配達仲介人を利用した配達証明付き電子メールの改良

今本健二[†] 櫻井幸一[††]

近年のインターネットの普及にともない，ネットワークを介したビジネスが拡大してきている．ネットワークを介した契約を行う際には公平な交換が必要となる．このような公平な交換を実現するためのシステムとして，配達証明付き電子メールが考えられている．本論文では現在までに提案されている様々な配達証明付き電子メールを基に，認証・秘匿性・完全性・非拒否性・効率性・Send-and-Forget などの性質を考慮に入れた 2 つの新しい方式を提案する．1 つは認証に共有秘密鍵を用いており，Abadi らの方式 [Abadi, et al., WWW2002, May 7–11, 2002] を基に，送信者認証・拡張性の観点から改善を行い，Abadi らの方式よりも，より有用性が高く，実現も容易な方式となっている．もう 1 つは電子署名を用いた方式である．この方式では，仲介人をどのように利用するかを，受信者が選択できる．これにより，様々な状況に対応可能であり，実用的な方式となっている．本論文ではこれらの方式を提案し，様々な面から考察を行う．

Improvements of Certified E-mail with Delivery Authority

Kenji Imamoto[†] and Kouichi Sakurai[††]

The business through the network is being expanded with the spread of the Internet in recent years. A contract through the Internet needs to realize some requirements. In this paper, we consider the requirements such as fairness, authentication, confidentiality, integrity, non-repudiation, efficiency, and Send-and-Forget. Then, we propose two Certified E-mail systems. One is the system with authentication by shared secret that is based on the system of Abadi, et al. [Abadi, et al., WWW2002, May 7–11, 2002]. We improve a sender's authentication and scalability of the system of Abadi et al. The other is the system using digital signature based on PKI. In this system, a receiver can choose the usage of delivery authority freely according to that time after taking the necessity and the situation of delivery authority and the sender into consideration. This system can deal with many situations, and is practical method. In this paper, we explain and analyse these proposed systems.

1. はじめに

1.1 メール配達証明問題

契約に関わる問題の 1 つとしてメール配達証明問題がある[1)]．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できるかどうか，というものである．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この機能が無意味になる場合も多い．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，相手にメールが届いたことを第三者にも受領書などによって証明できるようにしたい．

この問題で求められる最も重要な性質は，受信者がメールを受け取ったにもかかわらず送信者は受領書を受け取ることができないという状況，もしくは，送信者は受領書を受け取ったにもかかわらず受信者はメールを受け取ることができないという状況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きわめて重要な性質の 1 つとなっている[1)]．このようなメール配達証明問題を解決するためのシステムとして配達証明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 配達証明付き電子メール

現在までに様々な配達証明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[2)]．日本国内では，このようなサービスは政府の規

† 九州大学大学院システム情報科学府
Graduate School of Information Science and Electrical Engineering, Kyushu University
†† 九州大学大学院システム情報科学研究院
Faculty of Information Science and Electrical Engineering, Kyushu University

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．

配達証明付き電子メールのほとんどすべての方式では，取引を行う人以外に契約の仲介をする存在が含まれる．この仲介者的な存在は，契約の公平性・効率性の観点からシステムに導入される（研究によってはSemi-Trusted，またはNo-Trustedであるような第三者機関を用いる場合もある[3),4)]）．一方，このような仲介人を必要とせず，2者間だけで行うプロトコルも考えられている[5)]．しかし，2者間だけで公平な交換を行った場合，通信回数や計算などの効率が悪くなってしまい，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．そこで，本論文では仲介人を利用した配達証明付き電子メールについて考える．

本システムでは上であげたような公平性のほかにも，認証・秘匿性・完全性・非拒否性などの性質が重要である．また，Send-and-Forgetという機能がある．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なく，後は仲介人から受領書が届くのを待つだけというも のである．

配達証明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配達仲介人を利用する方式はOn-lineプロトコルと呼ばれる．一方，問題が起きた場合のみ仲介人を利用する方式はOptimisticプロトコルと呼ばれる．

