# 匿名通信システム Tor における SVMを用いたおとり Web サイト識別手法の検討

# 匿名通信システム Tor における SVM を用いたおとり Web サイト識別手法の検討

宗　裕文 a)・吉山　友樹 b)・横山　絵美里 a)・山場　久昭 c)・久保田　真一郎 d)
・岡崎　直宣 e)

# An Examination on Identifying a Number of Decoy Web Sites through Tor Anonymity Networks with SVM

Hirofumi SOU, Tomoki YOSHIYAMA, Emiri YOKOYAMA, Hisaaki YAMABA,
Shinichirou KUBOTA, Naonobu OKAZAKI

## Abstract

The Onion Routing (Tor) is the most famous anonymity system supporting the anonymous transport of TCP over the Internet. Tor provides to communicate over public network without compromising the privacy of people. However, in some cases, Tor is used by abusing users for the antisocial purpose. As a countermeasure against this problem, a method to identify the abusing user has been proposed. The method enable to identify the abusing user PC on analyzing traffics between the abusing user PC and the decoy web site. In this paper, we propose a method to discriminate a number of the decoy web sites from others with SVM(Support Vector Machine) analysis, and evaluate our proposal method effective using 9 samples sites.

*Keywords*: Anonymous Comunication, Abuse Suppression, Onion Routing

## 1. はじめに

近年、インターネットの普及が進み、誰でもネットワークを介して様々な情報をやり取りできるようになっている。しかし、これに伴いインターネットを利用する際に通信内容を盗聴し、ユーザがアクセスした Web サイトを特定する行為が問題となっている [1]。

現在、この問題を解決するために、自身を特定するような情報を通信相手に知られることなく通信が可能な匿名通信システム [2]The Onion Router（Tor）[3, 4]が注目されている。Tor によりユーザが特定されることなく通信が可能であるが、Tor は違法行為を匿名で行うユーザ（以下、悪用ユーザ）に利用されるケースがある。悪用ユーザの利用が多くの善良なユーザの利用を妨げになっている。

この問題の対策として、悪用ユーザにとっておとりとなる Web サイト（以下、「おとり Web サイト」）を導入し、悪用ユーザが「おとり Web サイト」を利用することで、悪用ユーザの IP アドレスを特定する手法が提案されている [5]。しかし、文献 [5]では「おとり Web サイト」をいくつまで増やすことができるか議論されていない。「おとり Web サイト」を増やすためには複数の「おとり Web サイト」を識別しなければならないが、文献 [5]では複数の「おとり Web サイト」の識別はできていない。文献 [6]で複数の「おとり Web サイト」を識別する手法が提案されており、4 つの「おとり Web サイト」を識別することができるが、9 つの「おとり Web サイト」を識別することができていないことが示されている。

本論文では、Support Vector Machine（SVM）を用いて複数の「おとり Web サイト」を識別する手法を提案する。そしてこの手法がいくつの「おとり Web サイト」を識別できるのか調査実験を行う。

a)情報システム工学専攻大学院生
b)情報システム工学科学部生
c)情報システム工学科助教
d)情報システム工学科准教授
e)情報システム工学科教授

## 2. The Onion Router（Tor）

### 2.1 概要

Tor の通信は多段階プロキシを利用して行われる。Tor の仕組みを図 1 に示す。Tor のユーザは Tor ネットワーク内のオニオンルータ（以下、OR）と呼ばれる中継プロキシを無作為に三つ選択し、それぞれの OR と鍵交換を行う。このとき、ユーザに近いほうから順に、入口 OR、

中間 OR、出口 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 を特定することができない。また、OR 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 は政府機関、活動家、ジャーナリストなどの様々な目的に利用されている [7]。ところが、Tor が違法薬物の取引サイトへのアクセスに使われたり、パソコンの遠隔操作に利用されたり本来の目的以外に利用されている [8、,9]。本論文では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。違法行為を防ぐために、日本の警察庁は、サイト管理者に Tor からのアクセスをブロックするように促している [10]。日本の警察庁、並びにアメリカ国家安全保障局（以下、NAS）では悪用ユーザに対して様々な対策を行っている。

