Torネットワークにおける悪用ユーザ特定手法の検討

宗 裕文[1]　横山 絵美里[1]　川端 良樹[1]　久保田 真一郎[1]　岡崎 直宣[1]

概要：近年，利用者がアクセスしたWebサイトが特定されてしまうことを防ぐ匿名通信システムが注目されている．その中で最も普及しているのがThe Onion Routing（Tor）である．Torは健康相談や電子投票等の，誰がどこに送信したか，ということを知られたくない場合の情報交換に利用されることを本来の目的としているが，違法行為を匿名で行う目的で悪用ユーザに利用されるケースがある．このことが，多くの善良なユーザが本来の目的でTorを利用することを妨げることにつながっていると考えられる．そこで本稿では，悪用ユーザの利用を抑制するために，悪用ユーザに利用されることの多い情報を扱うWebサイトを模擬するサイトを導入し，そのサイトと協調動作をすることで，高い確率で悪用ユーザを特定する手法を提案する．実験により，従来の不特定のサイトの指紋情報を用いる方法と比較し，提案手法の効果を検証する．

キーワード：匿名化通信，不正利用抑止，The Onion Routing

An examination on the abusing user identification method of the Tor anonymity system

Abstract: The Onion Routing (Tor) is the most famous anonymity system supporting the anonymous transport of TCP stream over the Internet. Tor provides the foundation for applications to communicate over public network without compromising their privacy. However, in some cases, it is used by abusing users, for the antisocial purpose. This has prevented the increase of "good" user of the Tor system. In this article, we propose a method for identification of the abusing user of the Tor anonymity system. In the proposed method, Tor system cooperate with Web sites that simulate sites dealing with illegal information, and uses the fingerprint information of the Web sites to identify the users accessing the sites.

Keywords: Anonymous Comunication, Abuse Suppression, The Onion Routing

1. はじめに

現在，インターネットは私たちの生活に欠かせないものになっている．しかしながら，インターネットを利用する上で，パケットのヘッダ情報を盗聴し利用者がアクセスしたWebサイトが特定されてしまうことが問題になっている．この対策として匿名通信システムが注目されている．匿名通信システムにはMix-NetやCrowdsなどあるがその中で最も普及しているのがThe Onion Routing(Tor)である．Torは健康相談や電子投票等の，誰がどこに送信したか，ということを知られたくない場合の情報交換に利用されることを本来の目的としている．しかし，Torは違法行為を匿名で行う目的で悪用ユーザに利用されるケースがある．このことが，多くの善良なユーザが本来の目的でTorを利用することを妨げることにつながっていると考えられる．

本稿では，おとりとなるWebサイトを導入し，そのWebサイトと協調動作をすることで，悪用ユーザを特定する手法を提案する．そして，実験により，従来の不特定のサイトの指紋情報を用いる手法と比較し，提案手法の効果を検証する．

2. The Onion Routing(Tor)

2.1 概要

Torとは，元々アメリカ海軍調査研究所（USNRL）[1]により開発された，低遅延の匿名化通信技術である．Torの

[1] 宮崎大学
University of Miyazaki

一日あたりの利用者数は，2012 年 8 月から 2013 年 8 月の間およそ 50 万人程度で推移しており，現在最も利用されている匿名化技術である．Tor は複数のプロキシを経由させるオニオンルーティングと呼ばれる仮想回線接続により匿名性をもつ通信を実現している．

ここで Tor の仕組みを図 1 に示す．Tor は図 1 のように Tor ネットワークから無作為に選ばれた三つのプロキシ（以下，OR）を経由し Web サイトへアクセスする多段プロキシ・システムである．本稿では，ユーザに最も近い OR を入口 OR と呼び，Web サイトに最も近い OR を出口 OR，入口 OR と出口 OR の間にある OR を中間 OR と呼ぶこととする．Tor では，経由する OR は常に切り替えられ，経由した OR を特定することは難しい．また OR 間の通信は暗号されているため，盗聴を防ぎ安全な通信を可能としている．

