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

平成　２９　年　　６　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：　2014～2016
課題番号：　２６３３０１０１

研究課題名（和文）DNSオープンリゾルバを悪用した増幅攻撃に対する検知手法と動的防御システムの確立

研究課題名（英文）The design and Implementation of the detection and defense system against packet amplifier attacks using open resolver DNS servers.

研究代表者

関谷　勇司（SEKIYA, Yuji）

東京大学・情報基盤センター・准教授

研究者番号：３０３６１６８７

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究では、主にDNSを主としたパケット増幅攻撃に対して、その攻撃の予兆を分析するための手法提案とシステム実装を行った。実装したシステム、誰でも利用できるオープンな実装として公開した。また、本システムを使った検知の事例を示し、パケット増幅攻撃や情報漏えいにつながる攻撃をSDN技術を用いて防御するための手法を提案した。本防御手法は、インターネットの基幹部分であるインターネットエクスチェンジ（IX）において機能する手法であり、複数の IX にて連携動作させることで、より効果的な防御対策となる。さらに、プロアクティブな攻撃対策を行うために、深層学習を用いた攻撃予測の可能性について検討した。

研究成果の概要（英文）：In this research, we propose a method and system to analyze predictions of attack against packet amplification attack, mainly DNS. We released the packaged system as open software on that anyone can use. In addition, we published some examples of detection using this system and proposed a method for defending attacks leading to packet amplification attacks and information leaks by using SDN technology. This defense method works on Internet eXchange (IX) which is a public backbone part on the Internet, and it becomes a more effective defense measure by making it cooperate with multiple IX. In addition, we investigated the possibility of attack prediction using deep learning to make proactive attack measure.

研究分野：　インターネットプロトコル

キーワード：　サイバーセキュリティ　DNS　SDN　NFV　Hadoop　深層学習

１．研究開始当初の背景

オープンリゾルバを用いた DNS クエリ増幅攻撃は、現在 DNS の安定性とその存在を脅かす最大の脅威となっている。この攻撃は、DNS が基本的に UDP を用いて通信していることに起因するものであり、いわば DNS のプロトコル仕様を悪用した攻撃と言える。そのため、DNS の問い合わせや応答を TCP のみで行うよう DNS プロトコルを変更する等の、仕様変更を行わない限り根本的な対応が難しい。一方で DNS 運用者に対する啓発 [SAC008] や、DNS サーバの実装に制限を加える試み [RRL2013] も行われている。しかし、あくまでも攻撃に利用される DNS サーバを減らす試みであり、根本的な解決策ではない。

実際の攻撃時には、攻撃者は複数の DNS サーバを用いて DNS クエリ増幅攻撃を行う。この攻撃にはブロードバンドルータが用いられた実例[IPA]も報告されており、インターネットバックボーンを輻輳させる[SAC008], [SpamhausDDoS]深刻な問題となっている。

２．研究の目的

本研究は、現在世界規模にて発生している DNS オープンリゾルバを利用した Distributed Denial of Service (DDoS) 攻撃を事前に検知する手法を確立し、クラウド基盤を用いて動的に防御するためのシステム設計と実装を行うことを目的とする。DNS クエリ増幅攻撃は、DNS の安定性とその存在を脅かす最大の脅威となっている。この攻撃の特徴は、少ない労力（トラフィック）にて攻撃を行うことが可能で、かつ攻撃者を特定するのが非常に難しいという点である。そのため、全世界規模での動的な防御システムの構築が必要であり、この攻撃を防御することは、DNS の安定性と存在自体を脅かす脅威を排除し、健全なインターネットのサービス運用を確保することにつながる。そこで本研究では図 1 に示す通り、(1)攻撃の予兆を検知し、(2)攻撃者の意図や攻撃の手法を分析し、(3)それをインターネットの基幹部分にて連携して防御する仕組みを提案することを目指す。

