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：２４４０２
研究種目：基盤研究(B)（一般）
研究期間：2019～2021
課題番号：１９Ｈ０４０９７

研究課題名（和文）気づきと確信による情報インフラ自動化

研究課題名（英文）Automated Operations of Information Infrastructure with Process from Perception to Conviction

研究代表者
阿多　信吾（Ata, Shingo）

大阪市立大学・大学院工学研究科・教授

研究者番号：３０３２６２５１

交付決定額（研究期間全体）：（直接経費）　　13,500,000円

研究成果の概要（和文）：本研究では、人工知能を用いた情報インフラの運用自動化について、これまでは考えられていない「気づき」から「確信」へのプロセスを取り入れ、人手による運用管理と同様に高い確度の情報に裏付けられた信頼性の高いオペレーションを実現するアーキテクチャを提唱し、その要素技術に関する研究開発を行った。確信のための機器同定精度向上手法、ネットワークスイッチ情報からの気づき検出手法、学習データの逐次蓄積による学習ベース異常検知手法、についてそれぞれ提案、実装ほか、大阪市立大学キャンパスネットワーク上でプログラマブル基盤を用いた導入を行った。

研究成果の学術的意義や社会的意義
複雑化する情報インフラの運用自動化は、これまで高度な専門的知識を有する技術者の経験に基づいて行われていた情報システムの運用管理の負担を軽減するだけではなく、今後ますます重要となる情報セキュリティへの対応コストを大幅に削減できる可能性があり、我が国のみならず世界的な情報セキュリティレベルの向上に大きく寄与するものと考えられる。本研究成果は、より確実なオペレーションを安全に実施するための確度の高い情報収集・分析・処理技術であり、情報インフラの自動化に大きく貢献できる。

研究成果の概要（英文）：In this study, we focus on the process from "perception" to "conviction" in automation of operations and management on IT infrastructure with Artificial Intelligence, to achieve high confidence of automated operations like operations by human. For this purpose, we specifically propose (1) methods of device identification based on multiple information of traffic monitoring to make stronger conviction, (2) methods of detection of anomalies roughly from a global behavior of the network, and (3) a method of sequential accumulation of training data in learning-based anomaly detection. We also implement and deploy these systems over a programmable framework running on the campus network in Osaka City University and evaluate their feasibilities.

研究分野：情報ネットワーク

キーワード：運用自動化　異常検知　プログラマブル基盤　トラヒック計測と分析　運用管理技術　機械学習　機器種別同定

１．研究開始当初の背景

現在、ネットワークをはじめとする情報インフラストラクチャは社会基盤化し、人々の生活において必要不可欠なものとなっている。それに伴い高度化、複雑化する情報ネットワーク、およびその基盤上で動作する各種情報システムは、高い可用性、安定性、頑健性、およびセキュリティが求められている。本研究では情報流通基盤であるネットワーク、およびその基盤上で提供されるサービスシステムを総称し、以降では情報インフラと呼ぶ。

情報インフラの運用管理は今後ますます重要性が高まると考えられるが、現状は高度な技術と豊富な経験を有する管理運用者が自身の経験則に基づいて行っているにすぎない。特に情報インフラに対する運用管理を適切に行える人材、いわゆるインフラエンジニア、およびインフラ・セキュリティに関するオペレータ・アナリストの人材は現在圧倒的に不足しており、それらの人材育成は喫緊の課題である 一方で、人材リソースだけに依存した運用管理ではもはや限界があることから、情報インフラの運用管理自動化についても近年活発に研究開発が進められている。

情報インフラの運用管理自動化は、大きく(1) インフラ挙動を把握するためのデータ収集、(2) 収集したデータを分析し、特定の挙動検出、あるいは異常検知、そして (3) 検出された内容にもとづき情報インフラを適切に制御、の 3 つの手順から構成される。ここで最も重要となるのは、適切なオペレーションを実現するための情報収集、すなわち情報インフラにおける可視性（Visibility）である。情報インフラの運用管理においては、インフラの可視性について極めて高い確度・信頼性が求められる。

