H12－認証・公証WG－３

電子署名文書長期保存に関する
中間報告

平成１３年３月

電子商取引推進協議会

認証・公証WG

はじめに

１９７０年ごろにその起源を発し、２０世紀最後の約５年間でその利便性が向上し格段の発展を遂げたインターネットは、業種を問わずおびただしい数の個人や企業がその日常生活や事業推進の中で様々な目的で活用している。この中では情報の検索、受発注、決済、物流等の各段階において、様々なかつ大量の文書がやり取りされている。また、音楽やプログラムなどのデジタルコンテンツは、それ自体がインターネット上で配布されている。

このようなインターネット利用の拡大に伴い、なりすまし、改竄、否認といった、現実の社会においてよりも発生しやすい犯罪が増加傾向にある事は否定できない事実である。これに対応するべく、電子文書に電子署名を施して送り、送付者の本人性と電子文書の完全性を保証する等の電子認証技術が各方面で検討されまた実務に応用されて来ている。しかし、たとえ電子文書に電子署名が施されていても、暗号解読技術の進展等により、長期間の保存に耐えられなくなる状況も考えられるうえ、公開鍵証明書の有効期限を過ぎた後も電子署名の有効性検証を行わなければならない事態が発生する事も想定される。

このような状況を踏まえ、電子商取引のより一層の発展と普及に寄与する目的で、本年度から来年度にかけて、電子認証技術の動向や各方面の対応状況を調査し電子署名文書の長期保存を可能にする為の技術基盤を洗い出すとともに、電子署名文書の長期保存を可能とする為の要件を明確にし、電子署名文書長期保存システムのモデルシステム案を作成・提言する事とした。本年度は、前半の電子認証技術の動向調査・対応状況調査による技術基盤洗出し及び、電子署名文書長期保存を可能とする為の要件を整理したので、ここに中間報告として報告する。

なお、残された課題には次の各事項がある。

（１） 利用局面毎のタイムスタンプの必要性、取得時期、および取得者
（２） 署名ポリシーの具体的内容と署名の有効性判定
（３） 署名者、検証者、仲裁者の観点からの電子署名長期保存に対する要件検証

来年度は、今年度の成果も元にしながらこれらについての検討を深め、電子署名文書長期保存システムのモデルシステム案を作成・提言する予定である。

本中間報告書は、以下の５章で構成されている。

第 1 章では、実社会において長期保存が必要なケースを述べると供に、印影と電子署名の対比について述べる。また、電子文書の真正性（本人性及び完全性）が電子署名によりどのように保証されるのかを述べる。

第２章では、公開鍵証明書と、公開鍵証明書に基づく電子署名－デジタル署名－それ自体の制約について述べ、どのような場合に公開鍵証明書が無効である又は有効であることを確認する事が可能か、あるいは不可能か、署名が生成された時間による違いについて述べる。そして最後に、真正性を長期にわたって保証するための要件について整理する。

第３章では、第２章で述べた様々な要件を受けて、最初に電子署名文書の長期保存に利用できる要素技術とその実装システムについて紹介する。次に、電子文書を改竄できない安全な領域を実現する技術である原本性保証システムと、電子認証と並び電子申請・企業間商取引・電子文書長期保存を支えるプラットフォームである電子公証について紹介する。

第４章では、今回の中間報告書で使われている用語の内、主なものについて解説すると供に、調査の過程で参考とした文献について紹介している。

第５章では、検討メンバーリストを掲載している。

今回の中間報告を元にして来年度末の報告をより実効的なものとする為に、各界各方面から忌憚の無いご意見を頂きたいと考えております。ご意見等ございます方は下記連絡先までお寄せ頂くようお願い申し上げます。

連絡先

電子商取引推進協議会（ＥＣＯＭ）
認証・公証ＷＧ
〒 135-8073
東京都江東区青海 2-45　タイム 24 ビル 10 階
TEL. 03-5500-3600
FAX. 03-5500-3660
Ｅ-mail： info@ecom.or.jp
http://www.ecom.or.jp/