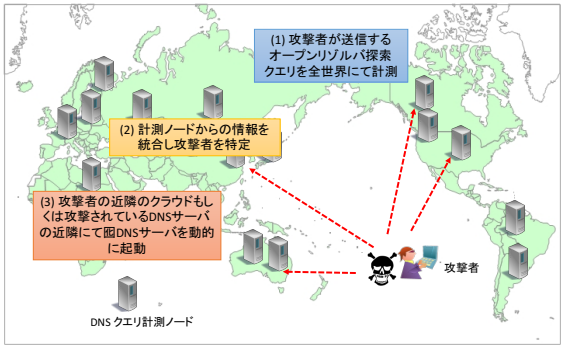

図 1：本研究課題の実現手法

３．研究の方法

本研究は、次に示す 5 つの段階に従って研究を進める。

1. DNS クエリ計測ノードの設置とデータ収集
2. オープンリゾルバ探索挙動の特定
3. 攻撃を浄化するための手法の確立
4. クラウドと準仮想化を利用した攻撃防御システムの設計
5. 攻撃防御システムの実装と展開・評価

なお、研究成果は随時学会や国際会議において発表し、本システムの必要性と有用性をアピールすることを目指す。

まず段階 1 においては、著者の先行研究である Gulliver Project[PAM], [ROOT] の成果を生かし、DNS クエリ計測ノードを各地に設置する。DNS 計測ノードとしては、安価な小型 PC である Raspberry Pi を利用する。

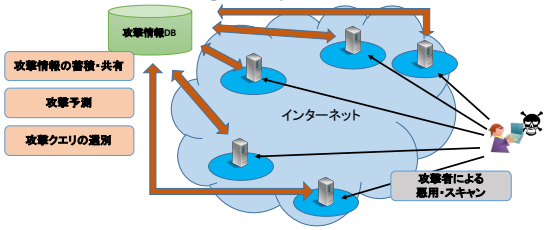

図 2 ： 攻撃者によるスキャニング

図 2 に示す通り、UDP パケット増幅攻撃では、攻撃者は踏み台として利用するオープンリゾルバ DNS サーバを発見するために、スキャニングを行なう。本研究では、このスキャニングの挙動を攻撃の予兆としてとらえ、攻撃との因果関係を明らかにするためにデータを収集し、攻撃情報データベースにそのスキャニングに用いられた DNS 問い合わせの情報を蓄積する。

次に段階 2 においては、DNS クエリ計測ノードからスキャニングデータを収集し分析することで、オープンリゾルバを探索するための DNS クエリの種別や中身、スキャニングの周期、ならびにスキャニングをかけてくる範囲や順番等の規則性を発見する。

段階 3 においては、実際に発生した DNS クエリ増幅攻撃に関する情報を CERT や DNS 関連組織より取得し、本研究にて収集したデータと比較する。これにより、予兆と実際に発生した攻撃のパターンを照合し、より正確にスキャニングを発見するための手法を確立する。また、スキャニング自体を失敗させるために有効となる防御手法に関しての検討も行う。具体的には、スキャニングに用いられる DNS クエリの中身を分析することで、スキャニング自体を不成立にする手法を検討する。

さらに段階 4 においては、攻撃が発生した場合に世界規模において連携して行う防御手法に関する検討を行う。具体的に、次の技術に関して研究開発を行う。

- ホスト仮想化技術を用いた DNS サーバ分身の即時生成
- オーバレイネットワークを用いたクラウド間のネットワーク連携
- ネットワーク環境にあわせた攻撃クエリの誘導技術

これら要素技術を元に、攻撃防御システムの設計と開発を行う。

最後に段階 5 において、世界各地のクラウドにて本防御システムを展開し、連携して防御を行うための手法に関して検討する。

４．研究成果

本研究の成果として次の 3 点があげられる。

(1)多種のログ情報を統合して異常を検知・分析するためのシステム提案と実装の提供

(2)DNS を主としたパケット増幅型攻撃や異常通信攻撃の検知手法と防御手法の提案

(3)動機や意図を持った攻撃を予測するための新たな手法の提案

本研究開始時には、DNS や NTP といった UDP プロトコル自身の特性を利用したパケット増幅攻撃が多発しており、インターネットの基幹部分における攻撃トラフィックの増大が深刻な問題となっていた。2017 年 3 月現在、UDP を用いたパケット増幅攻撃は下火になりつつあるが、愉快犯による発生件数が減少しただけに過ぎず、意図的かつ組織的に行われる DDoS 攻撃は依然として存在する。2016 年のリオオリンピック期間中にも、最大 540Gbps の DDoS が観測されたとの報告[ARBOR]があり、管理の甘い IoT 機器を利用した UDP 増幅攻撃であったと分析されている。このように、UDP を用いたパケット増幅攻撃が有名になることにより管理者による対策が進んでいる一方で、管理の甘い機器は依然として存在する。また、UDP を利用したパケット増幅攻撃以外に、意図的かつ組織的に情報を盗み取ろうとする攻撃が頻発するようになり、これらの攻撃が社会問題[NENKIN][JTB]として取り上げられることが多くなった。

