Vol.2021-IOT-52 No.15
2021/3/1

Webページの類似性を利用したTorにおける複数セッションに対するフィンガープリンティング攻撃

滕　文杰[1]　吉浦 紀晃[1]

概要：匿名化通信を可能にする Tor では，パケットから通信を行っている実際の IP アドレスが分からない．よって，Tor を用いて Web サイトへアクセスしているとき，アクセス先の Web サイトは不明である．一方，Tor に対して，どの Web サイトへアクセスしたかを特定する手法としてフィンガープリンティング攻撃がある．フィンガープリンティング攻撃の多くは，Web サイトへの 1 つのアクセスを攻撃対象としており，同時に複数の Web サイトへアクセスしている場合に，これらの Web サイトを特定することを想定していない．複数の Web サイトへアクセスの特定する手法も研究されているが，特定の精度は低い．本研究では，同時にアクセスする Web サイトの類似度が高いという前提の下で，特定の精度に影響があるかを分析する．

キーワード：Tor ネットワーク，Web サイトフィンガープリンティング攻撃，匿名性ネットワーク

Fingerprinting Attack for plural Webpages accesses on Tor by using similarity of Webpages

Teng Wenjie[1]　Yoshiura noriaki[1]

Abstract: Tor is a low-latency anonymity network. Tor will hide IP address when communicating so that the destination server will not be discovered. On the other hand, Website Fingerprinting attack that pose security threats to the Tor network. In the past, the attack method was aimed at the situation where the user only visited one website. When visiting multiple websites at the same time, then Website Fingerprinting Unable to Decision the website succesfuly. In this paper, we try to find the factors that affect accuracy while user visiting multiple websites at the same time.

Keywords: Tor network, Website Fingerprinting, Anonymity network

1. はじめに

匿名性ネットワークである Tor は，通信先に自らの IP アドレスを知らせることなく通信を行うことが可能であり，個人情報を秘匿できる利点を持つ，このことから，Tor の利用者数は年々に増えている，近年，パケットを復号せずにユーザのアクセス先を特定する研究が多くなっており，この攻撃の主なものとして，Web サイトフィンガープリンティング攻撃 (WF 攻撃) がある，WF 攻撃に関する既存研究のほとんどは，1 つの Web ページへのアクセスする場合に，アクセスした Web ページの特定率を上げることを目指している，一方，同時に複数の Web ページへアクセスとした場合に，アクセスした Web ページを特定する研究は極めて少なく，また，その少ない研究においては，特定率は極めて低い，この原因は，複数の Web ページへのアクセスのパケットが暗号化されているために区別できないためである，本研究では WF 攻撃の特定率を向上させるために，その原因を分析する，そのため，Web ページの類似度に着目し，複数の Web ページへのアクセスの際に相互に与える影響を分析する，まず，ユーザは同

[1] 埼玉大学大学院理工学研究科数理電子情報部門情報領域
Department of Information and Computer Sciences, Saitama University

時に複数の Web ページへアクセスするときに，2 番目の Web ページへのアクセスする時刻により，ネットワーク中に生じたトラフィックを，positive time separate， zero time separate， negative time separate の 3 種類に分類する， そして，3 種類に対して，Web ページの特定率に変化があるかを調べる，次に，本研究では，特定率を上昇させるために，Web ページの内容によって起こる特定の誤りを減少させるため，ニュースサイトのサブページを利用する，この理由は，ニュースサイトの Web ページは主に文字と画像で構成されており，さらにフォーマットなどが類似しているためである，Web ページの類似度が高くなればなるほど，Web ページの内容を読み込む際に，ネットワーク中に生じたトラフィック量が近くなる，同時に複数の Web ページへアクセスする場合に，アクセスした Web ページらの所属 Web サイト異なる場合に，Web ページの特定の変化を研究する，結果として，同一 Web サイトの場合の Web ページの特定率は 49.3%になり，一方で，異なる Web サイトの場合の Web ページの特定率は 0.729 となった，また，Web サイトは違うが，Web ページの内容は似ている場合，特定率は 0.453 になり，同一 Web サイトの結果とほぼ同じになった，Tor ブラウザのバージョンにより，実施された通信方法に異なるところがあると思われる．先行研究によって，1 つの Web ページへアクセスする場合に，アクセスした Web ページの特定において，トレーニングデータとテストデータの双方が，異なるバージョンの Tor ブラウザを利用しパケットをキャプチャーすると，特定率は極めて低い，一方，双方の使用される Tor ブラウザのバージョンが一致であれば精度が 70 %になる (詳しいテータは表 1 に示している)．本研究では，同時に複数の Web ページへアクセスする場合に，Tor ブラウザのバージョンの差異により，アクセスした Web ページの特定率に与える影響を調べる，今回採用した Tor ブラウザのバージョンは，10.0.8，9.4.10，8.0.9 の 3 つである，同一 Web サイトへ 3 つの異なるバージョンの Tor ブラウザでアクセスし WF 攻撃を行ったところ，トレーニングデータとテストデータで異なるバージョンのものを用いると，特定率は下がった，従って，ユーザが使用しているバージョンと攻撃者に使用されるバージョンが異なると，Web ページの特定は困難になる，

