マルチメディア通信と分散処理 30－7
（１９８６．７．２５）

電気通信における内容証明・配達証明サービスの研究動向

田中良明　内田孝則　秋山　稔
東京大学工学部

本稿では，電子メールにおける内容証明，配達証明の研究動向を紹介する．最近検討されている方式では，通信はいずれも調停者を介して行うものとしている．中尾の方式は，送信者の利益保護のための内容証明を実現する方式である．秋山・東・鳥居の方式は，受信者が，受取ったメッセージが正当なものであるかを確認するというメッセージ認証を実現する方式である．この方式は内容証明と配達証明を同時に実現する．受領印押捺後開封方式は，更に受信者による受領拒否の防止を含めた方式である．また，この方式では，通信終了後の調停者による情報保管を不要としている．

SURVEY OF THE DEVELOPMENTS OF CONTENTS AND DELIVERY CERTIFICATION SERVICE IN ELECTRONIC MAIL

Yoshiaki TANAKA, Takanori UCHIDA and Minoru AKIYAMA
Fuculty of Engineering, The University of Tokyo

The fundamental functions of contents and delivery service are to prevent the receiver's disavowal of the fact of receiving and to prevent the sender's disavowal of the fact of sending. These functions can be easily realized. But, the most important problem in contents and delivery certification service is the receiver's refusal to receive a mail. This problem is difficult to solve.

This paper surveys the recent progress in the research of this service.

1．まえがき

電子メールの発達により，従来郵便で行われてきた内容証明，配達証明のサービスを，電子メールにおいても行う必要が生じてきている[1],[2]．内容証明は，配達が行われなければ無意味であるので，通常，配達証明を伴って用いられる．現在，郵便で行われている内容証明，配達証明サービスでは，利用者が多いと通信業者のメッセージ保管量が膨大となる，通信業者の不正に対し無防備である，受信者の受領拒否に対抗できないなどの問題点がある．特に，受信者の受領拒否は，解決が容易でない問題である．これらの問題点は，電子メールにおいても同様に生ずるが，電子メールの場合は，暗号の利用による解決の道がある．

本稿では，この問題に関連して，まず２．で中尾の方式[1]，３．で秋山・東・鳥居らの方式[2]を簡単に紹介した後，４．で筆者らが提案している方式（受領印押捺後開封方式）を説明する．

なお通信を行う前に，公開鍵は公開ファイルに登録されており，秘密鍵は各人が秘密に保管しているものとする．

2．中尾の方式[1]

中尾の方式は，送信者が，いつ，どのような内容のメッセージを，誰が，誰に差し出したかを，中立の立場にある調停者が証明するための方式である．

2．1　方式の説明

方式を図１に示し，以下にその手順を述べる．ここでは送信者をユーザ，調停者をシステムと呼ぶことにする．

（１）ユーザ（A）は，メッセージ（M）（エンベロープ（E）とコンテント（C））をユーザの公開鍵K_{PA}で暗号化し，K_{SA}（M）をシステム（C）に送る．

（２）システムは以下のことを行う．

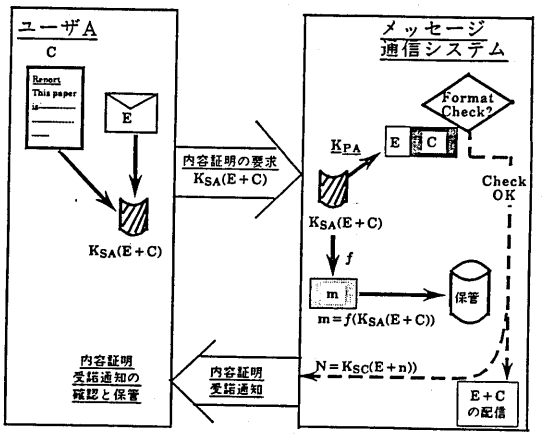
① ユーザから送られてきたK_{SA}（M）より，ユーザの公開鍵K_{PA}を用いてMを得る．

② M＝E＋Cのフォーマット・チェックを行う．このフォーマットが正しいことは，正当なユーザによるメッセージであることの証となる．

③ K_{SA}（M）をシステム固有の関数ｆを用いてダイジェスティブ情報（m＝ｆ（K_{SA}（M））を作成し，それをシステムに保管する．このことで，システムに保管する情報が少なくなると同時に，K_{SA}（M）はユーザしか作成できないため，システム内での改ざんを防止することもできる．