そこで本研究では、当初の UDP を用いたパケット増幅攻撃のみに限らず、より広い範囲で攻撃の兆候や侵入を試みる兆候をとらえるための手法とシステム実装に取り組んだ。また、散発的に行われる愉快犯による攻撃ではなく、より意図的かつ組織的に行われる攻撃に対して、社会的データを利用してその攻撃動機を分析する手法の確立を目指した。その結果、前述の 3 点を達成することができた。それぞれの成果について詳細に述べる。

まず、(1)のログ情報の収集ならびに分析のためのシステムについては、論文[11]にてその詳細を述べた。本研究課題の研究者と北陸先端科学技術大学院大学の研究者が協力し、分散処理系と分散ファイルシステムを利用した、ログデータ蓄積と処理のためのシステムを提案し構築した。このシステムはオープンソースの Apache Hadoop を基盤として利用することで分散処理と分散ファイルシステムを実現し、同じくオープンソースの Apache Hive と Facebook Presto を利用することで、リアルタイムに送信されてくるネットワーク機器からのログデータを蓄積しながら SQL のような構文を用いてデータ分析を行うことを実現した。具体的には、図 3 に示す種類のログ情報を収集し、蓄積した。

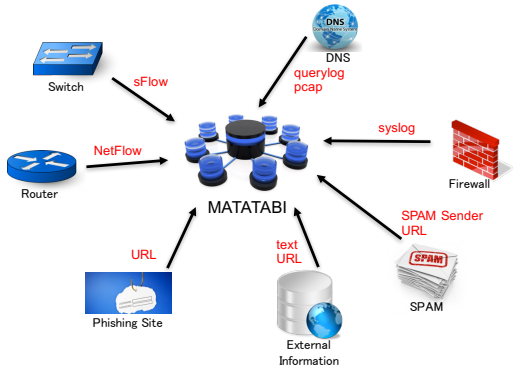

図 3 ： MATATABI に蓄積したログ情報

各ログ情報はネットワーク機器等からリアルタイムにて送信され、一時蓄積領域に蓄積される。その後、ログ情報のフォーマット種別に従って短いものでは毎分、長いものでは一日に一回データ形式の変換が行われ、MATATABI 内部の分散ファイルシステム(HDFS)に蓄積される。この時点で SQL 構文を用いた分析に利用できるようになっており、複数種類のログ情報を統合して検索することができる。このシステムはオープンソースとして公開し、簡単に利用できるよう Docker イメージ[15]として提供した。

次に、(2)の検知手法と防御手法の提案に関して報告する。(1)のシステムを用いた攻撃検知手法に関しては、論文[4][6]にてその手法を述べ、図書[13][14]においてその利用方法を解説した。また、発表[17]の国際会議においてもその利用方法を広くアピールした。攻撃防御手法に関しては、論文[5][8][9][12]において様々な防御手法を提案し、発表[18]の国際会議において手法の実用性に関して議論を行った。また論文[2][3][10]において、各種防御手法のクラウドへの展開手法について述べた。

分析手法に関しては、通常の DNS 問い合わせではあり得ない種別の DNS クエリに着目し、それを攻撃の兆候としてとらえる手法を提案した。(1)にて提案したシステムを用いて DNS への攻撃兆候を分析するための SQL 構文例を図 4 に示す。

- Normally
  # of query from resolver server > # of query to resolver server
- Counting number of queries from resolver server

```
select floor(ts/60),count(*) from dns_pcaps where dt = '20150401' and dns_qr=false and
dns_flags not like '%rd%' and server='ns1-pcap' group by floor(ts/60);
```