２．研究の目的

本研究では以上の背景を鑑み、人工知能を用いた情報インフラの運用自動化について、これまでは考えられていない「気づき」から「確信」へのプロセスを取り入れ、人手による運用管理と同様に高い確度の情報に裏付けられた信頼性の高いオペレーションを実現するアーキテクチャを提唱し、その要素技術に関する研究開発を行う。これは、単に SOC オペレーション自動化に留まらず、多様性を有するアプリケーションに対する適切な制御など、より一般的な情報インフラの運用管理に対し、気づき→確信のプロセスによる自動化を導入するものである。

本研究で対象とする「気づき」「確信」について具体的に以下で述べる。図 1 に「気づき」と「確信」の比較を示す。まず「気づき」とは、日常的に流れる情報インフラに関するさまざまなログを定常的に観測し、「通常（日常）とは異なる」ことを感覚的に認識することを指す。AI においては、日々のログ情報（観測値）を入力として学習させ、観測値が通常とは異なる異常値であると判断された時に、コントローラに通知する処理を指す。一方「確信」とは、「気づき」によって認識された「インシデント」と思われる（この時点では偽陽性も含まれる）事象に対し、さまざまな方法により裏付けを行い、その事象が真に認識された「インシデント」であることを、エビデンスをもって断定する行為を指す。ここでは、複数の「検証手法」を複合的かつ多角的に用い、その分析結果をもとに極めて高い確からしさをもって事象を断定する。

表 1　「気づき」と「確信」の比較

項目	気づき	確信
目的	少しでも疑いのあるものをできるだけ多く検出し「検証」により「確信」への判断につなげる	「気づき」で集められたさまざまな未確定事象を、検証プロセスによって確度を高め、断定可能な事象を特定する
目標	偽陽性を恐れることなく可能な限り多くの事象を検出する	偽陽性をさまざまな検証手法で排除し、最終的に確度の高い事象を絞り込む
手法	必ずしも意味論的に「気づく」必要はなく、ランダム性の高いログ情報において特定の情報が連続することを検知するなど、単純かつ異なる視点からの検出が必要	複数の異なる検証手法を用い、インシデントと判断できるだけのエビデンスを収集
根拠	「気づく」ことが主たる目的であり気づきの根拠を正確に把握する必要はない	エビデンスとして足る根拠を説明できることが重要

３．研究の方法

本研究の具体的な課題項目を以下に示す。本研究は 3 年により行うこととし、第 1 年度は課題 1 および 2 における個別機能の研究開発、第 2 年度は課題 1 の機能を結合・連携させたフレームワークの構築、第 3 年度はキャンパスネットワークへの適用とフィードバックを中心に研究を推進する。

課題 1　「気づき」→「確信」→「制御」の一貫した自動化を実現するため、これら全体を統合

的に扱い、「気づき」から「制御」さらにその結果をフィードバック情報とする新たな「気づき」へつなげ、「気づき」→「確信」→「制御」のループによる自動化フレームワークを完成させる。
課題２　適切な「確信」のための「気づき」の深化を行う。
課題３　実用化に向け、本学キャンパスネットワークによる実証を行う。

４．研究成果
課題１:「気づき」→「確信」のための連携フレームワーク

ここでは主に２つの項目について取り扱った。まず、「気づき」に対してより正確にその事象を「確信」させるための、通信挙動の精度向上に関する検討を行った。本研究ではとくに通信トラヒックパターンからの通信機器種別同定に着目して検討を行ってきた。通信機器種別同定は、これまでにポート番号情報を用いる手法や通信トラヒックの統計情報を用いる手法、ペイロードを用いる手法などが存在するが、個別の手法を用いるだけでは同定精度に限界がある。ここでは、複数の観測情報および同定結果を相互に活用し同定精度を向上させる新たな手法を提案する。具体的には、複数の異なる観測情報を用いて複数の同定結果を取得し、その複数の同定結果から決定される機器同士の類似度という指標を定義し、類似度をもとに機器同定を行う。各個別同定手法の重要性を表す重みという指標を定義し、各手法の重みを考慮して類似度を算出することで、誤同定が少なく詳細な情報まで同定可能な手法の影響が大きくなる同定が可能となる。