Optimisticプロトコルでは問題が起きない限り仲介人を利用しないため，送信者はメールを送信した後も受信者が返信してくるのを待つ必要がある．同様に，受信者も相手の返事を待つ必要があるため，Send-and-Forgetが実現できない．On-lineプロトコルの場合はプロトコルの途中で必ず仲介人を利用するため，仲介人に対して通信や計算の負荷が大きくなってしまう問題があるが，送信者はメッセージを送った後，受信者と仲介人のやりとりに任せることができるため，Send-and-Forgetが実現できる．

本論文ではユーザを，配達証明付き電子メールシステムにおける送信者と受信者から構成される存在と定義する．このとき，上で説明したように，On-lineプロトコルはユーザが行うべき通信回数が少なく，Send-and-Forgetの実現が容易，などの利点があるが，毎回仲介人を利用するため仲介人への過大な負荷が問題となる．一方，Optimisticプロトコルの場合，問題が起こった場合だけ仲介人を利用するため，仲介人への負荷が少ないという利点があるが，Send-and-Forgetが実現できない．すなわち，On-lineプロトコルはユーザにとって利用しやすい方式であり，Optimisticプロトコルは仲介人の配置が容易な方式という見方ができる．

そこで本論文では，従来の配達証明付き電子メールについて考察を行い，新たに2つの方式を提案する．最初に，Abadiらの方式[6)]を基にし，共有秘密鍵を用いた，より拡張性の高い方式を説明する．次に，受信者が状況に応じて自由にプロトコルを選択できる，実用的な方式を説明する．

本論文は以下のような手順で説明を行う．まず，2章で提案方式で使用するモデル・ 記号を定義し，3章では配達証明付き電子メールに求められる性質について定義する．4章で2つの提案方式を説明，考察し，5章で本論文のまとめを行う．

2. 準　　備

本章では，本論文で提案する2つの方式で共通して使用されるモデルの説明を行う．

モデル

プロトコルには送信者，受信者，配達仲介人の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，両ユーザは配達仲介人をプロトコルの仲介者として利用する．また，送信者・受信者・配達仲介人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）についてはすでに了解しているものとする．また，仲介人の公開鍵は公開されており，誰でも入手可能とする．また，仲介人と各ユーザ間で使用する通信路は，信頼性のある通信路とする．ここで信頼性のある通信路とは，送った情報が通信相手に正しく届く通信路である．一方，信頼性がない通信路とは，情報が通信中に書き換えられる，もしくは情報が通信中になくなるような通信路を意味する．また，メッセージなど，サイズが大きなものに署名する場合は，メッセージ全体ではなく，そのハッシュ値に対して署名を行う．

3. 求められる性質

本章では配達証明付き電子メールに求められる性質の説明を行う．

公平性：両方のユーザが望んでいる結果を得る，またはどちらのユーザも得ることができない．
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ない．
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

ができない．

効率性：できる限り少ない計算，通信回数，通信量でプロトコルが実行できる．

Send-and-Forget：送信者が受信者にメールを送った後，送信者は状態を保つ必要がない．

これらの性質の中でも配達証明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．また，非拒否性には，受信者がメールを受け取ったことを後で否定できない受信非拒否性と，送信者がメールを送信したことを後で否定できない送信非拒否性がある[7),8)]．

4. 提案方式

本論文では 2 つのプロトコルを提案する．1 つは認証に共有秘密鍵を用いた方式，もう 1 つは電子署名を用いた方式となっている．

提案方式 1 は共有秘密鍵を用いているため，PKI が整備されていない環境でも実現が容易な方式である．本方式は Abadi らの方式を基にし，Abadi らの方式で問題となっていた，認証・非拒否性・システムの拡張性などの問題を解決している．

一方，提案方式 2 では電子署名を用いることにより，提案方式 1 で問題となる配達仲介人への依存の問題を軽減することができる．また，従来は送信者が On-line プロトコル・Optimistic プロトコルのどちらを使用するか決定していたが，本方式では，仲介人をプロトコル内でどう使用するかを，受信者が選択できる方式となっている．これにより提案方式 2 は，様々な状況に対応可能で，より実用的な配達証明付き電子メールとなっている．

