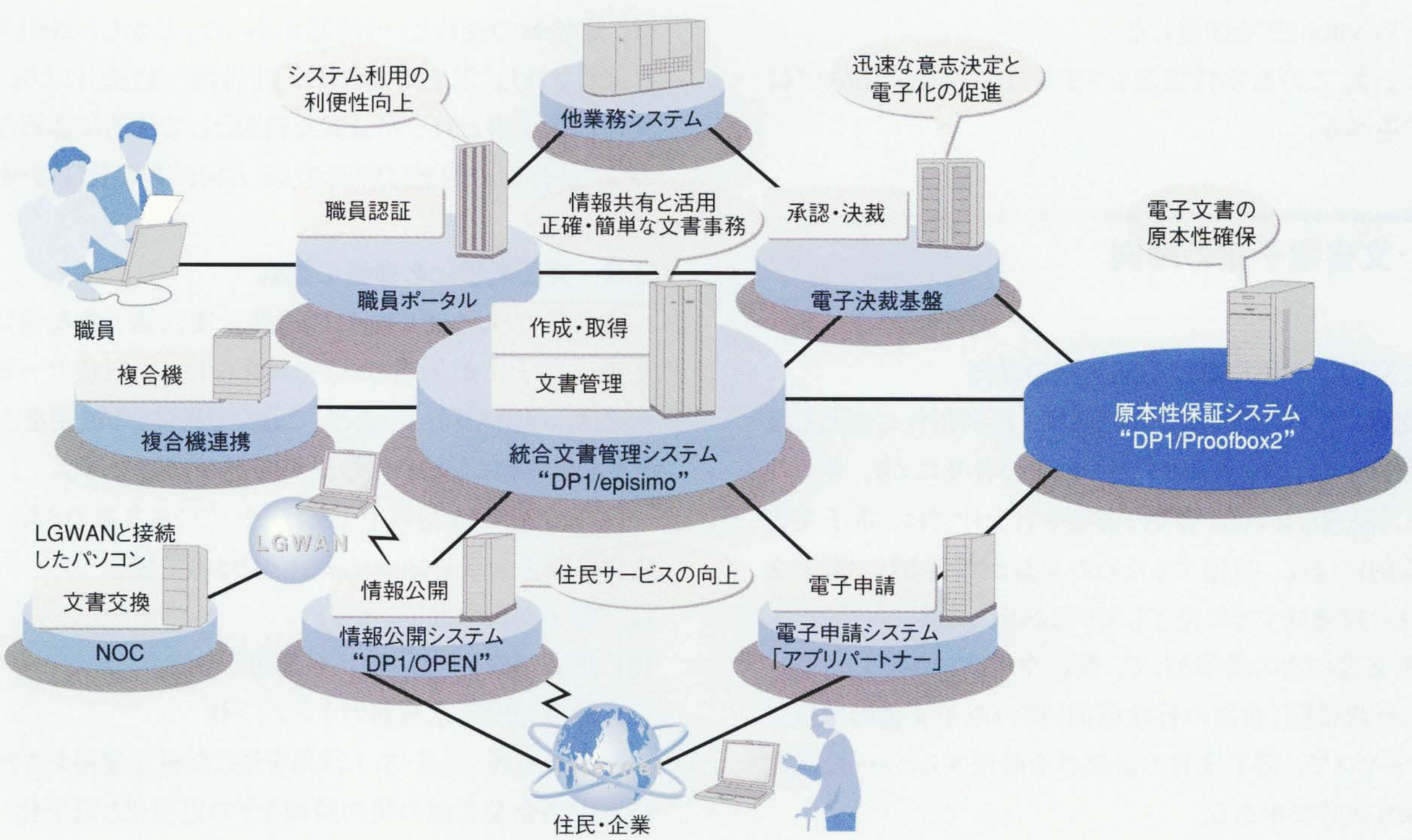
電子文書への不正なアクセスや改ざんを防止する原本性保証システム“DP1/Proofbox2”

Originality Assurance System for Securely Storing Digital Documents

小林 淳二 *Junji Kobayashi*　本多 義則 *Yoshinori Honda*
甲谷 和也 *Kazuya Kôtani*　布上 裕康 *Hiroyasu Nunokami*



注：略語説明　LGWAN（Local Government Wide Area Network），NOC（Network Operations Center）

さまざまな電子文書の関連

健全な行政サービスには，住民からの申請，他省庁・自治体からの文書，庁内業務で発生した文書など，行政のさまざまな場面で発生する電子文書の原本性を保証するシステムが必要である。原本性保証システム“DP1/Proofbox2”では，健全なサービスと，文書保管コスト削減のソリューションを提供する。