④ ユーザに内容証明受諾情報（N）を送る．Nはシステムのみが作成できる情報であり，エンベロープ（E）と内容証明受諾番号（n）をシステムの秘密鍵K_{SC}で暗号化したものである．

（３）ユーザは送られてきた内容証明受諾証明（N）をシステムの公開鍵K_{PC}で復号化し，自分の送ったエンベロープ（E）と一致することをチェックし，システムの正当性を確認する．また，照合のためには，受諾情報（N）を保管する．



K_{SA}: Aの秘密鍵　　f: メッセージ通信システム固有の秘密関数
K_{PA}: Aの公開鍵
K_{SC}: システムの秘密鍵　　N: 内容証明受諾情報
K_{PC}: システムの公開鍵　　n: 内容証明受諾番号

図１　内容証明要求／受諾

2．2　内容照合手順

内容照合手順を図２に示し，それを以下に述べる．

（１）ユーザはK_{SA}（M）と受諾情報（N）をシステムに送る．

（２）システムでは以下のことを行う．

① 内容証明受諾証明（N）をシステムの公開鍵K_{PC}で復号化し，Nの正当性を確認する．またNの中のｎを頼りに，保管情報mを引き出す．

② ユーザから送られてきたK_{SA}（M）をシステム固有の関数ｆでｍ＝ｆ（K_{SA}（M））を作成する．

③ 上記①と②のｍを比較し，等しい場合はユーザに内容照合証明書（Ｉ＝K_{SC}（M＋ｉ）を送る．Ｉは照合証明情報（ｉ），メッセージ（M）によって構成され，システムの秘密鍵K_{SC}で暗号化されているので，システム以外のものによる偽造は不可能である．

④ ユーザは送られてきた内容照合証明書Ｉをシステムの公開鍵K_{PC}で復号し，システムと情報Ｉの正当性をチェックし，Ｉを保管する．

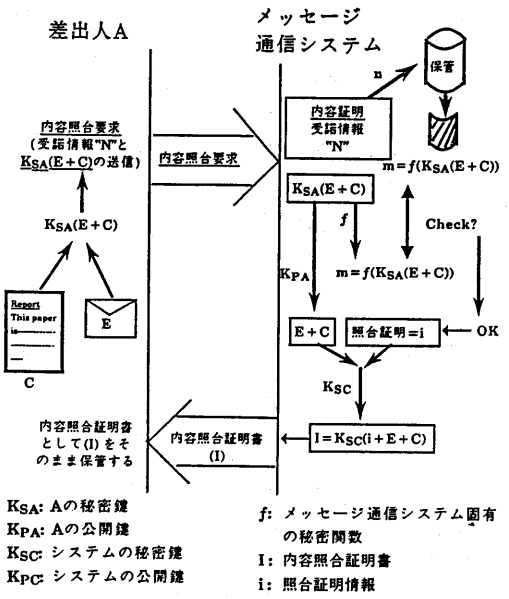


図２　内容照合手順

２．３　まとめ

中尾の方式は，基本的には現在郵便で行われている内容証明サービスと同じである．システムが保管する情報量をダイジェスティブ関数を用いて圧縮しているので，全部保管するよりは保管量が少なくなっている．メッセージMの内容はシステムに対し，秘密の扱いにはなっていない．また，配達および配達証明については従来の方式をとっている．

３．秋山・東・鳥居の方式[2]

秋山・東・鳥居の方式は，受信者の受け取ったメッセージが正当なものであるか（送信者が送ったメッセージと同じであるか，つまりメッセージ認証）を実現する方式である．

３．１　方式の説明

方式を図３に示し，その手順を以下に述べる．ここでは，送信者をＡ，受信者をＢ，調停者をＳとおく．また，公開鍵配送方式（ＰＫＤＳ）を用い，通信は共通鍵で行う．

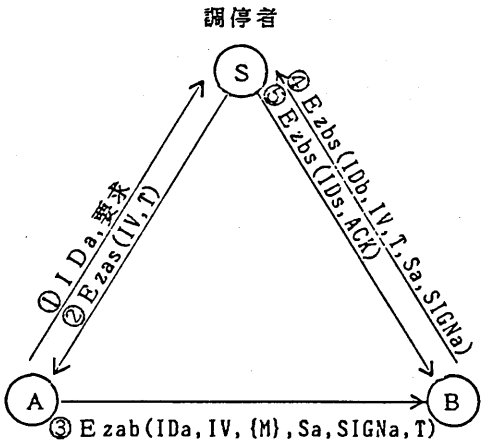
（１）ＡはＳに対し，Ａの識別コードＩＤ$_a$と認証スタンプＴの発行要求を通知する．

