名
第34回回路とシステムワークショップ（招待講演）

４．発表年
2021年

１．発表者名
Xiangnan Pan, Shingo Yamaguchi, Taku Kageyama

２．発表標題
Machine-Learning-Based White-Hat Worm Launcher Adaptable to Large-Scale IoT Network

３．学会等名
IEEE GCCE 2021（国際学会）

４．発表年
2021年

１．発表者名
Daisuke Makihara, Shingo Yamaguchi

２．発表標題
A Proposal of Patrol Function by White-Hat Worm in Botnet Defense System

３．学会等名
IEEE ICCE-Asia 2021（国際学会）

４．発表年
2021年

１．発表者名
Kazuki Ohsaki, Shingo Yamaguchi

２．発表標題
A Proposal of Heterogeneous White-Hat Botnet in Botnet Defense System

３．学会等名
IEEE ICCE-Asia 2021（国際学会）

４．発表年
2021年

１．発表者名
Mohd Anuaruddin Bin Ahmadon, Shingo Yamaguchi

２．発表標題
Evaluation on White-Hat Worm Diffusion Method Based on the Evolution of Its Lifespan in Wireless Networks

３．学会等名
IEEE ICCE 2022（国際学会）

４．発表年
2022年

１．発表者名
Xiangnan Pan, Shingo Yamaguchi

２．発表標題
A DBSCAN-based White-Hat Worm Launcher for Botnet Defense System

３．学会等名
IEEE LifeTech 2022（国際学会）

４．発表年
2022年

１．発表者名
Taku Kageyama, Shingo Yamaguchi

２．発表標題
On Tactics to Deploy White-Hat Worms in Botnet Defense System

３．学会等名
IEEE GCCE 2021（国際学会）

４．発表年
2021年

１．発表者名
Shingo Yamaguchi

２．発表標題
Botnet Defense System and Its Basic Strategy Against Malicious Botnet

３．学会等名
IEEE ICCE-TW 2020（国際学会）

４．発表年
2020年

１．発表者名
Shingo Yamaguchi

２．発表標題
Influence Analysis of Network Density on White-Hat Worm and Basic Strategy for Botnet Defense System

３．学会等名
ECTI-CON 2020（国際学会）

４．発表年
2020年

１．発表者名
Mohd Hafizuddin Bin Kamilin, Shingo Yamaguchi

２．発表標題
White-Hat Worm Launcher Based on Deep Learning in Botnet Defense System

３．学会等名
IEEE ICCE-Asia 2020（国際学会）

４．発表年
2020年

１．発表者名
Shingo Yamaguchi

２．発表標題
A Basic Command and Control Strategy in Botnet Defense System

３．学会等名
IEEE ICCE 2021（国際学会）

４．発表年
2021年

１．発表者名
Megha Quamara, B. B. Gupta, Shingo Yamaguchi

２．発表標題
An End-To-End Security Framework for Smart Healthcare Information Sharing Against Botnet-Based Cyber-Attacks

３．学会等名
IEEE ICCE 2021（国際学会）

４．発表年
2021年

１．発表者名
Amrita Dahiya, B.B. Gupta, Shingo Yamaguchi, Kostas Psannis

２．発表標題
Mitigating Botnet Based DDoS Attacks by Selecting Incentivized Cooperating ISPs for Risk Transfer

３．学会等名
IEEE ICCE 2021（国際学会）

４．発表年
2021年

１．発表者名
Shingo Yamaguchi

２．発表標題
Botnet Defense System: Concept and Basic Strategy

３．学会等名
IEEE ICCE 2020（国際学会）

４．発表年
2020年

１．発表者名
Shingo Yamaguchi

２．発表標題
Formal modeling and analysis of battle between IoT malware Mirai and IoT worm Hajime

３．学会等名
ECTI-CON 2019（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Shingo Yamaguchi

２．発表標題
Modeling and Evaluation of IoT Worm with Lifespan and Secondary Infectivity by Agent-Oriented Petri Net PN2

３．学会等名
IEEE ICCE-TW 2019（国際学会）

４．発表年
2019年

１．発表者名
Hiroaki Tanaka, Shingo Yamaguchi, Monika Mikami

２．発表標題
Quantitative Evaluation of Hajime with Secondary Infectivity in Response to Mirai's Infection Situation

３．学会等名
IEEE GCCE 2019（国際学会）

４．発表年
2019年

１．発表者名 山口 真悟
２．発表標題 ボットネット防衛システムの提案と基本戦略について
３．学会等名 電子情報通信学会システム数理と応用研究会
４．発表年 2020年

〔図書〕　計4件

１．著者名 Shingo Yamaguchi	４．発行年 2024年
２．出版社 Springer	５．総ページ数 200
３．書名 Malware - Handbook of Prevention and Detection	

１．著者名 Shingo Yamaguchi, Brij Gupta	４．発行年 2021年
２．出版社 IGI Global	５．総ページ数 304
３．書名 Advances in Malware and Data-Driven Network Security	

１．著者名 Shingo Yamaguchi	４．発行年 2020年
２．出版社 Vide Leaf	５．総ページ数 18
３．書名 Prime Archives in Sensors	

1．著者名 Shingo Yamaguchi, Brij Gupta	4．発行年 2020年
2．出版社 Information Science Reference	5．総ページ数 16
3．書名 Security, Privacy, and Forensics Issues in Big Data	

〔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	ＡＮＵＡＲＵＤＤＩＮ　ＭＯＨＤ (Bin Ahmadon Mohd Anuaruddin) (80804492)	山口大学・大学院創成科学研究科・助教 (15501)	

	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
研究協力者	Ｇｕｐｔａ　Ｂｒｉｊ (Gupta Brij)	アジア大学・教授	インド国立クルクシェトラ工科大学から台湾アジア大学へ異動

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			
インド	インド国立クルクシェトラ工科大学			
台湾	アジア大学			