- Counting number of answers to resolver server

```
select floor(ts/60),count(*) from dns_pcaps where dt = '20150401' and dns_qr=true and
dns_flags like '%aa%' and server='ns1-pcap' group by floor(ts/60);
```

- If not, it is possibly ddos or cache poisoning attack against our DNS resolver server

図 4:攻撃兆候分析 SQL 構文例

図 4 の例では、通常ならば一致しているはずの DNS サーバへと問い合わせと応答数の差異を見ることで、DNS サーバへの攻撃の兆候

を捉えようとしている。

防御手法に関しては、主に SDN 技術を用いてインターネットの基幹部分に位置するインターネットエクスチェンジにて攻撃を防御する手法、ならびに組織内の末端においても SDN 技術を用いて加害者や情報漏えいの原因となり得る通信を防御する手法を提案した。

さらに研究を進めていくにつれて、攻撃に対が発生した場合に対応を行うリアクティブな攻撃対策のみならず、スキャニング等の攻撃の予兆の増加や攻撃者の攻撃動機の高まりを予測することで、未然に対策を行うプロアクティブな攻撃対策が必要なのでは、との考えに至った。これは、情報漏えいを狙った意図的かつ組織的な攻撃が複数見受けられるようになり、実際に大学等においてもそのような攻撃が行われた実例が発生したためである。そこで本研究では、ネットワーク機器から取得できるインフラ的なログ情報のみならず、Web や SNS から得られる社会的なデータを用いて、攻撃者の攻撃動機の高まりを予測できないかと考えた。

具体的には、クローリングにて Web や SNS から攻撃動向につながる情報を得て、そのキーワードの出現動向から何らかの攻撃動機が高まっていないか、を判定できる手法を確立することを目指した。しかし、本研究期間内には手法の確立まで至ることはできず、その予備実験を行うにとどまった。予備実験は、過去に発生した攻撃に対してそれを予測できる情報が攻撃発生以前の Web や SNS にどの程度存在していたか、また予測確度はどの程度であったかを検証した。予備実験のために集めたデータを表 1 に示す。

表 1: 収集した社会的データ

	データ名	ソース	数量	収集手段	期間
1	サイバー攻撃履歴（全世界）	インターネット	約1400件	Google Custom Search APIによるクローリング	2015/01/01 ~ 2016/10/30
2	サイバー攻撃履歴（日本国内）	インターネット	約150件	手動	2008/10/30 ~ 2010/4/30
3	サイバー攻撃被害者に関連するニュース記事（全世界）	15個のメディア（米国6, 欧州2, ロシア2, 中国2, アラビア2, 日本2）	約3万記事	Google Custom Search APIによるクローリング	2014/12/01 ~ 2016/4/30
4	セキュリティー脆弱性フィード（全世界）	https://cve.mitre.org/	約7万5千件	手動	1988/10/01 ~ 2016/10/03
5	ラベル付きの脆弱性フィード（全世界）	Exploit DB, https://www.exploit-db.com/	約2500件	手動	2009/01/01 ~ 2011/12/31
6	ツイット（全世界）	https://twitter.com/	約90個のhacktivistアカウント約30万ツイット	Twitter API	2016/03/06 ~
7	ツイット（日本国内）	荒牧先生（NAIST）（http://isw3.naist.jp/Contents/Research/mi-08-ja.html）	約1.5億ツイット		2008/10/25 ~ 2010/4/30

過去に実際に発生した攻撃を約 1550 件収集し、深層学習を用いることでこれらの攻撃を予測できる記事が Web や SNS 上に存在したかを判定する判定機を、CNN を用いて構築した。

