インターネット上で匿名性を有するサービスを実現するために

Toward Realization of Anonymous Services on the Internet

関西大学　社会安全学部
河　野　和　宏
Kansai University, Faculty of Safety Science
Kazuhiro KONO

SUMMARY

This paper presents current situations, issues, and several practical use scenarios of anonymous communication which provides sender anonymity and receiver anonymity in a communication. As methods for providing anonymous communication on the Internet theoretically, we describe our developing anonymous communication system in addition to three anonymous communication systems Onion Routing, Crowds, and 3-Mode Net. We also consider several issues which we have to resolve in order to provide services with anonymity on the Internet actually. Furthermore, we illustrate how services with anonymity are considered when anonymous communication systems are used.

Key words

Anonymous Communication, Privacy, Anonymity, Internet

1．はじめに

近年のパソコン・携帯電話やインターネットの急速な普及により，インターネット上では便利なサービスや新しいコミュニケーションツールが登場している．例えば，Amazon に代表されるネットショッピングを用いることにより，外出することなく欲しい商品を購入することができ，ソーシャル・ネットワーキング・サービス（SNS）などのコミュニケーションツールを使うことにより，気軽に世界中の誰とでもコミュニケーションをとることが可能である．これらの新しいサービスやツールは登場するたびに人々の今までの生活を塗り替え，日常生活に日々浸透してきている．

しかしながら，こうした便利なサービスが増加した半面，インターネット上では，セキュリティの問題が多々現れてきている．インターネットは，基本的に公開されたネットワークであり，不特定多数の人がアクセスすることができるため，簡単にインターネット上の通信を盗聴・改ざんすることが可能である．そのため，インターネット上で通信を行う際の問題として，氏名や住所，クレジット番号などの個人入力が必要となるオンラインショッピングなどのような通信内容の秘匿が求められるサービスや，電子

投票や医療相談などのような通信内容の秘匿だけでなく，誰と誰が通信しているかを秘匿することが要求されるサービスをどのように実現するかが課題となっている．氏名や住所などの重要なデータを通信する際は，Secure Socket Layer（SSL）などのセキュリティ技術を用いることにより，安全に通信を行うことが可能である．しかしながら，通信において高い匿名性が要求されるサービスを実現する場合，SSL などの既存の通信内容を保護するセキュリティ技術では対応できず，誰と誰が通信を行っているかを秘匿する技術を新たに構築する必要がある．

以上の背景から，現在まで様々な送受信者の匿名性を有する通信システムが開発されてきている．古くは 1981 年に提案された Mix-Net [1] から匿名通信方式の開発が進められており，現在まで Onion Routing [2] や Crowds [3] を筆頭に Tor [4]，Freenet [5]，Hordes [6]，Herbivore [7]，AP3 [8]，Valkyrie [9]，Slice Onion [10]，3-Mode Net [11] など様々な方式が提案されている．

しかしながら，匿名通信方式自体の確立やその解析といった理論面は研究が進められているが，実際に匿名通信システムとして実用化されたアプリケーションの数は少ない．これは，誰と誰が通信しているかわからないために悪用される恐れがあること，不正利用されないために匿名認証方式（匿名のままで正規の利用者かどうか確認できる認証方式）など別の枠組みを新たに構築する必要があることから，匿名通信方式単独では実用化しにくいことが考えられる．また，電子投票などの明らかに匿名性が必要となる特殊な場合を除くと，一般の人々がインターネットを使う上で匿名性を必要とするシナリオが少ないために開発されないことも考えられる．

そこで本稿では，我々が開発中の匿名通信システム [12] を紹介するとともに，これからの技術的課題および今後インターネット上で匿名通信システムが普及するためにはどのようなシナリオが考えられるかを検討する．

2．インターネット上で匿名性を有する通信方式の実現手法

インターネット上で通信の送受信者双方の匿名性を確保する最も簡単な方法は，信頼ある第三者を中継して通信を行う方法である．例えば，インターネットでオークションを行う際，基本的にお互いは見知らぬ相手となるため，自身の情報を開示したくない場合がある（オークションの出品者は，代金納入のための銀行の口座番号を教える必要があり，落札者は落札物を受け取るために，自身の住所を教える必要があるが，これらの情報は，見知らぬ相手に気軽に教えられるものではない）．そのため，お互いの個人情報を相手に開示する代わりに，信頼ある第三者（オークションを提供する業者・配送業者）に情報を開示し，その第三者を仲介することにより，出品者と落札者はお互いの情報を知ることなく取引が可能となる．

しかしながら，信頼ある第三者を用いることの大きな問題点は次のとおりである．

- 信頼することができる第三者を用意する必要がある．
- 信頼ある第三者には送受信者双方の情報がわかる．

インターネット上ではお互いに見知らぬ相手であるため，仲介する第三者も見知らぬ場合が多々あり，第三者をどのようにして信頼するかが難しい．さらに，信頼ある第三者には全ての情報が提供されるため，その第三者は全てを知ることが可能になり，第三者に対して匿名性が保たれないという欠点がある．