以下のセクションでそれぞれの方式について説明し，考察を行う．

4.1 提案方式 1

メッセージ全体を配達仲介人に送信する場合，小さい容量のメールなどを送信する場合は問題ないが，デジタルコンテンツの配布など，送受信するファイルサイズが大きい場合には，仲介人の通信にかかる負担が大きくなりすぎてしまう．このような仲介人への通信量の増加問題を解決した方式が Abadi らの方式[6)]である．彼らの方式では，仲介人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．この方式では，仲介人に直接メッセージを送信しないため，ユーザから仲介人への通信量を減らすことが可能となっている．

Abadi らの方式では共有秘密鍵を認証に利用しており，送信者は受信者とのみ秘密鍵を共有し，受信者は送信者と仲介人の両方と秘密鍵を共有する必要がある．これに関連して，以下のような問題が起こる．送信者は仲介人と秘密鍵を共有していないため，仲介人が送信者を認証する際は，送信者が送ってきた秘密鍵と受信者が送ってきた秘密鍵が等しいことにより，送信者が正しい通信相手と認証する方法をとっている．この方法では第三者が送信者に成りすますことはできないが，受信者が送信者に成りすますことが可能である．よって，メッセージが送信者によって送られたのか，それとも受信者が送信者への成りすましを行ったのか，第三者は判断することができないため，送信非拒否性が実現できない．また，送信者・受信者間で秘密鍵を共有する必要があるため，多くの通信相手にメッセージの送受信を行う場合のシステムには適していない．

本セクションでは，Abadi らの方式が持つ利点はそのまま維持しつつ，共有秘密鍵を用いた認証の際に起こる問題を解決した，提案方式 1 を説明する．提案方式では送信者・受信者間では秘密鍵を共有せず，送信者・受信者は，それぞれ仲介人と秘密鍵を共有するようにする．これにより，送信者の認証・送信非拒否性が実現され，取引相手が増えた場合でも送信者・受信者が覚える必要のある共有秘密鍵は 1 つだけでよい．そのため，拡張性の高い方式となっている．本提案方式は，Abadi らの方式同様，PKI が整備されていない環境で使用可能である．

4.1.1 準　　備

ここでは，提案方式 1 で用いられる仮定，記号について説明する．

仮定

送信者・受信者とも，自身の署名鍵を持っていない．送信者・受信者は，それぞれ配達仲介人と秘密鍵を共有している．配達仲介人の公開鍵は誰でも手に入れることができる．

記号

M：メッセージ
件名：送信メッセージの内容を大まかに説明した文章
S，R，D：送信者/受信者/配達仲介人の ID 情報
K，L：セッション鍵
H(·)：一方向性ハッシュ関数
$E_K(\cdot)$，$E_L(\cdot)$：セッション鍵 K，L による共通鍵暗号
$E_D(\cdot)$：配達仲介人の公開鍵を用いた暗号化
$SIG_D(\cdot)$：配達仲介人による電子署名
em：E_K(M)
P_{SD}：送信者と配達仲介人が共有している秘密鍵
P_{RD}：受信者と配達仲介人が共有している秘密鍵
X：E_D(K, P_{SD}, S, R, 件名, H(em))
Y：E_D(L, P_{RD}, S, R, 件名, H(em))

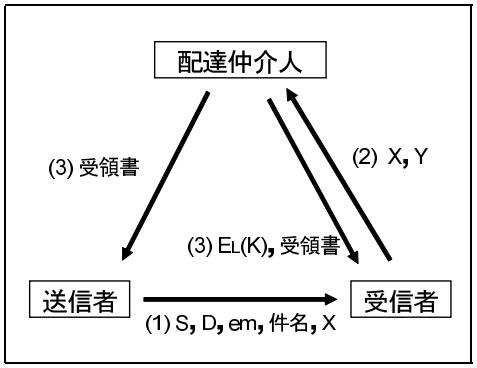

図 1 提案方式 1
Fig. 1 Proposed Method 1.

