匿名通信システムにおける指紋攻撃の対策に関する一検討

富田 旋[†1]　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 は多段プロキシを利用することで安全な通信を提供しているが，これを脅かすような攻撃が考案されつつある．その中でも流れるトラフィックの特徴からユーザのアクセスする Web サイトを特定する「指紋攻撃」が脅威になっている．本論文では，Tor に対する攻撃手法の中でも最も実現可能性が高い指紋攻撃について，その攻撃の効果を実験により検証し，指紋攻撃対策である Camouflage 手法の問題点を言及した後に，その問題点を改善した手法の提案と評価を行う．

キーワード：匿名化通信，The Onion Router，Tor，指紋攻撃，Camouflage 手法

An examination on countermeasure against fingerprinting attack in an anonymous communication system.

Meguru Tomita[†1]　Hirofumi Sou[†1]　Emiri Yokoyama[†1]　Hisaaki Yamaba[†1]　Shinichiro Kubota[†1]
Mirang Paku[†2]　Naonobu Okazaki[†1]

Abstract: Tor(The Onion Routing) is the most famous anonymity system and provides a secure communication by using a multi-stage proxy. However, it cannot completely hide the size of the contents and the timing of transmission of packets. Fingerprinting attack uses these features to infer the website being accessed by the specific client, and it has become a serious threat against Tor. In this article, we propose a new countermeasure toward the fingerprinting attacks and examine the feasibility and effectiveness of the proposed method.

Keywords: Anonymity System, The Onion Router, Tor, Fingerprinting Attack，Camouflage Technique

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おり，様々な情報がやり取りされている．しかし，これに伴いインターネットを利用する際にパケットの通信を盗聴し，ユーザがアクセスする Web サイトを識別する行為が問題となっている．そこで，通信経路を秘匿することでユーザがアクセスした Web サイトを秘匿する匿名通信システム [1] が研究されている．匿名通信システムで現在最も利用されているものは The Onion Router（Tor）[2][3] である．Tor は，「オニオンルーティング」という複数のプロキシを経由して Web サイトにアクセスする方式を用いて匿名通信を実現している．しかし，Tor を利用することで確実に匿名性のある通信が行えるわけではない．データを中継するプロキシの一部または全部が悪意ある第三者（以下，攻撃者）が提供するものだった場合，攻撃者がトラフィックに信号を含めたりトラフィックパターンの解析をしたりすることで，ユーザがアクセスした Web サイトを識別される問題がある．本論文では，Tor に対する攻撃手法の中でも最も実現可能性が高い指紋攻撃 [5] について，その攻撃の効果を実験により検証し，指紋攻撃対策である Camouflage 手法の問題点を言及した後に，その問題を改

[†1] 現在，宮崎大学
Presently with Uniersity of Miyazaki
[†2] 現在，神奈川工科大学
Presently with Kanagawa Institute of Technology

善した手法の提案と評価を行う．

2. The Onion router(Tor)

2.1 概要

Tor とは，元々アメリカ海軍調査研究所（USNRL）[4] により開発された，低遅延の匿名通信技術である．Tor の一日あたりのユーザ数は 200 万人（2016 年 1 月現在）であり，現在最も利用されている匿名通信システムである．Tor ネットワークから無作為に選ばれた複数のプロキシ（以下，オニオンルータ：OR）を経由し，「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．このときの通信の様子を図 1 に示す．ここで、送信者に最も近いノードを入口オニオンルータ，受信者に最も近いノードを出口オニオンルータ，二つの間のノードを中間オニオンルータと呼ぶこととする．ユーザはそれぞれの中継プロキシの鍵で順番に暗号化を施したパケットを転送する．そして，それを受け取った中継プロキシは自分の鍵で復号を行い次の宛先に転送する．このプロキシが順番に復号を行っていく様がタマネギの皮むきに似ていることが The Onion Router の名前の由来となっている．また，Tor では TCP のみサポートしており，UDP の通信は不可能である．そのため，ストリーミング配信などの一部のサービスは Tor 上で利用できない．

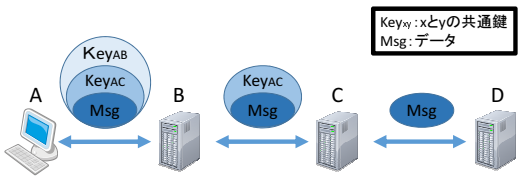

図 1 Tor における通信の概要
Fig. 1 Overview of communication in Tor.