Tor において悪用ユーザの IP アドレスは、悪用ユーザを抑制したい立場の者にとって有益な情報である。そこで、次章では悪用ユーザの利用を抑制することを目的とした悪用ユーザの IP アドレス特定手法 [5]について説明する。

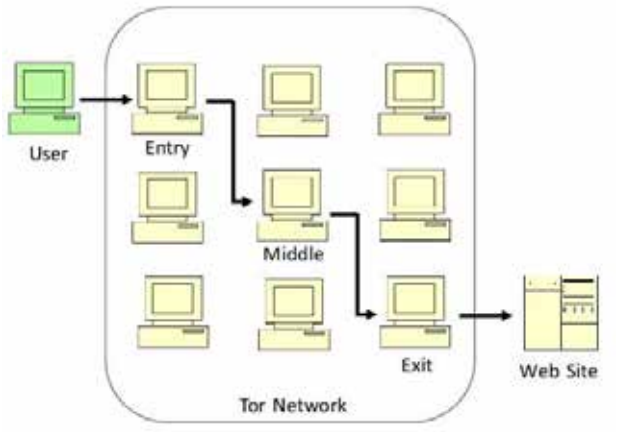


図 1． Tor の概略図.

## 3. おとり Web サイトを利用した悪用ユーザの IP アドレス特定手法 [5]

本章では宗裕文ら [5]が行った Tor における「おとり Web サイト」を利用した悪用ユーザの IP アドレスを特定する手法について説明する。本論文では悪用ユーザを抑制したい立場の者が提供した入口 OR を Suppress OR（SOR）と呼ぶこととする。文献 [5]では悪用ユーザの利用を抑制することを目的に、「おとり Web サイト」を導入している。「おとり Web サイト」でアクセスの度に特徴的なトラフィックを挿入したパケットを返し、SOR で特徴的なトラフィックを検知することで、悪用ユーザが「おとり Web サイト」を利用したと判断し、悪用ユーザの IP アドレスを特定する手法を提案している。

### 3.1 おとり Web サイト

「おとり Web サイト」とは、悪用ユーザがアクセスする可能性がある Web サイトを模して作成した悪用ユーザにとっておとりとなる Web サイトである。「おとり Web サイト」には現実の Web サイトへのアクセスと区別するために特徴的なトラフィックをパケットに挿入する機能をもつ。SOR でこの特徴的なトラフィックを検知することで、悪用ユーザが「おとり Web サイト」を利用したと判断する。特徴的なトラフィックは、図 2 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数回付加して送信することで実現する。

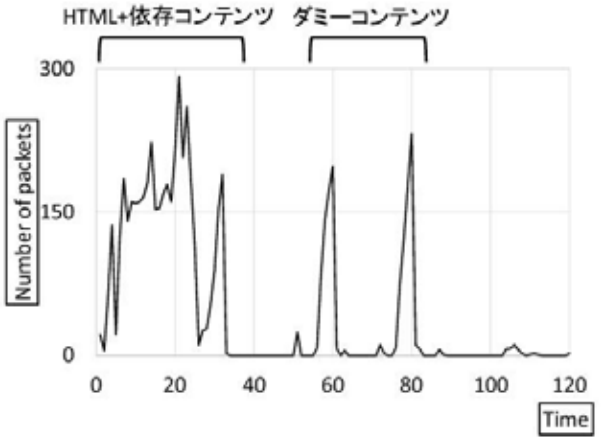


図 2. おとり Web サイトの通信トラフィック.