近年，行政機関は，電子政府・電子自治体の実現に向けて，申請手続きや調達手続きの電子化を進めている。政府の「e-Japan戦略Ⅱ」では，「民間保存文書の電子的保存の制度面・技術面の検討および電子文書の長期保存の技術開発支援」が掲げられている。これは，電子化した文書では，改ざんや成り済ましなどがあってもその痕跡が残りにくいことから，電子文書の原本性を保証するシステムが必要となっているためである。

日立製作所は，横浜国立大学，早稲田大学，および東京電機大学と共同で開発したヒステリス署名技術を用いて，電子化された文書の原本性を容易に長期間保証する原本性保証システム“DP1/Proofbox2”を開発した。これにより，行政文書や，民間での保存が義務づけられている文書を，信頼できる電子文書として保管し，行政サービスの向上と，文書保管コストの削減を支援する。

1 はじめに

電子文書は，紙文書に比べて改ざんが容易で，その痕跡が残りにくいという問題があることから，電子文書の原本性を証明する技術として，電子署名が一般的に適用されている。しかし，暗号解読技術の進展などにより，時間の経過に伴って電子署名が改ざんされる危険性が増大しているので，署

名の有効期限が定められている。このため，署名の有効期限を超えて長期保存する必要のある大量の文書では，できるだけコストと時間をかけずに署名の有効性を維持することが課題となっている。

政府の「e-Japan戦略Ⅱ」では，2003年度に民間保存文書の電子的保存に関する方向性を定める検討が行われ，2005年度までに電子文書を長期保存するための基礎技術に関する研究開発を進めることになっている。このような文書の電子化の動向を踏まえ，日立製作所は，電子文書の原本性を長期間安全に確保することを目的に，原本性保証システム“DP1/Proofbox2”を開発した。

ここでは，この原本性保証システム“DP1/Proofbox2”について述べる。

2 文書電子化の動向

2.1 文書電子化における法整備の動向

紙文書に比べて保管場所をとらず，再利用性に優れる電子文書は，電子メールやインターネットの普及により，今や社会に広く浸透している。多くの企業や官公庁では，電子文書を日常的に作成，蓄積するための基盤が整備され，電子文書普及の段階はすでに完了している状況である。

電子文書の次の段階として，契約や申請といった，企業・個人と行政機関（複数の行政機関）間の電子文書の交換によるサービスで，電子文書の証拠性を確保するといった課題を解決する必要がある。

電子文書の証拠性を考える場合，紙文書に比べて以下のような課題があげられる。

(1) 目で見るだけでは確認が不可能であり，確認のためにはパソコンなどの装置を必要とする。

(2) コピーが容易であり，元の電子文書の複製を無制限に作成することが可能である。

(3) 文書上に内容更新の記録・痕跡が残らないため，通常の内容更新以外に，悪意の利用者による改ざんも含まれることがある。

(4) 電子文書の作成日付は文書ファイルの作成日時の形で保存されるが，これは変更が可能であり，そのままでは信用できない。

以上の課題を解決することが，「電子文書の原本性の保証」につながる。これについては3章で述べる。

電子文書を証拠書類として扱うことが困難となった背景には，法整備の遅れという問題があった。しかし，2001年4月に施行された「電子署名法」と「IT書面一括法」により，電子文書は紙文書と同等に公式な書類として法的に認められたので，法律面の問題は解消される方向にある（**図1参照**）。

2.2 文書電子化の今後の動向

官公庁では，2001年4月の情報公開法施行を契機に，紙文書の電子化が加速した。それを受けて，行政サービスの面では，申請や届け出など，これまで紙による運用を主体としてきた業務にも電子化の波が広がろうとしている。