2.2 Tor の匿名性に対する脅威

Tor は高い匿名性を持つ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．本論文では，Tor の匿名性を低下させようとする者を「攻撃者」，攻撃者の提供するオニオンルータを「攻撃者オニオンルータ」と呼ぶこととする．例えば，ユーザが Fully Qualified Domain Name(FQDN) で Web サイトを指定した場合，名前解決がユーザ側で行われることがあり，DNS にユーザがアクセスした Web サイトの情報が残ってしまう．また，ユーザが Web サイトへアクセスする際に，攻撃者オニオンルータが経路に含まれていた場合，Tor の匿名性が失われることがある．本研究では攻撃手法の中でも最も現実的な「指紋攻撃」に着目している．次章では指紋攻撃について述べる．

3. 指紋攻撃

3.1 指紋攻撃とは

指紋攻撃 [5][6][7][8][9] とは，Web サイトごとに異なるトラフィックに着目しユーザがアクセスした Web サイトを識別する手法である．Web サイトは画像ファイルやスクリプトファイルなど多種多様なファイルから構成されており，その数やサイズも Web サイトごとにユニークである．そのため，その Web サイトごとにユニークなトラフィック（以下，指紋）を観測することで，ユーザがアクセスした Web サイトを特定することができる．指紋攻撃は攻撃者オニオンルータがユーザに流れたトラフィックを観測する入口オニオンルータ 1 つだけで良いことが最大の特徴である．そのため指紋攻撃は実現可能性が高く，今後 Tor の大きな脅威になると考えられる．

3.2 指紋情報

本節では指紋攻撃時に用いられる指紋情報について説明する．指紋情報とは，攻撃の際に攻撃者によって集められるユーザと Web サイト間に流れるトラフィックの特徴である．本研究で想定する指紋攻撃で利用する指紋情報を以下に示す．

『指紋情報の要素』

- $S_{total}^{p \to q}$：p から q に向かう総パケットサイズ (Bytes)
- $N_{total}^{p \to q}$：p から q に向かうパケットの総数
- $S_{avg}^{p \to q}$：p から q に向かうパケットの平均サイズ (Bytes)
- $S_{var}^{p \to q}$：p から q に向かうパケットの分散 (Bytes)
- $C_{avg}^{p \to q}$：p から q に向かうチャンクの平均サイズ (Bytes)
- $C_{var}^{p \to q}$：p から q に向かうチャンクの分散 (Bytes)

p と q はそれぞれクライアント c または Web サイト w を表している．よって，合計 12(=6*2) の指紋情報を使用する．通信チャンクとは，パケットの向き（上り下り）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あわせたパケットの塊のことである．指紋情報の具体例について図 2 に示す．左図の 1 つのまとまり，c，w，矢印はそれぞれパケット，ユーザ，Web サイト，パケットの向きを表している．例えば，「$c \to w$ size20」はユーザから Web サイトへ 20byte のパケットが流れたことを表している．そして，左図のようなトラフィック収集し，そこから各指紋情報を抽出した結果を右図に示している

3.3 指紋攻撃の処理手順

ここでは想定する指紋攻撃における処理手順について記述する．まず，本論文で想定する指紋攻撃は大きく指紋情報収集フェーズと識別フェーズに分けられる．

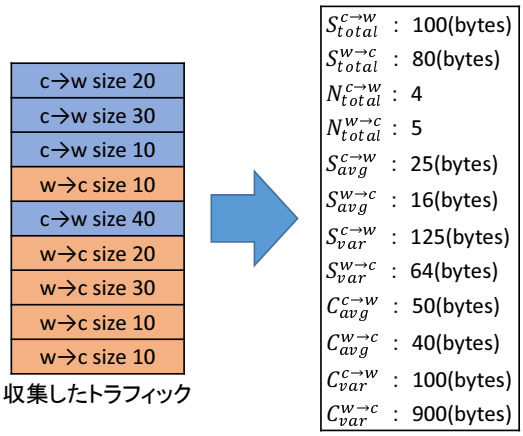

図 2　指紋情報の具体例
Fig. 2　Specific examples of the fingerprint information.

