解説

エレクトロニック・コマースを担う電子文書証明サービスの実現に向けて

三谷 慶一郎　（株）NTTデータ経営研究所
鈴木　邦康　（株）NTTデータ

電子文書証明サービスの背景

近年エレクトロニック・コマースの領域はますます拡大の一途を辿っており，それに従い業務上重要な意味を持つさまざまな文書・記録が，従来の紙による管理から電子文書による管理へと移りつつある．この流れは企業間の商取引のみにとどまらず，いわゆる「電子政府」の実現に向けて今後急激に整備されるであろう電子申請システムの中においても，同じ方向へシフトしていくことは確実である．このように管理対象が紙から電子文書へ切り替わることで，検索や情報の加工性などの利便性が著しく向上する反面，克服しなければならない新たな課題もまたいくつか存在している．その課題の1つとして「電子文書の原本性をいかにして確保するか」という問題，つまりいかにして電子文書の改ざんを防止・抑制するか，という問題がある．この問題に関しては，総務庁の共通問題研究会において検討が行われ，1999年4月に中間報告という形でその指針がすでに示されている．したがって，今後は電子政府のみならず企業間のエレクトロニック・コマースにおいても，この指針に沿った原本性確保システムが共通基盤の一部となるであろうことが予想される．

このような背景を受けて，NTTデータは2000年4月から電子的な記録の原本性と作成時刻を証明する「電子文書証明サービス」の提供を開始する．このサービスは，米国Surety.com社が開発した「Digital Notary™ Service」をベースにしたものであり，技術的優位性や実績といった面で他を大きくリードしたものとなっている．

本稿では電子的な記録の管理上の問題点や原本性証明の必要性・重要性を整理し，本サービスの技術的な概要について解説を行う．さらに，日本における各分野での適用可能性について考察を述べる．

文書ディジタル化の現状と障害

「電子文書管理システム」というものは，古くからある情報システムの1ジャンルであり，特に新しいものではない．また，情報システムというのは，多かれ少なかれ「文書管理」機能を必ず持っているともいえる．いわゆる経理システム，人事・

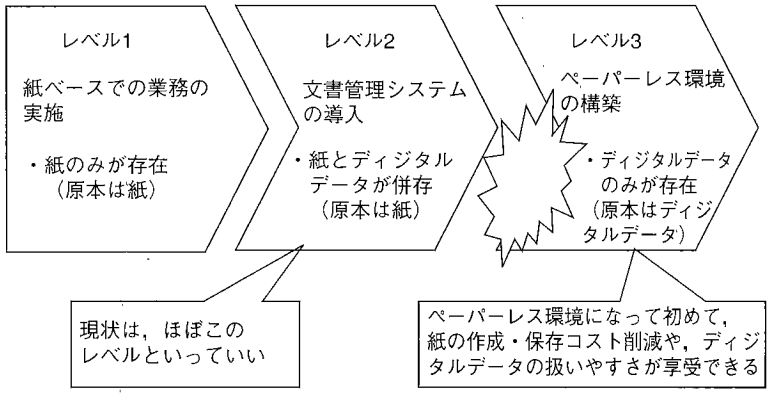

図-1　文書のディジタル化レベル

給与システム，身近ではワープロなどというアプリケーションはきわめて分かりやすい文書管理システムの一例といえるかもしれない．

さて，ここでは文書の電子化のレベルを3つに分けて考えたい（**図-1**）．

- **レベル1**：紙ベースで業務が遂行されており，文書管理システムは未導入の段階（当然原本は「紙ベースの文書」そのものとなる）
- **レベル2**：電子文書管理システムはとりあえず導入したものの，実際には文書作成・出力マシンとして動いており，紙ベースの文書とディジタルデータとが併存している段階（あくまでも原本は「紙ベースの文書」）
- **レベル3**：真にペーパーレス環境に移行し，ディジタルデータをベースとした文書管理が行われている段階（原本はディジタルデータとなり，紙は出力してもあくまでテンポラリーに使われているだけ）

現状の企業・行政機関においては，電子文書管理システムを導入している場合においてもほとんどが，レベル2の段階にとどまっていることは否定できない．レベル2においては，多少の文書作成支援的，あるいは美麗な出力ができる程度の恩恵は得られているものの，ディジタル化の本来的な効果である「紙ベースの文書」の作成・保存コストの削減や，ディジタルデータとしての扱いやすさ，利活用の容易さを享受できていない．この大きな原因は「紙」を捨て去ることができないことに尽きる．

