[2019]九州大学情報統括本部年報 : 2019年度

出版情報：九州大学情報統括本部年報. 2019, pp.1-, 2020-12-01. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第 4 章　先端ネットワーク研究部門

4.1 スタッフ一覧

職名	氏名	研究キーワード
教授	岡村 耕二	インターネット、新世代ネットワーク、サイバーセキュリティ、マルウェア解析、教育
助教	笠原 義晃	計算機ネットワーク、インターネット運用技術、侵入検知、ネットワークセキュリティ

4.2 研究事例紹介

「エントロピーを用いた国単位でのアクセス状況の変化の顕著化に関する研究」

概要

学内のある DNS サーバーは日々 180 近い国に向け通信している。通信相手国数が非常に多い原因の調査を目的に、このサーバーの通信フローをバイト数、パケット数、通信相手国数の変化に基づいて解析した。その結果、通常時に比べ通信相手国数が微小に増加している時間帯を特定した。しかし、通信相手国数の変化がわずかな為、日中のネットワーク利用者が多く、国数が自然と増加する時間帯との区別が困難であった。更に解析をした結果、この時間帯は、通常は日本に集中している通信量が複数ヶ国に分散していることが分かった。そこで、データの散らばり度合いを数値化する分散（Variance）で、国単位での通信量の散らばり度合いを数値化し、異常時の国単位の通信量の散らばりを表現することで、通常時と異常時の区別を試みた。しかし、通信相手先の国数によっては、分散でも区別が困難な時間が確認できた。そこで、本稿では、情報理論分野で用いられるエントロピーで、一定時間間隔毎の国単位での通信量の割合を数値化することで、異常時の国単位での通信量の割合の変化を顕著化する。本稿では、この提案手法を実データに適応し、本手法の有効性や妥当性を検討する。

1. まえがき

近年、サイバー攻撃がますます巧妙になっており、すべてを未然に防ぐことは困難である。そのため、被害を最小化する事後対策が注目されている。現在、フォレンジックやセキュリティの観点から、ネットワークのフローデータや 、IDS･IPS, FW 等のログが収集される。こういったデータを分析することで、異常を早期に検知し、被害を最小限に抑えることが出来る。しかし、膨大なログを全て人手で統合・監視・分析することは困難である。そのため、複数種類のログの一元管理やログを利用した異常検知等に関する研究が行われている。ログの一元管理・視覚化システムを構築することで多量なログの管理・解析が容易となる。

本稿では、九州大学のネットワークの全パケットのコピーを取得し、そのフローデータ を研究対象とする。大規模データを詳細に解析する為、データの格納や、格納したデータの全文検索ツールである Elastic Search 内のデータの視覚化等を可能とする Kibana を使用している。また、無償の IP 地理位置情報デー

タベース GeoLite2 を使用することで、送信元・送信先の都市名や国名といった情報をフローデータに付与している。セキュリティ運用の効率化に向けた有益な情報の抽出等を目的に、国情報付きフローデータの解析を行っている。
対象ネットワークが通信している国に着目して視覚化した結果、日々 190 以上の国に通信していることが分かった。学術目的だけで、西アジアやアフリカを含むほぼ全ての国に向け毎日通信が生じるとは考え難い。そのため、通信相手先の国数が多い原因の調査を行った。

対象ネットワーク内には、複数種類のサーバーが存在する。それらの内、どのサーバーが多数の国に向け通信しているかを知るため、対象ネットワーク内の IP アドレス毎の通信相手先の国数を降順にソートした。その結果、ある権威 DNS サーバーが日々 180 近い国に通信していることが分かった。そこで、このサーバーの通信相手先の国数に着目して解析を行った。
まず、解析対象となる DNS サーバーの 1 秒間隔毎の通信相手先の国数をグラフ化し、国数が多い時間帯の特定を試みた。2019 年 9 月 10 日～2019 年 10 月 31 日の 52 日間でグラフ化した結果、下記の 3 日間で、通常と比べ、通信相手先の国数がわずかに増加している時間帯が特定できた 図 3. この 3 つの時間帯を解析した結果、同様の結果が得られたため、以降は 9/25 を例として表記する。

- 2019/09/25 21:23:30 ～ 21:37:00
- 2019/10/11 05:36:40 ～ 05:47:00
- 2019/10/29 00:17:20 ～ 00:29:20

次に、通常時と、特定した時間帯の 1 秒毎の国単位での通信量の割合では通常は通信量の約 70% を日本が占めている。一方、特定した時間帯は約 15 秒間隔で通信量が複数ヶ国に分散し、通信量の割合が大きく変化していることが分かる。通信量がこの様に複数ヶ国に分散することは通常なく、通信相手先の国数に着目して特定した時間帯は、明らかに通常ではない、つまり異常であることが判明した。
最後に、異常検知で一般的に利用される、バイト数やパケット数との比較を行った。対象 DNS サーバーの一秒毎のバイト数の合計、パケット数の合計、通信相手先の国数についてをそれぞれ比較した。通信相手先の国数の増加によって特定した時間帯で、バイト数やパケット数に顕著な変化は確認できなかった。つまり、今回特定した異常な時間帯は、通信相手先の国数に着目したことで特定できたものである。
バイト数やパケット数では特定が困難な異常が含まれる時間帯が、通信相手先の国数に着目することで特定可能であると分かった。しかし、通信相手先の国数に着目して解析する際の課題もある。それは、 異常時の変化がわずかな為に、2 値分類の基本的な手法である閾値を用いた検知等が困難な点である。 異常が含まれる時間帯と、日中の通常の時間帯、それぞれの通信相手先の国数を比較する。目安として、11 ヶ国を閾値とした。 異常時に多くの点で閾値を超えているのと同様に、日中の通常の時間帯でもいくつかの点で閾値を超える点が確認できる。これは、日中はネットワークの利用者が多く、通信相手先の国数も自然と増加するためだと考えられる。上記の理由から、通信相手先の国数のみで解析をする場合、閾値等を用いた、通常時と異常時の区別が困難だという課題がある。

