コンピュータセキュリティ　18−24
(2002.　7.　19)

認証・拡張性を考慮した配達証明付き電子メールの一提案

今本 健二† 櫻井 幸一‡

九州大学大学院システム情報科学研究院

〒812-8581 福岡市東区箱崎 6 丁目 10 番 1 号

E-mail: †imamoto@tcslab.csce.kyushu-u.ac.jp, ‡sakurai@csce.kyushu-u.ac.jp

あらまし 近年のインターネットの普及に伴い、ネットワークを介したビジネスが拡大してきている。公平な契約には、認証・秘匿性・完全性・非拒否性・公平性・効率性などの性質が必要である。インターネットを介した契約においてこのような機能を実現するシステムとして、配達保証付き電子メールがある。このシステムには様々な方式が考えられているが、特に Abadi らの方式[AGHP02]は必要な通信回数が少なく、TTP への送信量も少ない。しかし Abadi らの方式では、送信者と受信者が共有しているパスワードによって送信者の認証を行うため、取引相手が増えるほど、両ユーザーにとってパスワードを用意・管理する負担が大きくなる。そこで本論文では Abadi らの方式で行われている認証方法を修正し、送信者も TTP とパスワードの前登録を行わせるように変更することによって、取引相手がいくら増えたとしてもユーザー側はパスワードをひとつだけ用意すれば良い方式を提案する。

キーワード 配達保証付き電子メール, Certified E-mail, メール配送保証問題, 電子契約, パスワード認証

Proposal of Certified E-mail in consideration of Authentication and Scalability

Kenji IMAMOTO† Kouichi SAKURAI‡

Graduate School of Information Science and Electrical Engineering Kyushu University

6-10-1 Hakozaki, Higashi-ku, Fukuoka, Fukuoka 812-8581, Japan

E-mail: †imamoto@tcslab.csce.kyushu-u.ac.jp, ‡sakurai@csce.kyushu-u.ac.jp

Abstract The business through the network is being expanded with the spread of the Internet in recent years. However, the Internet is not equipped with the functions required for business or fair contracts. These functions require some characteristics such as authentication, confidentiality, integrity, non-repudiation, fairness and efficiency. Then, Certified E-mail is considered as a system which realizes such characteristics. Various systems and commercialization as Certified E-mail are proposed. Especially, Abadi's proposal system [AGHP02] requires small number of times of communication and also has few amounts of transmission to TTP. However, sender is authenticated by password shared with receiver, so the burden of preparation and management of passwords becomes large for both users when dealings partners increase in number. Then, in this paper, we modify the authentication method of Abadi's system. The modification is that the sender also makes pre-registration of a password with TTP. This modification realizes the system with which a user side should just prepare only one password when there are many partners.

Keyword Certified E-mail, Certified mail problem, Electronic Contracts, Password Authentication

1. はじめに

1.1. メール配送保証問題

契約に関わる問題のひとつとしてメール配送保証問題がある[Mo01]。これはメールの送信者が、自分が送りたい相手にメールが届いたかどうかを確認するものである。電子メール・プログラムの中には、送信者が受領書の返送を求めるメッセージを添付できるものがあるが、返送するかどうかは受信者次第であるため、相手を信用できない場合には利用できない。相手が信

用できない場合にでも、送りたい相手以外にメッセージを読まれることがなく、自分がメールを送ったことを第三者にも受領書などによって証明出来るようにしたい。

この問題で求められる最も重要な性質は、相手がメールを受け取ったのに送信者は受領書を受け取ることが出来ない、または相手はメールを受け取っていないのに送信者は受領書を受け取るということが起こらないという性質である。このような性質は公平性と呼ばれ、電子商取引においても極めて重要な性質の１つとなっている[Mo01]。

このようなメール配送保証問題を解決するためのシステムとして配達保証付き電子メールと呼ばれるシステムが考えられている。

1.2. 配達保証付き電子メール

現在までに様々な配達保証付き電子メールが考えられ、実際に国内外に商用的なシステムも存在している[Dai01, Cer98]。日本国内では、このようなサービスは政府の規制緩和により、請求書・クーポン・給与明細書など、法的な文書の交付を電子的手段でも行えるようになったことから、さらに重要性を増してきている。