（２）ＳはＡがメッセージ（Ｍ）の初期値ＩＶとＳの時刻付認証スタンプＴをＡＳ間の共通鍵Z_{as}で暗号化してＡへ送る．

（３）ＡはＳよりの電文を復号化し，ＩＶとＴを得る．このＩＶをメッセージの初期値としてＭをハッシング処理し認証子S_aを作り，ＩＤ$_a$，ＩＶ，Ｍ，S_a，ＳＩＧＮ$_a$，Ｔをまとめて ＡＢ間の共通鍵Z_{ab}で暗号化してＢへ送る．ただし，ＳＩＧＮ$_a$はＩＶ，Ｔ，S_aをＡＳ間の共通鍵Z_{as}で暗号化したものである．

（４）ＢはＭ，S_a，Ｔを保管し，次にＩＤ$_b$，ＩＶ，Ｔ，S_a，ＳＩＧＮ$_a$をＳＢ間の共通鍵Z_{bs}で暗号化してＳへ送る．

（５）Ｓは送られてきたＩＶとＴが（１）で発行したものと同一であり，さらにＳＩＧＮ$_a$を復号化して得られたＩＶ，Ｔと一致することもチェックする．次に送られてきたS_aが，ＳＩＧＮ$_a$を復号化して得られたS_aと同じで



$E_{Zxy}(Q)$：Ｘ，Ｙの共通鍵Z_{xy}によるＱの暗号化

図３　メッセージ認証プロトコル

あることを確認し，その事実を保管する．その後，ID_sとACK信号をBS間の共通鍵Z_{bs}で暗号化してBへ送る．

（6）BはACK信号を受取ることにより，Aから送られてきたメッセージが正当なものであることを知る．

後日，受信者はACK信号を調停者に提出することにより，メッセージの内容証明を受けられる．

3．2　まとめ

秋山・東・鳥居の方式は，調停者がACKを発行したという事実の保管することで，内容証明と配達証明を同時に実現している．しかし，この方式でも，調停者が保管しなければならない情報が存在する．その他にメッセージの内容によって，受領拒否が可能であるという問題がある．つまり，送信者から電文を受取った段階で，受信者はメッセージMの内容を知ることができる（Mは暗号化されていない）ので，もし，その内容が受信者にとって不都合なものであれば，受信者はメッセージ認証を行わないことがある．この場合は，内容証明，配達証明ともに実現できない．

4．受領印押捺後開封方式[3]

4．1　内容証明・配達証明サービスの内容と問題点

従来の電子メールにおける内容証明・配達証明サービスでは，受信者が電子メールを読み出すことをもって配達が実行されたとし，送信者に配達通知するというものが多い．つまり，電子メールを正当な受信者が確実に受取ったことを確認する代わりに，電子メールを読み出す受取人の正当性をシステムへのログ・オン時にパスワード等を用いて確認することで済ませている．これでは，受取人の正当性を確認したにすぎず，受取人の受領を確認したことにはならない．さらに，システム提供者の不正に対しては，無防備である．

受信者が，受取ったメッセージにディジタル署名を施して返送することにすれば，受領の証明，内容の証明が共に可能となる．しかし，受信者が受取りたくないメッセージにディジタル署名しないということもありうる．この受信者による受領拒否は，内容証明・配達証明サービスの最大の問題点であるといえる．

4．2　前提条件

ここでは，内容証明・配達証明サービスの検討に当たって，次のような前提条件を置くものとする．

（a）送信者と受信者の間に調停者を置き，送信者，受信者は調停者を介して通信を行う．調停者を仲介させるのは，送信者受信者間の直接通信では，受領拒否を防止できないためである．

