修 士 論 文

秘匿・匿名通信の分類に関する研究

北陸先端科学技術大学院大学
情報科学研究科情報科学専攻

川瀬 拓哉

2012 年 3 月

修 士 論 文

秘匿・匿名通信の分類に関する研究

指導教官　篠田陽一 教授

審査委員主査　篠田陽一 教授
審査委員　丹康雄 教授
審査委員　知念賢一 特任准教授

北陸先端科学技術大学院大学
情報科学研究科情報科学専攻

0810016 川瀬 拓哉

提出年月: 2012 年 2 月

概 要

インターネット上で金銭に関わるやりとり等の重要な通信を安全に行うため、通信内容や情報の発信者を隠蔽する技術が利用されている。この技術により、インターネット上で秘匿性や匿名性を確保した通信を行うことが可能となっている。しかし、この秘匿性や匿名性を悪用して、ファイル共有ソフトによる著作権の侵害、掲示板への誹謗中傷の書き込みといった行為が行われ問題となっている。そのため、これらの通信を制御・監視する技術の研究開発が行われ利用されている。両技術の関係はどちらか一方が強い状況になると、悪用が横行したり、安全を確保したサービスの提供が出来なくなる可能性がある。そこで、両技術が対等な関係を維持し続けるため、両技術の関係を明らかにする手法が必要となる。本研究の目的は、数多く存在する秘匿・匿名通信の技術を比較し、制御・監視する者にとって脅威となり得る技術を洗い出す手法の提案である。

本研究では、秘匿・匿名通信を「なんらかの情報を隠蔽する通信」と定義し、この通信を実現する技術を秘匿・匿名技術と呼ぶ。秘匿・匿名通信が隠蔽する情報として、「通信内容・種類」「通信経路」「通信した事実」がある。一般的な定義では、秘匿通信が「通信内容・種類を隠蔽した通信」、匿名通信が「通信経路を隠蔽した通信」に当てはまる。秘匿通信の代表的な技術には、共通鍵方式の AES(Advanced Encryption Standard)、公開鍵方式の RSA 暗号等がある。匿名通信の代表的な技術には、プロキシ, Tor, I2P, Freenet 等がある。3 つ目の「通信した事実の隠蔽」には、ランダムな通信を行って目的の通信を隠蔽する技術や、ステガノグラフィ技術を応用して他の通信に見せかける方法等がある。匿名通信が匿名化のため、秘匿通信の暗号化を行って通信内容・種類の隠蔽もしている場合があるように、多くの秘匿・匿名技術は上記 3 つの情報を隠蔽する技術に排他的に分類することは出来ない。また、ある 2 つの技術が同じ技術に該当したとしても、同じ機能を持っているとは限らず、その特徴を比較するのに使うことは出来ない。

本研究では、情報を隠蔽する行為が「”ある情報”が”ある相手”に対して隠蔽される」という形であることに着目し、”隠蔽する情報 (隠蔽情報)” と”隠蔽する相手 (隠蔽相手)” にあてはまる項目の検討を行った。隠蔽情報と隠蔽相手の項目を検討する上で、TCP/IP におけるアプリケーション層・トランスポート層・ネットワーク層の 3 層に分けることとし、各層において、隠蔽される可能性のある情報と相手の洗い出しを行った。その結果、隠蔽情報と隠蔽相手の 2 軸を持った表を用いて、各秘匿・匿名技術を比較する方法を提案した。秘匿・匿名技術に提案する表を適用して得られた表は、その技術によって隠蔽可能となる情報と相手を表す。この表を複数の技術間で比べることで、各秘匿・匿名技術の違いを表すことが出来る。

提案した手法の有用性を確認するため、秘匿・匿名技術として HTTP(HyperText Transport Protocol),HTTPS(HyperText Transport Protocol over Secure Socket Layer), プロキシ (Proxy), オニオンルーティング (Tor) を挙げて適用し考察を行った。その結果、各技術間の隠蔽可能とする情報と相手の違いを表すことが出来た。また、技術の組み合わせに

よって隠蔽可能となる情報を正しく表すことが出来た。しかし、技術によって組み合わせ可能な場合と不可能な場合があり、組み合わせの可否を判断する手法を別に検討する必要がある。また、隠蔽情報と隠蔽相手の洗い出した項目には、まだ考慮しなければならない要素があることが分かった。ただし、この問題に関しては、更に多くの秘匿・匿名技術に適用することで選別を進めることが可能であると考えられる。この手法を用いることで、制御・監視する者にとって脅威となる秘匿・匿名技術を提示することができる。また、新たな秘匿・匿名技術を研究開発する場合にも、既存の技術との関係を明らかにする手段として利用することができる。これらのことから、秘匿・匿名技術と制御・監視技術の対等な関係を維持するために有効な手法であると考える。

目 次

第1章　序論

本章では、本研究の背景と目的を述べ、本論文の構成を説明する。

1.1　研究背景

今日、メールやチャットといった単純なメッセージのやりとりや、情報を一方的に発信する Web ページがメインだったインターネットは、音声通話や SNS(Social Networking Service)、クレジットカードによる決済、機密情報の投稿といった様々なやりとりが行われようになっている。インターネットは、様々な人・組織が管理するネットワークとコンピュータが相互に接続され、通信はその間を転送される形で成り立っている。そのため、個々のやりとりに直接関わる人・組織以外にもそのやりとりに関わる人・組織が存在する。その上で、第三者に漏れてはいけない金銭に関わる情報のやりとりや情報の発信者を特定されてはならない内部告発を行うためには、やりとりの内容や発信者を隠蔽する必要がある。そこで、インターネット上で秘匿性や匿名性を確保する技術が数多く研究・利用されている。一方で、この技術を悪用して個人の誹謗中傷や著作権の侵害といった問題が発生しており、これを防ぐための制御や監視する技術も数多く研究・利用されている。

図 1.1 は両技術の関係を大まかに表している。

- 技術 A：制御・監視技術の研究されていない秘匿・匿名技術が存在する
- 技術 D：他の技術を応用することで秘匿・匿名性を向上させることが可能である
- 技術 T：他の技術に応用可能である

上記 3 つは例であるが、これらを含めたいくつかの事象は、両技術の関係を揺らがす可能性のある事象であり、関係は複雑である。両技術は、どちらか一方の技術が強まってはならず、常にバランスを保つように両技術の研究が行われている必要がある。

1.2　研究目的

秘匿・匿名技術と制御・監視技術が、常に対等な関係にある必要がある。本研究では、多種多様な秘匿・匿名技術が存在する中で脅威となり得る技術が存在するのか明らかにする。そのために、複数の秘匿・匿名技術を比較する手法の提案をし検討を行う。本研究の

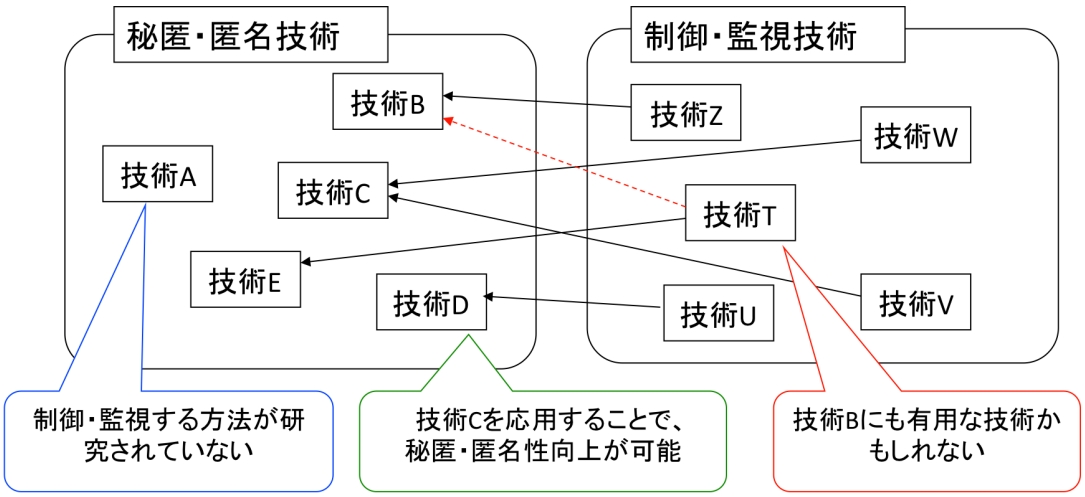

図 1.1: 秘匿・匿名技術と制御・監視技術の関係

提案手法で、新たに研究すべき制御・監視技術を提示することが出来、両技術の関係が対等である状態を保つ事が可能となる。合わせて、新たな秘匿・匿名技術を検討する上での道具としても使える手法とする。

1.3　本論文の構成

本論文の構成は、初めに 2 章で本研究で登場する用語を説明し、3 章と 4 章で主な関連技術に触れる。5 章では本研究の提案を行う。6 章では、提案した手法を実際の技術に適用して検討する。7 章では、実際の技術に適用した結果を考察する。8 章では、まとめと今後の課題について述べる。

第2章　秘匿・匿名通信とは

本研究において、“秘匿・匿名通信”とは、コンピュータネットワーク上で、なんらかの“情報”を隠蔽する技術が利用されている通信のことを指す。この秘匿・匿名通信で利用される技術のことを、秘匿・匿名技術と呼ぶ。一般的に秘匿通信や匿名通信を呼ばれる通信はもちろん含むが、それ以外にも含む可能性がある。本研究で定義する“情報”については、5章にて詳細を述べる。

2.1　秘匿・匿名通信の特徴と関係

秘匿・匿名通信が隠蔽する情報として、「通信内容・種類」、「通信経路」、「通信した事実」の3つがある。以下で、この3つの情報が隠蔽される例と関連技術に触れる。関連技術の詳細は3章で述べる。

2.1.1　通信内容・種類の隠蔽

通信内容・種類の隠蔽とは、送信者と受信者の間でやりとりされるデータの内容や種類を隠蔽することである。隠蔽する技術として、3.1節と3.4節で述べる暗号化やステガノグラフィ技術などがあげられる。

図2.1は暗号化技術を利用して通信内容を隠蔽している例である。端末Sから端末Gへテキストデータを送信する際に、テキストデータを暗号化している。これにより、第三者はデータの内容であるテキストを知ることは出来ない。ただし、端末Sから端末Gへ暗号化されたデータが送信されていることは知ることが出来る。

図2.2はステガノグラフィ技術を利用して通信の種類を隠蔽している例である。端末Sから端末Gへテキストデータ“abcdef”を送信する際に、ステガノグラフィ技術により画像データに埋め込んでいる。これにより、第三者からは画像データが送信されたと見え、データの内容だけでなくデータの種類まで知ることが出来ない。