Tor は上記のような仕組みにより高い匿名性のある通信を実現できるが，様々な要因によりその匿名性が崩れることがある．例えば，幾つかの OR が Tor の匿名性を低下させようとする者（以下，攻撃者）により占拠（以下，汚染）された場合，Tor の匿名性が失われることがある．

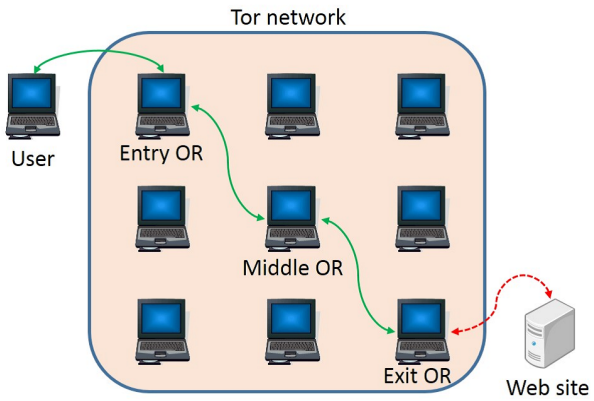

図 1　Tor の仕組み
Fig. 1　Structure of Tor

2.2　Tor のユーザ

現在 Tor は軍，ジャーナリスト，警察官，人権活動家などの人々によって様々な目的のために利用されている．例えば，ジャーナリストは，より安全に不正の告発者や反体制派の人らと接触する為に Tor を利用し，人権活動家は危険地帯からの情報発信する為に Tor を利用している．

ところが，上記の本来の用途以外に，海外では Tor が児童ポルノ画像をやり取りする際や違法薬物の取引サイトへのアクセスに使われたり，また日本国内においては，殺人予告，不正アクセス，パソコンの遠隔操作や警視庁国際テロ捜査情報流出事件に Tor が利用されたりしている．本稿ではこれらの違法行為を匿名で行う目的のユーザを「悪用ユーザ」，それ以外を「正規ユーザ」と呼ぶこととする．

米国家安全保障局（以下，NSA），並びに日本の警察庁は悪用ユーザに対して様々な対策をしている．まず，NSA は Firefox の脆弱性を突いて悪用ユーザのパソコンにマルウェアを感染させた．そして，悪用ユーザのホスト名・MAC アドレスを取得することで，悪用ユーザを特定していた．次に日本の警察庁は，Tor からのアクセスをブロックするようにサイト管理者に協力を求めている．最近ではこのようなニュースが度々放送されるようになり，一般の人々は Tor に対して良い印象を持っていない．一般の人々の中には Tor というものは悪いことをする為に使用するものだと思い込んでいる人もいるかもしれない．このままでは Tor の正規ユーザが減り，匿名通信技術自体も衰退していく恐れがある．

そこで，本論文では悪用ユーザの利用を抑制することを目的に悪用ユーザを特定する手法を提案する．これにより Tor に対する印象が改善し，Tor の正規ユーザが増加することを期待している．

本研究では，Tor の匿名性を下げる目的である利用者特定手法を参考にする．次章では Tor における利用者特定手法について説明する．

3.　利用者特定手法

本章では利用者特定手法を紹介する．ここで紹介する手法は元々は攻撃者によって行われる攻撃手法であるが，適用方法によっては本研究の目的にも利用できると考えられる．

(1)　タイミングを利用した手法

タイミングを利用した手法とは二つの経路の同一性を判定する手段である．ここに入口 OR に繋がった送信者 A の経路 I と出口 OR に繋がった受信者 B の経路 J という二つの経路があるとする．[2] の手法では，攻撃者は入口 OR と出口 OR を汚染し各 OR を流れるトラフィックを解析する．そして，入口 OR と出口 OR で生じた通信に，時間差で強い相関が観測できたとする．その入口 OR と出口 OR の強い相関は，入口 OR を始点とする経路 I と出口 OR を終点とする経路 J が同一の経路であることを示している．そして，経路 I=J であれば，送信者 A は受信者 B にメッセージを送っていた事が分かる．

