5. 通信におけるインフォメーションハイディング

松本　勉　横浜国立大学大学院環境情報研究院
tsutomu@mlab.jks.ynu.ac.jp
井上大介　横浜国立大学大学院工学研究科
dai@mlab.jks.ynu.ac.jp
鈴木雅貴　横浜国立大学大学院環境情報学府
suzuki@mlab.jks.ynu.ac.jp

■通信における 2 つの情報ハイディング

通信における情報ハイディング技術を，通信プロトコルや通信行為を媒体とする技術と匿名通信の 2 つに分けて紹介する．前者は，見せかけの通信に真の通信を紛れ込ませ，その存在を第三者に秘匿することを目的とするものが多いが，IP パケットに逆探知のための情報を埋め込み，不正パケットの発信源を突き止めようとする IP トレースバック技術などへの応用もある．匿名通信は，通信に携わるエンティティを隠す技術であり，送信者を特定する IP アドレスなどの情報を受信者や第三者に対して隠すことを狙ったものが多い．匿名での Web アクセスやオンラインカウンセリングなどプライバシ保護が必要となる場面で役立ち，多くの電子投票方式の要素技術としても用いられる．

■通信の仕組みを利用した情報ハイディング

TCP/IP 階層におけるネットワークインタフェース層，インターネット層，トランスポート層，アプリケーション層のそれぞれにおいて，通信プロトコルや通信行為を媒体とする情報ハイディング技術が考えられている．登場するエンティティを，Alice（送信者），Bob（受信者），Carol（第三者），Wendy（攻撃者）とする（**図 -1**）．

◇ネットワークインタフェース層

パルス信号の電圧を用いた方式

同軸ケーブルやツイストペアケーブルなどの伝送媒体では，0 と 1 の 2 値の情報を，それぞれ 0V と 5V のように対応させ，パルス信号として送出するが，伝送途中のノイズの影響を考慮し，受信側ではたとえばパルス信号が 5V と 5.5V のどちらであってもそれを 1 として判断する．R. Popa[1] は，Alice が埋込情報に応じて 5V または 5.5V のパルス信号を送信し，Bob が受信したパルス信号の電圧を通常よりも精密に観測するという通信方法を示している．

Ethernet の衝突を用いた方式

Ethernet では同時にデータを送信してデータの衝突を起こした 2 つの端末が再衝突することを回避するために，ランダムな時間（バックオフ時間）をおいてデータを再送する決まりである．T. G. Handel と M. T. Stanford[2] は，2 つの端末のどちらが先にデータを再送するかという事象を利用した情報ハイディングが可能であることを示している．Alice は Ethernet 上で Carol のデータ送出を検出すると，即座に自身もデータを送出し故意に衝突を発生させる．そして埋込情報に応じて再送の順序を Carol よ

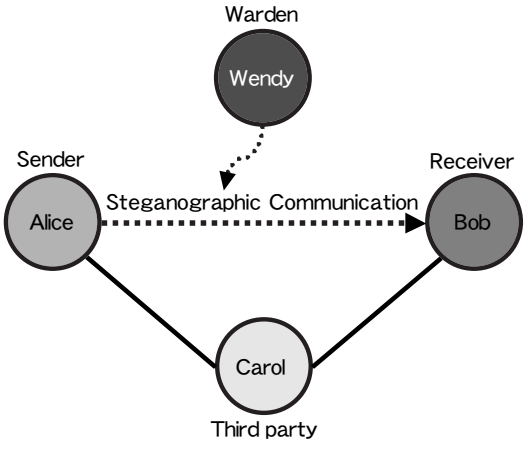

図 -1　登場エンティティ

り先にするか後にするかを決定し，先の場合は短いバックオフ時間で再送，後の場合は Carol の再送が終了するのを待って再送する．Bob は，Alice と Carol のデータ再送の順序を観察して埋込情報を知ることができる．なお Alice のデータ信号の宛先は誰であってもよい．