（b）送信者，受信者及び調停者はそれぞれ複数いるものとし，任意の送信者，受信者が，任意の調停者を介して通信できる．

（c）送信者，受信者，調停者，その他の第三者のいずれも不正を行う可能性がある．

（d）誰でも盗聴を行うことができる．

（e）誰でもメールを送ることができる．

（f）通信に用いられる暗号の強度は十分であり，鍵の管理は万全である．

（g）通信の秘密はできるだけ確保する．

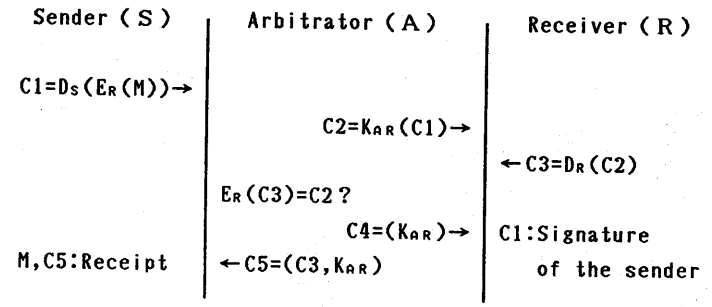
（h）調停者が記憶しなければならない情報はできるだけ少なくする．

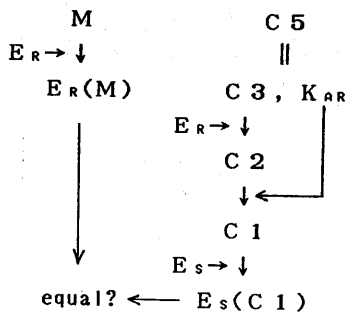
4．3　方式の原理

現在筆者らが提案している受領印押捺後開封方式の基本原理を説明する．ただし，日付時刻を含めると説明が複雑になるので，まずここでは，それを除いた方式について説明する．図4に，方式の基本原理を示す．

通信に先立ち，送信者（sender，S），受信者（receiver，R）と調停者（arbitrator，A）は，公開鍵暗号系の暗号化鍵E_X（X=S,R,A）及び復号化鍵D_Xを作成し，暗号化鍵E_Xは公開ファイルに登録し，復号化鍵D_Xは各自が秘密に保管する．但し，図4の基本原理では，簡単にするため，E_A，D_Aは用いていない．ここで，Xの公開鍵E_Xによる文Qの暗号化をE_X（Q），Xの秘密鍵D_Xによる文Qの復号化または文Qへの署名をD_X（Q），XとYの間の共通鍵K_{XY}による文Qの暗号化をK_{XY}（Q）と表すことにする．但し，X，Yは，S，A，Rのいずれかである．

まず，送信者は，メッセージ（message，M）を受信者の公開の暗号化鍵E_Rで暗号化し，さらに自分の秘密の復号化鍵D_Sで署名したものを調





M:Message(Plain text)
Ex(Q):Encryption of text Q by X's public key Ex
Dx(Q):Decryption of text Q or signature for text Q by X's secret key Dx
Kxy(Q):Encryption of text Q by common key Kxy of X and Y
X,Y=S,A,R

図5　受信者の否定に対する判定方法

図4　受領印押捺後開封方式の基本原理

停者に送る．次に，調停者は，それを受信者が知らない暗号化鍵K_{AR}で暗号化して受信者に送る．この暗号は共通鍵暗号[4]でよい．この段階では，受信者はK_{AR}を知らないので，メッセージを読むこと，すなわち開封はできない．また，メッセージの送信者が誰であるかも分からない．次に，受信者は，暗号文に秘密の復号化鍵D_Rでディジタル署名して調停者に返す．これが受領印（receipt）となる．調停者は，送った暗号文に署名がなされていることを確認した後，受信者に鍵K_{AR}を送る．受信者は，その鍵でメッセージを読むこと，すなわち開封ができる．そのメッセージには送信者の署名（signature）が付いている．調停者は，さらに，鍵K_{AR}と受信者から来たディジタル署名を送信者に送る．これをメッセージMと組合せることによって内容証明書兼配達証明書となる．

もっとも，受領印を必要とするメールは督促状など受取りたくないものであることが多いので，受信者は，送信者や内容が分からないようにしてあっても受領を拒否することも考えられる．それに対しては，調停者である通信業者が，配達証明を必要としない通常のメールに対しても時々受領印をもらうという方法で対抗可能である．