2. 分散を用いた国単位での通信量の散らばり度合いの数値化による異常の特定

前章で述べた、通信相手先の国数を用いた解析時の課題を解決するため、異常時には国単位での通信量の割合が大きく変化する点に着目した。異常時には、約 15 秒間隔で通信量が複数ヶ国に分散している。

データの散らばり度合いを数値化する分散（Variance）を用いて、国単位での通信量の散らばり度合いを数値化することで、異常時の国単位での通信量の散らばりを表現し、閾値等での検知精度向上を試みた。

1 秒間隔毎の国単位での通信量の散らばり度合いを数値化するため、分散の各パラメータを以下の様に定義した。

$$\sigma^2 = \frac{1}{l}\sum_{i}^{n}\left(x_i - \mu(x)\right)^2 \qquad (1)$$

n 対象サーバーから1秒間に生じた通信相手先の国名の集合
i 集合 n 内の１つの国名
xi 国 i が一秒間に生じたバイト数の合計 / 対象サーバーが1 秒間に生じたバイト数の合計
l 集合 n 内の要素数
μ(x) パラメータ x の平均
※ l = 1 の場合、分散 σ2 = 0 となり、 通信相手先の国数が多い時間帯の異常の特定を目的とする本稿では、異常検知の妨げとなる。よって、l = 1 の場合は分散 σ2 = 0.15（通常時の分散の平均値）とする。

分散は、集合 n 内の各国の1秒間に生じたバイト数の割合 x と、平均値 μ(x) との距離を数値化する。 通常は、日本が通信量の7割以上を占めているため、平均値 μ(x) と大きく異なる。よって、通常時の分散 σ2 は大きな値となる。それに対し、異常時は複数ヶ国に通信量が分散する為、各国のバイト数の割合 x は、平均値 μ(x) に近くなる。よって、異常時の分散 σ2 は、小さな値となる。正常時と異常時の国単位での通信量の割合の違いを、上記の様に分散を用いて表現することで、閾値等を用いた異常検知の精度向上が期待できる。

本稿では、通信相手先の国数が増加している時間帯に含まれる全てのデータを異常、それ以外を全て正常と定義する。異常な時間帯を含む1日（本稿では、例として 9/25 を示す）の内、閾値を用いて異常なデータ（9/25 21:23:30 ～ 21:37:00 の全てのデータ）のみをどれだけ検知できるかを評価する。閾値を用いた検知精度の評価指標には、機械学習の分類問題の評価指標で用いられる適合率（Precision）を使用した。正常・異常といった、二値分類の正解・不正解には表 3 の4種類がある。また、二値分類の正解・不正解の４つの要素を計算に用いた評価指標は、一般的に 表 4 が用いられる。本稿では、単純な通信相手先の国数だけでは異常時と通常時の値の差がほとんどなく、閾値を用いた異常の判別が困難であることを課題としている。つまり、適合率（Precision）や再現率（Recall）が非常に低いことが課題である。本稿の異常な時間帯の定義では、異常な時間帯に含まれる、通常時と同様の通信を行っている多数の時間も異常とラベリングする。そのため、再現率は検知手法に関わらず常に小さな値となり、本稿の評価指標には適さない。一方で、適合率は閾値を超えた点の内、どれだけのデータが異常な時間帯のデータであるかの割合を示す。つまり、本稿のラベリングでも、通常時と異常時の値の差を大きくする程、適合率は大きくなる。よって、本稿では適合率を検知精度の評価手法とした。

単純な通信相手先の国数と分散を用いた手法で、それぞれ閾値を動かした時の適合率（Precision）の変化

をグラフにした 図 1. 単純な通信相手先の国数の場合、閾値が 14 ヶ国の時に適合率は最大で 0.128 となる。適合率がかなり低いことから、通常時と異常時の区別がかなり困難であることが分かる。一方、分散を用いた手法の場合、閾値が 0.015 の時に適合率が最大で 0.488 となる。単純な通信相手先の国数に比べ、適合率が 0.360 上昇した。分散を用いた手法で異常時の国単位での通信量の割合の変化を表現したことで、閾値での異常の区別がより可能となったことが分かる。しかし、適合率は最大で 0.488 と未だ低い値となっている。この原因を調査するため、通常時と異常時、それぞれの分散の値の推移をグラフにして解析を行った 図 2. 目安として、適合率が最も高い時の閾値 0.015 に赤線を引いている。異常時に複数の点で閾値を下回っているのと同様に、通常時もいくつかの点で閾値を下回っていることが確認できる。原因を調査した結果、これらの点は共通して、国単位での通信量の割合は、日本が全体の約6割を占めており通常時に近いが、通信相手先の国数が 2,3 ヶ国のみ(通常時の平均は 5.4 ヶ国)である、という特徴が確認できた。