2.1.2　通信経路の隠蔽

通信経路の隠蔽とは、あるデータがどこからどこまでどの経路を通ったのか、通信に関わった者を隠蔽することを指す。この場合、情報の送信者・受信者・転送者のそれぞれ、

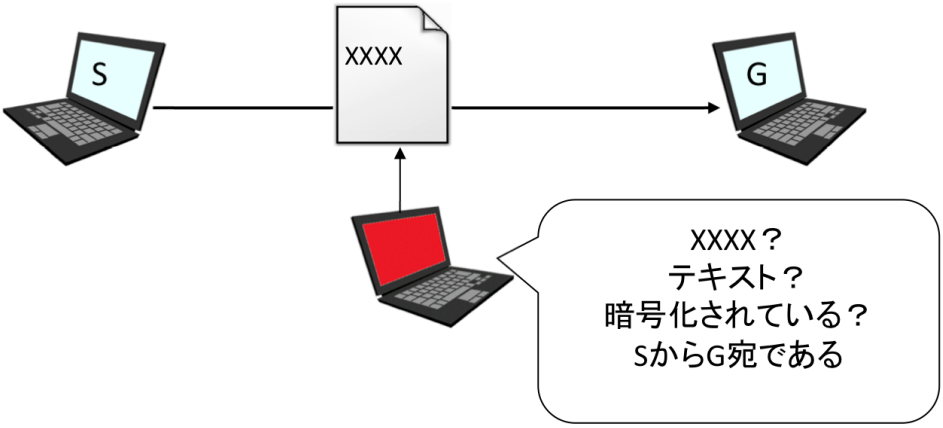

図 2.1: 通信内容・種類の隠蔽例 (暗号化)

図 2.2: 通信内容・種類の隠蔽例 (ステガノグラフィ)

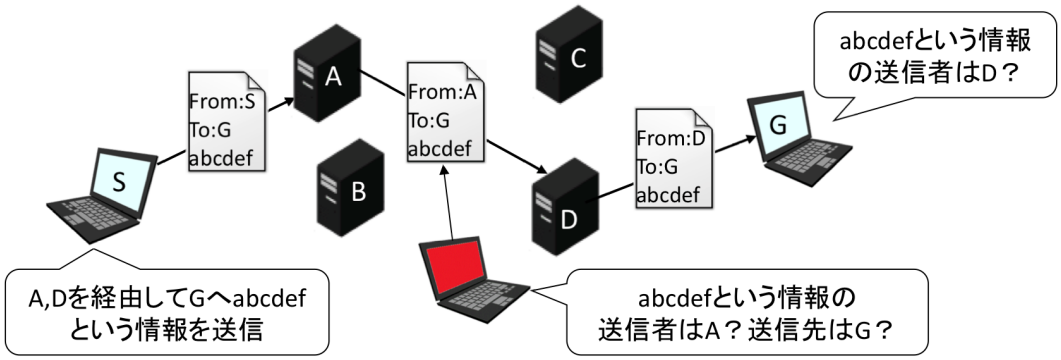

図 2.3: 通信経路の隠蔽例

またはいくつかの組合せを隠蔽する場合が考えられる。ただし、技術によってはデータやパケットの送信者を隠蔽するのみで、通信内容は隠蔽していない場合がある。代表的な技術に、Tor[10] とプロキシ、他には I2P[1]、Freenet[7]、Crowds[8] 等があげられる。

図 2.3 は、プロキシ技術を利用した例である。この図では、端末 A,D がプロキシサーバーに当たる。端末 S は端末 A,D を経由して端末 G へテキストデータ”abcdef”を送信してる。端末 A は指示に従い、端末 D を経由して端末 G へテキストデータ”abcdef”を送信する。端末 D はテキストデータ”abcdef”を端末 G へ送信する。第三者が端末 A,D の間の通信を覗いた場合、その通信は送信者が端末 A で端末 D を経由して端末へテキストデータ”abcdef”が送信されていることが分かる。送信者の端末 S について知ることは出来ない。また、端末 G には端末 D がテキストデータ”abcdef”を送信したように見え、端末 S,A について知ることは出来ない。

2.1.3 通信した事実の隠蔽

通信した事実の隠蔽とは、通信を行った事実を他者に対して隠すことである。実際の通信を見つかりにくくするため、ランダムに通信を行ったり無意味な通信を行うことで隠蔽を行う。

図 2.4 は、無意味な通信をすることで実際の通信を隠蔽している例である。隠蔽される実際の通信は、端末 S と端末 G の間でやりとりされるチャットである。端末 G は関係の無い Web サーバと通信を行う。また、端末 S は Web サーバの様に振る舞い、あたかも端末 G が端末 S という Web サーバにアクセスしているように見せる。端末 S は、端末 G へ送信するデータの中に、実際のチャットデータを含めて送信する。これによって、第三者からは、単に端末 G が Web サーバ A,B,S と通信を行っているように見える。

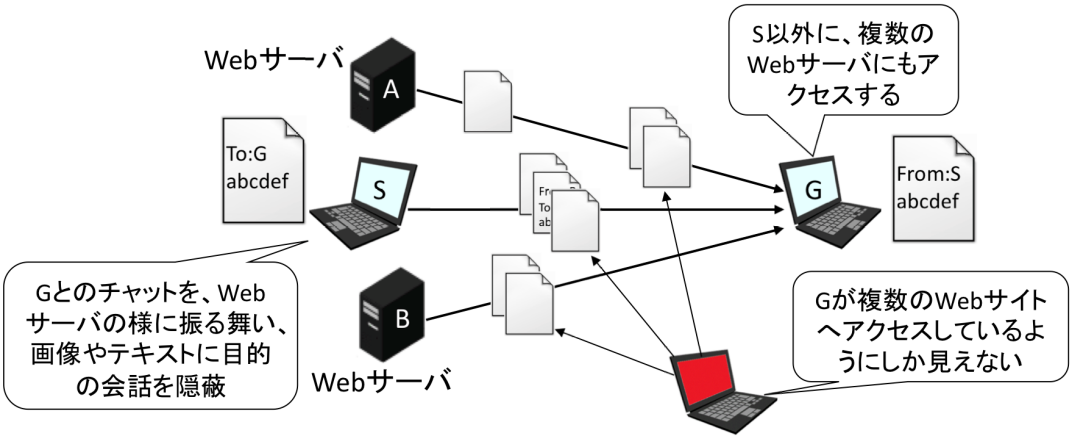

図 2.4: 通信した事実の隠蔽例

2.1.4 技術の積み重ね

前の 3 節で説明した 3 つの特徴は、それぞれ排他的な関係ではない。例えば、通信した事実の隠蔽で説明した端末 S の Web サーバの様な振る舞いはステガノグラフィの一種でもある。また、通信経路の隠蔽をする Tor は暗号化技術を利用しており、どちらも通信内容・種類の隠蔽に該当する技術を利用している。このことから、図 2.5 のように各技術は他の技術を利用して、目的とする隠蔽を行っている。図では、上位の技術は 1 つしか下位の技術を使っていないことになっているが、複数の技術を利用する場合もある。また、Tor と I2P が共通の技術 AES を利用している。これは、AES に対する制御・監視技術が存在したとき、Tor と I2P にも影響することを意味している。

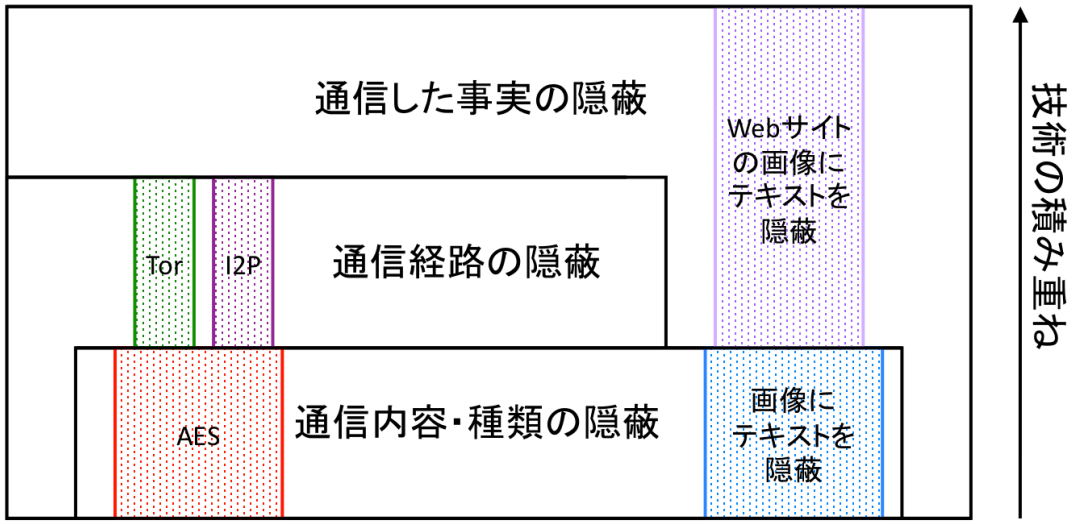

図 2.5: 技術の積み重ねの例

第3章　主な秘匿・匿名技術

本章では、秘匿・匿名通信で利用されている主な技術について述べる。

3.1　共通鍵暗号方式と公開鍵暗号方式

暗号化を行う技術として、共通鍵方式と公開鍵方式がある。

共有鍵暗号方式は、送信者と受信者の間で同じ鍵を用いて暗号化と復号化を行う。この鍵は、第三者に対して秘密にしておく必要があるため、秘密鍵暗号とも呼ばれる。送信者と受信者で共に利用される共通鍵は、事前に共有しておく必要がある。また、送信者毎に異なる共通鍵を作成する必要がある。鍵の共有方法としては、ディフィー・ヘルマン鍵交換 (Diffie-Hellman key exchange)[9] が利用される。この方法は、通信が盗聴される可能性がある上でも、事前に両者で秘密を共有をする必要無しに安全に鍵を受け渡しできる。共通鍵暗号方式の代表的な技術には、トリプル DES(Triple Data Encryption Standard) と AES(Advanced Encryption Standard) がある。

公開鍵暗号方式は、暗号化に用いる鍵と復号化に用いる鍵が異なる方式である。受信者は、事前に公開鍵と秘密鍵を用意し、送信者へ公開鍵のみを伝える。送信者は、受け取った公開鍵を用いて暗号化を行い、受信者へ暗号化したデータを送る。受信者は、受け取った暗号化されたデータを秘密鍵を用いて復号化を行う。暗号化されたデータは秘密鍵を知らないと復号化できないため、受信者は 1 組の公開鍵と秘密鍵を用意すれば複数の相手と暗号化した通信を行うことが出来る。公開鍵暗号方式の代表的な技術には、RSA 暗号 [13] や ElGamal 暗号 [11]、共通鍵を共有する方法でも利用されるディフィー・ヘルマン鍵交換がある。

3.2　プロキシ

プロキシ (Proxy) とは、送信者と受信者の間に入り通信の中継を行う技術である。プロキシには様々な種類がある。ここでは、代表的なプロキシについて触れる。プロキシサーバーの代表的なソフトウェアには Squid[4] がある。通信が検閲されている国で監視網をすり抜ける技術として Telex[15] が提案されている。この技術もプロキシの一種であり、暗号化した通信路を利用している。

3.2.1 Web プロキシ

Web プロキシとは、Web サービスを中継する技術である。このプロキシは、Web ブラウザと Web サーバの間に入り、Web ブラウザに対しては Web サーバのように機能し、Web サーバに対しては Web ブラウザのように機能する。Web ブラウザは Web サーバーへリクエストを送信するのと同じようにプロキシへリクエストを送信する。プロキシは、受け取ったリクエストを Web ブラウザの代理として Web サーバへ送信する。Web ブラウザからのレスポンスを受け取ったプロキシは、そのレスポンスを Web ブラウザへと転送する。