受領書：SIG_D(H(X), S sent 件名 to R)

4.1.2 プロトコル

具体的な手順は以下のとおり（**図 1** 参照）.

(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，D，em，件名，X 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．そして配達仲介人へ，X，Y を送信する.

(3) 配達仲介人は，受信者が送ってきた X，Y に含まれる P_{SD}，P_{RD} が正しいこと，X，Y の両方に含まれる S，R，件名，H(em) が等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 E_L(K)，受領書を送信する．また，送信者に受領書を送信する.

4.1.3 考　　察

本提案方式では送信者・受信者とも配達仲介人と秘密鍵を共有する必要があるため，仲介人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秘密鍵を共有しなくても自分の身元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前もって秘密鍵を共有する手間がないため，不特定多数の相手とのやりとりが可能であり，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，安心してメッセージを受け取ることができるというメリットがある.

3 章で定義した性質について考察する．受信者はメッセージを読む場合，Y を正しく生成し仲介人に送る必要がある．仲介人は受け取った X，Y が正しく生成されている場合にのみセッション鍵と受領書を各ユーザに配布するため，仲介人が正しく働く限り，公平性が保たれている．また，送信者・受信者は，仲介人と共有した秘密鍵で認証を行うことが可能となっている．メッセージを暗号化したセッション鍵は仲介人の公開鍵で暗号化されているため，仲介人以外の第三者から読まれることはなく，メッセージの秘匿性が保たれている．また，送信者から受信者への通信路上で仲介人を除く第三者によって暗号文 em が改ざんされた場合，もしくは受信者が H(em) の値を偽って Y を生成した場合でも，仲介人が X，Y の正当性を検証することによりこれらの攻撃は検出されるため，メッセージの完全性が保たれている．送信非拒否性，受信非拒否性はともに受領書によって保たれている．さらに，送信者はメッセージを送った後は仲介人に処理を任せるため，Send-and-Forget が可能である.

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：E_D(K, P_{SD}, S), E_K(R, 件名, H(em))

Y：E_D(L), E_L(P_{RD}, 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・受信者とも配達仲介人と秘密鍵を共有する必要があるため，全ユーザが本サービスへの前登録をする必要がある点である．Abadi らの方式では，送信者は受信者と共有し，受信者は仲介人と送信者の両方と共有する．よって，提案方式 1 と Abadi らの方式において，それぞれのパーティが所有すべき共有秘密鍵の数は**表 1** 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共有秘密鍵の数は Abadi らの方式よりも減らすことができ，送受信対象が増えたとしても共有秘密鍵を新たに用意する必要はない.

ただし，仲介人が管理すべき共有秘密鍵の数は，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数となり，用意すべき共有秘密鍵の数は増えている．よって，全ユーザ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，提案方式における仲介人の管理する共有秘密鍵の数は Abadi らの方式よりも特に多くなる．逆に全

表 1 それぞれのパーティが管理すべき共有秘密鍵数の比較
Table 1 Comparison of the number of shared secrets each party manages.

	送信者	受信者	配達仲介人
Abadi らの方式	受信相手数	送信相手数 仲介人数	全受信者数
提案方式 1	仲介人数	仲介人数	全利用者数

ユーザ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が少ない場合，提案方式と Abadi らの方式における仲介人の管理する共有秘密鍵の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は少ないと思われるため，提案方式での仲介人が共有秘密鍵を管理するためにかかるコストは，Abadi らの方式と大きな違いはない．

本方式では，認証やメッセージの暗号化を配達仲介人にすべて任せているため，送信者・受信者とも，仲介人を完全に信用する必要がある．仲介人が悪意を持っている場合，メッセージの盗聴・送信者/受信者への成りすまし・受領書の偽造などの攻撃が可能となっている．また，送信者/受信者と仲介人が共謀することにより，配達証明付き電子メールで最も重要な性質である公平性が崩されるという問題がある．