目　次

1　電子署名文書長期保存の必要性

1.1　長期保存が必要なケース

私たちは日常生活において､紙面に印刷されたさまざまな書式の｢文書｣を目にすることがある。例えば、町内会の回覧板に綴じてある「お知らせ」から、企業等で使用される「稟議書」や「決算報告書」、国会での「議事録」や「審議録」等、その種類は実にたくさんある。

さて、ある時点における「ことがら」を文書として著し、それをその当事者がある期間保管しておくことによって、その「ことがら」がある時点に存在していたことを保証することができる。例えば、「売買契約書」、「領収書」、「土地の権利書」、「借用書」等がこれにあたる。

このように、「ことがら」の当事者によってある期間の保管を必要とする「文書」のうち、法律によって長期的な保管を義務付けている文書がある。ここで、行政・医療等を例として保存期間が 1 年、3 年、5 年、10 年、30 年以上の長期的保存が義務付けられている文書の一部を示す。

1.1.1　行政

「行政文書の管理方策に関するガイドライン」［1］では、行政文書の最低保存期間基準を以下のように定めている。

1. 保存期間 30 年

① 法律又は政令の制定、改正または廃止その他の案件を閣議にかけるための決済文書

A.　条約その他の国際約束の署名、又は締結のための決済文書

B.　法律の制定・改廃の決済文書

C.　特殊法人の設立・廃止の決済文書

D.　基本的な計画の策定・変更・廃止の決済文書

E.　予算・組織・定員の基本的事項の決済文書

② 特別の法律により設立され、かつ、その設立に関し行政官庁の認可を要する法人（以下「認可法人」という。）の新設又は廃止に係る意思決定を行うための決済文書

A.　認可法人の設立・廃止の決済文書

③ ①又は②に掲げるものの他、国政上の重要な事項に係る意思決定を行うための決済文書

A.　関係閣僚会議付議のための決済文書

B.　政務次官会議付議のための決済文書

C.　事務次官等会議付議のための決済文書

④ 内閣府令、省令その他の規則の制定、改正又は廃止のための決済文書

A.　府省令等の制定・改廃のための決済文書

B.　行政文書の管理に関する定め

⑤ 行政手続き法（平成 5 年法律第 88 号）第 2 条第 3 号に規定する許認可等（以下単に「許認可等」という。）をするための決済文書であって、当該許認可等の効果が 30 年間存続するもの