タイミングを利用した手法は入口 OR と出口 OR を汚染しなければならず実現可能性が低い．

(2)　エラーを利用した手法

エラーを利用した手法とは，Tor の暗号化の仕組みを利用してエラーを発生させて，それを利用して利用者がアクセスしている Web サイトを特定する手法

である．[3] は，入口 OR は利用者から送られてきたパケットを複製（以下，複製パケット）し，複製元パケットと複製パケットを出口 OR まで送信する．Tor では AES の CTR モードを使用しているため，出口 OR でパケットを復号する際に，エラーが発生する．出口 OR がエラーを認知すると入口 OR と出口 OR は同一上の経路にあると判断できる．

エラーを利用した手法もタイミングを利用した手法と同様で二ヵ所を汚染しなければならず実現可能性が低い．

(3) Web サイトの指紋情報を利用した手法

Web サイトの指紋情報を利用した手法とは，Web サイトにアクセスした際のトラフィックに含まれるサイト独自の特徴（以下，指紋）に着目しそれを観測することで利用者がアクセスした Web サイトを特定するという手法である．

[4] は，機械学習を併用した手法である．指紋情報には，パケットの総数，HTML ファイルのサイズなど，Web サイトから抽出できるような情報を用いている．また，指紋情報の分類には，Support Vector Machines(SVM) を使用している．[4] は 54% の確率で Web サイトを特定できることが示されている．

[5] は Tor に Web サイトの指紋情報を利用した手法の対策をされたとしても有効な手法である．これは，Web サイトの指紋情報を利用した手法の対策としてトラフィックに様々な加工を施された場合でも，それらの加工を打ち消すトラフィック逆加工を行うことで，対策を無効化するものである．[5] では，Web サイトの指紋情報を利用した手法の対策がされた Tor に対しても利用者がアクセスした Web サイトの特定が可能であり，75% 以上の確率で Web サイトを特定できることが示されている．

Web サイトの指紋情報を利用した手法は入口 OR を汚染するだけでよく，実現可能性が高い．しかし，利用者がアクセスした Web サイトを特定する確率が高くない．

(4) 特徴的なトラフィックを利用した手法

特徴的なトラフィックを利用した手法とは，入口 OR と出口 OR を汚染し出口 OR が特徴的なトラフィックを利用者へ送信し，そのトラフィックを入口 OR が観測することで利用者を特定する手法である．

[6] では，出口 OR が，トラフィックのパケット数を変化させることで信号を含め利用者へ送信する．信号を含んだトラフィックを，入口 OR が認知することで，Web サイトへアクセスした利用者を特定することができる．この手法では 65% から 100% の確率で Web サイトを特定できることが示されている．

[7] は出口 OR がトラフィックに直接拡散方式の疑似ノイズを含ませることによって特徴的なトラフィックにしている．疑似ノイズを用いることで，攻撃が行われているかどうかの判断が難しいため，対策が困難となる．

特徴的なトラフィックを利用した手法は Web サイトを特定する確率は高いが二ヵ所を汚染しなければならず実現可能性が低い．

4. 提案手法

4.1 概要

本提案手法では悪用ユーザがアクセスしそうなおとりとなる Web サイト（以下，おとり Web サイト）を導入し，そのサイトと入口 OR が協調動作をすることで，特徴的なトラフィックを利用した手法の実現可能性が低いというデメリットを解決し，特徴的なトラフィックを悪用ユーザに送信する．このことにより実現可能性が高く，高い確率でおとり Web サイトにアクセスした悪用ユーザを特定することを目指す．

以下で図 2 を用いて本提案手法の動作手順を説明する．ここで管理者 OR とは悪用ユーザを抑制したい立場の Tor 管理者が入口 OR に位置した OR である．