◇インターネット層とトランスポート層

パケットの到着順序を用いた方式

K. Ahsan と D. Kundur[3] は，パケットの送出順序と到着順序がネットワークの輻輳などにより必ずしも一致しないことを利用した情報ハイディングの手法を示している．K 個のパケットには K! 個の順序があるが，ネットワーク上で本当に起こる順序の変化を吸収するため，K! 個の中から N 個の順序を選びそれぞれに情報を割り当てておく．Alice は埋込情報に対応した順序でパケットを送信し，Bob はパケットの到着順序から埋込情報を特定する．ネットワーク上でパケットの順序が入れ替わり N 個の順序のどれにも該当しない場合，Bob は受信した順序に最も近い順序を選択し埋込情報を推定する．Ahsan らはパケットの順序の判別に，IPsec の AH ヘッダや ESP ヘッダのシーケンス番号を利用している．

TCP ヘッダや IP ヘッダを用いた方式

Handel らや Ahsan らなど多くの研究者によって，IP データグラムや TCP セグメントのヘッダに含まれる未使用のフィールドや，送信者が値を任意に設定できるフィールドを利用した情報ハイディング手法が提案されている [1)〜3)]．IP ヘッダと TCP ヘッダのうち，情報ハイディングに利用可能であると示唆されているフィールドを**図 -2** に示す（灰色のフィールドが利用可能）．なお，追跡のための情報の格納に IP ヘッダの Identification フィールドを利用する IP トレースバック方式がある．

ICMP エラーメッセージを用いた方式

通信経路上でパケットに何らかのエラーが検出された場合，エラーの種類とエラーを起こしたオリジナルパケットの一部を含んだ ICMP（Internet Control Message Protocol）エラーメッセージがパケットの送信者宛てに発行される．M. Suzuki と T. Matsumoto [4] は，Alice と Bob が間接的に通信する次のような方法を示している．Alice は，たとえば到達不能なアドレスを宛先に指定するなど，埋込情報を含んだパケットがエラーを起こすように操作すると共にパケットの送信元アドレスに Bob のアドレスを設定して送出する．このパケットのエラーを検知した通信経路上のルータ Carol は，ICMP エラーメッセージを送信元アドレスに設定されている Bob 宛てに発行する．Bob は受信したエラーメッセージのオリジナルパケットの部分から埋込情報を抽出する．

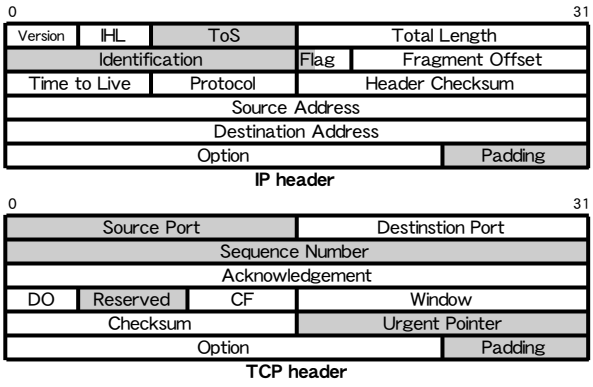

図 -2　TCP/IP ヘッダの埋込可能フィールド

送信元アドレスを操作して第三者を介した通信を行う方法にはこの他，C. H. Rowland [5] による TCP の 3-way handshake を利用したものがある．

◇アプリケーション層

画像・音声・テキストなどをカバーメディアとした方式も，アプリケーション層に属する情報ハイディング技術と捉えることができるが，ここではアプリケーション層における通信プロトコルや通信行為そのものをカバーメディアとする方式について触れる．

ファイルへのアクセス行為を用いた方式

カバートチャネルの存在を指摘した B. W. Lampson [6] は，Alice が自身のディスク内にある特定のファイルについて，外部からのアクセスを許可するか否かで，アクセスしてきた Bob に情報が伝達可能であることを示している．Handel ら [2] は Bob のディスク上に外部からアクセス可能な複数のファイルを置いておき，Alice がどのファイルにアクセスするかによって Bob に情報を伝えるというアプローチを示している．