そこで，インターネット上で送受信者を秘匿可能な通信（匿名通信）を実現するためには，

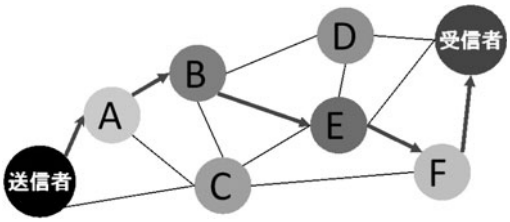

図１　中継のノードを用いた匿名通信の実現方法

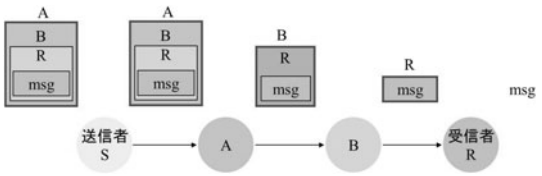

図２　Onion Routing の動作例

信頼ある第三者を仲介するのではなく，複数の第三者（ノード）を中継することにより，匿名性を提供する方法が一般的である．例えば，ある送信者がメッセージを受信者に送る際に，図１のようにノードＡ，ノードＢ，ノードＥ，ノードＦを中継して送信者から受信者にメッセージが送られる場合を考える．この時，メッセージの受信者からすると，メッセージはノードＦから送られているように見えるため，送信者の匿名性が保たれていると言える．

また，中継ノードＢからすると，ノードＡより以前の経路がわからないため，ノードＡが送信者であるかどうかも分からず，ノードＥに対しても，それ以降の経路がわからないため，ノードＥが受信者であるかどうかも分からない．そのため，第三者（送受信者以外のノードを指しており，ここでは中継ノード）に対して送受信者の匿名性を保つことが可能となる．

ノード中継により匿名通信を実現すためには，1）多重暗号化を用いた方式，2）中継ノードの確率的動作選択を用いた方式，3）ネットワークトポロジに環状路を用いた方式，の３つの手法が挙げられる．特に多重暗号化を用いた方式である Onion Routing [2]，中継ノードの確率的動作選択を用いた方式である Crowds [3] の２つの方式が有名である．本節では，この２つの方式に加え，我々が開発中の匿名通信方式の基本となる，多重暗号化と中継ノードの確率的動作選択の両方の方式を用いた 3-Mode Net（3MN）[11] について述べる．

2.1　Onion Routing の概要

本節では，図２を用いて Onion Routing の動作概要を示す．Onion Routing では，メッセージ送信者はまず，最終的な受信者までの経路情報をあらかじめ設定する．この時，図２では中継ノードとしてノードＡおよびノードＢが選ばれている．この場合，メッセージ送信者は次のようにしてメッセージの多重暗号化を行う．

(a)送信者は，受信者Ｒと Ｒの公開鍵によって暗号化されたメッセージから構成されるデータセットを作成する．

(b)次に，(a)で作成したデータセットをノードＢの公開鍵で暗号化し，そのデータと宛先Ｂからなるデータセットを作成する．

(c)最後に，(b)で作成したデータセットをノードＡの公開鍵で暗号化し，そのデータと宛先Ａからなるデータセットを作成する．

その後，(c)で作成したデータセットを中継ノードＡに送信する．Ａは受け取ったデータセットを復号化することにより，Ｂの暗号鍵で暗号化されたデータおよび次の宛先Ｂを知ることができる（つまり，(b)で作成したデータセットが復号化により得られる）．そのため，Ａは宛先Ｂにデータセットを送信する．ＢはＡと同様に，受け取った暗号化データの復号化することにより，(a)で作成したデータセットを得ることができ，次の宛先であるＲへ送信する．最終的に，

Rは受け取ったデータを復号化することにより，Sからのメッセージを得ることができる．

Onion Routingでは，中継ノードは前後の経路情報しかわからないため，送受信者双方の匿名性が提供可能である．しかしながら，全てのノードにおいて暗号化・復号化の処理があるため，中継ノードへの計算負荷がきわめて大きいという欠点がある．また，送信者が作成するデータセットには，メッセージだけではなく各中継ノードの情報が全て含まれているため，通信上に流れるデータサイズがメッセージだけの場合と比べて大きくなるという欠点も存在する．

2.2　Crowdsの概要

Crowdsでは，送信者Sはまず，受信者Rの宛先と暗号化されたメッセージから構成されるデータセットを作成する．その後，送信者Sは作成されたデータセットをCrowdsのネットワークに参加する自分以外のノードに送信する．データセットを受信したノードは，図3に示す通り，受信者Rに送信するか，受信者以外の別のノードに送信するかを確率に基づいて決定する．データセットの転送は，確率$1-q$で受信者以外のノードに中継される限り続けられ，ある中継ノードが確率qでデータセットを受信者に送信したときに，受信者はデータセットを復号化することにより，メッセージを得ることができる．

Crowdsにおいて，データセットを受信した中継ノードは，そのノード自身に送信してきた直前のノードが送信者であるのか，Crowdsのノードの一つであるのかを区別することができないため，送信者Sの匿名性を提供できる．また，暗号化はメッセージの暗号化にのみ必要であり，他に暗号化処理を必要としないため，中継ノードの計算負荷が小さいという利点も持つ．しかしながら，データセットの宛先は常に受信者Rを示しているため，受信者の匿名性が保持されないという問題がある．

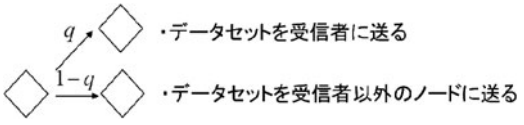

図3　Crowdsにおける中継ノードの行動

2.3　3-Mode Netの概要

3-Mode Net（3MN）は，図4に示す3つのモードを確率的に選択することにより，暗号化・復号化を繰り返しながら受信者までデータセットを転送する方式である．ここで，3MNにおけるデータセットは，次の宛先と多重暗号化されたデータセットから構成されるデータの集合である．