論文の構成はつぎのとおりである．第 2 章は Tor を説明する．第 3 章では関連研究を説明する．第 4 章は Tor における WF 攻撃の発展と同時に複数の Web ページへアクセスする場合に，個々の Web ページを特定する手法を説明する．第 5 章は実験に使用されたデータと，自らに開発した実験のシステムを説明する．第 6 章 Web ページの特定率に影響している要因について説明する．第 7 章は今回の研究に存在している不足点を指摘し，今後の研究の展望を述べる．

2. Tor(The Onion Router)

2.1 Tor の概要

近年，インターネットのセキュリティ問題は，より深刻になっている，プライバシー漏洩や個人情報の流出など事件の頻発がもたらしたのは，インターネットの安全性に対するユーザの不安が高まってきた．Tor(The Onion Router) は匿名性ネットワークである．個人情報の保護を目的として発明された．最初に，アメリカ海軍研究所により開発され，公的な機関にまで使われたことがある，最近，個人用途に広範囲に利用されている．2021 年 1 月 21 日，Tor ネットワークの運営グループである Torproject に公開されたデータによると，Tor の利用者数のピークは，2013 年 9 月である．ピーク時の常駐人数は 600 万であったが，最近は 300 万にまで減少している．一方，Tor ノードの数は，2013 年 9 月以来今まで，常に 8000 台で安定している．Tor は以前より利用されなくなっている理由は，政府の監視，また Tor に対する攻撃技術の発達があげられる．Web サイトフィンガープリティング攻撃 (下記に WF 攻撃と略称する) は，安定性及び高特定率で知られている，既存研究により，機械学習の発展につれて WF 攻撃の成功率は 90%に達している．しかし，既存研究の WF 攻撃手法の多くは，一つの Web ページへアクセスする場合に，Web ページの特定精度を向上させることを目指している．一方，同時に複数の Web ページへアクセスする場合に，暗号化されているパケットを区別できないため，Web ページの特定率が低い．本研究は，Web ページの特定率が低くなる原因について研究する．

2.2 Tor の仕組み

匿名性ネットワークである Tor は通信経路を匿名化することが可能であり，広く使われている．Tor での通信では実際に通信を行なう 2 つの機器の間に Tor の通信路が作られる．この通信路を Tor 回路と呼ぶ．Tor 回路は複数のリレーを介してサーバに接続する形をとる．図 1 にあるように，Tor は 3 つのノードを経由してサーバと通信する．それぞれのノードは，エントリーノード，ミドルノード，イグジットノードと呼ばれる．エントリーノードは，ユーザからのリクエストを最初に中継するノードである．Tor ユーザと直接に通信するため，バンド幅と安定性の要求が高い．ミドルノードに対しては特別な要求がなく，他のノードに中継する作用を担当する．イグジットノードは Tor の内部ネットワークからサーバに通信を中継するノードである．イグジットノードと Web サーバ間の通信は暗号化されている必要はない．

Tor 回線を構築するとき，Tor ノードのリストの中からランダムに 3 つのノードを選ぶ．そして，クライアント側は 3 つのノードとセッションキーを作り，パケットに三重暗