HTTP クッキーを用いた方式

松本・糸山・池田・村瀬 [7] は HTTP クッキーを利用した情報ハイディング方式を提案している．HTTP クッキーは Web サーバがクライアントの情報やアクセス履歴などをクライアント自身のディスク内に記憶させるためのプロトコルであり，クッキー情報の中の NAME エントリはセミコロン，コロン，空白を除く任意の文字列を取り得るため情報の埋込個所として利用できる．いま Alice を Web サーバ，Bob をクライアントとする．Bob は Alice にアクセスする際に Bob 自身が適当に生成したクッキー情報を Alice に送る．Alice は送られてきたクッキー情報が Alice 自身の生成したものかどうかを検査し，

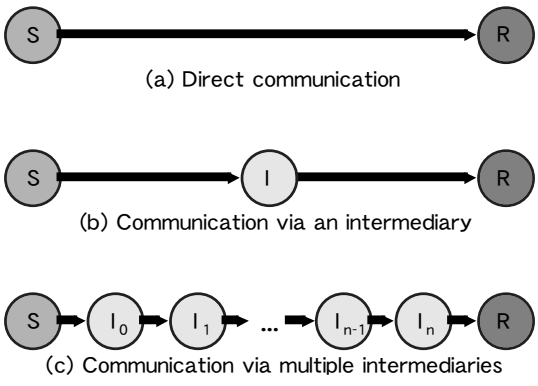

図 -3　転送型ネットワーク

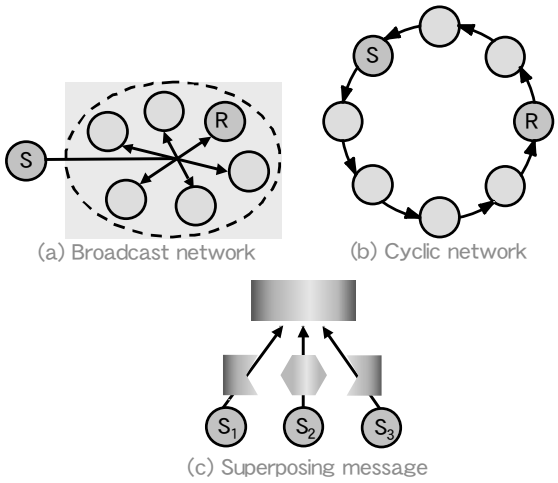

図 -4　転送型以外の匿名通信

そうでない場合には通信相手が Bob であると判断する．そしてクッキー情報の更新と見せかけて，NAME エントリに埋込情報を設定して Bob に送信する．一方，一般のクライアントである Carol がアクセスしてきた際には，Alice は通常の Web サーバとして振舞う．

ネットワークゲームを用いた方式

陳・井上・鈴木・松本 [8] はネットワーク対戦型のゲームをカバーメディアとしたステガノグラフィ方式を提案している．多くのゲームはある局面を 1 つの状態と考え，その局面で選択可能な手を枝と見なすと状態遷移図として記述できる．Alice と Bob がゲームの任意の状態（局面）から出る複数の枝（選択可能な手）に対して情報を割り当てるための規則を共有しておき，ゲームをする際に埋込情報に対応した手を選択することで，Alice と Bob 間で双方向のステガノグラフィ通信が行える．また，枝への情報割り当ての規則を Alice と Bob が共有しておけば，Alice が Carol と対戦し Bob がそれを観戦するという形態でも，Alice から Bob へ情報を伝えることができる．

■匿名通信

匿名通信は，通信に携わるエンティティを一意に特定可能とする情報の守秘を目的とした情報ハイディング技術である．

◇匿名通信の原理

送信者が受信者と直接通信を行う通信形態では送信者の匿名性を守ること，すなわち送信者のアイデンティティを受信者や経路上の第三者に対して秘匿することが難しい（**図 -3 (a)**）．そこで匿名通信の最も単純な方法として，送信者と受信者との通信に中継者を 1 つ介在させる方法が考えられる（**図 -3 (b)**）．中継者が送信者から送られてきたメッセージから送信者を特定可能な情報を削除して受信者に転送する方法をとれば，受信者が送信者を特定することは困難になる．インターネット上に点在する Proxy サーバの利用は，この形態の匿名通信であるとみなせる．単一の中継者に送受信者の対応を知られることが問題である場合には，複数の中継者を鎖状に連結して転送を繰り返す方法が利用できる（**図 -3 (c)**）．

