# 匿名通信システム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]　山場 久昭[1]　久保田 真一郎[1]　朴 美娘[2]　岡崎 直宣[1]

**概要**：近年，ユーザがアクセスした 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．しかし，Tor 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．そこで本提案は，本来 Tor の匿名性を低下させようとする者が行う既存のユーザ特定手法を有効に利用することができないかと考えた．具体的には，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の IP アドレス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．

# An examination on the abusing user identification method of anonymous communication systems

Hirofumi Sou[1]　Emiri Yokoyama[1]　Hisaaki yamaba[1]　Shinichirou Kubota[1]　Mirang Park[2]
Naonobu Okazaki[1]

## 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，通信内容を盗聴することやパケットのヘッダ情報を盗聴しユーザがアクセスした Web サイトが特定されてしまうことが問題になっている．前者の対策として暗号化技術があり，これを利用することで通信内容を秘匿することができる．しかし，後者の問題については，ユーザがアクセスした Web サイトが特定されてしまうため暗号化技術では対策にならない．したがって，インターネットにおける発信元を突き止めるような問題に対して匿名性を保護することが必要である．

そこで，通信経路の秘匿を目的として考案されたプライバシー保護技術が匿名通信システムである．匿名通信システムには Mix-Net [12] や Crowds [13] などがあるが，最も普及しているのが The Onion Routing(Tor)[1] 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，悪用ユーザの IP アドレス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 の一日あたりのユーザ数は約 200 万人であり，現在最も利用されている匿名化技術である [14]．Tor は複数のプロキシ

1 宮崎大学
University of Miyazaki
2 神奈川工科大学
Kanagawa Institute of Technology

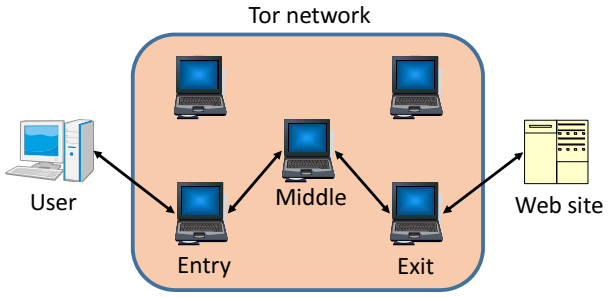


図 1　Tor の概略図
**Fig. 1**　Basic components in Tor

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．

Tor の仕組みを図 1 に示す．Tor は 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，オニオンルータ）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．ここで，三つのオニオンルータをユーザに近い側から順に，Entry オニオンルータ，Middle オニオンルータ，Exit オニオンルータと呼ぶ．Entry オニオンルータは，ユーザは分かるがユーザがアクセスしている Web サイトは分からない．また，Exit オニオンルータは，ユーザがアクセスしている Web サイトは分かるがユーザは分からない．このようにして Tor は匿名性を確保している．Tor では，経由するオニオンルータは常に切り替えられ，経由したオニオンルータを特定することは難しい．またオニオンルータ間の通信は暗号化されているため，盗聴を防ぎ安全な通信を可能としている．

### 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を発信する為に 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，パソコンの遠隔操作に 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．例えば日本の警察庁は，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 [2]．最近では，上記のように Tor が悪用されているという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おらず，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可能性がある．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の IP アドレス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が期待できる．本研究では，Tor の匿名性を下げる目的であるユーザ特定手法を参考に提案手法を考える．次章では Tor におけるユーザ特定手法について説明する．

## 3.　ユーザ特定手法

本章では既存のユーザ特定手法を紹介する．ここで紹介する手法は元々は Tor の匿名性を低下させようとする者（以下，攻撃者）によって行われる手法であるが，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．本論文では攻撃者により占拠されたオニオンルータを汚染オニオンルータと呼ぶこととする．