配達保証付き電子メールのほとんど全ての方式では、取引を行う人以外に契約の仲介者的な存在が含まれる。この仲介者的な存在は TTP (Third Trusted Party) と呼ばれ、主に契約の公平性を満たすためにシステムに関わっている（研究によっては Semi-Trusted、または No-Trusted な第三者機関を用いる場合もある[SR98]）。また、いくつかの方式ではこのような TTP を必要とせず、二者間だけで行うプロトコルもある[Mar78]。しかし、このようなプロトコルは通信回数や計算などの効率が悪く、安全性にも疑問点があるなど、実用的な方式は考えられていない。

本システムでは上で挙げたような公平性のほかにも、認証・秘匿性・完全性・非拒否性・効率性などの性質が重要である。また、send-and-forget という機能もある。これは送信者がメールを受信者に送った後、受領証明書を受け取るまでの間、送信者は状態を保つ必要が無く、後は TTP から受領書が届くのを待つだけというものである。

配達保証付き電子メールを実現するプロトコルの中でも、プロトコルを完了するまでの間に必ず TTP を利用する方式は On-line プロトコルと呼ばれている。一方、プロトコルの実行中に問題が起きた場合にのみ TTP を利用する方式は Optimistic プロトコルと呼ばれる[ASW98]。TTP を利用しない方式や Optimistic プロトコルなどでは、問題が起きない限り TTP を利用しないため、送信者はメッセージを送った後も送信者と受信者が何回かの通信のやり取りを行わなければならない[AR02, ASW98]。そのため、送信者はメールを送った後も相手が応答するのを待つ必要がある。一方、On-line プロトコルの場合はプロトコルの途中で必ず TTP を利用するため、TTP に対して通信や計算の負荷が大きくなってしまうという問題があるが、送信者はメッセージを送った後は受信者と TTP のやり取りに任せることが出来るため、send-and-forget の機能が実現出来る。

従来の On-line プロトコルでは TTP へメール全体を送る方式がほとんどである。例えば、配達保証付き電子メールの商業サービスを提供する Certifiedmail.com [Cer98]では、送信者はメッセージを作成し、同社のウェブサイトを通して相手に送信する。メッセージを送った後は Certifiedmail.com のサイトを訪れ、自分が送った電子メールメッセージがどうなったかチェックできる。受信者は配達証明付き電子メールメッセージの到着を告げるメッセージを受け取り、そのメッセージに記載されている URL から Certifiedemail.com のサイトに行ってメッセージを取り出す、という手順でやり取りが行われる。このようにメッセージ全体を TTP に送信する場合、小さい容量のメールなどを送信する場合は問題無いが、デジタルコンテンツの売買への利用を考えた場合[HPS01]などの送受信するファイルサイズが大きい場合には TTP の通信に掛かる負担が大きくなりすぎてしまう。他にも利用ユーザーが増加した場合にも同様の問題が起こる。そこで、このような問題を解決した方式が Abadi らの方式[AGHP02]である。彼らの方式では、TTP へ送信する通信量は送信メッセージの容量に比例せず、サービスの利用回数に比例する。TTP に直接メッセージを送信しないため、ユーザーから TTP への通信量を減らすことが可能となっている。

上で説明したように、On-line プロトコルはユーザーが行うべき通信回数が少なく、send-and-forget の実現が容易である、などの利点があるが、毎回 TTP を利用するため TTP への負荷が問題となる。一方、Optimistic プロトコルの場合、問題が起こった場合だけ TTP を利用するため、TTP への負荷が少なくて済むという利点があるが、ユーザーの通信回数が On-line プロトコルより多くなる場合が多く、send-and-forget 機能の実現が難しい。すなわち、On-line プロトコルはユーザーにとって利用しやすい方式であり、Optimistic プロトコルは TTP の配置が容易な方式である。