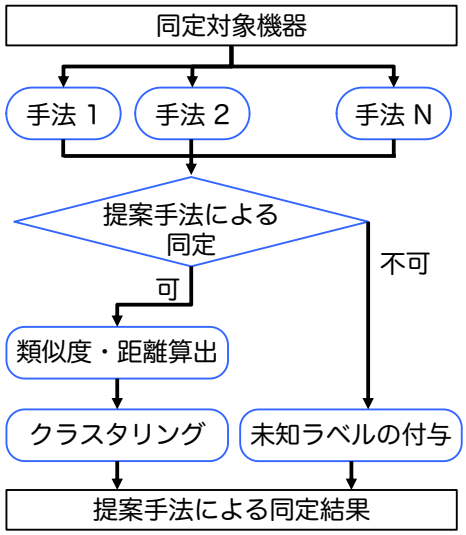

図 1 複数の観測情報による機器同定

本研究で提案する、複数同定技術の組み合わせによる同定精度向上手法について、その概要を図１に示す。単一の観測情報を用いる機器同定技術は、その観測情報からの同定が困難な機器に対して同定を行う手段がないため、さまざまな種類の機器の高精度な同定を維持することが難しい。本研究ではある観測情報からの同定が困難な機器が存在した場合でも別の観測情報からの同定結果からその機器の同定を可能にする。

ここでは複数種類の同定結果をもとに、同定対象機器に含まれる機器の中で未知の機器でない全ての機器同士の組に対して類似度を算出する。ある手法で同じ結果を得た機器同士はその手法が用いた観測情報において類似しているという考えから、複数の同定結果から二つの機器がどれだけ類似しているかを表す指標が機器間の類似度である。複数の同定結果から二つの機器の類似度を決定する単純な考え方は、それらの機器が同じ同定結果を得ている手法の数である。しかしこの考え方を定義とすると、複数の同定手法を同じ程度重要として扱うことにより異なる種類の機器間の類似度が等しい種類の機器間の類似度より大きくなるという問題が発生する。このため、各個別手法の重要さの程度を表す重みという指標を定義し、重みを考慮して類似度の定義を行う。

表 2 同定結果

機種＼手法	I_1	I_2	I_3	I_4	I_5	I_6	提案手法
PC・サーバ	0/44	35/44	36/44	11/44	4/44	3/44	44/44
プリンタ	4/12	0/12	0/12	0/12	0/12	0/12	4/12
無線 AP	6/11	6/11	4/11	0/11	0/11	0/11	6/11
NAS	0/4	0/4	0/4	0/4	2/4	2/4	4/4
スイッチングハブ	0/3	0/3	0/3	0/3	0/3	0/3	0/3
合計	10/74	41/74	40/74	11/74	6/74	5/74	58/74

表 2 に同定結果を示す。ここでは、正解があらかじめわかっている機器（合計 74 台）について、6 種類の個別同定技術とそれを組み合わせた提案手法の結果を比較している。なお 6 種類の観測は Web スクレイピング、SSH バージョンおよび暗号化手法、SMB/AFP のプロトコル情報および OS 情報であり、いずれも nmap 等でオペレーティングシステムのフィンガープリンティングで代表的に使用されているものである。この結果より、単独の観測結果と比較しても提案手法の検出精度が向上していることがわかる。

次に、さらなる機器同定精度の向上のため DNS（Domain Name System）の観測ログを用いた機器同定情報の補完技術を検討した。前項の機器同定では、あくまでも観測された情報に何らかのラベルが付与され、そのラベルの補正のために複数の観測情報を相互検証することで、付与されたラベルの正確性を向上させることを目的としており、そもそも観測の結果ラベル付与が難しい（未知の機器と認定された）場合はラベル付与が行えない。ラベル付与の境界線をより広く取ることで未知と判別される機器の数を減らすことも可能であるが、一方でこのような手法は各ラベル付け自体の曖昧性が増すため、結果として同定精度の低下が起こってしまう。このような問題を解決するため、前項の手法によるラベル精度の向上に加え、各観測情報では未知と判