### 3.2 悪用ユーザの IP アドレスを特定する手順

(1) 「おとり Web サイト」はユーザからアクセス要求がきたことを検知する。
(2) 「おとり Web サイト」はパケットキャプチャを開始する。
(3) 「おとり Web サイト」は SOR にパケットキャプチャを開始するように指示する。
(4) SOR はパケットキャプチャを開始する。
(5) 「おとり Web サイト」は特徴的なトラフィックを挿入し、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 SOR 側のキャプチャデータから相互相関係数を算出し、類似度を求める。
(7) 類似していれば SOR を入口 OR として「おとり Web サイト」にアクセスしてきたユーザであると判断し、SOR は「おとり Web サイト」へアクセスしてきたユーザの IP アドレスを特定する。

文献 [5]において、悪用ユーザを特定する可能性を高める方法の 1 つに「おとり Web サイト」の数を増やすことが考えられる。「おとり Web サイト」の数を増やすことができればその数だけアクセスする悪用ユーザも増えるので、

悪用ユーザを特定する可能性がさらに高くなると考えられる。しかし、文献[5]では「おとり Web サイト」をいくつまで増やすことができるかという議論はされていない。「おとり Web サイト」の数を増やすためには複数の「おとり Web サイト」を識別しなければならない。文献[5]では複数の「おとり Web サイト」の識別は行われていない。次章では、複数の「おとり Web サイト」を識別する手法について説明する。

## 4. 相互相関係数を用いたおとり Web サイト識別手法[6]

本章では宗裕文ら[6]が行った複数の「おとりWebサイト」を相互相関係数を用いて識別する手法について説明する。相互相関係数とは2つのデータ間の類似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。文献[6]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を求め、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、Webサイト識別率を求める。そのために、事前実験を行い、複数の「おとりWebサイト」を識別するために有効な特徴を調査した結果、ダミーコンテンツのサイズと送信間隔の2つの特徴が「おとりWebサイト」の識別に有効であることが分かった。そして、事前実験で得られた特徴の組み合わせでいくつの「おとりWebサイト」を識別できるか評価実験を行った結果、4つの「おとりWebサイト」を識別することができたが、9つの「おとりWebサイト」を識別することができなかった。

## 5. 提案手法

本提案手法は、Support Vector Machine(SVM)[12]を用いて複数の「おとり Web サイト」を識別する手法を提案する。本論文で Discriminate OR(DOR)とは SVM の機能を持った SOR である。また、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いない可能性が高いと考えられるため、「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。SVM を用いた識別は、ユーザがアクセスする Web サイトを特定する手法[11]を参考に実装を行う。文献[11]は、Tor の匿名性を低下させようとする者（以下、攻撃者）が入口 OR となり Tor ネットワーク上を流れるトラフィックを観測することで、ユーザがアクセスする Web サイトを特定する手法である。Web サイトは様々な画像ファイルやスクリプトファイルから構成されているため、Web サイトごとにファイル数やサイズ、トラフィックの流れなどにユニークな特徴（以下、指紋）が表れる。攻撃者は指紋情報をトラフィックから収集し、Web サイトを特定する。

SVM を用いて識別する手順はまず、悪用ユーザを抑制したい立場の者は SVM への学習データとして予め DOR を介して「おとり Web サイト」に訪問してトラフィックデータを取得する。次に 3。2 節の(1)(3)(4)(5)を順に行い、最後に、DOR はキャプチャデータを自身の SVM に予測データとして読み込ませる。SVM は DOR で取得した予測データがどの「おとり Web サイト」に当てはまるか判定をする。

## 6. 調査実験

### 6.1 評価指標

本論文では、複数の「おとり Web サイト」を識別することが目的であるため、全体識別率と Web サイト識別率で評価を行う。全体識別率とは、各 Web サイトへのアクセス回数に対するアクセスした Web サイトの識別成功総数の割合である。また Web サイト識別率とは、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 サイトの識別成功数の割合である。実験では、全体識別率を $E_{sr}$、Web サイト識別率を $W_{sr}$ とし、それぞれの算出方法を式 1 に示す。ここで、$S_i$ は各 Web サイトの識別成功数、$W_i$ はアクセスする Web サイトの数、$A_i$ はアクセス回数である。

$$E_{sr} = \frac{\sum_{i=1}^{W_i} S_i}{W_i \cdot A_i}, \qquad W_{sr} = \frac{S_i}{A_i} \tag{1}$$

