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　２ 年　 ６ 月 ２２ 日現在

機関番号：１７１０２
研究種目：基盤研究(C)（一般）
研究期間：2016～2019
課題番号：１６Ｋ００４８０

研究課題名（和文）サイバーセキュリティ攻撃の水平・垂直解析によるサイバー演習支援に関する研究

研究課題名（英文）Research on Cybersecurity education based on interaction from human and society

研究代表者
岡村　耕二（OKAMURA, Koji）

九州大学・情報基盤研究開発センター・教授

研究者番号：７０２５２８３０

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：社会的な大きな問題の一つとして注目されているサイバーセキュリティ攻撃に対して必要となる人材を教育、育成するためのサイバーセキュリティ教育コンテンツを迅速に作成するための研究と、サイバーセキュリティ攻撃防御のための管理者から利用者までより広く受講できるための様々な教育コンテンツを作成するための研究を行なった。

研究成果の学術的意義や社会的意義
本研究の独創的な点は、サイバーセキュリティ攻撃を解析してそのメカニズムを解明する研究を教育に応用している点である。本研究で取り組むサイバーセキュリティ攻撃を自動的、あるいは、半自動的に解析する研究は、本研究の目的である教育コンテンツの迅速化だけではなく、サイバーセキュリティ攻撃対策そのものにも役に立つ技術である。

研究成果の概要（英文）：Various technologies for an automatic and quick production method of quizzes for Cybersecurity education and various educational contents for wide range students from manager to end user about Cybersecurity has been researched. The Cybersecurity threats are serious social issues in the world and this kind of research for Cybersecurity education is very important.

研究分野：情報学

キーワード：サイバーセキュリティ　教材　脅威メール　IoTセキュリティ　ペネトレーションテスト　機械学習　文書解析　マイニング

１．研究開始当初の背景

本研究の計画を策定した 2015 年は、サイバーセキュリティ攻撃が社会的な大きな問題の一つとして注目されていた。アメリカの戦略国際問題研究所などによって全世界のサイバーセキュリティ犯罪の被害額が示され、サイバーセキュリティ攻撃が、他人の資産の奪取が目的であるものへと変化し、早急に対処すべき問題になってきていた。サイバーセキュリティ攻撃は、従来からの組織を対象にしたものに加え、標的型攻撃に代表されるように、個人を対象にしたものも急増してきていた。このような状況で、サイバーセキュリティ対策のできる人材を教育、育成する目的で、サイバーセキュリティ演習による教育が普及し始めていた。サイバーセキュリティ演習では、仮想計算機を用いて、典型的なサイバーセキュリティ攻撃を経験し、その対策方法を学習するものであるが、実システムに近い環境を用いることで、実用的な教育効果がもたらされている。また、サイバーセキュリティ演習は、ネットワークを用いた分散システムとして構築することで、教育コンテンツをより多くの受講者で共有し、さらに受講者が時間や場所の制約を受け難くすることが可能であるため、今後のサイバーセキュリティ対策のできる人材を教育、育成するための教育支援システムとして、非常に期待されていた。

２．研究の目的

このサイバーセキュリティ演習を、今後、サイバーセキュリティ攻撃対策の教育支援システムとして、広く普及させるための課題は、以下の２点であった。

1)　教育コンテンツ作成の迅速化
2)　教育対象者の拡大

サイバー空間では、全く新しい種類のサイバーセキュリティ攻撃が、短期間で発生していた。また、いずれの攻撃も、複雑であった。そのために、いままで存在しなかった攻撃を学習するためのコンテンツをより迅速に作成するための新しい技術が必要であった。従来のサイバーセキュリティ演習は、組織のサイバーセキュリティ対策を行なう人材を育成する目的であるため、組織の電子メールや Web サーバなどのサイバーセキュリティ攻撃対策が主であった。それに対して、最近のサイバーセキュリティ攻撃は、特定の個人を対象にしたものが増加している。そのため、サイバーセキュリティ演習のコンテンツも、サイバーセキュリティ管理者用のものに加えて、より一般的な利用者を対象にしたものが必要になっていた。
このような背景で、本研究では、サイバーセキュリティ演習の教育コンテンツを迅速に作成するための研究と、サイバーセキュリティ攻撃防御のための管理者から利用者までより広く受講できるための教育コンテンツを作成するための研究を行なった。