3.3.1　指紋情報収集フェーズ

このフェーズでは，攻撃者は自分の提供するオニオンルータを入口オニオンルータとして様々な Wen サイトへアクセスする．そして Web サイトにアクセスしたときのトラフィックから指紋情報を収集し分類機に学習させ、データベース化する．このように，定期的に Web サイトへアクセスすることでニュースサイトやショッピングサイトのような時間とともに変化するサイトにも対応することができる．

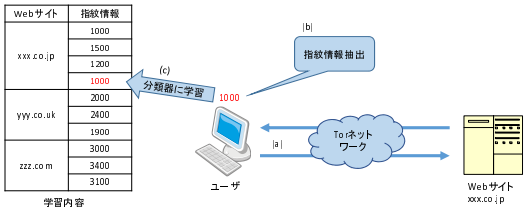

図 3　指紋情報収集フェーズの概略図
Fig. 3　Schematic diagram of the fingerprint information collection phase.

3.3.2　識別フェーズ

このフェーズでは攻撃者は図 4 のように入口 OR としてターゲットが接続してくるのを待つ．攻撃者はターゲットの接続を確認すると，3.3.1 節と同様にしてターゲットのトラフィックから指紋情報を収集する．指紋情報の抽出が終わると指紋情報を分類器にかけ，ユーザのアクセスした Web サイトを識別する．

3.4　実験

本節では，前述した指紋攻撃の脅威を実験により測る．さらに本節では，指紋攻撃の対策についても述べる．

3.4.1　実験環境

本実験環境を表 1 に示す．また，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 [10] の上位から国ドメインだけが違うだけで同じ

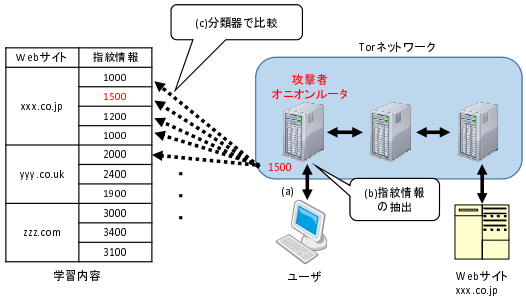

図 4　識別フェーズの概略図
Fig. 4　Schematic view of the identification phase.

サイトなどの重複をさけて 100 サイト選択した．また，パケットキャプチャには Wireshark [11]，分類器には R 言語の SVM(Support Vector Machine) を用いた．

表 1　実験環境
Table 1　Experiment environment.

OS	Windows7 Professional
CPU	Corei7 3.40GHz
Memory	8.00GB
Browser	Internet Explorer 11
Tor	Tor Browser Bundle for Windows version 17.0.7
Perl	perl 5.20.2

3.4.2　実験方法

本実験では、指定した URL をブラウザに入力すると，Tor ネットワーク経由で接続される．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し指紋情報を抽出する．ターゲットが Web サイトにアクセスする際，トップページだけを閲覧しトップページが表示されるまでキャプチャを行う．また，100 サイトの Web サイトに 20 回アクセスし収集する．そして，交差検証を用いて学習データと識別データの作成し SVM で学習と識別を行う．交差検証とは，データを n 個に分割し一つ目を識別データ，残りを学習データとして識別を行う方法である．そしてこれを n 回繰り返す．

3.4.3　実験結果

実験の結果、全体識別率は約 41% であった．図 5 は 100 サイト全ての Web サイトの識別率をグラフで表したものである．図 6 は図 5 の結果を識別率ごとに集計したものである．

3.4.4　考察

図 5 から分かるように Web サイトによって識別率には差があり，0% のものから 100% のものまで様々である．また，図 6 から識別されない Web サイトは 15 サイトしかなく，残り 85 サイトは少なからず識別される可能性がある．このことから，指紋攻撃は現在の Tor に対して非常に有効な攻撃手段であり，対策の必要があると言える．次章では指紋攻撃への対策に関する既存研究を紹介する．

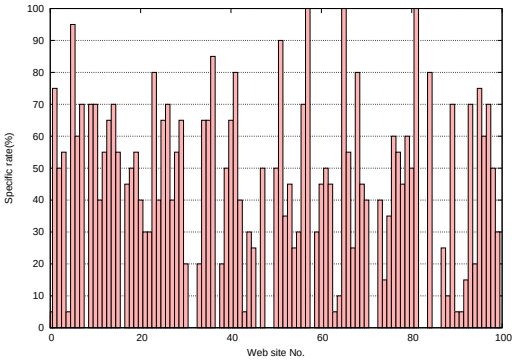

図 5　Web サイト識別率
Fig. 5　Web site identification rate.

