社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30（52）
2005／7／22

匿名通信路における配達証明配送手法

山中　晋爾†

†（株）東芝 研究開発センター　〒212-8582 川崎市幸区小向東芝町1
E-mail: †shinji1.yamanaka@toshiba.co.jp

あらまし　配達証明とは，ネットワーク上の二者が通信を行い，送信者から受信者に対してあるデータが送られた場合に，受信者に当該データが確かに届けられた，という事実を送信者に対して証明するものである．そして，匿名通信路とは，ネットワーク上の二者が通信を行う際に，第三者に対して誰と誰が通信しているかが特定できないような通信路を指す．このとき，信頼できる第三者機関が介在する場合や，受信者が信頼できる場合には，匿名通信路において配達証明の仕組みを実現することは容易だが，このような仮定を置かない場合に匿名通信路において配達証明を配送する手法は存在しない．本稿では，匿名通信路にける配達証明を実現する一方式を提案し，その匿名性やメッセージサイズについて考察を行う．

キーワード　匿名通信，オニオン・ルーティング，配達証明

New Construction of Anonymous Communication Scheme with Return Receipt

Shinji YAMANAKA†

† TOSHIBA Corporation　Toshibacho 1, Komukai, Saiwai-ku, Kawasaki-shi, 212-8582 Japan
E-mail: †shinji1.yamanaka@toshiba.co.jp

Abstract　Proof of delivery (or return receipt) is a certificate of reception on network transaction from message sender to message receiver. Anonymous communication system can hide ones action such as data transfer or communication on the network, which will protect privacy of the correspondents. These two properties, delivery certificate and anonymity, are very useful for online activity. However it is not easy to build a system which has both two properties without Trusted Third Party or without confidence of message receiver. We propose a new construction of such anonymous communication scheme with return recipient, and we consider the anonymity of our scheme and compare the message size of our scheme with that of Onion Routing scheme.

Key words　anonymous channel, onion routing, return receipt

1. まえがき

1.1 背　景

インターネットの普及に伴い，ネットワークを介した電子データの送付は，一般的な情報伝達手段となってきている．そして伝送される電子データの種類はテキスト・音声・静止画像・動画像など多岐にわたっており，その内容によってはデータ送信者，あるいはデータ受信者のプライバシに関わるものとなりうる．また，伝送内容のみならず，自分が誰と通信をしているかを秘匿したい状況もある．例えば，ある特有の持病を持っている人が，ネットワークを介してその特定分野の医療機関に相談をする場合に，第三者に対しては医療相談をしていることを知られたくないだろう．このような匿名性に関する問題の解決策としては，ミックスネットやオニオン・ルーティングなど匿名通信技術の利用があげられる．

一方，受信者が確かに情報を受け取ったということを，情報の送信者が確信したい（あるいは，証明したい）という場面も想定される．現実の世界で，例えば郵便においては，配達証明郵便を利用することで郵便物が配達された事実を証明することができる．具体的には，郵便局において配達証明を指定して発送を依頼すれば，差出人は，当該郵便物配達後に，配達証明書を受け取ることができる．そして，この配達証明書により，その手紙が受取人に配達されたことと配達の日付を証明することができる．また，インターネット上であっても電子メールの送受信においては，この配達証明の仕組みが実現されている．例えば信頼できるサーバを介する方法（ＩＢＭ社・ノーツメールの

「受信確認」機能，あるいはReturnReceipt(注1)など）や，メールクライアントソフトの機能を利用する方法（Microsoft社・Outlook(注2)の「開封確認」機能や，RimArts社・Becky(注3)の「開封確認」機能など）などがあげられる．

1.2 問題点

前述の2つの要求，すなわち送信者や受信者の匿名性の実現と配達証明の配送とを同時に満たす方式は，これまでに知られていない．ひとつの解決策としてまず，信頼できるサーバを介してデータを送信することで匿名性を維持することは，理論的には可能である．しかしながら，そのような仮定を置く（すなわち，信頼できるサーバが構成できると仮定する）ことは実現可能性の面で疑問が残る．また，データ受信者が信頼できる場合には，匿名通信技術を利用するだけで問題を解決することができる．すなわち，データ送信者は匿名通信路技術を用いてデータを送信し，受信者はメッセージを受け取った場合に匿名返信機能を利用して，配達証明をデータ送信者に返送することができる．