３．研究の方法

本研究は、下記の４つの研究課題に取り組んだ。

1)　サイバーセキュリティ攻撃の水平方向の解析手法の研究
人間に対するサイバー攻撃について解析を行うことによって、サイバーセキュリティ攻撃そのもののプロトコル解析を行ない、サイバーセキュリティ攻撃のメカニズムを把握するための研究を行なう。
2)　サイバーセキュリティ攻撃の垂直方向の解析手法の研究
サイバー攻撃がもたらす人間や社会への影響について解析を行うことによって、サイバーセキュリティ攻撃が与える人的・社会的な影響の解析を行ない、サイバーセキュリティ攻撃によってもたらされる内容を把握するための研究を行なう。
3)　教育コンテンツの自動作成手法研究
サイバーセキュリティ攻撃のメカニズムや人的・社会的影響の情報等を用いて、サイバーセキュリティ攻撃を防御する教育コンテンツを自動化生成する研究を行う。
4)　サイバーセキュリティ教育の評価に関する研究
本研究者の組織で開講している講義を通じて、サイバーセキュリティ教育の評価に関する研究を行う。

４．研究成果

1)　サイバーセキュリティ攻撃の水平方向の解析手法の研究

本研究は、サイバーセキュリティ脅威となるマルウェアを実行した時の通信や端末での挙動を全て記録できる環境を構築し、収集したマルウェアを実行して研究を進めた。図１ は、その実行環境である。マルウェアは仮想計算機では思ったように動作しないので、解析用のノートパソコン上で動作させた。また、色々な属性を持つネットワークへの通信も可能とした。

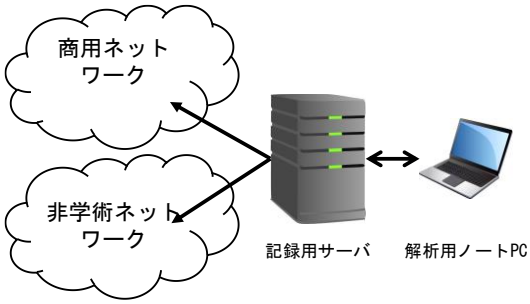

図 1:マルウェア実行環境

この実行環境を用いた研究によって、水平方向の解析として、以下の知見を得ることができた。

未知の脅威が含まれるメールについて，メール中の URL がクリックされた場合の Web ページの遷移あるいは，メール中のマルウェアの実行に伴うプログラムの連鎖を動的解析によってコールグラフとして表現し，正常の場合のコールグラフとの差分情報によって，メール中の未知の脅威の検知を可能にする手法を考案し，実環境で評価を行った。代表的なスパイウェアである URSNIF やランサムウェアのダウンローダー，様々なフィッシングの URL が含まれるメールを用いた評価によって，Windows に標準で装備されているアンチウィルスソフト Defender の検知率が，49.5% であったのに対し，本手法では 89.9% の検知率であった。検知が困難であるフィッシングメールのヘッダと本文から機械学習のための新しい特徴量を抽出し，より精度の高い検知率を得た。本研究では新しい特徴量の抽出のために，本文の機械翻訳による情報，脅威メールに含まれやすい新しい単語を基にした 4 か国語のデータベースやヘッダの時刻情報などを用いている。一般に公開されているフィッシングメールと通常のメールを用いた評価では従来の手法のセロデイ脅威の検知率が，60% 台前半であったのに対して，本手法による検知率は 78% であった。未知の脅威を利用した攻撃によって URSNIF が Windows にインストールされたことを Windows の様々なシステム用パラメータが格納されているレジストリへのアクセス情報によって検知する手法を提案した。本研究では通常のソフトウェアがインストールされ実行される場合と 8 種類の URSNIF がインストールされ実行される場合のレジストリのアクセスについて，アクセスが成功する回数とアクセスが失敗する回数の組み合わせによる識別手法を提案し，従来の Windows Defender ではインストール後，それを検知することは不可能であった 8 種類全ての URSNIF がインストールされたことを他のソフトウェアと区別しながら検知することが可能になった。さらに，既知のマルウェアで評価した結果，従来の Windows Defender での検出率が最高で 97.22% であったのに対して本手法の検知率は 98.68% であった。