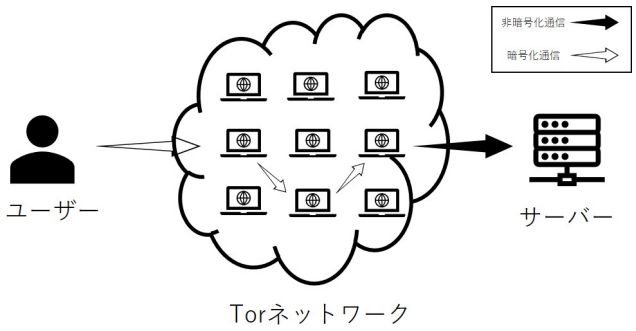

図 1 Tor ネットワークの仕組み
Fig. 1 Tor network

号化したトラフィックをエントリーノードに送信する．エントリーノードはクライアントから送られてきた通信をクライアントとエントリーノードのセッションキーで復号化し，ミドルノードに送信する．ミドルノードとイグジットノードも同様に通信を復号化し送信する．イグジットノードはパケットを復号化した後，中身に書いてあるサーバの宛先情報によって送信する．サーバからの返信はこれとは逆の手順により行なう Tor はこの仕組みを採用し，途中のノードをランダムに変え続けることにより，追跡できないようにしている．アクセスしたサーバはイグジットノードが送信元であると認識するため，実際にアクセスしたユーザの IP アドレスが分からない．

3. 関連研究

3.1 トラフィック分析攻撃

先行研究によると，攻撃者は Tor 回路のエントリーノードとイグジットノードを同時にコントロールすると，通信回路中に転送するトラフィックの転送量と転送時間からの分析によってユーザを特定できる．Danezis ら [11] は同じトラフィック分析法を使用するが，特定率を向上させるためにトラフィックの監視を改良した．彼らはサーバ側にトラフィック衝突を引き起こし，その衝突を利用してアクセスした Web サイトを特定する．トラフィック衝突と同様な特徴を持つトラフィックが発見されたとき，ユーザが使用している Tor 回線を特定することができる．

3.2 WF 攻撃について

2006 年 Herrmann ら [10] は，匿名性ネットワーク内に暗号化されている通信に対して，「Fingerprint」という Web サイトの固有特徴を利用し，アクセスした Web サイトを特定する手法を提示した．彼らの研究は Danezis のトラフィック分析攻撃法と根本的な差異がある．それは，「Fingerprint」の使用である．しかし，Tor ネットワークは，通信を暗号化しているため，Web ページの特定において有効な「Fingerprint」が簡単には見つからないため，Herrmann は Tor ネットワークに対する Web ページの特定率は 2 %しかない．2011 年 Panchenko[9] は，Herrmann と同じデータセットと「Fingerprint」を利用し，アルゴリズムを単純ベイズアルゴリズムから SVM アルゴリズに変更し，特定率は 30.98%となった．精度が向上しない理由として，「Fingerprint」の不十分ではないと考えられた．そこで，「Fingerprint」にパケットの「送受信の順序」，「長さ」，「向き」を追加することにより，Web ページの特定率は，Close-world setting において 54%に向上し，Open-world setting は 73%に達した．続いて，2014 年 Wang は k-NN アルゴリズムに基づき，「Fingerprint」の数を一気に 3000 個まで増やし，Close-world setting において Web ページの特定率 85%を獲得した．Panchenko は SVM アルゴリズムによる開発した WF 攻撃を増幅し，CUMUL 法 [8] を公開した．結果として，Web ページの特定率は Wang の研究の 85%より 5%上がった，Tor ネットワークを運営するグループである Torproject は，次々と発明された攻撃手段 [7,8,9] に対抗するために，対応策を講じている．