本論文では必要な通信回数や send-and-forget の実現など、ユーザーにとって使いやすい方式であることから、On-line プロトコルに注目する。特に Abadi らの方式[AGHP02]は、On-line プロトコルの欠点である TTP

への通信に掛かる負荷を軽減した方式であるが、拡張性などの面で問題があり、送信相手が不特定多数の場合に不向きな方式である。本論文では、この問題について解決した新しい方式を提案する。また、Abadi らの方式では省略されていたTTPと受信者間のセキュアチャンネルの実現法について、新たなセッション鍵の導入を提案する。同じ方法は Abadi らの方式にも適用可能である。Abadi らの方式の詳細については次の章で説明する。

2. 求められる性質

本章では配達保証付き電子メールに求められる性質の説明を行う。

公平性：両方のユーザーが望んでいる結果を得る、またはどちらのユーザーも得ることが出来ない
認証：通信相手が確かに目的の相手である
秘匿性：第三者にメッセージを読まれることが無い
完全性：途中でメッセージが書き換えられていない
非拒否性：前に行った行動を後になって取り消すことが出来ない
効率性：出来る限り少ない計算、通信回数、通信量でプロトコルが実行できる

これらの性質の中でも配達保証付き電子メールでは、特に公平性の実現が重要となっている。本論文ではユーザーの使いやすさを考えて On-line プロトコルを利用しているため、TTP に負荷が掛かりやすい。そこで効率性について考察を行う。Abadi らの方式では認証の際に拡張性の問題があるので、これについても考察する。また、秘匿性については必要な場合と、必ずしも必要ではない場合があるが本論文では満たすべきものとする。

3. Abadi らの方式

Abadi らの方式[AGHP02]は利用のたびに必ず TTP と通信を行う On-line プロトコルである。On-line プロトコルを利用した従来の方式のほとんどは、TTP へメッセージ全体を送る方式をとっているが、これでは TTP にかかる通信の負荷が大きい。そこで、Abadi らは TTP の通信量がメッセージの容量に比例することが無く、TTP の通信量を減少させた方式を提案した。また、Abadi らの方式では受信者は公開鍵のペアを持っておらず、PKI も整備されていないものとしており、認証方法としてパスワードを利用している。

プロトコルは大まかには以下のようになっている。

① 送信者はセッション鍵 K をランダムに生成する。送信メッセージは K で暗号化し、K を TTP の公開鍵で暗号化する。そして受信者にセッション鍵 K で暗号化したメッセージと、TTP の公開鍵で暗号化した鍵 K を送る。さらにオプションとして、受信者と送信者が共有しているパスワードを利用することも出来る。
② 受信者は受け取った通信の中から暗号化された鍵 K、TTP と共有しているパスワードを TTP に送る。
③ TTP は受信者の身元を確認し、K を復号化して受信者に送り返す。このとき送信者に、受信者がメッセージを受け取ったことを証明する受取書を送る。
④ 受信者は K を用いてメッセージを復号化する。

よって、TTP がユーザーから受け取る通信はメールそのものではなく、暗号化されたセッション鍵 K や認証情報であるため、TTP が通信に掛かる負荷は少ない。途中のプロトコルに不正があった場合、TTP は取引を中止する。具体的な手順は次の節で示す。

3.1. プロトコル

モデルと前提：
プロトコルには送信者、受信者、TTP の 3 つのパーティが存在する。送信者は配達証明付き電子メールを受信者に送り、両ユーザーは TTP をプロトコルの仲介者として On-line で利用する。また、送信者・受信者・TTP とも使用する暗号技術(共通鍵暗号、公開鍵暗号、ハッシュ関数、署名方式など) については既に了解しているものとする。受信者と TTP の間の通路は SSL,IPsec などを利用し、セキュアであり、攻撃者に盗聴されない。TTP は公開鍵を持っており、送信者・受信者ともこの公開鍵を知っている。ただし、送信者・受信者とも自分の公開鍵は持っていない、または公開鍵インフラ（PKI）が整備されていない。よって認証のため、受信者は TTP に前もって登録を行い、パスワードを共有している。また送信者と受信者が、相互認証、または TTP からメッセージを隠すために、パスワードを共有することも出来る。