次に IoT デバイスの安全性のために、IoT デバイスシステムを水平解析し、通し(End to end)でペネトレーションテストできるフレームワークの研究を行った。図 2 にその構成図を示す。安価でリソースの制約のある IoT デバイスに組み込みのセキュリティプロトコルがないため、攻撃者はこれらのデバイスの脆弱性を悪用して目的のシステムに侵入する。 Mirai、Wannacry、Stuxnet などのサイバー攻撃は、被害者の一連のデバイスの脆弱性が悪用される。これらの脆弱性をタイムリーに検出してパッチを適用することで、将来の攻撃を回避することが可能である。ペネトレーションテストは、このような脆弱性の特定に利用することができる。ただし、従来のペネトレーションテスト方法エンドツーエンドの通しではないので、システム全体への攻撃の検出が困難である。個々のシステムが何らかの脅威モデルの下で安全であっても、攻撃者はキルチェーンを使用してターゲットシステムに到達することが可能である。

本研究では、IoT デバイスを利用したシステム全体へのペネトレーションテストフレームワークである IoT-PEN を開発した。このフレームワークは、すべての IoT ノードがクライアントとして機能するクライアントサーバーアーキテクチャに従い、サーバーとしての「リソースを備えたシステム」。 IoT-PEN は、攻撃者がターゲットグラフを使用してターゲットシステムに侵入する可能性のあるすべての方法を発見するための、エンドツーエンドのスケーラブルで柔軟な自動侵入テストフレームワークである。重要なノード、効率的なパッチ適用のためのクリティカルパスを特定して、パッチの優先順位付けを推奨可能である。本研究の評価によって、IoT-PEN は大規模で複雑な IoT ネットワークへの拡張は容易に可能であることが示されている。

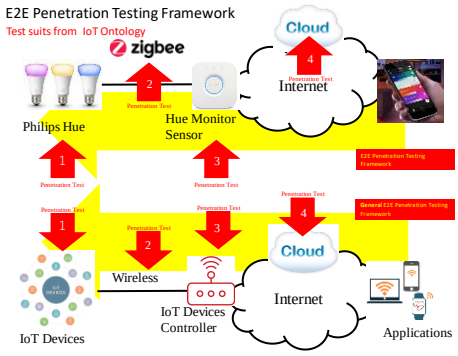

図 2：End to end ペネトレーションテストフレームワーク

その他、STIX(Structured Threat Information eXpression, 脅威情報構造化記述形式)の拡張による多様化するマルウェアの記述や、インターネットのミクロな脅威リスク分析などの研究など、人間に対するサイバー攻撃に関する解析について、様々な研究を行った。

2) サイバーセキュリティ攻撃の垂直方向の解析手法の研究

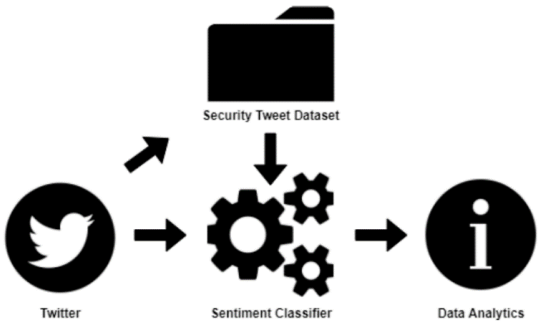

図 3：システム構成図

サイバーセキュリティ攻撃の垂直方向の解析手法の研究としては、SNS にあるセキュリティに関する情報を機械学習を用いて抽出・整理し、セキュリティ脅威を事前に予測し、警告を出すフレームワークに関する研究を行った。図 3 にその構成図を示す。
サイバー脅威の状況に関する情報によって、潜在的な脅威が発生する前に適切に計画および準備のために利用可能な多くの新しいデータソースが存在する。これらのデータソースから関連情報を効率的に取得できれば、サイバー攻撃を防御する際に十分な情報に基づいた意思決定に役立つ予測することが期待できる。このような背景で、ソーシャルネットワーキングサイト www.twitter.com からセキュリティ関連情報を効率的に取得し、感情分析とデータ分析手法に基づいてリアルタイムのサイバー状況認識情報を提供することを目的としたシステムの研究を行った。まず、正当なサイバーセキュリティ関連のツイートを効率的かつ正確に取得して保存する。ソーシャルメディアには豊富なデータがあるため、関係のある正当なデータのみを扱うことが重要である。次に、主観分析を使用してツイートを分類します。この機能を追加することで、サイバーイベントの社会的見解に対するより深い予測のために使用できる有用なデータを提供可能となる。最後に、アナリストがサイバー攻撃のリスクレベルを評価し、組織を防御するためのアクションを実行し、潜在的な攻撃を事前に予測して準備するためのデータの視覚化を行う。