3.2.2 多段プロキシ

多段プロキシとは、複数のプロキシが送信者と受信者の間に入り中継する技術である。プロキシサーバーを 1 つだけ利用した場合には、送信者と受信者についてプロキシサーバに記録が残すことが可能である。しかし、多段プロキシを利用した送信者について受信者が知るためには、中継をしたプロキシサーバのすべてから記録を辿らなければならない。2.1.2 節で説明した例は、プロキシサーバを 2 つ利用した場合となっている。

3.3 オニオンルーティング

オニオンルーティングとは、多段プロキシと暗号化を組み合わせた技術である。

多段プロキシでは、一切暗号化を行っていない場合、中継を行ったプロキシサーバの記録が辿られれば Web サーバからでも初めにリクエストを送信した Web ブラウザの端末を特定することが可能である。また、Web ブラウザが初めに送信したリクエストの内容を見ることが出来れば、転送を行った複数のプロキシサーバを特定することが出来る。

オニオンルーティングでは、これらの問題を解決するため、中継を行う端末間で次々と暗号化した通信経路 (暗号通信路) を作成し、暗号通信路の多重化を行う。これにより、中継を行う端末は自身の前後に位置する端末以外を知ることが出来ない。

Tor は、オニオンルーティングの仕組みを実装したアプリケーションであり、ディフィー・ヘルマン鍵共有と AES が利用されている。Mixmaster[3] も同様にオニオンルーティングの仕組みを利用している。

3.4 ステガノグラフィ

ステガノグラフィとは、データを他のデータに埋め込む技術である。暗号化がデータの内容を読めないようにする技術であるのに対して、元のデータの存在を隠す技術である。存在を隠すためのデータをカバーデータと呼び、多くの技術は画像データや音声データが用いられ、著作権保護のための電子透かし等に利用されている。通信技術では、ICMP(Internet Control Message Protocol)[16]、HTTP Cookie を用いた例がある。

第4章　主な制御・監視技術

本章では、通信を制御・監視する主な技術について述べる。

4.1　IP アドレス・ポート

IP アドレスはインターネット上の住所であり、ポート番号はその住所に住む人を現すようなものである。通信を制御・監視する方法として、この IP アドレスとポート番号を利用することは常套手段となっている。

ポート番号にはウェルノウンポートがあり、容易に通信の種類を特定することが可能である。ポート番号を利用した制御の例として、OP25B(Outbound Port 25 Blocking) がある。これは、メール転送プロトコルの SMTP(Simple Mail Transfer Protocol) を意味する TCP ポート 25 番を利用する通信を規制する。

IP アドレスを利用した制御の例として、uRPF(unicast Reverse Path Forwarding)[5] がある。これは、ルータがパケットを転送する際に、受け取ったパケットの送信元 IP アドレスが経路表に存在するのか確認を行う。そして、経路表に存在しない場合にはパケットを破棄する。更に単純な例として、IP アドレスのブラックリストを作成し、パケットの送信元 IP アドレスまたは宛先 IP アドレスと一致すればパケットを破棄する方法がある。

4.2　パターンマッチ

パターンマッチは、特定の文字列や正規表現を使い、通信内容に一致する箇所を検出し制御する方法である。暗号化された通信に適用しても意味が無いが、平文の通信であれば誹謗中傷などの特定のキーワードを用いることで検出することができる。また、特定のプロトコルやアプリケーションに限ると、通信の開始時などに決まったパターンの送受信を行うことに注目して検出を行う方法がある。例として、ネットワーク上でモニタリングして Winny の実行されている端末を特定する技術がある。

4.3　トレースバック

トレースバックとは、パケットの送信元を特定する技術である。手法は、SNMP(Simple Network Management Protocol) を使ったシンプルなものから、複数の ISP が連携して構

築されたシステム [6] まである。複数のネットワークを横断してトレースバック網を構築する InterTrack がある。[2]

第5章　本研究の提案

本章では、本研究で提案する手法について述べる。

5.1　本研究の着目点

2.1 節で述べたように、秘匿・匿名通信の特徴は大きく分けて 3 種類ある。しかし、技術によっては複数にまたがることが多々あり、分類手法としては十分とは言えない。そこで、「通信内容を隠蔽する」、「発信者を隠蔽する」、「第三者から隠蔽する」といった大まかな粒度ではなく、細かな粒度で分類を行う。情報を隠蔽することは、「”ある情報”が”ある相手”に対して隠蔽される」という形をしている。そこで、「隠蔽する情報 (隠蔽情報)」と「隠蔽する相手 (隠蔽相手)」について、それぞれを細かく項目を挙げていくこととした。

5.2　隠蔽情報と隠蔽相手による分類

本節では、「隠蔽情報」と「隠蔽相手」に着目した分類手法について述べる。

5.2.1　階層を分ける

コンピュータネットワークは、プロトコルスタックになっている。現在主流となっている TCP/IP は、リンク層・ネットワーク層・トランスポート層・アプリケーション層に分けられる。リンク層では L2 スイッチ、ネットワーク層ではルータというように、ネットワークを情報が伝わるときに経由する端末は、各層毎に異なる。また、TLS(Transport Layer Security) はアプリケーション層で暗号化を行っているが、IPSec(Security Architecture for Internet Protocol) はネットワーク層で暗号化を行っている。このことから、階層が変わると隠蔽する情報や通信に関わる端末が変わることから、階層を分けて隠蔽情報と隠蔽相手を考えることとした。ただし、リンク層に関しては、無線ネットワークの電波漏洩といった物理的な要素まで含み、関連する技術が広範になりすぎるため、ネットワーク層・トランスポート層・アプリケーション層の 3 層を対象とした。

5.2.2 隠蔽情報

本節では、ネットワーク層・トランスポート層・アプリケーション層、それぞれの層における隠蔽される可能性のある情報について検討し選び出した。以下では、各項目について説明をする。

- アプリケーション層
  - 送信者、受信者、転送者
  - 送信者・転送者・受信者の 2 者または 3 者以上の組み合わせ
  - データ：内容、種類、送信量、受信量、パターン
- トランスポート層
  - 送信者、受信者、転送者
  - 送信者側の NAPT・ゲートウェイ、受信者側の NAPT・ゲートウェイ
  - 送信者・転送者・受信者の 2 者または 3 者以上の組み合わせ
  - データ：内容、種類、送信量、受信量、パターン
- ネットワーク層
  - 送信者、受信者、転送者
  - 送信者側の NAT・ゲートウェイ、受信者側の NAT・ゲートウェイ
  - 送信者・転送者・受信者の所属ネットワーク、所属国
  - 送信者・転送者・受信者の 2 者または 3 者以上の組み合わせ
  - データ：内容、種類、送信量、受信量、パターン

すべての層において、送信者・受信者・転送者がある。これは、ある通信が行われた際に、その通信に関わった者を指す。メールサービスであれば、アプリケーション層ではメーラが送受信者、SMTP サーバや POP サーバが転送者に当てはまる。トランスポート層では各アプリケーションが利用するポート番号、ネットワーク層では IP アドレスが当てはまる。転送者に関しては、複数存在する場合がある。アプリケーション層では HTTP プロキシが当てはまり、ネットワーク層においてはパケットを転送したルータすべてが当てはまる。また、送信者・受信者・転送者のどれか 2 つもしくはすべてを組み合わせたものも隠蔽されうる情報となる。送信者と受信者の組み合わせはその 2 者間で通信が行われたことを意味し、送信者と転送者の組み合わせは送信者が発した情報を転送者が中継したことを意味する。トランスポート層では NAPT(Network Address Port Translation)、ネットワーク層では NAT(Network Address Translation) によって送受信者のポート番号と IP アドレスが変換されることがあるため、それぞれを追加した。そして、NAT/NAPT

を介して送受信者が通信を行う際には、多くの場合 1 つのゲートウェイが存在することから、送受信者にそれぞれゲートウェイを追加した。ネットワーク層では、GeoIP 等によって IP アドレスから所属ネットワーク (企業、ISP) や所属国を特定することが可能であることから、これらを追加した。純粋な HTTP 通信であればアプリケーション層とトランスポート層の転送者は存在しないように、ここで提示した項目は、すべての通信に存在するわけではない。

データとは、通信でやりとりされた情報であり、各層のペイロードに含まれるデジタルデータを指す。内容は、テキストデータであれば一字一句、画像データであればピクセル単位までを意味する。種類は、”テキストデータである”、”画像データである”、”暗号化されたデータである”ことまでを意味する。送信量と受信量は、送信者が送出したデータの量と、受信者が受信したデータの量を意味する。パターンは、時間軸の変化によるデータ受け渡しの変化を意味する。

5.2.3 隠蔽相手

本節では、ネットワーク層・トランスポート層・アプリケーション層、それぞれの層における隠蔽する相手を検討し選び出した。以下では、各項目について説明をする。

- アプリケーション層
  - 送信者、受信者、転送者
- トランスポート層
  - 送信者、受信者、転送者
  - 送信者側のゲートウェイ、受信者側のゲートウェイ
- ネットワーク層
  - 送信者、受信者、転送者
  - 送信者側のゲートウェイ、受信者側のゲートウェイ
  - ISP,IX

隠蔽情報と同様に、すべての層において送信者・受信者・転送者が存在する。トランスポート層とネットワーク層におけるゲートウェイは、送受信者が送受するパケットが必ず通過する端末となることから追加した。ネットワーク層の ISP と IX は、転送者にも当てはまるが、隠蔽情報で挙げた所属ネットワークと所属国に関わることから追加した。

ここで挙げた候補は、制御・監視技術を利用する者に該当する可能性がある。直接的には、アプリケーション層の送受信者や転送者はソフトウェアであり、ネットワーク層の転送者はルータやコンピュータである。しかし、情報を隠蔽することはその端末やソフト

を管理する人に対して隠蔽する意味合いが強い。特に、ISP や IX は送受信者の一方または両者のゲートウェイとなる可能性が高く、制御・監視技術を利用する重要なポイントとなっている。

5.2.4 送信者と受信者

通信には、必ず情報の送信者と受信者が存在する。しかし、多くの通信では双方向に通信を行っていることから、送信者と受信者が逆の立場になる場合がある。本研究では、双方向にデータのやりとりが行われる通信の場合、通信を最初に始めた端末を送信者として扱う。

5.2.5 隠蔽情報と隠蔽相手の関係

5.2.2 節と 5.2.3 節で選び出した隠蔽情報と隠蔽相手の関係について説明する。

本章の始めに述べた「”ある情報”が”ある相手”に対して隠蔽される」ことから、隠蔽情報と隠蔽相手はすべての項目において関係する可能性がある。そこで、隠蔽情報と隠蔽相手の 2 軸をもった表を作成することができる。同じ階層では、送信者に関わる情報が送信者に隠蔽されるという、現在のシステムでは不可能な関係も含まれてしまうことになる。表 5.1 は、こういった箇所に斜線を入れた表である。ただし、以降の表では便宜上斜線とせず、×としている。

表 5.2 は、ここまで検討した隠蔽情報と隠蔽相手を行と列に設定し作成した表である。セルには○, ×, △が入力されている。この入力は適用する秘匿・匿名技術によって変化する。○は、そのセルの行に該当する情報が、列に該当する相手に対して隠蔽可能であることを意味する。×は、隠蔽不可能であることを意味する。△は、隠蔽可能か不可能か判断できない、または、一部で隠蔽不可能であることを意味する。表 5.2 の○, ×, △は、説明のために適当に設定したもので、特に意味を持っていない。