「e-Japan戦略Ⅱ」の中であげられている方策のうち，電子文書に関係する主なものは以下のとおりである。

(1) 電子カルテ・電子レセプト

(2) 患者情報システムの相互運用

(3) 診療報酬請求業務のオンライン化

(4) 食の生産・流通・加工段階を通じた相互運用システム

(5) 中小企業金融の契約情報などの定型化と電子化

(6) 中小企業金融の電子手形サービス

(7) 行政サービスの各種システム間の相互運用性

(8) 民間に保存が義務づけられている文書・帳票の電子的な保存

今後は，民間分野の文書の電子化についても法が整備

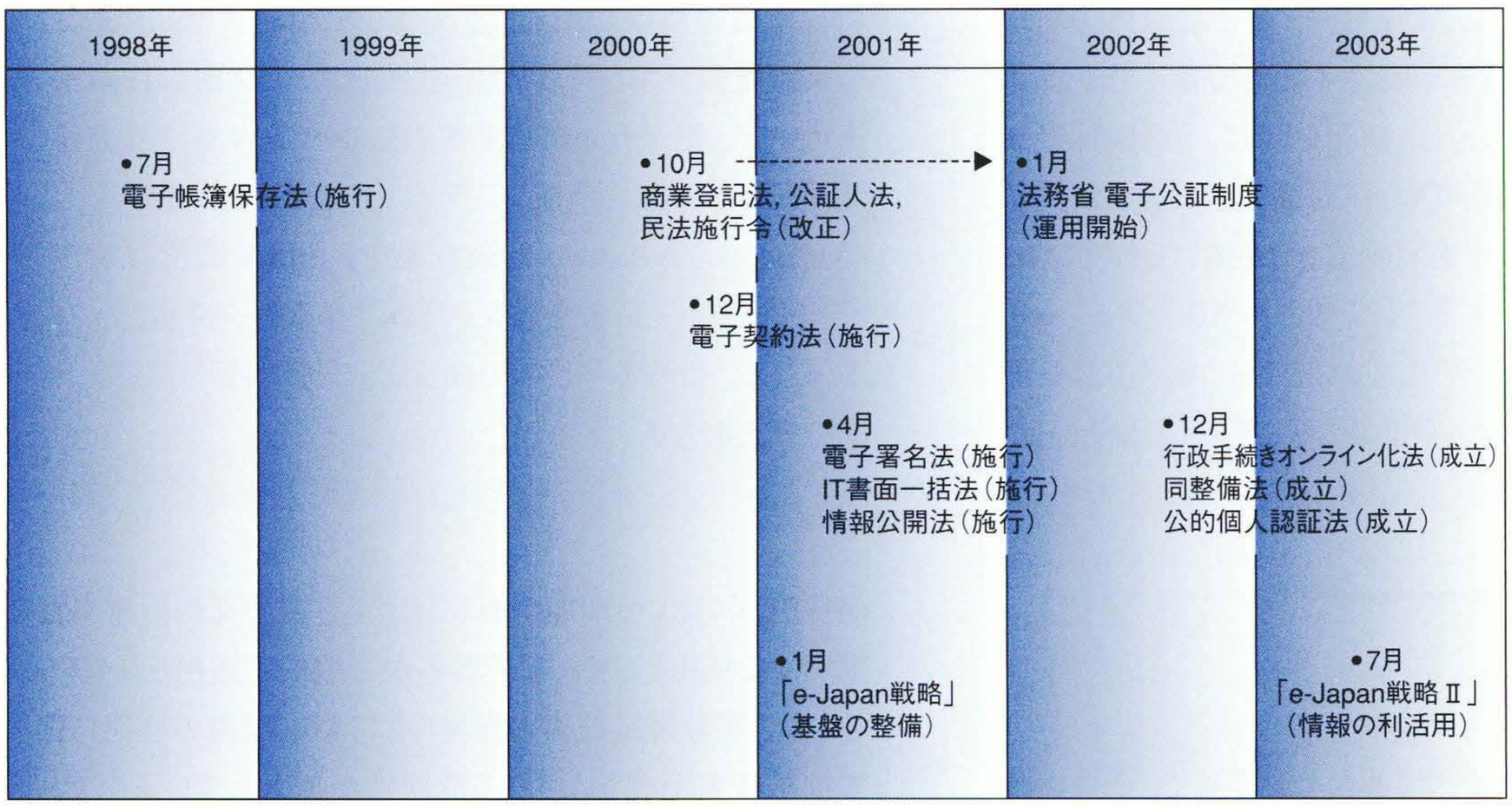


図1 文書電子化に関する法整備の動向
インターネットの普及によって電子文書利用の機会が増加したため，「e-Japan戦略」と並行して，各分野での電子文書に関する法整備が活発化してきている。

表1 規制緩和対象となりうる文書例
各分野で用いられる文書の電子保存が許可される可能性が高い。

分　野	法　令	対象文書(保存年限)
商業	商法	取引帳簿，決算関係書類，現金受け払い・有価証券取引時の証憑(ひょう)書類等(7年)など
税務	所得税法，法人税法，消費税法など	定款，社債原簿等(永久)，株主総会議事録，重要な商業帳簿等(10年)など
保険	保険業法	決約書等(保険契約消滅後5年)など
医療	医師法，薬剤師法，歯科医師法など	診療録(一連の診療完了後5年)，調剤録(3年)など
安全衛生	労働安全衛生法など	健康診断個人票(5年)，被爆線量記録(30年)など

