# 電子郵便サービス
## ――インターネット時代の新しい郵便サービス

# Digital Postal Service
## ――New Postal Service of Internet Age

三ツ矢　裕一

**要　約**　平成 13 年 4 月に施行された IT 書面一括法と 2003 年度に実施される郵政事業の公社化は，現在の郵便事業の構造改革を促進する出来事である．日本ユニシスも 2000 年 2 月 1 日からサービスを開始したハイブリッドめーるサービスの構築および運用に携わっている関係から，これらの動きに対応すべく，新しい郵便サービスとして電子郵便サービスの検討を開始した．本稿では，これらの二つの出来事が郵便事業に与えた影響とそれに対応する電子郵便サービスの必要性および機能について紹介する．また，このサービスを構築するための要素技術である，通信文同一性保証と電子消印についても紹介する．

**Abstract**　IT Comprehensive Law enforced in April 2001 and the transfer of government-owned Postal Service into the public corporation to be scheduled in April 2003 is landmark event that promotes the structural reform of a current Postal Services. Nihon Unisys began study of the digital postal services, as a new style of postal services because we have been operating Hybrid Mail Service since February 2000, and our concern is how Hybrid Mail Service will be changed after 2003.

This paper discusses the possible influences on the current postal services resulted from above event, and the requirements and functionalities of the future postal services to counter it, and also introduces the technological elements used to build this digital postal services, such as the digital signature, digital certificates, and the identity assurance of transferred messages.

## 1. はじめに

インターネットの急速な普及とともに，より低コスト，より簡便さを求める企業によって，ビジネス文書の交換や商取引の決済等をインターネット上で行うことが徐々に始まってきている．また，これらのサービスを享受している利用者は何の不安も抱かずに利用している．一方では，インターネットという管理者のいない非常に不安定で，セキュリティに問題があり，送信したものが相手に届いたかどうか分からない環境での商取引文書の交換を行うことに不安を持っている企業，利用者がいることも事実である．そのため，機密性が高い文書の送信に関しては，いまだに既存の郵送という手段（書留や配達証明）を用いざるを得ない状況である．しかし，2001 年 4 月から施行された「書面の公布等に関する情報通信技術の利用のための関係法律の整備に関する法律（以降 IT 書面一括法）」によって，電子的な情報でも書面としての有効性を法律上認めることになったことから，インターネット上で機密性が高いビジネス文書の送受信要求が高まってきている．

このように，ビジネス文書の交換が紙媒体から電子媒体へと変化しているなか，郵政事業庁（旧郵政省）は，すでに三つの電子的郵便サービス（①コンピュータ郵便サ

ービス　②ハイブリッドめーるサービス　③e-内容証明サービス）を開始している．しかし，2003 年度の郵政事業の公社化に向けて，新たな郵便事業の検討を始めていることが各種メディアや郵政事業庁のホームページ上でも報じられている．この検討の中に，当然これらの三つのサービスをどのように統廃合してサービスの拡張を行うかについても含まれていることは想像に難くない．

一方，IT 技術に注目すると，電子署名による改ざん防止，原本保証技術，電子消印等の実装技術の進歩も目覚ましく，また PC の能力の向上によって，今までは机上の空論的な技術が家庭にある PC 上でも問題なく実装できる環境が整ってきた．

本稿は，これらの環境の変化に対応すべく，今後の郵便事業ビジネスにおける新しい郵便サービス，「電子郵便サービス」の仕組み，構築に向けての要素技術等について，日本ユニシス（以下，当社）の提案内容を紹介するものである．

## 2. 郵便事業の構造改革

具体的な電子郵便サービスの内容は，3 章で述べることとし，ここでは郵便事業の構造改革を引き起こすような二つのトピックスについて，その内容と郵便事業への影響について述べる．

### 2.1 IT 書面一括法の施行

まず，第一は，2002 年に旧通商産業省が示した「IT 書面一括法」である．この法律改正の趣旨は以下のとおりであり，この法律は，2001 年 4 月 1 日から施行されている．

1） 経済の IT 化が進展する中で，書面の交付あるいは書面による手続きを義務付けている規制が電子商取引等の阻害要因になっていることの見直し．
2） 民ー民間の書面の交付あるいは書面による手続き義務につき，従来の手続きに加え，電子的手段を容認すること．
3） 送信者側も受信者側も「電子的手段」の方が望ましいと判断する場合に限り，その選択肢を与えるもの．

これらの趣旨にしたがって，民ー民間の書面の交付あるいは書面による手続きを義務付けている諸法律が改正された．

例えば，図 1 や図 2 で示したような場合にも，書面の代わりに電子メール等の電子的手段によって行えるようになった．

従来，図 1 および図 2 の例では『紙媒体』での交付を前提にしてきたが，この IT 書面一括法の施行により『電子媒体』での交付（電子交付）も可能になった．例えば投資信託の販売会社や運用会社は大量の目論見書や取引報告書の作成・印刷・配布に大きな手間とコストをかけてきたが，電子交付によってコスト軽減を図ることが可能になる．また，利用者にとっても時間とコストの削減につながり，効率性，利便性が向上することが期待できる．