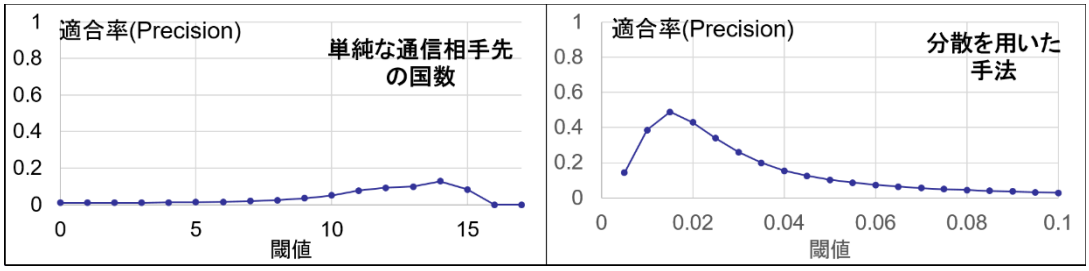

図 1 単純な通信相手先の国数と分散を用いた手法の適合率(Precision)

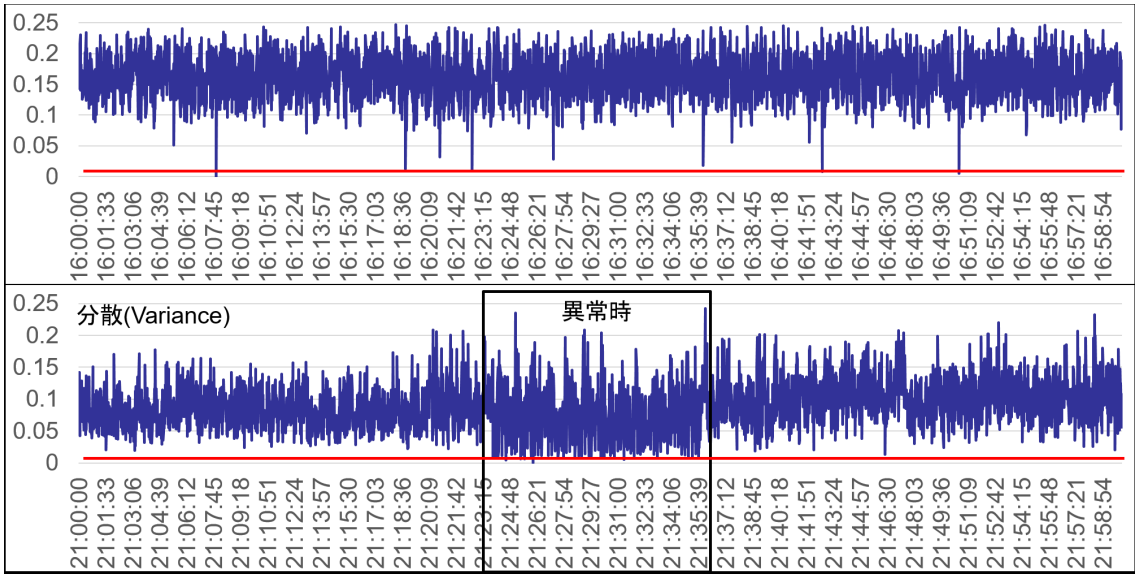

図 2 通常時の例 (2019/09/25 16～17 時) と異常時の分散の推移

つまり、分散を用いた手法では、国単位の通信量の割合が通常通りでも、通信相手先の国数が少ない時間は、異常時と同様に分散の値が小さくなり、正常と異常の区別が困難である。従って、適合率が小さな値になったのである。

3. エントロピーを用いた国単位での通信量の割合の偏りの数値化による異常の特定

前章では、分散を用いて国単位での通信量の散らばり度合いを数値化し、異常時の通信量の割合の変化を表現した。その結果、適合率を上げることはできたが、通常時で通信相手先の国数が小さい場合と異常時との区別が困難であり、適合率は未だ小さな値となった。
そこで、本稿では、情報理論分野のエントロピーを用いた手法を提案する。エントロピーは、一定時間間隔毎のデータの割合の偏りを数値化する。対象サーバーは、通常時の通信量の約7割が日本に向けてである。つまり、通常時は国単位での通信量の割合が日本に大きく偏っている。この状態をエントロピーで数値化することで、異常時の通信量の割合の変化を表現することが可能となる。これによって、閾値等による検知精度の向上が期待できる。

一秒間隔毎の国単位での通信量の割合の偏りを数値化するため、エントロピーの各パラメータを以下の様に定義した。

$$H = -\sum_i^n p_i \, log \, P_i \quad (2)$$

n 対象サーバーから1秒間に生じた通信相手先の国名の集合
i 集合 n 内の１つの国名
pi 国 i が一秒間に生じたバイト数の合計 / 対象サーバーが1 秒間に生じたバイト数の合計

エントロピーは、データの割合 pi の偏りが大きい程、小きな値となる。通常時は、通信量の約7割が日本では、国単位での通信量の割合の偏りが大きく、通常時のエントロピーは小さな値となる。一方、異常時は複数ヶ国に通信が分散するため、各国の通信量の割合 pi の偏りは小さい。よって、異常時のエントロピーは、大きな値となる。通常時の、日本に偏った通信量をエントロピーで表現することで、異常時の国単位での通信量の割合の偏りの変化を顕著に表現することができ、閾値等による検知精度の向上が期待できる。
更に、エントロピーには、一定時間間隔のデータの割合の偏りが同一の場合、データ数が大きいほど、エントロピーの値も大きくなる、という性質がある。本稿の場合だと、国単位での通信量の割合の偏りが同一の場合、通信相手先の国数が多いほど、エントロピーの値も大きくなるのである。例として、日本の通信量が6割、その他の国が残り4割の通信量を均等に分け合うとして、その他の国数を変化させた時のエントロピーの推移をグラフにした 図 3. 異常な時間帯は、通信相手先の国数が通常よりもわずかに増加する。このエントロピーの性質から、国数の増加に伴ってエントロピーの値も増加するため、異常時の変化をより顕著に表現できる。加えて、分散では異常時との区別が困難であった、国数が少ない通常の時間帯に関しても、エントロピーでは、国数が小さいほど小さな値をとることから、区別が容易となることが期待できる。

