Vol.2017-IOT-36 No.32
2017/3/4

Torネットワークにおける 匿名サーバのIPアドレス収集手法

小泉 賢人[1]　吉浦 紀晃[1]

概要：近年, プライバシー保護等の観点から, インターネット 利用におけるユーザの匿名性について関心が高まってきた．インターネットの通信経路を匿名化できる，最も普及しているソフトウェアとして The Onion Router(Tor) がある．Tor にはユーザとサーバの匿名性を保つ機能として，Hidden Service が利用できる．この機能を利用したサーバを匿名サーバと呼ぶ．本論文では，匿名サーバの通信の特徴を分析した結果について述べる．また，分析結果に基づき，匿名サーバの IP アドレスの収集手法を提案する．さらに，実験により提案手法の有効性を示す．

キーワード：Tor, Hidden Service, 通信分析

A Method of collecting the IP addresses of Hidden Server in Tor networks

Kento Koizumi[1]　Noriaki Yoshiura[1]

Abstract: Anonymity in the Internet has attracted attention from the viewpoint of privacy protection and so on in recent years. The Onion Router (Tor) is one of the most popular software that can anonymize the Internet connection paths. Tor can provide Hidden Service that keeps the anonymity for both of users and servers. A server that uses this function is called a hidden server. This paper analyzes the communication characteristics of hidden servers. Based on the results of the analysis, this paper also proposes a method to collect IP addresses of hidden servers. Furthermore, the effectiveness of the proposed method is shown by experiment.

Keywords: Tor, Hidden Service,Communication analysis

1. はじめに

近年，プライバシー保護等の観点から，インターネット利用におけるユーザの匿名性について関心が高まってきた．通常，インターネットを利用した通信にはユーザに関する様々な情報が付随するため，インターネットサービスプロバイダ (ISP) の協力があれば，通信を行ったユーザの特定が可能である．このような状況は，インターネットユーザのプライバシーが保護されているとは言えない．現在，インターネットの通信経路を匿名化できる，最も普及しているソフトウェアとして Tor(The Onion Router) が挙げられる．Tor は Tor ユーザ（client ノード）から送信されたパケットを，relay ノードと呼ばれる PC 等が中継することにより，Tor ユーザの匿名性を実現している．さらに Tor にはユーザのみではなく，サーバ側の匿名性を保つ事が可能なサービスとして，Hidden Service が存在する．Hidden Service とは，ユーザ側もサーバ側も匿名性を保ちつつ，HTTP サーバ等の各種サーバを提供することができるシステムである．Hidden Service では”半角英数字 16 桁.onion”の特殊なアドレスを用いて通信を行う．また，Hidden Service を利用したサーバを”匿名サーバ”と呼ぶ．本来，Tor は通信検閲への対抗策として利用される

[1] 埼玉大学大学院理工学研究科
Graduate school of Science and engineering.
Saitama University

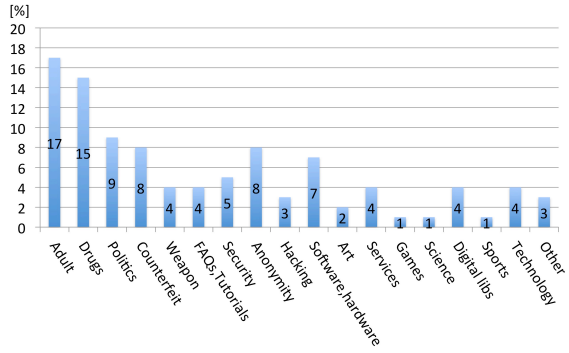

図 1　Hidden Service による web ページの内容
Fig. 1　Content of web pages by Hidden Services

が，一方で，その匿名性を悪用した犯罪が発生している．Silk Road[7] という Hidden Service では違法薬物や偽造パスポートの取引が行われていた．また，児童ポルノの配布・販売を行う Hidden Service も存在する．

Biryukov らの研究 [2][3] では，英語で記述された 1813 個の Hidden Service による web ページを提供している内容により分類した．その結果は，違法薬物，アダルトコンテンツ，偽造 (盗品のクレジットカード，ハッキングされたアカウント等)，武器と分類された Hidden Service が 44%を占めた．これらの事から Hidden Service は本来の目的として利用されている可能性が低いと考えらえる．

しかし，匿名サーバを特定することは極めて困難である．匿名サーバが直接接続している relay ノードであれば匿名サーバの IP アドレスを知ることはできるが, relay ノードは，その IP アドレスが匿名サーバのものであるか否かの判断ができない．また，relay ノードへ送信されるパケットは暗号化されているため，relay ノードはパケットの中身を知ることはできない．2015 年 9 月に京都府警らによって，匿名サーバへ児童ポルノをアップロードしていた 3 人が逮捕された [13]．しかし，これは匿名サーバ上で児童ポルノの取引に使われていた BitCoin[14] の購入履歴から特定された容疑者である．匿名サーバへ児童ポルノをアップロードしていた人は少なくとも 800 人以上いると見られており，匿名サーバの管理者も逮捕されていないという実態がある．このような状況は好ましくないため，匿名サーバの特定に関する情報を収集する必要がある．