別された機器について異なる情報を用いたラベル補完手法を提案する。ここでは、DNS の問い合わせ情報を用いた機器クラスタリングを行い、未知の機器をグルーピングするとともに、同一グループにラベルの付与された機器が存在する場合、その機器のラベルで補完する手法を考える。

DNS のクエリ情報が類似している端末を分類するために DNS クエリログから端末ごとの特徴値を抽出し、その特徴値をベクトルで表現する。そしてそのベクトルをクラスタリングすることで特徴が類似している端末を同一クラスタに分類する。DNS クエリについては最も問い合わせの多い A レコードを対象とする。A レコードには問い合わせの FQDN (Fully Qualified Domain Name) が含まれるが、FQDN ごとに発生回数をカウントしてベクトルを作成した場合、負荷分散等による類似の FQDN が独立して計上され、特徴量の値が曖昧となることが懸念される。このため FQDN を直接的に用いるのではなく、第 2 レベルドメインまで集約を行い、第 2 レベルドメインごとに出現数をカウントすることで特徴量ベクトルを作成する。さらに出現頻度の極めてまれな FQDN についての影響を排除するため、全体として出現回数が少ない FQDN については特徴量ベクトルの生成から除外することとする。次に特徴量ベクトルにもとづくクラスタリングを実施する。ここでは、目標とすべきクラスタ数（すなわち機器同定種別の種類数に相当）は事前に設定することはできない（機器が未知であるなら機器種別の数も未知であるため）。そこで本研究ではクラスタ数を順に増やしていき、それぞれのクラスタの重心および半径を計算し、それらの値が収束した時点で求めるべきクラスタ数とする。

表 3 に本提案手法による機器情報補完結果の例を示す。グループ 3 においては、端末 E が機器種別が未知となっていたが、他の 2 つの端末が Linux の汎用サーバであることから、その情報が保管できることがわかる。また、グループ 4 の機器 I については、サーバであると識別されているが他の機器種別から NAS (Network Attached Storage) であることが同定されていることから、この機器も NAS であると訂正することが可能である。またグループ 5 の機器については、多機能ルータであるため複数ことなる同定結果が示されているが、本提案手法によりそれらが同一の機器であることが検出可能となっている。

表 3　DNS による機器情報補完

No.	端末	通信先	機器種別
3	端末 E	fedoraproject.org (171) linux.yz. yamagata-u.ac.jp (12) mirrors.fedoraproject.org (10)	none
	端末 F	fedoraproject.org (407) mirrors.fedoraproject.org (17) linux.yz. yamagata-u.ac.jp (8)	SERVER
	端末 G	fedoraproject.org (414) linux.yz. yamagata-u.ac.jp (20) mirrors.fedoraproject.org (19)	SERVER
4	端末 H	payment.synology.com (5) pkgautoupdate. synology.com (5) tylp.lp.cs.quickconnect.to (5)	NAS
	端末 I	autoupdate.synology.com (2) update.synology.com (2)	SERVER
	端末 J	www.synology.com (24) global.download. synology.com (19) global.quickconnect.to (14)	NAS
	端末 K	checkip.synology.com (8) payment.synology.com (2) pkgautoupdate. synology.com (2)	NAS
	端末 L	checkip.synology.com (8) payment.synology.com (2) pkgautoupdate. synology.com (2)	NAS
5	端末 M	iosupdate.iodata.jp (3) www.narsus.jp (2) ntp.nict.jp (1)	NAS
	端末 N	iosupdate.iodata.jp (2) ntp.nict.jp (1)	WiFi-AP
	端末 O	iosupdate.iodata.jp (1) ntp.nict.jp (1)	NAS
	端末 P	www.narsus.jp (8) iosupdate.iodata.jp (4) ntp.nict.jp (1)	PRINTER