前章と同様に、エントロピーを用いた手法で、閾値を動かした時の適合率（Precision）の変化をグラフにした 図 4. エントロピーを用いた手法の場合、閾値が 2.6 の時に適合率は最大で 0.833 となった。単純な通信相手先の国数や分散を用いた手法に比べ、適合率は最大値（=1）に大きく近づいた。エントロピー

を用いて、通常時の日本に偏った通信量を表現したことで、異常時の通信量の割合の偏りの変化がより顕著化し、閾値での異常の区別が容易となった。

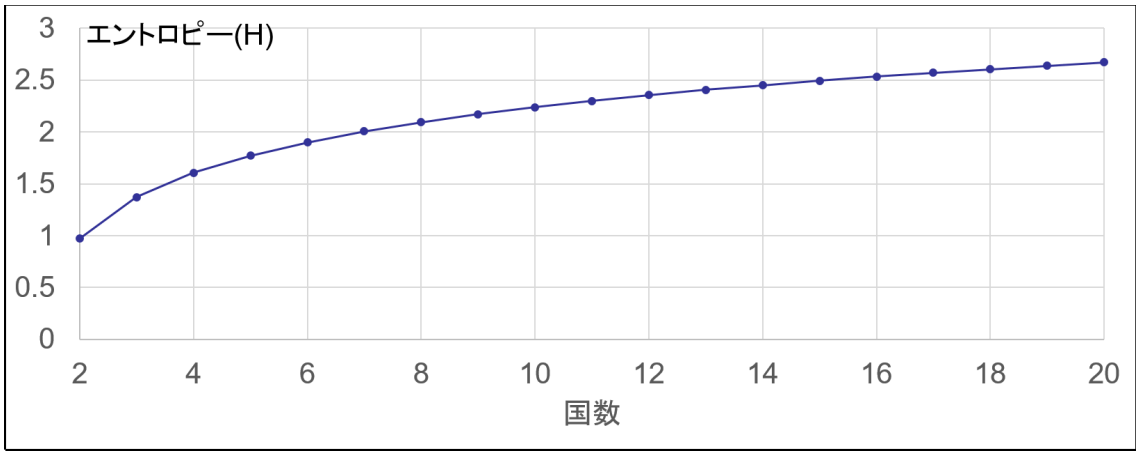

図 3 通信量の 6 割が日本，その他の国が残り 4 割の通信量を均等に分け合うとして，その他の国数を変化させた時のエントロピーの推移

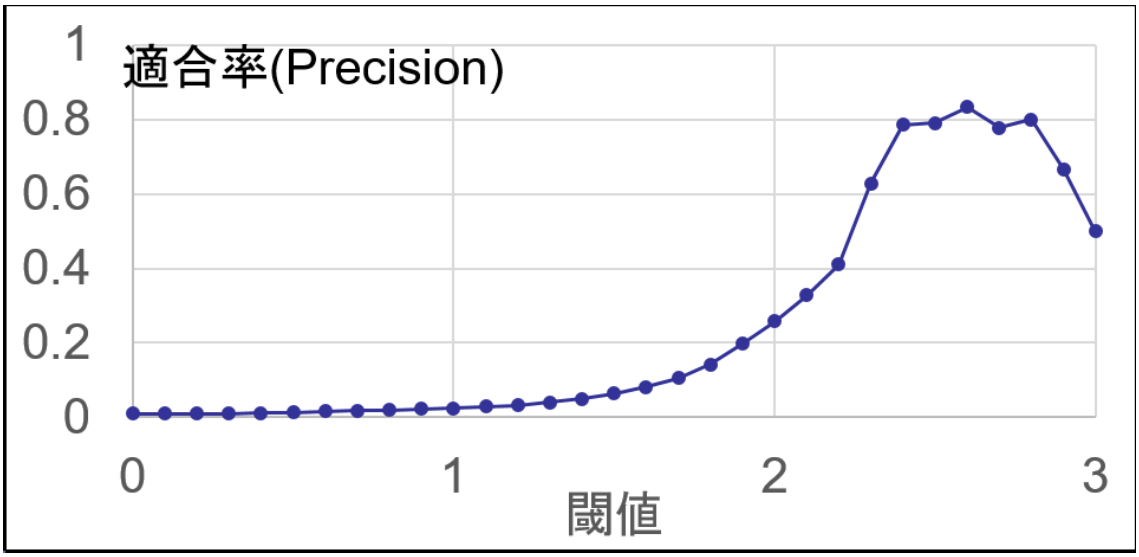

図 4　エントロピーを用いた手法の適合率 (Precision)

4. 考察

本稿で特定した異常な時間帯には以下の2つの特徴がある。

（ 1 ）　通信相手先の国数がわずかに増加する

（ 2 ）　国単位での通信量の割合が 15 秒間隔で通常時から大きく変化する

分散を用いた手法では、(2)の特徴のみを利用したが、エントロピーを用いた手法では、(1)、(2)の両特徴を利用できたため、適合率（Precision）が大きく上昇したと考えられる。更に、分散を用いた手法では、通常時でも通信相手先の国数が小さい場合には、異常時と同様の値をとっていたのに対し、エントロピーを用いた手法では、通常時の値を定常状態として表現することができた。例として、通常時と異常時、そ