紙を捨て，レベル3のペーパーレス環境に移行できない要因には，大きく4つの観点が考えられる．まず，企業等において，法制度・行政指導上の理由によって紙ベースの文書の保存義務がある点．そもそも紙ベースの文書を前提とした商慣習そのものが根強く残っている点．ディジタルデータそのものの脆弱性に対する不安感．そして，法律上の証拠力を担保するために紙ベースの文書を保存する必要がある点である．

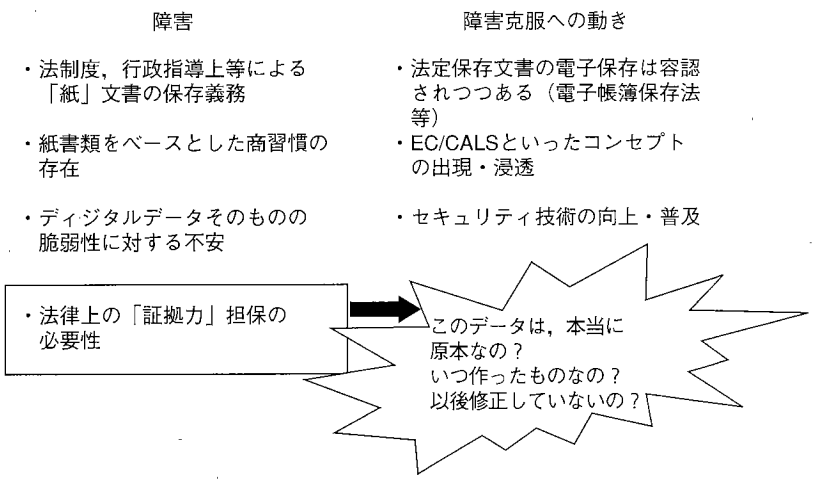

図-2　ペーパーレス環境実現への障害

このうち，先の3つの要因については最近多少なりとも解決の方向が見えつつあるように思える．すなわち法制度上の問題については，規制緩和の流れの中で，法定保存文書（法律で保存を義務づけられている文書）の電子保存が容認されつつあるし，EC/CALSといったディジタルデータを基盤とするコンセプトの出現・浸透により，昔ながらの商慣習も少しずつ変わり始めている．また，ディジタルデータの脆弱性に対してもセキュリティ技術の向上により，比較的廉価に各々のリスクを軽減することが可能となってきている．

ただし，1つ残った「法律上の証拠力担保の必要性」については，いまだに大きな問題として存在しつづけている．法廷において証拠書類としてディジタルデータを提出したときに，「このデータは本当にオリジナルの原本なのか？　いつ作成されて，以後修正していないことがどのようにして証明できるのか？」という裁判官の問いに対して応えられないこと．これがペーパーレス化移行への最大の障害であるといえる．逆にいえばこの障害が克服できれば，紙の呪縛から逃れ，ディジタル化本来の大きなメリットを受けることができるのである（**図-2**）．

電子文書証明サービス

法的証拠力担保の方向性

さて，ディジタルデータに対する法的な証拠力を担保するために，まず考えられるのが，「信頼される第三者機関」にデータそのものを預けるなどにより，証明をしてもらうスキームである．たとえば法務省の公証人役場，郵政省の内容証明郵便等がディジタルデータに対応すればこれに近いイメージになると考えられる（事実，両省とも類似したサービスの実施を検討している）．ただし，この場合はあくまで「行政機関」が実施することで信頼性を構築しているわけで，実現には行政側の決断を待つしか方法はない．

代替策として考えられるのが，同様の「信頼できる環境」を純技術的

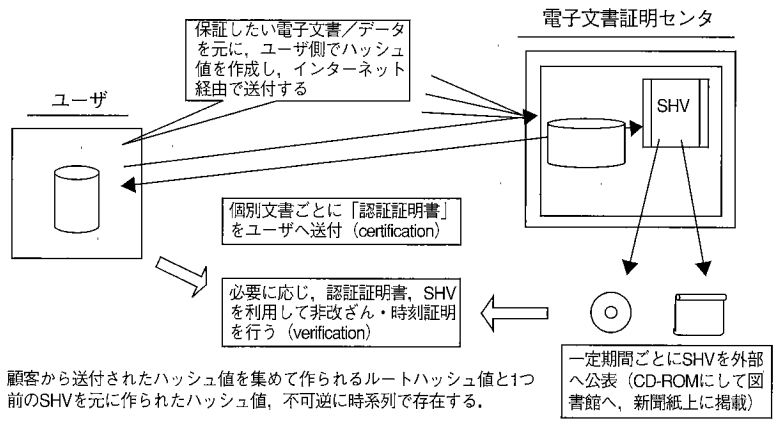

図-3　「電子文書証明サービス」概要

に作りあげるスキームである．今回紹介するSurety.com社の「電子文書証明サービス」は，このスキームを成立させた希有な例といえる．

「電子文書証明サービス」とは

Surety.com社の電子文書証明サービスは，ひとことでいうと「電子化された情報がある特定の日時に確かに存在していたこと」かつ「それ以降電子化された情報の内容が改ざんされていないこと」を証明するサービスである．これまでに多くの企業において導入実績を持ち，米国の法廷において，実際に本サービスを利用したディジタルデータの証拠力が担保されたケースもすでに存在する．