そこで，次節では PKI が整備されているという前提を置き，仲介人への依存を軽減した，提案方式 2 を説明する．

4.2 提案方式 2

提案方式 1 のような On-line プロトコルの場合，受信者は仲介人の助けを借りてセッション鍵 K を得るので，送信者の状況にかかわらずいつでも復号化することが可能である．ただし，仲介人が，受信者の要求に対応できない場合，プロトコルがまったく実行できないという問題がある．

一方，Optimistic プロトコルの場合，通常は送信者・受信者間のみで通信が行われるため，仲介人の状況にかかわらず利用が可能である（ただし，仲介人が利用可能になるまで問題解決はできない）．しかし，受信者がメッセージを読もうとしたときに送信者が対応できない状況では，プロトコルの実行ができないため，相手が対応できるようになるまで待つ必要がある[9),10)]．

これらのことより，受信者がメッセージを読もうとした時点の送信者または仲介人の状況次第により，適したプロトコルが変わることが分かる．よって，どちらのプロトコルを利用するかは受信者が判断すべきである．

本章では On-line プロトコルと Optimistic プロトコルの両方を備え，受信者がメッセージを読む時点の送信者や仲介人の状況により，どちらのプロトコルを利用するかを，受信者が決めることが可能な配達証明付き電子メールシステムを説明する．これにより，受信者は様々な状況に対応してメッセージを受け取ることが可能となる．

具体的には，送信者が最初に送る通信内容を，システム内で使用する On-line プロトコル・Optimistic プロトコルとも，同じ内容にすることにより，受信者がプロトコルを選択することが可能となる．また，どちらのプロトコルを利用したとしても同じ受領書を得ることができ，どちらのプロトコルも同じ程度の効率性を持つように設計する．これらの性質により，受信者は送信者・仲介人の対応状況のみを考慮に入れたうえで，プロトコルの選択が可能になる．

ユーザが Optimistic プロトコルを利用する場合は無料で配達証明付き電子メールが送れるが，On-line プロトコルを利用する場合はユーザに課金するようにする．これにより，送信者の対応を待つことなく，仲介人に残りの処理を任せたい受信者は On-line プロトコルを利用し，送信者に処理を任せた方が都合の良い場合は Optimistic プロトコルを利用するため，受信者が選択するプロトコルが分散される．これにより，仲介人への処理の集中による過剰な負荷を減らすことができる．

提案方式 2 でも提案方式 1 同様，送信者・受信者とも，仲介人にメール自体を送らないため，仲介人に対する通信量が少ない．また，メッセージを暗号化しているセッション鍵は，仲介人の公開鍵のほかに受信者の公開鍵でも暗号化しているため，仲介人に対してもメッセージの秘匿性が保たれている．また，提案方式 1 で最も防ぐべき攻撃の 1 つとして仲介人による受領書の偽造があるが，提案方式 2 では仲介人はどのような状況においても受領書の生成にかかわらないため，受領書の偽造を防ぐ ことが可能となっている．

4.2.1 準　　備

ここでは，提案方式 2 で用いられる仮定，記号について説明する．

仮定

送信者・受信者とも，自身の署名鍵を持っている．各パーティの公開鍵・署名検証鍵は誰でも手に入れることができる．

記号

M：メッセージ
件名：送信メッセージの内容を大まかに説明した文章
S，R，D：送信者/受信者/配達仲介人の ID 情報
K：セッション鍵
H(·)：ハッシュ関数
$E_K(\cdot)$：セッション鍵 K による共通鍵暗号
$E_R(\cdot)$，$E_D(\cdot)$：受信者/配達仲介人の公開鍵を用いた暗号化
$SIG_S(\cdot)$，$SIG_R(\cdot)$，$SIG_D(\cdot)$：送信者/受信者/配達仲介人による電子署名

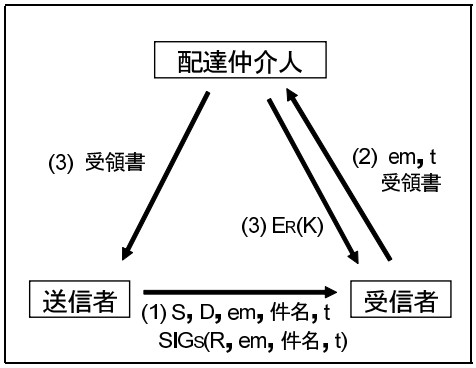

図 2 提案方式 2：On-line プロトコル
Fig. 2 Proposed Method 2: On-line protocol.