(1)　タイミングを利用した手法

二つのオニオンルータ間で強い相関性のあるトラフィックが観測できたとき，その二つのオニオンルータは同一上の経路にあると判断できることを利用した手法である．ここに Entry オニオンルータに繋がった送信者 $A$ の経路 $I$ と Exit オニオンルータに繋がった受信者 $B$ の経路 $J$ という二つの経路があるとする．[3] の手法では，攻撃者は Entry オニオンルータと Exit オニオンルータを汚染し各オニオンルータを流れるトラフィックを解析する．そして，Entry オニオンルータと Exit オニオンルータで生じた通信に，時間差で強い相関が観測できたとする．その Entry オニオンルータと Exit オニオンルータの強い相関は，Entry オニオンルータを始点とする経路 I と Exit オニオンルータを終点とする経路 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 Entry オニオンルータと Exit オニオンルータを汚染しなければならず実現可能性が低いという問題がある．

(2)　エラーを利用した手法

Tor の暗号化の仕組みを利用してエラーを発生させて，それを利用してユーザがアクセスしている Web サイトを特定する手法である．図 2 は送信者と受信者間の通信を確立した後，送信者が「Hello」というメッセージを受信者へ送信している時の流れを表したものである．[4] は，図 2 の $OR1$(Entry オニオンルータ) はユーザから送られてきたパケットを複製し

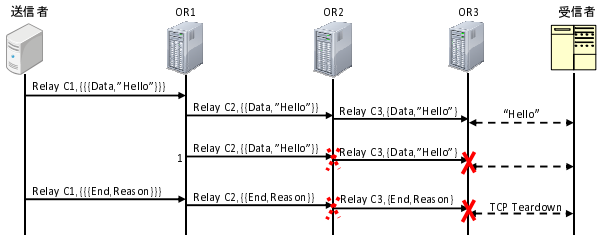


図 2　エラーを利用した手法の概略図
**Fig. 2**　Schematic of a method using an error

（図 2 の 1）（以下，複製してできたパケッを複製パケット，複製元となったパケットを複製元パケットと呼ぶこととする），複製元パケットと複製パケットを $OR3$(Exit オニオンルータ) まで送信する．Tor では AES の CTR モードを使用しているため，$OR3$ でパケットを復号する際に，エラーが発生する．$OR3$ がエラーを認知すると $OR1$ と $OR3$ 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という問題がある．

(3)　Web サイトの指紋情報を利用した手法

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，これを観測することでユーザがアクセスした Web サイトを特定するという手法である．[5] 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．[5] 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．

[6] 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．[6] 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 に対してもユーザがアクセスした Web サイトの特定が可能であり，75% 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汚染 Entry オニオンルータだけ用意すればよく，実現可能性が高い．しかし，本論文の目的である悪用ユーザの IP アドレスを特定し，利用を抑制するためには，さらに高い特定率が望まれる．

(4)　特徴的なトラフィックを利用した手法

汚染 Entry オニオンルータと汚染 Exit オニオンルータを用意し汚染 Exit オニオンルータが特徴的なトラフィックをユーザへ送信し，そのトラフィックを汚染 Entry オニオンルータが観測することでユーザを特定する手法である．[7] では，Exit オニオンルータが，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ユーザへ送信する．信号を含んだトラフィックを，Entry オニオンルータが認知することで，Web サイトへアクセスしたユーザを特定することができる．[7] 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．

[8] は Exit オニオンルータ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ユーザがアクセスした Web サイトを特定する確率は高いが汚染オニオンルータを二つ用意しなければならず実現可能性が低い．

## 4.　提案手法

本章では，4.1 で提案手法の概要を述べ，4.2 で提案手法における前提条件について説明する．さらに 4.3 で提案手法の流れを述べ，4.4 で提案手法の具体的なアルゴリズムを説明する．

### 4.1　概要

本提案手法では，悪用ユーザを推定するための有力な手がかりを与える手段を提供することを目的とする．具体的な手法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 Web サイトと Entry オニオンルータが協調動作し，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，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，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の IP アドレスを特定することを目指す．