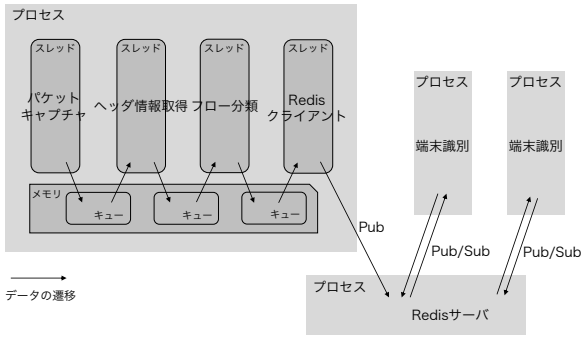

図 2 Pub/Sub による連携フレームワーク

最後に、これらの気づき→確信プロセスの連携について検討する。気づきから確信への連携については、課題 2 での異常検知情報をもとに、課題 1 での機器同定技術を組み合わせることで、どのような場所でどのような機器が情報インフラ全体に影響を与えているかを連携して分析するフレームワークを構築している。具体的には、KVS (Key-Value Store) を用いた Pub/Sub (Publish/Subscribe) システムを用い、気づきや観測情報、異常検知などのイベントを非同期に連携する仕組みを導入し、気づきによるイベントが発生した段階でイベントが Publish され、それを確信に相当する機器同定エンジンが Subscribe し、その機器に関する情報を複数の観測結果から取得、さらに提案手法による情報補完をおこなうことで最終的な同定情報を決定するアルゴリズムを開発した。

さらに同定された機器種別をもとに、それらを独立・分離した形でネットワークに接続できるよう、キャンパスネットワークで稼働中の申請システム（大阪市立大学キャンパスネットワークの仮想ネットワークに関する制御を行うオーケストレータ）に制御プログラムを導入した。具体的には、端末識別システムで判別された機器種別をもとに、申請システムはその機器が接続すべき仮想ネットワーク（機器種別ごとに独立して動的に構築）を決定し、その情報を認証サーバに

登録する。認証サーバは、端末通信時に機器の MAC アドレスを参照し、その MAC アドレスの機器をどの仮想ネットワーク（VLAN）に接続するかを認証スイッチに認証結果の属性情報を（Radius の Attribute として）返す。これにより認証スイッチ以降ではそれぞれの機器が独立したネットワークに接続されることになる。

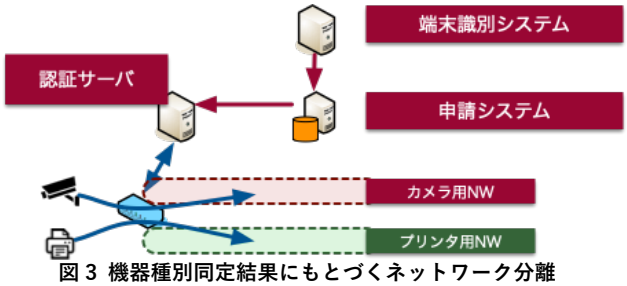

図 3 機器種別同定結果にもとづくネットワーク分離

課題 2　適切な「確信」のための「気づき」の深化

情報インフラにおける「気づき」をより高精度に検知するため、キャンパスネットワークに設置された 346 台の認証スイッチ（各居室の情報コンセントを集約しているスイッチ）に対し、入出力トラヒックを定期的に観測し、その統計値を曜日、時刻、大学における行事等によってラベル化したものを学習データとして蓄積し、それらに対して機械学習を用いることで、特定の観測時間におけるラベル予測を行う。

そして実際に付与すべきラベルとの相違を見ることで以上の予兆を検知する手法を設計・実装する。なお機械学習モデルとしてはロジスティック分析および SVM (Support Vector Machine) を用いる。通信ログには 5 分ごとの各スイッチのポート単位の入力、出力バイト数が記録されており、スイッチにおいて基幹ネットワーク向けに接続されたポートを観測対象とする。なお、学習データおよび検出対象とするラベルは曜日および時間帯にもとづき表 2 のとおり割当を行う。