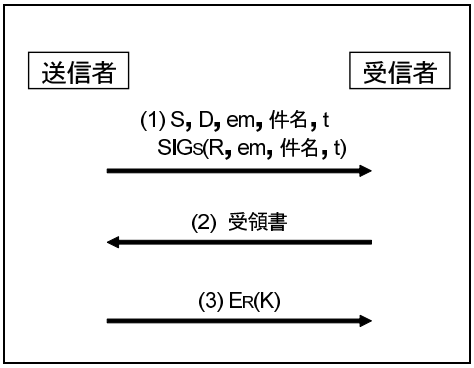

図 3 提案方式 2：Optimistic プロトコル
Fig. 3 Proposed Method 2: Optimistic protocol.

em：$E_K(M)$
t：$=E_D(S, R, E_R(K))$
受領書：$SIG_R(SIG_S(R, em, 件名, t))$

4.2.2 On-line プロトコル

ここでは提案方式 2 で使用する On-line プロトコルを説明する．

On-line プロトコルの具体的な手順は以下のとおり（**図 2** 参照）．

(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，D，em，件名，t，$SIG_S(R, em, 件名, t)$ を送信する．
(2) 受信者は送信者の署名を確かめる．正しければ，$SIG_S(R, em, 件名, t)$ に自分の署名を施し，em，t，受領書を配達仲介人に送信する．
(3) 配達仲介人は t を復号化し，受領書にある送信者・受信者の署名を確かめる．正しければ，$E_R(K)$ を受信者に送信する．さらに，受領書を送信者に送信する．

3 章で定義した性質について考察する．受信者はメッセージを読む場合，仲介人に受領書を送る必要があるため，公平性が保たれている．また，送信者・受信者は，電子署名による認証が行われる．メッセージを暗号化したセッション鍵 K は仲介人・受信者の公開鍵で暗号化されているため，仲介人を含む第三者から読まれることはない．メッセージを途中で書き換えた場合，電子署名を確認することにより，誰でも検出可能である．非拒否性は電子署名によって実現している．さらに，提案方式 1 同様，送信者はメッセージを送った後，仲介人に処理を任せるため，Send-and-Forget が可能である．

4.2.3 Optimistic プロトコル

ここでは提案方式 2 で使用する Optimistic プロトコルを説明する．

Optimistic プロトコルの具体的な手順は以下のとおり（**図 3** 参照）．

(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，D，em，件名，t，$SIG_S(R, em, 件名, t)$ を送信する．
(2) 受信者は送信者の署名を確かめる．正しければ，自分の署名を施し，受領書を送信者に送信する．
(3) 送信者は受領書の署名を確かめる．正しければ $E_R(K)$ を受信者に送信する．

また，受信者は Optimistic プロトコルが上手く実行できない場合，途中で On-line プロトコルに切り替えることも可能である．

3 章で定義した性質について考察する．認証・秘匿性・完全性・非拒否性については On-line プロトコルと同じく実現している．受信者がプロトコルを手順 (2) まで正しく行ったにもかかわらず，送信者が $E_R(K)$ を送ってこない場合，受信者は On-line プロトコルに方式を変更することが可能である．そのため，公平性が保たれている．ただし，送信者・受信者はそれぞれ通信を送った後，お互いの返事を待つ必要がある．そのため，Send-and-Forget は実現していない．

4.2.4 システム全体への考察

提案した On-line プロトコル・Optimistic プロトコルのそれぞれの方式で実行される最初の通信は，どちらのプロトコルも同じ内容である．本システムでは，送信者は配達証明付き電子メールを送信する場合，どちらのプロトコルを使用するか選択せず，最初の通信を受信者に送る．受信者はこの通信を受け取った後，そのときの仲介人や送信者，もしくは自分の状況を考慮に入れたうえで，どちらのプロトコルを使用するか受信者が選択できるシステムとなっている．