され，規制緩和されていく可能性が高い(**表1**参照)。しかし，これらの文書の電子化を実現するにあたっては，電子文書の原本性を保証することが必要となる。

「e-Japan戦略Ⅱ」では，原本性保証に関して，「電子文書について，故意または過失による改ざん，および消去を防止しつつ，長期間にわたって保存する技術が未整備であるため，技術開発を進める。」という方策が明記されている。

3 電子文書の原本性確保

3.1 電子文書の原本性確保の要件

2000年3月に旧総務庁の共通課題研究会がまとめた「インターネットによる行政手続き実現のために」では，システムとして電子文書の原本性確保を考える場合に，備えるべき三つの要件として，(1) 完全性，(2) 機密性，および(3) 見読性について言及している。

3.2 完 全 性

完全性とは，電子文書が確定的なものとして作成または取得された後に，記録媒体の経年劣化などによる電子文書の消失と変化を防ぎ，さらに，電子文書の改変履歴を記録することによって電子文書の改ざんなどを未然に防止し，改ざんの事実が検証できるような形で保存，管理されることを表す。

システム的には，電子文書のバックアップの取得機能による経年劣化への対策や，電子署名技術の利用などにより，電子データが改ざんされていないことを保証する仕組みを指す。

3.3 機 密 性

機密性とは，重要書類(紙文書)を格納する「金庫」に当たる機能を指す。電子文書は，権限のない者から不正にアクセス(参照・更新・削除)されてはならず，盗難，漏えい，盗み見などを未然に防止する形態で，保存，管理されることが求められる。

システム的には，セキュリティ対策を講じて適切なアクセス制御を行い，電子文書を不正アクセスから防御したり，電子文書の暗号化によって盗み見などを未然に防止する。

3.4 見 読 性

電子文書の保存期限を通して，内容の参照が可能であることを保証することを意味する。重要文書などの長期保存が必要な情報については，作成当時のフォーマットが年月の経過とともに参照できなくなるおそれがある。

長期間保存する文書では，数十年後にも内容の表示が可能であることが必要である。しかし，今のところ，標準的な電子文書のデータ形式は定義されていない。ここ数年はPDF(Portable Document Format)形式が主流であるが，この形式で表示するためには，保存前にPDFを変換して格納するなどの措置が必要である。また，現在のPDF形式が数十年後にも参照が可能かどうかはだれにも予測できない。このため，市場の動向を注意深く見ていくことが必要である。さらに，XML(Extensible Markup Language)形式やTIFF(Tagged Image File Format)形式，テキスト形式などでの保存も併用することが，現状取りうる最も有効な手段であると考える。

導入時に保存形式の選択を誤ると，将来再び形式を変換する必要がある。電子署名や暗号化と組み合わせた運用を前提とした場合，大規模な移行作業が発生するおそれがあるため，保存形式の選択時には慎重な検討を要する。

4 原本性保証システム“DP1/Proofbox2”