具体的なサービスのイメージを以下に列記する．

- ユーザが，非改ざん証明を行いたいディジタルデータを選択する
- 対象データに対して，ユーザ側のシステムにおいてハッシュ関数によって「ハッシュ値」を作成する（ハッシュ値：任意長のデータをある関数に入力し，結果として出力される短い固定長のデータ．一方向性でありハッシュ値から元のデータを復元することは不可能）
- インターネット経由でハッシュ値を電子文書証明センタに送信する
- 電子文書証明センタでは，不特定多数のユーザからのハッシュ値を集めてさらにスーパーハッシュ値を時系列に生成・管理すると同時に，個別データごとに「認証証明書」を発行する
- 電子文書証明センタは，ウィークリーハッシュ値と呼ばれる値（1週間のスーパーハッシュ値をさらにハッシュした値）を外部に一般公開し，「公知の事実」とすることでセンタ運用の非改ざん性を保証する（CD-ROMとして図書館へ寄贈，あるいは新聞に掲載）
- ユーザは，必要に応じて，「元のディジタルデータ」「認証証明書」を利用して非改ざん・時刻証明を行うことができることになる（**図-3**）

このサービスの特色としては，ユーザが電子文書証明センタに送付するのは，ディジタルデータそのものでなく，ハッシュ値のみであり第三者にデータの内容を見られることがないため心理的な抵抗感が少ない点．外部へ定期的にウィークリーハッシュ値を公表しているため，電子文書証明センタ自体が内部不正を行ってもユーザ側からすぐに見破られてしまう点があげられる．

ディジタルデータごとの固有のハッシュ値（Surety.com社はこれをDigital Finger Print（電子指紋）と呼んでいる）を不特定多数集め，さらにスーパーハッシュ値を作成・保存することにより，1ユーザだけでは不正が不可能な，いわば相互牽制的な環境，すなわち「信頼感」を構築しているといえる．

「電子文書証明サービス」の技術的概要

電子文書証明サービスは，大きく分けて以下の2種類のトランザクションから成り立っている．

- 電子文書の登録依頼（Notary）
- 登録済み文書の実証依頼（Validation）

それぞれのトランザクションについて，具体的にどのような処理がクライアントおよびサーバ上で行われているか，以下に説明する．

●電子文書の登録依頼（Notary）

1. 登録対象の（原本性と時刻証明を行いたい）文書から，288bitのハッシュ値を生成する．288bitのハッシュ値生成には，MD5とSHA1が使用される．この処理はクライアント端末上

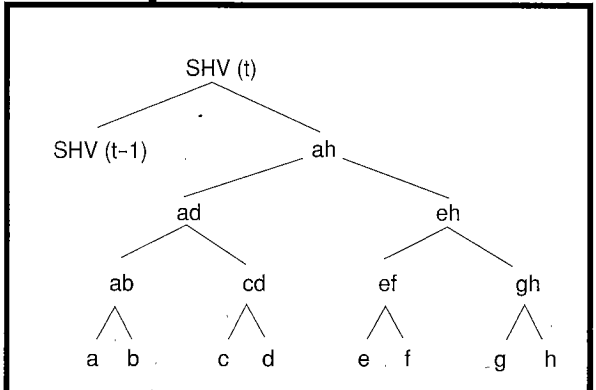

図-4　8つのleafを持つツリーの例

で行われる.

2. 1.により生成されたハッシュ値をaとし，この処理が行われた時間間隔をtとする．時間間隔tに，同時に8つの登録依頼が行われた（8ユーザが同時にサービスを利用し，それぞれa, b, c, d, e, f, g, hというハッシュ値を生成した）と仮定する.

3. 各ハッシュ値が電子文書証明センタにインターネット経由で送信される．センタはこれらを受信すると，ハッシュツリーを作成する（**図-4**）．このツリーは二分岐であり，各ハッシュ値から新たなハッシュ値を生成することで，最終的にルートハッシュ値（RHV，図中のahに相当）と呼ばれる値を作成する.