3.3 複数 Web ページによる WF 攻撃について

既存研究によると，Tor に WF 攻撃は実行可能であることを示したが，実際に使用した際に，問題が相次いで発生する．2016 年 Juarez[7] は，Tor ネットワークにより，暗号化された通信に対して，WF 攻撃を実施しアクセスした Web ページの特定率に与える影響を研究した，Juarez の実験結果の一部は，表 1 に示している．これは，1 つの Web ページへアクセスしたとき，ユーザが使用した Tor のブラウザと教師データに使用された Tor ブラウザのバージョンが異なる場合の Web ページの特定率を示している，結果により，双方は同じバージョンの Tor ブラウザを使用する場合，Web ページの特定率は 80%に近づく，一方，双方の Tor ブラウザが異なると，Web ページの特定率がかなり低くなる，Tor ブラウザのバージョンの問題以外，同時に複数の Web ページへアクセスしたとき，Web ページの特定率に対しても影響がある，その結果は表 2 にある．Web ページを通常にブラウジングの上，バックグランドページを追加すると，元の Web ページへの特定率は極めて低くなる．さらに，データ規模の増加 (データの規模がは 16 から 100 まで増加する) に従って，特定率が減ってきた．この結果にり，同時に複数の Web ページへアクセスする場合，暗号化された通信が区別できなく，従来の WF 攻撃手法は有効ではなくなる．2016 年 Wang[1] らは，Juarez らに指摘された WF 攻撃を擁する複数の問題において，改善方法を発表した．Wang は従来の WF 攻撃は，問題が発生する時に柔軟に対応できないことを示した．特に，同時に複数の Web ページへアクセスする時，Web ページの特定率が低くなる原因は，アクセスした Web ページのトラフィックを区別できないと指摘した．その故に Wang らは，同時に複数の Web ページへアクセスする時，ネットワーク中に生

表 1　Tor ブラウザのバージョンによる境目の特定率 (Juarez)
Table 1　Probability(FP+FN) of use verious browser'version.

	2.4.7 (test)	3.5 (test)	3.5.2.1 (test)
2.4.7(train)	62.7%	29.93%	12.30%
3.5(train)	16.25%	76.38%	72.43%
3.5.2.1(train)	6.51%	66.75%	79.58%

表 2　バックグランドページが存在する場合の Web ページの特定率
Table 2　website identification when background is exist

	16	32	64	100
arracry	67%	50%	41%	34%

成したトラフィックを 3 種類，「positive time separate」，「zero time separate」，「negative time separate」に分けている．これらについては，第 5 章で説明する．また，Wang はトラフィックを Web ページ事により，分割する方法を提案した．

4. WF 攻撃

Web サイトの「Fingerprint」として，一般的に「HTTP クッキー」，ACCEPT ヘッダなどがあげられる．しかし，Tor ネットワークの場合，ネットワーク中の通信が暗号化され，利用できる「Fingerprint」は，「パケットの転送時間」，「パケットの転送サイズ」，「パケットの向き」のみであり，Web ページの特定が困難である．WF 攻撃は 2 種類に分けることがあり，この 2 つとは Close-world test と Open-world test である．

4.1 Close-world test

攻撃者にとって，Web ページは 2 種類がある．Monitored Web ページと Unmonitored Web ページである [11]. Monitored Web ページは，攻撃者に注目している Web ページであり，ユーザが Monitired Web ページへアクセスすると，アクセスした Web ページが攻撃者に特定される可能性が高い．一方，Unmonitored Web ページは，攻撃者が注目しおらず監視されない Web ページである．Close-world test は，Monitored Web ページのデータを利用し，ユーザがアクセスした Web ページを特定することである．一般的に，Close-world setting を利用し各 Web ページの特定手法の精度への検証として使用する場合が多い．

4.2 Open-world test

Open-world test は，Monitored Web ページのデータと Unmonitored Web ページのデータの両方とも使用し，ユーザがアクセスした Web ページの特定ではなく，ユーザがアクセスした Web ページを Monitored Web ページと Unmonitored Web の種類によって分類する，なお，ユーザが，攻撃者が知らない Web ページへアクセスする場合，

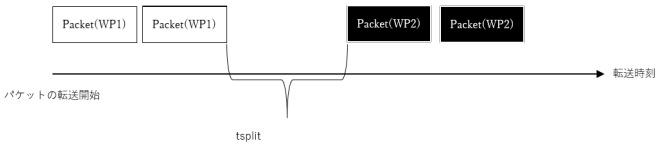

図 2　t_{split}
Fig. 2　t_{split}

アクセスした Web ページを，Monitored Web ページと Unmonitored Web の種類によって分類できる．

4.3 複数へアクセスの WF 攻撃

本論文は，同時に複数の Web ページへアクセスする場合を，2 つの Web ページへのアクセスに限定して研究を行なう．3 つ以上の Web ページへの同時アクセスは考慮しない．以後，本論文では，2 つの Web ページへアクセスを複数の Web ページへのアクセスと呼ぶ．