表の見方を、表中太枠で囲んだ行と列を使って説明する。

- 隠蔽情報：アプリケーション層転送者 (表中、上から 5 行目)
  - アプリケーション層の転送者に該当する隠蔽情報は、プロキシサーバや、メールサービスの SMTP サーバ、POP サーバのソフトウェアである。多段プロキシを利用した通信であった場合には、転送者 (ソフトウェア) は複数存在することになる。ここでは、多段プロキシの場合を説明をする。
  - アプリケーション層の隠蔽相手：送信者は自身のプロキシサービスを利用する Web ブラウザである。受信者はその Web ブラウザがアクセスしている Web サーバである。転送者は自分自身と、送信者が選んだ複数のプロキシサーバである。

表 5.1: 表中で考慮する必要の無い項

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
アプリケーション	送信者														
	受信者														
	転送者														
	複数の転送者														
	送信者・受信者														
	送信者・転送者														
	受信者・転送者														
	送信者・転送者・受信者														
	データの内容														
	データの種類														
	データの送信量														
	データの受信量														
	データのパターン														
トランスポート	送信者														
	送信者(NAPT)														
	送信者GW(NAPT)														
	受信者														
	受信者(NAPT)														
	受信者GW(NAPT)														
	転送者														
	複数の転送者														
	送信者・受信者														
	送信者・転送者														
	受信者・転送者														
	送信者・転送者・受信者														
	データの内容														
	データの種類														
	データの送信量														
	データの受信量														
	データのパターン														
ネットワーク	送信者														
	送信者(NAT)														
	送信者GW(NAT)														
	送信者の所属ネットワーク														
	送信者の所属国														
	受信者														
	受信者(NAT)														
	受信者GW(NAT)														
	受信者の所属ネットワーク														
	受信者の所属国														
	転送者														
	転送者の所属ネットワーク														
	転送者の所属国														
	複数の転送者														
	送信者・受信者														
	送信者・転送者														
	受信者・転送者														
	送信者・転送者・受信者														
	データの内容														
	データの種類														
	データの送信量														
	データの受信量														
	データのパターン														
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
		アプリケーション			トランスポート					ネットワーク					

- トランスポート層の隠蔽相手：送受信者は上記の Web ブラウザと Web サーバの TCP ポートを担当するソフトウェアである。転送者は自身自身が利用する TCP のサービスと他のプロキシサーバの利用する TCP サービスである。送受信者 GW はそれぞれが利用する NAPT の動作する GW である。
- ネットワーク層の隠蔽相手：送受信者は、Web ブラウザと Web サーバーが動作する端末の IP のサービスである。GW はネットワーク層のゲートウェイと同じであり、NAT の可能性がある。転送者は、送信者が選んだプロキシサーバーの端末と、送信者とプロキシ、プロキシ同士、プロキシと受信者の間で IP パケットを転送するすべての端末である。ISP と IX はこのすべての端末の一部となる。

- 隠蔽情報：ネットワーク層データの内容 (表中、下から 7 行目)
  - ネットワーク層におけるデータの内容とは、送信者の端末から送出された IP パケットのペイロード部のことである。この項目が×であることは、上位の層で暗号化といったことがされていないことを意味する。○となっている場合は、その相手を IP パケットが通過する際に必ずデータ内容の隠蔽がされていることを意味する。△の場合は、送信者が受信者へ向けたデータが途中で暗号化または復号化されていることを意味する。

- 隠蔽相手：ネットワーク層送信者 (表中、右から 6 列目)
  - ネットワーク層における送信者は、送信者の端末で動作する IP サービスのことである。直接関係を持つのは自身 (送信者) の端末で上位に位置する TCP サービスやアプリケーションである。初めに情報を送信しようとしている端末である。

表 5.2: 隠蔽情報と隠蔽相手の関係

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
アプリケーション	送信者	×	○	△	×	×	○	○	△	×	×	○	○	△	△
	受信者	×	×	△	×	○	×	×	△	×	○	×	×	△	△
	転送者	△	○	×	△	△	○	○	×	△	△	○	○	△	△
	複数の転送者	△	○	△	△	○	○	○	△	△	○	○	○	△	○
	送信者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	送信者・転送者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	受信者・転送者	×	△	△	×	○	△	△	△	×	○	△	△	△	△
	送信者・転送者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	データの内容	×	×	△	○	○	×	×	△	○	○	×	×	△	△
	データの種類	×	×	○	○	○	×	×	△	○	○	×	×	△	△
	データの送信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データの受信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データのパターン	×	×	△	×	△	×	×	△	×	△	×	×	△	△
トランスポート	送信者	×	○	△	×	×	○	○	△	×	×	○	○	△	△
	送信者(NAPT)	×	○	○	×	×	○	○	○	×	×	○	○	○	○
	送信者GW(NAPT)	×	○	△	×	×	○	○	△	×	×	○	○	△	△
	受信者	×	×	△	×	○	×	×	△	×	○	×	×	△	△
	受信者(NAPT)	○	×	○	○	○	×	×	○	○	○	×	×	○	○
	受信者GW(NAPT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	△	△	×	△	△	△	△	×	△	△	△	△	×	△
	複数の転送者	△	○	△	△	○	○	○	△	△	○	○	○	△	△
	送信者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	送信者・転送者	×	○	△	×	△	○	○	△	×	△	○	○	△	△
	受信者・転送者	×	△	△	×	○	△	△	△	×	○	△	△	△	△
	送信者・転送者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	データの内容	×	×	△	○	○	×	×	△	○	○	×	×	△	△
	データの種類	×	×	△	○	○	×	×	△	○	○	×	×	△	△
	データの送信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データの受信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データのパターン	×	×	△	×	×	×	×	△	×	×	×	×	△	△
ネットワーク	送信者	×	○	△	×	×	○	○	△	×	○	○	○	△	△
	送信者(NAT)	×	○	○	×	×	○	○	○	×	○	○	○	○	○
	送信者GW(NAT)	×	○	△	×	×	○	○	△	×	○	○	○	△	△
	送信者の所属ネットワーク	×	○	△	×	×	○	○	△	×	○	○	○	△	△
	送信者の所属国	×	○	△	×	×	○	○	△	×	○	○	○	△	△
	受信者	×	×	△	×	×	×	×	△	×	○	×	×	△	△
	受信者(NAT)	○	×	○	○	○	×	×	○	○	○	×	×	○	○
	受信者GW(NAT)	×	×	×	×	×	×	×	×	×	○	×	×	×	×
	受信者の所属ネットワーク	×	×	△	×	×	×	×	△	×	○	×	×	△	△
	受信者の所属国	×	×	△	×	×	×	×	△	×	○	×	×	△	△
	転送者	△	△	×	△	△	△	△	×	△	△	△	△	×	△
	転送者の所属ネットワーク	△	△	×	△	△	△	△	×	△	△	△	△	×	△
	転送者の所属国	△	△	×	△	△	△	△	×	△	△	△	△	×	△
	複数の転送者	△	○	△	×	○	○	○	△	△	○	○	○	△	△
	送信者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	送信者・転送者	×	○	△	×	△	○	○	△	×	△	○	○	△	△
	受信者・転送者	×	△	△	×	○	△	△	△	×	○	△	△	△	△
	送信者・転送者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	データの内容	×	×	△	○	○	×	×	△	○	○	×	×	△	△
	データの種類	×	×	△	○	○	×	×	△	○	○	×	×	△	△
	データの送信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データの受信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データのパターン	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
		アプリケーション			トランスポート					ネットワーク					

第6章　提案手法の検討

本章では、5章で提案した提案手法を実際の技術に適用した場合の例を挙げる。そして、それぞれの結果を比較や結合することによって、技術毎の差異や技術の組み合わせによる隠蔽情報の変化を検証する。

6.1　実際の技術に適用

技術の例としてHTTP(HyperText Transfer Protocol)[12] とHTTPS(HyperText Transfer Protocol over Secure Socket Layer)[14]、プロキシ(Proxy)、オニオンルーティング(Tor)を扱う。これらの技術は相互に共通する部分が多く、比較をすることで明らかになった結果を検討しやすいことから選択した。各技術毎に情報の隠蔽の可否を考察し、表を作成した。

6.1.1　HyperText Transfer Protocol(HTTP)

表6.1は、HTTPを利用した際の隠蔽情報と隠蔽相手の関係を表したものである。

HTTP通信利用時のアプリケーション層の送信者と受信者は、Internet ExplorerやOperaといったWebブラウザと、Apacheやnginxといったウェブサーバが当てはまる。これらのアプリケーションが利用するポート番号がトランスポート層の送受信者、IPアドレスがネットワーク層の送受信者を指す。図6.1は、各層と送信者・受信者・転送者の関係を表した図である。転送者は、アプリケーション層とトランスポート層では存在しないため、すべて×とした。ネットワーク層における転送者は、IPパケットの送信先IPアドレスによってルーティングを行っている端末すべてが当てはまる。図中では、例として2つの転送者が書いてある。実際には、透過プロキシといったアプリケーション層まで関係する転送者が存在する可能性があるが、単純なHTTP通信を行った場合を考えるため対象としていない。透過プロキシが利用されている場合を考えるには、別途表を作成する必要がある。HTTPは、通信内容を一切暗号化しないため、当然のことながら通信はすべて平文で行われる。そのため、情報の伝わる経路上のすべての箇所において、データの内容、送受信者のIPアドレスとポート番号を覗くことが可能である。このため、アプリケーション層・トランスポート層・ネットワーク層のどの層においても、送信者と受信者に関わる情報が隠蔽されない。ネットワーク層における転送者の情報は、送信者と受信者のIPア

ドレスが分かれば容易に調べることが可能である。ただし、実際はISP内のネットワークは透過的であったりするため、すべての転送者 (情報の転送に関わった端末) を特定することは困難である。以上のことより、隠蔽される情報はNAT/NAPTを利用している場合の、送信者のアプリケーションが持つポート番号とIPアドレス、受信者のポート番号とIPアドレスだけである。

6.1.2 HyperText Transfer Protocl over Secure Socket Layer(HTTPS)

表6.2は、HTTPSを利用した際の隠蔽情報と隠蔽相手の関係を表したものである。HTTPSとは、エンドツーエンドで暗号・復号を行うTLS(Transport Layer Security)を利用してHTTP通信を行う。TLSはトランスポート層の上位に位置するため、ネットワーク層やトランスポート層では通信の内容が隠蔽されている。HTTPSはHTTPの時と同様に、アプリケーションはWebブラウザとWebサーバが当てはまり、それぞれの利用するIPアドレスとポート番号がネットワーク層とトランスポート層の送受信者に当てはまる。アプリケーション層とトランスポート層では転送者に当てはまるものは無く、ネットワーク層にのみ転送者が存在する。TLSは、エンドツーエンドでやりとりされるTCPパケットのペイロード部を隠蔽するだけであり、送受信者のIPアドレスとポート番号を隠蔽することは無い。このことから、アプリケーション層・トランスポート層・ネットワーク層のどの層においても送受信者を隠蔽することは無い。よって、ネットワーク層の転送者に関する情報も隠蔽不可能であり、送受信者と転送者に関わる情報はすべて隠蔽不可能である。データの内容や種類に関する情報については、TLSの通信を行っていることは送受信するアプリケーション以外にも判別することができるため、パケットサイズややりとりされたパケットの履歴から送受信量・通信のパターンが分かる。