この様に，電子交付は企業・利用者の双方にとってメリットばかりがあるように思えるが，電子交付に問題が無いわけではなかった．最大の問題は，電子交付することの定義が「当該顧客の使用に係る電子計算機に備えられたファイルに記録する方法」となっている点である．つまり，投資信託の販売会社等は顧客に交付した電子媒体で

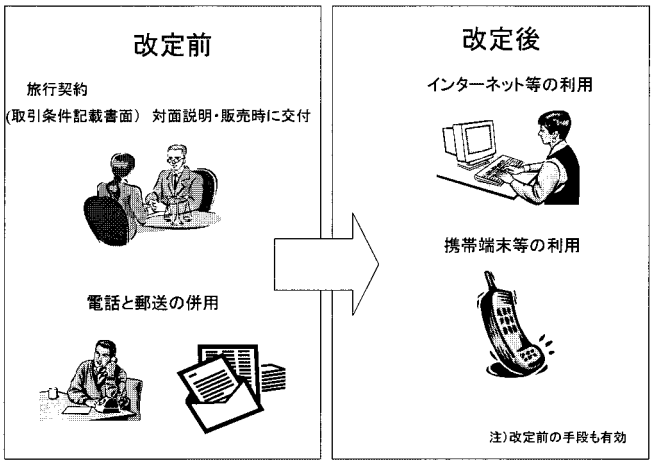



**図 1　旅行契約の取引条件書等の交付**

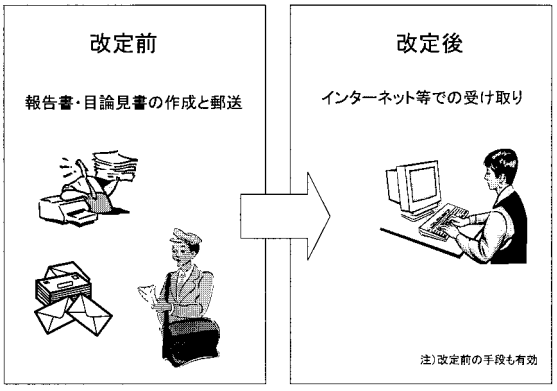



**図 2　目論見書や取引報告書の交付**

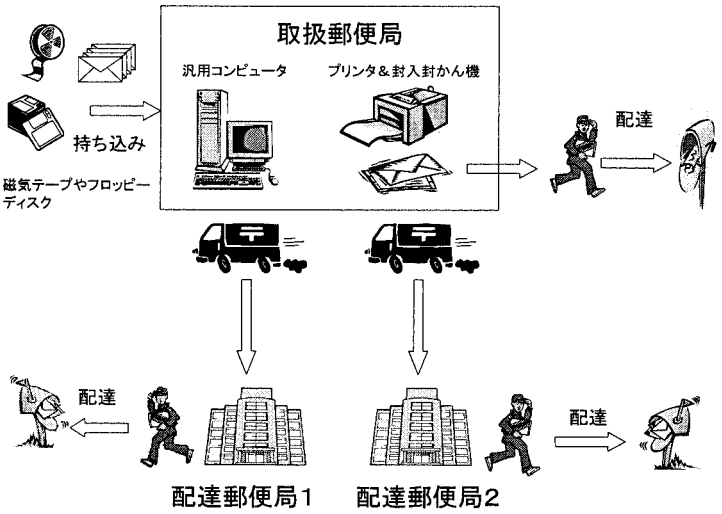
の書類（ファイル）が確実に到達し，かつ保存されたことを確認する義務を負う必要がでてきたことである．今までは，郵送であれば郵便局に持ち込むことによって責任を達成したことと比べると責任範囲が明らかに拡大されている．具体的な例をあげると，例えばホームページ上で目論見書や取引報告書の PDF ファイル等を表示しただけでは「閲覧」にとどまり，「交付」にはならないことを意味する．「交付」とするためには，そのファイルがダウンロードされて顧客のパソコンのディスクに保存されたことを確認して始めて「交付」となる．この確認方法が低コストで簡便な方法で実現されない限り電子交付の急速な普及は難しい．また，この状況は，郵政事業庁にとっては従来の紙媒体での交付から電子媒体での交付への移行によって，郵便利用率が下がることが予想されることから全くの逆風である．しかし，この問題を解決することが可能であれば，逆にこの逆風を順風に変えられる可能性がでてきた．