表 2　ラベル割当

	休日	平日
0:00		
6:00	1	1
8:30		
9:00		2
12:00	3	4
15:00		
18:00		
19:00	1	1
0:00		

図 4 は、2019 年 11 月から 2020 年 2 月までの観測データを使用したラベル識別結果の推移例を示したものである。ラベルの横軸は時刻、縦軸はラベルが正解であった場合を 1、不正解であった場合を 0 としたものである。この図のように大部分においてラベルが正確に検出されていると同時に、不正解については連続する傾向であることが観測されている。これは一旦正常とは異なる挙動が観測された場合、それが一定時間継続することが確認されたものである。なお全体としての識別精度は、ロジスティック回帰において約 87%、SVM において約 90%であった。

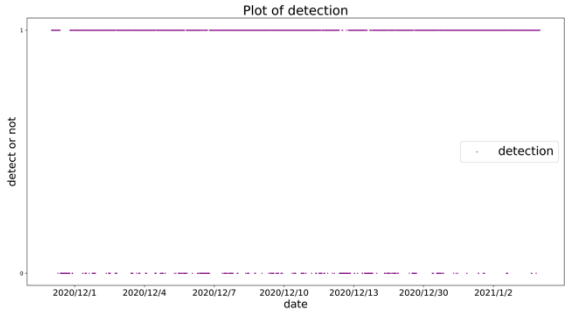

図 4　ラベル識別結果の推移例

次に、「確信」となる情報からより「気づき」の精度を高めることを目標として、学習データの逐次蓄積による異常検知手法の検討を行った。機械学習ベースの異常検知において高い精度で検知を行い、さらに将来出現する未知の異常についても迅速に対応するためには、良質な教師データの継続的な蓄積が必要不可欠であるが、このようなラベル付けはこれまで人の手によって行われるなど、自動化に向けては課題が存在する。

本研究では学習データの継続的な蓄積を実現するため、意図的にセキュリティを弱めることで実攻撃の情報を収集する「ハニーポット」を用いて攻撃を収集・分類し、さらに通信トラヒックパターンとの相関性を分析し、学習データを自動作成，蓄積することでそこから異常を検知する手法を提案する。運用期間が長期化することで異常検知の元となる学習データの蓄積が進み、より高い精度での異常検知が行えるものと期待されるため、どのような蓄積を行うことで有効に機能するかといった性能面の検証を行うことで、逐次蓄積された学習データと異常検知性能の関係を定量的に明らかにするとともに、検知性能を向上させるための学習データ抽出手法を提案する。提案手法を実装した検証環境を構築し，暗号化シェル（ssh）の脆弱性を有するハニーポットを対象とした評価実験を行った結果、逐次蓄積された学習データを単純に使用しただけでは分類精度向上の有無が生じることとなった。一方、蓄積されたデータを観測状況にもとづき抽出する提案手法のアルゴリズムを適用することで、検出精度が蓄積データ量の増加に対し単調増加で向上することを明らかにした。