『提案手法の流れ』

(1) おとり Web サイトは悪用ユーザからアクセス要求がきたことを確認する．

(2) おとり Web サイトはパケットキャプチャを開始する．

(3) 管理者 OR にパケットキャプチャを開始するように指示する．

(4) 管理者 OR はパケットキャプチャを開始する．

(5) 悪用ユーザへ応答を返す．

(6) おとり Web サイト側のキャプチャデータと管理者 OR 側のキャプチャデータを比較して悪用ユーザを特定する．

4.2 前提条件

Tor ネットワークで用いられる役割に応じた条件を表 1 に示す．

以上の条件を元に，次節で提案手法の動作手順を示す．

4.3 動作手順

提案手法のアルゴリズムはおとり Web サイトを作成す

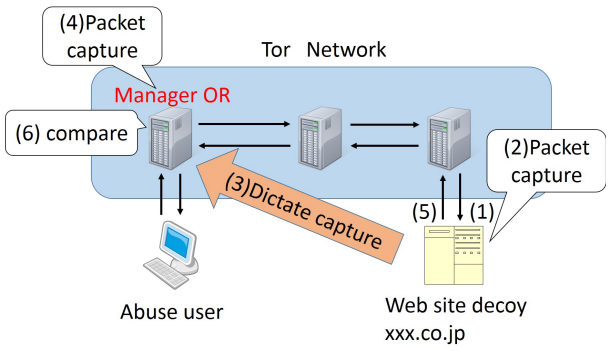

図 2　提案手法の概略図
Fig. 2　The schema of proposal technique

表 1　前提条件
Table 1　A precondition

役割	条件
クライアント	特になし
入口 OR	Web サイトの指紋情報を利用した手法における汚染 OR の役割を持ち，情報を抽出できる
中間 OR	特になし
出口 OR	特になし
Web サイト	PKI で認証されていない，悪用ユーザがアクセスするような，コンテンツを持っている

るおとり Web サイト作成フェーズ，図 2 の (3)，(4) の処理に当たる協調動作フェーズ，図 2 の (6) の処理に当たる悪用ユーザ決定フェーズの三つに分けられる．

以下でそれぞれのフェーズについて詳しく説明する．

(1)　おとり Web サイト作成フェーズ

おとり Web サイトには現実の Web サイトと区別をつけるために信号を含ませる．この信号とは特徴的なトラフィックであり，これを観測することでおとり Web サイトを一意に判別できるものとする．信号を含める前後のトラフィックの様子を図 3 と図 4 に示す．図 4 の 55 秒から 80 秒の間のパケット通信が通常のサイトと区別をつけるための信号である．提案手法では，おとり Web サイトがこのような信号をトラフィックに含め，管理者 OR でそれを受け取ることで利用者が当該おとり Web サイトを利用したことを判断している．以下でおとり Web サイト作成の手順を示す．

『おとり Web サイト作成の手順』

(a)　Web サイトの作成
Tor の管理者は悪用ユーザがアクセスしそうなサイトを作成する．

(b)　ダミーコンテンツに含ませる遅延の設定
まず，ダミーコンテンツの数 N とそれぞれのサイズ S_i を定義する．次に，それぞれのダミーコンテンツを送信する待ち時間 T_i（秒）を設定する．そして，おとり Web サイト本来のコンテンツを送信した後，それぞれのダミーコンテンツを T_i だけ待って送信する．
例えば，図 4 は N=3, S_1=S_2=S_3=300(KB), T_1=30, T_2=40，T_3=50 と設定した場合の信号である．