このシステムでユーザが利用できる 2 つのプロトコルの安全性は同じである．また，どちらのプロトコル

でも最終的に同じ受領書（$=SIG_R($ $SIG_S(R, em, 件名, t))$）を得ることができる．異なる点は仲介人の利用法・送信者が行う通信回数の違いのみである．さらに，プロトコルが途中で失敗した場合，受信者は別のプロトコルに変更することが可能である．よって提案システムでは，受信者は自身の要求や，送信者または仲介人の対応状況に応じてプロトコルを使い分けることができる．ただし，このシステムでは，送信者が最初の通信を送った時点では最終的に選択されるプロトコルを知ることができない．よって，2つのプロトコルを組み合わせた場合，Send-and-Forget を実現することはできない．

このとき，送信者・受信者にとっては On-line プロトコルの方が使いやすい方式であるため，On-line プロトコルに集中する危険がある．そこで，仲介人への過剰な負荷を避けるために，受信者が On-line プロトコルを利用する場合は課金することで，ユーザが分散し，仲介人への負荷を軽減させることができる．

4.3 提案方式のまとめ・比較

本論文では2つの配達証明付き電子メールシステムを提案した．提案方式1は共有秘密鍵を利用した拡張性の高い配達証明付き電子メール，提案方式2は配達仲介人や送信者の状況に合わせて，使用するプロトコルを受信者が決定することができる配達証明付き電子メールシステムとなっている．

提案方式1は PKI が整備されている必要がないが，提案方式2は PKI が整備されていることが前提である．提案方式1では仲介人単独によるメッセージの盗聴・送信者/受信者への成りすまし・受領書の偽造などを防ぐことができないが，提案方式2では電子署名・公開鍵暗号によりこれらの攻撃を防ぐことが可能である．また，提案方式1では仲介人にアクセスできない場合，まったくプロトコルを実行することができないが，提案方式2では，問題が起きない限り，2者間でプロトコルを実行することが可能である．

これらの性質から，それぞれの提案方式は使用に適した環境が異なる．提案方式1は，共有秘密鍵を利用した非常に単純なシステム構成となっているため，現在のプロバイダを用いたメールシステムに容易に組み込むことが可能である．一方，提案方式2では，仲介人の電子署名は用いずに，ユーザ自身の公開鍵や電子署名を用いることにより，仲介人が悪意を持っている場合でも受領書の偽造はできず，また認証や秘匿性，完全性，非拒否性を崩すことはできない．以上のことより，提案方式2は提案方式1よりも安全性が高い方式と考えることができる．すなわち，PKI が整備されておらず，ユーザは仲介人と秘密鍵を共有する方が実現しやすいのであれば提案方式1を選択し，すでに PKI が整備されている環境であれば提案方式2を選択する．また，どちらの環境とも実現されている場合，仲介人に対する依存の割合の違いが選択基準となる．依存の割合の観点から判断すると，提案方式2の方が優れていると考えられる．そのため，どちらの方式を利用するかについては，それぞれの前提条件の実現のしやすさと，仲介人への依存の割合を考慮に入れることが必要である．2つの提案方式の選択基準は**図4**のとおりである．また，受信者が仲介人の利用法を選択できるため，非常に実用的な方式となっている．

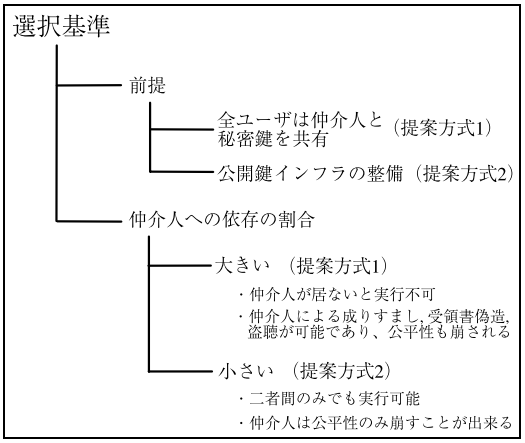

図4 提案方式の選択基準
Fig. 4 Criterions of choice for proposed systems.