## 2.2　現行郵政事業庁の電子的郵便サービス

そして，第二は，2003 年度に実施される郵政事業の公社化である．各種メディアから，公社化に向けて総務省が郵政事業についての見直しを開始したことや，郵政事業庁のホームページ上でもその内容について徐々に明らかになってきた．当然，採算性・効率性の観点から現在郵政事業庁が実施している三つの電子的郵便サービスについても見直しがされることは明白である．そこで，当社では，これら三つのサービスの問題点を明らかにし，その問題点をクリアできる新しいサービスの検討を開始した．

### 2.2.1　コンピュータ郵便サービス

コンピュータ郵便は，1985 年に郵政省が初めて開始した電子的郵便サービスである．図 3 にコンピュータ郵便での通信文の流れを示している．




① 差出人は特定のフォーマットで記録した磁気テープもしくはフロッピーディスクを取扱郵便局へ持ち込む．

② 磁気テープとフロッピーディスクを引き受ける郵便局は，日本橋郵便局，大阪中央郵便局，名古屋中郵便局の 3 局．フロッピーディスクのみを引き受ける郵便局は，芝郵便局，上野郵便局，新宿郵便局，豊島郵便局，大阪東郵便局の 6 局．

③ もしくは，差出人はインターネットやパソコン通信で通信文を申し込む．

④ 同封物を事前に取扱郵便局に持ち込むことによって同封することができる．

⑤ 取り扱い郵便局で印刷し封入封かんし，配達する．

**図 3　コンピュータ郵便の通信文の流れ**

なお，コンピュータ郵便には以下の問題があると考えられる．

① 汎用コンピュータで構築されているため，プリンタ等の拡張性が低い．

② 大量印刷のデータは，磁気テープ，MD，FD を特定の郵便局に持参しなければならない．

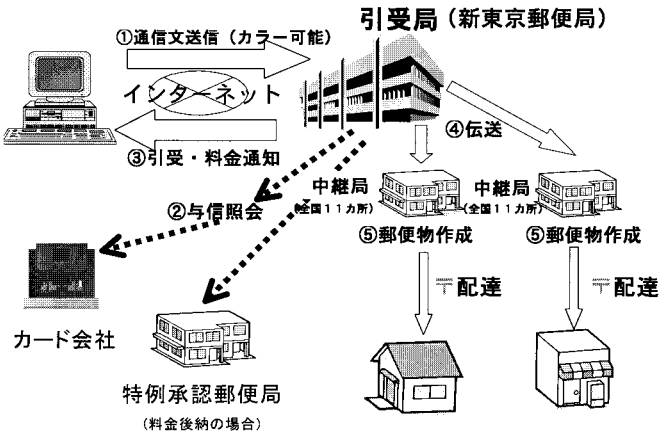
③ 利用者は，磁気テープや FD に印刷データを書き込む時に，コンピュータ郵

便サービス専用のソフトウェアを使用する．そのため，WORD や EXCEL といった文書ファイルを直接扱うことや画像データの印刷ができない．

④　印刷枚数が 2 枚までと少ない．

### 2.2.2　ハイブリッドめーるサービス（www.hybridmail.go.jp）

このサービスは 2000 年 2 月 1 日から開始された．当社はこのサービスの当初からの提案ベンダーであり，現在の運用に携わっている．図 4 に実際の通信文の流れを示すとともに，サービスの特徴，指摘されている問題について記す．




① 差出人は，パソコンからインターネット経由で，このサービスのホームページ（www.hybridmail.go.jp）を通して通信文を送信することができる．
② 料金支払いのため，引受け局ではリアルタイムでクレジットカードの与信を実施する．また，事前に特例承認郵便局での許可を受けていれば郵便口座もしくは銀行口座からの振り替えでの支払いが可能．
③ 与信が完了後，料金と引受け完了通知が差出人に通知される．
④ 引受け局は，宛先の郵便番号によって，全国 11 カ所の中継郵便局に配信する．中継郵便局は，札幌中央，仙台中央，さいたま新都心，長野東，金沢中央，名古屋郵便集中，　新大阪，広島中央，高松南，久留米東，那覇中央の１１局．
⑤ 中継局では，通信文を印刷し，専用封筒に封入封緘し，通常の郵便物配達ルートによって配達する．
⑥ 利用者は，差し出した郵便物が中継局に届いたことと封入封緘されたことをホームページから確認することができる．