### 6.2 実験環境

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[14]の上位から 100 サイトを選択した。ただし、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は除く。また、著作権上の問題を回避するために現実のサイトの 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「おとり Web サイト」に見立てた擬似 Web サイトを作成した。パケットキャプチャには Wireshark[15]を用いた。

### 6.3 実験方法

文献[6]の事前実験の結果を元にサイズの異なるダミーコンテンツのサイズとダミーコンテンツの送信間隔の組み合わせで、識別できる「おとり Web サイト」の数を調査する。

実験では、文献[6]と同じ以下の 2 つの場合において実験する。

実験 1：サイズが異なるダミーコンテンツを 2 通り、ダミーコンテンツの送信間隔を 2 通りで構成される 4 つの「おとり Web サイト」

実験 2：サイズが異なるダミーコンテンツを 3 通り、ダミーコンテンツの送信間隔を 3 通りで構成される 9 つの「おとり Web サイト」

ダミーコンテンツのサイズが大き過ぎたり、送信間隔が長過ぎると「おとり Web サイト」の読み込み速度が遅くなるなどの問題が考えられる。その場合に、悪用ユーザにアクセスしているサイトが「おとり Web サイト」だと判断されてしまう可能性がある。そのためにまず、全体のダミーコンテンツのサイズの上限値、ひとつのダミーコンテンツのサイズの上限値、ダミーコンテンツの送信時間の上限値、ダミーコンテンツの送信間隔の最大値を求める。ダミーコンテンツの数を N、ダミーコンテンツのサイズを $s_i$(i=1,…,N)、ダミーコンテンツを送信するまでの時間を $T_i$[s]と定義する。今回は付加するダミーコンテンツの数は 2 つ、1 つ目のダミーコンテンツを送信するまでの待ち時間を $T_1$=5[s]と設定した。「おとり Web サイト」のダミーコンテンツのサイズと送信間隔の設定方法を以下に示す。

(1) ダミーコンテンツのサイズを設定

ダミーコンテンツのサイズ $s_1$、$s_2$ を設定する。そのためにまず、全体のダミーコンテンツのサイズの上限値を決める。全体のダミーコンテンツのサイズの上限値は各「おとり Web サイト」における HTML 及び依存コンテンツの合計サイズの中央値とした。次に、ひとつのダミーコンテンツのサイズの上限値を求める式を式(2)に示す。最後に、ひとつのダミーコンテンツのサイズの上限値を幾通りに分割し $s_1$、$s_2$ のパラメータとして設定する。

$$(\text{ひとつのダミーコンテンツの上限値}) = \frac{(\text{全体のダミーコンテンツの上限値})}{N} \quad (2)$$

(2) ダミーコンテンツの送信間隔を設定

2 つ目のダミーコンテンツを送信するまでの待ち時間 $T_2$ を設定する。そのためにまず、ダミーコンテンツの送信時間の上限値を決める。ダミーコンテンツの送信時間の上限値は、各「おとり Web サイト」における HTML 及び依存コンテンツを送信し終えるまでの時間の中央値とした。次に、ダミーコンテンツの送信間隔の最大値を求める式を式(3)に示す。最後に、ダミーコンテンツの送信間隔の最大値を幾通りに分割し、$T_2$ を式(4)により設定する。式(4)の $\Delta T_i$ はダミーコンテンツの送信間隔の最大値を分割した値、$D_1$ は $s_1$ のダウンロード時間を表す。

$$\begin{aligned}&(\text{ダミーコンテンツの送信間隔の最大値})\\&= (\text{ダミーコンテンツの送信間隔の上限値})\\&- (\text{全体のダミーコンテンツのサイズの}\\&\qquad \text{上限値のダウンロード時間}) \quad (3)\end{aligned}$$