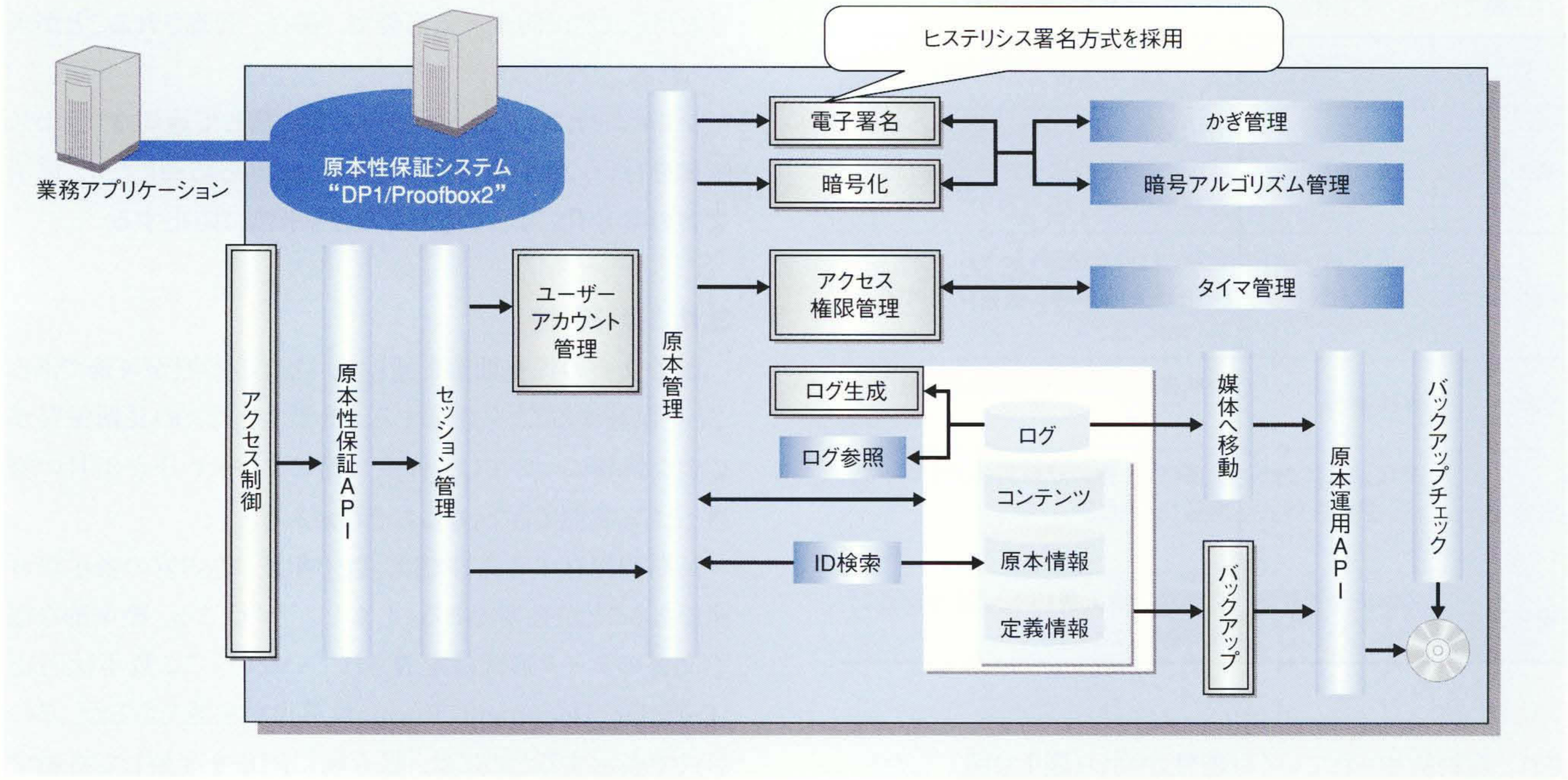
日立製作所は，上述した原本性確保要件に準拠した原本性保証システム“DP1/Proofbox2”を製品化し，提供している(**図2**参照)。この製品の機能と技術について以下に述べる。

4.1 原本性確保要件への対応(完全性・機密性・見読性の確保)

4.1.1 完全性の確保

(1) 電子署名

原本に公開かぎ暗号技術に基づいた電子署名を付与することにより，電子文書が確定的なものとして作成されたあとの，改ざん事実の有無を検証可能にする。しかし，電子署名作成に利用する暗号アルゴリズムは，計算機性能の増大によってぜい弱化するおそれがあるので，公開かぎ証明書には有効期限が設けてある。また，秘密かぎの漏えいなどに



注：略語説明　API(Application Programming Interface)，ID(Identification)

図2 原本性保証システム“DP1/Proofbox2”の機能概要

各種業務アプリケーションとAPIを連携し，DP1/Proofbox2の機能により，電子文書の原本性確保要件(完全性，機密性，見読性)を満たす。特に電子署名では，ヒステリシス署名方式を採用することにより，長期原本性保証を可能にしている。

よって公開かぎ証明書が失効する場合があるため，長期保存という観点では，電子署名だけでは完全とは言えない。

DP1/Proofbox2では，ヒステリシス署名技術を利用し，署名間に連鎖構造を持たせることにより，署名の安全性と有効性を長期間維持している。ヒステリシス署名技術は，日立製作所，横浜国立大学，早稲田大学，および東京電機大学が共同で開発したものである。ヒステリシス署名については，4.2で詳述する。

(2) 書き換え，消去不可の制御

原本として登録された文書には書き換えを一切許さず，文書内容の更新はすべて新しい版の作成として行う。すなわち，更新前の版を残し，更新日時や更新ユーザーなどの履歴を記録する。また，文書の保存期限を設定し，期限前の削除ができないように制御する。