表 2 ： 攻撃動機に関する判定結果

隠れ層の数	a	b	a - b	b - c	LINE
4	AC: 66.9% PRE: 0.29 REC: 0.37	AC: 70.9% PRE: 0.22 REC: 0.38	**AC: 92.3%** **PRE: 0.71** **REC: 0.99**	AC: 84.4% PRE: 0.97 REC: 0.67	AC: 71.9% PRE: 0.33 REC: 0.46
3	AC: 69.7% PRE: 0.29 REC: 0.37	AC: 70.0% PRE: 0.22 REC: 0.38	**AC: 79.4%** **PRE: 0.71** **REC: 0.99**	AC: 85.3% PRE: 0.97 REC: 0.67	AC: 74.5% PRE: 0.39 REC: 0.62
2	AC: 74.7% PRE: 0.45 REC: 0.46	AC: 70.2% PRE: 0.23 REC: 0.22	AC: 82.8% PRE: 0.38 REC: 0.75	**AC: 91.5%** **PRE: 1.00** **REC: 0.79**	AC: 74.0% PRE: 0.31 REC: 0.44
1	AC: 70.4% PRE: 0.11 REC: 0.24	AC: 77.2% PRE: 0.51 REC: 0.65	**AC: 82.1%** **PRE: 0.48** **REC: 0.74**	AC: 79.4% PRE: 1.00 REC: 0.63	AC: 78.1% PRE: 0.60 REC: 0.66

表 3: 攻撃種類に関する判定結果

隠れ層の数	セキュリティメトリック	キーワード出現頻度	LINE
4	ACC: 82.2% PRE1: 0.97 REC1: 0.89 PRE2: 0.48 REC2: 0.79 PRE3: 0.60 REC3: 0.42 PRE4: 0.37 REC4: 0.63	ACC: 85.9% PRE1: 0.97 REC1: 0.93 PRE2: 0.73 REC2: 0.73 PRE3: 0.64 REC3: 0.75 PRE4: 0.52 REC4: 0.57	**ACC: 87.6%** **PRE1: 0.99 REC1: 0.95** **PRE2: 0.64 REC2: 0.78** **PRE3: 0.72 REC3: 0.68** **PRE4: 0.55 REC4: 0.62**
3	ACC: 79.9% PRE1: 0.97 REC1: 0.88 PRE2: 0.35 REC2: 0.77 PRE3: 0.48 REC3: 0.63 PRE4: 0.45 REC4: 0.41	**ACC: 88.8%** **PRE1: 0.96 REC1: 0.97** **PRE2: 0.76 REC2: 0.70** **PRE3: 0.72 REC3: 0.76** **PRE4: 0.55 REC4: 0.56**	ACC: 85.4% PRE1: 0.95 REC1: 0.93 PRE2: 0.61 REC2: 0.74 PRE3: 0.87 REC3: 0.70 PRE4: 0.54 REC4: 0.59
2	ACC: 82.7% PRE1: 0.96 REC1: 0.91 PRE2: 0.45 REC2: 0.77 PRE3: 0.65 REC3: 0.58 PRE4: 0.42 REC4: 0.50	**ACC: 87.6%** **PRE1: 0.96 REC1: 0.94** **PRE2: 0.66 REC2: 0.79** **PRE3: 0.79 REC3: 0.75** **PRE4: 0.64 REC4: 0.64**	ACC: 87.3% PRE1: 0.96 REC1: 0.94 PRE2: 0.75 REC2: 0.80 PRE3: 0.69 REC3: 0.83 PRE4: 0.61 REC4: 0.58
1	ACC: 79.8% PRE1: 0.96 REC1: 0.87 PRE2: 0.44 REC2: 0.87 PRE3: 0.64 REC3: 0.64 PRE4: 0.40 REC4: 0.41	**ACC: 87.3%** **PRE1: 0.97 REC1: 0.95** **PRE2: 0.59 REC2: 0.70** **PRE3: 0.61 REC3: 0.62** **PRE4: 0.62 REC4: 0.57**	ACC: 87.8% PRE1: 0.97 REC1: 0.95 PRE2: 0.67 REC2: 0.76 PRE3: 0.64 REC3: 0.64 PRE4: 0.49 REC4: 0.61

その結果として、攻撃動機に関する判定結果を表 2 に、攻撃種別に関する判定結果を表 3 に示す。表中の略語は、AC or ACC: Accuracy、PRE: Precision、REC: Recall を意味する。これらの結果から、攻撃動機や攻撃種別に関しては Web や SNS のデータからでもある程度予測可能という結論が得られた。しかし、攻撃時期に関しては予想が難しく、今回の予備実験では高い確度を得ることができなかった。これらの成果に関しては、論文[1][7]にて詳しく述べた。また、このプロアクティブな攻撃対策を、深層学習を用いて行うプロジェクトを NML: Network Muscle Learning[16]と名付け、今後さらに研究を進めることとした。より確度の高い予測と、セキュリティ運用者の助けとなるシステムの構築を目指す。