後日紛争が起こったときは，次のようにして解決される．

（a）受信者が受信の事実または受信文の内容を否定したとき，送信者は判定者にMとC5を提出する．判定者は図5の手順に従ってどちらの言い分が正しいか判定する．

（b）送信者が送信の事実または送信文の内容を否定したとき，受信者は判定者にMとC1を提出する．C1は送信者のディジタル署名であるから，判定者は容易にどちらの言い分が正しいか判定できる．

4．4　基本方式の構成と手順

4．3の基本原理を実際に適用する場合の最も基本的な方式を，基本方式と呼ぶことにし，その手順を詳しく述べる．ここでは，日付時刻も含めて説明する．また，ディジタル署名には通信文復元法を用いることにする．

図6に基本方式を示す．手順は，以下のとおりである．

（a）送信者

① 送りたいメッセージに，送信者，調停者，受信者の識別番号（S-ID,A-ID,R-ID）を加えたものをMとする．

② Mを受信者の公開鍵E_Rで暗号化し，現在の時刻T_sを加え，まとめて秘密鍵D_sで署名し，C1とする．

③ C1に，S-ID,A-IDと調停者の公開鍵E_Aで暗号化したR-IDを加え，まとめて秘密鍵D_sで署名し，C2とする．

④ C2にS-ID,A-IDを付けて調停者に送る．

（b）調停者

① 送信者から送られてきたC2を送信者の公開鍵E_sで復号化し，IDが一致すること

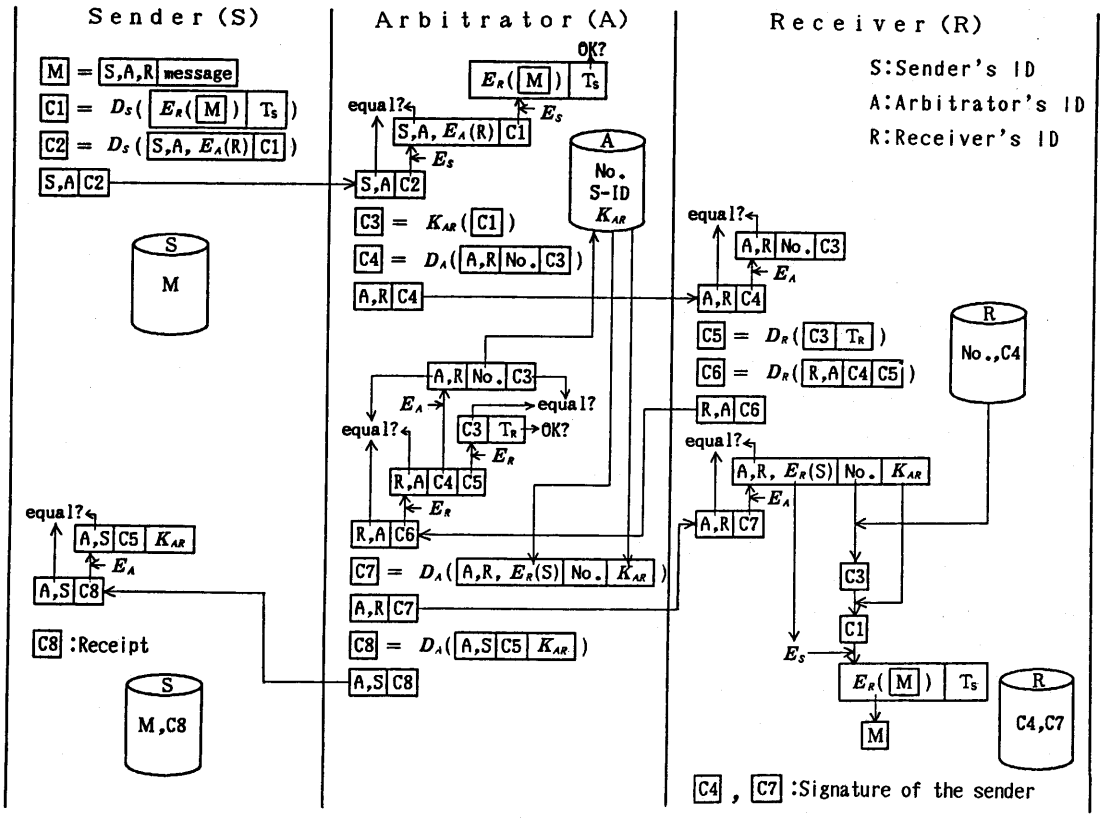


図６　基本方式

を確かめる．また，TSが正しいことを確かめる．

② 任意に鍵KARを発生し，受付番号（No.），S-IDと共に記憶する．

③ Ｃ１をKARで暗号化し，Ｃ３とする．

④ Ｃ３にA-ID,R-ID,No.を加え，まとめて秘密鍵DAで署名し，Ｃ４とする．

⑤ Ｃ４にA-ID,R-IDを付けて受信者に送る．

（ｃ）受信者

① 調停者から送られてきたＣ４を調停者の公開鍵EAで復号化し，ＩＤが一致することを確かめる．

② Ｃ３に現在の時刻TRを加え，まとめて秘密鍵DRで署名する．

③ Ｃ４，Ｃ５にR-ID,A-IDを加え，まとめて秘密鍵DRで署名し，Ｃ６とする．

④ Ｃ６にR-ID,A-IDを付けて受信者に送る．

（ｄ）調停者

① 受信者から送られてきたＣ６を受信者の公開鍵ERで復号化し，ＩＤが一致することを確かめる．また，Ｃ４，Ｃ５をそれぞれ調停者の公開鍵EA，受信者の公開鍵ERで復号化し，Ｃ３が改ざんされていないことを確認する．さらにTRが正しいことを調べる．

