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　 ５ 月　 ２ 日現在

機関番号：１２６０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2021
課題番号：１８Ｋ１１２５７

研究課題名（和文）設備ネットワークのセキュリティ・脆弱運用対策の研究

研究課題名（英文）A study on security and vulnerability management of facility networks

研究代表者
落合　秀也（Ochiai, Hideya）

東京大学・大学院情報理工学系研究科・准教授

研究者番号：１０６１５６５２

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デバイスが接続されるネットワークのセキュリティを向上させるネットワーク機器向けの通信学習＆制御アルゴリズムを開発した。また新たな手法によるLAN内部の異常検知装置も開発し、マルウェア感染が深刻な東南アジア地域に50台規模で展開して、IoTを取り巻くサイバー攻撃の実態を調査した。その結果として、LAN内不審活動の可視化や体系化に成功した。IoTシステムの末端となる設備ネットワークの物理的セキュリティを向上させるための新たな異常検知システムの開発も行った。

研究成果の学術的意義や社会的意義
ネットワーク・セキュリティの研究は、これまでネットワークの上流での異常検知や管理が一般的であったが、本研究はIoTを取り巻く環境すなわちLAN内部の通信管理や異常検知に主眼を置いている。また本手法で確立した装置をマルウェア感染が深刻な地域に実際に多数展開し、そこからLAN内不審活動の可視化・体系化を行ったことは、これまでにない学術的な意義を持つ。

研究成果の概要（英文）：We developed an algorithm for learning and controlling communication flows for improving the security of IoT device connected networks. We also developed anomaly detection devices for local area networks (LANs) based on our own new method, and deployed 50 devices around the regions of South East Asia where are suffuring from severe malware encounter rates. We could successfully make a taxonomy of suspicious LAN internal device-to-device communications and visualization of them with the collected events. We further developed another anomaly detection scheme for improving the physical security of facility networks where are connected at the edges of IoT systems.

研究分野：IoTセキュリティ

キーワード：IoT　セキュリティ　設備ネットワーク

様　式　Ｃ－１９，Ｆ－１９－１，Ｚ－１９（共通）

１．研究開始当初の背景

IoT 時代の到来とともに，さまざまな物理的な社会インフラがネットワーク接続され，IT により管理されるようになってきていた．一方，IoT 端末（本研究では設備管理ネットワークにおける空調，照明，電力などの監視制御装置を想定する）へのサイバー攻撃は実世界を停止させうる重大な脅威となっていた．フィッシングメールなどを使い，スパイウェア・ウイルスを時間かけて徐々に浸透させていき，時期を見計らって一気に攻撃を活性化させることで，電力設備，交通設備，ビル設備，工場設備などに対して同時多発的に攻撃を仕掛けることが原理的に可能になっている．IoT 端末のサイバー・セキュリティ対策は，一般のパーソナル・コンピュータやスマートフォン(以降，Human 端末と呼ぶ)と比べ不十分な状態にある．原因としては，IoT 端末は，Human 端末と比べて，(1) 運用管理を行き届かせることが現実的に困難であり脆弱性が放置されるためであったり，(2) 専用のファームウェアで稼働するものがあり，そのセキュリティアップデートに困難を伴ったり，(3) 大量に送り付けられたパケットを処理しきれない，などがある．

２．研究の目的

「IoT 端末には脆弱性が伴うもの」という大前提で，IoT 端末をネットワーク側で保護するプラットフォームの開発を研究の目的とした．ネットワーク側といっても，昨今のサイバー空間上の脅威を考えれば，LAN 内部へのマルウェア侵入と，そこからの IoT 端末への攻撃が十分に考えられる．そこで，従来型のネットワーク上流で LAN 内の端末を保護したり，マルウェア侵入検知をするのではなく，ネットワークの末端を収納するスイッチ（すなわち LAN の内部で）でトラフィックを IoT 端末のトラフィックを学習して，それ以外の通信を制限したりすることで IoT 端末を悪性トラフィックから保護する方針を取った．また，LAN 内に監視装置を設置することで，LAN 内で行われる不審な活動を検知する仕組みを構築することとした．そして，この観測装置をマルウェア感染が深刻な東南アジア地域に広く展開し，実際的な不審活動を分析するとともに，どのように IoT 端末を保護できるかを実際の環境下で検証することとした．