使用する記号
M：メッセージ
件名：送信メッセージの内容を説明
S：送信者の ID
R：受信者の ID
T：TTP の ID

K：セッション鍵
PSR：送信者と受信者の共有パスワード
PRT：受信者と TTP の共有パスワード
H(・)：ハッシュ関数
EK(・)：鍵 K で暗号化
ET(・)：TTP の公開鍵で暗号化
SIGT(・)：TTP による署名
em：EK(M)
authoption：認証方式選択
h：H(件名, PSR, em)
S2T：ET(K, h, S, R, authoption)
受領書：SIGT("S sent K to R for S2T.")

具体的な手順は以下の通り

① 送信者はセッション鍵 K をランダムに生成し、受信者へ、S, T, em, authoption, 件名, S2T を送信する。
② 受信者は S から相手を判断し、h を生成する。そして TTP へ、S2T, h, PRT を送信する。
③ TTP は受信者の送ってきた PRT が正しく、送信者・受信者が生成した h の値が等しいことが確かめる。正しければ、S2T からセッション鍵 K を取り出し、受信者に K を送信する。また、送信者に受領書を送信する。
④ セッション鍵 K を用いて em からメールを復号する。

authoption により、送信者は受信者を認証する方式として、PSR による認証・PRT による認証・両方のパスワードを利用した認証・認証無しの 4 つから選択可能である。

本方式において、送信者は送信 1 回・受信 1 回、受信者は送信 1 回・受信 2 回、TTP は送信 2 回・受信 1 回行う。この特徴としては、送信者はメールを送信した後は受領書が送られてくるまで待つだけでよく、send-and-forget が可能である。また、受信者がメールを受け取った際に送信者がオフラインだったとしても、受信者はメッセージを復号化して読むことが可能である。TTP は受領書を送信した後、状態を保つ必要が無い。

3.2. 送信者認証に関する問題

Abadi らの方式では認証にパスワードを利用している。送信者は、受信者を認証する方式として、PSR による認証・PRT による認証・両方のパスワードによる認証・認証無しの 4 つから選択する。また送信者の認証についても、送信者自身が PSR による認証・認証無しから選択する。これらの認証方法の選択は送信者に任されているため、以下のような問題が考えられる。

- PSR を利用することにより、受信者はメッセージの送信者が誰であるのかをメッセージを受け取る前にはっきりさせることが出来る。受信者にとってはメッセージを送ってきた相手が誰であるのか確かめることが出来るため、問題が起きた場合は送信者に対処を求めることが出来る、というメリットがある。しかし、PSR による認証を行う場合、通信者同士で前もって共有パスワードを用意する必要があるため、多くの取引相手がいる状況ではパスワードの前準備・管理にかかる手間が大きい。そのため、本オプションを利用した場合、システムの拡張性が乏しくなる。

- PSR を利用しない場合、送信者・受信者間でパスワードを共有する必要が無いため、取引相手が増えたとしても新たにパスワードを増やす必要は無い。しかし、送信者を認証することが無いため、受信者は誰がメッセージを送ってきたのか確かめることが出来ない。

本サービスの性質上、不特定多数のユーザーへの有料コンテンツ配布などへの利用も考えられる。このような場合、ユーザーはコンテンツ配布者が誰であるかをはっきりさせたい。この場合、PSR を利用する必要があるが、それぞれのユーザーとパスワードを共有するのは大変な手間になる。そのため、拡張性は大きな問題である。

一方、PSR を利用しない場合、送信者にとっては目的の相手にメッセージを届けることが出来るため、有用なサービスであるが、受信者にとってはメッセージを他の人に見られることが無いということ以外にはメリットが無い。このことは公平な契約の理念から外れている恐れがある。また、受信者は TTP とパスワードを共有している必要があるため、受信者自身が本サービスに加入していなければいけない。よって、受信者にとってもメリットの大きく、魅力のある方式でないとサービスの利用者も増えにくい。そのため、これらの送信者認証の際に起こる問題を解決した方式が必要である。