図4において，Decryptionモード（Dモード）では，ノードはデータセットを直接指定された宛先に送信する．転送後，データセットを受信したノードは復号化を行い，新たなデータセットを生成する．

Transmissionモード（Tモード）では，ノードはデータセットの宛先とは異なる宛先にデータセットを転送する．

最後に，Encryptionモード（Eモード）では，ノードは次の3つの動作を行う：まず，データセットを宛先以外のノードの暗号化鍵で暗号化

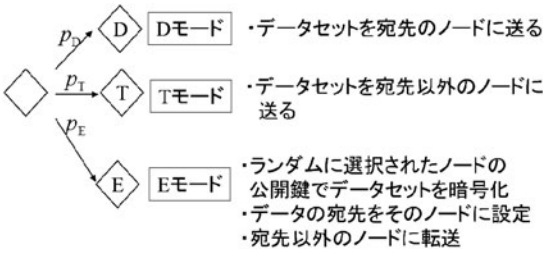

図4　3-Mode Netにおける中継ノードの行動

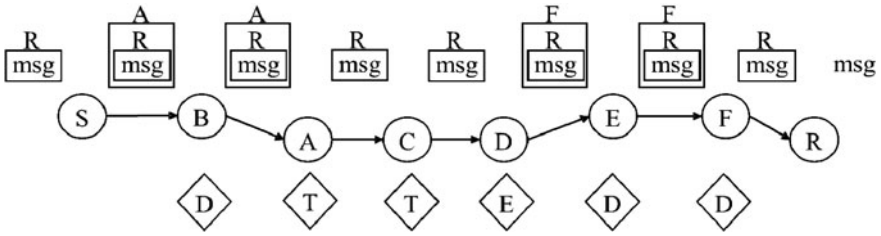

図５　3-Mode Net の動作例

し，新しいデータを作成する；次に，作成されたデータの宛先としてその選択されたノードを設定し，データセットを作成する；最後に，選択されたノード以外のノードにデータセットを転送する．

Ｅモードにより宛先の異なるデータセットが作成されるため，中継ノードはデータセットの宛先が最終的な受信者か，もしくは単なる中継ノードの一つなのかどうか判別することができない．これにより，3MN では受信者の秘匿が可能となる．これは Crowds との大きな違いである．また，中継ノードは直前のノードがメッセージの送信者かどうかも判別することもできないため，送信者の秘匿も可能である．

次に，図５に 3MN におけるデータセットの転送例を示す．ここで，図５における長方形内のデータは，暗号化されていることを意味し，長方形の上にある文字は次の宛先を表し，菱形内の文字については，選択されたモードを表す．

図５からも分かる通り，データセットの宛先には受信者Ｒだけではなくノード A およびノードＦも宛先として使われているため，メッセージの受信者Ｒを一意に決定することができない．また，通信の経路上には，送信者Ｓ以外に中継ノードが複数現れているため（A，B，C，D，E，F），送信者Ｓを特定することもできない．最終的にデータセットは受信者Ｒに届けられているため，送信者Ｓは 3MN を用いることにより，第三者に送受信者双方の情報を提供することなく，かつ受信者に対しては送信者の情報を伝えることなくメッセージを届けることができる．

さらに，図５では暗号化処理が３回（送信者Ｓのメッセージの暗号化で２回，ノードＤにおけるＥモードの選択による暗号化の１回），復号化処理が３回（データセットの宛先であるノード A，ノードＦ，および受信者Ｒにおける復号化がそれぞれ１回）行われているが，全てのノードで暗号化・復号化を行っているわけではない．そのため，全てのノードで暗号化・復号化処理が要求される Onion Routing よりも中継ノードへの計算負荷が小さいという利点も持つ．

しかしながら，3MN にもいくつか欠点が存在する．例えば，3MN を Crowds と比較した場合，3MN は受信者の匿名性が保証されているという大きな利点があるが，3MN には多重暗号化の仕組みが存在するため，Crowds よりも中継ノードの計算負荷が大きいという欠点も持つ．

また，Ｅモードが選択された場合に作成されるデータセットは新しい宛先を追加するため，受信したデータセットよりもデータサイズが大きくなり，送信するデータサイズは一定ではない．そのため，受信者Ｒの宛先と暗号化されたメッセージから構成される Crowds と比較すると，3MN のネットワーク上に流れるデータサイズが大きくなり，ネットワークへの負荷が大きいという問題がある．

3．多重暗号化を用いない匿名通信方式の実現手法

第 2 節では，代表的な 2 つの匿名通信方式 Onion Routing と Crowds，および Onion Routing と Crowds の両方の特徴を持つ 3MN について，それぞれの概要を述べた．各方式の課題として，Crowds では，受信者の匿名性が保持されないという問題点，Onion Routing と 3MN では，多重暗号化の仕組みがあるために，中継ノードの計算負荷やネットワークへの負荷が大きくなるという問題点がある．Onion Routing や 3MN のように多重暗号化の仕組みを導入した場合，中継ノードへの計算負荷やネットワークへの負荷の増大は避けられない．そこで本節では，多重暗号化を使わずに送受信者の秘匿が可能な匿名通信方式手法 [12] について述べる．提案手法では，Crowds を基本にし，中継ノードの確率的動作選択のみを用いて匿名通信路を実現する．