れぞれのエントロピーの値をグラフで示す 図 5. 目安として、適合率が最も高い時の閾値 2.6 に赤線を引いている。異常時には 2.6 を超える点が複数あるのに対し、通常時の値は 0～1.5 と、安定して小さな値となっていることが分かる。エントロピーを用いて、通常時の値を定常状態として表現できたことでも、適合率が大きく上昇したと考えられる。

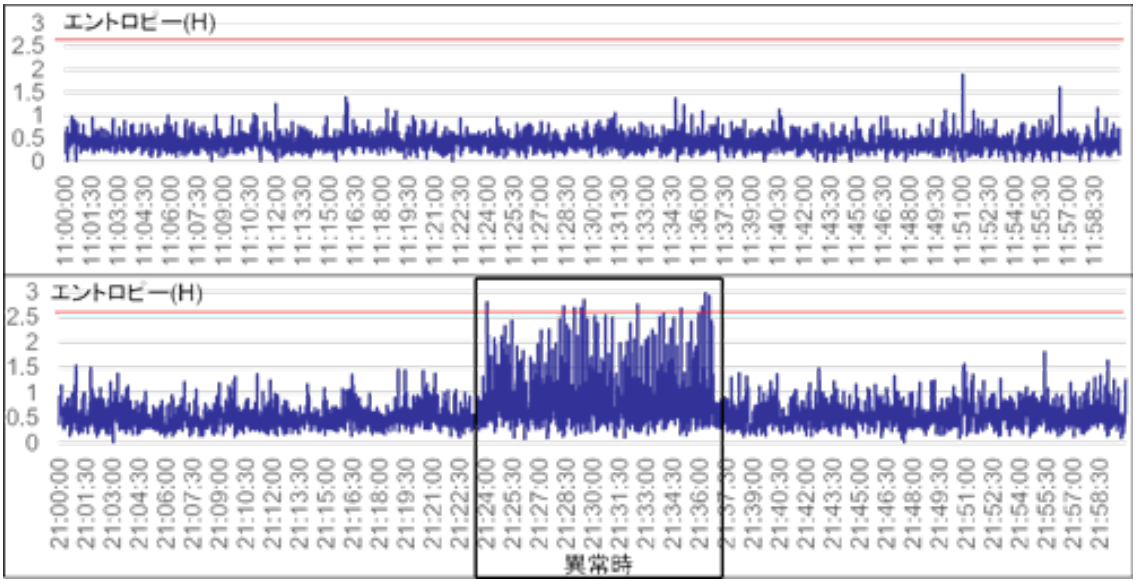

図 5　通常時の例 (2019/09/25 11～12 時) と異常時のエントロピーの推移

5. おわりに

研究対象ネットワークが通信をしている国数が多い原因の特定を目的に、通信相手先の国数が最も多いサーバーの調査を行った。その結果、通信相手先の国数がわずかに増加している時間帯を特定した。この時間帯は、国単位での通信量の割合が通常ではない変化をしており、異常であると分かった。加えて、異常検知でよく利用される特徴であるバイト数やパケット数では、この時間帯に顕著な変化は確認できなかった。 従って、通信相手先の国数に着目したことで、この異常な時間帯が特定できたのである。しかし、単純な通信相手先の国数では、異常時の変化がわずかであり、日中の利用者が多い時間帯との区別が困難であった。実際に、閾値を用いて異常な時間帯の特定を試みた場合でも、適合率は最大で 0.128 と非常に小さな値である。本稿では、エントロピーによって、国単位での通信量の偏りを数値化することで、異常時の通信量の割合の変化を顕著に表現する手法を提案した。提案手法によって、通常時と異常時の区別が容易となり、適合率は最大で 0.833 まで上昇した。特定した時間帯にどの様な通信が生じていたのかは、今後調査予定である。また、提案手法でも、異常な時間帯以外で閾値を超える点が複数存在している。こういった点の解析も今後行う予定である。

従って、今後の課題として以下の 2 点が挙げられる。

- 提案手法により特定が容易となった時間帯に、どの様な通信が生じていたかの詳細な調査・解析
- 提案手法を用いた場合でも、通常時で閾値を超えた時間に対しての、詳細な調査・解析

4.3 研究内容紹介

4.3.1 岡村 耕二

研究内容

私は、1988 年に九州大学工学部で卒業研究を行って以来、三菱電機株式会社、奈良先端科学技術大学院大学、神戸大学、九州大学において、20 年以上にわたって、コンピュータ・ネットワークに関わる研究や仕事、また、学生への教育をしてまいりました。九州大学の助教授に着任しました 1998 年以降の約 12 年間の教育や研究内容について、1) 基礎技術的な内容のもの、2) 応用・実践的あるいは国際的な内容のものに分けて紹介いたします。

1) 基礎技術的な内容の教育・研究

インターネットに関する基礎的な内容の教育・研究は、学術振興会・未来開拓研究「知的で動的なネットワーキング」（コアメンバー）、総務省通信総合研究所（現在の情報通信研究機構）と取り組んだ「新世代モバイル通信技術」、韓国の大学・研究機関との総合的な共同研究である学術振興会・日韓拠点大学プロジェクト、国立情報学研究所とともに取り組んでいる CSI (Cyber Science Infrastructure)プロジェクトそして、最近では新世代ネットワークの研究などを通じて行ってきました。