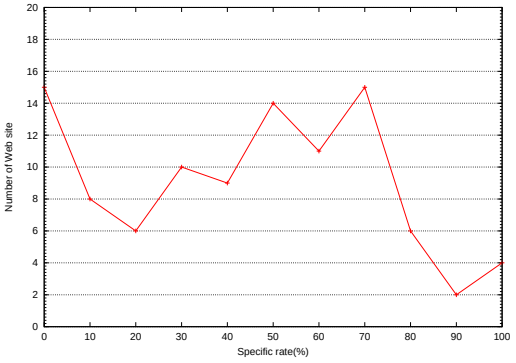

図 6　識別率ごとの Web サイト数
Fig. 6　Web site number of each identification rate.

4.　指紋攻撃への対策

3 章で指紋攻撃が Tor にとって非常に大きな脅威であることが分かった．本章では，指紋攻撃への対策として Camouflage 手法に着目し具体的に説明する．

4.1　Camouflage 手法

これは，挿入するダミー情報を人口のものではなく，現実の Web サイトから取得する手法である．[5] はユーザがアクセスしたい Web サイト（以下，目的サイト）へアクセスする際に，ランダムに選択された別の Web サイト（以下，追加サイト）へ同時にアクセスすることで，目的サイトと追加サイトの指紋情報を混在させ，目的サイトの指紋情報を撹乱する手法である．これにより，目的サイトの指紋情報を抽出することを防ぎ指紋攻撃を軽減することができる．[5] は最も容易に実装でき指紋攻撃に有効であることが示されている．次節で Camouflage 手法の具体的なアルゴリズムと問題点について説明する．

4.2　Camouflage 手法のアルゴリズム

Camouflage 手法の概略図を図 7 に示す．図中の EntryOR，MiddleOR，ExitOR はそれぞれ入口オニオンルータ，中間オニオンルータ，出口オニオンルータを表している．ユーザは追加サイトの URL が複数書かれたリスト（以下，URL リスト）を保持している．ユーザは目的サイトの URL を入力する（図 7 の (a)）．Camouflage システムは URL リストからランダムに追加サイトを選択する（図 7 の (b)）．目的サイトと追加サイトへ同時にリクエストを送信する（図 7 の (c)）．上記の処理を行う事により，入口オニオンルータで指紋情報を収集する攻撃者には，目的サイトと追加サイトの指紋情報が混在して見え，目的サイトの識別が困難になる．しかし，4.3 節で述べるような問題点があり改善する必要がある．

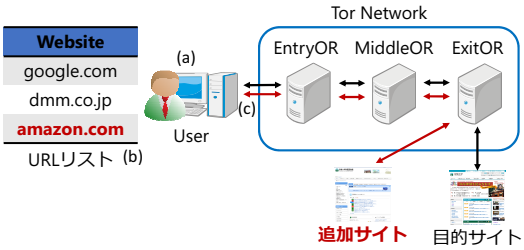

図 7　Camouflage 手法の概略図
Fig. 7　Schematic view of Camouflage technique.