各中継者は自身の前後の中継者を知るだけであり，一中継者が単独で送信者を特定することは困難である．また転送経路上で送信者に最も近い中継者（I_0）は送信者から直接メッセージを受け取っているが，送信者の振舞いが他の中継者のそれと類似していれば，I_0 が送信者を中継者と区別することは難しい．このような転送型ネットワークは既存の匿名通信方式でよく用いられている．なお受信者が匿名の送信者に対して返信メッセージを送るには，転送経路を逆順に辿って送り届ける方法が普通であり，そのためには，中継者が転送したメッセージごとに前後の経路情報を一定期間保存しておく必要がある．

匿名通信には転送型ネットワーク以外の方法もたくさんある．たとえばブロードキャスト型ネットワーク（**図 -4 (a)**）は，送信者が受信者をすべて特定した上でメッセージを送信するのではないから，受信者の匿名性を満たす匿名通信路を形成している．

環状にホストが配置された環状ネットワーク（**図 -4 (b)**）では，送信者が発したメッセージが環状ネットワークを構成するすべてのホストを巡回する．この結果，微視的に見れば転送型ネットワークであり，その特性である送信者の匿名性を持つ．また，巨視的に見ればブロードキャスト型ネットワークであり，その特性である受信者の匿名性も持つ．

この他の匿名通信方式として，送信者を含む，協力者

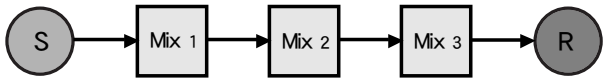

図 -5　Mix-net

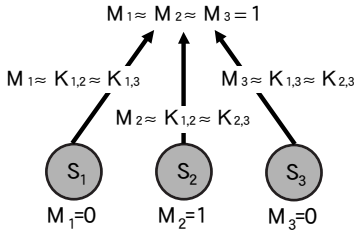

図 -6　DC-net

全員がメッセージに暗号的な処理を施して一斉送信し，そのすべての結果を重ね合わせることで送信者のメッセージが復元されるというアイディアにより送信者の匿名性を保護する方式もある（**図 -4 (c)**）．

◇匿名通信方式の例

Mix-net

Mix-net は D. Chaum [9] が提案した公開鍵暗号系を用いた匿名通信方式であり，Mix と呼ばれる中継サーバを複数経由した転送型ネットワークによって送信者の匿名性を保護する．**図 -5** の例では，送信者 S は受信者 R に近い側の Mix から順にその公開鍵 PK_{Mix_n} を用いてメッセージ M を各エンティティのアドレス A_n と共に次のように多重暗号化する（暗号化の際にパディングされる乱数は簡単のため省略する）：PK_{Mix1} $(A_{Mix2}\|PK_{Mix2}$ $(A_{Mix3}\|PK_{Mix3}$ $(A_R\|M))$）．

この多重暗号化されたメッセージを受け取った Mix1 はこれを PK_{Mix1} に対応した秘密鍵で復号し，次のアドレス A_{Mix2} を知り，残りのメッセージを Mix2 に転送する．以下同様に各 Mix で復号を繰り返し，最終的に M が受信者 R に送り届けられる．このとき各 Mix は自身の前後の経路しか知り得ない（Mix2 には送信者も受信者も分からない）．なお各 Mix では第三者による追跡を困難にするため複数のメッセージがバッチ処理され，その順序がシャッフルされる．また各 Mix 間を流れるメッセージを固定長に制御すればさらにメッセージの追跡が困難となる．