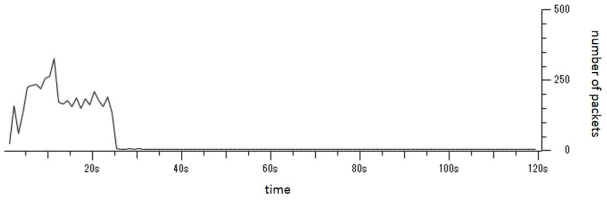

図 3　信号なし
Fig. 3　The graph which does not include a signal

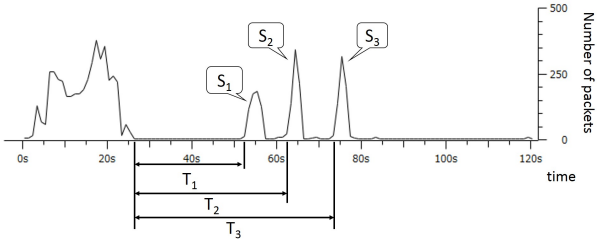

図 4　信号あり
Fig. 4　The graph which include a signal

(2)　協調動作フェーズ

協調動作フェーズの挙動を以下に示す．

『協調動作フェーズ』

(a)　悪用ユーザからおとり Web サイトにアクセス要求があった時，おとり Web サイトはパケットキャプチャを開始する．

(b)　管理者 OR にユーザと管理者 OR 間のパケットをキャプチャするように指示する．

(c)　管理者 OR はキャプチャを開始する．

(3)　悪用ユーザ決定フェーズ

協調動作フェーズで収集したユーザと管理者 OR 間のキャプチャデータと出口 OR とおとり Web サイト間のキャプチャデータからグラフを作成する．そして，このふたつのグラフを比較し類似していれば悪用ユーザはおとり Web サイトへアクセスしたのが分る．

図 5 はおとり Web サイトにアクセスした時のおとり Web サイトで観測したパケットをグラフで表したものである．また，図 6 は管理者 OR でパケットの観測した結果を表したものである．この二つのグラフを比較する指標として相関係数を用いる．相関係数と

は二つのデータ間の類似性の度合いを示す指標である．相関係数が 1 に近いほど正の相関があり，ゼロに近ければ無相関であり，−1 に近ければ負の相関がある．相関係数 r の算出方法を数式 1 に示す．ここで，$f_1(t)$，$f_2(t)$ はそれぞれ図 6，図 5 のようなグラフを表している．そして，$f_1(t)$，$f_2(t)$ の平均値をそれぞれ avg_1，avg_2 と表す．また，N は観測したデータのサンプリング数である．また，相関係数 r には表 2 のような基準が設けてある．

$$r = \frac{\frac{1}{N}\sum_{t=1}^{N}(f_1(t) - avg_1)(f_2(t) - avg_2)}{\sqrt{\frac{1}{N}\sum_{t=1}^{N}(f_1(t) - avg_1)^2}\sqrt{\frac{1}{N}\sum_{t=1}^{N}(f_2(t) - avg_2)^2}} \quad (1)$$

表 2　相関係数の基準
Table 2　The standard of the coefficient of correlation

$\|0.7\| < r \leq \|1\|$	かなり強い相関がある
$\|0.4\| < r \leq \|0.7\|$	やや相関あり
$\|0.2\| < r \leq \|0.4\|$	弱い相関あり
$\|0\| \leq \mathrm{r} \leq \|0.2\|$	ほとんど相関なし

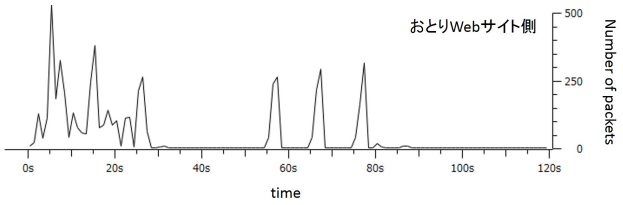

図 5　ハニーポット側で収集したデータグラフ
Fig. 5　The data graph which collected at the honeypot side

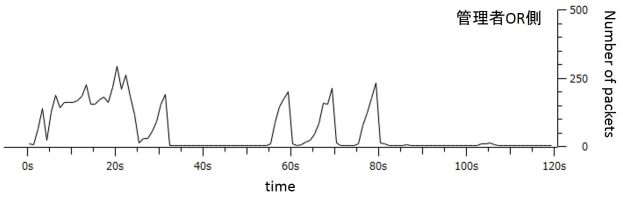

図 6　入口 OR 側収集したデータグラフ
Fig. 6　The data graph which collected at the entry OR side

5. 評価実験

本章では，利用者特定手法の中でも幅広く研究がされている Web サイトの指紋情報を利用した手法と提案手法の有効性を示すために評価実験を行う．

5.1 評価指標と評価対象

本論文では Web サイトにアクセスした悪用ユーザを特定することが目的であるため，全体特定率と Web サイト特定率で評価を行う．ここで，全体特定率とは，各 Web サイトへのアクセス回数に対する，アクセスした Web サイトの特定正解総数の割合である．また，Web サイト特定率とは，ある Web サイトへのアクセス回数に対する，アクセスした Web サイトの特定正解数の割合である．Web サイト特定率は Web サイトごとの特定率を表している．これらの特定率が高いほどユーザがどこにアクセスしたのか容易に分かることを示す．それぞれの特定率を求め，それらの値で評価する