以上の通り、本研究では(1)多種のログ情報を統合して異常を検知・分析するためのシステム提案と実装の提供、(2)DNS を主としたパケット増幅型攻撃や異常通信攻撃の検知手法と防御手法の提案、(3)動機や意図を持った攻撃を予測するための新たな手法の提案、を行った。この提案手法は、東京大学内でのセキュリティ対策の一つとして実運用する方針であり、導入を進めている。また、さらなる改良とパッケージ化を図り、他の大学や研究機関などにも展開を目指すとともに、プロアクティブな攻撃対策について研究を進める。

参考文献

[SAC008] ICANN Security and Stability Advisory Committee and others. “SSAC Advisory SAC008, DNS Distributed Denial of Service (DDoS) Attacks”, March 2006.

[RRL2013] Thijs Rozekrans, Matthijs Mekking, and Javy de Koning. “Defending against dns reflection amplification attacks.” 2013.

[SpamhausDDoS] “The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)”. http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho. (Accessed on 21st October 2013). [IPA] JPCERT/CC and IPA, 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題, http://jvn.jp/jp/JVN62507275/index.html, 2013 年 9 月

[PAM] Yuji Sekiya, Kenjiro Cho, Akira Kato, Ryuji Somegawa, Tatsuya Jinmei, Jun Murai, “Root and ccTLD DNS server observation from worldwide locations”, Proceedings of Passive and Active Measurement 2003,

pp.117–129, Apr. 2003.
[ROOT] Bu-Sung Lee, Yu Shyang Tan, Yuji Sekiya, Atsushi Narishige, Susumu Date, “Availability and Effectiveness of Root DNS servers: A long term study”, Proceedings of the 12th IEEE/IFIP Network Operations and Management Symposium (NOMS 2010),pp.862–865, Osaka, Japan, April 2010.
[ARBOR] Arbor Networks 社によるリオオリンピック関連サイトに対する DDoS 攻撃分析,
https://www.arbornetworks.com/blog/asert/ddos-attacks-iot-botnets-dont-mean-game/
(2017 年 5 月 31 日現在)
[NENKIN] 日本年金機構における不正アクセスによる情報流出事案について,
http://www.nenkin.go.jp/oshirase/topics/2015/0104.html
(2017 年 5 月 31 日現在)
[JTB] 不正アクセスによる個人情報流出の可能性について,
https://www.jtbcorp.jp/jp/160824.html
(2017 年 5 月 31 日現在)

５．主な発表論文等

〔雑誌論文〕（計 3 件）

[1] Munkhdorj Baaatarsuren, and Yuji Sekiya, “Cyber attack prediction using social data analysis”, IOS Press, Journal of High Speed Networks, vol. 23, no. 2, pp. 109-135, 2017, DOI: 10.3233/JHS-170560, April 2017.

[2] Ryo Nakamura, Kouji Okada, Yuji Sekiya, and HiroshiEsaki : “A common data plane for multiple overlay networks”, Elsevier, Computer Networks Journal, ISSN 1389-1286, October 2015, DOI: 10.1016/j.comnet.2015.09.031.

[3] 関谷勇司, 中村遼, 岡田和也, 堀場勝広 :「SDN と NFV による新たなネットワークサービス構造の提案」, 電子情報通信学会, Vol.J98-B,No.4, pp. 333-344, 2015 年 4 月 (招待論文)

〔学会発表〕（計 9 件）

[4] 西山泰史, 熊谷充敏, 岡野 靖, 神谷和憲, 谷川真樹, 岡田和也, 関谷勇司 :「HTTP 通信に着目した Deep Learning に基づくマルウェア感染端末検知手法と検知性能評価」, 電子情報通信学会, 信学技報, vol. 116, no. 522, ICSS2016-52, pp. 49-54, 長崎県立大学シーボルト校（長崎県西彼杵郡長与町), 2017 年 3 月 13 日

[5] 佐藤康次, 関谷勇司 :「出口対策に向けた耐感染性を有したネットワーク監視並びに防御システムの検討」, 電子情報通信学会, 信学技法, vol. 116, no. 361, IN2016-82, pp. 91-96, 広島市立大学(広島県広島市), 2016 年 12 月 16 日

[6] Tomohiro Ishihara, and Yuji Sekiya, “Case-based study and Discussion of threat analysis on DNS traffic using MATATABI platform”, IA2016 - Workshop on Internet Architecture and Applications 2016, IEICE Tech. Report, vol. 116, no. 282, IA2016-48, p. 99-102, Taipei, Taiwan, 2016/11/03-2016/11/04.