ただし，これらの方式では仲介人と送信者/受信者が共謀した場合，プロトコルの公平性を崩すことが可能となっている．これらの問題に対する対処法としては，複数の配達仲介人を利用した，秘密分散共有が考えられる．ただし，この方式は効率性と安全性のトレードオフがあるため，どのように使用するかは送信するメッセージの重要性次第で決定することになる．

5. おわりに

本論文では2つの配達証明付き電子メールシステムを提案した．提案方式1は共有秘密鍵を利用した拡張性の高い配達証明付き電子メールシステム，提案方式2は配達仲介人や送信者の状況に合わせて，使用するプロトコルを受信者が決定することができる配達証明付き電子メールシステムとなっている．

今後はこれらのシステムを実システム（デジタルコンテンツの配布・オークション・選挙・カジノなど）への適用について考察する．また，配達仲介人の不正を効率良く防ぐ方式についても考察を行う．

参 考 文 献

1) Molnar, D.: Signing Electronic Contracts (Jan. 2001). http://www.acm.org/crossroads/xrds7-1/
2) http://www.certifiedemail.com/ (1998).
3) Ateniese, G., de Medeiros, B. and Goodrich, M.T.: TRICERT: A Distributed Certified E-Mail Scheme, *ISOC 2001 Network and Distributed System Security Symposium* (*NDSS '01*), San Diego, CA, USA (Feb. 2001).
4) Schneier, B. and Riordan, J.: A Certified E-Mail Protocol with No Trusted Third Party, *13th Annual Computer Security Applications Conference*, ACM Press (Dec. 1998).
5) Markle, R.: Secure Communications over insecure channels, *Comm. ACM*, Vol.21, pp.294–299 (Apr. 1978).
6) Abadi, M., Glew, N., Horne, B. and Pinkas, B.: Certified Email with a Light On-line Trusted Third Party: Design and Implementation, *WWW2002*, Honolulu, Hawaii, USA (May 7–11, 2002).
7) Kremer, S. and Markowitch, O.: Selective Receipt in Certified E-mail, *Progress in Cryptology — INDOCRYPT 2001 Second International Conference on Cryptology in India*, Chennai, India (Dec. 16–20, 2001).
8) Markowitch, O. and Kremer, S.: An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party, *4th International Conference* (*ISC2001*) (Oct. 1–3, 2001).
9) Ateniese, G. and Rotaru, C.N.: Stateless-Recipient Certified E-mail System based on Verifiable Encryption, Topics in Cryptology — CT-RSA 2002, Preneel, B. (Ed.), Lecture Notes in Computer Science, Vol.2271, pp.182–199, Springer-Verlag (Feb. 2002).
10) Asokan, N., Shoup, V. and Waidner, M.: Optimistic Fair Exchange of Digital Signatures, *Proc. EUROCRYPT '98* (1998).

(平成 14 年 11 月 29 日受付)
(平成 15 年 6 月 3 日採録)

今本 健二

2002 年九州大学工学部電気情報工学科卒業．同年より同大学大学院システム情報科学府情報工学専攻修士課程，現在に至る．既知共有鍵を用いた認証付き鍵交換，配達証明付き電子メールに関する研究に従事．電子情報通信学会会員．

櫻井 幸一（正会員）

1988 年九州大学大学院工学研究科応用物理専攻修士課程修了．同年三菱電機（株）入社．現在，九州大学大学院システム情報科学研究院情報工学部門教授．1997 年 9 月より 1 年間コロンビア大学計算機科学科客員研究員．2001 年 4 月より九州大学システム LSI 研究センター併任．暗号理論・情報セキュリティ・社会情報工学の研究に従事．博士（工学）．2000 年情報処理学会坂井特別記念賞受賞．2000 年情報処理学会論文賞受賞．電子情報通信学会，日本数学会，ACM 各会員．