同時に複数の Web ページへアクセスする時，ネットワーク中のトラフィックが t_{split} の値に基づき 3 種類に分かれている．t_{split} は，最初にアクセスした Web ページによって生じるトラフィックにおける最後尾のパケットの送受信時刻 (t_{first}) と，次からアクセスした Web ページによって生じたトラフィックにおける前頭の受信パケットの送受信の時刻 t_{second} の差である．つまり，以下の数式で定義される．

$$t_{split} = t_{first} - t_{second} \quad (1)$$

ここで，positive time separate，zero time separate，negative time separate は次のように分類される．

- t_{split} の値は 1 秒より大きくなる場合に，トラフィックは positive time separate とする．
- t_{split} の値は 0 秒から 1 秒の間になると，トラフィックは zero time separate として分類する。
- t_{split} の値はマイナスの場合に，トラフィックは negative time separate として分類する。

これらの種類に対して解決方法が提案されている．これを説明する．

- **Time-based splitting :** positive time separate のように (詳細は第 5 章で説明する)，2 つの Web ページを時間順にアクセスし，また，各 Web ページのトラフィックは重なり合う状況が発生しない場合，Time-based splitting 法で対応する．Time-based splitting はネットワーク中のトラフィックを，t_{split} 図 2 にあるように，トラフィック Web ページ毎によって，2 つに部分を分割する．
- **Classifcation-based splitting:** t_{split} 時間の長さは，トラフィックの分割精度において影響を与える．t_{split} 時間は長くなると，分割精度が高い，一方，t_{split} 時間は短くなると，トラフィックの分割精度が落ちる．

トラフィックの分割精度が高くなると Web ページの特定率が上がる．しかし，同時に複数の Web ページへのアクセスの場合に，トラフィック中の t_{split} の多くは，1 秒より短くなり，さらに存在しない時もある．この時 Time-based splitting で対応すると，有効にならない．classifcation-based splitting は，t_{split} の有無を判断できない状況のために提案されたトラフィックの分割手段である．classifcation-based splitting は，Tor ネットワークのような通信が暗号化された匿名性ネットワークに対して，トラフィック中に利用できる 3 つの「Fingerprint」(「パケットのサイズ」,「パケットの受送信時間」,「パケットの向き」) と，前後のパケットとの関係についてなど 24 個の「Fingerprint」を利用する．そして，24 個の「Fingerprint」により，同時に複数の Web ページへアクセスする場合に，生成したトラフィックを Web ページ毎により分割する．

5. 実験の準備

5.1 トラフィックの種類

本章は，複数の Web ページへアクセスする場合に，ユーザの Web ブラウジング操作により，ネットワーク中に生成した 3 種類のトラフィックについて説明する．

- **Positive time separate:** 同時に 2 つ Web ページへアクセスする場合，最初の Web ページが閉じてから，t_{split} 時間に経た後，2 つ目の Web ページを開くという操作で生成したトラフィックである．一般に，positive time separate に対して，time-based splitting 法で，パケットの流れを分割する．先行研究に，positive time separate のトラフィックの分割する精度が 92%になり，本研究は positive time separate を扱わない．
- **Zero time separate:** Positive time separate と同様に，2 つの Web ページへアクセスする場合に生成したトラフィックである．Positive time separate と異なる点は，2 つのトラフィックの間に t_{split} はなし，または 1 秒より短くなっている．この状況は，主に Web ページの内部リンクによる Web ページの移動によりおきる．
- **Negative time separate:** 同時に 2 つの Web ページへアクセスする．この操作により，2 つ Web ページのトラフィックがネットワーク中に重なり合いになっている．Negative time separate はトラフィックの分割において，困難な状況である．Time-based splitting や classification based splitting のどちらを使用しても，トラフィックをうまく分割できない．本論文は negative time separate と zero time separate に対して，トラフィックの分割精度を向上させることを目指す．また分割精度が上がらない原因を調べる．

5.2 境目について

2 つのトラフィックの境目の大部分は，2 番目の Web ページへアクセスする場合，ネットワーク中に生じたトラフィック中の先頭のアウトプットパケットである．このパケットにより，トラフィックを時間順で 2 つの部分に分けることが必要である．前述した通り，同時に複数の Web ページへアクセスする場合に，ネットワーク中に生成したトラフィックを，Web ページ毎により分割することが重要である．