(3) 原本への操作履歴管理

原本として登録した電子文書に，どのようなアクセス(登録，更新，参照，削除，署名検証)が行われたかの履歴を自動的に記録する。

(4) バックアップ·リストア

バックアップ·リストア機能により，記録媒体の経年劣化などによる電子文書の消失と変化を防ぐ。

4.1.2 機密性の確保

(1) アクセス制御

DP1/Proofbox2へのアクセスは専用API経由だけとし，それ以外のアクセスを受け付けない。また，不正アクセスを防止するため，システムを利用するクライアントに，識別のための記号や番号を含む「アカウント(取引窓口)」を発行してID·パスワードによるアクセス制御を行い，ログイン·ログアウトの履歴も記録する。さらに，原本へのユーザーの操作権限や，使用しているファイル操作権限を細かく設定する。

(2) 暗 号 化

万が一，原本が盗難にあったり，盗み見された場合でも，情報の漏えいを未然に防ぐために，原本を暗号化して登録する。

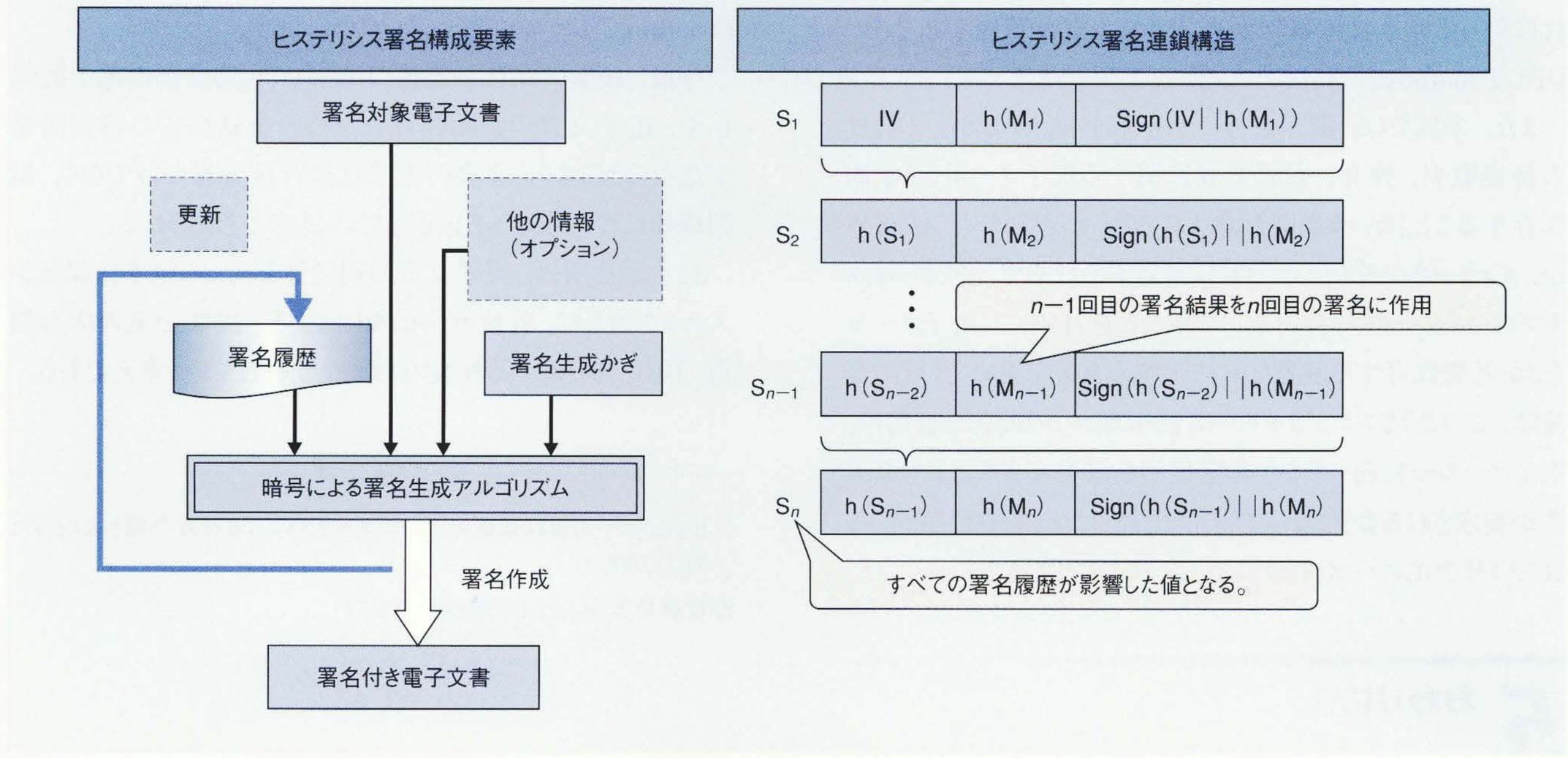
4.1.3 見読性の確保

DP1/Proofbox2では，登録する原本のデータ形式に制限はない。API経由により，原本は作成された形式のまま保管され，データ取得時にはそのままの形式で取り出すことができる。