A.　公益法人設立許可の決済文書

B.　事業免許、資格免許等の許認可の決済文書

⑥　国又は行政機関を当事者とする訴訟の判決書

A.　判決書（正本）

⑦　国有財産法（昭和 23 年法律第 73 号）第 32 条に規定する台帳

A.　国有財産台帳

⑧　決済文書の管理を行うための帳簿

A.　決済簿

⑨　施行令第 16 条第 1 項第 10 号の帳簿

A.　行政文書ファイル管理簿

⑩　公印の制定、改正又は廃止を行うための決済文書

A.　公印の制定、改正又は廃止を行うための決済文書

⑪　①から⑩までに掲げるもののほか、行政機関の長がこれらの行政文書と同程度の保存期間が必要であると認めるもの

A.　特殊法人又は認可法人の管理に必要な台帳

2. 保存期間 10 年

①　内閣府設置法第 37 条若しくは第 54 条、宮内庁法第 16 条第 1 項又は国家行政組織法第 8 条の機関の答申、建議又は意見が記録されたもの

A.　審議会等の答申、建議または意見

②　行政手続法第 5 条第 1 項の審査基準、同法第 12 条第 1 項の処分基準その他の法令の解釈又は運用の基準を決定するための決済文書

A.　法令の解釈・運用基準の決済文書

B.　許認可等の審査基準

C.　不利益処分の処分基準

③　許認可等をするための決済文書であって、当該許認可等の効果が 10 年間存続するもの（1.の項⑤に該当するものを除く。）

A.　有効期間が 10 年以上の許認可等をするための決済文書

④　①から③までに掲げるもののほか、所管行政上の重要な事項に係る意思決定を行うための決済文書（1.の項に該当するものを除く。）

A.　条約その他の国際約束の解釈・運用基準の決済文書

B.　所管行政に係る重要な政策の決定に係る決済文書

⑤　不服申立てに対する裁決又は決定その他の処分を行うための決済文書

A.　行政不服申立て、行政審判その他の争訟の裁決書、裁定書、決定書

⑥　栄典又は表彰を行うための決済文書

A.　叙勲、褒賞又は各種表彰の決済文書

⑦　①から⑥までに掲げるもののほか、行政機関の長がこれらの行政文書と同程度の保存期間が必要であると認めるもの（1.の項に該当するものを除く。）

A.　政策決定の基礎となった国際会議等の決定

B.　概算要求書

3.　保存期間 5 年

①　法律又はこれに基づく命令により作成すべきものとされる事務及び事業の基本計画書若しくは年度計画書又はこれらに基づく実績報告書

A.　事務又は事業の方針・計画書

B.　事務又は事業の実績報告書

②　独立行政法人、特殊法人、認可法人又は民法（明治 29 年法律第 89 号）第 34 条の規定により設立された法人の業務の実績報告書

A.　業務実績報告

B.　指導監督の結果報告書

③　許認可等をするための決済文書であって、当該許認可等の効果が 5 年間存続するもの（1.の項⑤又は 2.の項③に該当するものを除く。）

A.　有効期間が 5 年以上 10 年未満の許認可等をするための決済文書

④　行政手続法第 2 条第 4 号の不利益処分（その性質上、それによって課せられる義務の内容が軽微なものを除く。）をするための決済文書

A.　許認可等の取消しの決済文書

B.　資格剥奪の決済文書

C.　欠格期間が 5 年間以上の不利益処分の決済文書

⑤　①から④までに掲げるもののほか、所管行政に係る意思決定を行うための決済文書（1.の項、2.の項、4.の項又は 5.の項に該当するものを除く。）

A.　補助金交付決定書

B.　補助事業実績報告書

⑥　予算決算及び会計令（昭和 22 年勅令第 165 号）第 22 条に規定する書類又はその写し

A.　請求書、領収書、契約書

B.　決議書（支出決議書等）

⑦　取得した文書の管理を行うための帳簿、又は行政文書の廃棄若しくは移管の状況が記録された帳簿（施行令第 16 条第 1 項第 9 号の記録を含む。）

A.　廃棄簿

B.　移管引継簿

⑧　①から⑦までに掲げるもののほか、行政機関の長がこれらの行政文書と同程度の保存期間が必要であると認めるもの（1.の項または 2.の項に該当するものを除く。）

A.　指導要綱等複数の者に対する行政指導書

4. 保存期間 3 年

①　許認可等をするための決済文書であって、当該許認可等の効果が 3 年間存続するもの（1.の項⑤、2.の項③または 3.の項③に該当するものを除く。）

A.　有効期限が 3 年以上 5 年未満の許認可等をするための決済文書

②　所管行政上の定型的な事務に係る意思決定を行うための決済文書（5.の項に該当するも

のを除く。）

A.　研修実施計画

③　調査または研究の結果が記録されたもの

A.　政策の決定または遂行に反映させるために実施した調査または研究の結果報告書

④　③に掲げるもののほか、所管行政に係る政策の決定または遂行上参考とした事項が記録されたもの