そこで，本論文では匿名サーバと直接接続する relay ノードを用いて通信をキャプチャし，その通信の特徴から匿名サーバを識別する手法を提案する．これにより，匿名サーバと直接接続する relay ノードは，キャプチャした通信から匿名サーバの IP アドレスを収集することが可能である．本論文では実際の Tor ネットワーク上に，匿名サーバ，relay ノード，client ノードを用意し通信の特徴を分析した．分析方法は，匿名サーバが Tor ネットワークを利用し始める時の通信と，client ノードが Tor ネットワークを利用し始める時の通信を、それぞれが直接接続する relay ノードにてキャプチャし，その通信の特徴を分析した．分析の結果，client ノードが relay ノードに直接接続する際と，匿名サーバが relay ノードに直接接続する際には，接続の開始直後の数秒の通信の特徴に大きな違いが出ることが分かった．

また，提案手法の有効性を検証するため，relay ノードに直接接続してきたノードが匿名サーバであるか否かを判定する実験を行った．実験では relay ノードに直接接続してきたノードが匿名サーバであるか否かを 100 %判定することが可能であった．これにより匿名サーバの IP アドレスを収集することが可能となる．

本論文は，全 8 章から構成される．2 章は Tor について，3 章は Hidden Service について述べる．4 章は Hidden Service の通信分析について，5 章では提案手法について述べる．6 章では提案手法の有効性を検証する実験とその結果について述べる．7 章に関連研究を紹介し，最後の 8 章ではまとめと今後の課題について述べる．

2. Tor

2.1 Tor の概要

Tor はパケットを Tor ネットワークに参加しているノードを経由することにより通信経路を秘匿化する．Tor ネットワークとは以下のノードと directory サーバから構成される [8]．

client ノード
Tor ネットワークを利用して匿名通信を行うだけのノードである．client ノードがパケットを中継することはない．Tor をインストールすると，初期設定では client ノードとなる．

relay ノード
他のノードから送信されたパケットを中継する．直接 Tor ネットワーク外のサーバへは接続せず，他の relay ノードまたは exit ノードへパケットを中継するのみである．

guard ノード
relay ノードの中でも，client ノードと直接接続する特別なノードである．帯域幅が大きく，安定して稼働している relay ノードのみが guard ノードになることが可能である．

exit ノード
relay ノードから送信されたパケットを直接 Tor ネットワーク外のサーバへ送信する．Tor ネットワーク外のサーバのログとして残るのはこの exit ノードの IP アドレスとなる．

directory サーバ
relay ノードや exit ノードのリストを client ノードに

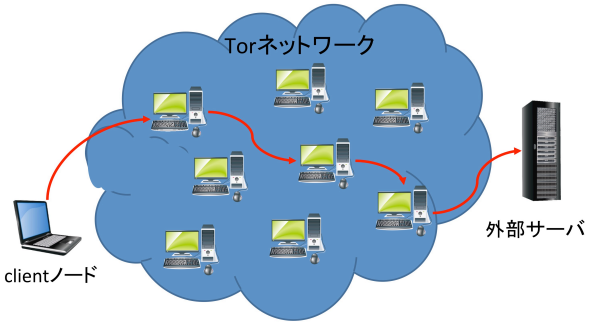

図 2　Tor ネットワーク
Fig. 2　Tor Network

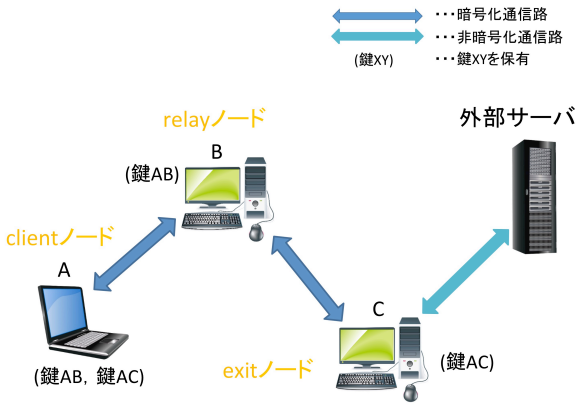

図 3　Tor の匿名通信経路
Fig. 3　Anonymous communication circuit in Tor

提供する．client ノードはこのリストから relay ノードと exit ノードを選び，通信経路を確立する．また，このリストには relay ノードの帯域幅の情報等も記載されている．