3MN では Crowds に多重暗号化の枠組み（図 4 における E モード）を導入することにより，データセットの宛先が常に受信者と一致しない状況を作り出している．そのため，多重暗号化を用いずにデータセットの宛先が変化する枠組みを導入する必要があり，そのための準備として，次節ではまず List と呼ばれる概念について説明する．

3.1　List の導入

一般のルータや中継サーバを考慮した場合，これらはログといった，特定の送信 / 受信記録を持つことが可能である．そのため，本節では List と呼ばれる記録を定義する．

List とは，データセット内の暗号化されたメッセージのハッシュ値とそのデータセットに記されている宛先を一組として記録した集合である．ここで，データセットは，Crowds と同様，暗号化されたメッセージとその宛先から構成される．例えば，あるノードがノード A を宛先としたデータセットを受信し，List に記録する場合，データセット内の暗号化されたメッセージのハッシュ値と A のアドレスを一組として記入する．

Onion Routing や Crowds では返信を可能にするため，各中継ノードは送信時において，前後のノードを記録している．また，分散ハッシュテーブル（Distributed Hash Table, DHT）[1] を用いた匿名通信方式も提案されている [13]．そのため，上記の List のようなデータの記録を用いることは一般的である．

本手法では，各ノードは，自身の List を所有していると仮定する．

3.2　ループバックを用いた匿名通信方式における中継ノードの動作選択

提案手法は，3MN と同じく 3 つのモードを持ち，それぞれ S モード，R モード，L モードから構成される．提案手法における選択モードの構成図を図 6 に示す．各中継ノードは確率に応じて上記の 3 つのモードの中から 1 つのモードを選択する．

図 6 において，第 1 のモードでは，ノードはデータセットを直接指定された宛先に送信する．このモードは，直接宛先に転送するモードであるため，Straight モード（S モード）と呼ぶ．

第 2 のモードでは，ノードはデータセットの宛先とは異なる宛先にデータセットを転送する．このモードは，他の宛先にデータセットを転送するため，Relay モード（R モード）と呼ぶ．

第 3 のモードでは，中継ノードは次の 3 つの動作を行う：まず，データセットに指定されているノードの宛先とそのデータセット内の暗号化されたメッセージのハッシュ値を一組として List に記入する；次に，データセットの宛先を

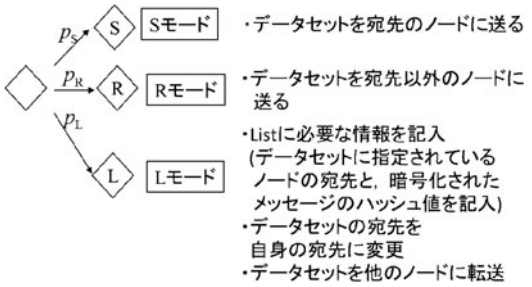

図6　ループバックを用いた方式における中継ノードの行動

自ノードの宛先に変更する；最後に，データセットを他ノードに転送する．このモードが選択された場合，データセットの宛先は自ノードに変更されるため，最終的に自分自身に対してデータを転送する，つまりループバックの動作を行うことになる．そのため，このモードをLoopbackモード（Lモード）と呼ぶ．

3番目のLモードにより，データセットの宛先が変更されるため，中継ノードはデータセットの宛先が最終的な受信者かどうか判別することができない．そのため，3MNと同様，提案手法では受信者の秘匿が可能である．また，2番目のRモードにより，データセットはメッセージの受信者とは異なる宛先に転送されているため，中継ノードは直前のノードがメッセージの送信者かどうか判別することもできない．そのため，CrowdsやMNと同様，送信者の秘匿も可能である．

提案手法は，多重暗号化を用いずにデータセットの宛先が常に受信者とならない仕組みに変更しているだけであるため，3つのモードから確率に基づいて中継ノードの動作を決定する枠組み自体に変化はない．そのため，匿名性に関しては，提案手法は3MNと同様であるが，図6に示す通り，提案手法には，暗号化・復号化処理を含むモードは存在しない．これは，3MNとは大きく異なる点である．そのため，提案手法ではCrowdsと同様，中継ノードの計算負荷が小さく，かつ通信時間として中継ノード数のみを考慮すれば良いこともわかる．

また，各データセットは常に暗号化されたメッセージと宛先から構成されるため，Crowdsと同じデータサイズとなり，3MNやOnion Routingよりもデータサイズが小さくなり，ネットワークへの負荷が小さいという利点も持つ．

3.3　ループバックを用いた匿名通信方式における動作例

本節では，図7を用いて提案手法における各ノードの送信動作を示す．ここで，図7における長方形内のデータは，暗号化されたメッセージを表す．また，長方形の上にある文字は次の宛先を表す．菱形内の文字については，選択されたモードを表す．以降，これら2つのデータからなる集合をデータセットと呼ぶ．