② Ｃ４の復号文の中のNo.からS-IDとKARを取り出す．No.とKARにA-ID,R-IDと受信者の公開鍵ERで暗号化したS-IDを加え，まとめて秘密鍵DAで署名し，Ｃ７とする．

③ Ｃ７にA-ID,R-IDを付けて受信者に送る．

④ Ｃ５とKARにA-ID,S-IDを加え，まとめて秘密鍵DAで署名し，Ｃ８とする．

⑤ Ｃ８にA-ID,S-IDを付けて送信者に送る．

（ｅ）受信者

① 調停者から送られてきたＣ７を調停者の公開鍵EAで復号化し，ＩＤが一致することを確かめる．

② No.からＣ３を取り出し，KARで復号化し，Ｃ１を得る．ER（S-ID）を秘密鍵DRで復号化して S-IDを知り，送信者の公開

鍵E_SでC１を復号化する．最後に，E_R（M）を秘密鍵D_Rで復号化し，Mを得る．紛争が起こったときのために，C４とC７が送信者の署名文であることを確認した後，保管する．確認方法は，４．６で述べる．

（ｆ）送信者

① 調停者から送られてきたC８を調停者の公開鍵E_aで復号化し，ＩＤが一致することを確かめる．紛争が起こったときのために，C８が受信者の受領印であることを確認した後，保管する．確認方法は，やはり４．６で述べる．

サービス終了後，調停者はこの通信に関するすべての情報を削除できる．

４．５ 長文用方式

基本方式において，公開鍵暗号系として例えばＲＳＡ法[4]を用いると，ｎ（法の公開鍵）未満のメッセージしか暗号化，復号化ができない．従って，長文の場合には，メッセージを分割する必要がある．また，受領印の長さが元のメッセージ以上であるのも，通信量の点で問題である．これらを改良した方式が長文用方式である．

長文用方式の基本方式からの変更点は，次のとおりである．

（ａ）送信者，受信者がそれぞれ署名文，受領印を作成する際，文を公開圧縮関数Ｈを用いて圧縮したものに署名する．圧縮関数の値域をｎ未満に定めるとメッセージを分割せずに一度で署名できる．そのため，分割の必要がなくなる．

（ｂ）送信者がメッセージを送る際は，メッセージ自体は共通鍵暗号で暗号化し，その鍵は受信者の公開の暗号化鍵E_Rで暗号化し配送する．つまり，メッセージをM，共通鍵をK_{SR}で表すと，まず送信者は調停者にK_{SR}（M）とE_R（K_{SR}）を送る．次に調停者はE_R（K_{SR}）は保管しておき，K_{SR}（M）を受信者に送る．さらに調停者は，受信者からの受領印を受取った後，受信者にE_R（K_{SR}）を送る．メッセージが長くても，共通鍵暗号だから変換速度が速い．