上記を用いて Tor ユーザは，client ノード→ guard ノード→ relay ノード→ exit ノード→外部のサーバへとアクセスすることにより，通信経路を秘匿化する．

2.2　匿名通信経路の設立

Tor ネットワークを用いた通信は多段に暗号化されている．以下に client ノードから Tor ネットワーク外のサーバへの通信の概略を図 3 に記す．通常 relay ノード 2 台と exit ノード 1 台を用いて形成されるが，ここでは説明の簡略化のため relay ノード 1 台と exit ノード 1 台を用いる．

(1) A は directory サーバから relay ノードと exit ノードのリストを入手する．このリストには relay ノードや exit ノードの公開鍵等の匿名経路通信に必要な情報が含まれている．A はリストの中からランダムに B，C を選択する．
(2) A から B へ接続要求を行い，暗号化通信路用のセッションキー（以下，鍵 AB とする）を交換し，AB 間での暗号化通信路が作られる．
(3) A から B へ，BC 間の暗号化通信路の確立を要求し，BC 間の暗号化通信路が確立される．同時に AC 間のセッションキー（以下，鍵 AC とする）を生成する．
(4) B から A へ，BC 間の暗号化通信路が確立されたことを通知する．
(5) A から B へ，「外部サーバとの接続を要求する」という命令を鍵 AC で暗号化し，さらに，「このパケットを C へ送信することを要求する」という命令を鍵 AB で暗号化し送信する．B は鍵 AB でパケットを復号化し，C へ送信する．B は鍵 AC で暗号化された命令は復号化できない．
(6) C は B から送信されたパケットを鍵 AC で復号化し，外部サーバとの接続を確立する．
(7) C から B へ，「外部サーバとの接続が確立された」ことを鍵 AC で暗号化し，B へ送信する．
(8) B から A へ，C から送信されたパケットを鍵 AB で暗号化し，A へ送信する．
(9) A は B から送信されたパケットを鍵 AB，鍵 AC を用いて復号化し，外部サーバとの匿名通信経路が確立されたことを確認する．
(10) AD 間の通信は A → B → C → 外部サーバ と経て行われる．以上により，AD 間の匿名通信経路が確立される．

2.3　TorBrowser

Tor のユーザが Tor ネットワークを利用して web ブラウジングを行う際は，TorBrowser[12] がよく利用されている．TorBrowser は Tor の運営団体である Tor Project が利用を推奨しているブラウザである．Tor の匿名性を脅かす脆弱性を持つとして知られている JavaScript を利用した web ページを表示しない等の機能を初期設定として持つ．

3.　Hidden Service

Hidden Service は”半角英数字 16 桁.onion”という特殊なアドレスを持つ．以下の要素と client ノードから構成される [8]．

匿名サーバ/Hidden Server(HS)
Hidden Service を提供しているサーバである．Hidden Service の提供を開始すると公開鍵・秘密鍵のペアと“半角英数字 16 桁.onion”というアドレスを生成する．

Introduction Point(IP)
Hidden Service の要求を受けて，client ノードからの接続を待ち受ける．IP は relay ノードのリストの中から選ばれる．

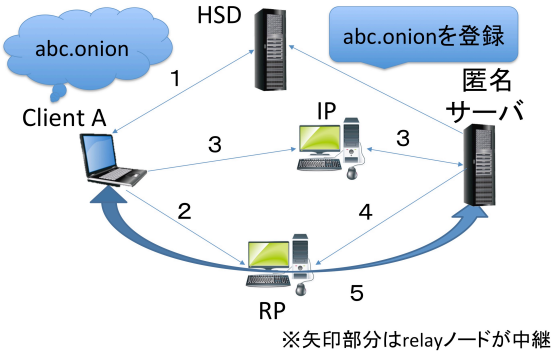

図 4　Hidden Service へのアクセス
Fig. 4　Access to Hidden Service

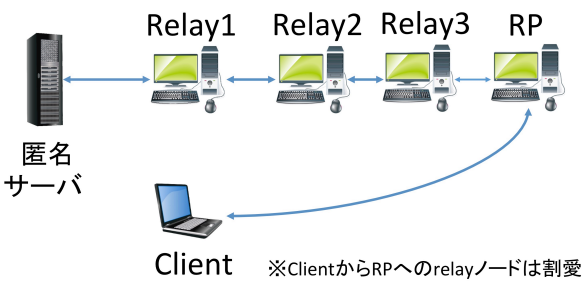

図 5　匿名サーバと通信を行う際に使用する経路
Fig. 5　Circuit used to communicate with hidden server

Hidden Service Directory Server(HSD)
“半角英数字 16 桁.onion”のアドレスと対応する HS を識別するための情報と IP の位置情報を持っている．Hidden Service における DNS サーバの役割を果たす．