また、インターネット上のサイバーセキュリティに関する文書を収集・解析し、そのトピックスを抽出することで、サイバーセキュリティ脅威について社会が注目していることを示す研究を行った。図 4 は、解析する文書中の語彙の関連を示すネットワークである。ICT の分野における最近の進歩は、人々がニュースを容易に閲覧できる方法を提供しただけでなく、特に見出しが毎分変化しているときに、人間が大量のニュースを理解することを可能にした。 ビッグデータ、自然言語処理（NLP)、機械学習（ML）の技術は、あらゆるドメインの研究者が膨大な量のデータのパターンとテーマを発見するための定番として利用可能である。 この研究では、NPL と ML の手法を利用して、日米の主要新聞（デジタル版）のサイバーセキュリティ関連の新聞記事を分析した。日米は密接な同盟国であり、各国にとって重要性が高まっているため、サイバーセキュリティの分野で協力している。 ただし、人口統計、文化、政治的行動は両国で異なるため、両国の新聞がサイバーセキュリティの問題にどのように対処しているかを分析することは魅力的で非常に重要であった。

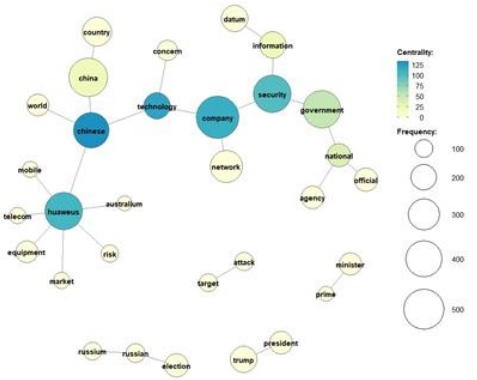

図 4：語彙関連ネットワーク

3) 教育コンテンツの自動作成手法研究

教育コンテンツの自動作成手法研究として、セキュリティオントロジーを利用した選択形式の試験問題自動生成に関する研究と、自然言語処理を利用した穴埋め形式の試験問題自動生成に関する研究を行った。セキュリティオントロジーを利用した選択形式の試験問題自動生成に関する研究では、IoT デバイスに注目した。近年、IoT デバイスシステムは人間の生活の中に深く織り込まれていますが、同時に、深刻なリスクを引き起こすサイバー攻撃への対応が IoT デバイスシステムの大きな課題である。 この研究では、オントロジー手法に基づく体系的な E ラーニングシステムを通じて、ユーザーのセキュリティ意識の向上を目指した。まず、サイバーセキュリティと IoT デバイスシステムの両方の概念を分類、分析、特徴付けし、有用な情報と語彙を抽出し、ユーザー向けの学習資料として提供した。 次に、分類と分析に基づいて IoT セキュリティオントロジーを構築した(図 5)。そのオント

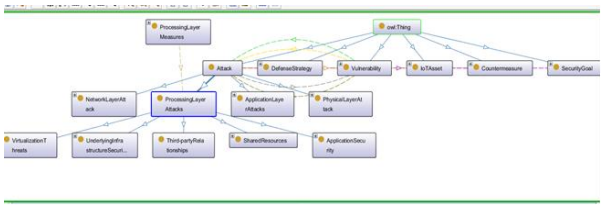

図 5：オントロジーのための分類とその階層

ロジーのデータベースを利用して、複数の選択肢の質問を自動的に生成できるソフトウェアを開発した。 最後に、E ラーニングシステムを使用した後のユーザーの意識レベルを評価するために、Moodle を使用して実際の小テストの試作を行った。

E ラーニングの問題作成の自動化は、E ラーニングシステムを効果的に管理するという課題を解決するために重要である。 さらに、自然言語処理とディープラーニング技術のメリットに基づいて、E ラーニング自動化が期待できる。 例えば、E ラーニングのオンライン問題を自動的に生成し、生徒の質問に自動的に回答することが可能になる。 この研究は主に、E ラーニングシステム管理の難しさの問題を解決するための E ラーニングコンテンツ作成の強力な方法を見つけることに焦点を当てた。 本研究では、主に 4 つのステップに分けて開発を行った。(1)最初に、ソースバージョンから直接のテキストを取得するために、関連するテキストを自動的に要約する。(2)次に、生成された要約からキーワードを検出します。(3)三番目に、検出されたキーワードを要約文章から抜き出し、問題のひな型を作成する。(4) 最後に、前のステップでのキーワード出力を並べ替えて、オンラインの質問と学習のための資料を生成する。図 6 に試作した問題の例を示す。