**図 4　ハイブリッドめーるの通信文の流れ**

1）　サービスの特徴

①　通信文として PC 上で作成した文書ファイル（WORD や EXCEL 等）を送信することができる．

②　通信文を直接ホームページから入力することで通信文の作成も可能．

③　カラー印刷が可能．

④　クレジット決済もしくは郵便料金後納を利用できる．

⑤　同報差出（500 差出）が可能．

2)　ハイブリッドめーるで指摘されている問題点

①　本設計構想が同報通信のため，同一差出人で内容が異なる大量発信には対応できない．

②　通信枚数の最大が 2 枚と少ない

③　ダイレクトメールとして差し出された場合，地方局に集中するケースが多い．決して，全国に分散されることはない．地方局での印刷能力が低い．

④　中小企業がダイレクトメールとして利用するには一度の受付単位が 500 宛先は少ないといわれている．

### 2.2.3　e-内容証明サービス（www 3.hybridmail.go.jp）

e-内容証明サービスとは，現行の内容証明郵便を電子化し，インターネットを通じて 24 時間受付けを行うサービスである．差出人から送信された電子内容証明文書を郵便局の電子内容証明システムにて受付ける．その後，電子内容証明の証明文，日付印を文書内に挿入し，差出人宛て謄本，受取人宛て原本を自動印刷する．印刷時には文書が確実にプリントアウトされていることを再電子化してオリジナル電子文書とつき合わせることにより確認し，自動封入封かんを行い郵便物として発送するサービスである．このサービスは，2001 年 2 月 1 日から開始されている．

通信文の流れを図 5 で示す．

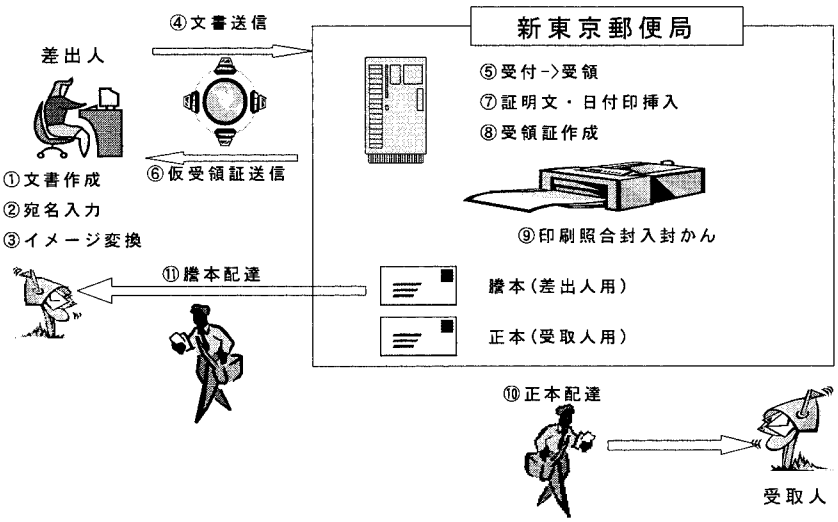



**図 5　e-内容証明サービスの通信文の流れ**

これらの三つの電子的郵便サービスのうち，コンピュータ郵便とハイブリッドめーるサービスとではサービス内容に重複する部分が多いことがわかっている．そして，コンピュータ郵便サービスをオープン化することによって経費削減と利用者拡大になると考えられる．

また，利用者からは，郵政事業庁が提供しているインターネットを利用したサービスにも関わらず，ハイブリッドめーると e-内容証明を利用するのに個別の利用申請が必要となることで利便性が損なわれているといった意見も聞かれる．この問題は，

単にこの二つのサービスだけではなく，郵政事業庁の全てのサービスにおいても同じ事がいえる．今後の郵政事業庁のインターネットを利用したサービスを何らかの形で一本化する必要がある．

### 2.3 郵便サービスと電子化の範囲

現在の郵政事業庁でサービスしている郵便業務のうち，これらの三つのサービスでカバーされるのは，通常郵便と内容証明郵便の一部である（図 6）．

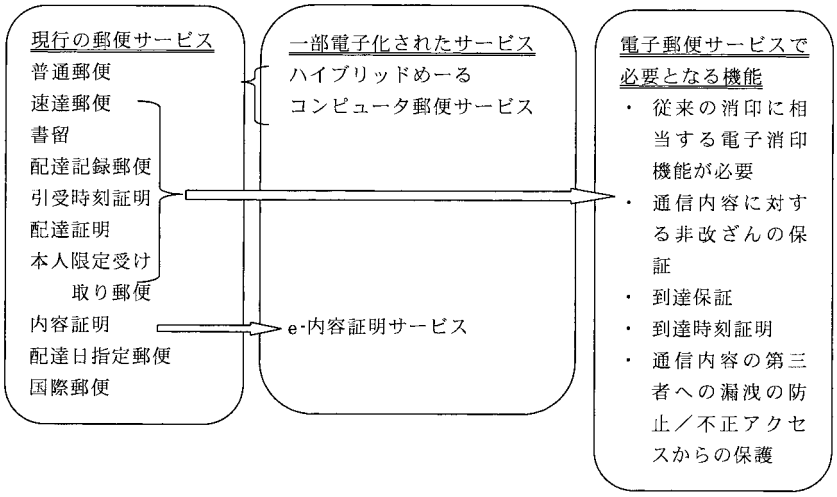



**図 6 郵便サービスと電子化対応**

図 6 からもわかるように，約 10 種類の郵便サービスのうち，電子化されているのは 2 種類である．残りの 8 種類の郵便サービスを見ると，すべてのサービスに「配達確認」もしくは「内容の保証」という機能が必要なことがわかる．これは IT 書面一括法で要求されている「受信者が確実に送信者が送った通信文と同じ通信文を受け取ったことを証明すること」を実現することと同じことになる．IT 書面一括法の施行により，紙媒体での交付では通常郵便でよかったものが，電子媒体での交付では書留や配達証明郵便の機能を持った電子郵便として運用されなくてはならない．一方，電子郵便サービスは，図 6 に示す機能を実現することにより，電子媒体による郵便の問題点を解決することができる．