しかしながら，受信者がデータを受け取ったにもかかわらず「受信していない」と主張するような場合においては問題解決は単純ではない．なぜならば，匿名通信路を使用しているために送信者にとっては，受信者が本当に情報を受信していないのか，情報を受信しているにもかかわらず，偽証しているのかを確かめる術が存在しないのである．このように，信頼できるサーバを介すること無く，また受信者の信頼性に頼らずに，匿名性を維持しながら配達証明の配送を実現する方式は存在していない．

1.3 解決方法

本稿ではこの問題の解決方法を，「匿名通信路における配達証明配送手法」と定義し，これを実現する方法を提案する．提案方式では，既存の匿名通信方式の一つであるオニオン・ルーティング方式を改良することにより，問題の解決を図る．具体的には，(1) 全ての中継ノードは，メッセージ送信者に対して配達証明を送信する，(2) 配達証明の発信にも匿名通信を利用する，の2点により問題を解決する．(1) により，配達証明を送信した中継ノードは，自身の転送先ノードが受信者かどうかを特定できない．また，(2) により送信者が誰であるかを特定できなくなる．

2. 関連研究

本章では，提案方式に関連する匿名通信技術について示す．匿名通信における最初の論文は，D. Chaumにより1981年によって書かれた[1]．この論文において，Chaumはミックスネットという多重暗号化を利用した匿名通信方式を提案した．ミックスネット方式は，ネットワーク上に配置された複数のミックスサーバにより構成される．メッセージ送信者は，送信したいメッセージを各サーバの公開鍵を用いて多重に暗号化し，これを最初のミックスサーバに送信する．各サーバは入力された暗号文を複数個（あるいは一定時間）保持した後に，それを復号したうえでシャッフルしてから次のノードにその暗号文群を送信する．このような処理を行うことにより，あるノードにおける入力と出力の関係を断ち切ることが可能となり，結果として送信者と受信者のつながりを切ることができる．図1に，ミックスネットの動作の様子を表す．同図は，N個の入力（メッセージ）がM個のミックスサーバを通過して，受信者に届けられる状況を表している．

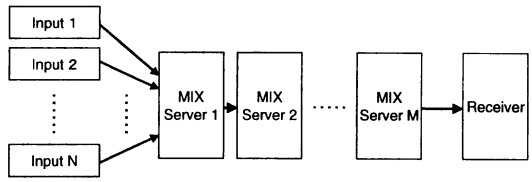


図1 Mix-netの概観

その後，ミックスネット方式を基本としていくつかの匿名通信方式が提案されてきた[6]が，その中でも即時性の高い通信を実現する方式として，オニオン・ルーティング方式がGoldschlagらよって提案された[4]．オニオン・ルーティング方式では，オニオン・ルータと呼ばれる複数の情報転送ノードをネットワーク上に配置する．そして，メッセージ送信者は、メッセージが複数のオニオン・ルーティングを経由するように経路を設定し、この経路情報（オニオン）にメッセージを含ませて発信する。一般的なオニオン・ルーティングの動作の様子を図2に示す．同図は，ネットワーク上に複数のオニオン・ルータが存在し，送信者1（Sender1）が受信者1（Receiver1）にメッセージを送信し，同様に送信者2（Sender2）が受信者2（Receiver2）にメッセージを送信している様子を表している．

オニオン・ルーティングの具体的な動作を説明する．まずメッセージ送信者は，何らかの仕組みを用いてネットワーク上に存在するオニオン・ルータのIDやアドレス，公開鍵等を入手する．続いて，メッセージ送信者は送信したいメッセージを，経由させるオニオン・ルータの公開鍵を用いて多重暗号化する．この際，メッセージを受信して暗号文を復号したルータが次にどのルータに転送したらよいかを指示するアドレス情報も埋め込むようにする．この様子を，図3に示す．同図において，Sはメッセージ送信者，Rはメッセージ受信者を意味する．また，A, B, Cはメッセージを中継するオニオン・ルータである．

送信者は，まずメッセージを受信者Rの公開鍵で暗号化し，これに宛先情報Rを結合した後に全体をCの公開鍵で暗号化する$(K_C(R||K_R(M)))$．そして，これに宛先情報Cを結合した後に全体をBの公開鍵で暗号化する$(K_B(C||K_C(R||K_R(M))))$．さらに，これに宛先情報Bを結合した後に全体をAの公開鍵で暗号化する$(K_A(B||K_B(C||K_C(R||K_R(M)))))$．メッセージ送信者は，このデータをオニオン・データパケットとして最初の転送ノードAに送信する．