5.3 データ収集

データ収集であるパケットのキャプチャーは，2021 年 1 月 10 日から 2021 年 1 月 23 日の間に実施した．そして，プログラムの作成を Python3.7 により行なった．さらに，selenium を利用して自動 Web ページブラウジングのシステムを開発する．Selenium のバージョンは 3.141.0 である．加えて，パケットのキャプチャーは Wireshark の内蔵プログラムである tshark でパケットのキャプチャー実現する．Selenium と tshark の結合によって自動 Web ページへアクセスする同時にパケットのキャプチャプも実行できる．

複数の Web ページへアクセスする場合に，Web ページの所属している Web サイトが異なる状況に対して，境目の特定率の変化を研究するために 20 種類の Web サイトがある．本実験に，ニュースサイトと動画サイトが使用される．動画サイトの内容は動画と画像に構成されている．一方，ニュースサイトの Web ページは基本的に文字からなる．ほとんど類似しないため，誤差が少ない．そして，境目の特定は機械学習を利用して実施する．もし，トレーニングデータとテストデータを収集する時，異なるバージョンの Tor ブラウザが使用されると，境目の特定率に与える影響を研究するために，Tor ブラウザを 8.0.9，9.4.10，10.0.8 の 3 つのバージョンを利用する．

5.4 データ内容

この実験を実施した Web サイトフィンガープリンティング攻撃は，Tor ユーザ側 (クライアント) からエントリーノードまでの回線のキャプチャーデータを元に，Web サイトの「Fingerprint」を利用して Tor ユーザは Tor ブラウザでアクセスした Web ページを判定する．「Fingerprint」として「パケット送受信の順序」と「パケット長」と「パケット転送時間」は，ネットワークの通信が暗号化された場合でも有効である．この 3 つの「Fingerprint」から派生した 24 個の「Fingerprint」を利用して同時に複数の Web ページへアクセスする場合，ネットワーク中に生じたトラフィックを Web ページ毎により，分割するための境目を特定する．

(1) 同時に複数の Web ページへ 60 回程度アクセスし，パケットをキャプチャーする．

(2) キャプチャーしたパケットを 24 個の「Fingerprint」によるデータ整形を行い，「Fingerprint」にする．毎回にキャプチャーしたデータをログファイルに保存し，データとする。また，データ中のパケットを 24 の「Fingerprint」により，データを整形する。

(3) k-NN 法 (k-nearest neightbor algorithm) を利用し整形したデータに対して，境目であるかによって分類する．

24 個の「Fingerprint」について説明する。

- 最初のパケット 5 つパケットの転送時間 (Fingerprint」は 5 個)
- パケットのネットワーク中に転送時間の平均値 (Fingerprint」は 1 個)
- 送受信の最初のパケットと最後のパケットそれぞれ 15 個の中で転送時間が最も長いパケットの転送時間 (Fingerprint」は 2 個)
- 送受信の最初のパケットと最後のパケットそれぞれ 15 個目の転送時間 (Fingerprint」は 2 個)
- 最後のパケットの受信時刻 (Fingerprint」は 1 個)
- 送受信の 2 つのパケットを 1 つの組として，さらにそう送受信の時刻により，個々組の送受信の時間差を計算したもの (Fingerprint」は 9 個)
- 送受信のパケットの最初と最後のパケット 5 つのうちの受信パケットの数と，最初と最後のパケット 10 つのうちの受信パケットの数 (Fingerprint」は 4 個)

6. 実験

本章でに，実験の結果を示す．同時に複数の Web ページへアクセスする時，トラフィック中の境目を特定するために前述に紹介した 24 個の「Fingerprint」を特徴として k-NN アルゴリズムで計算し境目を特定する手法を実行する．また，zero time separate と negative time separate のにおける実施した結果を示す．