本実験では，以下の手法において評価を行う．

- 提案手法
- Web サイトの指紋情報を利用した手法

ここで想定する Web サイトの指紋情報を利用した手法について述べる．この手法は，Tor ネットワークの攻撃者の入口 OR（以下，攻撃者 OR）を用いて利用者宛てに流れるトラフィックを収集できることを前提としている．また，あらかじめ攻撃者が事前に指紋情報のデータベース（以下，攻撃者データベース）を作成し，その攻撃者データベースを定期的に更新していくものとする．そして，利用者がアクセスした際に攻撃者 OR で収集される指紋情報を攻撃者データベースで比較し指紋情報が最も近いものを利用者がアクセスした Web サイトとする．

指紋情報は通信トラフィック総量，通信パケット数，通信トラフィック平均，通信トラフィック分散，通信チャンク平均，通信チャンク分散とする．ここで通信チャンクとは，パケットの向きが変わる度に，前回向きが変わった点から向きが変わる直前までのパケットを足し合わせたパケットのまとまりのことである．

5.2 実験環境

本提案手法と Web サイトの指紋情報を利用した手法の実験環境を表 3 に示す．

表 3　実験環境
Table 3　Experiment environment

CPU	Core2 Duo E8400 3.00GHz
OS	Windows 8 Pro
Browser	Mozilla FireFox 25.0.1
Tor のバージョン	v0.2.3.25
Perl のバージョン	ActivePerl 5.16.3
Apache	v2.4.6

実験に用いる Web サイトは，Web サイトのアクセスランキング付けを行っている Alexa [8] の上位から国ドメインだけが違うだけで同じサイトなどの重複をさけて 100 サイト選択した．また，Apache を利用し 100 サイトのサー

バを立てるため，著作権上の問題から現実のサイトを用いることができない．そこで，現実のサイトの HTML 及びその他コンテンツサイズ，コンテンツ数を元にダミーデータで Web サイトを作成した．また，パケットキャプチャには wireshark [9] を用いる．

5.3 実験方法

Web サイトの指紋情報を利用した手法と提案手法の実験方法を以下に示す．本実験では各比較対象の全体特定率を示す．提案手法では動画，検索，ショッピング，企業 HP，ニュースサイトの 5 種類から選択しておとり Web サイトを作成する．Web サイトの指紋情報を利用した手法と比較するために，Web サイトの指紋情報を利用した手法においても上記の 5 種類の Web サイトを選択する．そして，互いの各 Web サイト特定率で比較する．

(1) Web サイトの指紋情報を利用した手法

指定した URL をブラウザに入力すると，Tor プロキシ経由で接続される．この時の通信トラフィックを利用者側でパケットキャプチャすることで指紋情報とする．

本実験では全体特定率を T，Web サイト特定率を t としたときそれぞれ，$T = S/N \cdot M$，$t = s/M$ で表すことができる．ここで，N，M，S，s はそれぞれアクセスする Web サイト数，アクセス回数，全体の特定正解数，Web サイトごとの特定正解数である．本実験では $N = 100$，$M = 10$ とし 1000 データで攻撃者データベースを作成する．また，同様に利用者の指紋情報を 1000 データ用意する．この利用者の指紋情報にそれぞれ最も類似した指紋情報を攻撃者データベースから求める．そして，対応する Web サイトが本当に利用者のアクセスした Web サイトかどうか判断する．これを 1000 データ全てで行い，全体特定率及び Web サイト特定率を求める．

本実験では，簡単化のため利用者が Web サイトにアクセスする際に閲覧するページはトップページのみとする．閲覧時間については Tor を利用して Web サイトを閲覧する際，接続に時間がかかることや経路によって帯域が異なることを考慮した時間を設定する．上記の理由から本実験では閲覧時間を 2 分間に固定に設定する．

