光ディスクと原本性保証技術

山口雅浩

光ディスク等の大容量記憶媒体を用いて，これまで主に紙を媒体として取り扱われてきた文書類をディジタルデータとして保存する際には，紙を前提に成り立ってきた従来の仕組みとの整合性が問題になる．近年，法令で保存が義務づけられた文書等をディジタルデータとして保存することが容認されているが，同時にディジタルデータの原本性を確保する必要性が指摘されている[1]．

現在，政府はいわゆる「電子政府」を実現することを目標に掲げ，文書保存の電子化や，申請や届出手続きの電子化・オンライン化等を，民間の負担軽減，事務の効率化，公平性確保等の観点から重要な課題として取り上げている．一方で，申請・届出手続きの電子化を進めるには，電子文書の原本性，受発信者の認証の仕組み，手数料の納付方法等の共通課題を解決する必要がある．

最近，保存義務がある文書等の電子保存における原本性確保のために，「原本性保証電子保存システム」の開発が行われている[2,3]．また，原本性保証電子保存システムを利用することは，申請や届出手続き等のオンライン化を図る際にも有効であることが明らかになってきた．本稿では，原本性保証電子保存システムの概要と，原本性保証技術を用いた電子申請システムを紹介し，それらにおける光ディスクの位置づけについて考察する．

1.　原本性保証電子保存システム

1.1　ディジタルデータの原本性とは

電子商取引等における情報システムの利用の拡大とともに，法令で保存を義務づけられた文書等を紙として保存するためのスペースや管理は企業等にとって大きな負担となっており，文書保存の電子化が強く要望されている．これを受けて政府は，電子媒体を利用した保存方法を原則として容認することとし，会計帳簿や診療録等の電子保存は制度的にはすでに可能となっている．

しかし，ディジタルデータにおいては，完全な複製を容易に作成できることや，改変の痕跡が残らない等の点で，紙を媒体とした文書類と異なる性質をもつため，ディジタルデータの原本性，すなわち真正性，見読性および保存性を確保することが必要となる[1,4]．ここで，真正性確保とは，データの故意または過失による虚偽入力，書き換え，消去および混同を防止すること，見読性とは，データの内容を必要に応じ肉眼で見読可能な状態に容易にできること，保存性とは，保存期間内において復元可能な状態でデータを保存することとされている．また，裁判等におけるデータの証拠性（証拠能力および証明力）を確保することも必要である．これらの要件は，一般に，「技術的」「組織的」「制度的」対策を適切に組み合わせることにより満たされる[4]．現状の紙ベースの文書保存においては，すべての脅威に対して上記のいずれかの対策が取られていると解釈されるため，電子保存にあたって生じる新たな脅威に対する対策を講じる必要がある．

原本性保証電子保存システムは，このような背景の下に，保存義務のある文書等の電子保存を可能とし，会計帳簿やカルテ等のペーパーレス化を推進する目的で開発されたものである[2,3]．このシステムは，記録されたデータに対する物理的かつ論理的なプロテクト機構を装備し，技術的に紙と同様の安全性を実現する．このため，組織的または制度的対策の援用を得なくても容易に電子保存を実施することが可能になる．

1.2　原本性保証の方法

原本性保証電子保存システムにおいては，CPU（cen-

東京工業大学像情報工学研究施設（〒226-8503 横浜市緑区長津田町 4259）
E-mail: guchi@isl.titech.ac.jp

tral processing unit）を装備したインテリジェントな保存装置を用い，装置内部の制御プログラムによって保存されたデータを保護する機構をもつ．具体的には，以下に示す方法を用いる．

(1) メモリーに対するすべてのアクセス（書き込み・読み出し等）はCPUによって管理される
(2) ホストからのアクセスは，標準的な入出力ポートのみを介して行われる
(3) メディア全体をパッケージ化し，部品の入れ換えやデータの書き換えができないようにする

図1に，これらの機構を模式的に示す．これにより，外部からのアクセスは入出力ポート経由のみに制限され，管理者であっても制御プログラムに規定された以外の方法によるアクセスを行うことはできない．制御プログラムは，原本として保存されたファイルの保存期間内の消去，改変を禁止するとともにアクセス履歴の保存を行う．

実際の運用を考えると，原本以外のファイルを保存することも想定されるため，保存されるファイルの種別として，4種類（仮原本，原本，謄本，一般ファイル）が定義されており，それぞれの種別に応じて追記以外の書き換えや消去が禁止されている．