Rendezvous Point(RP)
client ノードからの要求を受けて，HS との接続に用いられる．通常，relay ノードのリストの中からランダムに選ばれる．

client ノード A が“abc.onion”という Hidden Service に接続する際の手順は以下のようになる．概要は図 4 に示す．

(1) A は“abc.onion”というアドレスを知り，HSD に対してそのホストネームの IP に関する情報と HS の公開鍵を要求し，入手する．
(2) A は relay ノードからランダムに RP とするノードを選び，Rendezvous Cookie(RC) と呼ばれるワンタイムパスワードを伝える．
(3) A は IP へ，RP に関する情報と RC を HS の公開鍵で暗号化して送信し，この情報を HS へ送信することを要求する．IP はこの情報を HS へ送信する．
(4) HS は秘密鍵で復号化し，RP に関する情報と RC を得る．また，RP へ接続要求と RC を送信する．
(5) RP は RC が正しいことを確認し，A に対して，HS との匿名通信経路が確立されたことを通知する．以降，この匿名通信経路を用いて A さんと HS は互いに匿名のままに通信が可能となる．

以上の手順により，A と HS が互いに実際の IP アドレスを知る事が無く，相互に通信が可能となる．また，A と HS の間で匿名通信経路を確立する際にセッションキーを生成しているため，RP に通信の内容を知られることはない．

4. Hidden Service の通信分析

4.1 目的

guard ノードにてパケットをキャプチャし，client ノードからの通信と匿名サーバからの通信の特徴に違いを発見することを目的とする．client ノードからの通信と匿名サーバからの通信の特徴に違いを発見する事ができれば，guard ノードにて収集したパケットログから client ノードの IP アドレスと匿名サーバの IP アドレスに分類することができる．これにより匿名サーバの IP アドレスが収集可能となる．client ノードや匿名サーバと直接接続する guard ノードは，relay ノードの IP アドレスが公開されているため Tor ネットワーク外からの通信であることは判断できるが，client ノードからの通信であるか，匿名サーバからの通信であるかはパケットの暗号化のため判断することができない．

4.2 分析方法

client ノード，relay ノード，匿名サーバを実際の Tor ネットワーク上に用意した．client ノードが使用するブラウザは TorBrowser，匿名サーバで提供する web ページはサーバソフトウェアである Apache2[1] のデフォルトページとした．guard ノードを用意することはネットワークの環境上困難であった．guard ノードとなるためには，少なくとも 2Mbytes/sec 程度の帯域幅が必要となる．relay ノードに用いた PC の帯域幅を BNR スピードテスト [4] を利用し観測したところ，約 11.25Mbytes/sec であることを確認した．Tor では relay ノードの帯域幅の測定する際に，directory サーバから relay ノードを用いて外部サーバへ通信経路を確立し，ファイルをダウンロードすることにより relay ノードの帯域幅を測定する．これにより観測された用意した relay ノードの帯域幅は最高で 1Mbytes/sec 程度であった．また，日本で最も帯域幅の大きい relay ノードでも約 3.8Mbytes/sec である．

これは，Tor の暗号化プロセスによる遅延の他に，directory サーバが欧米に位置することに起因すると考えられる．物理的な位置が離れていることから，測定される relay

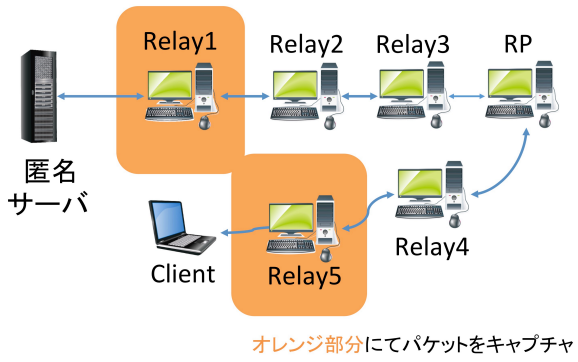

図 6　Hidden Service の通信分析
Fig. 6　Analysis of communication with hidden server

ノードの帯域幅低くなる可能性が高い．日本で guard ノードとなっているノードは 2017 年 1 月現在 2 つのみである．しかし，本来 guard ノードでなければ client ノードや匿名サーバと直接接続することはできないが，client ノードと匿名サーバの Tor 設定ファイルである”torrc”を改変し，relay ノードでも client ノードや匿名サーバと直接接続できるように設定した．この設定変更によるパケットを中継する PC の数等への影響はない．client ノードから匿名サーバへアクセスする際の通信を，client ノードと匿名サーバに直接接続する relay ノードにてパケットをキャプチャし，通信の特徴を分析した．概要は図 6 のようになる．client ノードと匿名サーバ間で送受信される全てのパケットを relay ノードにてキャプチャした．また，パケットのキャプチャソフトには wireshark[11] を使用した．client ノードと匿名サーバ間の通信ではパケットが暗号化して送信されるため，relay ノードではパケットの内容を読み取ることはできない．そのため，パケット長，パケットの送受信回数から通信の特徴を分析する．