## 3. 電子郵便サービス

この電子郵便サービスの検討を始めた二つのきっかけについて 2 章で述べてきたが，本章では，電子郵便サービスを検討するにあたっての基本的考え方をまとめた．

1） IT 書面一括法の施行により，郵便利用率が下がることが予想されるため，それに歯止めをかけるための新しい郵便サービスが郵政事業庁には必要になる．
2） IT 技術の進歩によって，IT 書面一括法で要求される電子媒体の保証が可能になってきた．
3） 郵政事業の公社化に向けて，総務省と郵政事業庁で現在の電子的郵便サービスの見直し，統廃合そして新しい郵便サービスの展開が図られ始めている．

世間動向や技術の進歩や効率性を考えればこれで十分ではある．しかし，国民への公平なサービスという観点から見ると，弱者への配慮は必要不可欠である．そのため，次の 4 番目の項目を追加した．

4) 新しいサービスには，デジタルディバイドを発生させない仕組みが必須．

これを実現するためには，この新しいサービスにも従来の紙媒体での配信の仕組みを取り込み，かつ電子⇔電子で提供できるサービスを電子⇒紙でも同等に提供できるものとする必要がある．

以上の 4 項目の要素を含んだ新しいサービスである，電子郵便サービスを検討した．

### 3.1 サービス内容

今回検討したサービスの概要を図 7 で示す．

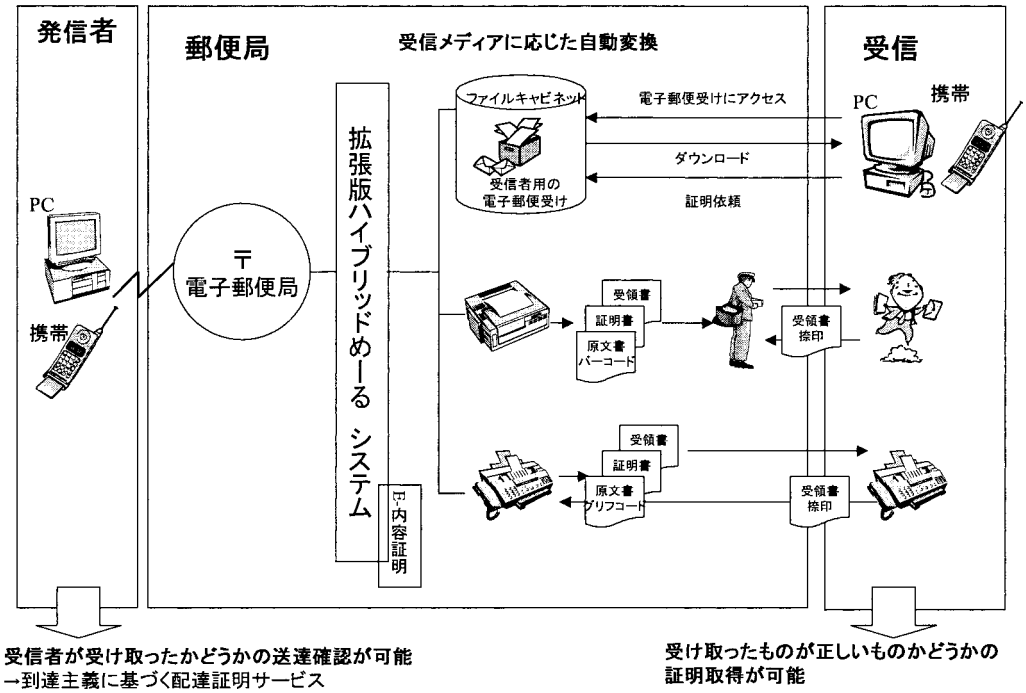



**図 7　電子郵便サービス概要図**

この新しい電子郵便サービスで実現されるサービスは以下の通りである．

1) 発信者は，ネットワークを介して，24 時間・365 日の発信が可能（含む，i モード等のモバイル端末）

2) 受信者は，『電子郵便受け』を利用することで，ネットワーク環境があれば何処でも受け取ることが可能になる．

3) 発信者は，ネットワークを介して，受信者の設備に応じたメディア変換を指定することで，相手がネットワーク利用者であれば電子媒体で，ネットワーク未加入者であれば紙媒体で，FAX 所有者であれば FAX として送信することができる．