A.　予算要求説明資料

B.　業務上の参考としたデータ

C.　行政運営上の懇談会の検討結果

⑤　職員の勤務の状況が記録されたもの

A.　兼業の申請、承認に係るもの

B.　退職手当支給に係るもの

⑥　①から⑤までに掲げるもののほか、行政機関の長がこれらの行政文書と同程度の保存期間が必要であると認めるもの（1.の項から 3.の項までに該当するものを除く。）

A.　欠格期間が 3 年以上 5 年未満の不利益処分に係る決済文書

5. 保存期間 1 年

①　許認可等をするための決済文書（1.の項⑤、2.の項③、3.の項③または 4.の項①に該当するものを除く。）

A.　有効期間が 1 年以上 3 年未満の許認可等をするための決済文書

②　所管行政上の軽易な事項に係る意思決定を行うための決済文書

A.　欠格期間が 1 年間以上 3 年未満の不利益処分に係る決済文書

B.　事案照会

C.　会議開催通知書

D.　講師依頼書

E.　資料送付書

F.　式辞、祝辞

③　所管行政に係る確認を行うための決済文書（1.の項から 4.の項までに該当するものを除く。）

A.　請願書

B.　届出書

1.1.2　医療

1.　保存期間 5 年間

①　診療録（医師法第 24 条、歯科医師法第 23 条）

②　助産録（保健婦助産婦看護婦法第 42 条）

③　救急救命処置録（救急救命士法第 46 条）

2. 保存期間 3 年間

① 調剤録（薬剤師法第 28 条）

② 療養の給付の担当に関する帳簿及び書類その他の記録（保健医療機関及び保健医療養担当規則第 9 条）

③ 療養の給付に関する処方箋及び調剤録（保健薬局及び保健薬剤師療養担当規則第 6 条）

④ 記録（歯科衛生士法施行規則第 18 条）

3. 保存期間 2 年間

① 指示書（歯科技工士法第 19 条）

1.1.3 その他

① 国税関係帳簿書類［2］

A. 仕訳帳、総勘定元帳等の帳簿（7 年）

B. 棚卸表、賃借対照表、損益計画書（7 年）

C. 注文書、見積書、契約書の控え（7 年）

D. 財産形成非課税貯蓄申込書、異動申請書（5 年）

E. 商業帳簿（10 年）

② 公正証書

公証役場における公正証書の保存期間は、原則として 20 年と定められている。ただし公証する内容が、例えば定期借地権などで 50 年の契約であるような場合には、その期間保存義務がある。

1.2 印影と電子署名の対比

一般に、長期的な保管を必要とする類の文書には、その真正性[1]を保証するために印影を押印する場合が多い。さて、このような紙媒体の印影付文書を電子化するためにはどのようにすればよいだろうか。

上記の問題を解決するものとして、現在「電子署名」が注目されている。本節では、電子署名の運用を電子的な印鑑登録制度と解釈し、印鑑[2]（実印[3]）を秘密鍵（署名鍵）に、印影を電子署名（デジタル署名）に、そして印鑑登録証明書を公開鍵証明書に対応させ、電子署名が電子文書に対して有効であることを述べる。

---

[1] ここでいう「真正性」とは、文書が作成者本人によって作成されたということ（本人性）、およびその文書が第三者によって加筆・修正されていないということ（完全性）を指す。

[2] 印鑑には、「実印」、「銀行印」、「認印」がある。また印鑑には、本来の用途とは別に「契印（割印）」、「訂正印」、「捨印」等の使い方がある。それぞれの詳細については本節末を参照。

[3] 市区町村役場に印鑑登録されている印鑑。印鑑登録を行うためには一定の基準（＊）を満たしている必要がある。＊：印鑑登録証明事務処理要領（昭和 49 年 2 月 1 日　自治振興第 10 号各都道府県総務部長あて自治省行政局振興課長通知「印鑑の登録及び証明に関する事務について」）

1.2.1　印影と印鑑登録証明書との関係

- **法制化：「印鑑の登録及び証明に関する事務について」（昭和 49 年 2 月 1 日 自治振第 10 号自治省行政局振興課長から各都道府県総務部長あて通知　最終改正 平成 11 年 12 月 22 日 自治振第 175 号）**
- **登録先：地方自治体（市区町村役所）**
- **手続き（個人）：印鑑の登録を受けようとする者（登録申請者）は、原則として登録を受けようとする印鑑を自ら持参し、登録の申請を書面で市町村長に対して行う。**
- **手続き（法人）：登記所（法務局）が厳格な商業登記申請手続に基づき代表者などを登記する手続きを行っており、これに基づいて発行される。**
- **登録者への発行：印鑑登録証明書**

図 1-1に、印影（実印）と印鑑登録証明書との関係を示す。発信者は、受信者に対して押印文書とともに印鑑登録証明書を添付して送付する。一方、受信者は押印文書の印影と印鑑登録証明書の印影とを比較することで、実印によって押印された文書であるか否かを判断できる[4]。