4.3　分析結果

4.3.1　パケット長

client ノードから匿名サーバへアクセスする際に送受信されるパケットを relay ノードにてキャプチャし，パケット長を測定した．結果は，66bytes，283bytes，609bytes，2962bytes のパケットを client ノードと直接接続している relay ノードと匿名サーバと直接接続している relay ノードの両方で確認した．66bytes のパケットは ACK の送信に用いられるもので，2962bytes のパケットは [TCP segment of a reassembled PDU] と呼ばれる，パケット受信時にセグメントが分割されて送られたことを意味するパケットである．66bytes と 2962bytes のパケットは Tor によって暗号化されないパケットである．実際に匿名サーバの web ページの情報を含んだパケットは 283bytes，と 609bytes

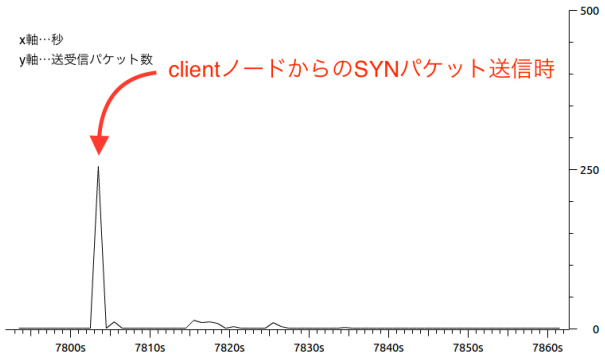

図 7　client ノードと relay ノードのパケット送受信記録
Fig. 7　Sending and receiving records of packets between client node and relay node

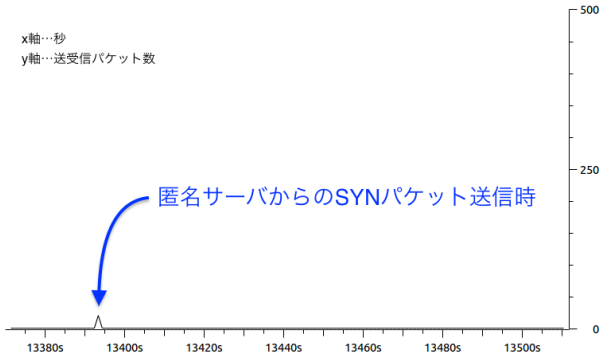

図 8　匿名サーバと relay ノードのパケット送受信記録
Fig. 8　Sending and receiving records of packets between hidden server and relay node

であるが，このパケットも client ノードと直接接続している relay ノードと匿名サーバと直接接続している relay ノードの両方で見られ，通信の特徴に違いを見つけることは困難であった．また，パケット長は client ノードが動画サイト等の通信量の大きいサイトを閲覧した際に増加するが，動画等を提供している匿名サーバからの通信量も増えるためパケット長から通信の特徴に違いを見つけるのは困難である．

4.3.2　パケットの送受信回数

client ノードから匿名サーバへアクセスする際には，client ノードと直接接続している relay ノードと，匿名サーバと直接接続しているノードの両方とも約 50 回の送受信が行われていた．しかし，client ノードと匿名サーバが通信を行う以前の，client ノードが Tor ネットワークに接続する際と，匿名サーバが Tor ネットワークに接続する際には，relay ノードで観測されるパケットの送受信回数が異なることが分かった．client ノードが Tor ネットワークへ接続する際には 265 回，匿名サーバが Tor ネットワークへ接続する際には 20 回のパケットの送受信が relay ノードと行われた．図 7 は client ノードと relay ノード間，図 8 は匿名サーバと relay ノード間の Tor ネットワークへ接続する際のパケット送受信回数をグラフにしたものである．relay