### 4.2　前提条件

Entry オニオンルータは Web サイトの指紋情報を利用した手法における汚染オニオンルータと同様の役割を持ち，情報を抽出できるものとする．また，おとり Web サイトは公開鍵認証基盤で認証されていないものを作成する．これは，悪用ユーザがアクセスするような Web サイトは認証されておらず，また，正規ユーザはウイルスの危険性が

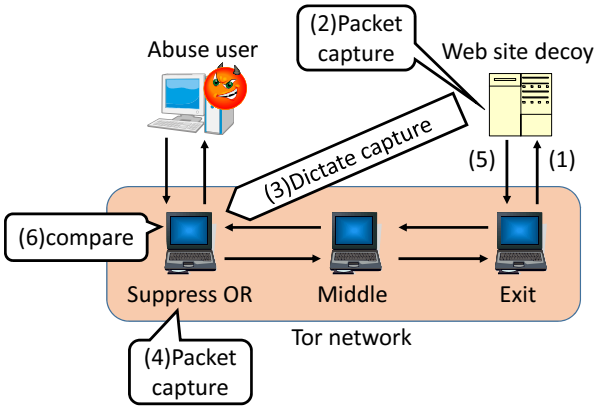


図 3　提案手法の流れ
**Fig. 3**　Flow of the proposed method

ある認証されていない Web サイトにはアクセスしないと考えたからである．ここから，おとり Web サイトは悪用ユーザのみをを対象とし，正規ユーザはおとり Web サイトへアクセスしないものとする．

### 4.3　提案手法の流れ

以下で図 3 を用いて本提案手法の流れを説明する．ここで図 3 の Suppress OR とは悪用ユーザを抑制したい立場の者が Entry オニオンルータに位置したオニオンルータである．

(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)　Suppress OR にパケットキャプチャを開始するように指示する．

(4)　Suppress 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 Suppress OR 側のキャプチャデータを比較して悪用ユーザの IP アドレスを特定する．

### 4.4　動作手順

提案手法の動作手順はおとり Web サイトを作成するおとり Web サイト作成フェーズ，図 3 の (3)，(4) の処理に当たる協調動作フェーズ，図 3 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．

I　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特定の信号を含ませる．図 3 の Suppress OR でこの信号を受け取ることで悪用ユーザが対応するおとり Web サイトを利用したことを判断する．ここで信号は，図 4 のように Web サイト本来の HTML 及び依存コンテンツを送信した後に，特定の間隔で遅延させたダミーコンテンツを複数回付加して送信することで実現する．付加するダミーコンテンツの量とその遅延時間については以下のように定める．

まず，ダミーコンテンツの数 $Num$ とそれぞれのサイズ $Size_i(i$=1,⋯,$Num)$ 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 $Time_i$（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 $Time_i$ だけ待って送信する．

図 4 は $Num$=3，$Size_1$=$Size_2$=$Size_3$=300($KB$)，$Time_1$=30，$Time_2$=40，$Time_3$=50 と設定した場合の信号である．