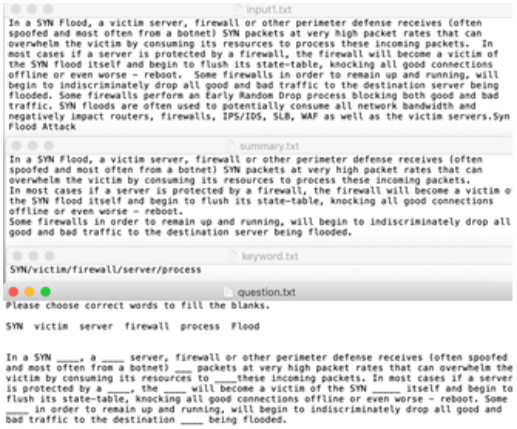

図 6: 試作した問題の例

4) **サイバーセキュリティ教育の評価に関する研究**

九州大学で全学必須で開講しているサイバーセキュリティ基礎論は実践的な教育であるので、教わった内容が小テストで評価の後それで全てが修了するでは不十分である。つまり、習ったことが自分の実生活で役に立つことを実感できることが重要である。そのためには、講義時間外の時にもサイバーセキュリティについて気に掛ける習慣をつけることが必要である。そのようなことは通常、予習、復習という形で行われるが、学生に自主的に自学を促すのは困難である。このような背景で、GRCS 社が開発したシリアスゲームを平成 28 年度にトライアルで実施し、平成 29 年度から全学的に導入した。このシリアスゲームは、ゲーム感覚で自分のスマートフォンでも利用可能であるため、講義時間外に時間も場所も選ばずに自学が可能である。シリアスの利用が講義時間外にサイバーセキュリティのことを気に掛ける習慣作りのきっかけになるのではないかと考えた。シリアスゲームはパソコンの他に、スマートフォンでも動作可能である。そこで、学生が帰宅後あるいは通学中にあえて受講させるために、回答開始時刻を 4 時間目終了からある程度時間の経過した 17 時からとし、終了時刻を翌日の 13 時として、実施することにした。平成 28 年度のトライアル実施や本使用が始まった平成 29 年度の実施において、学生の感想をサンプリングしておおよそ前向きな評価である感覚を得ている。しかし、新しい教材として継続的に利用するためにはシリアスゲームの導入の効果をより詳細に分析する必要がある。

シリアスゲーム導入の目的は、学生が時間外に復習をすることの抵抗感を下げることであり、学力の向上とは若干異なる。そのため、導入した場合としなかった場合の通常の小テストの点数の比較などでは目的となる評価をすることはできない。これに対し、シリアスゲームの課題では、その感想を必ず記述することになっているため、その感想からシリアスゲームの評価をすることが期待できる。しかし、一クラス 200 名程度の受講者がいるため、一人あたり数行の感想を書いたとしても、講義あたり文章の数は 600 以上になり、本研究で対象とした 5 講義分の学生の感想の文章群は、3,000 を超えていた（本論文で分析した感想の文章は 3,111）ので、読むだけでも 50 時間程度要する。また、感想は自由記述方式であり、読みながら、その分類を行えば、さらに労力が増すことが予想される。そのため、何かのツールを利用することは必須であり、オープンソースソフトウェアを中心にその検討を行ってきた。結果、計量テキスト分析ツール KH Coder を発見し、これを用いることにした。

アンケートで、主要な言葉を講義キーワードとして抽出し、評価を行った。各講義キーワードは、講義ごとに偏りがあるが、知識の定着を示す”身に付いた”というキーワードの数は毎回同自由程度であることがわかった。よって、講義キーワードに対して、他の単語の頻度・パターンなどは同じ傾向にあると予想できた。そのため、KH Coder の本来の計量テキスト分析によって、講義ごとにその定着度に関するクラスタの自動抽出が可能であることがわかった。