また、Abadi らの方式では TTP は送信者と前もってパスワード登録などの手続きが無い。そのため、TTP は送信者を認証する方法が無い。このことにより、例え authoption で PSR,PRT の利用を選択していたとしても、受信者は X,Y を正しく生成することが可能である。このことを利用して、受信者は送信者に成りすまし、送信者からメッセージを送られてきた振りをすることが可能である。

パスワード認証の検証やセッション鍵の復号などはTTPが全て行うため、もし悪意のあるTTPが存在した場合、成りすましやメッセージの盗聴が可能となってしまう。さらに攻撃者が①の通信を盗聴した場合、リプレイ攻撃に使用される可能性がある。

4. 提案方式

Abadiらの方式には3章で説明したように、送信者の認証に関して問題がある。しかし、ユーザーはそれぞれ送受信を1回行うだけで良く、全通信回数は4回で済む、TTPへの送信量が少なくて済む、送信者はメッセージを受信者に送った後は状態を保つ必要が無くsend-and-forget が可能である、などの点において、優れた方式である。

そこで、Abadi らの方式を基にし、上で挙げた利点はそのまま維持しつつ、プロトコルで行われる認証方法に修正を加えることによって、送信者認証の際に起こる問題を解決した方式を提案する。

Abadi らの方式において、送信者は受信者とのみパスワードを共有している。しかし、Abadi らの方式では送信者と受信者が共有しているパスワードの検証をTTPが行うため、認証のためにユーザー同士がパスワードを共有したとしても、TTPの成りすましを防ぐことは出来ない。そこで、提案方式では送信者・受信者間のパスワード共有を廃止して、送信者はTTPとの共有パスワードをTTPに前登録するようにする。すなわち、両ユーザーともTTPとのみパスワードを共有するようにする。このような変更により、送信者の認証が可能で、かつ取引相手が増えた場合でもユーザー側が覚える必要のあるパスワードはひとつだけでよく、拡張性の高い方式が可能となった。本提案方式でもAbadi らの方式同様に送信者・受信者共に公開鍵ペアは必要なく、PKIが整備されていない環境でも使用可能である。

4.1. プロトコル

モデルと前提：

本プロトコルでもAbadiらの方式同様、送信者・受信者・TTPの3つのパーティが存在し、両ユーザーはTTPをプロトコルの仲介者としてOn-lineで利用する。また、送信者・受信者・TTPとも使用する暗号技術についても既に了解しているものとする。本方式でもTTPは公開鍵を持っており、送信者・受信者ともこの公開鍵を知っている。また、送信者・受信者とも自分の公開鍵は持っていない、または公開鍵インフラ(PKI)が整備されていない。本方式では認証のため、送信者・受信者ともTTPに前もって登録を行い、パスワードを共有している。

記号の定義

K,L：セッション鍵
PST：送信者とTTPの共有パスワード
PRT：受信者とTTPの共有パスワード
X:ET(K, PST, S, R, 件名, H(em), authoption)
Y:ET(L, PRT, S, R, 件名, H(em), authoption)
EL(・)：セッション鍵Lで暗号化
受領書:SIGT(H(X), S sent 件名 to R, authoption)

具体的な手順は以下の通り（図参照）

① 信者はセッション鍵Kをランダムに生成し、受信者へ、S, T, em, 件名, X, authoption を送信する。
② 受信者はSから相手を判断し、Yを生成する。そしてTTPへ、X, Yを送信する。
③ TTPは受信者の送ってきたYが正しいことを確かめる。正しければ、XとYからセッション鍵K, Lを復号化し、受信者に EL(K)と受領書を送信。また、送信者にも受領書を送信