利用者の登録やタイマー設定等を行う保存装置の管理機能についても作業履歴が保存される．たとえば，仮にシステム管理者の権限を悪用し，タイマーの設定を変更して過去のデータの改ざんが試みられた場合でも，その痕跡が残される．なお，記録された履歴情報は，原本ファイルと同様に管理者でも削除できない．また，アクセス履歴を記録することは，不正行為に対する抑止力としても有効と考えられる．

使用する保存媒体が光ディスク等の取り外し型媒体の場合には，媒体上のデータを他のシステムで改変される可能性が生じるため，各媒体に固有の識別番号を与えることや，メッセージ認証や暗号化等によりデータを保護する．識別番号や暗号鍵の情報を保存装置に保管しておくことで，他の装置によりデータが変更されても検知が可能である．ただし，書き換え可能な取り外し型媒体の場合には，他の装置による改ざんや消去（初期化等）を完全に禁止できない点に注意が必要である．なお，医用画像の電子保存のための共通規格に準拠した光磁気ディスクを用いる場合は，特殊な安全機構により一般の光磁気ディスクドライブでアクセスできない仕組みが組み込まれているので，改ざんや消去は基本的に不可能である[4]．

さらに，他の保存装置にコピーを作成したり，原本ファイルを移動するために，装置間での謄本作成および原本の

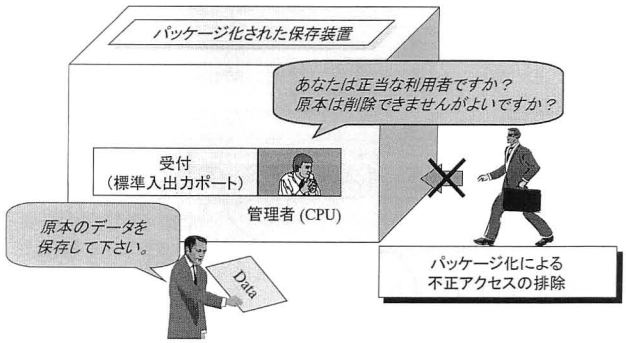

図1　原本性保証電子保存システムにおける保存機能の概念図．保存等の操作はすべてCPUによって管理され，利用者は直接保存媒体にアクセスすることはできない．

移動機能を有している．原本を移動した場合には，元の原本データは消去され，移動先のファイルが原本となる．ファイルの移動や謄本作成は，正しい原本性保証電子保存システム間でのみ行われる必要があるので，システム間での相互認証やメッセージ認証等により正しくコピーまたは移動されたことを検証する．

1.3　原本性保証電子保存システムの利用形態

本システムにおいては，入出力仕様のみが規定され，CPUやメモリーの大きさ・種類は限定されないことから，たとえば持ち運び可能なハンディー型，外付け型ハードディスクのような装置からサーバーとして利用可能な大規模なシステムまで，さまざまな実現形態が考えられる．さらに，保存媒体の種類も制限はなく，磁気ディスク，光ディスク，半導体メモリー等，目的に応じて最適なメモリーを用いればよい．さらに，今後の技術の進展により新たな大容量メモリーが出現しても，システムへの影響をほとんど与えずに保存媒体の追加や更新を行うことが可能である．

2.　原本性保証技術に基づく電子申請システム

2.1　電子申請システムの要件

申請・申告の電子化は，行政分野の情報化における重要な課題として位置づけられている．これまでにフロッピーディスク等を用いたオフライン型や，専用線を利用したオンライン化は実現されているが，現在はインターネット等のオープンなネットワーク環境からの申請を実現することが期待されている．

電子申請を行う場合においても，紙を用いて対面で申請する場合と申請者や受付者等の役割は基本的に変わらない．特に，申請データ等に関する責任の所在が明確にされていなければ電子申請システムの導入は不可能といえる．そこで，申請における申請者，受付者の役割を単純化して整理すると，申請書の作成と提出は基本的に申請者の責任