５．主な発表論文等

〔雑誌論文〕　計13件（うち査読付論文　13件／うち国際共著　5件／うちオープンアクセス　0件）

１．著者名 Koji OKAMURA	４．巻 1
２．論文標題 An Introduction of Serious-Game for Cybersecurity Education	５．発行年 2019年
３．雑誌名 International Workshop on Cyber-Physical Systems and Cyber-resilience	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） 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

１．著者名 Ariel Rodriguez and Koji OKAMURA	４．巻 1
２．論文標題 End to End Real Time Cyber Situational Awareness System Design and Methodology	５．発行年 2019年
３．雑誌名 International Workshop on Cyber-Physical Systems and Cyber-resilience	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） 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

１．著者名 Sanouphab Phomkeona, Kento Kono, Koji Okamura	４．巻 1
２．論文標題 An Unknown Malware Detection Using Execution Registry Access	５．発行年 2018年
３．雑誌名 STPSA 2018: The 13th IEEE International Workshop on Security, Trust, and Privacy for Software Applications	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） 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

１．著者名 Sanouphab Phomkeona and Koji Okamura	４．巻 1
２．論文標題 The design of an active method for spyware detection	５．発行年 2018年
３．雑誌名 The 12th International Workshop on Information Search, Integration, and Personalization (ISIP2018)	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） 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

1．著者名 Alaa Allakany, Toshihide Muto, Koji Okamura, Srishti Kulshrestha and Ranjan Bose	4．巻 1
2．論文標題 Systematic building of E-Learning contents for secure IoT	5．発行年 2018年
3．雑誌名 The 12th International Workshop on Information Search, Integration, and Personalization (ISIP2019)	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） 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

1．著者名 Mohd Zafran B Abd Aziz and Koji OKAMURA	4．巻 17-10
2．論文標題 Leveraging SDN for Detection and Mitigation SMTP Flood Attack through Deep Learning Analysis Techniques	5．発行年 2017年
3．雑誌名 International Journal of Computer Science and Network Security	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） 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 Mohd Zafran B Abd Aziz and Koji OKAMURA	4．巻 15-7
2．論文標題 A Collaborative Mitigation SMTP flood Attack using SDN platform on Multi Site	5．発行年 2017年
3．雑誌名 International Journal of Computer Science and Network Security	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） 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 Mohd Zafran B Abd Aziz and Koji OKAMURA	4．巻 17-6
2．論文標題 A Method to Detect SMTP Flood Attacks using FlowIDS Framework	5．発行年 2017年
3．雑誌名 International Journal of Computer Science and Network Security	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） 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 Alaa M. Allakany and Koji Okamura	4．巻 15-4
2．論文標題 International Journal of Computer Science and Information Security	5．発行年 2017年
3．雑誌名 International Journal of Computer Science and Network Security	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） 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 Alaa M. Allakany and Koji Okamura	4．巻 17-4
2．論文標題 Efficient Multicasting Algorithm Using SDN, International Journal of Computer Science and Network Security	5．発行年 2017年
3．雑誌名 International Journal of Computer Science and Network Security	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） 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 Sanouphab Phomkeona, Yoshitatsu Ban and Koji Okamura	4．巻 1
2．論文標題 An Investigation and Analysis Method for Suspicious Zero-day Malicious Emails	5．発行年 2017年
3．雑誌名 Proceedings of International Conference on Internet (ICONI 2017)	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） 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 Sanouphab Phomkeona, Kristan Edwards, Yoshitatsu Ban and Koji Okamura	4．巻 1
2．論文標題 Zero-day Malicious Email Behavior Investigation and Analysis	5．発行年 2017年
3．雑誌名 Proceedings of Research Network Workshop 2017	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） 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 Alaa M. Allakany and Koji Okamura	4．巻 1
2．論文標題 Latency Monitoring in Software-Defined Networks	5．発行年 2017年
3．雑誌名 Proceedings of the 12th International Conference on Future Internet Technologies 2017	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） 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 －

〔学会発表〕　計18件（うち招待講演　0件／うち国際学会　2件）

1．発表者名 Piyush Ghasiya and Koji OKAMURA
2．発表標題 Quantitative Content Analysis of Japan’s Cybersecurity Strategies and How the Cybersecurity Landscape has changed in Japan since 2013
3．学会等名 情報処理学会 第81回全国大会
4．発表年 2019年