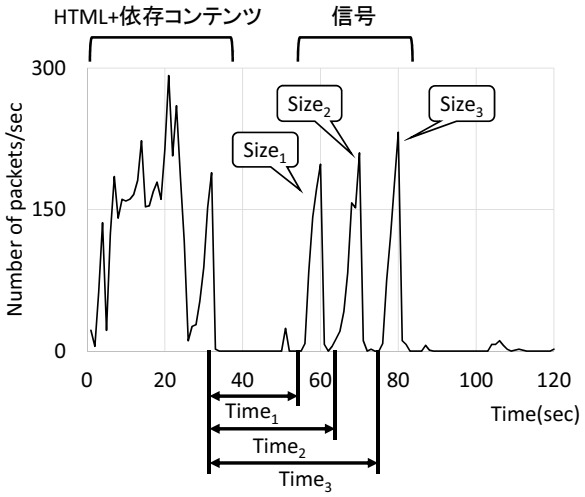


図 4　おとり Web サイトの通信トラフィック
**Fig. 4**　Communication traffic of the Web site decoy

II　協調動作フェーズ
協調動作フェーズでは 4.3 の「提案手法の流れ」における (1) から (3) までの動作を行う．

III　悪用ユーザ決定フェーズ
協調動作フェーズで収集した悪用ユーザと図 3 の Suppress OR 間のキャプチャデータと Exit オニオンルータとおとり Web サイト間のキャプチャデータを比較する．そして，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ことが分る．図 5 の実線は，おとり Web サイトにアクセスした際のおとり Web サイトで観測したパケットを表したものである．点線は，図 3 の Suppress OR で観測した結果を表したものである．ここで，図 5 の二つのデータを見ると Suppress OR で観測したデータに遅れが生じていることが分かる．このまま，相関を調べても期待する結果は得られ

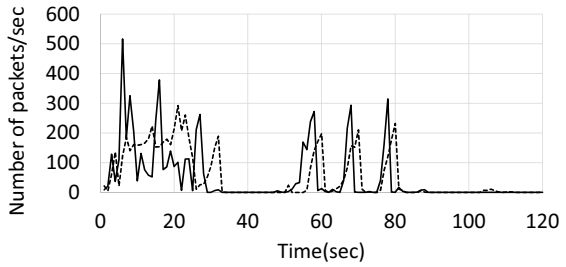


図 5　Suppress OR 及びおとり Web サイト側で収集したデータ
**Fig. 5**　The data graph which collected at the Web site decoy side and Suppress OR side

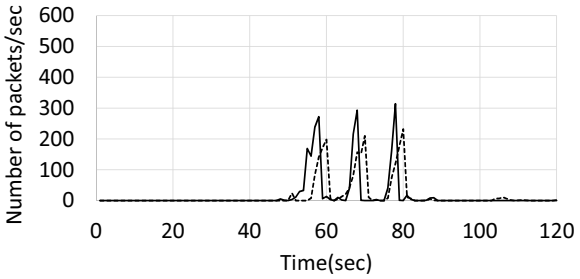


図 6　図 5 にマスク処理した
**Fig. 6**　Graph was masking Figure 5

ない．そこで二つの値を比較する指標として相互相関係数を用いる．相互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．相互相関係数が 1 に近いほど相関があることを表している．相互相関係数は式 1 で表される．ここで，$f_1(t)$，$f_2(t+t_u)$ はそれぞれ図 3 の suppress OR 側で収集したデータ，おとり Web サイト側で収集したデータを表しており，それらの”ずれ”を $t_u(\in [T_l, T_h])$ で表す．$T_l$，$T_h$ は $t_u$ の下限と上限である．そして，$f_1(t)$，$f_2(t+t_u)$ 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．そして，おとり Web サイトで観測したデータを $T_l$ と $T_h$ の間で $t_u$ 間隔で相関係数を求め，その最良値を当サイトの相関係数の値とする．さらに，収集したデータの HTML 及び依存コンテンツの部分をマスク処理することで相互相関係数の増加を図る．マスク処理は，収集したデータの時間経過に対するパケット数の変化を見ていき，パケット数が 0 の時間を区切りとし，それより以前のパケットを全て 0 に置き換える．図 6 は図 5 を実際にマスク処理したデータを表している．

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

## 5. 評価実験

本章では，ユーザ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の IP アドレス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．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．本実験では全体特定率を $Esr$，Web サイト特定率を $Wsr_i$ とし，それぞれの算出方法を式 2 に示す．ここで，$Success_i$，$WebSite$，$Access$ はそれぞれ，各 Web サイトの特定成功数，アクセスする Web サイトの数，アクセス回数である．

$$Esr = \frac{\sum_{i=1}^{WebSite} Success_i}{WebSite \cdot Access}, \quad Wsr_i = \frac{Success_i}{Access} \quad (2)$$