4.3　Camouflage 手法の問題点

Camouflage 手法は目的サイトと追加サイトへ同時にアクセスするため，目的サイトと追加サイトのサイトサイズの組み合わせによって攻撃者に目的サイトの指紋情報を与えてしまう可能性がある．ここで，サイトサイズとは Web サイトへアクセスした際の総通信量のことである．また，Camouflage 手法本来の目的は目的サイトの指紋情報を攻撃者に与えない事である．ユーザがサイズの大きな目的サイトへアクセスする際に，サイズの小さな追加サイトが選択された場合，目的サイトの指紋情報を隠す事ができず，攻撃者に与えてしまう恐れがある．Camouflage 手法では上記のような組み合わせとなる場合が存在する．例えば URL リストに含まれる Web サイトが Alexa の Top100 サイトの場合である．図 8 は Alexa の Top100 サイトを URL リストに加えた場合のサイズ毎の選択される確率を表した模式図である．Alexa の Top100 サイトはサイズの小さいサイトが多いため，この手法のように追加サイトをランダムで選択した場合，図 8 のようにサイズの小さいサイトが選択される確率が格段に高くなってしまう．そのため，サイズの大きな目的サイトへアクセスする際に，サイズの小さな追加サイトが選択される状況が極めて高くなってしまう．次章では Camouflage 手法の問題点を改善する手法を提案する．

5.　提案手法

4.3 節で述べた Camouflage 手法の問題点を改善した対策手法を提案する．

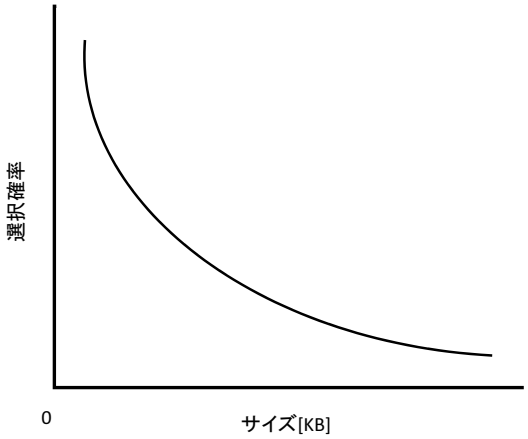

図 8　Camouflage 手法のサイズ毎に選択される確率を表した模式図
Fig. 8　Schematic diagram illustrating a probability of being selected for each size of Camouflage techniques.

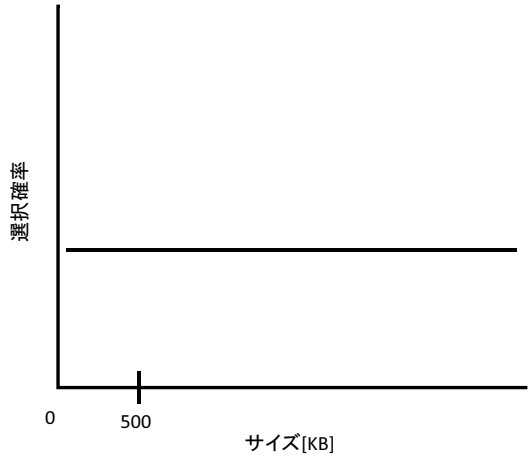

図 9　提案手法のサイズ毎の選択される確率を表した模式図
Fig. 9　Schematic diagram illustrating a probability of being selected each time the size of the proposed method.

5.1　提案手法の概要

Camouflage 手法は目的サイトへアクセスする際に，同時に URL リストからサイズを考慮せずにランダムで選択された Web サイトにアクセスするものである．そのため，4.3 節で述べたように URL リストによっては，あるサイズが片寄って選択される場合がある．本研究では追加サイトの選択方法においてサイズに着目することにより Camouflage 手法の問題点を改善できるのではないかと考えた．そこで，URL リスト内のサイトのサイズを事前に調査し，URL リスト内に URL とサイズを保持することで，各サイズに属するサイトが同じ確率で選択される手法を提案する．図 9 は提案手法を適用した場合のサイズ毎の選択される確率を表した模式図である．図 9 のように各サイズが同じ確率で選択されることによって，Camouflage 手法より指紋攻撃耐性を持たせる事のできる手法を考えた．本提案手法は Camouflage 手法とは異なり事前に URL リスト内のサイトのサイズを調査する必要がある．これは，指紋攻撃を実行する攻撃者側が様々なサイトへアクセスし指紋情報を収集することができるのと同様に，指紋攻撃を対策する側（例：Tor の管理者）も事前に調査することは可能だと考える．