1．発表者名 Xie Wen, Alaa Allakany, Koji Okamura
2．発表標題 A study on Zigbee security: Attacks and Mitigation
3．学会等名 情報処理学会 第81回全国大会
4．発表年 2019年

1．発表者名 Sanouphab Phomkeona, Koji Okamura
2．発表標題 Collecting useful features for zero-day malicious emails detection
3．学会等名 情報処理学会 第81回全国大会
4．発表年 2019年

１．発表者名
Alaa allakany, Geeta yadav, Vijay kumar, Kolin paul, Koji okamura

２．発表標題
An Automated end-to-end penetration testing for the Internet of Thing

３．学会等名
情報処理学会 第81回全国大会

４．発表年
2019年

１．発表者名
Wang Yiyi, Allakany Alaa, Kulshrestha Srishti, Bose Ranjan, Koji Okamura

２．発表標題
Automatic Generation E-Learning contents Based on IoT Security Ontology

３．学会等名
情報処理学会 第81回全国大会

４．発表年
2019年

１．発表者名
岡村耕二

２．発表標題
サイバーセキュリティ教育授業アンケートの分析に関する研究

３．学会等名
ICT推進協議会2018年度年次大会

４．発表年
2018年

１．発表者名
Sanouphab Phomkeona and Koji Okamura

２．発表標題
An evaluation of method for zero-day malicious email detection using email header information analqaysis (EHIA) and deep-learning approach

３．学会等名
Internet Conference 2018

４．発表年
2018年

１．発表者名
PIYUSH GHASIYA and KOJI OKAMURA

２．発表標題
How Japan's Approach Towards Cybersecurity has Changed: Quantitative Content Analysis of Cybersecurity Strategy from 2013 to 2018

３．学会等名
Internet Conference 2018

４．発表年
2018年

１．発表者名
Sanouphab Phomkeona and Koji Okamura

２．発表標題
A Design Method for Zero-day Malicious Email Detection Using Email Header Information Analysis (EHIA) and Deep-Learning Approach

３．学会等名
コンピュータセキュリティシンポジウム2018

４．発表年
2018年

１．発表者名
Ariel Rodriguez and Koji Okamura

２．発表標題
Generating security intelligence through social network sentiment analysis

３．学会等名
コンピュータセキュリティシンポジウム2018

４．発表年
2018年

１．発表者名
Sanouphab Phomkeona and Koji Okamura

２．発表標題
Zero-day Malicious Email Detection Using Email Header Information Analysis Combining with Deep-Learning Approach

３．学会等名
World Social Science Forum 2018（国際学会）

４．発表年
2018年

１．発表者名
PIYUSH GHASIYA and KOJI OKAMURA

２．発表標題
Perception & Vulnerability Towards Cybersecurity Among Elderly Citizen in Japan

３．学会等名
World Social Science Forum 2018（国際学会）

４．発表年
2018年

１．発表者名
上本 悠貴，岡村 耕二

２．発表標題
STIXを用いた多様化する脅威情報の表現拡張に関する研究

３．学会等名
情報処理学会 DICOMOワークショップ

４．発表年
2018年

１．発表者名
北川 大喬，岡村 耕二

２．発表標題
STIXを用いた攻撃手法の分類に関する研究

３．学会等名
情報処理学会 DICOMOワークショップ

４．発表年
2018年

１．発表者名
岡村耕二

２．発表標題
サイバーセキュリティ基礎教育へのシリアスゲームの導入効果に関する研究

３．学会等名
大学ICT推進協議会2017年度年次大会

４．発表年
2017年

１．発表者名
向野 賢人,岡村 耕二

２．発表標題
レジストリの変化量に着目した未知のマルウェアの検知に関する研究

３．学会等名
コンピュータセキュリティシンポジウム2017論文集

４．発表年
2017年

１．発表者名
岡村耕二

２．発表標題
九州大学におけるサイバーセキュリティ教育の紹介

３．学会等名
大学ICT推進協議会2016年度年次大会

４．発表年
2016年

１．発表者名
金子晃介，伴芳龍，岡村耕二

２．発表標題
セキュリティエンジニアを育成するためのインストラクショナルデザインの考察

３．学会等名
大学ICT推進協議会2016年度年次大会

４．発表年
2016年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
九州大学サイバーセキュリティセンター
https://cs.kyushu-u.ac.jp/ja/
九州大学　サイバーセキュリティセンター
https://cs.kyushu-u.ac.jp/ja/

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