課題 3　実用化に向けた本学キャンパスネットワークによる実証

課題 1 および課題 2 では、本学キャンパスネットワーク上で実装、設置し、実証を行っていることから具体的な内容については各項目にて参照されたい。

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 深澤那月，阿多信吾，岡育生	４．巻 121
２．論文標題 逐次蓄積型学習ベース異常検知における学習データ抽出手法	５．発行年 2022年
３．雑誌名 電子情報通信学会技術研究報告（ICM）	６．最初と最後の頁 84-89
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 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 林航平,土江康太,中村信之,八百健嗣,阿多信吾	４．巻 121
２．論文標題 基幹ネットワークにおける拡張可能な端末識別のためのリアルタイム処理アーキテクチャ	５．発行年 2021年
３．雑誌名 電子情報通信学会技術研究報告（IN）	６．最初と最後の頁 13-18
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 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 深澤那月，吉田直樹，阿多信吾，岡育生	４．巻 119
２．論文標題 逐次蓄積型学習ベース異常検知における学習データの効用	５．発行年 2021年
３．雑誌名 電子情報通信学会技術研究報告（ICM）	６．最初と最後の頁 49-54
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 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 Imamura Yuki、Nakamura Nobuyuki、Yao Taketsugu、Ata Shingo、Oka Ikuo	４．巻 -
２．論文標題 A Device Identification Method Based on Combination of Multiple Information	５．発行年 2020年
３．雑誌名 IEEE/IFIP Network Operations and Management Symposium 2020	６．最初と最後の頁 1-4
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/NOMS47738.2020.9110448	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 Umoto Keishu、Ata Shingo、Chimura Yasubumi、Nakamura Nobuyuki、Yao Taketsugu	４．巻 -
２．論文標題 An Automatic Error Identification Method in Call Control Protocol Using Levenshtein Distance	５．発行年 2020年
３．雑誌名 Proceedings of ICIN 2020	６．最初と最後の頁 1-5
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ICIN48450.2020.9059524	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 深澤那月，吉田直樹，阿多信吾，岡育生	４．巻 119
２．論文標題 通信トラヒックを活用した学習ベースの異常検知における学習データの自動蓄積	５．発行年 2020年
３．雑誌名 信学技報	６．最初と最後の頁 49-54
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 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 平澤卓也，阿多信吾，岡育生	４．巻 119
２．論文標題 DNSクエリの類似性にもとづく機器情報補完手法	５．発行年 2019年
３．雑誌名 信学技報	６．最初と最後の頁 23-28
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 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 今村裕揮，中村信之，八百健嗣，阿多信吾，岡育生	４．巻 119
２．論文標題 複数の観測情報を用いた機器同定精度の向上	５．発行年 2019年
３．雑誌名 信学技報	６．最初と最後の頁 29-34
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 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 －

〔学会発表〕　計8件（うち招待講演　5件／うち国際学会　1件）

１．発表者名 阿多信吾
２．発表標題 ネットワークプログラマビリティを通じたネットワーク運用管理のサービス化に向けて
３．学会等名 電子情報通信学会インターネットアーキテクチャ研究会（IA）（招待講演）
４．発表年 2022年

１．発表者名 Shingo Ata
２．発表標題 Sliced Networking for Safe and Secure Management of IoT Device
３．学会等名 Digital Around the World 2021（招待講演）（国際学会）
４．発表年 2021年

１．発表者名 阿多信吾
２．発表標題 アフターコロナに向けたキャンパス情報インフラのあり方について
３．学会等名 電子情報通信学会情報通信マネジメントワークショップ2020（招待講演）
４．発表年 2021年

１．発表者名 阿多信吾
２．発表標題 COVID-19におけるキャンパスシステム・ネットワーク運用
３．学会等名 電子情報通信学会総合大会（招待講演）
４．発表年 2021年

１．発表者名
阿多信吾

２．発表標題
アフターコロナにおけるキャンパスネットワーク技術

３．学会等名
大学 ICT 推進協議会年次大会（招待講演）

４．発表年
2020年

１．発表者名
瓦井太雄，深澤那月，中山裕貴，林經正，阿多信吾

２．発表標題
データマイニングを用いたオペレーションログの解析による障害対応操作の標準化と再利用可能な頻出パターンの探索手法

３．学会等名
電子情報通信学会超知性ネットワーキングに関する分野横断型研究会

４．発表年
2019年

１．発表者名
ネットワーク運用管理における時系列データ予測による異常予兆検知手法

２．発表標題
正木健太，阿多信吾

３．学会等名
電子情報通信学会超知性ネットワーキングに関する分野横断型研究会

４．発表年
2019年

１．発表者名
トラヒックパターンとハニーポットログによるSSH攻撃分類手法

２．発表標題
深澤那月，吉田直樹，阿多信吾，岡育生

３．学会等名
電子情報通信学会超知性ネットワーキングに関する分野横断型研究会

４．発表年
2019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

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