1999 年からコアメンバーとして参加した学術振興会・未来開拓研究「知的で動的なネットワーキング」プロジェクトでは、専門家以外には難解なネットワークの設定について、その自動化をめざし、最終的にはネットワークの構成要素が変化してもネットワークがその変化に追随して最適なネットワーク環境が自動的に構成されることを目標にした研究に取り組みました。この研究の一部は当時の学生の修士研究としても進められましたが、その成果は最終的に情報処理学会の論文誌に掲載することができました。2003 年から、韓国の主要な大学・研究機関と日本の間の総合的な共同研究を行う、日韓拠点大学方式の総括責任者として、本プロジェクトを遂行するとともに、自分自身も韓国の研究機関と共同研究を行ってきました。私の主たるテーマは、国際的なネットワーク運用と、遠隔医療などの国際応用技術に関するものです。国際的なネットワークの運用のための技術として、私の研究室で行ってきた、蓄積されたネットワークのトラフィック・経路情報の統計処理技術と、韓国の実践的な解析技術を融合させることに成功し、2007 年末に発生しました台湾南沖地震で発生した日本と中国の間の光ファイバ切断がインターネットに与えた影響を、私の研究室と韓国の先生と共同で解析し、災害に対する現在のインターネット運用技術の課題をまとめることができました。これは当時の学生の修士研究、博士研究の一部として取り組み、この成果は、情報処理学会、電気通信学会のそれぞれの論文誌に掲載されました。さらに、次世代ネットワーク技術について着目した研究では、韓国人の博士課程の学生と韓国で一足先に始まった、次世代ネットワーク網のデータ解析を行い、それを日本に提言することができました。この成果も情報処理学会論文誌に掲載されております。また、最近では新世代ネットワークにおける仮想ネットワーク技術、新しいデータ交換技術、省電力運用技術に着目した研究を行い、すでにいくつかの国際会議にその成果を投稿し、発表しております。

2) 応用・実践的、国際な内容の教育・研究

応用・実践的、国際な教育・研究として、総務省・情報通信研究機構が提供する JGN (Japan Giga Network) に関連する公募によるもの、日韓光ファイバに関連するもの、国際遠隔医療に関するものなどに取り組んできました。JGN を用いた研究として、高精細動画像伝送に関わる研究、IPv6 に関する研究、次世代型インターネット拠点のアーキテクチャに関する研究に取り組んできました。次世代型インターネット拠点のアーキテクチャに関する研究では、福岡に設立された九州ギガポッププロジェクト (QGPOP) の主要なメンバーとして研究活動を行い、このプロジェクトで培った高度なネットワーク運用技術はのちの実証実験で活用されています。日韓光ファイバに関する研究では、九州・山口経済連合が導入した福岡と釜山の間の光ファイバの利活用について、産官学非常に多くのさまざまな方々と玄海プロジェクトを 2001 年に設立させ、2003 年にはインターネットとしての利用に成功、さらに、総務省からそのネットワークを利用した 5 年後の IT 社会を模索する研究 (e! プロジェクト) を委託され、国際的な近未来的な遠隔講義、遠隔医療の実証実験に取り組みました。さらに、この活動が評価され、学術振興会による日韓拠点事業が認められました。この事業は 8 年にわたって行われ、私はその総括責任者として日韓で 200 名以上の研究者の代表として事業を成し遂げました。国際遠隔医療は、2002 年から九州大学病院と構想を練り始め、2003 年から韓国と実施をはじめ、以降、九州大学の P&P や学術振興会・アジアコアプログラムの支援などを利用してアジアの各国、オセアニア、米国、欧州などの共同研究医療機関を開拓し、現在では約 20 カ国、世界中の約 90 の医療機関と高精細動画像を用いた遠隔医療の先進的な事例実験に成功しています。この遠隔医療の実証研究の成果・評価の一つとして、九州大学病院にアジア遠隔医療センター (TEMDEC) の設置への貢献をあげることができます。遠隔医療に関する学術的な研究成果は九州大学病院の教員と共著で多くの国際会議などで発表し、高い評価を得ております。

以上のように私は、コンピュータ・ネットワーク技術について、基礎的な内容での教育・研究活動を継続して行い、その成果を論文誌、国際会議論文誌また学会誌に残してきています。また、この延長で、いままで主査として 2 名の学生に博士号（大学院システム情報科学府）を授与させることができました。応用・実践的、国際的な教育・研究の推進で、企業や省庁、自治体と連携した実用的な研究活動や、海外の多くの研究機関とも連携した国際的な研究活動を行い、研究室の学生に国際的な共同研究の機会も与えるとともに、対外的に九州大学のプレゼンスをあげ、その研究活動で得た最新の技術を九州大学のキャンパスネットワークなどの IT インフラや九州大学病院の活動に還元してきました。

所属学会名

IEEE，教育システム情報学会，電子情報通信学会，情報処理学会

主な研究テーマ

・　新世代ネットワークに関する研究
　　キーワード：新世代ネットワーク，2010.04～

- 省電力化を考慮した先進的なネットワーク運用
  キーワード：グリーン IT，省電力，先進的ネットワーク運用，2010.04～
- サイバーセキュリティ
  キーワード：サイバーセキュリティ，2014.03～
- 国際的インターネット実証研究
  キーワード：イーサイエンス，2013.04～
- 日韓およびアジア次世代インターネットおよびその応用に関する研究
  キーワード：インターネット技術，インターネット応用，韓国，アジア，2001.05～