本提案方式でもAbadiらの方式同様、authoptionによって、送信者・受信者を共に認証、受信者のみ認証、送信者のみ認証、認証無しの中から選択することが可能である。基本的に契約は公平なものであるので、契約の際は送信者・受信者を共に認証する方式を推奨するが、特別な場合や取引者間で既に認証に関する話し合いが行われている場合は他の認証方式の利用も可能である。例えば、ある人に匿名で寄付をしたい場合には受信者のみ認証する方式を使い、誰が受信してもよいが受け取った事実のみを確かにしたい場合には送信者のみの認証、または認証無しの方式を選択すると良い。

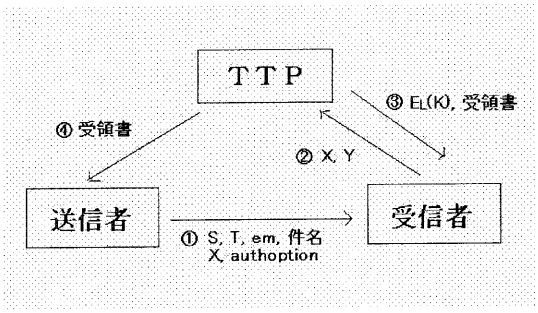
また、受信者が正規の手続きを経てセッション鍵Kを復号したにも関わらず、メッセージが正しく復号できない場合(明らかに件名と内容が合致しない等)は、領収書とX,em,Kを示すことで、送信者に件名と内容が合ったメッセージが復元できる鍵を送信するように訴えることが可能である。送信者側も受領書を示すことによって、自分が受信者にメッセージを送信した事実を、第三者にも証明することが可能である。

この方式は複数の受信者にマルチキャストなどを利用して、同時に配達保証付き電子メールを送りたい場合にも容易に拡張可能である。

送信相手がはっきり決まっていて、それ以外の相手にはメールを読まれたくない場合には以下のようにす

る。まず、送信者はXを生成する際に受信者欄にメールを送りたい相手の一覧を書き込むようにする。TTPはXを復号した際に、X,Yを送信してきた受信者の名前が含まれているかどうかを確認し、パスワードが正しければ相手に鍵と受領書を送り、送信者に受領書を送る。

また、送信相手がはっきり決まっておらず、TTPに登録している相手なら誰でも受信可能にしたい場合は以下のようになる。Xの送信者欄を空白にし、メールを受け取った相手は通常通りにYを生成してTTPに送信する。TTPはパスワードが正しければ受信者が誰であっても鍵と受領書を送り、送信者にも受領書を送る。この方式を利用することにより、セキュリティに保護されていないようなサイトに送信者欄を空白にしたX置いておき、X自体は認証無しで誰でもダウンロード可能、という環境であったとしても、信頼あるコンテンツをユーザーに持ち逃げされないよう安全に配布することが可能である。



図：提案方式

提案方式においてもAbadiらの方式同様、送信者は送信1回・受信1回、受信者は送信1回・受信2回、TTPは送信2回・受信1回であり、同様の性質を持つ。すなわち、送信者はsend-and-forgetが可能であり、受信者は送信者の状態に関わらずいつでもメッセージを復号化して読むことが出来、TTPは受領書を送信した後、状態を保つ必要が無い。

4.2. 安全性の解析

攻撃者はX,Yを盗聴したとしても、パスワードやセッション鍵はTTPの公開鍵で暗号化されているため、メッセージを復号されることは無い。

他にも、受信者がセッション鍵Kを不正に入手するために、他のユーザーに成りすまそうとしても、Xに含まれている宛先IDによって受信者が特定されているため、この攻撃は成功しない。また、Yの送信者を示すSを別の人物のIDであるS'としたとしても、Xに含まれている送信者IDと異なることからこの攻撃はTTPによって検出される。よって、X,Yの書き換えによって送信者を偽造することも出来ない。同様に送信者が受信者IDを書き換えた場合もTTPは検出可能である。

提案方式では送信者の認証も行うようにしているため、authoptionで送信者の認証を選択した場合、受信者は正しくXを生成することが出来ない。よって、Abadiらの方式で問題であった、受信者が送信者に成りすますことを防ぐことが可能である。