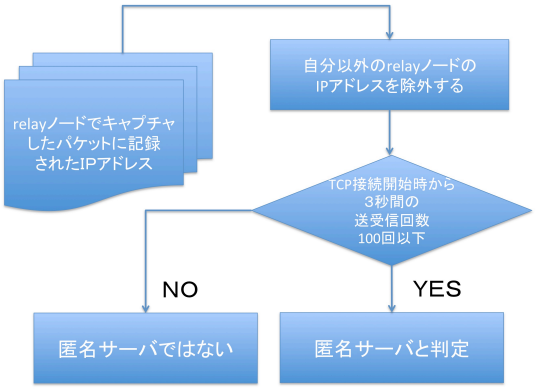

図 9　提案手法
Fig. 9　Proposed method

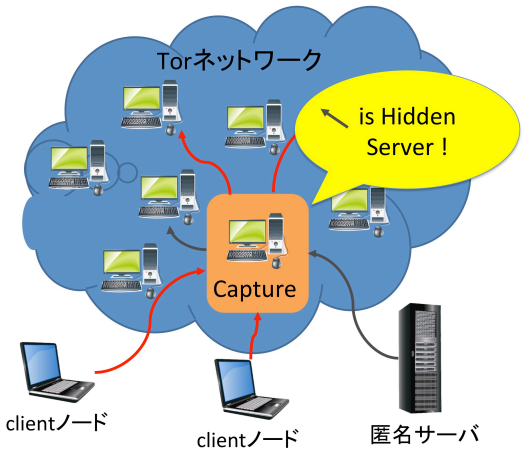

図 10　guard ノードによる匿名サーバの推定
Fig. 10　Estimate hidden servers by guard nodes

ノードが SYN パケットを受信してから 3 秒間の送受信回数の差は大きく，明らかな通信の特徴の違いを確認できる．また，Tor ネットワークへ接続する際に通信の特徴の違いが見られるため，client ノードがどのような web サイトを閲覧するか，あるいは匿名サーバがどのような web サイトを提供するかといった状況に影響されにくいと考えられる．

5.　提案手法

relay ノードでのパケットの送受信回数の分析結果に基づき，図 9 に示す手法を提案する．また，本論文での TCP 接続開始時とは，client ノードまたは匿名サーバが Tor ネットワークに接続する際の SYN パケットを relay ノードが受信した時を指す．提案手法では，まず，relay ノードでキャプチャしたパケットに記録された IP アドレスから自分以外の relay ノードの IP アドレスを除外する．これは，relay ノードの IP アドレスは Tor Network Status[5] や directory サーバから提供されるファイルにて確認することができる．次に，TCP 接続開始時から 3 秒間のパケットの送受信回数を relay ノードのパケットログから測定する．TCP 接続開始時から 3 秒間のパケットの送受信回数が 100 回以下であれば匿名サーバと判定する．この提案手法では，図 10 のように，guard ノードのみで匿名サーバを推定することが可能なため，実現可能性が高い．また，提案手法では guard ノードでパケットをキャプチャするのみで匿名サーバの推定することが可能なため，匿名サーバから見れば，この guard ノードは通常の振る舞いに見える．これにより匿名サーバの管理者に気付かれる可能性は極めて低いと考えらえる．

6.　実験

6.1　実験方法

client ノードとして Tor ネットワークに接続する際の通信と，匿名サーバとして Tor ネットワークに接続する時の通信を relay ノードにてパケットをキャプチャし，提案手法により匿名サーバであるか判定する実験をした．また，OS や PC の性能による影響を排除するため，client ノードとして利用する PC と匿名サーバとして利用する PC は同一の PC を用いて実験を行った．

6.2　実験結果

提案手法により匿名サーバであるか判定する実験を行った結果を表 1 に示す．図 11 は実験時の client ノードと relay ノードのパケット送受信記録の例，図 12 は実験時の匿名サーバと relay ノードの送受信記録の例である．提案手法を利用することにより，100 %匿名サーバを判定することが可能であった．TCP 接続開始時から 3 秒間のパケット送受信回数は，匿名サーバでは最大 24 回と閾値の 100 を大きく下回る結果となった．client ノードとの TCP 接続開始時から 3 秒間のパケット送受信回数は最小 168 回，最大 448 回と送受信回数に振り幅が大きかった，しかし，振れ幅はあるが閾値を下回ることはなく，提案手法による匿名サーバの IP アドレスの判定が有効であることを示した．

6.3　実験結果の考察

client ノードとの通信の特徴と匿名サーバとの通信の特徴に大きな違いが出た理由は，client ノードでは TorBrowser を起動することに起因すると考えられる．匿名サーバでは Introduction Point との通信経路を設立するのみだが，client ノードでは TorBrowser の初期画面のデータや接続が切れた際のための予備の通信経路等のパケットの送受信が行われるため，client ノードの方が TCP 接続開始後 3 秒間のパケットの送受信回数が格段に多かったと考えられる．

実験で用いる client ノードには，TorBrowser のデフォルトページを使用したが，TorBrowser には起動時に空白のページを表示することが可能である．この空白のページ

表 1　実験結果
Table 1　Result of the experiments

TCP 接続開始時から 3 秒間のパケット送受信回数	匿名サーバ	client ノード
最小	20 回	168 回
最大	24 回	448 回
平均	21.2 回	277.8 回
試行回数	100 回	100 回
閾値 100 以下	100 回	0 回