オニオン・データパケットを受け取ったノードAは，自身の秘密鍵を用いてメッセージを復号する．ノードAは，オニオ

(注1)：http://www.returnreceipt.com/
(注2)：http://www.microsoft.com/japan/office/outlook/prodinfo/
(注3)：http://www.rimarts.co.jp/index-j.html

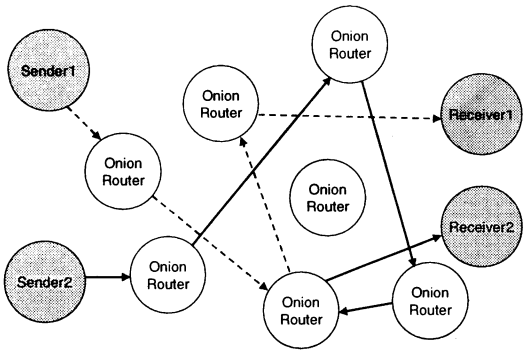
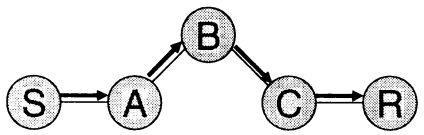


図 2　オニオン・ルーティングの概観

ン・データパケットの転送先がノード B であることを確認し，復号したデータ：$K_B(C||K_C(R||K_R(M)))$ をノード B に転送する．そして各ノードが同様の，「復号および転送」という処理を行うことにより，最終的には，メッセージ M が受信者 R に届けられる．

図 3 に示したようなデータ構造にすることにより，各中継ノードは自分の直前のノードと直後のノード以外に，メッセージ送信系路上にどのノードが存在するかを識別することができなくなる．すなわち，ノード B は，自分にメッセージを送ったノード A と自分がメッセージを転送するノード C の存在は確認できるが，ノード A より以前にどのノードが存在するか（この例ではノード S），ノード C より後ろにどのノードが存在するか（ノード R）を知ることができない．同様に，ノード A にとっては，ノード S が真の送信者かどうか識別することはできず，ノード C もノード R が真の受信者かどうかを識別することはできない．

そして他にも，第二世代オニオン・ルーティングである Tor [2] や Universal Re-Encryption を用いた方式 [3], [5] など様々な匿名通信方式が提案されてきている．しかしながら，これらの匿名通信方式では，信頼できない受信者がメッセージを受け取ったときに，わざと配達証明を送信者に対して返信しない場面を想定していない．これに対して提案方式では，送信者や受信者の匿名性を維持しつつ，受信者の信頼性に依存することなく，受信者にメッセージが届いたか否かを送信者が確認できる配達証明を，送信者に送ることが可能となる．



$$K_A(\, B \,||\, K_B(\, C \,||\, K_C(\, R \,||\, K_R(M))))$$

図 3　オニオン・ルーティングのデータ構造

3. 提案方式

本章では，提案方式の詳細を示す．初めに，提案方式が目的とする匿名性を示す．次に単純な解決策を示して問題点を提示した後に，提案方式の詳細について説明する．

3.1 仮定・定義・目的

仮定 1（攻撃者）：ネットワーク上において，2 種類の攻撃者を仮定する．一つは悪意のノードであり，もう一つはネットワーク盗聴者である．悪意のノードは，自分が受け取ったメッセージの中身を見ることはできるが，匿名通信方式のプロトコルには従うものとする．ネットワーク盗聴者は，ネットワーク上を流れるメッセージのヘッダを確認することにより、当該メッセージの送信者および受信者を調べることができるが，メッセージの改ざんや削除，再送攻撃は行わないものとする(注4)．また，攻撃者の計算能力は有限であり，適切なサイズの鍵長を用いることにより，暗号文の解読を不可能にできるものとする．

仮定 2（定常的なトラフィック）：ネットワーク上において，送信者 S と受信者 R 以外の誰も通信を行っていなければ，攻撃者は S と R が通信を行っていることを知ることが可能である．このため，ネットワーク上において，任意の二者のみが通信を行っていることを隠すことができる程度の、定常的なトラフィックが存在することを仮定する．