6.1.3 プロキシ

表6.3は、プロキシを利用した際の隠蔽情報と隠蔽相手の関係を表したものである。プロキシの概要は、3.2節で説明したとおりだが、ここで扱うプロキシは、ユーザと離れたネットワーク上に公開されたHTTPプロキシであり、ユーザの環境変数などを一切通知しないものとする。HTTPプロキシは、アプリケーション層において転送を行う。送受信者は、HTTPやHTTPSと同様にWebブラウザとWebサーバである。図6.2は、各層と送信者・受信者・転送者の関係を表した図である。送信者と転送者 (プロキシ)、転送者 (プロキシ) と受信者との間にはネットワーク層に転送者が1つずつ書いてあるが、実際には、複数存在する

Webブラウザはプロキシサーバに HTTP リクエストを送り、プロキシサーバがWebサーバへ、そのリクエストを送信する。WebサーバからHTTPレスポンスを受け取ったプロキシサーバは、そのレスポンスをWebブラウザへ送信する。なお、プロキシは暗号

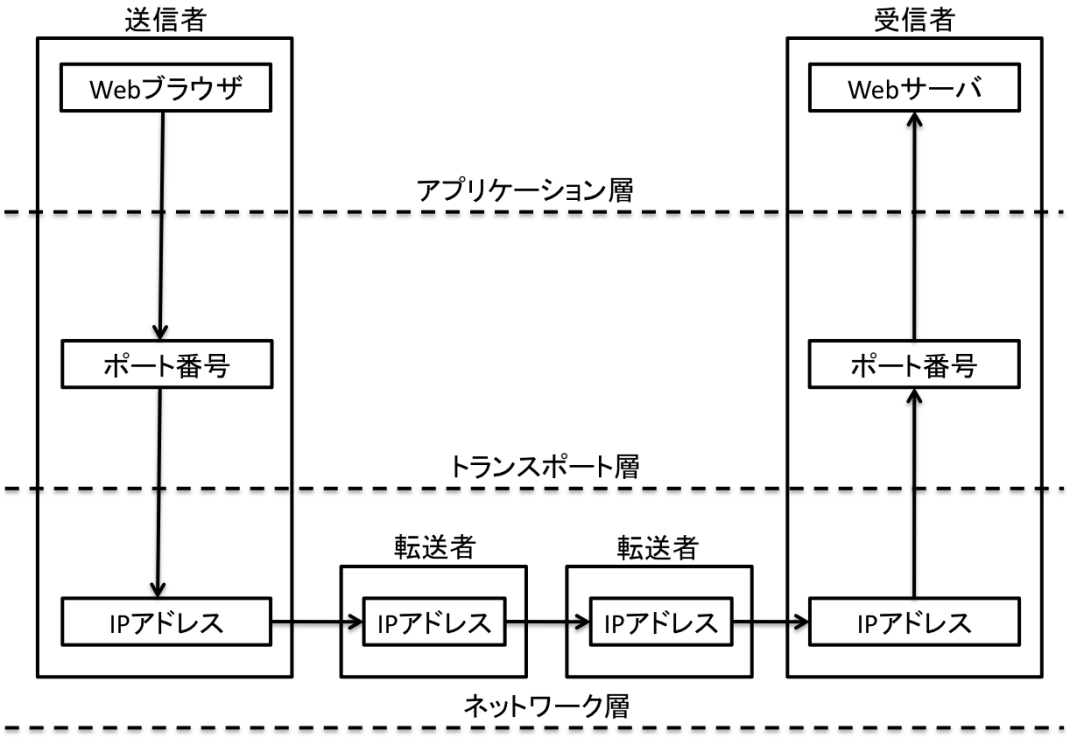

図 6.1: HTTP 通信の送信者と受信者

表 6.1: HTTP への適用

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
アプリケーション	送信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	複数の転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの内容	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの種類	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
トランスポート	送信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者(NAPT)	×	○	×	×	×	○	○	×	×	×	○	○	○	○
	送信者GW(NAPT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者(NAPT)	○	×	×	○	○	×	×	×	○	○	×	×	○	○
	受信者GW(NAPT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	複数の転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの内容	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの種類	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
ネットワーク	送信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者(NAT)	×	○	×	×	×	○	○	×	×	×	○	○	○	○
	送信者GW(NAT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者の所属ネットワーク	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者の所属国	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者(NAT)	○	×	×	○	○	×	×	×	○	○	×	×	○	○
	受信者GW(NAT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者の所属ネットワーク	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者の所属国	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者の所属ネットワーク	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者の所属国	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	複数の転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの内容	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの種類	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
		アプリケーション			トランスポート					ネットワーク					

表 6.2: HTTPS への適用

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
アプリケーション	送信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	複数の転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの内容	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの種類	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
トランスポート	送信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者(NAPT)	×	○	×	×	×	○	○	×	×	×	○	○	○	○
	送信者GW(NAPT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者(NAPT)	○	×	×	○	○	×	×	×	○	○	×	×	○	○
	受信者GW(NAPT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	複数の転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの内容	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの種類	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
ネットワーク	送信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者(NAT)	×	○	×	×	×	○	○	×	×	×	○	○	○	○
	送信者GW(NAT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者の所属ネットワーク	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者の所属国	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者(NAT)	○	×	×	○	○	×	×	×	○	○	×	×	○	○
	受信者GW(NAT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者の所属ネットワーク	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者の所属国	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者の所属ネットワーク	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者の所属国	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	複数の転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの内容	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの種類	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
		アプリケーション			トランスポート					ネットワーク					

化を行わず平文でやりとりするため、Web ブラウザと Web サーバ間で暗号化をしない限り、データの内容やサイズ・種類は通信に関わるすべての端末に隠蔽されない。

ここまで空となっていたアプリケーション層とトランスポート層の転送者にプロキシサーバが当てはまり、ネットワーク層の転送者にも含まれる。また、Web ブラウザとプロキシサーバ、Web サーバとプロキシサーバ、それぞれが送信者・転送者、受信者・転送者に該当し、Web ブラウザ・プロキシサーバ・Web サーバを組み合わせたものが送信者・転送者・受信者に該当する。Web サーバは Web ブラウザの利用するポート番号や IP アドレスを知ることは出来ないため、送信者に関わる情報は受信者へ隠蔽される。

ISP,IX は、プロキシサーバと Web サーバのやりとりを中継する場合もあれば、Web ブラウザとプロキシサーバのやりとりも中継する場合がある。Web サーバ側のやりとりだけ中継していた場合は、Web サーバと同様に送信者に関わる情報は得ることが出来ない。一方で、Web ブラウザ側のやりとりを中継していた場合は、送信者・転送者・受信者に関わる情報はすべて把握でき、プロキシサーバを利用してどんな Web サーバと通信しているのかまで特定できる。

Web サーバは、プロキシサーバと通信する部分においては、HTTP の時と同様に転送者の情報等が把握できる。しかし、Web サーバは送信者が Web ブラウザなのかプロキシサーバなのかを特定は出来ない。

6.1.4 オニオンルーティング (Tor)

表 6.4 は、Tor を利用した際の隠蔽情報と隠蔽相手の関係を表したものである。Tor は、3.3 節で説明したとおり、複数のプロキシを多段利用し、送信者が各プロキシと暗号化した通信を行うものである。以下では、断りが無い限りオニオンルーティングの仕組みを実装したソフトの総称として”Tor”を使う。Tor は HTTP に限らず様々なプロトコルに対応する (現在の実装では TCP のみで、UDP 等のプロトコルには対応できていない)。ここでは、後で HTTP やプロキシの例と比較するため、Tor を利用して Web ブラウザと Web サーバが HTTP 通信を行う場合を扱う。

図 6.3 は、Tor 利用時の各層の送受信者と転送者を表したものである。アプリケーション層の転送者が Tor に当たり、送信者が Web ブラウザ、受信者が Web サーバに当たる。Web ブラウザの利用するポート番号と IP アドレスがトランスポート層・ネットワーク層の送信者になり、Web サーバの利用するポート番号と IP アドレスがトランスポート層・ネットワーク層の受信者となる。送信者は複数の Tor 端末を利用する。これは、アプリケーション層の転送者が複数存在することを意味する。この転送者が利用しているポート番号と IP アドレスは、トランスポート層・ネットワーク層の転送者にも属する。図中には書かれていないが、ネットワーク層には送信者・Tor の転送者・受信者の間に複数の転送者が存在する。

送信者が要求する接続先 (受信者を指す) へは、多段プロキシの最後の端末が接続を行う。受信者は、あたかもこの端末が通常の Web ブラウザがアクセスしているかのように

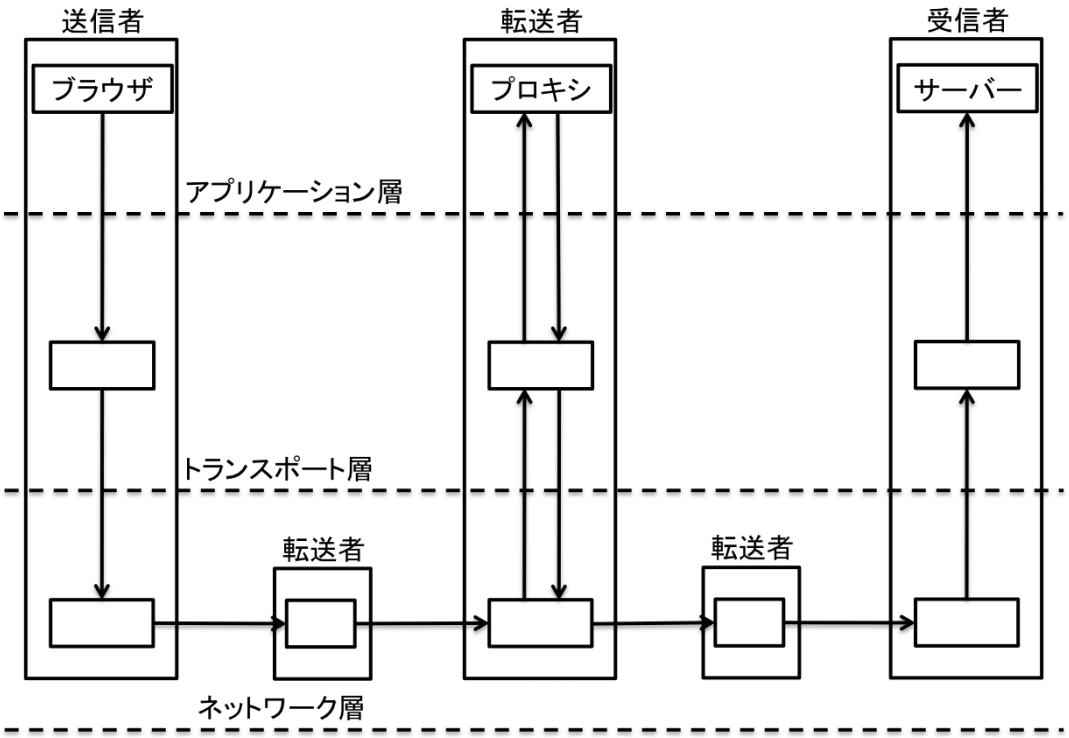

図 6.2: プロキシ利用時の送受信者と転送者

表 6.3: プロキシへの適用

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
アプリケーション	送信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	○	×	×	×	○	○	×	×	×	○	○	△	×
	複数の転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・受信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者・転送者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	データの内容	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの種類	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
トランスポート	送信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者(NAPT)	×	○	○	×	×	○	○	○	×	×	○	○	○	○
	送信者GW(NAPT)	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者(NAPT)	○	×	○	○	○	×	×	○	○	○	×	×	○	○
	受信者GW(NAPT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	複数の転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの内容	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの種類	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
ネットワーク	送信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者(NAT)	×	○	○	×	×	○	○	○	×	×	○	○	○	○
	送信者GW(NAT)	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者の所属ネットワーク	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者の所属国	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者(NAT)	○	×	○	○	○	×	×	○	○	○	×	×	○	○
	受信者GW(NAT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者の所属ネットワーク	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者の所属国	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	△	×	×	×	△	△	×	×	×	△	△	×	△
	転送者の所属ネットワーク	×	△	×	×	×	△	△	×	×	×	△	△	×	△
	転送者の所属国	×	△	×	×	×	△	△	×	×	×	△	△	×	△
	複数の転送者	×	△	×	×	×	△	△	×	×	×	△	△	×	△
	送信者・受信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者・転送者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	データの内容	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの種類	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
		アプリケーション			トランスポート					ネットワーク					