4. センタでは一定の時間間隔でスーパーハッシュ値（SHV）を管理している．この時点でt-1秒のSHVまでが存在しており，このSHV（t-1）とRHVであるahから，さらにハッシュ値を生成する．この値がSHV（t）であり，時間間隔tに登録された文書の原本性と時刻を保証する値となる.

5. 以上の処理が終了すると，センタは各クライアント端末に対して認証証明書を送り返す．認証証明書には，タイムスタンプやIDのほかに，a, b, cd, eh, SHV（t-1）が含まれている.

●登録済み文書の実証依頼（Validation）

1. 登録済みの文書から，再度ハッシュ値をクライアント端末上で生成する．この値をa'とし，この値がaと等しくない場合には，文書に何らかの変更が加えられたと判断する.

2. a'=aの場合，実際にセンタに登録されている値（SHV（t））との比較を行うことで，原本性と時刻の証明（実証手続き）を行う．まず，1.で作成したa'と証明書中のb, cd, ehを組み合わせ，RHV ah'を作成する．次に，ah'と証明書中のSHV（t-1）を組み合わせ，SHV（t）'を作成する.

3. このSHV（t）'とセンタに登録されているSHV（t）の値を比較し，等しければ「その文書が登録されて以降改ざんされておらず，その時刻に存在していたこと」が証明される.

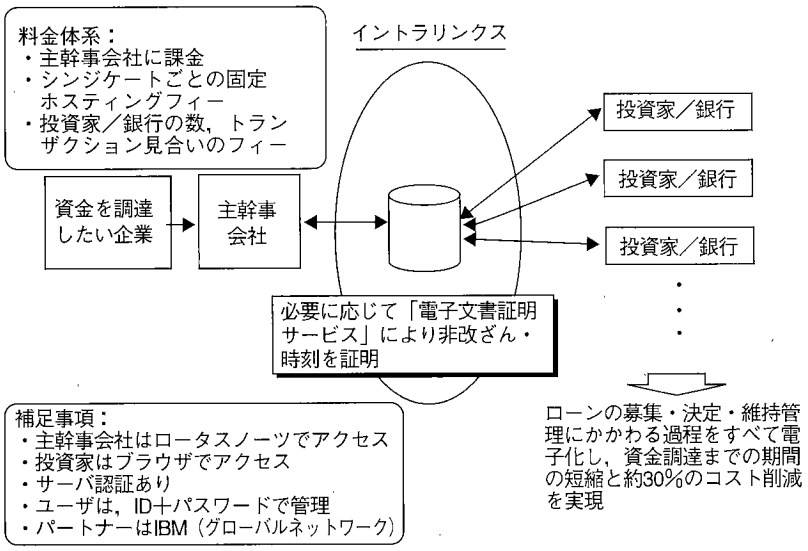

図-5　適用事例：イントラリンクス

米国における適用事例

電子文書証明サービスについて実際の適用事例を以下に示す.

医薬品大手メーカであるファイザーでは，自社の研究開発部門で電子文書証明サービスを導入している．既知の通り米国における特許は「先発明主義」であるため，研究開発担当者の毎日の実績は実験ノートとして日付と共に厳重な管理が必要となる．ただし，昨今は手書きではなく，ワープロ等のディジタルデータに移行しつつあるため，ペーパーレス環境で同様の管理を行う必要性が生じている．ファイザーではこの分野に本サービスを適用し，開発担当者が作業を完了した都度，作成したディジタルデータに対して非改ざん・時刻証明が自動的に行われるシステムを構築している.

金融関係では，イントラリンクス（IntraLinks）という企業が行っているイントラローンというサービスにおいて電子文書証明サービスが使われている．これは，シンジケートローン（各国の銀行がシンジケートを結成し，政府機関や民間企業に対して行う高額かつ中長期の融資）の募集・決定・維持管理に関してペーパーレス環境を提供するサービスであり，すでに大きなコスト削減効果をあげている模様である．「非改ざん・時刻証明機能付きエクストラネット」というと分かりやすいだろうか（**図-5**）.

同様に，ロープラス（LAWPlus）という企業においては，裁判所と法律事務所等をエクストラネットで結び，法律事務に関する文書管理についてペーパーレス環境を実現しており，同様に電子文書証明サービスを適用している．裁判関連の書類等は，いうまでもなく「証拠力」が必要なものであり，これらの書類の電子化は，まさに本サービスが必要となるジャンルであるといえる（**図-6**）.