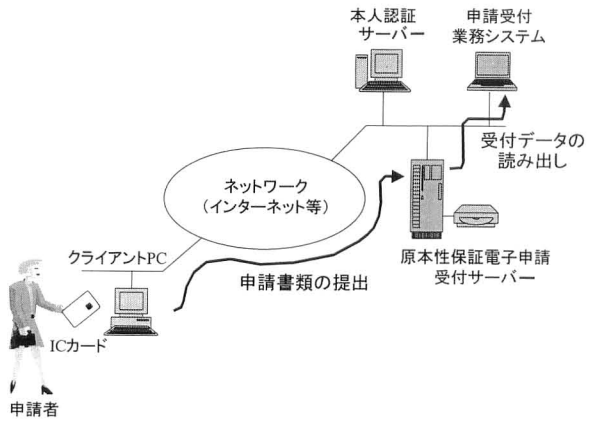

図2　原本性保証電子保存システムを用いたオンライン電子申請の概念図．申請者は原本性保証電子保存システムによって構成される受付サーバー（原本性保証電子申請受付サーバー）まで申請データを伝送する．受付者は受付サーバーに提出された申請データの処理を行う．

であり，申請受付窓口に提出された申請書を受け付けた後，受付者がこれを管理する責任を負う．したがって，受付窓口が申請者と受付者の責任分界点になる．

オンライン電子申請システムのセキュリティーに関わる主な機能としては，① 申請者の本人確認，② 提出された電子文書の原本性確保，③ 提出時におけるデータのセキュリティー，④ 電子的な記名押印，等が挙げられる．責任分界点の議論より，これらのうち②は主に受付者側から，③は申請者側から挙げられる要件である．なお，①および④についても電子認証技術等に基づいて実現するべき機能であるが，本稿の主題から外れるため省略する[4,5]．

受付者の立場から考えると，仮に何らかの問題が発生した場合，受付者は，自らの責任範囲については間違いなく管理していたことを，申請者等に対して証明しなければならない．このため，提出された申請データが改変されていないことを保証できるシステムが必要とされる．一方，申請者の立場からは，ネットワークを通じて正しく申請データを伝送する手段が必要である．そして，自らが提出した申請書が，改変・紛失・すり換え等がなく正しく受け付けられたことを確認できなければならない．

2.2　電子申請システムの構成

オンライン電子申請における申請者と受付者の責任関係を明確にするために，原本性保証電子保存システムを用いることが有効である．図2に原本性保証技術を利用した電子申請システムの構成を示す．図2では，原本性保証電子保存システム（原本性保証電子申請受付サーバー，以下，原本性保証受付サーバーと略す）は，申請業務における受付窓口の役割を担っている．

申請者は，申請データを作成し，必要に応じて押印の代用として暗号技術を用いた電子署名を付加する．提出時には，ICカード等を用いた電子認証により，申請者の本人確認およびサーバー認証を行った後，申請データを伝送する．伝送においては，暗号化によりデータを秘匿するとともに，メッセージ認証を用いて申請データが伝送中に改変を受けていないことを検証する．正しく伝送されれば，原本性保証受付サーバーに保存され，保存されたことが申請者に通知される．これにより，申請者は申請データを正しく提出できたことを確認できる．提出された申請データの改変や消失等は，原本性保証機能によって防止されるので，受付者は従来と同様に受付窓口に提出された申請書（原本性保証受付サーバーに保存された申請データ）の処理を行えばよい．

以上のようにして，原本性保証電子保存システムを利用することで，申請者と受付者の責任範囲を明確にできるので，申請手続きのオンライン化を円滑に導入することが可能になる．このとき，原本性保証電子保存システムが申請者と受付者の責任分界点としての役割を負う．また，原本性保証電子保存システムは，アクセス履歴を改変不可能な状態で保存する機能をもっているため，何らかの問題が発生した場合の原因究明等が容易になる．

2.3　東京工業大学におけるフィールド実験について

東京工業大学では，1999年度より全学生と職員の学生証・身分証明証をICカード化し，キャンパス内における本人確認，申請・申告の電子化等に関する実証実験を実施している[6]．本節では，同大学での実験の概要とその中で構築している電子申請システムについて紹介する．

CPU付ICカードは，プログラムによって内部のデータを保護できることや，暗号プログラムを内蔵していること等により，高いセキュリティー性と汎用性を有しており，サービス利用者の本人確認や情報のセキュリティー確保に有用である．現在，住民基本台帳カードや健康保険証ICカード等が検討されており，近未来には多数の国民が身分証明証等としてのICカードを携帯し，使用するようになると予想される[6]．そこで同実験では，電子的な身分証明証としてICカードを使用する際の効果や問題点等を明らかにすることを目的とし，現在までに以下の業務がICカード身分証明証を用いて実施されている．