定義 1（匿名性）：ここで，ある通信方式において送信者の匿名性が保たれるとは，悪意のルータがメッセージを受け取って復号した際あるいはネットワーク盗聴者が経路上のメッセージを盗み見た際に，そのメッセージの送信者が誰であるかを有意な確率で特定できない状態を指す．また，ある通信方式において受信者の匿名性が保たれるとは，悪意のルータがメッセージを受け取って復号した際あるいはネットワーク盗聴者が経路上のメッセージを盗み見た際に，そのメッセージの受信者が誰であるかを有意な確率で特定できない状態を指す．

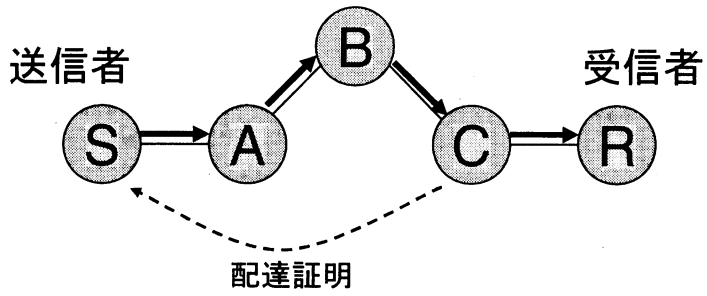
提案方式の目的は，前述の仮定 1・2 の条件において定義 1 の匿名性を保つことにある．

3.2 シンプルケース

まず，単純な解決策として，メッセージ受信者にメッセージを転送する最終中継者が，メッセージ送信者に配達証明を送信することを考える．この様子を図 4 に示す．

図 4 において，ノード S はメッセージ送信者，ノード R はメッセージ受信者である．またノード A,B,C は中継ノードである．まず，ノード S はノード C が復号する部分に，自分への宛先 S と，自分宛の配達証明 certToS を含ませておき，多重暗号化したメッセージを生成する．ノード A とノード B は，受け取ったメッセージを復号した後に，通常のオニオン・ルーティングと同様の処理を行い次ノードへと転送する．ノード C は，メッセージを復号してノード R にメッセージを送信した後に，ノード S に配達証明を送信する．

(注4)：実際にはメッセージの改ざんに対しては改ざん検知の機能を持たせればよく，再送攻撃に対しては re-encryption 方式などを用いてメッセージが毎回同一とならないようにすることで対抗できる



PkA(B || PkB(C || PkC(R || PkR(M) || S || CertToS)))

図 4　配達証明送信のための愚直な解決策

このような仕組みにすることで，受信者ノード R の信頼性によらずに，ノード S は配達証明を受け取ることが可能となる．しかしながら，この方式では送信者 S および受信者 R の匿名性を，最終中継ノード C に対して保つことができない．

3.3　提案プロトコル

本節では，提案方式についてその詳細を示す．前述の方式（シンプルケース）では，最終中継ノード C に対して匿名性が保たれていない点が問題であった．そして，最終中継ノードに対して匿名性を保つには，送信者 S の匿名性と受信者 R の匿名性が得られれば良いことがわかる．そして送信者の匿名性は，送信者に配達証明を送信する際に，匿名通信路を利用することで保つことが可能である．また，全ての中継ノードが配達証明を送信するプロトコルとすることで，受信者の匿名性を保つことが可能となる．この様子を図 5 に示す．

図 5 において，ノード S はメッセージ送信者，ノード R はメッセージ受信者である．またノード A,B,C,D,E,F,X,Y,Z は中継ノードである．送信者 S が，メッセージ中継ノードが発信する配達証明を配送するためのオニオン（配達証明オニオン）を作成して，通常のオニオン・ルーティングのデータパケットに含めることで，目的のプロトコルを実現することができる．

3.3.1　配達証明オニオンの作成

送信者 S は，まず中継ノード A が発信する配達証明オニオンを作成する．ノード A が送信者ノード S に対して発信する配達証明 $certA$ は，ノード A からノード X，ノード D，ノード S と転送されるものとする．まず，配達証明情報 $certA$ を送信者ノード S の公開鍵で暗号化し，$PK_S(certA)$ を生成する．これとノード S のアドレス情報を結合して，ノード D の公開鍵で暗号化し，$PK_D(S \parallel PK_S(certC))$ を生成する．さらにこれとノード D のアドレス情報を結合し，ノード X の公開鍵で暗号化して，$PK_X(D \parallel PK_D(S \parallel PK_S(certC)))$ を生成する．つまり，