データセット$\mathrm{R} \| K_{\mathrm{R}}(\mathrm{msg})$を作成した送信者Sは，そのデータセットをランダムに選択されたノードAへ転送する．ただし，$\|$はデータの連結を表す．ノードAは宛先が自ノードでないことを確認した後，3つのモードのうち1つを選択する．図7の場合，ノードAはLモードを選択している．この場合，ノードAは自身のListに暗号化されたメッセージ$K_{\mathrm{R}}(\mathrm{msg})$のハッシュ値と宛先Rを記入した後，データセットの宛先を自ノードであるAのアドレスに書き換え，新しいデータセット$\mathrm{A} \| K_{\mathrm{R}}(\mathrm{msg})$を作成する．その後，他のノードBにそのデータセットを転送する．ノードBはデータセットを受信した後，データセットの宛先が自ノードではないことを確認した後，3つのモードのうちの1つを選択する．図7の場合，ノードBはRモードを選択している．この場合，ノードBは他のノードCにデータセットを転送する．ノードCはデータセットを受信した後，データセット

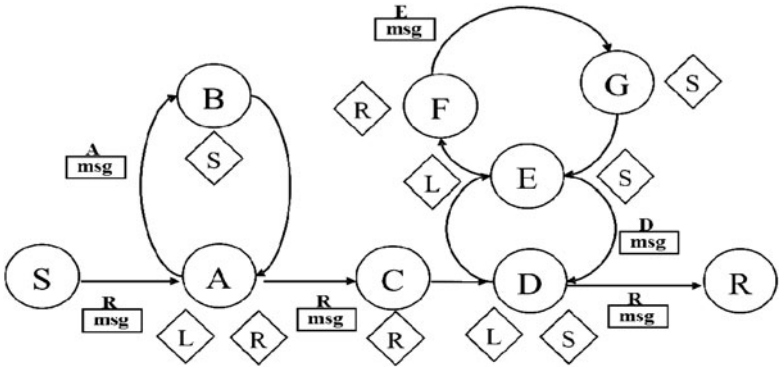

図7　ループバックを用いた方式における動作例

の宛先が自ノードではないことを確認し，Sモードを選択している．この場合，ノードCはデータセットの宛先であるノードAにデータセットを転送する．ノードAはデータセットを受信した後，データセットA ‖ K_R（msg）の宛先が自ノードであるため，受信したデータ内にある暗号化されたメッセージ K_R（msg）のハッシュ値とListのハッシュ値を照合し，データセットの宛先をノードRに変更する．その後，3つのモードのうちの1つのモードを選択・実行する．以降，このようなデータセットのノードの置き換えと転送を繰り返しながら，データセットは最終的に受信者Rへと転送される．受信者Rは宛先が自ノードであるため，データセットR ‖ K_R（msg）を復号化することにより，メッセージmsgを復号化する．これにより，メッセージの送信が完了する．

4．匿名通信方式における技術的課題

前節では，多重暗号化を用いない，送受信者双方の匿名性が保たれる匿名通信方式として，ループバックを用いた匿名通信方式の概要を述べた．ループバックを用いた方式の重要な特徴の一つとしては，中継ノードは3MNと同様に，3つのモードから1つのモードを確率に基づいて自身の動作を決定している点である．そのため，3MNの解析手法を応用することにより，送受信者双方の匿名性の度合いや送信者から受信者へ届くまでの中継ノード数が理論的に評価可能となる[12]．そこで本節では，提案方式における評価以外の残りの技術的課題を考察する．

4.1　返信方法の確立

匿名通信を用いることにより，送受信者を特定することができなくなるため，メッセージの受信者も，第三者である中継ノードと同様，メッセージの送信者が誰なのか知ることはできない．そのため，送信者への返信が必要となる場合，受信者は送信者がわからない状態で返信を行うことになる．提案手法における単純な返信方法としては，次の2つが考えられる．

(a)中継ノードは送信時の経路（前後の中継ノード）を記憶し，返信時には送信時の経路を遡る．

(b)存在する中継ノード全てに返信の情報を送る（マルチキャスト）．

実際にOnion RoutingやCrowdsでは(a)の方法により返信を可能としている．しかしながら，(a)の方法では，送信時の経路に現れた中継ノードが一つでも離脱した場合は返信ができない（ネットワークの動的変化にロバストではない）点，(b)の方法では，全ノードに送信が必要となるた

め，ネットワークへの負荷が大きすぎるという問題がそれぞれある．

また，全く別の方法として，多重暗号化を用いて返信時の経路をあらかじめ複数決定し，そのうちの一つを用いて返信する手法も考えられる．しかしながら，提案手法ではOnion Routingのように，あらかじめ経路が決められているわけではなく，手法(a)と同様，あらかじめ経路を決定するため，ネットワークの動的変化に弱いという欠点もある．

そのため，ネットワークの動的変化に強く，かつネットワークへの負荷も小さい返信手法を確立することが求められる．

4.2 匿名通信と匿名認証・匿名署名を両立した方式の確立

匿名通信方式を用いることにより，送受信者の秘匿は可能となるが，医療相談や電子投票などの特定の状況下では，なりすましや通信内容の改ざんを防ぐために，送受信者を秘匿したまま，送信者およびメッセージが正しいかどうかを判別する必要がある．なりすましや改ざんを防ぐための解決策として，それぞれ以下の技術が必要となる．

- 匿名認証方式
  匿名認証方式とは，送信者を特定できなくとも，その送信者が正しい権利（サービスを受ける権利）をもっているかどうかの判別が可能な認証方式である．
- 匿名署名方式（グループ署名方式）
  匿名署名方式とは，あるグループの誰かが署名したことはわかるが，その中の誰が署名したか特定することができない署名方式である．