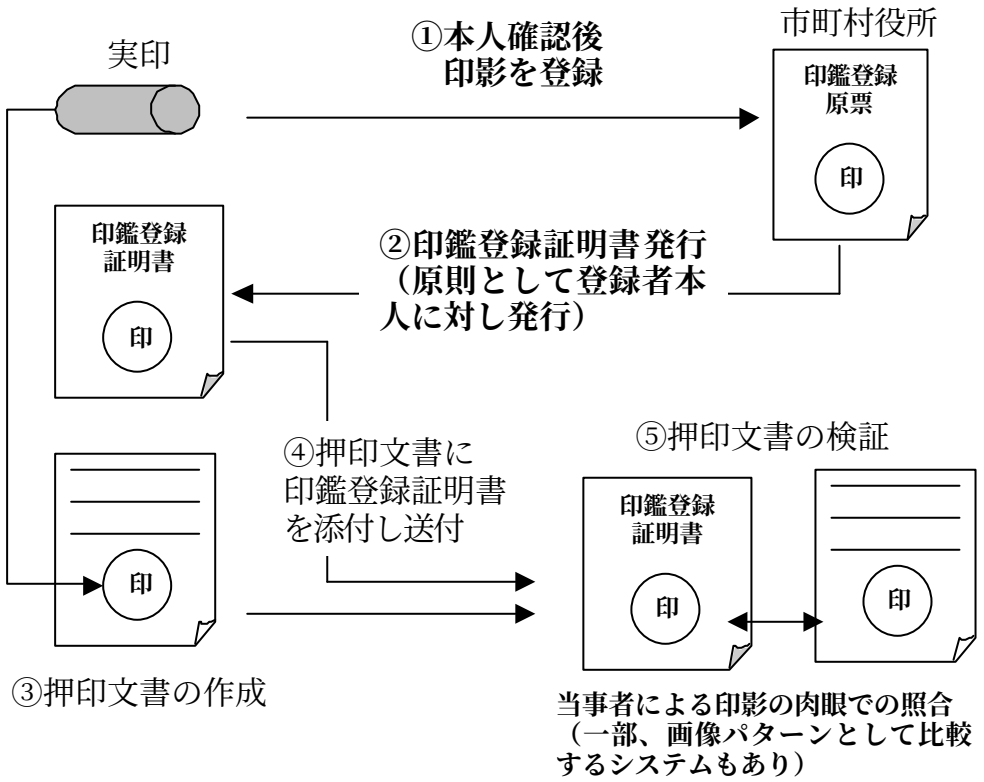

図 1-1 印影と印鑑登録証明書との関係

[4] **民事訴訟法第 228 条第 4 項に、「私文書は、本人又はその他の代理人の署名又は押印があるときは、真正に成立したものと推定する」とあるように、印鑑登録証明書で示した印影と押印文書の印影が同じであれば、押印文書が実印で押印されたものであることを判断できる。ただし、登録した印鑑は所持者によって厳密に保管されていなければならない。**

1.2.2　電子署名と公開鍵証明書との関係

- 法制化：「電子署名法」（電子署名及び認証業務に関する法律）
- 登録先：認証機関
- 手続き：認証機関が公開鍵の登録時に行うべき本人確認の方法は、電子署名法で認定を受ける認証機関については別途省令等で規定する基準に従うことになっている。
- 登録者への発行：公開鍵証明書

図 1-2に示すように、署名者は文書のハッシュ値を署名鍵で暗号化して電子署名（デジタル署名）文書を作成し、認証機関より発行された公開鍵証明書を添付して送付する。受信者は公開鍵証明書から公開鍵を取出し、送付文書からのハッシュ値と公開鍵でデジタル署名を検証して取出したハッシュ値を比較することで、電子署名が公開鍵と対である秘密鍵によって付与されたことが検証できる。