$$CertA = PK_X(D \parallel PK_D(S \parallel PK_S(certA)))$$

が，ノード A の配達証明オニオンとなる．同様にして，ノード B およびノード C の配達証明オニオンを，次式で示す形で生成する．

$$CertB = PK_Y(E \parallel PK_E(S \parallel PK_S(certB))),$$

$$CertC = PK_Z(F \parallel PK_F(S \parallel PK_S(certC))).$$

次に送信者は，これらの配達証明オニオンを含む形でオニオン・ルーティングのデータパケットを作成する．メッセージ m を受信者ノード R の公開鍵 PK_R で暗号化し，受信者のアドレス R，配達証明の転送先アドレス Z および配達証明 $CertC$ と結合して，ノード C に対する平文 M_C を次に示す形式で生成する．

$$M_C = (Z \parallel CertC \parallel R \parallel PK_R(m)).$$

そして，この M_C をノード C の公開鍵 PK_C で暗号化し，ノード C のアドレス C，配達証明の送り先アドレス Y および配達証明情報 $CertB$ と結合して，ノード B に対する平文 M_B を次に示す形式で生成する．

$$M_B = (Y \parallel CertB \parallel C \parallel PK_C(M_C)).$$

同様にして，ノード A に対する平文 M_A を次に示す形式で生成する．

$$M_A = (X \parallel CertA \parallel B \parallel PK_B(M_B)).$$

そして，最後に M_A をノード A の公開鍵で暗号化してオニオンデータパケット $PK_A(M_A)$ を生成し，オニオン・データパケットが完成する．オニオンデータパケット全体の様子を図 6 に示す．この図において，X, D, S は，それぞれノード X，ノード D，そしてノード S のアドレス情報を意味する．そして，B, Y, E および，C, Z, F, R も，同様にそれぞれのノードのアドレス情報を意味する．ただし，図 6 において，多重暗号化やパディングについては省略してある．メッセージ送信者 S は，これをノード A に送信する．

3.3.2　メッセージの転送・配達証明の発信

$PK_A(M_A)$ を受け取ったノード A は，まずこれを自身の秘密鍵を用いて復号する．復号の結果ノード A は，メッセージの転送先情報 B および，ノード B に転送すべきメッセージ $PK_B(M_B)$，そして配達証明の転送先情報 X および，ノード X に転送すべき配達証明情報 $CertA$ を入手する．ノード A は

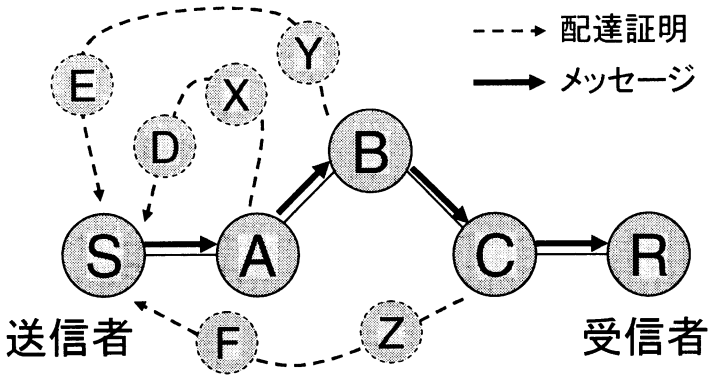


図 5　提案方式の概観

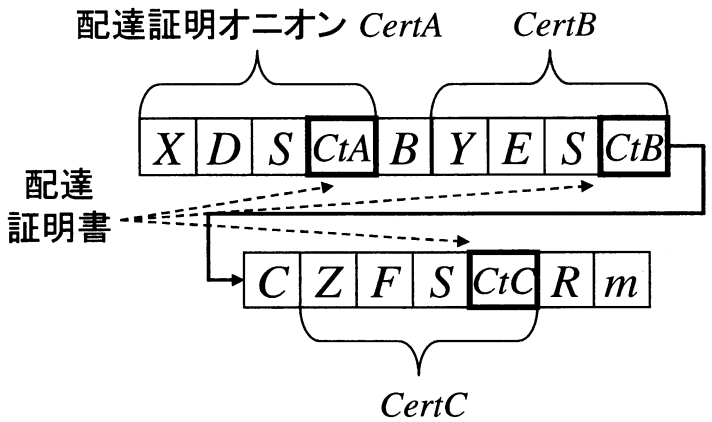


図 6　提案方式のオニオンデータパケットの構造

メッセージ $PK_B(M_B)$ に対して，必要に応じて復号前の暗号文と同じメッセージ長になるようにパディングを行う．そして，ノード A はメッセージ $PK_B(M_B)$ をノード B に転送した後に，配達証明情報 $CertA$ をノード X に発信する．