5.2　提案手法の特徴

本提案手法の特徴について述べる．まず，サイズを考慮することによって追加サイトに選択されるサイトのサイズに偏りがなくなり，目的サイトの指紋情報を撹乱させる効果が大きくなる．つまり，Camouflage 手法よりも匿名性をさらに向上させることが期待できる．しかし，追加サイトとして選択されるサイズの種類が増える事によって Camouflage 手法よりも全体的に見て通信量が増加してしまう欠点もある．通信量が増加することによりサイトのロード時間の増加，つまりユーザビリティの低下の懸念がある．次章でロード時間に関する評価もしているが，ロード時間を比べても Camouflage 手法と差がほとんどみられなかったため，ユーザビリティの低下という懸念は少ないと考えている．

5.3　提案手法のアルゴリズム

提案手法のアルゴリズムは，大きくサイズ調査フェーズと追加サイト選択フェーズに分けられる．サイズ調査フェーズでは，Tor の管理者が定期的に URL リストを更新し，各サイトのサイズを調査する．追加サイト選択フェーズでは，ユーザが目的サイトへアクセスする際に，決められた選択方法によって追加サイトを選び，そのサイトへ同時にアクセスする．以下で，それぞれのフェーズについて詳しく説明する．

5.3.1　サイズ調査フェーズ

サイズ調査フェーズの挙動を図 10 に示し以下で説明する．サイズの調査には Tor ネットワークに接続できる PC が必要になる．Tor の管理者はこの PC から Tor ネットワークを経由して様々な Web サイトにアクセスする（図 10(a)）．そして，このときのトラフィックから総通信量を抽出する（同図 (b)）．抽出した総通信量を URL リストの対応する Web サイトに追加する（同図 (c)）．上記の処理を定期的に行い，URL リストを更新する．これにより，時間とともにコンテンツが変化するニュースサイト・動画投稿サイトなどにも対応できるようになる．更新された URL リストを Tor ネットワークの経路情報を管理しているディレクトリサーバへ送信する（同図 (d)）．ディレクトリサーバは，ユーザが経路情報を取得する際に URL リストも同時に送信する（同図 (e)）．

5.3.2　追加サイト選択フェーズ

追加サイト選択フェーズの挙動を図 11 に示し以下で説明する．ユーザは目的サイトの URL を入力する (図 11 の (a))．URL リスト内の各サイトのサイズを考慮してランダ

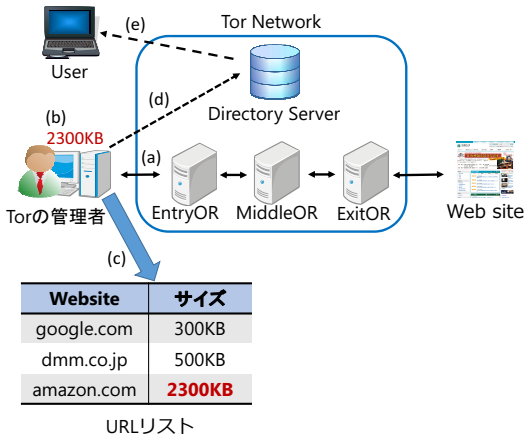

図 10　サイズ調査フェーズの概略図
Fig. 10　Schematic view of the size examination phase.

ムに URL を選択する (同図の (b))．目的サイトと追加サイトへ同時にリクエストを送信する（同図の (c))．

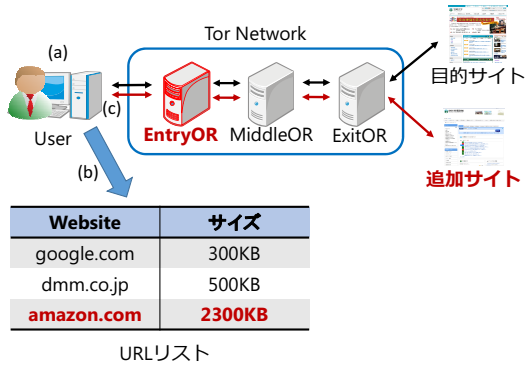

図 11　追加サイト選択フェーズの概略図
Fig. 11　Schematic view of the additional site selection phase.