見え、複数経由しているTor端末や送信者の情報は一切把握できない。そのため、受信者はアプリケーション層では1つの転送者しか把握できず、送信者と複数の転送者には関知しない。トランスポート層においても同様である。ネットワーク層では、多段プロキシの最後の端末となった転送者と自身の間を中継した転送者 (Tor端末では無い) の情報のみ得ることが可能である。

Webブラウザと Webサーバでやりとりされる情報は、オニオンルーティングによって暗号化されることはない。しかし、Webブラウザが初めに利用するTor端末が、次のTor端末を1つ経由する毎に暗号化が行われる。経由されたTor端末はWebブラウザの情報を得ることは出来ず、多段プロキシの自身の前後に位置するTor端末についてのみ把握している。Webブラウザと Webサーバでやりとりされるデータは、Webブラウザが初めに利用するTor端末から最後のTor端末までの間でのみ暗号化されている。つまり、Webブラウザと最初のTor端末の間、最後のTor端末と Webサーバの間では平文のままやりとりされている。このやりとりを中継するネットワーク層の転送者は、容易にデータの内容や種類・サイズ・パターンを把握できる。アプリケーション層における転送者 (Tor端末) では、多段プロキシの最初と最後になった端末でのみデータの内容に関知できる。

6.1.5 各技術の比較

技術の隠蔽度合いを比較する時、隠蔽不可の×が○や△になった場合、これは隠蔽できる情報が増え隠蔽度合いが強化されたと言える。逆に、○や△が×になった場合、これは隠蔽できる情報が減り隠蔽度合いが悪化したと言える。

表6.5はHTTPとHTTPSの比較をしたものである。前節で作成を行った隠蔽情報と隠蔽相手の関係の表を比較しているためとても大きな表となっているが、そもそも隠蔽される情報が少ないため差分は少ない。HTTPS通信はTLSを利用したHTTP通信であるため、差分として得られる結果はTLS技術によって隠蔽される情報のはずである。TLSはトランスポート層以下の送受信・転送者に対してデータの内容を隠蔽する技術であり、その項目の隠蔽度合いを強化していることを表が現していることが分かる。

表6.6はHTTPとプロキシの比較をしたものである。6.1.3節で扱ったプロキシはHTTPプロキシであるため、差分として得られる結果はプロキシ技術によって隠蔽される情報のはずである。プロキシは送信者の代理をすることで受信者へ送信者の情報を隠蔽する技術である。表では、NAT/NAPTの場合が含まれ、送信者の利用するGWも隠蔽度合いを強化していることになった。また、HTTPでは存在しなかったアプリケーション層とトランスポート層の転送者に関する情報も強化していることも含んでいる。

6.2 技術の組み合わせ

秘匿・匿名技術を複数利用して隠蔽できる情報を増やしたり強化することは、2.1節で述べたように多くの秘匿・匿名技術で行われている手法である。本節では、前節で例に挙

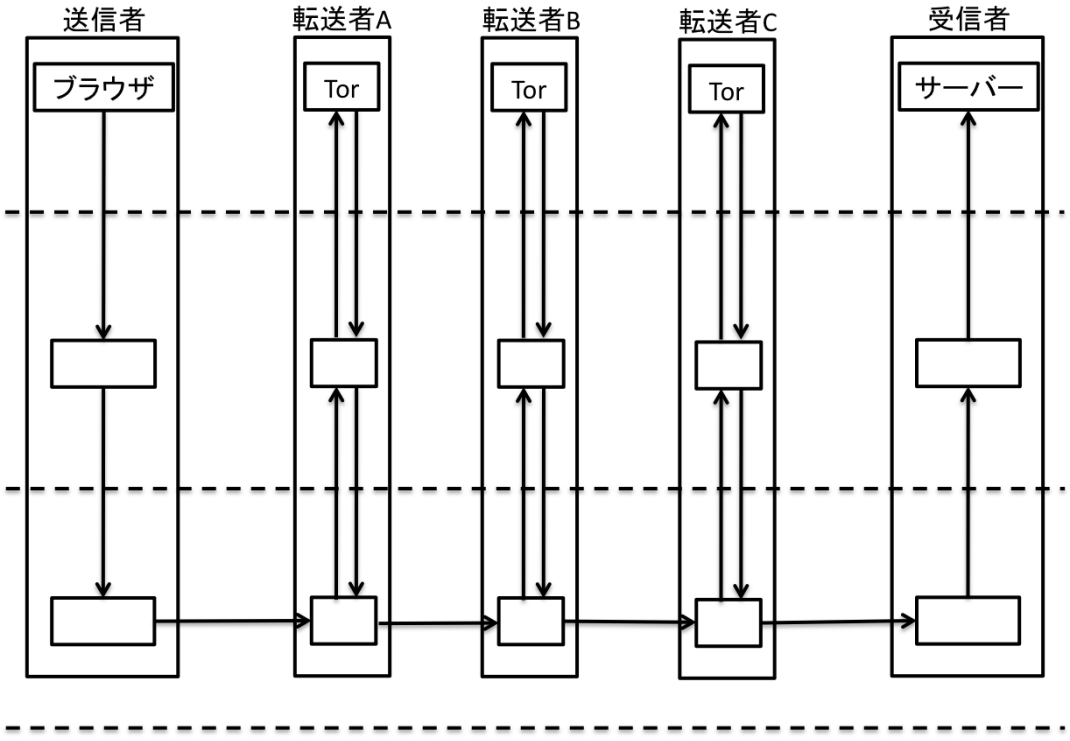

図 6.3: Tor 利用時の送受信者と転送者

表 6.4: Tor への適用

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
アプリケーション	送信者	×	○	△	×	×	○	○	△	×	×	○	○	△	△
	受信者	×	×	△	×	○	×	×	△	×	○	×	×	△	△
	転送者	△	○	×	△	△	○	○	×	△	△	○	○	△	△
	複数の転送者	△	○	△	△	○	○	○	△	△	○	○	○	△	○
	送信者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	送信者・転送者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	受信者・転送者	×	△	△	×	○	△	△	△	×	○	△	△	△	△
	送信者・転送者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	データの内容	×	×	△	○	○	×	×	△	○	○	×	×	△	△
	データの種類	×	×	○	○	○	×	×	△	○	○	×	×	△	△
	データの送信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データの受信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データのパターン	×	×	△	×	△	×	×	△	×	△	×	×	△	△
トランスポート	送信者	×	○	△	×	×	○	○	△	×	×	○	○	△	△
	送信者(NAPT)	×	○	○	×	×	○	○	○	×	×	○	○	○	○
	送信者GW(NAPT)	×	○	△	×	×	○	○	△	×	×	○	○	△	△
	受信者	×	×	△	×	○	×	×	△	×	○	×	×	△	△
	受信者(NAPT)	○	×	○	○	○	×	×	○	○	○	×	×	○	○
	受信者GW(NAPT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	△	△	×	△	△	△	△	×	△	△	△	△	×	△
	複数の転送者	△	○	△	△	○	○	○	△	△	○	○	○	△	△
	送信者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	送信者・転送者	×	○	△	×	△	○	○	△	×	△	○	○	△	△
	受信者・転送者	×	△	△	×	○	△	△	△	×	○	△	△	△	△
	送信者・転送者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	データの内容	×	×	△	○	○	×	×	△	○	○	×	×	△	△
	データの種類	×	×	△	○	○	×	×	△	○	○	×	×	△	△
	データの送信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データの受信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データのパターン	×	×	△	×	×	×	×	△	×	×	×	×	△	△
ネットワーク	送信者	×	○	△	×	×	○	○	△	×	○	○	○	△	△
	送信者(NAT)	×	○	○	×	×	○	○	○	×	○	○	○	○	○
	送信者GW(NAT)	×	○	△	×	×	○	○	△	×	○	○	○	△	△
	送信者の所属ネットワーク	×	○	△	×	×	○	○	△	×	○	○	○	△	△
	送信者の所属国	×	○	△	×	×	○	○	△	×	○	○	○	△	△
	受信者	×	×	△	×	×	×	×	△	×	○	×	×	△	△
	受信者(NAT)	○	×	○	○	○	×	×	○	○	○	×	×	○	○
	受信者GW(NAT)	×	×	×	×	×	×	×	×	×	○	×	×	×	×
	受信者の所属ネットワーク	×	×	△	×	×	×	×	△	×	○	×	×	△	△
	受信者の所属国	×	×	△	×	×	×	×	△	×	○	×	×	△	△
	転送者	△	△	×	△	△	△	△	×	△	△	△	△	×	△
	転送者の所属ネットワーク	△	△	×	△	△	△	△	×	△	△	△	△	×	△
	転送者の所属国	△	△	×	△	△	△	△	×	△	△	△	△	×	△
	複数の転送者	△	○	△	×	○	○	○	△	△	○	○	○	△	△
	送信者・受信者	×	○	○	×	○	○	○	○	×	○	○	○	○	○
	送信者・転送者	×	○	△	×	△	○	○	△	×	△	○	○	△	△
	受信者・転送者	×	△	△	×	○	△	△	△	×	○	△	△	△	△
	送信者・転送者・受信者	×	○	○	×	○	○	○	○	○	○	○	○	○	○
	データの内容	×	×	△	○	○	×	×	△	○	○	×	×	△	△
	データの種類	×	×	△	○	○	×	×	△	○	○	×	×	△	△
	データの送信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データの受信量	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	データのパターン	×	×	△	×	×	×	×	△	×	×	×	×	△	△
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
		アプリケーション			トランスポート					ネットワーク					