DC-net

D. Chaum [10] が提案したメッセージの重ね合わせに基づく匿名通信方式．レストランで食事を共にしていた 3 人の暗号学者（Dining Cryptographers）S_1, S_2, S_3 が，その場の支払いがすでに済んでいることをウエイターに告げられた．彼らは 3 人のうちの誰かが支払いをしたのか，それとも NSA（米国家安全保障局）が肩代わりしたのかを，支払い者を（もし 3 人の中にいるのであれば）秘密にしたまま知りたいと考えた．暗号学者 S_1 は 2 値のメッセージ M_1（0：支払っていない，1：支払った）と，S_2 と共有した鍵 $K_{1,2}$，および S_3 と共有した鍵 $K_{1,3}$ との排他的論理和を送信する（**図 -6**）．S_2 も S_3 も同様の作業をする．3 人の送信結果の排他的論理和をとるとそれぞれの鍵が相殺され，この例では 3 人のうちの誰かが支払ったことを示すメッセージ「1」が得られる．このように送信にすべてのメンバが協力しメッセージを重ね合わせることで，真の送信者を隠したまま意図したメッセージが得られる．ただしメンバ数に関するスケーラビリティの問題や，複数のメンバがメッセージを同時に送信を試みた際の衝突の問題などがある．

メッセージの重ね合わせを用いた匿名通信には，この他，H. Kikuchi [11] の方式などがある．

Anonymous Remailer

匿名リメーラは電子メールの中継サーバとして働き，送信者の受信者に対する匿名性を達成するものであり，3 つのタイプがある．

Type 0 remailer：最も単純な単一中継者型の匿名リメーラ．匿名メールの送信者はメール本文の先頭に特定の形式で受信者のメールアドレスを記し，匿名リメーラに送信する．匿名リメーラは受信者のメールアドレスをメール本文から取り去った後，そのアドレス宛てにメール本文（もとの送信者のアドレスなし）を転送する．

Type 1 remailer：通称 Cypherpunk remailer. 多重暗号化された電子メールが複数の匿名リメーラ間で転送され，受信者に送り届けられる．

Type 2 remailer：通称 Mixmaster. Cypherpunk remailer の機能に加え，メッセージの追跡をさらに困難にするため，Mixmaster におけるメッセージのシャッフルと，Mixmaster 間のパケットを固定長に保つ機能を有する．

Anonymizer（http://www.anonymizer.com/）

単一中継者型の匿名通信サービス．ユーザ（送信者）からのHTTPリクエストをWebサーバに転送し，Webサーバからのリプライをユーザに届けることで，ユーザのWebサーバに対する匿名性を保護する．中継の際にAnonymizerはHTTPヘッダに記載されたユーザに関連した情報を削除し，Webサーバがユーザのディスクにクッキー情報を書き込むことを防ぎ，ブラウザが保持している個人情報にWebサーバがアクセスできないようJavaおよびJavaスクリプトの動作を停止させる．

E. Gabberら[12]が示した“LPWA”（Lucent Personalized Web Assistant）は，Anonymizerと同様にHTTPのプロキシとして機能するが，アクセスするWebサーバごとにユーザにaliasと呼ばれる擬似的なIDを割り振る．

Onion Routing（http://www.onion-router.net/）

米Naval Research Lab[13]によるMix-netに基づく汎用の匿名通信方式．インターネット上に設置されたonion routerと呼ばれる特殊なルータを複数中継した転送型ネットワークにより送信者の匿名性を保護する．経路情報は複数のonion routerの公開鍵を用いて多重暗号化され（この多重暗号化された経路情報はonionと呼ばれる），転送過程で各onion routerがonionを1層ずつ復号することで匿名のコネクションが確立される．Onion Routingでは暗号化処理によるオーバーヘッドを軽減するために，メッセージ本体は共通鍵暗号方式によって多重暗号化される．このためonionには経路情報とともにメッセージ暗号化用の共通鍵が含まれている．なお経路の設定やonionの生成（共通鍵の生成を含む）は送信者に隣接したonion（proxy onion）によって行われる．受信者からの返信メッセージは共通鍵で多重暗号化されながら転送経路を逆順に辿ってproxy onionまで届き，そこで復号されて送信者に平文として届けられる．類似技術に“Freedom Net”（http://www.freedom.net/）や“PipeNet”（http://www.eskimo.net/~weidai/pipenet.txt）などがある．