6.　提案手法の有効性

本章では，5 章で提案した手法の有効性を実験により評価する．また，Camouflage 手法も実験を行い提案手法と比較評価する．

6.1　概要

本実験の目的は，3 章で示した指紋攻撃の脅威に対して提案手法がどの程度有効であるかを評価することである．本実験では二つの状況を想定している．

『想定する状況』

Case1　攻撃者は対策が適用されていない Tor を使用して学習し，ユーザは対策が適用された Tor を使用している場合

この場合，攻撃者は目的サイトの指紋情報を収集して学習することができるが，識別フェーズでは目的サイトの指紋情報を収集することができない．

Case2　攻撃者は対策が適用された Tor を使用して学習し，ユーザは対策が適用された Tor を使用している場合

この場合，攻撃者は学習フェーズ及び識別フェーズにおいて，目的サイト本来の指紋情報を収集することができない．

本実験では，評価指標として全体識別率，目的サイトのロード時間，全体の総通信量（目的サイト+追加サイト)，追加通信量を用いる．ここで，追加通信量とは提案手法または Camouflage 手法を適用した場合の追加サイトの平均の総通信量を表している．また，ロード時間，全体の総通信量においては対策を適用しない場合についても評価する．

6.2　実験環境

実験環境は 3 章と同様である．ただし，本提案手法ではサイズの大きいサイトは対象としないため，実験で用いる Web サイトは 2700KB 未満のサイト 100 サイトとする．また，簡易的に行うため実験でアクセスする Web サイトのリスト（目的サイトリスト）と URL リストは同じものを使用する．URL リストは予め構築しておく．

6.3　実験方法

実験方法は 3 章と同様である．

6.4　実験結果

*Case*1，*Case*2 における識別率を表 2 に示す．また，表 3 は提案手法または Camouflage 手法を適用した場合，対策を適用しない場合の総通信量，追加通信量，ロード時間を表している．図 12，図 13 は，それぞれ各状況における識別率ごとのサイト数を表している．

表 2　*Case*1，*Case*2 における識別率
Table 2　identification rate in *Case*1,*Case*2.

状況	Camouflage 手法	提案手法
*Case*1	7.95%	5.05%
*Case*2	8.15%	4.40%

表 3　各対策の適用における総通信量，追加通信量，ロード時間
Table 3　The total amount of communication and additional traffic and the load time in the application of each measure.

	総通信量	追加通信量	ロード時間
対策なし	911KB		17.04 秒
Camouflage 手法	1752KB	928KB	17.41 秒
提案手法手法	2029KB	1406KB	17.30 秒

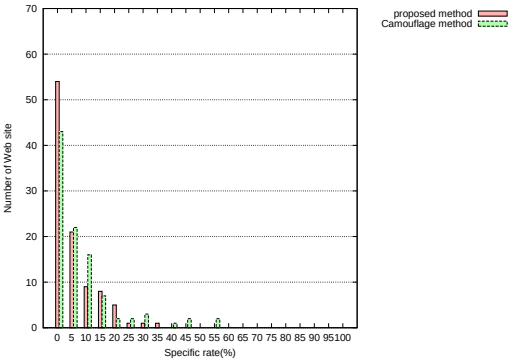

図 12　*Case*1 における特定率ごとのサイト数
Fig. 12　The number of sites for each specific rate of *Case*1.

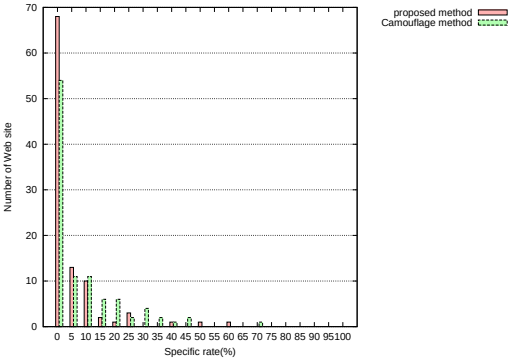

図 13　*Case*2 における特定率ごとのサイト数
Fig. 13　The number of sites for each specific rate of *Case*2.