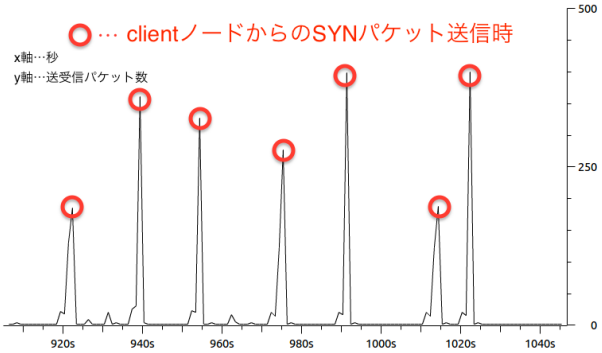

図 11　実験時の client ノードと relay ノードの
パケット送受信記録の例
Fig. 11　Example of sending and receiving records of packets between client node and relay node during experiments

図 12　実験時の匿名サーバと relay ノードの
パケット送受信記録の例
Fig. 12　Example of sending and receiving records of packets between hidden server and relay node during experiments

を表示する設定の client ノードと直接接続する relay ノードの TCP 接続開始時から 3 秒間のパケット送受信回数は約 22 回程度であった．これは匿名サーバと直接接続する relay ノードとのパケット送受信回数と似ている．しかし，client ノードの場合は TorBrowser を起動後に何らかの web ページを表示する可能性が高い．web ページを表示した際には 100 を悠に超える回数のパケットの送受信を行う．この挙動は匿名サーバでは考え難い．よって，TCP 接続開始後 30 秒間程度のパケット送受信回数にも着目することで，TorBrowser 起動時に空白のページを利用しているユーザと匿名サーバの通信の特徴に違いを見つけることができると考えられる．

7.　関連研究

7.1　匿名サーバの IP アドレス特定手法

Øverlier らの研究 [6] では，Hidden Service を提供している匿名サーバを特定する攻撃手法を提案した．特定方法は，以下のようなものである．また，図 13 は攻撃者が狙う位置関係を示す．

(1) 攻撃者は client ノードと relay ノードを用意する．
(2) 攻撃者の client ノードはターゲットの Hidden Service へアクセスし，その時に用いた匿名通信経路を破棄する．これを繰り返し，Hidden Service への匿名通信経路を何度も生成する．
(3) 攻撃者の relay ノードでは通信記録を取得し，攻撃者の client ノードと Hidden Service が同一の匿名通信経路上に存在するかをタイミング解析により確認する．
(4) 攻撃者の relay ノードが Hidden Service と直接接続する relay ノードとなるまで続ける．

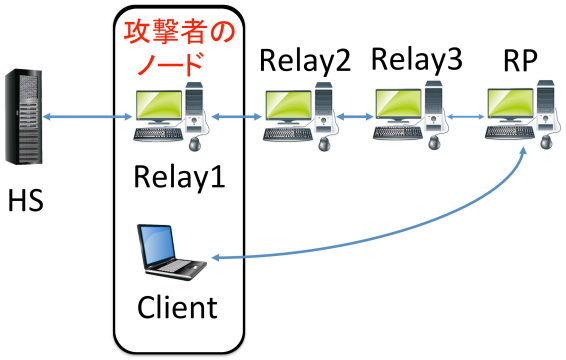

図 13　匿名サーバ特定時に攻撃者が狙う位置関係
Fig. 13　The positionnal relationship targeted by a attacker when specifying a hidden server

これにより，攻撃者は Hidden Service の IP アドレスを取得し，サーバの位置を特定することが可能である．しかし，これは 2006 年以前の Hidden Service への有効な攻撃方法である．現在では，Hidden Service と直接接続する relay ノードを，予め選んだ数個の内から用いて，30 日〜60 日間使用し続ける“Entry Guard”とよばれるプロトコ

ルが存在する．これにより，通信経路を破棄することを繰り返しても，Hidden Service の IP アドレスを取得することができない．

本論文では，匿名サーバへ攻撃すること無く匿名サーバの IP アドレスを収集する．受動的に情報収集を行うことが可能なため，匿名サーバの管理者に気付かれる可能性が低い．

7.2 guard ノードへの DoS 攻撃

“Entry Guard”により，攻撃者は狙った Hidden Service の guard ノードとなり Hidden Service の IP アドレスを取得することが困難になった．そこで，Jansen らの研究 [9] では guard ノードへ DoS 攻撃を行い，guard ノードの OS から Tor プロセスを終了させる攻撃手法を提案した．実際の Tor ネットワークへの影響を考慮し，実験には Tor ネットワークのシミュレーターとして Shadow[10] を用いた．攻撃手法は以下のようなものである．