これらの特定率が高いほどユーザがアクセスした Web サイトが容易に分かることを示す．本提案手法は Entry オニオンルータを使用するためユーザがアクセスした Web サイトが判れば，その Web サイトへアクセスしたユーザも判ることとなる．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，以下の二つの手法を評価対象とする．

- Web サイトの指紋情報を利用した手法（従来手法）
- 提案手法

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．この手法では，Tor ネットワークの攻撃者の Entry オニオンルータ（以下，攻撃者オニオンルータ）を用いてユーザ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，ユーザがアクセスした際に攻撃者オニオンルータ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ユーザがアクセスした 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．

表 1　実験環境
**Table 1**　Experiment environment

| | |
|---|---|
| CPU | Core(TM)i7-4770 CPU 3.40GHz |
| OS | Windows 7 Pro |
| Browser | Mozilla FireFox 28.0 |
| Tor のバージョン | v0.2.3.25 |
| Perl のバージョン | ActivePerl 5.16.3 |
| Apache | v2.4.9 |

### 5.2　実験環境

実験に用いた実験環境は表 1 の通りである．

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サイトである Alexa [9] の上位から国ドメインだけが違うだけで実質的に同じサイトとなるものなどの重複を除き 100 サイト選択した．また，著作権上の問題を回避するため現実のサイトの 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からなる Web サイトを作成した．また，パケットキャプチャには wireshark [10] を用いた．

### 5.3　実験方法

本実験では各比較対象の全体特定率及び Web サイト特定率で比較する．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．

(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ユーザ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 $WebSite = 100$，$Access = 10$ とし 1000 データで攻撃者データベースを作成する．また，同様にユーザの指紋情報を 1000 データ用意する．このユーザ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 サイトが本当にユーザのアクセスした 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，簡単化のためユーザが 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 分間に設定する．

表 2　各おとり Web サイトの遅延 (sec)
**Table 2**　A delay of each web site decoy

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

(2)　提案手法
(1) と同様に，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ユーザの入出力に加え，Web サイトの入出力でもパケットキャプチャを行う．提案手法では，おとり Web サイトに悪用ユーザのみがアクセスしたと仮定している．

本実験では，各ダミーコンテンツサイズが 300KB である 5 つのおとり Web サイトを作成した．各おとり Web サイトにおけるダミーコンテンツ毎の遅延を表 2 に示す．また，$T_l$，$T_h$ はそれぞれ，代表的な Web サイトを調べた結果により，1 秒，3 秒，$t_u$ は 1 秒とした．そして，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互相関係数 $r$ 求め，$r$ が最も大きい Web サイトが対応するおとり Web サイトかどうか判断する．そして，全体特定率及び Web サイト特定率を求める．相互相関係数の算出には R 言語の ccf 関数 [11] を用いた．

### 5.4　実験結果

表 3 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 4 の False recognition，特定サイトアクセス判定率，不正サイトアクセス判定率はそれぞれ，提案手法の実験を行って対応するおとり Web サイトが別のおとり Web サイトを誤って判断した回数，ある特定の Web サイトにアクセスしたことを判定できる確率，不正サイトにアクセスしたことを判定できる確率を表している．

表 3　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 3**　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 | 78% |