研究プロジェクト

- 成長分野を支える情報技術人材の育成拠点の形成(enPiT)セキュリティ分野
  2016.10～2021.09，代表者：岡村耕二
- 安全な IoT サイバー空間の実現
  2016.11～2022.09，代表者：岡村耕二，サイバーセキュリティセンター，インド工科大学デリー校
- サイバーセキュリティ
  2014.04～，代表者：岡村耕二，メリーランド大学ボルチモア校
- 九州大学サイバーセキュリティ
  2013.03～，代表者：安浦寛人
- 九州ギガポップ プロジェクト
  2000.04～，代表者：岡村耕二，九州大学情報基盤研究開発センター
- 九州大学合成システム生物学研究センター　生命創発システム設計
  2012.01～2016.03，代表者：岡本正宏，九州大学大学院農学研究院
- アジア遠隔医療研究開発
  2008.10～，代表者：清水周次，九州大学病院
- 日韓およびアジア地域次世代インターネットプロジェクト
  2001.07～，日本，韓国，タイ，シンガポール
  日韓およびアジアでの次世代インターネットのリーダーシップをとる

研究業績

● 原著論文

1. Piyush Ghasiya、Sachio Hirokawa and Koji OKAMURA, The Changing Cybersecurity Landscape in Japan and Quantitative Content Analysis of its Cybersecurity Strategies, Proceedings of ISA Asia-Pacific Conference 2019, 2019.07.

2. Yiyi Wang and Koji Okamura, Automatically Generate E-Learning Quizzes from IoT Security Ontology, Proceedings of 8th International Congress on Advanced Applied Informatics, 2019.07.
3. Geeta Yadav, Alaa Allakany, Vijay Kumar, Kolin Paul and Koji Okamura, Penetration Testing Framwork for IoT, Proceedings of 8th International Congress on Advanced Applied Informatics, 2019.07.
4. Ariel Rodriguez and Koji OKAMURA, Generating Real Time Cyber Situational Awareness Information Through Social Media Data Mining, Proceedings of COMPSAC, IEEE Computer Society International Conference on Computers, Software & Applications 2019, 2019.07.
5. Geeta Yadav, Alaa Allakany, Vijay Kumar, Kolin Paul and Koji Okamura, IoT-PEN: A Penetration Testing Framework for IoT, Proceedings of The 34th International Conference on Information Networking (ICOIN 2020) , 2020.01.
6. Yiyi Wang and Koji Okamura, Automatic Generation of E-Learning Contents Based on Deep Learning and Natural Language Processing Techniques, Proceedings of The 8-th International Conference on Emerging Internet, Data & Web Technologies (EIDWT-2020) , 2020.02.
7. Sanouphab Phomkeona and Koji Okamura, Zero-day Malicious Email Investigation and Detection Using Features with Deep-learning Approach, 情報処理学会論文誌, 2020.03.
8. Ariel Rodriguez and Koji OKAMURA, Social media data mining for proactive cyber defense, 情報処理学会論文誌, 2020.03.
9. Motoyuki Ohmori, Koji Okamura, The Equal Deepest Vertex First Reboot: Rebooting Network Edge Switches in a Campus Network, 情報処理学会論文誌, 2020.03.

● 学会発表

1. 今村弦, 岡村耕二, Kappa 指標による大学別 UDP リフレクタ数の分析, 情報処理学会 DICOMO ワークショップ, 2019.07.
2. 上本 悠貴, 岡村耕二, エントロピーを用いた通信相手国数の増加検知手法, コンピュータセキュリティシンポジウム, 2019.11.
3. 岡村耕二, 橋口勝弘, 上拾石弥生, 新里亜希, 九州大学サイバーセキュリティセンターの紹介, 大学 ICT 推進協議会 2019 年度年次大会, 2019.12.
4. 北川大喬, 岡村耕二, 片方向通信に着目した異常検知に関する研究, 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, 2020.01.
5. 上本悠貴, 岡村耕二, エントロピーを用いた国単位でのアクセス状況の変化の顕著化に関する研究, 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, 2020.01.
6. 小野貴臣, 岡村耕二, 5G 環境下におけるブロックチェーンアプリケーションの性能に関する研究, 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, 2020.01.

研究資金

● 科学研究費補助金

1. 2016 年度～2019 年度, 基盤研究(C), 代表, 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

● 競争的資金

1. 2016 年度～2020 年度，文科省 成長分野を支える情報技術人材の育成拠点の形成，分担，実践的セキュリティ人材の育成
2. 2016 年度～2021 年度，JST 戦略的国際共同研究プログラム，代表，安全な IoT サイバー空間の実現

● 共同研究、受託研究

1. 2019.11～2021.03, 代表，ネットワークトラフィック情報から脅威情報の抽出技術の研究

教育活動

● 担当授業科目

1. 2019 年度・夏学期，ソフトウェア技術を利用したシステム構築のための技術論 I
2. 2019 年度・冬学期，ソフトウェア技術を利用した創造的サービス構築論 I
3. 2019 年度・後期，ソフトウェア技術を利用した創造的サービス構築論 II
4. 2019 年度・春学期，サイバーセキュリティ基礎論
5. 2019 年度・前期，サイバーセキュリティ演習
6. 2019 年度・後期，情報知能工学講究第一
7. 2019 年度・後期，情報知能工学講究第三
8. 2019 年度・後期，情報知能工学演習第一
9. 2019 年度・後期，情報知能工学演習第三
10. 2019 年度・後期，情報ネットワーク特論
11. 2019 年度・後期，【ｻｲﾊﾞｰ】情報ネットワーク特論
12. 2019 年度・後期，情報ネットワーク
13. 2019 年度・後期，サイバーセキュリティ
14. 2019 年度・秋学期，通信工学通論
15. 2019 年度・冬学期，通信工学通論 B
16. 2019 年度・夏学期，企業から見たサイバーセキュリティ
17. 2019 年度・冬学期，企業から見たサイバーセキュリティ
18. 2019 年度・冬学期，警察実務から安全な生活について学ぶ