また、本方式ではAbadiらの方式では省略されていたTTPと受信者間の通信盗聴に対する防止方法についても提案する。提案方式ではPRT盗聴防止のためにTTPの公開鍵を利用し、セッション鍵K盗聴防止のためにセッション鍵Lを導入している。③の通信で送信しているセッション鍵Kはセッション鍵Lによって暗号化されているため、攻撃者が盗聴したとしても鍵Kを知ることは出来ない。提案方式では、このセッション鍵Lの導入によりAbadiらの方式で受信者・TTP間で必要だったセキュアチャンネルが必要なくなっている。同じ方法はAbadiらの方式にも適用可能である。

ただし本方式では、TTPは不正を働かないということが前提になっている。もしも悪意のあるTTPが存在した場合、送信者への成りすまし、あるいは①の通信を盗聴することによるメッセージの復元などの攻撃が可能である。TTPによる盗聴はユーザーの公開鍵、または既知共有鍵を利用してメッセージを暗号化することによって防ぐ方法しかない。この点についてはAbadiらの方式と同様に問題となっている。今回の提案方式ではユーザーの使いやすさや少ない通信回数、send-and-forgetの機能実現などに重点を置いたが、TTPの不正防止については今後考える必要がある。

Abadiらの方式では送信者のみに受領書が渡されるが、契約中に何らかの問題が起こって裁判沙汰になった場合、送信者が受領書を捨ててしまえば、受信者は取引があった事実を第三者に示すことが難しくなる。そこで本提案方式では、受信者も受取証明として受領書を受け取れるようにした。TTPは送信者・受信者共に同じ内容の受領書を送る。そのため、受領書生成にかかる計算の手間は、送信者だけに送信する方式と変わらない。また、攻撃者にXを盗聴された場合、受信者・TTPに対するリプレイ攻撃に使用される可能性がある。この場合、受け取ったXからH(X)を計算し、受領書に記されているH(X)と比較する。二つが同じ値の場合、このメッセージはリプレイ攻撃とみなし、メッセージを廃棄するという対策が考えられる。

4.3. 提案方式の考察

本提案方式では送信者・受信者とも TTP とパスワードを共有する必要があるため、TTP への前登録が必要である。その代わり、送信者は各受信者とパスワードを共有しなくても自分を証明することが可能である。また、通信相手それぞれに対してパスワードを用意することが無いため、不特定多数の相手とのやり取りが可能であり、拡張性が高い。また、受信者側にとっても通信相手が誰であるのか認証可能であるため、安心して取引が出来るというメリットがある。

また、X,Y の生成・復号の際、公開鍵の計算にコストがかかる場合は、X,Y をそれぞれ以下のように定義し直すことも可能である。

X:ET(K, PST, S), EK(R, 件名, H(em))

Y:ET(L), EL(PRT, S, R, 件名, H(em))

特に件名の長さに関しては任意であるため、コンテンツの説明などにより非常に長くなることも考えられる。このような場合には、件名がセッション鍵 K,L という共通鍵で暗号化・復号化することによる計算の高速化は大きな意味を持つ。

この方式の欠点としては、送信者・受信者とも TTP とパスワードを共有する必要があるため、全ユーザーが本サービスへの前登録をする必要がある点である（認証方式の選択によっては必要ないユーザーもいる)。authoption で送信者・受信者の認証を行う場合、それぞれのパーティが所有すべきパスワード数は以下の表のようになる。この表からも分かるように、送信者・受信者とも管理すべきパスワードの数は Abadi らの方式よりも減らすことが出来、送受信対象が増えたとしてもパスワードを新たに用意する必要は無い。ただし、TTP は Abadi らの方式が全受信者数だけでよいのに対し、提案方式では全ユーザー数となり、用意すべきパスワード数は増えている。よって、全ユーザー数と比べて受信者数の割合が少なく、送信のみをするパーティが多い場合、提案方式における TTP の管理するパスワード数は Abadi らの方式よりも特に多くなる。逆に全ユーザー数に比べて受信者数の割合が多い、または送信のみをするユーザーが少ない場合、提案方式と Abadi らの方式における TTP の管理するパスワード数はほとんど同じ数である。実際のシステムを考えた場合、送信のみをするユーザーは少ないと思われるため、提案方式での TTP がパスワードを管理するために掛かるコストは、Abadi らの方式と大きな違いは無い。