想定される市場

翻って，国内において電子文書証明サービスが必要となる「市場」はどこにあるかを民間分野と行政分野それぞれについて整理したい．基本的には「きわめて付加価値が高く，法廷等で証拠書類として提出の可能性のある文書」が存在している領域においては市場性があると考えていい．

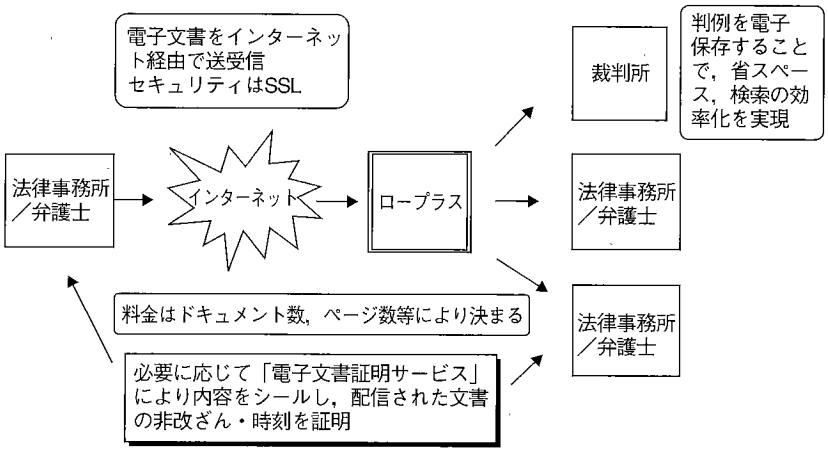

図-6　適用事例：ロープラス

民間分野

民間市場においては，先述のファイザーのような，「技術開発部門における文書管理」が有望視される．特に，米国企業を相手にした特許紛争を抱える可能性のあるような業種（医薬品メーカ，化学メーカ等）において，そのニーズは高いと思われる．

製造業においては，設計図・仕様書等といった付加価値の高い文書の電子化が推進されており，これらを活用する開発・製造工程，いわゆるCALS的な分野にも適用の可能性はある．

また，高額の契約書が電子化され流通するような場面においてもニーズは生まれると思われる．たとえば金融分野において最近注目されているオンライントレーディング等のサービスなどが有望ではないであろうか．

一方，先にあげた法定保存文書の電子保存容認の流れは注目に値する．特に昨年4月に認可された，「診療録（カルテ等）の電子化」は，本サービスの適用可能性に大きな影響を与えるであろう．

行政分野

行政分野においては，真っ先にあげられるのが，中央省庁，自治体等における「公文書の電子化」であろう．行政機関において，公文書は一般にかなり重要なものであり，情報公開法制定の流れの中で，ディジタル化は今後急激に進行していくことが予想される．公文書に関するペーパーレス環境を実現するためには，電子文書証明サービスの適用はきわめて有効であろう．

行政情報化推進基本計画の中で最近，クローズアップされている「電子申請」や「ワンストップサービス」というコンセプトも，「ディジタル化された公文書が行政・民間間を流通すること」と解釈できるわけであり，同様に本サービスの適用分野となり得るといっていい．

総務庁では一昨年来，行政情報化計画遂行の上で，省庁共通的な課題についての検討を目的として，有識者を集めて「共通課題研究会」を開催している．この研究会においても「ディジタル化した文書をどのように保証するか」という「原本性保証問題」は重要課題の1つとして検討されており，当分野における行政側の関心の高さを物語っているといえる．

総括

「エレクトロニック・コマース」は，ごく大雑把にいえばディジタル化された文書の流通を意味するものであるし，最近流行の兆しがある「ナレッジマネジメント」というのも，ディジタル文書の管理・利活用の方向性を示すものであるといえるかもしれない．どちらの分野においても，第三者に対して文書の正当性（非改ざん性）を主張できる仕組みを導入しない限り，高付加価値な文書をディジタルデータとして扱うのは困難であろう．たとえば，エレクトロニックコマースにおいて，額面の大きな取引きに関する係争が発生した場合，どの当事者の主張が正当であるのか判断するためには，関連するディジタル文書の「非改ざん性」を証明することが必須になると思われる．これは，ナレッジマネジメントの分野や，加えて官公庁の情報公開・公文書管理などにも当てはまることであり，そのようなシステムにおいて「電子文書証明サービス」が重要な構成要素となる可能性はきわめて高い．

（「電子文書証明サービス」に関する問合せ先：（株）NTTデータ　新世代情報サービス事業本部
（E-mail:notary@ains.nttdata.co.jp））

（平成12年3月10日受付）