境目の特定は 2 種類がある．Decision と Find である．

- **Decision:** すべてのデータにおいて境目の有無を識別することである．正しく検出する場合に X_i は 1 になる．一方，検出が失敗すると，X_i は 0 になる．データ中の複数のパケットは，送受信の順序によって並べる．i は，パケットの順位である．n はデータ数とする．公式 (1) の通りに計算すし，結果は表 3 にある．結果として，Web ページの Web サイトは同様や，Web ページの Web サイトは異なるなどの条件が変わると，「Find」の結果は 99%である．実験によると，境目の有無はトラフィックの種類に関係がないことを示す．

$$P = \frac{1}{n}\sum_{i=1} X_i \tag{2}$$

結果は表 4 に示している．境目の有無はトラフィックの種類に関係がない．

- **Find:** 24 個の「Fignerprint」を利用する k-NN 法による境目の位置を特定することである．境目を正しく特定すると，Z_i は 1 になる．一方，特定は失敗の場合に，Z_i は 0 になる．TP(True positive) を計算するとき，Y_i は一斉に 0 になる．結果を表 4 に示す．

$$P = \frac{1}{n}\sum_{i=1} Z_i + Y_i \tag{3}$$

FP + FN(False positive かつ False negative) は，境目の特定が誤りになることを表す．境目の位置を正しく検出する時，Y_i は 1 になる．失敗すると，Y_i は 0 になる，FP + FN を計算する時，Z_i は一斉に 0 になる．結果は表 5 に示している．

表 3 Web サイトと Web ページ内容による「Decision」の特定率
Table 3 Decision's Probability of verious Website or content.

	positive	zero	negative
同サイト, 内容類似	99.0%	99.0%	99.0%
異サイト, 異内容	99.0 %	99.0%	99.0%
異サイト, 内容類似	99.0%	99.0%	99.0%

表 4 Web サイトと Web ページ内容による「Find」の特定率 (TP)
Table 4 Find's (TP) of verious Website or content.

	zero	negative
同サイト，内容類似	49.3%	70.9%
異サイト，異内容	72.9%	84.3%
異サイト, 内容類似	45.3%	68.4%

表 5 Web サイトと Web ページ内容による「Find」の特定率 (FP+FN)
Table 5 Find's (FP+FN) of verious Website or content.

	zero	negative
同サイト，内容類似	20.4%	1.6%
異サイト，異内容	27.5%	2.5%
異サイト, 内容類似	23.0%	4.6%

7. 考察

第 6 章の実験結果によると，同時に複数 Web ページへアクセスする場合に，Web ページの所属 Web サイトの差異により，境目の特定率における影響があるとわかった．双方の Web ページが同じ Web サイトに所属するとき，境目の特定率は 49.3%になる．一方，2 つの Web ページの所属 Web サイトが異なる場合の境目の特定率は，72.9%である．Web サイトが同じに比べ，異なる時に境目の特定率は，より精度が高まるとわかったが，この結果の理由は分からない．そこで，その原因を探究するために対照実験を行った．対照実験の内，Web ページの内容と所属 Web サイトという 2 つの条件を通して境目の特定率が低下する原因がわかった．表 6 はその結果である．Web サイトが異なる時に内容が似ていると，境目の特定率は 45.3%である。Web サイトが異なり，内容が似ている状況とほぼ同じ結果

表 6　Web サイトと Web ページ内容による「Find」の特定率 (TP)
Table 6　(TP)verious Website or content.

	同 Web サイト 内容類似	異 Web サイト 異内容	異 Web サイト 同内容
精度	49.3%	72.9%	45.3%

表 7　地理的な距離による Web ページの特定率の変化
Table 7　Probability(TR) of verious location distance

	日本	アメリカ	英国
精度	49.98%	48.3%	16.3%

表 8　To r ブラウザのバージョンによる境目の特定率 (TR)
Table 8　Probability(TR) of use verious browser' version.

	8.0.9(test)	9.4.10(test)	10.0.8(test)
8.0.9(train)	99.0%	67.1%	66.6%
9.4.10(train)	48.2%	99.0%	38.0%
10.0.8(train)	68.8%	68.7%	99.0%

となった．従って，境目の特定は Web サイトに関係がなく，Web ページの内容とすることがわかった．

送信先の Web サーバの国が違う場合の境目の特定率を表 7 が示している．本論文では，Web サーバの所在国により，同時に複数の Web ページへアクセスする場合に，アクセスした Web ページの特定率を考察する実験を行なった．国は日本，米国，英国である．結果として，境目の特定率が最も低いのは英国であり，16.3%になる．日本とアメリカの結果それぞれには 49.98%と 48.3%になり，ほぼ同じである．国別により境目の特定における影響があると考えられるが，実際には，世界に Tor ノードは 8000 台あり，世界の各地域に散らばれている．且つ，ミドルノードとイグジットノードは，常に変更されることから，Web ページの特定率は国別より，イグジットノードから Web サーバまでの距離に影響されると考えられる．