4) 発信者の発信日付証明や受信者の受信日付の証明を行うことができる．

5） 発信者は，送信した通信文を受信者が確かに受信したことを確認でき，かつ受信者が受信した通信文と発信者が発信した通信文とが同一内容であることを確認できる．

6） ハイブリッドめーるの機能の内，出力部分が拡張されているため，従来は紙媒体のみをサポートしていたがこのサービスでは，電子媒体での配信やFAXでの配信まで可能になっている．

7） 従来のハイブリッドめーるサービスやe-内容証明サービスを取り込むことで，同一インタフェースによってこれらのサービスを利用することができる．

これらのサービスを提供することで，IT書面一括法施行による紙媒体から電子媒体への移行の要求に答えることができ，また紙媒体やFAX等のレガシー装置の活用によりデジタルオポチュニティの拡大に寄与することができると考えた．また，ここでは詳しく触れないが，現行の電子的郵便サービスの，コンピュータ郵便の機能の内，大量かつ個別内容のダイレクトメール機能をハイブリッドめーるに統合する案も含めて検討した．

このような電子郵便サービスを実現するにあたっては，基本となるエンジンが必要になる．特に，通信文の同一性を保証する仕組みや電子消印のような時刻証明機能を提供するエンジンとしてどの様な技術を適用するかが鍵になる．今回の検討のなかでは，株式会社日本電子公証機構（www.jnotary.com）が提供しているサービスをエンジンとして採用することとした．

次に，このサービスの中核をしめる二つの要素技術である通信文同一性保証と電子消印について述べる．

### 3.2 通信文同一性保証

ここでは，IT書面一括法における電子媒体での配信の要件となる，通信文同一性保証をどの様に実現するかについて，配信から受信の確認までの手順によって説明する．

1） 事前準備

送信者は，民間認証局からデジタル証明書を発行してもらうこと，電子郵便サービス利用申請を行うこと，電子郵便サービス利用のためのクライアントソフトウェアをインストールすること，が事前準備として必要となる．また，受信者も事前に電子郵便サービスの利用者登録をする必要はないが，受信した通信文の同一性を確認する必要がある場合は，事前に確認のためのクライアントソフトウェアを受信者のPCにインストールする必要がある．

2） 手　　順

① 発信者は，送信する通信文（電子媒体）から汎用一方向性ハッシュ関数[*1]を用いてメッセージダイジェスト[*2]を作成し，それを送信者の秘密鍵で暗号化する（電子署名）．これらの作業は，事前にインストールされているクライアントソフトウェアで実行される．

② 発信者は，通信文と電子署名と受信者のe-mailアドレスを電子郵便局に転送する．但し，通信文自身を受信者の公開鍵で暗号化するか否かはオプションである．

③　郵便局では，送信者のオプションによって，受信日時の証明書を発行する．この証明書がこの通信文が受信した時刻に存在したことを証明する．これが送信者に対する電子消印となる．この証明書が将来の電子入札等の時刻証明書となる．この仕組みについては後述する．

④　受信者は，e-mail によって送信者から通信文が送られてきたことを認識する．

⑤　e-mail には，特定の url が記述されている．この url 上には，送信者の情報とダウンロード先が表示されるので，受信者はダウンロード先をクリックすることで通信文をダウンロードして，受信者の PC に取り込むことができる．

⑥　受信者が取り込んだ通信文の同一性を確認するためには，事前にインストールしたクライアントソフトウェアを起動することで確認することができる．クライアントソフトウェアは，送信者の公開鍵（通信文とともにダウンロードされる）を使用して電子署名からメッセージダイジェストを取り出す．そして，受信した本文からメッセージダイジェストを生成する．これらの二つののメッセージダイジェストを比較して同一であれば，受信した通信文は改ざん等がされて無く送信者のそれと同一であると確認する．

⑦　確認後，クライアントソフトウェアは確認結果を電子郵便局のサーバに送信する．サーバ側では，この確認情報と確認時刻（電子郵便局の時刻サーバ）とを送信者に通知する．この情報が受信者の受信時刻証明書となる．

これらの作業が完了した時点で，送信者は自分が出した通信文がいつ電子郵便局が受け取り，いつ受信者が取り込んだか，そしてその取り込んだ通信文が送信した通信文と同一であることの証明を受けたことになり，IT 書面一括法に定められた要件を満足することになる．

## 3.3 電 子 消 印[1]

電子消印（時刻証明）の機能は，電子郵便サービス実現において重要な二つの機能のうちのもう一つにあげられる．電子消印とは，証明された時刻にデータが存在していて，その時刻以降改ざんされていないことを証明する機能である．この機能によって，通信文がいつ発信されたのか，またいつ受信者が受け取ったかの時刻を証明する事が可能になる．この電子消印の実現方法に関しては，複数の実現方法が提案されており，商用化（株式会社 NTT データの電子文書証明サービス「SecureSeal」が有名）されている．ここでは代表的な 2 種類の方法，単純電子消印プロトコルとツリー構造を用いたリンキング電子消印プロトコルについて説明する．