$$T_2 = T_1 + D_1 + \Delta T_i \quad (4)$$

調査の結果、全体のダミーコンテンツのサイズの上限値は 4600[kb]、ダミーコンテンツの送信時間の上限値は 36[s]、全体のダミーコンテンツのサイズの上限値のダウンロード時間は 16[s]だった。実験では、付加するダミーコンテンツの数を 2 つとするため、ひとつのダミーコンテンツのサイズの上限値は 2300[kb]となる。よって、ダミーコンテンツのサイズ $s_1$、$s_2$ は実験 1 では 1150[kb]と 2300[kb]、実験 2 では 700[kb]、1400[kb]、2100[kb]となる。また、全体のダミーコンテンツのサイズの上限値のダウンロード時間 16[s]のとき、ダミーコンテンツの送信間隔の最大値は 20[s]となるので、付加するダミーコンテンツの数を 2 つとすると、$\Delta T_i$ は実験 1 では 10[s]と 20[s]、実験 2 では 6[s]、12[s]、18[s]となる。

実験で用いたパラメータを表 2、3 に示す。表 2 の実験ではダミーコンテンツのサイズを 2 通り、送信間隔を 2 通りとするので、「おとり Web サイト」の数を 4 つにする。悪用ユーザがアクセスする可能性が低い企業 HP の「おとり Web サイト」を除外した。表 3 の実験ではダミーコンテンツのサイズを 3 通り、送信間隔を 3 通りとするので「おとり Web サイト」を 9 つにする。企業 HP を除く 4 種類の「おとり Web サイト」から 2 つずつ選択し、企業 HP の「おとり Web サイト」を 1 つ選択した。

実験では、4 つ及び 9 つの「おとり Web サイト」にそれぞれ 80 回ずつアクセスしたキャプチャデータを用いる。そしてキャプチャデータから、全体識別率及び Web サイト識別率を求める。全体識別率が 100%の場合のみ、「おとり Web サイト」を識別できるものとする。

表 2. 実験 1 のパラメータ.

| おとり Web サイト | $s_1$[kb] | $s_2$[kb] | $T_1$[s] | $T_2$[s] |
|---|---|---|---|---|
| A(動画) | 1150 | 1150 | 5 | 19 |
| B(検索) | 1150 | 1150 | 5 | 29 |
| C(ショッピング) | 2300 | 2300 | 5 | 23 |
| E(ニュース) | 2300 | 2300 | 5 | 33 |

表 3. 実験 2 のパラメータ.

| おとり Web サイト | $s_1$[kb] | $s_2$[kb] | $T_1$[s] | $T_2$[s] |
|---|---|---|---|---|
| A1(動画) | 700 | 700 | 5 | 15 |
| A2(動画) | 700 | 700 | 5 | 22 |
| B1(検索) | 700 | 700 | 5 | 29 |
| B2(検索) | 1400 | 1400 | 5 | 17 |
| C1(ショッピング) | 1400 | 1400 | 5 | 24 |
| C2(ショッピング) | 1400 | 1400 | 5 | 31 |
| D1(企業 HP) | 2100 | 2100 | 5 | 19 |
| E1(ニュース) | 2100 | 2100 | 5 | 26 |
| E2(ニュース) | 2100 | 2100 | 5 | 33 |

### 6.4 実験結果と考察

調査実験の結果、実験 1、実験 2 共に全体特定率 100%という結果が得られた。表 4、5 から SVM を用いること

で、4 つまたは 9 つの「おとり Web サイト」を識別でき、文献 6)の手法よりも高い確率で「おとり Web サイト」を識別することができた。つまり、ダミーコンテンツのサイズと送信間隔を特徴として「おとり Web サイト」を識別する場合は、文献 6)の相互相関係数を用いて識別を行う手法よりも、SVM を用いて識別を行う手法の方が「おとり Web サイト」の識別に有効といえる。

表 4. 実験 1 の Web サイト識別率.