表 6.5: HTTP と HTTPS で隠蔽される情報の比較

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
アプリケーション	送信者														
	受信者														
	転送者														
	複数の転送者														
	送信者・受信者														
	送信者・転送者														
	受信者・転送者														
	送信者・転送者・受信者														
	データの内容				強化	強化	強化	強化		強化	強化	強化	強化	強化	強化
	データの種類				強化	強化	強化	強化		強化	強化	強化	強化	強化	強化
	データの送信量														
	データの受信量														
	データのパターン														
トランスポート	送信者														
	送信者(NAPT)														
	送信者GW(NAPT)														
	受信者														
	受信者(NAPT)														
	受信者GW(NAPT)														
	転送者														
	複数の転送者														
	送信者・受信者														
	送信者・転送者														
	受信者・転送者														
	送信者・転送者・受信者														
	データの内容				強化	強化	強化	強化		強化	強化	強化	強化	強化	強化
	データの種類				強化	強化	強化	強化		強化	強化	強化	強化	強化	強化
	データの送信量														
	データの受信量														
	データのパターン														
ネットワーク	送信者														
	送信者(NAT)														
	送信者GW(NAT)														
	送信者の所属ネットワーク														
	送信者の所属国														
	受信者														
	受信者(NAT)														
	受信者GW(NAT)														
	受信者の所属ネットワーク														
	受信者の所属国														
	転送者														
	転送者の所属ネットワーク														
	転送者の所属国														
	複数の転送者														
	送信者・受信者														
	送信者・転送者														
	受信者・転送者														
	送信者・転送者・受信者														
	データの内容				強化	強化	強化	強化		強化	強化	強化	強化	強化	強化
	データの種類				強化	強化	強化	強化		強化	強化	強化	強化	強化	強化
	データの送信量														
	データの受信量														
	データのパターン														
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
		アプリケーション			トランスポート					ネットワーク					

表 6.6: HTTP とプロキシで隠蔽される情報の比較

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
アプリケーション	送信者		強化				強化	強化				強化	強化		強化
	受信者														
	転送者		強化				強化	強化				強化	強化	強化	
	複数の転送者														
	送信者・受信者		強化				強化	強化				強化	強化		強化
	送信者・転送者		強化				強化	強化				強化	強化		強化
	受信者・転送者														
	送信者・転送者・受信者		強化				強化	強化				強化	強化		強化
	データの内容														
	データの種類														
	データの送信量														
	データの受信量														
	データのパターン														
トランスポート	送信者		強化				強化	強化				強化	強化		強化
	送信者(NAPT)			強化					強化						
	送信者GW(NAPT)		強化				強化	強化				強化	強化		強化
	受信者														
	受信者(NAPT)			強化					強化						
	受信者GW(NAPT)														
	転送者														
	複数の転送者														
	送信者・受信者														
	送信者・転送者														
	受信者・転送者														
	送信者・転送者・受信者														
	データの内容														
	データの種類														
	データの送信量														
	データの受信量														
	データのパターン														
ネットワーク	送信者		強化				強化	強化				強化	強化		強化
	送信者(NAT)			強化					強化						
	送信者GW(NAT)		強化				強化	強化				強化	強化		強化
	送信者の所属ネットワーク		強化				強化	強化				強化	強化		強化
	送信者の所属国		強化				強化	強化				強化	強化		強化
	受信者														
	受信者(NAT)			強化					強化						
	受信者GW(NAT)														
	受信者の所属ネットワーク														
	受信者の所属国														
	転送者		強化				強化	強化				強化	強化		強化
	転送者の所属ネットワーク		強化				強化	強化				強化	強化		強化
	転送者の所属国		強化				強化	強化				強化	強化		強化
	複数の転送者		強化				強化	強化				強化	強化		強化
	送信者・受信者		強化				強化	強化				強化	強化		強化
	送信者・転送者		強化				強化	強化				強化	強化		強化
	受信者・転送者														
	送信者・転送者・受信者		強化				強化	強化				強化	強化		強化
	データの内容														
	データの種類														
	データの送信量														
	データの受信量														
	データのパターン														
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
		アプリケーション			トランスポート					ネットワーク					

げた HTTPS とプロキシを組み合わせた場合について検討を行う。

6.2.1 HTTPS とプロキシの組み合わせ

HTTP とプロキシを利用すると、送信者の情報を受信者に隠蔽できるが、プロキシサーバには送受信者の関係だけでなくやりとりしたデータの内容まで筒抜けである。また、送信者とプロキシサーバとの間に存在する端末にも同様に筒抜けである。その対策として、プロキシと合わせて HTTPS を利用しデータの内容を隠蔽することが行われている。そこで、HTTPS とプロキシ技術のそれぞれで作成した隠蔽可能な情報の表 6.2 と表 6.3 を組み合わせることについて考える。

2 つの秘匿・匿名技術を合わせて利用しようとした時、両技術が隠蔽しようとする情報に重複があると競合が起きる可能性が考えられる。この競合については、7.3 節にて詳しく触れる。HTTPS によって隠蔽される情報とプロキシ技術によって隠蔽される情報の重複は、すべて NAT/NAPT に関わる情報であり、HTTPS とプロキシ技術に影響を及ぼすことは無い。そこで、2 つの表を 1 つの表にまとめたのが表 6.7 である。表を結合する上で、以下の規則を適用した。

- 少なくとも一方の技術で隠蔽可能 (○) となっている場合は隠蔽可能 (○)
- どちらの技術も隠蔽不可能 (×) となっている場合は隠蔽不可能 (×)
- どちらの技術も隠蔽可能 (○) ではないが、少なくとも一方は一部隠蔽可能 (△) となっている場合は一部隠蔽可能 (△)

3 番目に関しては、7 節にて詳しく述べる。

ここで考えるべき事は、HTTPS とプロキシ技術を組み合わせた通信がどのようなものかである。HTTPS とプロキシ技術を使った通信には、以下の 2 種類がある。

1. Web ブラウザとプロキシサーバ間で HTTPS 通信を用いる
2. Web ブラウザと Web サーバ間で HTTPS 通信を用いる

6.1.2 節で扱った HTTPS 通信は、Web ブラウザ (送信者) と Web サーバ (受信者) の間で暗号化を行っていることから、ここでも 2 つめの Web ブラウザと Web サーバ間で HTTPS 通信を用いた場合に当てはまると考えられる。1 つめの通信方式の隠蔽情報を考える場合には、アプリケーション層における送信者と転送者間で HTTPS 通信を利用した時の隠蔽情報と隠蔽相手の関係を対象にする必要がある。

表 6.7: HTTPS とプロキシの組み合わせ

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
アプリケーション	送信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	○	×	×	×	○	○	×	×	×	○	○	△	×
	複数の転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・受信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者・転送者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	データの内容	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの種類	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
トランスポート	送信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者(NAPT)	×	○	○	×	×	○	○	○	×	×	○	○	○	○
	送信者GW(NAPT)	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者(NAPT)	○	×	○	○	○	×	×	○	○	○	×	×	○	○
	受信者GW(NAPT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	複数の転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの内容	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの種類	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
ネットワーク	送信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者(NAT)	×	○	○	×	×	○	○	○	×	×	○	○	○	○
	送信者GW(NAT)	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者の所属ネットワーク	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者の所属国	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	受信者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者(NAT)	○	×	○	○	○	×	×	○	○	○	×	×	○	○
	受信者GW(NAT)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者の所属ネットワーク	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	受信者の所属国	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	転送者	×	△	×	×	×	△	△	×	×	×	△	△	×	△
	転送者の所属ネットワーク	×	△	×	×	×	△	△	×	×	×	△	△	×	△
	転送者の所属国	×	△	×	×	×	△	△	×	×	×	△	△	×	△
	複数の転送者	×	△	×	×	×	△	△	×	×	×	△	△	×	△
	送信者・受信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	送信者・転送者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	受信者・転送者	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	送信者・転送者・受信者	×	○	×	×	×	○	○	×	×	×	○	○	×	△
	データの内容	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの種類	×	×	×	○	○	○	○	×	○	○	○	○	○	○
	データの送信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データの受信量	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	データのパターン	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
		アプリケーション			トランスポート					ネットワーク					

6.2.2 Torとの比較

6.2.1節で検討した秘匿・匿名通信技術は、データの内容を暗号化 (TLS) とプロキシを利用することで送信者を隠蔽している。Torも同様に、暗号化とプロキシを利用して送信者を隠蔽する技術である。そこで、この2つの技術について比較検討を行う。比較方法は6.1.5節と同じ方法である。表6.8は、HTTPSとプロキシを利用した通信技術に対するTorの隠蔽度合いを現したものである。全体としては、隠蔽度合いが強化されている情報が多い。これは、Torがプロキシを1つだけではなく複数利用することで転送者を増やし、各転送者と暗号化して通信を行うことで転送者間でも情報の隠蔽が行われているからである。注目すべき点は、データの内容と種類が、トランスポート層・ネットワーク層で受信者に対して隠蔽度合いが悪化していることである。これは、3.3節や6.1.4節でも述べてきた、送信者と受信者の間では暗号化を行っていないことによる。一方で、HTTPSとプロキシを組み合わせた通信では、HTTPSによって送信者と受信者の間でやりとりされるデータが暗号化されているためである。

Torはあくまでも送信者の情報を隠蔽する技術であり、通信データの内容を隠蔽するには別途暗号化を行う技術を利用する必要がある。Webサービスにおいては、HTTPS通信を用いることが考えられる。TorとHTTPSを組み合わせることで、実際にデータの内容が隠蔽できているのかを確認する方法として、本研究の手法を用いることで実現することが出来ると考えられる。

表 6.8: HTTPS &プロキシと Tor の比較

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
アプリケーション	送信者			強化					強化					強化	
	受信者			強化		強化			強化		強化			強化	強化
	転送者	強化			強化	強化				強化	強化				強化
	複数の転送者	強化	強化	強化	強化	強化	強化	強化	強化	強化	強化	強化	強化	強化	強化
	送信者・受信者			強化		強化			強化		強化			強化	
	送信者・転送者			強化		強化			強化		強化			強化	
	受信者・転送者		強化	強化		強化	強化	強化	強化		強化	強化	強化	強化	強化
	送信者・転送者・受信者			強化		強化			強化		強化			強化	
	データの内容			強化			悪化	悪化	強化			悪化	悪化		
	データの種類			強化			悪化	悪化	強化			悪化	悪化		
	データの送信量			強化					強化					強化	強化
	データの受信量			強化					強化					強化	強化
	データのパターン			強化		強化			強化		強化			強化	強化
トランスポート	送信者			強化					強化					強化	
	送信者(NAPT)														
	送信者GW(NAPT)			強化					強化					強化	
	受信者			強化		強化			強化		強化			強化	強化
	受信者(NAPT)														
	受信者GW(NAPT)														
	転送者	強化	強化		強化	強化	強化	強化		強化	強化	強化	強化		強化
	複数の転送者	強化	強化	強化	強化	強化	強化	強化	強化	強化	強化	強化	強化	強化	強化
	送信者・受信者		強化	強化		強化	強化	強化	強化		強化	強化	強化	強化	強化
	送信者・転送者		強化	強化		強化	強化	強化	強化		強化	強化	強化	強化	強化
	受信者・転送者		強化	強化		強化	強化	強化	強化		強化	強化	強化	強化	強化
	送信者・転送者・受信者		強化	強化		強化	強化	強化	強化		強化	強化	強化	強化	強化
	データの内容			強化			悪化	悪化	強化			悪化	悪化		
	データの種類			強化			悪化	悪化	強化			悪化	悪化		
	データの送信量			強化					強化					強化	強化
	データの受信量			強化					強化					強化	強化
	データのパターン			強化					強化					強化	強化
ネットワーク	送信者			強化					強化		強化			強化	
	送信者(NAT)										強化				
	送信者GW(NAT)			強化					強化		強化			強化	
	送信者の所属ネットワーク			強化					強化		強化			強化	
	送信者の所属国			強化					強化		強化			強化	
	受信者			強化					強化		強化			強化	強化
	受信者(NAT)														
	受信者GW(NAT)										強化				
	受信者の所属ネットワーク			強化					強化		強化			強化	強化
	受信者の所属国			強化					強化		強化			強化	強化
	転送者	強化			強化	強化				強化	強化				
	転送者の所属ネットワーク	強化			強化	強化				強化	強化				
	転送者の所属国	強化			強化	強化				強化	強化				
	複数の転送者	強化		強化		強化			強化	強化	強化			強化	
	送信者・受信者			強化		強化			強化		強化			強化	
	送信者・転送者			強化		強化			強化		強化			強化	
	受信者・転送者		強化	強化		強化	強化	強化	強化		強化	強化	強化	強化	強化
	送信者・転送者・受信者			強化		強化			強化	強化	強化			強化	
	データの内容			強化			悪化	悪化	強化			悪化	悪化		
	データの種類			強化			悪化	悪化	強化			悪化	悪化		
	データの送信量			強化					強化					強化	強化
	データの受信量			強化					強化					強化	強化
	データのパターン			強化					強化					強化	強化
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP,IX
		アプリケーション			トランスポート					ネットワーク					