３．研究の方法

スイッチによる IoT 端末の保護は，実際の IoT 機器が行う通信をスイッチのブリッジで取得し，そのトラフィックを学習して，スイッチによるアクセス制御ポリシーを生成させることで行った．IoT 機器は一般に Human 端末と比べて同じ通信を何度も繰り返す傾向にあり，また，新たな相手との通信は行わないのが通常である．そのため，正常状態下でモニタリングした通りの通信を許可すれば IoT システムとしてはそのまま動き続けるが，異常な通信はブロックすることができる．これが狙いである．

監視装置による不審活動の検知に関する研究は，まず，図 1 のように小型コンピュータにトラフィック監視機能を実装した．この装置を LAN に接続するだけで，図 2 のようにその LAN 内の通信状況を取得することができる．この可視化したものは ARP トラフィックに関するものであるが，TCP/UDP などの他のプロトコルに関するパケットも取得することができる．このようにして開発した装置をマルウェア感染が深刻な東南アジア地域に広く展開することで，多様な不審活動のサンプルを捉え，不審活動の体系化や異常検知に関する研究ができる．

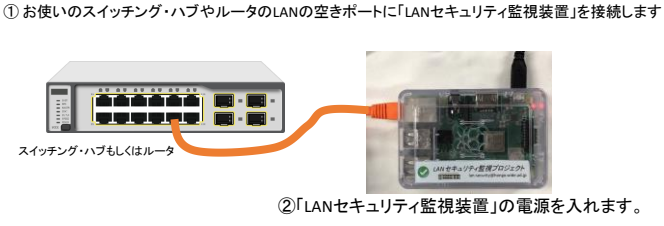

図 1：LAN セキュリティ監視装置

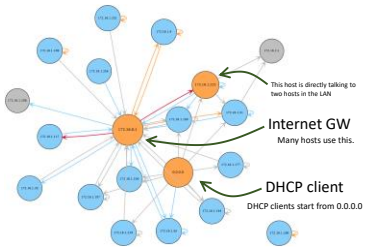

図 2：LAN 内通信状況の可視化

４．研究成果

スイッチによる IoT 端末の保護では INSTRUCT と呼ぶ K-means 法による IoT トラフィックの分別学習をする仕組みを開発した(図 3)．IoT 端末はデータサーバの他に，DNS や NTP，そして DHCP サーバなどとも通信を行うが（背景通信と我々は呼ぶ），INSTRUCT の仕組みでは，そのような仕様書には明示化されていない背景通信まで含めて自動的に学習することがで

きる．そして，そこで学んだパターンをアクセス制御リストにして，スイッチに設定し，LAN 内で突如発生した攻撃トラフィックから IoT 端末を保護できることを確認した．

LAN トラフィック監視装置については 2018 年に開発を行い，2019 年の一年間に東南アジア地域の大学組織の協力を得て，図 4 に示すように多数の設置を完了させた．この観測網により集められるデータは 1 日当たり 1GByte 程度に上り，その中には，LAN 内をスキャンしたり，ハニーポットにマルウェアを投入したり，する様子が日々観測された．このようなリアルな LAN 内部の不審活動を大量に捉えた学術観測網は他に類を見ない．かなり貴重な観測が行われたと考えている．