4.2 長期保存への対応(ヒステリシス署名)

ヒステリシス署名では，n番目の署名を生成する際，署名対象データ単独のハッシュ値ではなく，これに$n-1$番目の署名データ(署名履歴)を結合したデータを，秘密かぎで暗号化することによって署名を行う(**図3**参照)。

このようにすることで署名データ間に依存関係ができるので，攻撃者が文書を改ざん(署名を偽造)しようとした場合，その署名だけでなく，その署名に連鎖する署名(その署名に関連するすべての署名)を偽造しないかぎり，署名連鎖の検証によって改ざんの事実が判明することになる。



注：略語説明　IV(初期値)，h, Sign(一方向性ハッシュ関数，署名生成関数)，Mj・Sj(j番目に生成される署名の対象データ，および署名生成記録)，x||y(x:yとの結合)

図3 ヒステリシス署名の概要

署名間に連鎖構造を持たせることにより，署名の安全性と有効性を長期間維持することができる。ヒステリシス署名技術は，日立製作所，横浜国立大学，早稲田大学，および東京電機大学が共同で開発したものである。

そのため，認証局から発行された公開かぎ証明書の有効期限を過ぎても，文書の改ざん(署名の偽造)が確実に検知されるので，長期間にわたって署名の有効性を維持することができる。

さらに，信頼できる第三者機関に署名履歴を寄託したり，署名履歴の一部を公表することにより，ヒステリシス署名の運用の健全性を保証することができる。

4.3 統合文書管理システム“DP1/episimo”との連携

DP1/Proofbox2では，行政機関用の文書管理パッケージである統合文書管理システム“DP1/episimo”と連携することにより，文書関連業務の実運用に則した形で行政文書の原本性保証を可能にしている(**図4**参照)。

4.4 原本性確保が必要な文書の拡大

「e-Japan戦略」が発表されて以降，官庁を中心に，インターネットを利用した電子申請やワンストップサービスなど，行政サービス向上のためのシステム構築が加速されている。これらのシステムでは，電子文書の原本性保証確保を必須要件としている。さらに，「e-Japan戦略Ⅱ」により，多くの民間保