(1) 在学証明書，健康診断書等の証明書類の自動発行
(2) 入退室管理の自動化
(3) 図書の貸し出しや健康診断における受付の自動化

これまでに，以下の機能をもつオンライン電子申請システムを実装し，処理能力や操作性等の評価を行っている．同大学では，現在，実業務に適用する準備が進められてお

り，2000年度より，全学規模での電子申請が行われる予定となっている．

(1) 申請手続き案内の提供
(2) ICカードを用いた利用者の認証
(3) 暗号手法を用いたセキュリティー通信機能
(4) 提出された申請データの原本性保証
(5) 電子署名技術を用いた電子印鑑機能

3. 原本性保証における光ディスクの役割について

ディジタルデータの改ざん防止に対して，CD-R (compact disk recordable) 等のWORM (write once read many) 型保存媒体を用いることが有効といわれることが多い．しかし，WORM型保存媒体の場合でも，書き換え・消去が不可能であることが保証されているわけではない．一方，原本性保証電子保存システムでは，搭載されたプログラムによって媒体の種類に依らず保存データの保護を実現している．これらは，保存システムにおける異なる層の機能であり，各層の機能の組み合わせによりシステム全体のセキュリティー機能が定まる．

表1は，原本性保証電子保存システムの論理的な階層構造を簡略化して示したものであり，原本性保証電子保存システムでは，ファイルシステム層において改ざん防止等の機能をサポートしており，この層以下に対してOS (operation system) や別のプログラムを通じてアクセスできないようにする必要がある．専用のハードウェアを用いる場合には，保存装置をパッケージ化して物理的なアクセスを不可能にする方法が考えられる．このような形態の例としてICカードが挙げられる．しかし，ハードウェアとして汎用のコンピューターシステムを流用するときは，プログラムを搭載した保存装置やCPU等を施錠されたラックに保管したり，保存媒体を入室管理された部屋で取り扱う等の組織的対策が必要になる．これに対して，下位層において改変や媒体のすり換え等ができない機構をサポートすると，上述のような組織的対策に対する要求は緩和される．すなわち，各層の機能を適切に組み合わせて技術的対策を高度化することで組織的対策の比率が下がり，運用性が向上する．このような観点から，原本性保証の要件に対する光ディスクの役割を考察する．

3.1 真 正 性

たとえば，WORM型保存媒体の特性を利用して，媒体に対する直接アクセスを防止したり，アクセスがあった場合に検知できる機構を導入することが考えられる．このとき，上位のファイル管理プログラムやデバイスドライバーの機能と連携して改ざんや消去を防止するとさらに効果的である．たとえば，フォーマット等の工夫により原本性保証電子保存に対応していない汎用ディスクドライブでは，消去や書き込みをできないようにすること等が考えられる．これにより保存媒体の管理が相対的に容易になる．

また，取り外し型媒体の場合には，ディスクのすり換えによるデータの偽造も脅威として挙げられる．これに対する対策として，ディスクに固有識別番号を付加することが有効である．最近，DVD-RAM (digital versatile disk random access memory) 等において著作権保護を目的としてサポートされているディスクごとの個別情報等は電子文書の原本性保証にも有用であり，これを活用したシステムの開発が期待される．

表1 原本性保証電子保存システムにおける階層構成．

アプリケーション		
原本性保証プログラム		
ファイルシステム1		ファイルシステム2
デバイス ドライバー1	デバイス ドライバー2	デバイス ドライバー3
物理層(各種ディスクドライブ/保存媒体)		

保存媒体ごとにデバイスドライバーが存在し，媒体に依存した物理フォーマットをサポートしている．また，異なるファイルシステムの保存媒体を用いる場合でも，原本性保証プログラムからは共通の入出力インターフェースが提供される．ファイルシステムに直接アクセスすることは禁止されており，すべてのアクセスは，原本性保証プログラムを通じて行われる．

3.2 保 存 性

保存義務のある文書の中には，保存期間が10年とされているものもあり，保存に対する信頼性の高い媒体の重要性は高い．光ディスクは，磁気保存媒体等と比較して長期保存性にすぐれており，磁気等の環境に対する安定性も高いことから，原本性保証電子保存用の媒体として適している．このため，磁気ディスク等と比較してバックアップ等の運用的対策に要する負担が軽減される．