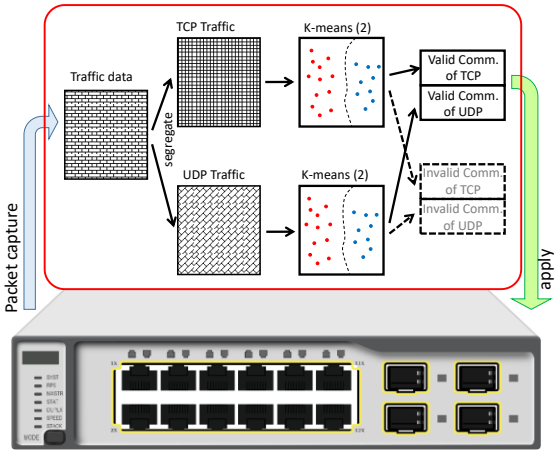

図 3：IoT トラフィックの学習・制御ポリシーの生成（INSTRUCT 法）

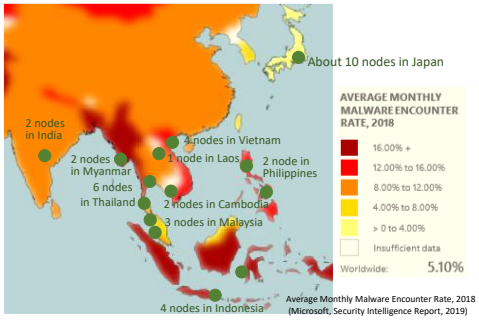

図 4：東南アジア地域に展開した LAN 監視装置

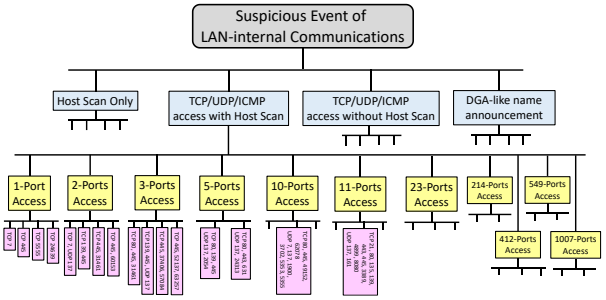

図 5：LAN 内の不審活動の Taxonomy

LAN トラフィック観測網を使って，数多くの異常検知に関する研究が行われた．特に，機械学習と協調学習をセットにした Segmented Federated Learning という仕組みでは，複数の背景が異なるネットワークで一つの学習を行うことを可能にした．ネットワークは規模・端末数・利用方法などが異なり，あるドメインで学習したモデルをそのまま他に適用することは難しい問題であったが，新たに提案した協調学習により，この問題を解決した．

また図 5 に示すように，LAN 内不審活動の体系化を進めることができた．これまで不審な通信はポート番号別に区別することが一般的とされてきたが，LAN 内に限っては，複数のポートに対してほぼ同時にアクセスするケースが多く見受けられ，この通信パターンは，その端末が感染しているマルウェアを特徴づけるものとして利用できる可能性を示している．

その後，LAN セキュリティ監視装置を OT ネットワークに拡張し，太陽光発電所や工場などの設備ネットワークに導入できる形に改良を行っている(図 6)．実際の太陽光発電所に設置し，OT ネットワークに特化した監視アルゴリズム開発を今まさに行っているところである．

図 6：LAN セキュリティ監視装置の OT Extension

５．主な発表論文等

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

１．著者名 Yuwei Sun, Hiroshi Esaki, Hideya Ochiai	４．巻 Vol.2
２．論文標題 Adaptive Intrusion Detection in the Networking of Large-Scale LANs With Segmented Federated Learning	５．発行年 2020年
３．雑誌名 IEEE Open Journal of the Communications Society	６．最初と最後の頁 pp.102-112
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 該当する

１．著者名 Sevvandi Kandanaarachchi, Hideya Ochiai, Asha Rao	４．巻 未定
２．論文標題 Honeyboost: Boosting honeypot performance with data fusion and anomaly detection	５．発行年 2022年
３．雑誌名 Elsevier journal on Expert Systems with Applications	６．最初と最後の頁 未定
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　0件／うち国際学会　18件）

１．発表者名 Zhiqing Zhang, Pawissakan Chirupphapa, Hiroshi Esaki, Hideya Ochiai
２．発表標題 XGBoosted Misuse Detection in LAN-Internal Traffic Dataset
３．学会等名 IEEE International Conference on Intelligence and Security Informatics（国際学会）
４．発表年 2020年

１．発表者名 Rikura Furuta, Hideya Ochiai, Hiroshi Esaki
２．発表標題 Mitigating Privacy Leak by Injecting Unique Noise into the Traffic of Smart Speakers
３．学会等名 IEEE SMARTCOMP（国際学会）
４．発表年 2020年

１．発表者名
Yuwei Sun, Hideya Ochiai, Hiroshi Esaki

２．発表標題
Intrusion Detection with Segmented Federated Learning for Large-Scale Multiple LANs

３．学会等名
IEEE WCCI/IJCNN（国際学会）

４．発表年
2020年

１．発表者名
Sheng Gong, Hideya Ochiai, Hiroshi Esaki

２．発表標題
Scan-based Self Anomaly Detection: Client-side Mitigation of Channel-based Man-in-the-Middle Attacks against Wi-Fi

３．学会等名
IEEE COMPSAC（国際学会）

４．発表年
2020年

１．発表者名
Yuwei Sun, Hideya Ochiai, Hiroshi Esaki

２．発表標題
Visual Analytics for Anomaly Classification in LAN Based on Deep Convolutional Neural Network

３．学会等名
IEEE International Conference on Informatics, Electronics and Vision（国際学会）

４．発表年
2020年

１．発表者名
Pawissakan Chirupphapa, Hiroshi Esaki and Hideya Ochiai

２．発表標題
INTAP: Integrated Network Traffic Analysis Pipeline for LAN Monitoring System