(1) Hidden Service の guard ノードを特定する．
(2) guard ノードに対して DoS 攻撃をしかけ，guard ノードの OS から Tor プロセスを終了させる．
(3) 攻撃者の用意した relay ノードが Hidden Service の guard ノードとなるまで 1. から繰り返す．

攻撃者の relay ノードが Hidden Service の guard ノードとして選ばれているか否かの判別は，7.1 節で述べたタイミング解析や，Biryukov ら [3] の提案したパディングによる指紋攻撃を用いる．また，DoS 攻撃の手法は，以下のようになる．

(1) 攻撃者の client ノードは，ターゲットの guard ノードを通信経路に用いて，Tor ネットワーク外のサーバーから大容量のデータダウンロードを行う．
(2) 攻撃者の client ノードは，ターゲットの guard ノードからのデータの読み込みを停止する．
(3) 攻撃者の client ノードは，exit ノードに対し，データを送信し続けるよう要求する．
(4) ターゲットの guard ノードは，OS から Tor プロセスが終了させられるまでデータをバッファし続ける．

これは，Tor ネットワークのプロトコルの欠陥を突いた DoS 攻撃であり，攻撃者の client ノードは 92 KB/sec しか帯域幅を使用せずに，ターゲットの guard ノードでは 2187 KB/sec も消費させる事が可能であった．また，この攻撃は並行して実行することが可能である．

本論文では，guard ノードへの攻撃を行うことはない．悪意のある Hidden Service を提供している匿名サーバの guard ノードであっても，guard ノードはその事を知らずにパケットを中継しているためである．

8. おわりに

本論文では，Tor ネットワークにおける匿名サーバの IP アドレス収集を目的として，Tor と Hidden Service について述べ，匿名サーバの通信の特徴についてパケット長とパケットの送受信回数から分析した結果についても述べた．また，匿名サーバと直接接続する relay ノードを用いて通信をキャプチャし, その通信の特徴から匿名サーバを識別する手法を提案した．これにより，匿名 サーバと直接接続する relay ノードは，キャプチャした通信から匿名サーバの IP アドレスを収集することが可能である．また，提案手法の有効性について実験した結果も述べた．

今後の課題として，より良い匿名サーバの IP アドレス収集手法の構築と匿名サーバの IP アドレスの特定手法の構築が挙げられる．

参考文献

[1] Apache Software Foudation : Apache HTTP server 入手先 ⟨http://www.apache.org⟩（参照 2017-01-15）.
[2] A. Biryukov, I. Pustogarov, F. Thill, and R. P. Weinmannn, “Content and popularity analysis of Tor hidden services”, In Proc. of the 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW), pp.188-193, 2014.
[3] A. Biryukov, I. Pustogarov, and R. P. Weinmannn, “Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization”, In Proc. of the 2013 IEEE Symposium on Security and Privacy, pp.80-94, 2013.
[4] Broadband Networking Rport : BNR スピードテスト http://www.musen-lan.com/speed/ （参照 2017-01-15）.
[5] Kasimir Gabert : Tor Status - Tor Network Status 入手先 ⟨https://torstatus.blutmagie.de⟩（参照 2017-01-10）.
[6] L. Øverlier and P. Syverson:Locating Hidden Servers, In Proc. of the 2006 IEEE Symposium on Security and Privacy, pp.100-114, 2006.
[7] N. Christin, :Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace, In Proc. of the 22nd International Conference on the World Wide Web, pp.213-223, 2013.
[8] R. Dingledine, N. Mathewson, and P. Syverson, : Tor: The Second-Generation Onion Router, In Proc. of the 13th USENIX Security Symposium, 2004.
[9] R. Jansen, F. Tschorsch, A. Johnson, B. Scheuermann, “The sniper attack: Anonymously deanonymizing and disabling the Tor network”, In Proc. of the 21st Annual Network & Distributed System Security Symposiumu(NDSS), 2014.
[10] R. Jansen and N. Hopper,: Shadow: Running Tor in a Box for Accurate and Efficient Experimentation,In Proc. of the 19th Symposium on Network and Distributed System Security (NDSS), 2012.
[11] The Wireshark team : Wireshark 入手先 ⟨https://www.wireshark.org⟩（参照 2017-01-15）.
[12] Tor Project:Anonymity Online https://www.torproject.org （参照 2017-01-15）.
[13] 発信元隠す匿名通信システム「Ｔｏｒ（トーア）」悪用した児童ポルノ法違反京都府警ら全国初摘発:産経 WEST, 入手先 ⟨http://www.sankei.com/west/news/150929/wst15092 90071-n1.html⟩ （参照 2017-01-10）.
[14] BitCoin: 入手先 ⟨https://www.bitcoin.com/⟩（参照 2017-01-15）.