1)　単純電子消印プロトコル

電子消印の発行手順は以下のようになる．

①　発信者がハッシュ関数を用いて，メッセージダイジェストを作成し，電子消印を発行する機関に送信する．

②　発行機関では，認定されている時刻サーバから時刻を取得し，その情報と送信されたメッセージダイジェストに発行機関の電子署名を付ける．これが電子消印となる．

③　送信者に，電子消印を送付する．

この電子消印を利用して，特定の文書がその時刻に存在したかを証明する手順は以下のようになる．

① 証明が必要な文書と電子消印を受信者に送付する．

② 受信者は，送付された電子消印を発行機関の公開鍵で復号化し，時刻とメッセージダイジェストを取り出す．

③ また，受信者は，受け取った文書からメッセージダイジェストを作成し，電子消印から取り出したメッセージダイジェストと比較する．これらが同一であれば，受け取った文書は，電子消印に収められた時刻に存在し，かつ現在まで改ざんされていないことが証明される．

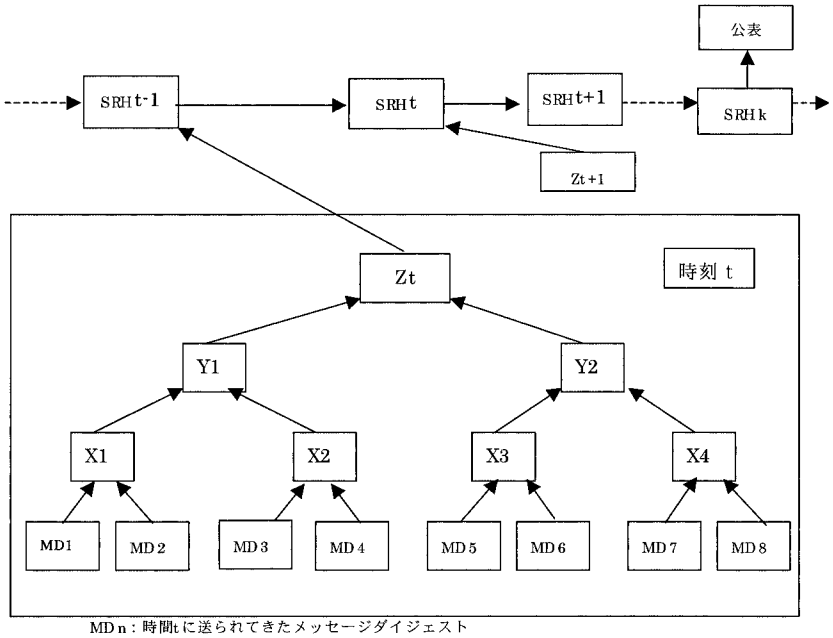
この様に，比較的簡単な仕組みで電子消印を実現することができる．しかし単純な仕組みのため，証明書発行機関と結託すると容易に電子消印を改ざんすることが可能になる．例えば，電子消印を発行する機関の担当者と文書作成表とが結託することにより，既に電子消印が発行された文書を修正してそのメッセージダイジェストと既に発行した時刻とを発行機関が電子署名することで，改ざんされた文書が改ざん前に存在したことを証明することができてしまう．これは証明書とメッセージダイジェストとが一対一で作成されているためこの様なことが可能になる．そこで，より改ざんし難くするために，全く関係の無い複数のメッセージダイジェストを組み合わせることでより安全な仕組みを実現する方法が提案されている．この代表的な方法がツリー構造を用いた電子消印リンキングプロトコルである．

2） ツリー構造を用いた電子消印リンキングプロトコル

この方法は，ある時間内に送られてきた複数のメッセージダイジェストを相互に関連付けるリンク情報を生成し，それぞれの電子消印がそれまでに生成されたすべての電子消印に依存するように生成されるプロトコルである．通常，時間間隔とその間で受け入れるメッセージダイジェストの個数を決めている．例えば受け入れる個数を 8 個と設定すると，時間間隔 t で処理された状態を図 8 に表現する．

このプロトコルでは，利用者 A が MD 1 というメッセージダイジェストを発行局へ送信すると，その時間内（通常ミリ秒単位）に別の利用者から送られてきたメッセージダイジェスト MD 2 とから X 1 というメッセーダイジェストを生成する．さらに MD 3 と MD 4 から生成された X 2 と X 1 から Y 1 というメッセージダイジェストが生成される．そして，残りの MD 5〜MD 8 から生成された Y 2 からこの時間帯のルートとなる Zt が生成される．生成には同じハッシュ関数が用いられていることはいうまでもない．この作業が，時間 t 間隔で繰り返され，それぞれのルートとなる Zi が生成される．さらに，Zt と時間的に一つ前に生成された SRHt−1 とから SRHt というメッセージダイジェストを生成し，あるタイミング（ある商用サービスでは 1 週間に一度）で SRHk が新聞等に公表される．このことで，ある時点でのメッセージダイジェストが公表されることで改ざん等の不正行為の防止につながる．