[7] Munkhdorj Baatarsuren, and Yuji Sekiya, “Cyber Attack Prediction using Social Data Analysis”, Proceedings of the 2nd International Conference on Data Compression, Communication, Processing, and Security, Cetara, Italy, 2016/09/22-2016/09/23.

[8] Daisuke Miyamoto, Ryo Nakamura, Takeshi Takahashi, and Yuji Sekiya, “Offloading smartphone firewalling using OpenFlow-capable wireless access points”, Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), pp. 1-4, DOI: 10.1109/PERCOMW.2016.7457060, Sydney, Australia, 2016/03/14-2016/03/18.

[9] 佐藤康次, 関谷勇司 :「SDN を用いた Network 監視によるデータ漏えい防止機構の検討」, 電子情報通信学会, 信学技報, vol. 115, no. 484, IN2015-139, pp. 183-188, フェニックス・シーガイア・リゾート（宮崎県宮崎市）, 2016 年 3 月 4 日

[10] Hajime Tazaki, Ryo Nakamura, and Yuji Sekiya, “Library operating system with mainline Linux kernel”, In Proceedings of The Technical Conference on Linux Networking (netdev 0.1), Ottawa, Canada, 2015/02/14-2015/02/17.

[11] Hajime Tazaki, Kazuya Okada, Yuji Sekiya and Youki Kadobayashi, “MATATABI: Multi-layer Threat Analysis Platform with Hadoop”, In Proceedings of International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2014), Wroclaw, Poland, 2014/09/11.

[12] Yuji Sekiya, “PIX-IE : Programmable Internet eXchange in Edo”, Asia-Pacific Information Infrastructure (APII) Workshop 2014, https://www.jgn.nict.go.jp/jgn-x_archive/english/reports/presentation/API_ws-2014.html, Osaka, Japan, 2014/10/08.

〔図書〕（計 2 件）

[13] 関谷勇司, 岡田和也 :「攻撃に強いネットワークの作り方 : 3-5 一歩進んだセキュリティ対策」, 技術評論社, Software Design 別冊 : インフラエンジニア教本, pp. 113-121, ISBN : 978-4-7741-8924-6, 2017 年 4 月

[14] 関谷勇司, 岡田和也 :「一歩進んだセキュリティ対策」, 技術評論社, Software Design 2015 年 10 月号, 2015 年 9 月, ASIN:B012875GJM

〔産業財産権〕
無し

〔その他〕
[15] MATATABI Docker image,
https://github.com/necoma/docker-matatabi
[16] NML : Network Muscle Learning プロジェクト Web ページ
https://www.sekiya-lab.info/?page_id=416

国際会議における講演
[17] Yuji Sekiya, “MATATABI : Cyber Threat Analysis and Defense Platform using Huge Amount of Datasets”, APNIC 40, APOPS Technical Session, Jakarta, Indonesia, 2015/09/03-2015/09/10.
[18] Yuji Sekiya, “Introduction of PIX-IE (Programmable Internet eXchange)”, Asia Pacific Internet Exchange Association (APIX), APNIC 38, Brisbane, Australia, 2014/09/09-2014/09/19.

６．研究組織
(1)研究代表者
関谷 勇司 (SEKIYA, Yuji)
東京大学・情報基盤センター・准教授
研究者番号：30361687

(2)研究分担者
石原 知洋 (ISHIHARA, Tomohiro)
東京大学・総合文化研究科・助教
研究者番号：60588242

(3)連携研究者
無し

(4)研究協力者
田崎 創 (TAZAKI, Hajime)
株式会社IIJ イノベーションインスティテュート
研究者番号：10611303