6.5　評価・考察

表 2 より対策を適用する事で対策を適用していない場合の結果（3.4.3 節）と比べて識別率を大幅に低下できており指紋攻撃の対策が成功していると言える．また，Camouflage 手法よりも提案手法の方が各状況において低い識別率を示しており，提案手法の方が有効であることが分かる．図 12，図 13 を見ても提案手法の方が最大識別率も低く，識別率が 0% である Web サイトの数が多いことから，提案手法の方が指紋攻撃に対する対策として有効なものであると言える．しかし，表 3 を見て分かるように総通信量と追加通信量において提案手法の方がサイズが大きく，Tor ネットワークに与える負荷が大きいことが分かる．総通信量において提案手法では対策を適用しない場合の約 2.2 倍，Camouflage 手法に対しては約 1.9 倍と対策の適用による通信量の増加は今後の課題である．ロード時間においてはどれもさほど変化がなかったためユーザビリティの低下は防ぐ事ができる．しかし，全てのユーザが提案手法を適用した場合，Tor ネットワークに対する負荷は，本実験よりも大きくなるためロード時間はさらに長くなると考えられる．今後は，提案手法の適用による通信量の増加の改善や，本提案手法では対象外としたサイズの大きなサイトも対象とした提案手法の改良を考えていきたい．また，提案手法の適用による Tor ネットワーク全体の負荷を調査するために，Tor のシミュレータを利用した実験も行いたい．

7.　まとめ

本論文では，匿名通信システムの Tor に対して匿名性を低下させる指紋攻撃についてその脅威を測り，既存の対策手法である Camouflage 手法の問題点を改善する手法の提案を行った．本提案手法は，対策を適用しない場合と比べて全体識別率を 36.4 ポイント下げ，Camouflage 手法と比べて 3.1 ポイント下げることができた．また，目的サイトのロード時間は対策適用前とさほど変わらない結果だったため，本提案手法はユーザビリティを低下させることなく Camouflage 手法よりも指紋攻撃対策として有効であることが分かった．今後の課題として，本提案手法を適用した場合に発生する追加の通信を抑えることが挙げられる．対策を適用しない場合より総通信量は約 2.2 倍増加しているため，Tor ネットワークへの負荷の増加が懸念される．追加の通信を抑える方法として，現実の Web サイトにアクセスするのではなく，目的サイトのサイズに応じて適宜，適切なサイズの追加サイトに変えることが考えられる．この場合，適切なサイズを調査する必要があるが，無駄を減らし効率的な指紋攻撃対策になると考えられる．

参考文献

[1] David Chaum, Communications Of The Acm, R. Rivest, and David L. Chaum: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, Vol.24, pp.84-88(1981).
[2] Tor Project: Anonymity online, (online), available from (https://www.torproject.org/)(accessed 2016-01-29).
[3] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In In Proceedings of the 13 th Usenix Security Sym-posium(2004).
[4] U.S. Naval Research Laboratory: U.S. Naval Research Laboratory (online), available from (http://www.nrl.navy.mil/)(accessed 2016-01-29).
[5] Panchenko, A., Niessen, L., , and Zinnen, A: Website ngerprinting in onion routing based anonymization networks, ACM, pp.1-10 (2011).
[6] Dominik Herrmann, Rolf Wendolsky, and Hannes Federrath: Website fingerprinting: attacking popular privacy enhancing technologies with the multinomial naive-bayes classier, In Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW'09, pp.31-42(2009).
[7] 横手健一, 松浦幹太: 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, Computer Security Symposium 2012, Vol.3, pp.624-631(2012).
[8] Yi Shi and Kanta Matsuura: Fingerprinting attack on the tor anonymity system, Sihan Qing, Chris J. Mitchell, and Guilin Wang, editors, ICICS,Vol.5927 of Lecture Notes in Computer Science, pp.425-438(2009).
[9] Xiang Cai, Xin Cheng Zhang, Brijesh Joshi and Rob Johnson: Touching from a distance: website fingerprinting attacks and defenses, CCS'12 Proceedings of the 2012 ACM conference on Computer and communications security, pp.605-616(2012).
[10] Alex Biryukov, Ivan Pustogarov, Ralf-Philipp Wein-

mann: TorScan: TracingLong-Lived Connections and Differential Scanning Attacks, Computer Security ESORICS 2012, Lecture Notes in Computer Science Vol.7459, pp.469-486(2012).
[11] Wireshark: Wireshark About(online), available from (http://www.wireshark.org/about.html)(accessed 2016-01-29).