次に，実際の時刻証明の手順を説明する．発行局は MD 1 を送った利用者に，（MD 1，MD 2，X 2，Y 2，Zt，SRHt−1，時刻）に電子署名した証明書を送る．




MDn：時間tに送られてきたメッセージダイジェスト

Xn：MDiとMdi+1から生成されたメッセージダイジェスト

Yn：XiとXi+1 から生成されたメッセージダイジェスト

Zt：Y1とY2から生成されたメッセージダイジェスト

SRHt：t-1に生成されたSRHt-1とZtから生成されたメッセージダイジェスト

**図 8　ツリー構造を用いた電子消印リンキングプロトコル**

先ず，利用者は，証明した通信文からメッセージダイジェスト MD* を生成し，証明書の MD 1 と比較する．これが違っていると通信文は改ざんされていることになり，この時点で証明作業は中止となる．MD 1 と MD* が等しかった場合は，MD 1 と MD 2 から X* を生成し，X* と X 2 から Y* を生成し，Y* と Y 2 から Z* を生成し，Z* と SRHt−1 から SRHt* を生成する．さらに，SRHt* と（Zt＋1，…，Zk）から公表されている SRHk* を生成する．ここで公表済みの SRHk と生成した SRHk* を比較して等しければ，この通信文は時刻 t に存在し，それ以降変更されていないことが証明できる．この証明手順のどこかのデータが不正操作された場合，ハッシュ関数がそれなりに安全であれば，公表されている SRHk と一致することは非常にまれなケースといえる．

## 4. おわりに

今回の電子郵便サービスで，今まで電子化できなかった郵便サービスを電子化する方法について，具体的に株式会社日本電子公証機構のサービスを基盤とすることで可能であることが確認できた．しかし，実際に運用するためにはさらに次の二つの課題をクリアする必要がある．

① IT 書面一括法で認められた電子媒体での交付を行うためには，郵政事業庁が電気通信事業者になる必要がある．

② 一般的に民間認証局（ベリサインやボルチモアが有名）が発行する証明書には有効期限があり，有効期限切れの対策が必要となる．

①については，郵政事業の公社化に向けて現在総務省を中心にして各種の法律改正が行われようとしている．公社化になった時点で，例えばアウトソーシングが可能になったりすることでこの問題をクリアすることができるかもしれない．

また，②の問題については，単に電子郵便サービスだけの問題ではなく，認証全般に絡む問題として捉えることができる．電子署名法では法律施行規則第六条四で「電子証明書の有効期限は，5年を超えないものであること」と規程されている．そのため，例えば10年保存義務のある文書に関しては電子署名が付けられていたとしても5年を経過すると誰が作成したかを証明する手段が無くなる．IT技術の進歩が著しい昨今では，5年間も同一の証明書を使用することはセキュリティ上問題があるといえる．現状では，1年間もしくは2年間で証明が切れる証明書がほとんどである．現在はまだ具体的な解決策は見出せてはいないが，旧証明書と新証明書とのリンキングを認証局側で証明する手順を確立する等でカバーできないかを模索中である．今後，電子調達や電子申請等が活発化するにつれてこの問題が顕在化するので，民間認証局および認証局を立ち上げた各省庁で対応策を検討中である．

最後に，電子郵便サービスの要件検討にあたり，アイデアおよび技術的サポートを頂いた，株式会社日本電子公証機構の菊田昌弘氏と畠卓子氏および三井物産株式会社高橋進氏と森尾周治氏に感謝の意を表したい．

---

＊1 汎用一方向性ハッシュ関数とは，ある与えられた入力値Xに対するハッシュ関数の出力値をH(X）としたとき，出力値がH(X）となる別の入力値Y(H(X)＝H(Y）かつX≠Y）を見つけることが統計的に困難であるという性質を持っている関数のことである．現時点では，ハッシュ値のサイズを160ビット以上に設定することが安全正常求められる．

＊2 メッセージダイジェストとは，データを決められた長さのデータに変換する暗号アルゴリズム（ハッシュ関数）を使用し作成される，決められた長さ（128ビットor160ビット）の出力値．元データが少しでも異なれば，メッセージダイジェストから元データを推測することは不可能．

**参考文献** ［1］ 宇根正志・松浦幹太・田倉昭デジタルスタンプ技術の現状と課題 日本銀行金融研究所/金融研究/2000. 4 pp. 105〜154

**執筆者紹介** 三 ツ 矢 裕一（Yuichi Mitsuya）
1980年3月慶応義塾大学大学院修士課程管理工学専攻修了．同年4月日本ユニシス(株)入社．日本語プリンタ支援プログラム開発，2200 LINCIIのサポート，官公庁ビジネスを経て，現在，情報システム部に所属．