Crowds

AT&T[14]によるWebに特化した匿名通信方式．Onion Routingと同様，複数の中継者を経由した転送型ネットワークにより送信者の匿名性を保護するが，中継者は静的なサーバではなく，送信者と同等なユーザからなる動的なグループ（crowd）である．匿名のWebアクセスを行いたいユーザはcrowdに参加し，そのメンバ（jondo）の一員となる．送信者はHTTPリクエストをcrowdから無作為に選んだjondoに転送する（自分自身に転送することもある）．リクエストの転送を受けたjondoは確率Pで無作為選出したjondoにさらに転送するか，または確率$1-P$でリクエストをWebサーバに送信する．このメカニズムによってリクエストの転送経路はランダムに形成される．なおリクエストは共通鍵暗号で暗号化された状態で転送され，Webサーバからの返信は転送経路を逆順に辿って送信者まで送り届けられる．

匿名で通信したいエンティティ同士がグループを形成しPeer-to-Peer通信を行うというアイディアは，M. J. Freedman[15]らによる“Tarzan”（http://pdos.lcs.mit.edu/tarzan/）にも用いられている．TarzanではCrowdsにおけるグループのメンバの各々がonion routerと同様な処理を行うことで匿名通信を実現している．

Rivulet

D. InoueとT. Matsumoto[16]が提案した転送型ネットワークとブロードキャスト型ネットワークの両方を用いる匿名通信方式．転送型ネットワークを利用した匿名通信のほとんどが一本鎖状の転送経路であるのに対し，Rivuletは2分木状の転送経路を形成する（**図-7**）．送信者は，メッセージを複数の断片に分割し，グループから無作為に選んだ2メンバに転送する．転送を受けたメンバは断片の1つを受信者に送信し，残りの断片を送信者と同様に他の2メンバに転送する．受信者は複数のメンバから断片を受け取り，それら断片から元のメッセージを復元する．一方，匿名の送信者への受信者からの返信は転送の際とは異なる経路，すなわちグループ全体へのマルチキャストで実現される．マルチキャストによる返信はネットワークの帯域を浪費するが，メッセージの転送に携わったメンバが返信のために経路情報を保持しておく必要がなく返信に関する中継者の負担は軽い．またRivuletは匿名通信における最大のボトルネックである暗号化処理を用いないという特徴を持つ．

ブロードキャスト型ネットワークを利用した匿名通信には，この他，C. ShieldsとB. N. Levine[17]による“HORDES”や，R. Sherwoodら[18]による“P5”（Peer-to-Peer Personal Privacy Protocol）などがある．

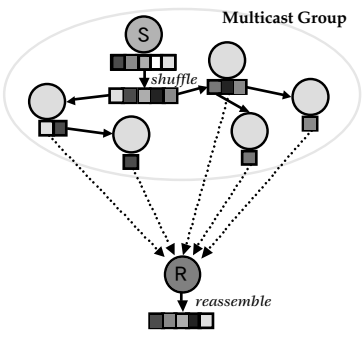

図-7　Rivulet

◇情報公開者の匿名性

Web サーバのような情報公開者の匿名性保護技術は送信者のそれと同様，中継者によるメッセージの転送に基づくものが多い．以下にあげる例の他にも M. Waldman ら [19] による“Publius”(http://publius.cdt.org/) や，I. Clarke ら [20] による“Freenet Project”(http://freenetproject.org/)，V. Scarlata ら [21] による“APFS”(Anonymous Peer-to-Peer File Sharing) などがある．

Rewebber Network および TAZ Server (http://www.rewebber.de/index.php3.en)

Rewebber は暗号化された URL を復号して中継することのできる Proxy サーバである．ユーザは閲覧したい URL (target_url) を Rewebber の公開鍵 PK で暗号化して Rewebber に送信する (http://rewebber_url/PK (target_url) / という形式でブラウザに入力)．Rewebber は暗号化された URL を復号して target_url にアクセスし，Web サーバからのレスポンスをユーザに返す．これによって第三者がユーザと Rewebber の間の通信を盗聴しても Web サーバを特定することは困難となる．また Web サーバ側が暗号化した URL を匿名でニュースグループに投稿するなどしてユーザに告知し，ユーザがその暗号化された URL を用いて Rewebber 経由で Web サーバにアクセスすれば，ユーザに対しても Web サーバの匿名性を守ることができる．