(2) 提案手法

本項では提案手法の実験方法について説明する．挙動は指紋情報型特定システムと同様であるが，パケットキャプチャするトラフィックが利用者の入出力に加え，Web site の入出力でも行う．

本実験では，5 つのおとり Web サイト及び 95 サイトのそれぞれに 10 回ずつアクセスした 1000 個のパケットキャプチャデータを用いる．そして，提案手法では全てのおとり Web サイトのキャプチャデータから相関係数 r 求め，r が 0.7 以上の Web サイトが当該おとり Web サイトかどうか判断する．相関係数の算出には R 言語の cor 関数を用いた．また，相関係数 r が 0.7 以上の Web サイトが複数存在した場合，正しく Web サイトを特定できていないとする．特定率の求め方は Web サイトの指紋情報を利用した手法と同様である．

各おとり Web サイトにおけるコンテンツ毎の遅延を表 4 に示す．また，各コンテンツサイズは全て 300KB とした．

表 4 各おとり Web サイトの遅延
Table 4 A delay of each web site decoy

おとり Web サイト	T_1	T_2	T_3
A（動画）	30 秒	40 秒	50 秒
B（検索）	20 秒	30 秒	40 秒
C（ショッピング）	10 秒	20 秒	30 秒
D（企業 HP）	30 秒	40 秒	50 秒
E（ニュース）	20 秒	30 秒	40 秒

5.4 実験結果

表 5 は提案手法と Web サイトの指紋情報を利用した手法の全体特定率を表している．また，図 7 の Proposal method は提案手法の各おとり Web サイトごとの Web サイト特定率を表している．また，Exsisting method は Web サイトの指紋情報を利用した手法の結果から各おとり Web サイトと同じ種類の Web サイトをそれぞれ一つずつ選択したときの Web サイト特定率を表している．図 7 の A,B,C,D,E はそれぞれ動画，検索，ショッピング，企業 HP，ニュースサイトの 5 種類から選択した Web サイトである．

表 5 Web サイトの指紋情報を利用した手法と提案手法の全体特定率
Table 5 The specific rate of two technique

手法	全体特定率
Web サイトの指紋情報を利用した手法	52%
提案手法	100%

6. 考察

表 5 より Web サイトの指紋情報を利用した手法では 52% の全体特定率を示した．一方，提案手法手法では 100% の全体特定率を示した．このことから，提案手法は非常に高い全体特定率を持ち，本研究の目的である悪用ユーザの特定に有効であることがわかる．

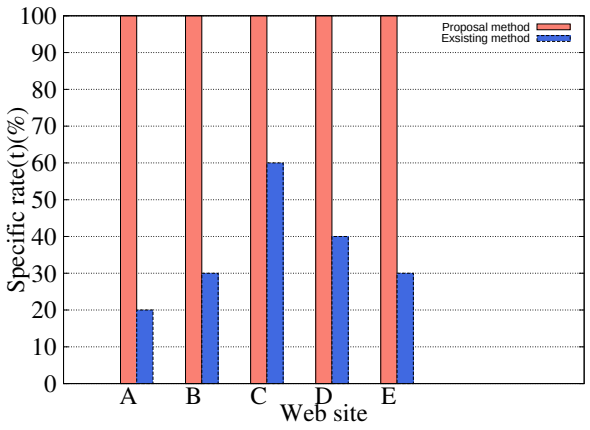

図 7　Web サイトごとの特定率
Fig. 7　The specific rate of two technique

図 7 において，どの種類の Web サイト特定率をみても Web サイトの指紋情報を利用した手法より提案手法の方が高いことが分かる．ここで，図 7 の Web サイトの指紋情報を利用した手法を見てみると動画サイトが最も低い特定率となっており，ショッピングサイトは最も高い特定率を示している．これは，Web サイトの指紋情報を利用した手法では，動画サイトは更新頻度が高いため指紋情報が頻繁に変化し特定率が低く，ショッピングサイトは指紋情報となりうるコンテンツが多いため特定率が高いと考えられる．一方，図 7 の提案手法では動画サイト，ショッピングサイトなど種類に依らず高い Web サイト特定率を示している．これは，提案手法では，Web サイトのコンテンツに依らない信号をトラフィックに含め，それにより Web サイトを特定しているためである．このような結果から，Web サイトの指紋情報を利用した手法は Web サイトのコンテンツによって特定率にバラつきが生じるが，提案手法はどのような Web サイトであっても常に高い特定率を示せることがわかる．