TBB(Tor ブラウザのバージョン) による特定率の変化を考察する実験について，パケットキャプチャーにおいて使用した Tor ブラウザのバージョンは，教師データとするパケットをキャプチャーする時に使用した Tor ブラウザのバージョンと同じになる．また，異なる場合に，複数の Web ページへアクセスする時，アクセスした Web ページの特定率を調べた．結果は表 8 と表 9 に示している．表 8 は，「Identiry」の TP（True Positive）の結果である．一方，「Identiry」の TP（True Positive）の結果について表 9 に示している．実験の実施において使用された Tor ブラウザにそれぞれ 3 つのバージョンがある．10.0.8，9.4.10，8.0.9 である．注意すべき点は，8.0.9 バージョンの Tor ブラウザによりキャプチャーしたデータを教師データとする時，Web ページの「Decision」による特定の失敗率（FN+FP）は異常に目立つ．理由は，Tor ブラウザは 8.0.9 以後，新しい制御技術が追加されたと考えられる．

表 9　To r ブラウザのバージョンによる境目の特定率 (FN+FP)
Table 9　Probability(FP+FN) of use verious browser' version.

	8.0.9(test)	9.4.10(test)	10.0.8(test)
8.0.9(train)	54.6%	55.3%	91.9%
9.4.10(train)	20.1%	21.3%	25.6%
10.0.8(train)	23.6%	25.4%	50.6%

8. おわりに

今回の実験によって，同時に複数の Web ページへアクセスする場合に，ネットワーク中のトラフィックをそれぞれに従属する Web ページによって分割しているもの境目を特定の研究を行った．さらに，境目の特定精度に影響を与える要因について，Web サイト，Web ページの内容，イグジットノードと送信先サーバに所在の地理的な距離，さらに Tor ブラウザのバージョンの 4 つから示した．しかし，WF 攻撃として 70 %と 80 %程度の成功率は良いとは言えない．やはり，境目の特定精度を上昇させるため，より優秀な手法を開発する必要がある．これは今後の課題とする．

参考文献

[1] Tao W. and Xiang C. : Effective attacks and provable defenses for website fingerprinting, Proceedings of 23rd USENIX conference on Security Symposium(2014).
[2] Marc J., and Sadia A. : A Critical Evaluation of Website Fingerprinting Attacks, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security(2014).
[3] Andriy P. and Fabian L., Andreas Z. : Website Fingerprinting at Internet Scale, Proceedings of the 23rd Internet Society (ISOC) Network and Distributed System Security Symposium(2016).
[4] Andriy P., Lukas N., Andreas Z. : Website fingerprinting in onion routing based anonymization networks, Proceedings of the 10th annual ACM workshop on Privacy in the electronic society(2011).
[5] Dominik H. and Rolf W., Hannes F. : Website fingerprinting:attacking popular privacy enhancing technologies with the multinomial naive-bayes classifier, Proceedings of the 2009 ACM workshop on Cloud computing security(2009).
[6] S. M. and G. D. : Low-cost traffic analysis of Tor, Proceedings of the 2005 IEEE Symposium on Security and Privacy (S&P'05)(2005).
[7] Xiang C. and Xin Z., R. J. : Touching from a Distance: Website Fingerprinting Attacks and Defences, Proceedings of the ACM Conference on Computer and Communications Security(2012).
[8] Jamie H. and G. D. : k-fingerprinting: A Robust Scalable Website Fingerprinting Technique, Proceedings of the 25th USENIX Conference on Security Symposium(2016).
[9] Tao W. and I. G. :Improved Website Fingerprinting on Tor, Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society(2013).
[10] Y. X. and Tao W., Q. L., Q. G., Y. C., Y. J. : A Multi-tab Website Fingerprinting Attack, Proceedings

of the 34th Annual Computer Security Applications Conference(2018).
[11] 阿部 航太 : 畳み込みニューラルネットワークによる Tor 上の匿名 Web 通信の識別，早稲田大学 (2017).