メッセージ $PK_B(M_B)$ を受信したノード B は，まず自身の秘密鍵を用いてこれを復号する．復号の結果ノード B は，メッセージの転送先情報 C および，ノード C に転送すべきメッセージ $PK_C(M_C)$，そして配達証明の転送先情報 Y および，ノード Y に転送すべき配達証明情報 $CertB$ を入手する．ノード B はメッセージ $PK_C(M_C)$ に対して，必要に応じて復号前の暗号文と同じメッセージ長になるようにパディングを行う．そして，ノード B はメッセージ $PK_C(M_C)$ をノード C に転送した後に，配達証明情報 $CertB$ をノード Y に発信する．ノード C も同様の処理を行い，メッセージ $PK_R(m)$ をノード R に転送した後に，配達証明情報 $CertC$ をノード Z に発信する．

一方，配達証明オニオンを受け取ったノード X は，通常のオニオン・ルーティングと同様の処理を行う．すなわち，受け取ったメッセージを復号し，転送先がノード D であることを確認した上で，暗号文 $PK_D(S \parallel PK_S(certA))$ をノード D に転送する．ノード Y，ノード Z も同様の処理を行う．この結果，送信者 S はメッセージが B まで転送された場合には $certA$ を，メッセージが C まで転送された場合には $certA$ および $certB$ を，そしてメッセージが受信者 R まで転送された場合には $certA$，$certB$ および $certC$ を受信することになる．

4. 評　　価

本章では提案方式の安全性と有効性について評価を行う．

送信者の匿名性：

提案方式では 2 種類の攻撃者，すなわち悪意のノードおよびネットワーク盗聴者の存在を仮定している．悪意のノードとしては，メッセージ転送経路上のノードと，配達証明転送経路上のノードが攻撃者となることが想定される．メッセージ転送経路上のノードについては，オニオン・ルーティングの性質上，メッセージ送信者から直接メッセージを送られる転送ノード（図 5 におけるノード A）以外は，真のメッセージ送信者を識別することはできない．そして，メッセージ送信者 S がオニオン・プロキシを利用するプロトコルにすれば，メッセージ送信者ノードもメッセージ転送能力を備えることになる．すると，メッセージ送信者 S から直接メッセージを送られた転送ノード A は，受け取ったメッセージが S から発信されたものか，S が

他のノードから受け取ったメッセージをAに転送したのかを区別できなくなる．この結果，全てのメッセージ転送ノードは，あるメッセージの真の送信者がSかどうかを識別できない．

配達証明転送経路上のノードについては，配達証明を送信者Sに最後に転送するノード（図5におけるノードD，E，F）以外は，真のメッセージ送信者を識別することはできない．そして，オニオン・プロキシを利用することで，配達証明を最後に転送するノードでさえ，転送したメッセージがS宛のものか，Sの先に別のノードが存在するのかを区別することはできない．この結果，全ての配達証明転送ノードは，ある配達証明の真の送信者がSかどうかを識別できない．

また，ネットワーク盗聴者は，あるノードから出力されるデータパケットや，ノードに入力されるデータパケットを観測して，メッセージの送信者が誰であるかを調査する．特に，配達証明を受信する場合には，通常よりも多数のデータがメッセージ送信者に対して送られるので，このデータの観測により有意な確率で送信者か否かを識別できる可能性がある．そして，送信者が発信したデータパケット以外のパケットがネットワーク上に存在しなければ，この攻撃は成功してしまう．しかしながら，仮定2の定常的なトラフィック量が維持され，さらに送信者が配達証明を受信したときにダミーのパケットを他のノードに送信する，というプロトコルにすることにより，ネットワーク盗聴者は，特定のノードがあるメッセージの真の送信者であるかどうかを識別できない．