本方式では 4.2 節で述べたように、認証やメッセージの暗号化を TTP に依存しているためユーザーは TTP を完全に信用する必要がある。受信者の公開鍵でメッセージを暗号化してからセッション鍵で暗号化することにより TTP からもメッセージを読まれることは無いが、受信者と TTP が共謀すると、送信者に受領書を送ることなくメッセージを読むことが可能であるため、配達保証付き電子メールで最も重要な性質である公平性を満たすことが出来ないという問題がある。

	送信者	受信者	TTP
Abadi ら	受信相手数	送信相手数 TTP 数	全受信者数
提案方式	利用 TTP 数	利用 TTP 数	全ユーザー数

表：Abadi らの方式と提案方式の比較
(それぞれのパーティが管理すべきパスワード数)

5. おわりに

電子契約を行う際に重要となる問題のひとつとして、メール配送保証問題がある。本論文では、この問題を解決するようなシステムである配達保証付き電子メールについて考察を行った。その結果、通信量や通信回数の面から Abadi らの方式に注目した。しかし、Abadi らの方式ではメッセージの送信者の認証に関して拡張性などの問題がある。そこで、本論文では送信者の認証が可能で、かつ拡張性のある方式を提案する。本方式では送信者・受信者とも TTP とパスワードを共有し、それを利用した認証を行う。この結果、提案方式ではユーザーは TTP とパスワードを共有すれば良く、通信相手ごとにパスワードを用意する必要が無いため、拡張性が高い方式となった。また、全ての通信はセキュアチャンネルを利用する必要が無くなっている。

本方式ではユーザーは TTP を完全に信頼する必要があるが、今後は Semi-Trusted、または No-Trusted な第三者機関を仮定した方式の考察、さらにデジタルコンテンツの売買への利用などさまざまな実システムへの利用についての考察を進める。

文　献

[AGHP02] M. Abadi, N. Glew, B. Horne and B. Pinkas, Certified Email with a Light On-line Trusted Third Party: Design and Implementation, WWW2002, May 7-11, 2002, Honolulu, Hawaii, USA.

[Mo01] D. Molnar, Signing Electronic Contracts, Jan 2001
http://www.acm.org/crossroads/xrds7-1/

[AMG01] G. Ateniese, B. d. Medeiros and M. T. Goodrich, TRICERT: A Distributed Certified E-Mail Scheme, In ISOC 2001 Network and Distributed System Security Symposium (NDSS'01), San Diego, CA, USA, Feb 2001.

[AR02] G. Ateniese and C. N. Rotaru, Stateless-Recipient Certified E-mail System based on Verifible Encryption, In B. Preneel, editor, Topics in Cryptology – CT-RSA 2002, volume 2271 of Lecture Notes in Computer Science, pages 182-199. Springer-Verlag, Feb 2002.

[ASW98] N. Asokan, V. Shoup and M. Waidner, Optimistic Fair Exchange of Digital Signatures, In Proceedings of EUROCRYPT '98, 1998.

[HPS01] B. Horne, B. Pinkas and T. Sander, Escrow Services and Incentives in Peer-to-Peer Network, 3rd ACM Conference on Electronic Commerce, 2001.

[SR98] B. Schneier and J. Riordan, A Certified E-Mail Protocol with No Trusted Third Party, 13th Annual Computer Security Applications Conference, ACM Press, Dec 1998.

[Dai01] 大和総研, 書留～る, May 2001.
http://www.dir.co.jp/system/kakitome-ru/

[Mar78] Markle. R, Secure Communications over insecure channels, Communications of the ACM 21:294-299, April 1978.

[Cer98] http://www.certifiedemail.com/, 1998.