| おとり Web サイト | SVM[%] |
|---|---|
| A(動画) | 100 |
| B(検索) | 100 |
| C(ショピング) | 100 |
| E(ニュース) | 100 |

表 5. 実験 2 の Web サイト識別率.

| おとり Web サイト | SVM[%] |
|---|---|
| A1(動画) | 100 |
| A2(動画) | 100 |
| B1(検索) | 100 |
| B2(検索) | 100 |
| C1(ショッピング) | 100 |
| C2(ショッピング) | 100 |
| D1(企業 HP) | 100 |
| E1(ニュース) | 100 |
| E2(ニュース) | 100 |

## 7. まとめ

本論文では、匿名通信システム Tor における「おとり Web サイト」を利用した悪用ユーザの IP アドレス特定手法の実現可能性を高めるために、SVM を用いた「おとり Web サイト」を識別する手法を提案し、「おとり Web サイト」をいくつ識別できるか調査実験を行った。その結果、SVM を用いた識別は 4 つまたは 9 つの「おとり Web サイト」を識別でき、文献 6)の相互相関係数を用いた識別よりも高い識別率を出すことができた。今後はさらに識別できる「おとり Web サイト」の数を増やすための手法、提案手法におけるダミーコンテンツのサイズや送信間隔の適切な上限値の調査を行っていく予定である。

## 参考文献


1) ITpro by 日経コンピュータ：NSA が Google および Yahoo！のデータセンターから通信傍受、米紙が報道, http://itpro.nikkeibp.co.jp/article/NEWS/20131031/515126/.
2) David Chaum, Communications Of The Acm, R. Rivest, David L. Chaum: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM,Vol.24, pp.84-88, 1981.
3) Tor Project: Anonymity online, https://www.torproject.org/.
4) Roger Dingledine, Nick Mathewson, and Paul Syverson: Tor: The Second-Generation Onion Router, In Proceedings of the 13th USENIX Security Symposium Volume13, pp.303-320, 2004.
5) 宗裕文, 横山絵美里, 山場久昭, 久保田真一郎, 朴美娘, 岡崎直宣: 匿名通信システムにおける悪用ユーザ特定手法の検討 マルチメディア, 分散, 協調とモバイル(DICOMO2014) シンポジウム, pp.506-513, 2014.
6) 宗裕文, 和斉薫, 横山絵美里, 山場久昭, 久保田真一郎, 朴美娘, 岡崎直宣:匿名通信システム Tor における悪用ユーザ推定手法の精度に関する検討 情報処理学会研究報告. MBL, [モバイルコンピューティングとユビキタス通信研究会研究報告] 2014-MBL-73(22), pp.1-7, 2014.
7) ZDNet Japan： Tor に匿名解除狙う攻撃--ユーザーにも警告, http://japan.zdnet.com/article/35051653/.
8) J-CAST ニュース ビジネス¥&メディアウォッチ: PC 遠隔操作事件で使われたソフト「Tor」発信元を匿名化、海外では悪用例も, http://www.j-cast.com/2013/02/12165010.html.
9) IT¥&メディア 読売新聞(YOMIURI ONLINE): パソコン遠隔操作事件が残したもの, http://www.yomiuri.co.jp/it/security/goshinjyutsu/20140523-OYT8T50256.html.
10) 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, http://wired.jp/2013/04/22/japan-police-stop-using-tor/.
11) Panchenko, A, Niessen, L, Zinnen, A, Engel, T: Website Fingerprinting in Onion Routing Based Anonymization Networks, In Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, pp.103-113, 2011.
12) Hearst, M.A, Dumais, S.T, Osman, E, Platt, J, Scholkopf, B：Support vector machines, IEEE Intelligent Systems and their Applications, Volume 13 Issue 4, pp18-28, 1998.
13) 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.
14) Alexa: Alexa, The top 500 sites on the web, http://www.alexa.com/topsites.
15) Wireshark: Wireshark, http://www.wireshark.org/.