受信者の匿名性：

ここでも，2種類の攻撃者；悪意のノードおよびネットワーク盗聴者による攻撃を考察する．悪意のノードとしては，やはりメッセージ転送経路上のノードと，配達証明転送経路上のノードが攻撃者となることが想定される．メッセージ転送経路上のノードについては，メッセージ受信者に直接メッセージを送る転送ノード（図5におけるノードC）以外は，オニオン・ルーティングの性質上，真のメッセージ受信者を識別することはできない．そして，メッセージ受信者Rがオニオン・プロキシを利用するプロトコルにすれば，Rに直接メッセージを送信する転送ノードCは，転送したメッセージがR宛のものか，Rの先に別のノードが存在するのかを区別することはできない．また，配達証明転送経路上のノードは，真の送信者Rに関する情報を全く得ることができないので，受信者の匿名性を脅かす攻撃者になり得ない．

次に，ネットワーク盗聴者による攻撃を考察する．すなわちネットワーク盗聴者が，あるノードに入力されるデータパケットや，ノードから出力されるデータパケットを観測することで，そのノードがメッセージの受信者であるかどうかを調査する．このとき，受信者が受信するあるデータパケット以外にネットワーク上にデータパケットが存在しなければ，受信者の匿名性は満たされない．しかしながら，仮定2の定常的なトラフィック量が維持され，さらに受信者がメッセージを受信したときにダミーのパケットを送信する，というプロトコルにすることにより，ネットワーク盗聴者は，特定のノードがあるメッセージの真の受信者であるかどうかを識別できない．

以上の送信者および受信者の匿名性に関する考察により，提案方式は定義1の匿名性を満たしている．

メッセージサイズ

オニオン・ルーティングと提案方式の間で，メッセージサイズを比較する．この比較は，ネットワーク上を流れるトラフィック量や，各オニオン・ルータが処理するメッセージの量にも関連が深い．まず，メッセージを転送する中継ノード数をn_{mes}，1つの配達証明オニオンにおける平均の中継ノード数をn_{cert}とする．例えば，図5では，$n_{mes}=3$，$n_{cert}=2$である．そして，中継ノード1つ分の宛先情報および転送するメッセージサイズをuとする．このとき，オニオン・ルーティングのメッセージサイズL_{onion}および提案方式のメッセージサイズL_{c_onion}は，

$$L_{onion} = (n_{mes}+1)u,$$

$$L_{c\_onion} = n_{mes}(n_{cert}+2)u + (n_{mes}+1)u,$$

となる．図5の例においては，$L_{onion} = (3+1)u = 4u$（宛先情報B,C,Dおよびメッセージmの4情報）であり，$L_{c\_onion} = 3(2+2)u+4u = 16u$（配達証明の分で，3×4u=12uが追加される）となる．すなわちオニオン・ルーティングにおけるメッセージサイズは，メッセージを転送する中継ノード数n_{mes}に対して比例するのに対して，提案方式のメッセージサイズは，n_{mes}および平均配達証明中継ノード数n_{cert}の両方に対してほぼ比例することがわかる．

5. ま と め

本稿では，匿名通信路における配達証明配送手法を提案した．同手法は，匿名通信路において受信者の信頼度に依存することなく，データが受信者に配送されたことを，データ送信者が確信できる（あるいは，証明できる）方式となっている．これは，送信者・受信者のプライバシを保護しつつ，郵便におけるいわゆる配達証明を実現することが可能な新しい手法であり，さまざまなアプリケーションへの応用が期待できる．

文　献

[1] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, Vol. 24, no.2, pp.84-88, 1981.

[2] R. Dingledine, N. Mathewson, and P. Syverson, "Tor:The Second-Generation Onion Router", Proceedings of the 13th USENIX Security Symposium, 2004.

[3] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, "Universal Re-Encryption for Mixnets," Proceedings of the 2004 RSA Conference, Cryptographer's track, LNCS Vol. 2964, Springer-Verlag, pp.163-178, 2004.

[4] D. M. Goldschlag, M. G. Reed and P. F. Syverson, "Hiding routing information," Information Hiding: First International Workshop, Lecture Notes in Computer Science, Vol. 1174, Springer-Verlag, pp.137-150, 1996.

[5] M. Klonowski, M. Kutyowski and F. Zagorski, "Anonymous Communication with On-line and Off-line Onion Encoding," Proc. of Theory and Practice of Computer Science, LNCS Vol. 3381, Springer-Verlag, 2005.

[6] R. Song and L. Korba, "Review of network-based approaches for privacy," Proc. of the 14th Annual Canadian Information Technology Security Symposium, NRC 44905, 2002.