匿名認証方式および匿名署名方式については，現在まで複数の方式が提案されているが[14][15]，これらの方式は，一般に匿名通信方式と関連付けて開発がなされておらず，独立した方式になっている．そのため，匿名通信方式と匿名認証・署名方式が必要となるサービスを提供する場合，それぞれの枠組みを導入する必要がある．その上，実際のシステムを組む際には両者の特性を考慮する必要があり，例えば匿名認証方式や匿名署名方式により提供される送信者の匿名性が，匿名通信方式による提供される匿名性よりも低い場合には，高い匿名性を提供する匿名通信方式を用いても意味をなさなくなる．

そのため，ループバックを用いた匿名通信方式の枠組みを考慮した匿名認証方式・匿名署名方式を開発する必要がある．

4.3 不正利用者に対するトレーサビリティ（追跡性）の確保

第2節で述べたとおり，匿名通信方式は一般に複数のノードを中継することにより，送受信者双方の匿名性を高める方式である．そのため，中継ノードの数が多いほど匿名性は高くなるが，不正者への追跡は，通信経路における中継ノードが増加しているため，より困難になる．

不正者追跡を行うためには，一般に各中継ノードが通信ログを取り，一定期間そのログを保存する必要がある．しかしながら，いつそのログが必要になるかわからないため，不正者の追跡を重視し，全ての通信のログを長期間残すことは，ノードへの負担を考慮すると，あまり現実的とは言えない．

また，閾値暗号方式[2)]を導入することにより，匿名性と不正者追跡を両立した通信方式[16]が提案されているが，中継ノード以外に不正者追跡を行うための複数の第三者機関（第2節で述べた，信頼ある第三者のことであり，オークションの例では，システムのサービス提供者などが当てはまる）が必要となる問題がある．そのため，ログの長期管理や第三者機関を必要とせ

ず，匿名通信方式の参加者のみで追跡可能な方式の確立が望まれる．

匿名通信システムの実用化に当たって，不正利用者追跡のための仕組みについては，どのような形であっても必ず実装しなければならないと考えられる．例えば，第5節でも言及するが，実際にインターネット上で使われている匿名通信システムである Tor [4] では不正利用者の追跡に対する対策は行っていない（理由は様々あるが，匿名性が低下する点，Tor 自体が悪用に不向きな点などが挙げられている）[17]．しかしながら，2010 年に発生した警視庁の国際テロ情報流出事件では実際に Tor が使われたため，追跡が困難であったといわれており，Tor を含め匿名通信が実際に犯罪に悪用されるケースが散見される [18] [19]．そのため，悪用されない枠組みの中で匿名通信システムを構築するか，悪用されたとしても，すぐに不正者が特定可能な仕組みを導入する必要がある．

5．インターネット上で匿名性を有するサービスの実現に向けての考察

第 1 節で述べたとおり，匿名通信方式は理論的には研究が進んでいるが，実用化はあまり進んでいない現状がある．そこで本節では，まず匿名性におけるメリット・デメリットを整理し，その後どのような匿名性を利用したサービスが必要となるかを考察する．

5.1　匿名のメリット・デメリット

一般に，匿名であることのメリット・デメリットは表裏一体の関係であることが多い．例えば，匿名性であることのメリットは次が挙げられる．

- 個人が特定されないため，個人のプライバシーが守られる．
- 誰でも平等に扱われるため，自由な発言・行動ができる．

反対に，それらのメリットに対応するデメリットとしては次の通りである．

- 個人が特定されないため，悪事や犯罪行為に使われるという恐れがある．
- 自由な発言・行動ができるために，ネット上での自身の発言・行動に責任が持てなくなり，誹謗中傷や迷惑行為が増える可能性がある．

そのため，高い匿名性を実現すればするほど，プライバシーが守られ，自由な行動が行える半面，悪事に使用され，誹謗中傷が増える可能性があることを常に考慮する必要がる．

5.2　想定されるシナリオ

匿名通信方式を実装することにより匿名性を有するサービスを実現する際には，匿名性であることのメリット・デメリットが両方含まれることを意識する必要がある．そのため，現実にインターネット上で匿名性を有する通信やサービスを提供する場合，匿名性がもたらすデメリットへの対策を行わなければならない．反対に対策を行わない場合，匿名通信を利用するユーザのマナー・道徳に依存してしまうため，場合によっては，デメリットがメリットよりも大きくなる可能性がある．

例えば，ファイルの不特定多数での共有を目的としたファイル共有ソフトがあるが，その特性上，もともと著作権侵害の温床になる可能性を秘めているソフトである．その上で，何も著作権侵害の対策をせず，匿名通信の原理を用いて匿名性を有するファイル共有ソフトを開発した場合，Winny [20] に代表されるように，身元が特定されないために一層著作権侵害が横行する可能性が高くなる．

また，実際に Onion Routing を実用化したシステムとして Tor [4] があるが，Tor では特定の

ソフトに対して匿名性を提供するのではなく，インターネット上の通信パケットの匿名化を提供する．そのため，インターネット通信を必要とする様々なサービスやソフトに対して匿名性を付与することが可能であるが，利用方法によっては悪事や誹謗中傷に利用することも可能である．実際，未然に悪用や迷惑行為を防ぐために，Wikipedia [21] などのオンライン電子百科や2ちゃんねる [22] に代表される電子掲示板では，Tor からのアクセス（主に書き込み）を禁止している．