（ｃ）署名通信では，認証子照合法[5]を用いる．圧縮関数として（ｂ）と同じものを用いると，認証子の作成も一度の署名でできる．

４．６ 安全性

不正行為には第三者による不正，送信者による不正，受信者による不正，及び調停者による不正がある．

受信者による受信の事実の否定という不正行為は，送信者が受信者の受領印を保管していることにより防止される．基本方式では，送信者は判定者にMとC８を提出し，判定者は図７の手続きによって判定する．

また，送信者による送信の事実の否定という不正行為は，受信者が署名文を保管していることにより防止される．基本方式では，受信者は判定者にM，C４とC７を提出し，判定者は図８の手続きによって判定する．

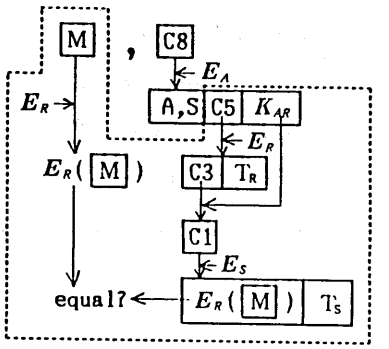


図７ 基本方式における
受信者の否定に対する判定方法

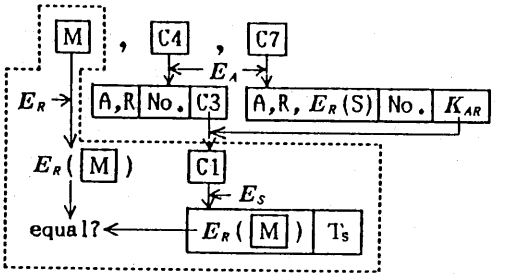


図８ 基本方式における
送信者の否定に対する判定方法

これらの不正も含めて，不正行為とその防止手段をまとめて表１に示す．

なお，長文用方式で導入した圧縮関数に関しても不正が考えられるが[5]，詳細は省略する．

表1　不正行為とその防止手段

	不正行為	防止手段
第三者	送信者，受信者，あるいは調停者と偽って送受信	送信者ー調停者，調停者ー受信者間の署名通信
	送信者から調停者への通信文のコピー再送	調停者がT_Sを確認
	送信者から受信者へのメッセージの解読	送信者ー受信者間の秘密通信
送信者	不正な時刻T_Sを付ける	調停者がT_Sを確認
	送信の事実の否定	受信者が署名文を保管
	受領印（送信内容）の偽造	受信者のディジタル署名
受信者	受信者の通信文の受領拒否	開封するまで送信者と内容がわからない
	不正な時刻T_Rを付ける	調停者がT_Rを確認
	受信の事実の否定	送信者が受領印を保管
	署名文（受信内容）の偽造	送信者のディジタル署名
調停者	送信者から受信者へのメッセージの解読	送信者ー受信者間の秘密通信
	別の内容の通信文を転送する	送信者，受信者のディジタル署名
	受信者に別の鍵を送る	鍵が異なると復号化したとき意味不明の文となり不正が検出される

4．7　まとめ

本方式では，受信者による受信事実の否定や送信者による送信事実の否定という紛争時に，正しい判定を行うことが可能である．また，配達証明の最大の問題点である受信者による受領拒否も防止できる．さらに，基本方式の変形として，メッセージが長い場合に通信量の節約になる長文用方式，調停者が一時的に記憶することにより通信量を減少させることができる調停者一時記憶方式，通信に調停者が介入したことを残しておく必要がない場合の調停者名無記録方式を提案した．これらの変形方式は，場合に応じ任意に組合せることも可能である．

5．むすび

本稿では，電子メールにおける内容証明・配達証明サービスの研究動向を紹介した．電気通信の発展に伴い，より一層の研究が必要であろう．

文　献

(1)中尾康二：”メッセージ内容証明サービスにおける暗号の適用”,第２回暗号と情報セキュリティ（ＣＩＳ）研究会(1985-02).

(2)秋山，東，鳥居：”ディジタル調停署名の一方式”，暗号と情報セキュリティシンポジウム，Ｃ１(1986-02).

(3)田中，内田，秋山：”暗号を用いた内容証明・配達証明サービス”，信学技報，IN86(1986-07).

(4)R.L.Rivest, A.Shamir, L.Adleman: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Commum. ACM, 21, 2 (Feb. 1978).

(5)D.W.Davies: "Applying the RSA Digital Signature to Electronic Mail", IEEE Computer, 16, 2, pp.55-62 (Feb. 1983).