第7章　考察

本章では、前章で得られた問題点とその原因について述べる。

7.1　NAT/NAPTの扱い

表 7.1 から、HTTP,HTTPS, プロキシ, オニオンルーティングの各技術に割り当てたどの場合でも、送信者 (NAPT), 受信者 (NAPT), 送信者 (NAPT), 受信者 (NAT) の項で隠蔽できる (○) となっていたことが分かる。表中では、すべての技術で○となっていた箇所を”重複”としている。これは、NAT/NAPT が情報を隠蔽する技術となっていたためである。当然ながら、2 章の定義より、NAT/NAPT は秘匿・匿名技術に含まれる。よって、隠蔽される情報から NAT/NAPT は除外する必要があった。そもそも、NAT/NAPT は情報を隠蔽するために考案された技術では無いが、結果として NAT/NAPT の内側に位置する端末の IP アドレスとポート番号を NAT/NAPT 外の端末に対して隠蔽している。このような、情報を隠蔽するために考案された技術では無いものが結果として情報を隠蔽しているということは、他の技術でもありうる。

7.2　部分的に隠蔽可能

作成した表の中で△となった箇所は、隠蔽相手に該当する端末が複数存在する状況で、その一部に対して隠蔽が出来ていないことを意味している。特に、転送者に関する部分で多かった。これは、ネットワーク層で転送者が複数存在するためであり、更に細かく分ける必要があると言える。

7.3　組み合わせ不可な技術

本節では、秘匿・匿名技術を複数組み合わせて利用しようとした時、技術的に競合し利用できない可能性があることについて検討する。

単純な例として、IP アドレスを偽装した IP パケットを送信する場合を考える。この時、偽装されたパケットが相手に届いたとする。受信者は、そのパケットの送信者を知ることは出来ず、転送者についてもすべてを把握することが困難である。この手法は DoS 攻撃 (Denial of Service attack) でよく用いられるが、秘匿・匿名技術として用いることも出来

表 7.1: HTTP,HTTPS, プロキシ, オニオンルーティングの重複

	情報＼相手	アプリケーション			トランスポート					ネットワーク					
		送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP.IX
アプリケーション	送信者														
	受信者														
	転送者														
	複数の転送者														
	送信者・受信者														
	送信者・転送者														
	受信者・転送者														
	送信者・転送者・受信者														
	データの内容														
	データの種類														
	データの送信量														
	データの受信量														
	データのパターン														
トランスポート	送信者														
	送信者(NAPT)		重複				重複	重複				重複	重複	重複	重複
	送信者GW(NAPT)														
	受信者														
	受信者(NAPT)	重複			重複	重複				重複	重複			重複	重複
	受信者GW(NAPT)														
	転送者														
	複数の転送者														
	送信者・受信者														
	送信者・転送者														
	受信者・転送者														
	送信者・転送者・受信者														
	データの内容														
	データの種類														
	データの送信量														
	データの受信量														
	データのパターン														
ネットワーク	送信者														
	送信者(NAT)		重複				重複	重複				重複	重複	重複	重複
	送信者GW(NAT)														
	送信者の所属ネットワーク														
	送信者の所属国														
	受信者														
	受信者(NAT)	重複			重複	重複				重複	重複			重複	重複
	受信者GW(NAT)														
	受信者の所属ネットワーク														
	受信者の所属国														
	転送者														
	転送者の所属ネットワーク														
	転送者の所属国														
	複数の転送者														
	送信者・受信者														
	送信者・転送者														
	受信者・転送者														
	送信者・転送者・受信者														
	データの内容														
	データの種類														
	データの送信量														
	データの受信量														
	データのパターン														
	情報／相手	送信者	受信者	転送者	送信者	送信者GW	受信者	受信者GW	転送者	送信者	送信者GW	受信者	受信者GW	転送者	ISP.IX
		アプリケーション			トランスポート					ネットワーク					

る。パケットは一方的に送信者から受信者へと転送されるのみで、受信者から送信者へとパケットが正しく届くことは無く、双方向に通信を行ってはいない。他の秘匿・匿名技術と組み合わせてこの技術を利用しようとした場合、多くの秘匿・匿名技術は双方向通信を必須としており、組み合わせて利用することは困難と言える。このことから、どんな秘匿・匿名技術でも組み合わせて利用することが出来るとは言えず、手当たり次第に秘匿・匿名技術を使って隠蔽情報を増やすことは出来ない。ただし、事前に IP アドレスを偽装して送信をすることが送受信者で共有できれば、活用することは可能である。事前の情報共有の方法に依るが、送受信者が共に IP アドレスを偽装したパケットを送信しあって双方向に通信をするができる。この通信を監視する者には、この送受信者が通信を行っているようには見えないだろう。

本研究の提案では、技術の組み合わせの可否を機械的に判別することが出来ないため、技術を理解した者による判別が必要となる。例えば Tor は、オーバーレイ・ネットワークによって上位に TCP と同等の機能を提供している。この場合であれば、TCP 通信を利用する秘匿・匿名技術との組み合わせが可能であると判別することが容易である。プロトコルスタックと同じように、秘匿・匿名技術を組み合わせて利用することを考える場合には、下位に位置する技術が上位に提供するサービスを考慮する必要があると言える。本研究の提案を有効に活用していくためには、機械的もしくは容易に判別可能とする方法を用意する必要がある。

第8章　結論

本研究は、秘匿・匿名技術と制御・監視技術の関係を明らかにするため、秘匿・匿名技術の相互関係を比較する手法の確立を目的とした。その手法として、技術の積み重ねと隠蔽される情報・相手に着目した。提案した手法で、各秘匿・匿名技術の特徴を表すことができ、容易に比較を行うことが出来た。これにより既存の秘匿・匿名技術間の関係を調査することができるようになり、制御・監視する者の脅威となり得る技術の洗い出しを可能とした。

本研究では、隠蔽される可能性のある情報と隠蔽される可能性のある相手を検討し選び出した。しかし、作成した表の中には一部で隠蔽できない (△) と判断した部分があった。これは隠蔽相手についての細分化が不足しているためであり、複数の転送者が存在する際に問題となった。また、複数の技術に当てはめても必ず同じ結果となる部分があった。これは、選び出した隠蔽情報と隠蔽相手の項目に不必要または統合可能である項目が含まれている可能性がある。これらの問題に関しては、更に多くの秘匿・匿名技術に適用することで、隠蔽情報と隠蔽相手に必要または不必要な項目が明確になるであろう。そして、秘匿・匿名技術と制御・監視技術の関係を明らかにする手法として有効性が向上するだろう。

本研究で提案した手法は、既存の秘匿・匿名技術と制御・監視技術の関係を明らかにするだけでは無く、新たに登場する秘匿・匿名技術にも対応可能である。また、一般的に考えられている秘匿通信や匿名通信の枠に囚われず、新たな秘匿・匿名技術を検討する際にも有効である。その際、新たに必要となる制御・監視技術も露呈することになるが、両技術が活発に研究・開発される良い起爆剤になるだろう。

謝辞

本研究を完遂するに当たって、多くの方々に御指導、御協力を賜りました。ここに感謝の意を示し、心からお礼申し上げます。主指導教員の篠田陽一教授には始終手厚い御指導を頂きました。主テーマ審査員の丹康雄教授、知念賢一特任准教授、副テーマ指導教員である飯田弘之教授には適切な御指摘を頂きました。本学の宇多仁助教には多くの御助言を頂きました。情報通信研究機構北陸 StarBED 技術センターの三輪信介氏、宮地利幸氏、中井浩氏には適切な御指導、御助言を頂きました。本研究室の高野祐輝氏、LATT Khin Thida 氏、安田真悟氏、井上朋哉氏、Nguyen Lan Tien 氏、Muhammad Imran Tariq 氏、明石邦夫氏、立花一樹氏、山田悠介氏、鍛治祐希氏、大野夏希氏、田部英樹氏、向井雄一朗氏、村上正太郎氏には数多くの御協力を頂きました。また、小原泰弘氏、SABER ZRELLI 氏、芳炭将氏、NGUYEN Nam Hoai 氏、松井大輔氏、佐川喜昭氏、栗原良尚氏、中村祐輔氏、 橋本将彦氏、吉岡慎一郎氏にも多くの御協力・御助言を頂きました。重ねて心からお礼申し上げます。最後に、研究や生活を支えてくれた家族に感謝致します。

参考文献

[1] I2P: Anonymous Network. http://www.i2p2.de/.

[2] InterTrack. http://intertrack.naist.jp/.

[3] Mixmaster. http://mixmaster.sourceforge.net/.

[4] Squid cache. http://www.squid-cache.org/.

[5] uRPF. http://itpro.nikkeibp.co.jp/article/COLUMN/20060224/230636/.

[6] トレースバック 研究ポータルサイト. https://www.telecom-isac.jp/tb/.

[7] Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong. Freenet: A distributed anonymous information storage and retrieval system. In *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, pp. 46–66, July 2000.

[8] George Danezis, Claudia Díaz, Emilia Käsper, and Carmela Troncoso. The wisdom of crowds: Attacks and optimal constructions. In Michael Backes and Peng Ning, editors, *Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS 2009), Saint-Malo, France, September 21-23*, Vol. 5789 of *Lecture Notes in Computer Science*, pp. 406–423. Springer, 2009.

[9] W. Diffie and M. E. Hellman. New Directions in Cryptography. In *IEEE Transactions on Information Theory*, Vol. IT-22, 1976.

[10] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[11] Taher Elgamal. A Public-Key Cryptosystem and a Sigunature Scheme Based on Discrete Logarithms. In *IEEE Transactions on Information Theory*, Vol. IT-31, 1985.

[12] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee. Hypertext Transfer Protocol – HTTP/1.1, RFC2616. June 1999.

[13] J. Jonsson and B. Kaliski. Public-Key Cryptography Standards (PKCS) 1: RSA Cryptography Specifications Version 2.1, RFC3447. February 2003.

[14] E. Rescorla. HTTP Over TLS, RFC2818. May 2000.

[15] Eric Wustrow, Scott Wolchok, Ian Goldberg, and J. Alex Halderman. Telex: Anticensorship in the Network Infrastructure. In *Proceedings of the 20th USENIX Security Symposium*, aug 2011.

[16] 松本 勉鈴木 雅貴. インターネット通信制御機構 ICMP を利用した秘匿通信の一方式. 電子情報通信学会技術研究報告. SST, スペクトル拡散, 2000.