Web サイトの指紋情報を利用した手法は，常に高い特定率を維持することが難しいがどのような Web サイトにも適用できるため，悪用ユーザが特定システムから逃れることは難しい．一方，提案手法は悪用ユーザがおとり Web サイトを利用しなければ悪用ユーザを特定できないが，利用した場合は高い確率で特定できる．このように，Web サイトの指紋情報を利用した手法と提案手法はお互いのデメリットを補完し合えるシステムであるといえる．今後は，提案手法と Web サイトの指紋情報を利用した手法を組み合わせて利用することで，常に高い特定率を維持しつつ，悪用ユーザが特定システムから逃れられないようなシステムを提案していきたい，

7. まとめ

本論文では匿名通信システム Tor における悪用ユーザ特定手法の提案を行った．本提案手法は，入口 OR と，おとりとなる Web サイトが協調動作して悪用ユーザを特定するものである．また，利用者特定技術の中でも幅広く研究されている Web サイトの指紋情報を利用した手法と提案手法の比較評価を行った．その結果，Web サイトの指紋情報を利用した手法は Web サイトのコンテンツによって Web サイト特定率にバラつきが生じるが，提案手法はどのような Web サイトであっても常に高い Web サイト特定率を示せることが分かった．このことから，提案手法はおとり Web サイトを利用した悪用ユーザを高い確率で特定できること分かった．しかしながら，提案手法ではターゲットとなる Web サイトを模擬するサイトを用意する必要がある．今後は提案手法と Web サイトの指紋情報を利用した手法を組み合わせ適用範囲を広げる方法についても検討したい．

参考文献

[1] U.S.Naval Reserch Laboratory: U.S.Naval Reserch Laboratory(online), available from, (`http://www.nrl.navy.mil/`) (2014.01.31).
[2] Brian N. Levine, Michael K. Reiter, Chenxi Wang, and Matthew Wright: *Timing Attacks in Low-Latency Mix Systems (Extended Abstract)*, Proceedings of the 8th international financial cryptography conference (FC 2004), key west, fl, usa, february 2004, volume 3110 of lecture notes in computer science, pp 251-265.
[3] Ryan Pries, Wei Yu, Xinwen Fu and Wei Zhao: *A New Replay Attack Against Anonymous Communication Networks*, In ICC’08, page 1578-1582,(2008).
[4] Andriy Panchenko, Lukas Niessen, and Andreas Zinnen: *Website Fingerprinting in Onion Routing Based Anonymization Networks*, Proceedings of the 10th annual ACM workshop on Privacy in the electronic society pp.103-114, (2011).
[5] 横手 健一・松浦 幹太 (2012): 匿名通信システム *Tor* の安全性を低下させるトラフィック逆加工, コンピュータセキュリティシンポジウム 2012 論文集 巻：2012 号：3 ページ：624-631.
[6] Zhen Ling, Junzhou Luo, Wei Yu, Xinwen Fu, Dong Xuan, and Weijia Jia: *A New Cell-Counting-Based Attack Against Tor*, Networking,IEEE/ACM Transactions on, Vol.20, Issue.4, pp.1245-1261, (2012).
[7] Wei Yu, Xinwen Fu, Steve Graham, Dong Xuan, and Wei Zhao: *DSSS-Based Flow Marking Technique for Invisible Traceback*, Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp.18-32, (2007).
[8] Alexa: Alexa Top 500 Global Site, available from, (`http://www.alexa.com/topsites`) (2014.01.31).
[9] Wireshark: Wireshark, available from, (`http://www.wireshark.org/`) (2014.01.31).