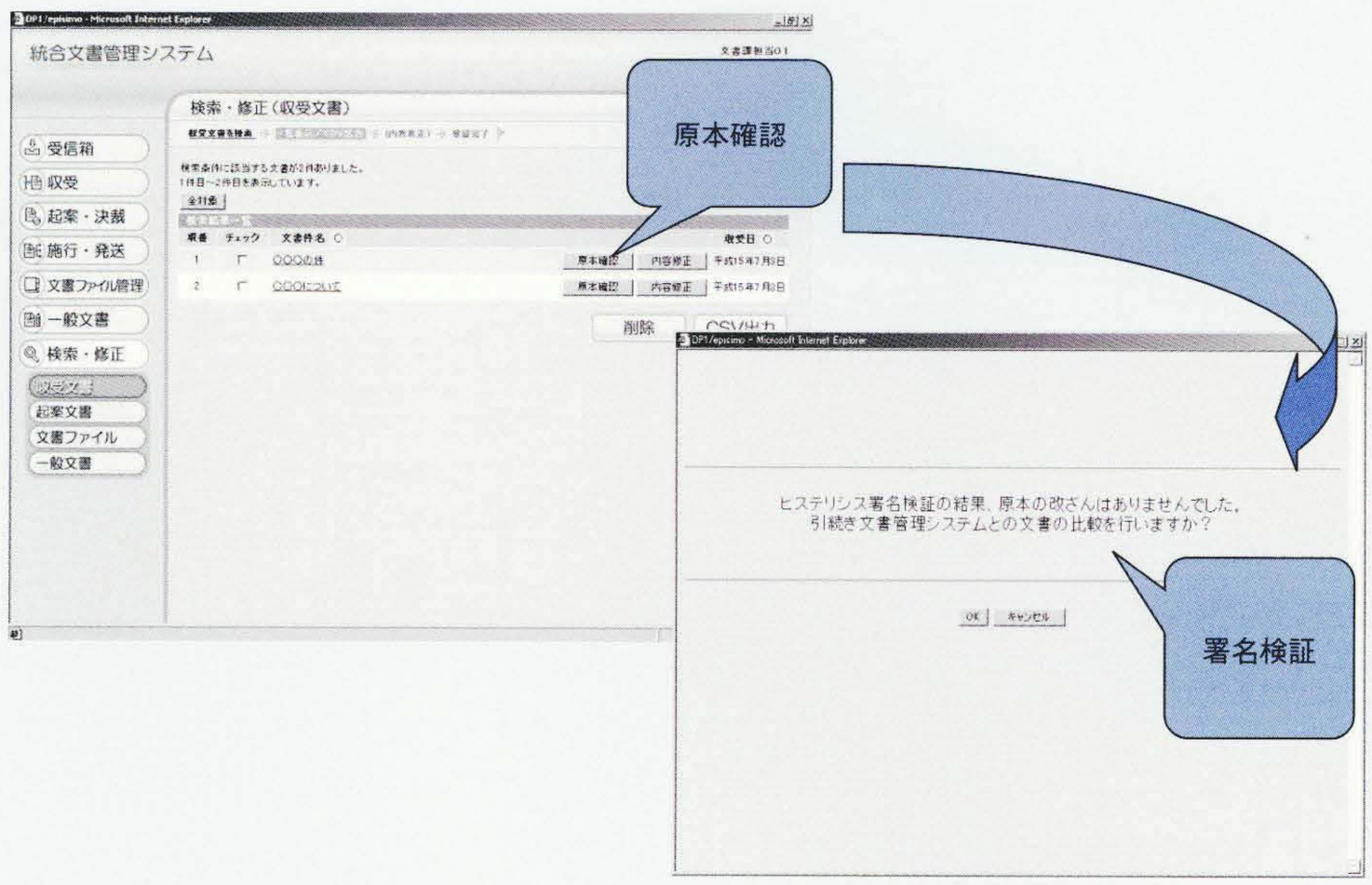


図4 DP1/episimoでの原本性保証システム連携画面例

統合文書管理システム“DP1/episimo”では，登録管理している文書を原本性保証システムにも登録することにより，任意のタイミングで原本を確認することができる。

存文書の電子保存が認可される可能性が高くなっており，それに伴って原本性の確保が要求される文書範囲が拡大し，DP1/Proofbox2の利用ニーズが高まるものと考える。

また，米国では，証券会社の不正取引調査のため，「自社の証券取引，仲介，売買業務に関する電子メールを3年間保存すること」という規則を設けている。わが国でも，法務省が，インターネットを使った犯罪に対処する目的で，インターネットプロバイダーや大手企業，学校などを対象に，電子メールを3か月間保存する義務を立法化する方針を決めている。今後は，このようなコンプライアンス(法令順序)の確保を目的に，電子メールや社内メモなど非定型的な電子文書などにも原本性が要求されるようになっていき，上述した技術や製品が，これらの社会的ニーズにも対応していくものと考える。

5 おわりに

ここでは，「e-Japan戦略II」における電子文書化の動向を踏まえ，日立製作所が開発した原本性保証システム“DP1/Proofbox2”について述べた。

今後，民間に保存が義務づけられている文書の電子的保存や，電子文書の長期保存のための基礎技術の研究開発が進むことにより，文書の電子化は行政分野だけでなく，規制緩和に伴う民間へも広がっていくものと考えられる。

日立製作所は，電子文書の利便性を支える原本性保証システムを通じて，行政サービスの向上と，民間企業の活力創造，国民が参画する社会の形成を支援していく考えである。

参考文献

1) 旧総務庁 共通課題研究会:インターネットによる行政手続き実現のために(2000.3)
2) 政府発表「e-Japan戦略II」(2000.7)

執筆者紹介

小林淳二

1988年日立製作所入社，情報・通信グループ 公共システム事業部 アプリケーションプロダクツ本部 総合行政アプリケーション開発部 第一部 所属
現在，統合内部事務システムの開発に従事
E-mail：j-kobayasi @ itg. hitachi. co. jp

甲谷和也

1990年日立製作所入社，情報・通信グループ 公共システム事業部 全国公共システム本部 関西公共システム第二部 所属
現在，地方自治体系システムの開発に従事
E-mail：koutani @ itg. hitachi. co. jp

本多義則

1991年日立製作所入社，システム開発研究所 第7部 所属
現在，セキュアアーカイブの研究開発に従事
E-mail：y-honda @ sdl. hitachi. co. jp

布上裕康

2000年日立製作所入社，情報・通信グループ 公共システム事業部 アプリケーションプロダクツ本部 総合行政アプリケーション開発部 第一部 所属
現在，統合内部事務システムの開発に従事
E-mail：Hiroyasu. Nunokami @ itg. hitachi. co. jp