TAZ Servers は Rewebber Network の機能拡張版であり，暗号化された URL を意味のある文字列に置き換えて使用できる．

参考文献

1) Popa, R. : An Analysis of Steganographic Techniques, Univ. of Timisoara (1998).
2) Handel, T. G. and Sandford, M. T. : Hiding Data in the OSI Network Model, Information Hiding, Lecture Notes in Computer Science, Springer-Verlag, No.1174, pp.23-38 (1996).
3) Ahsan, K. and Kundur, D. : Practical Data Hiding in TCP/IP, ACM Mulimedia'02 (2002).
4) Suzuki, M. and Matsumoto, T.: A Scheme of Secret Ccommunication Using Internet Control Message Protocol, IEICE Trans. Fundamentals., Vol. E85-A, No.1, pp.181-189 (2002).
5) Rowland, C. H. : Covert Channels in the TCP/IP Protocol Suite, First Monday, Vol.2, No.5 (1997).
6) Lampson, B.W. : A Note on the Confinement Problem, Communication of the A.C.M., Vol.16, No.10, pp. 613-615 (1973).
7) 松本 勉，糸山大志，池田竜朗，村瀬一郎：クッキーを用いた情報ハイディング方式とその応用，1999 年暗号と情報セキュリティシンポジウム講演論文集，pp.521-526 (1999).
8) 陳 利君，井上大介，鈴木雅貴：ゲームを用いたステガノグラフィ，2001 年暗号と情報セキュリティシンポジウム予稿集，pp.453-458 (2001).
9) Chaum, D. : Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Comm. ACM, Vol. 24, No. 2, pp.84-88 (1981).
10) Chaum, D. : The Dining Cryptographers Problem: Unconditionally Aender and Recipient Untraceability, Journal of Cryptology, pp.65-75 (1988).
11) Kikuchi, H. : Sender and Recipient Anonymous Communication without Public key Cryptography, IPSJ SIG Notes, 98-CSEC-1-8, pp.41-46 (1998).
12) Gabber, E., Gibbons, P., Matias, Y. and Mayer, A.: How to Make Personalized Web Browsing Simple, Secure, and Anonymous, Financial Cryptography'97, LNCS 1318, pp.17-31 (1997).
13) Syverson, P. F., Goldschlag D.M. and Reed, M.G.: Anonymous Connections and Onion Routing, IEEE Symposium on Security and Privacy, pp.44-54 (1997).
14) Reiter, M. K. and Rubin, A.D.: Crowds: Anonymity for Web Transactions, DIMACS Technical Report pp.97-15 (1997).
15) Freedman, M. J. , Sit, E., Cates, J. and Morris, R. : Introducing Tarzan, a Peer-to-Peer Anonymizing Network Layer, Proc. of the 1st International Workshop on Peer-to-Peer Systems (2002).
16) Inoue, D. and Matsumoto, T. : Rivulet: An Anonymous Communication Method Based on Group Communication, IEICE Trans. Fundamentals, Vol. E85-A, No.1, pp.94-101 (2002).
17) Shields, C. and Levine, B.N. : A Protocol for Anonymous Communication Over the Internet, Proc. of the 7th ACM Conference on Computer and Communication Security (2000).
18) Sherwood, R., Bhattacharjee, B. and Srinivasan, A. : P5 : A Protocol for Scalable Anonymous Communication, Proc. of the 2002 IEEE Symposium on Security and Privacy (2002).
19) Waldman, M., Rubin, A. D. and Cranor, L. F. : Publius: A Robust, Tamper-Evident, Censorship-Resistant Web Publishing System, Proc. of the 9th USENIX Security Symposium (2000).
20) Clarke, I., Sandberg, O., Wiley, B. and Hong, T.W. : Freenet: a Distributed Anonymous Information Storage and Retrieval System, Proc. of the International Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009 (2000).
21) Scarlata, V., Levine, B.N. and Shields, C. : Responder Anonymity and Anonymous Peer-to-Peer File Sharing, Proc. the IEEE International Conference on Network Protocols 2001 (2001).

(平成 15 年 2 月 13 日受付)