3.3 見 読 性

光ディスクの寿命は長期化しているが，データを書き込む際に使用したコンピューターシステム等は更新される場合が多く，媒体に記録するフォーマットがOSやアプリケーションソフトに依存する場合，実質的に読み出しできなくなる可能性がある．このためOSに依存しない記録形式(たとえば，UDF: universal data format) を用いることや，保存装置はホストコンピューターと分離可能とし，コンピューターが更新されても保存装置を接続できるようにしておくことが望まれる．また，アプリケーションソフトによって記録されるデータの形式は標準的なものであるか，公開されていることが必要である．

3.4 証 拠 性

電子データの真正性，保存性，見読性確保は，文書の電子保存における要件であり，これによってシステムや運用により講じるべき対策が決まることになる．しかし，裁判における証拠性（証明力）は，裁判官の自由な判断に委ねられているため，その対策として十分なレベルを定めることは困難である．このため，利用分野に応じて保存されるデータの信頼性を高めることが必要とされる．

通常の運用では，表1におけるアプリケーション層からすべてのデータにアクセスするが，裁判や犯罪捜査等においては，紙に記録された文書で紙質や筆跡等が重要な要素とされているのと同様，すべての層に対する調査分析が行われるものと考えられる．このとき，保存システムに対するアクセス履歴が重要になる．WORM型保存媒体であれば媒体上での記録順序やファイル削除の履歴が残されるので，これと保存装置のログとを照合できれば保存データの証明力が高まるものと考えられる．また，媒体や保存装置ごとの固有番号をディジタルデータに付加しておくことにより，原本性保証電子保存システム間で複製・移動された履歴をすべて追跡することも可能になる．

電子申請等のリアルタイム性が要求される利用においては，申請者から受信したデータの一時保管には，現時点ではアクセス速度等の点で磁気ディスクのほうが適していると思われる．光ディスクは長期保存用として利用される形態が多いものと見込まれる．しかし，磁気ディスクはホストコンピューターの交換に際して同時に入れ換える場合が多いのに対して，光ディスクはその数倍もの期間利用されることになる．したがって，原本性保証が要求される分野においては，上記の保存性や見読性を満たす方策を確保しておくことがますます重要になる．

本稿では，これまで紙で取り扱われてきた文書等の保存を電子化する際に生じる原本性保証の問題を取り上げ，その解決策を提供する原本性保証電子保存システムを紹介した．また，原本性保証電子保存システムを用いて，オンライン電子申請等における責任範囲を明確化したシステムを構築できることを述べた．そして，原本性保証の観点から光ディスクへの要求について考察した．現在，特に行政を中心とした分野で原本性保証技術が注目されており，光ディスクにもさらに高い信頼性，保存性，証拠性等が要求されると思われる．

さらに，PC等において個人が扱うデータについても，重要な情報を電子的に扱う機会が増えるにつれてデータの安全性確保のニーズが高まっている．機器の障害やコンピューターウィルスによって保存媒体が損傷を受けた場合，OSやアプリケーションソフトは復元可能であるのに対し，利用者が作成・収集したデータを復元するには多大な労力を要する．原本性保証電子保存システムにおいては，保存されたデータをCPUによって保護することで，コンピューター本体に障害が発生しても内部のデータを守ることができるので，個人用の保存システムとしても同様な機能が要求される可能性は高いと思われる．

なお，「原本性保証電子保存システムの開発」は，情報処理振興事業協会（IPA）による「創造的ソフトウェア育成事業」の一環として（財）ニューメディア開発協会により実施されたものである．2章3節に述べた実験は，通信・放送機構の「マルチメディアパイロットタウン構想」および「創造的通信・放送システム開発事業」に基づく委託により東京工業大学により実施されている．

文　　献

1) 高度情報通信社会推進本部制度見直し作業部会報告書（平成8年6月，総理府内政審議室）．
2) 国分明男，谷内田益義，山口雅浩：“原本性保証電子保存システムの構築”，創造的ソフトウェア育成事業成果報告（情報処理振興事業協会，1998）．
3) 山口雅浩：“原本性保証電子保存システムの構築実験”，機械振興，4月号（1998）62-68.
4) 大山永昭：“電子保存の現状と将来”，日本写真学会誌，**60**（1997）172-176.
5) 大山永昭：“社会の情報化と新たな技術課題”，応用物理，**67**（1998）20-26.
6) 平成10年度マルチメディア・パイロットタウン構想実証実験—高度セキュリティ・モバイル・コンピューティングシステム報告書（東京工業大学，1999）．

（2000年3月16日受理）