３．学会等名
IEEE ICIM（国際学会）

４．発表年
2021年

１．発表者名
Ying Luo, Zhiqing Zhang, Hiroshi Esaki, Hideya Ochiai

２．発表標題
Classification of TCP 445 Attacks and Global Snapshot with Honeypot Analysis

３．学会等名
IEEE ICAIT（国際学会）

４．発表年
2019年

１．発表者名
Yuwei Sun, Nagul Cooharojananone, Hideya Ochiai

２．発表標題
Aircraft Detection Based on Saliency Map and Convolution Neural Network

３．学会等名
IEEE ICSEC（国際学会）

４．発表年
2019年

１．発表者名
Yuwei Sun, Hiroshi Esaki, Hideya Ochiai

２．発表標題
Detection and Classification of Network Events in LAN using CNN

３．学会等名
IEEE InCIT（国際学会）

４．発表年
2019年

１．発表者名
Zhiqing Zhang, Hiroshi Esaki, Hideya Ochiai

２．発表標題
Unveiling Malicious Activities in LAN with Honeypot

３．学会等名
IEEE InCIT（国際学会）

４．発表年
2019年

１．発表者名
Hyuga Kobayashi, Zhiqing Zhang, Hiroshi Esaki, Hideya Ochiai

２．発表標題
Probing Firewalls of Malware-Infected Networks with Honeypot

３．学会等名
ACM CFI（国際学会）

４．発表年
2019年

１．発表者名
Zhiqing Zhang, Hiroshi Esaki, Hideya Ochiai

２．発表標題
Analysis of Malware Hidden Behind Firewalls with Back Scans

３．学会等名
IEEE International Symposium on Digital Forensics and Security（国際学会）

４．発表年
2019年

１．発表者名
Yuwei Sun, Ng S. T. Chong, Hideya Ochiai

２．発表標題
Text-based Malicious Domain Names Detection Based on Variational Autoencoder and Supervised Learning

３．学会等名
IEEE CISS（国際学会）

４．発表年
2020年

１．発表者名
Kai Matsufuji, S.Kobayashi, H.Esaki, H.Ochiai

２．発表標題
ARP Request Trend Fitting for Detecting Malicious Activity in LAN

３．学会等名
13th International Conference on Ubiquitous Information Management and Communication（国際学会）

４．発表年
2019年

１．発表者名
Porapat Ongkanchana, H.Esaki, H.Ochiai

２．発表標題
A Rule-based Algorithm of Finding Valid Hosts for IoT Device Using Its Network Traffic

３．学会等名
13th International Conference on Ubiquitous Information Management and Communication（国際学会）

４．発表年
2019年

１．発表者名
S.Limjitti, H.Ochiai, H.Esaki, K.Sripanidkulchai

２．発表標題
IoT-VuLock: Locking IoT Device Vulnerability with Enhanced Network Scans

３．学会等名
13th International Conference on Ubiquitous Information Management and Communication（国際学会）

４．発表年
2019年

１．発表者名
Hyuga Kobayashi, Hideya Ochiai, Hiroshi Esaki

２．発表標題
Visualizing Remote Network Reactions with Firewall Probe

３．学会等名
IEEE Symposium on Visualization for Cyber Security（国際学会）

４．発表年
2018年

１．発表者名
Mohd Saalim Jamal, Venkata Keerthy S, Hideya Ochiai, Hiroshi Esaki, Kotaro Kataoka

２．発表標題
INSTRUCT: A Clustering Based Identification of Valid Communications in IoT Networks

３．学会等名
IEEE International Conference on Internet of Things: Systems, Management and Security（国際学会）

４．発表年
2018年

１．発表者名
孫　昱偉、落合秀也、江崎　浩

２．発表標題
深層学習に基づくLAN内活動の検出システム

３．学会等名
電子情報通信学会 NS研究会

４．発表年
2019年

１．発表者名
松岡勝也、水谷将也、落合秀也、江崎　浩

２．発表標題
遠方LAN監視システムの開発

３．学会等名
電子情報通信学会 ICSS研究会

４．発表年
2018年

１．発表者名
長嶋 秀幸，落合 秀也，江崎 浩

２．発表標題
IoT機器の安全性を高める動的通信分別手法の研究

３．学会等名
情報処理学会　DICOMO

４．発表年
2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
LANセキュリティ監視プロジェクト
https://www.hongo.wide.ad.jp/~jo2lxq/meta/LAN-security-project.pdf
サイバーセキュリティ
https://www.hongo.wide.ad.jp/~jo2lxq/meta/cyber_security_white_paper_201810.pdf

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

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