社会貢献・国際連携等

● 社会貢献・国際連携活動概要

1. 通信・放送機構 委託研究評価委員
2. 北九州ギガビットラボ 利用促進部長
3. 北九州 IT 研究開発基盤利用促進協議会 会長
4. 福岡県 ギガビットハイウェイ 構想委員

● 一般市民、社会活動及び産業界等を対象とした活動

1. 2020.02, せきゅトーク 2020 in 福岡, 九州大学サイバーセキュリティセンター, JR 博多 City

大学運営

● 学内運営に関わる各種委員・役職等

1. 2012.04～, 全国共同利用運営委員会
2. 2007.04～, 全学情報環境利用委員会
3. 2003.04～, セキュリティ専門委員会

4.3.2 笠原 義晃

研究内容

・ 安定した情報サービスのためのサーバ品質の監視・異常検知・品質改善

インターネットではさまざまな種類の情報サービスが提供されている。九州大学でも構成員に向けてさまざまなサービスを提供している。サービスを提供する機器（サーバ等）の増加により、管理は複雑さを増しており、期待される性能が出ていなかったり、異常が発生していても迅速に対応できない場合が増えている。仮想化技術の進展により仮想計算機によるサービス構築も容易になったが、仮想化レイヤが増加することにより障害対応はより複雑になった。
本研究では、実サービスの運用管理を通して、仮想化システムも視野に入れた、統一されていない多数のサーバによるサービス提供環境において、管理者の負荷を低減し効率的に管理・運用が可能な手法の構築を目指す。

・ ネットワークトラフィック監視に基づく侵入検知・裏口検出に関する研究

インターネットを利用した計算機への不正アクセスや、ウィルス・ワーム・ボット等の自動化された侵入・拡散ソフトウェアによる被害は年々増加し、また手口も巧妙化している。これに対抗するには、ホストレベルからネットワークレベルに到る多層的な対策が必要となる。
本研究では、このうち特にネットワークでの対策に重点をおき、組織の基幹ネットワーク管理者の立場から組織内ネットワークでの不正な活動などを監視・検出する手法を研究・開発する。具体的には、ネットワークトラフィックを受動的に収集し、パターンによらない分類手法や、プロトコルの特徴を利用した異常検知手法について検討している。これにより、既存のパターン検出型侵入検知システムでの検知が難しい活動を発見する事を目指している。

・ その他の活動

九州大学の学内ネットワークである総合情報伝達システム（KITE）の管理・運用に参加し、学内外向け各種サーバの管理・運用、新規サービスの開発等を行っている。
また、管理者向け講習会の実施、管理者や利用者からの質問への対応、侵入検知システム等の監視による学内ネットワークの保全等、安定したネットワークを維持するための活動を続けている。

所属学会名

Association for Computing Machinery (ACM)，情報処理学会，電気情報通信学会

主な研究テーマ

・ 安定した情報サービスのためのサーバ品質の監視・異常検知・品質改善
キーワード：情報システム，サーバ管理・運用，仮想化，2012.04～.

・　ネットワーク監視に基づく侵入検知・異常検知
キーワード：インターネット，ネットワーク管理運用，侵入検知，ネットワークセキュリティ，
2001.04～.

研究業績

● 原著論文

1. Takao Shimayoshi, Yoshiaki Kasahara, Naomi Fujimura, Renovation of the Office 365 environment in Kyushu University: Integration of Account Management and Authentication, 2019 ACM SIGUCCS Annual Conference, SIGUCCS 2019

   SIGUCCS 2019 Proceedings of the 2019 ACM SIGUCCS Annual Conference, 10.1145/3347709.3347819, 135-139, 2019.11.

2. Yoshiaki Kasahara, Takao Shimayoshi, Tadayuki Miyaguchi, Naomi Fujimura, Migrate Legacy Email Services in Kyushu University to Exchange Online, 2019 ACM SIGUCCS Annual Conference, SIGUCCS 2019

   SIGUCCS 2019 Proceedings of the 2019 ACM SIGUCCS Annual Conference, 10.1145/3347709.3347817, 127-131, 2019.11.

● 学会発表

1. Yoshiaki Kasahara, Takao Shimayoshi, Tadayuki Miyaguchi, Naomi Fujimura, Migrate Legacy Email Services in Kyushu University to Exchange Online, 2019 ACM SIGUCCS Annual Conference, SIGUCCS 2019, 2019.11.
2. 笠原　義晃，嶋吉　隆夫，宮口　忠幸，藤村　直美，九州大学における電子メールサービスの Exchange Online 移行，大学 ICT 推進協議会 2019 年度年次大会，2019.12.

研究資金

● 共同研究、受託研究

1. 2017.10～2021.03，代表，軽量コンテナに基づく柔軟なホスティング・クラウド基盤の研究開発と大規模・高負荷テスト環境の構築

教育活動

● 担当授業科目

1. 2019 年度･春学期, サイバーセキュリティ基礎論
2. 2019 年度･春学期, サイバーセキュリティ基礎論
3. 2019 年度・秋学期, 情報処理概論（24 クラス）

大学運営

● 学内運営に関わる各種委員・役職等

1. 2016.10～, ウエストゾーン安全衛生部会 委員
2. 2014.04～, 情報基盤研究開発センター安全衛生部会 委員
3. 2013.04～, 九州大学病院情報基盤専門委員会 委員
4. 2012.04～, 生涯メール運営会議 構成員