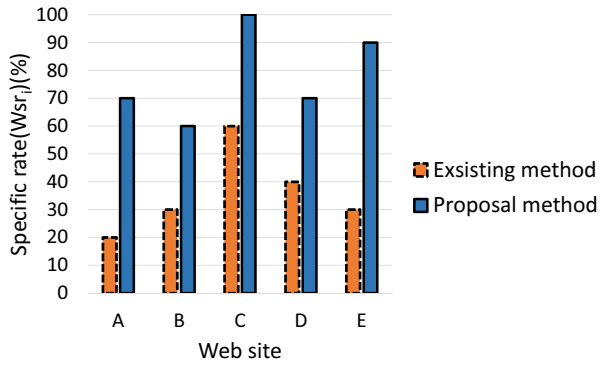


図 7　Web サイトごとの特定率

**Fig. 7**　The specific rate of two technique

表 4　誤認識回数と特定サイトアクセス判定率と不正サイトアクセス半定率

**Table 4**　Specific site access decision rate and Unauthorized site access decision rate and number of false negative

| おとり Web サイト | False negative | 特定サイトアクセス判定率 | 不正サイトアクセス判定率 |
|---|---|---|---|
| A(動画) | 1 | 70 | 80% |
| B(検索) | 1 | 60 | 70% |
| C(ショッピング) | 0 | 100 | 100% |
| D(企業 HP) | 2 | 70 | 90% |
| E(ニュース) | 0 | 90 | 90% |

## 6.　考察

表 3 より Web サイトの指紋情報を利用した手法では 52%，提案手法では 78% の全体特定率を示した．このことから，提案手法は Web サイトの指紋情報を利用した手法よりも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 IP アドレスの特定に有効であることがわかる．

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では A の動画サイトが最も低い特定率となっており，C の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，A の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，C の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 A の動画サイト，C の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．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の IP アドレスを特定できないが，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するものであるといえる．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，

表 4 において悪用ユーザがアクセスした特定の Web サイトを判定できる確率（特定サイトアクセス判定率の平均）は，78%である．また，悪用ユーザがアクセスした不正 Web サイトを判定できる確率（不正サイトアクセス判定率の平均）は，86%である．表 4 から分かるように他のおとり Web サイトを誤って判断したために特定サイトアクセス判定率が低下した．今後は，おとり Web サイト同士を識別できるように対策をしていきたい．. 特定サイトアクセス判定率を高めるための方策としては，挿入する信号をサイトごとに異なるものにする，信号を挿入するタイミングを時分割で管理するなどの方法が考えられる．

## 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，Entry オニオンルータと，おとりとなる Web サイトが協調動作して悪用ユーザの IP アドレスを特定するものである．また，ユーザ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．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]　Roger Dingledine, Nick Mathewson, and Paul Syverson: *Tor: The Second-Generation Onion Router*, In

In Proceedings of the 13th USENIX Security Symposium,(2004).

[2] WIRED：日本の警察庁、匿名化ツール「Tor」のブロックをサイト管理者に促す.
available from, (`http://wired.jp/2013/04/22/japan-police-stop-using-tor/`) (2014.01.31).

[3] 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.

[4] Ryan Pries, Wei Yu, Xinwen Fu and Wei Zhao: *A New Replay Attack Against Anonymous Communication Networks*, In ICC' 08, page 1578-1582,(2008).

[5] 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).

[6] 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.

[7] 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).

[8] 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).

[9] Alexa: Alexa Top 500 Global Site, available from, (`http://www.alexa.com/topsites`) (2014.01.31).

[10] Wireshark: Wireshark, available from, (`http://www.wireshark.org/`) (2014.01.31).

[11] 山田剛史，杉澤武俊，村井潤一郎: *R* によるやさしい統計学, pp.62-64, オーム社, (2008).

[12] David Chaum, Communications Of TheAcm, R. Rivest, and David L. Chaum, *Untraceable electronic mail, return addresses, and digital pseudonyms*, Communications of the ACM, Vol. 24, pp. 84?88, 1981.

[13] M. Reiter and A. Rubin（1998）, *Crowds: Anonymity for Web Transactions*, ACM Trans, Information and System Security, vol. 1, no. 1, pp. 66-92.

[14] Tor Metrics Portal: Directly connecting users, available from, (`https://metrics.torproject.org/users.html`) (2014.05.16)