以上から，匿名通信方式のみを実現した場合，悪用に使われる可能性が増加し，必要なサービスも受けられない可能性もある．また，デメリットの一つである誹謗中傷や迷惑行為にさらされるという行為は，インターネットの一般利用者から見ると，大きな脅威である．そのため，インターネット上で匿名性を提供する際には，匿名通信方式を実現するだけでなく，4.3 節で述べた不正利用者の追跡性も確保し，さらに必要とあれば，4.2 節で述べた匿名署名方式・匿名認証方式も同時に確立する必要がある．

最後に，インターネット上で使われるサービスに対して匿名性が提供され，かつ匿名によるメリットのみが受けられる場合，どのような利用方法が可能であるかを検討する．

(1) メールサービスの匿名化

メールで相手と通信を行う際，相手には自身が使用するメールアドレスが伝えられる．そのため，相手は与えられたメールアドレスから，自身の情報を調べることが可能であるため，自身の情報を完全に隠すことはできない．

匿名メールサービスを実現した場合，誰が送信者なのか隠すことが可能であるため，主に送信者のプライバシーが要求される内部告発や医療相談への適用が想定される．反対に，迷惑メールなどの不正行為・迷惑行為に利用される可能性が非常に高くなるが，不正者追跡が可能である場合，迷惑行為を行った者に対して摘発することが可能となる．

(2) 電子掲示板・SNS・チャットの匿名化

インターネット上で不特定多数のユーザとコミュニケーションをとる場合，掲示板や SNS，チャットが用いられることが多い．これらのサービスでは，ある一定のテーマに興味を持った複数のユーザもしくは知り合い同士が集まり，情報交換や議論などが行われる．

現在まで，実名，仮名（ハンドルネーム），匿名の電子掲示板・SNS・チャットが提供されている．例えば，匿名掲示板に代表される 2 ちゃんねる [22] では，匿名性のメリットを活用し，参加者全員が平等な立場から自由な議論が行われているが，反対にデメリットである，誹謗中傷や迷惑行為もまた多く見受けられる．

匿名通信を導入した場合，完全な匿名性が提供されるため，現在の匿名サービスと同等以上のサービスが提供可能であるが，それ以上に誹謗中傷や迷惑行為が増加すると予想される．

これらの対策については，誹謗中傷や迷惑行為を行ったユーザに対しては，不正利用者と判断し，追跡し特定することにより，対処可能である．また，誹謗中傷などを未然に防ぐために，あるグループに登録したユーザ以外は参加することができないといった処置も考えられる．この場合，匿名通信と併用して匿名認証を用いることが考えられる．匿名認証により，そのグループ内のユーザであることはわかるが，グループの誰であるかは特定されないため，匿名性を維持したまま，グループ内のユーザだけでコミュニケーションをとることが可能となる．

(3) オンラインショッピング・オークションの匿名化

実際に，ある店舗で商品を購入する際，店舗側には誰が購入したかはわからないことが一般である．紙幣には名前は存在せず，相手側と顔見知りでない限り，“誰が”“何を”購入したかは伝わらない．しかしながら，インターネット上で，あるサイトから商品を購入する際には，通常は ID とパスワードを用いて本人認証を行うために，匿名性が確保されることはない．自身の購入したものを含め，名前や住所などの個人情報をサイト側が全て管理することは，漏洩の危険性やサイト側の保守の手間を考えるとよい手法とはいえない．

匿名通信を用いることにより，商品の購入やオークションの取引自体は匿名で可能となるが，問題となるのは支払い方法および購入・落札商品の受け取り方法である．

支払い方法については，現金を使うことはできず，銀行振り込みやクレジットカードの利用も個人情報が含まれるため用いることができないが，あらかじめ個人情報が不要な WebMoney [23] と呼ばれる電子マネーを購入することにより，対応可能である．

また，商品の受け取り方法については，音楽データの購入などのデータファイルのやり取りのみの場合は，匿名通信を用いることにより，匿名性を確保できるが，形のある商品を受け取る場合は，どこで受け取るかが問題となる．この問題については，コンビニエンスストアなどの購入者・落札者自身とは関係のない場所で受け取ることにより，相手側に住所・氏名を教えることなく可能であると考えられる．

6．終わりに

本稿では，インターネット上で匿名性を有するシステムを構築するためのいくつかの手法を述べた．具体的には，複数の中継ノードを介することにより匿名性を提供する手法として，Onion Routing，Crowds，3-Mode Net，我々が開発中のループバックを用いた手法について説明した．さらに，匿名通信システムがインターネットで普及するためには，今後どのような課題が存在するか考察し，また匿名ネットワークを用いて，ユーザにどのようなサービスが提供可能かを検討した．

今後の大きな課題の一つとしては，安全・安心が重要視される現代の中で，安全・安心に関するどのような問題に対して，匿名通信を適用していくべきか検討することが挙げられる．本稿では個人のプライバシー保護の観点から匿名通信を論じているが，他にどのような安全に関わる課題があり，匿名通信を使ってどのようなアプローチができるか考慮する必要がある．この問題については，匿名通信の一般への普及に関わる根本的な問題でもあるため，今後十分に精査する必要がある．

我々の目的は，匿名通信システムがインターネットの一つのツールとして世界中に普及されることにある．決して非匿名のサービスを否定しているわけではないが，インターネットが魅力的であるのは，やはり匿名によるメリットが大きいからである．そのため，そのインターネットの匿名性を補助する一つの手段として，匿名通信の技術が使われるために，匿名性のメリットのみを享受可能なシステムを今後構築していく必要がある．

謝　辞

本研究の一部は，文部科学省研究費補助金（研究活動スタート支援）によるものである．

注

1） いわゆる P2P（Peer to Peer）方式を実現するために用いられる技術の一つである．URL

を用いてサーバにアクセスする従来のクライアント・サーバモデルでは，端末数が多くなるとサーバへの負担が大きくなるという欠点があったが，P2Pでは，参加するノードに必要となる情報を分散させることにより，各ノードに負荷を分散させ，情報を持つノードに一極集中となる状況を避けることが可能となる．P2Pを実現するための課題の一つとして，P2Pネットワークに存在する膨大なノードの中から，必要とする情報を持つノードを素早く見つけ出す点が挙げられるが，DHTを用いることにより，特定のノードに負荷をかけることなく，素早くノードを検索することが可能となる．

2） 閾値暗号では，復号化に必要な秘密鍵は複数の鍵に分割され，それらは別々に管理される．名称のとおり，ある閾値が定められており，暗号化されたデータを復号化するためには，その閾値を超える数の分割された鍵が集められたときのみ，復号化が可能となる特徴を持つ．この特性を応用し，文献［16］では，複数の第三者機関がそれぞれ分割された鍵を管理しており，第三者機関が複数集められ，閾値を越える数の鍵が集められたときのみ，不正者の追跡が可能となる仕組みを構築している．

参考文献

［1］ D. Chaum（1981）. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*. Communications of the ACM, vol. 24, no. 2, pp. 84-88.

［2］ M. Reed, P. Syverson, and D. Goldschlag（1998）. *Anonymous Connections and Onion Routing*. IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 482-494.

［3］ M. Reiter and A. Rubin（1998）. C*rowds: Anonymity for Web Transactions*. ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92.

［4］ R. Dingledine, N. Mathewson, and P. Syverson（2004）. Tor: The Second-Generation Onion Router. Proc. 13th USENIX Security Symposium, pp. 303-320.

［5］ I. Clarke, O. Sandberg, B. Wiley, and T. Hong（2000）. *Freenet: A Distributed Anonymous Information Storage and Retrieval System*. Proc. International Workshop on Design Issues in Anonymity and Unobservability, pp.46-66.

［6］ B. Levine and C. Shields（2002）. *Hordes: A Multicast Based Protocol for Anonymity*. ACM Journal of Computer Society, vol.10, no.3, pp.213-240.

［7］ S. Goel, M. Robson, M. Polte, and E. Sirer（2003）. *Herbivore: A Scalable and Efficient Protocol for Anonymous Communication*. Cornell University Computing and Information Science, Technical Report 2003-1890, 17 pages.

［8］ A. Mislove, G. Oberoi, A. Post, C. Reis, P. Druschel, and D. S. Wallach（2004）. *AP3: Cooperative, Decentralized Anonymous Communication*. Proc. 11th Workshop on ACM SIGOPS European Workshop, 6 pages.

［9］ 山中晋爾，古原和邦，今井秀樹（2005）. Valkyrie：非静的ネットワークに適応可能な匿名通信方式　情報処理学会論文誌　vol.46 no.8　pp.2025-2035.

［10］ 田村仁，古原和邦，今井秀樹（2007）. 動的ネットワークにおける双方向匿名通信路構築手法の提案　情報処理学会論文誌　vol.48　no.2 pp.494-504.

［11］ 三宅直貴，伊藤義道，馬場口登（2008）. 多重暗号化と確率的動作選択に基づく双方向通信可能な匿名通信方式：3-ModeNet　電子情報通信学会論文誌A　vol. J91-A no.10 pp. 949-956.

［12］ 河野和宏，伊藤義道，馬場口登（2010）. 多重ループバックを用いたCrowds型匿名通信方式　2010年暗号と情報セキュリティシンポジウム（SCIS 2010）6 pages.

［13］ 近藤正基，齋藤彰一，松尾啓志（2008）. DHTを用いた双方向匿名通信路の提案　電子情報通信学会技術研究報告　ISEC2008-43　pp. 61-68.

［14］ 中村徹，稲永俊介，池田大輔，馬場謙介，安浦寛人（2009）. PIRに基づく匿名認証とその応用　コンピュータセキュリティシンポジウム2009（CSS2009）pp.571-576.

［15］ 一色寿幸，尾花賢，佐古和恵（2010）. 複数人

のオープナーを指定可能なグループ署名方式 2010 年暗号と情報セキュリティシンポジウム（SCIS2010）6 pages.
［16］千田浩司，小宮輝之，林徹（2004）．匿名性確保と不正者追跡の両立が可能な通信方式　情報処理学会論文誌　vol. 45　no. 8　pp.1873–1880.
［17］http://rem.spline.de/tor/index.html.ja（2011 年 2 月 17 日確認）
［18］http://www.asahi.com/digital/internei/TKY201101030295.html（2011 年 2 月 17 日確認）
［19］http://www.sankeibiz.jp/business/nene/110118/bsj1101181016004-n1.htm（2011 年 2 月 17 日確認）
［20］金子勇（2005）．Winny の技術　アスキー 201 pages.
［21］http://ja.wikipedia.org/（2011 年 2 月 17 日確認）
［22］http://www.2ch.net/（2011 年 2 月 17 日確認）
［23］http://www.webmoney.jp/（2011 年 2 月 17 日確認）

（掲載決定日：2011 年 2 月 14 日）