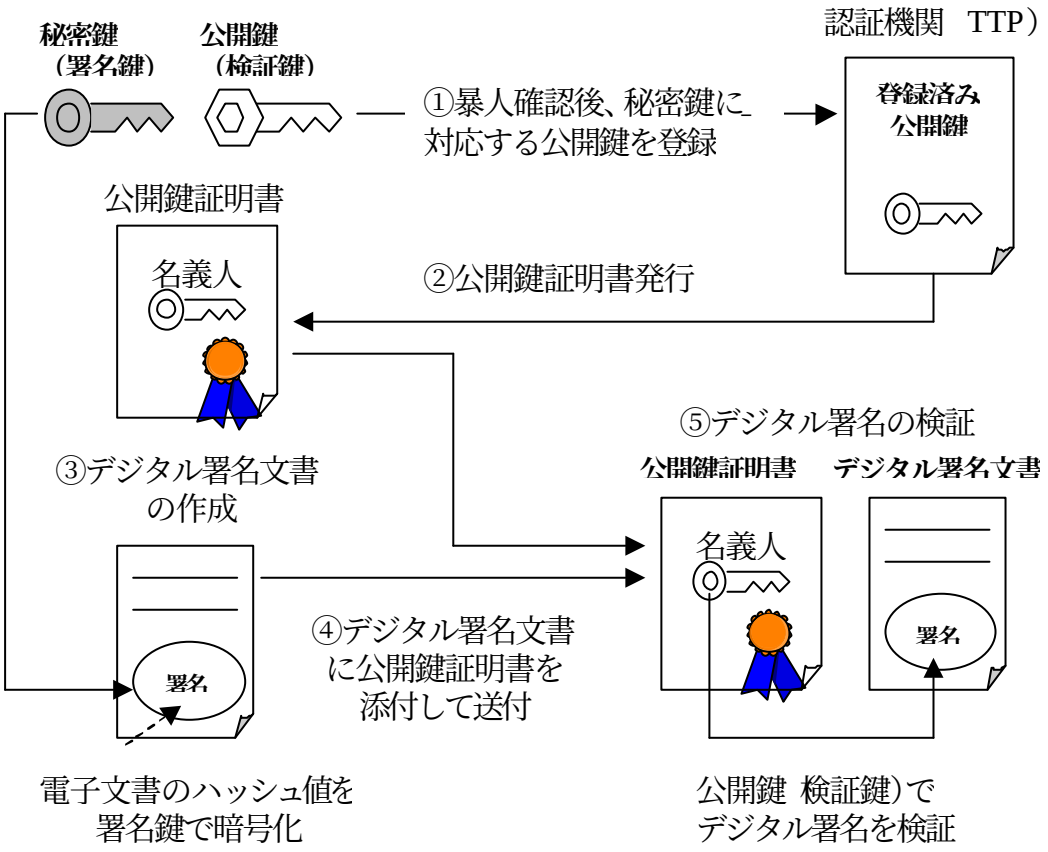

図 1-2　電子署名（デジタル署名）と公開鍵証明書との関係

参考

(1) 印鑑の種類と用途

① 実印

不動産の登記、自動車の売買／登録、金銭の貸借などの契約時に利用。押印者の責任が大きい。

② 銀行印

銀行で利用するために銀行へ届出ている印鑑。口座の開設や預金の引き出しなどに利用。実印と同様に押印者の責任が大きい。実印同様、登録者の身元確認を証明しなければ登録できないため、効力は実印に近い。

③ 認印（三文判）

実印、銀行印以外の印鑑を指す。日常生活の中で使用している印鑑。実印や銀行印に比べて、押印者の責任は小さい。

(2) その他の用途

契印（割印）：文書の頁と頁との間に続きを明らかにするために頁間に跨いだ押印。

訂正印：訂正した箇所、上部空白部への加筆または削除した文字数を記載後に押印。

捨印：あらかじめ押印しておく訂正印。

1.3 電子文書の本人性と完全性

一般に、電子文書には以下に示す 2 つの問題点がある。

(1) 本人性の検証が困難

例えば電子メールによって、作成者 A からある電子文書 M を受け取ったとする。作成者 A が電子文書 M を自らが作成したことを主張したとしても、受信者 B はその電子文書 M が作成者 A によって作成されたかどうかを検証すること（本人性の検証）は困難である。また、電子文書 M の作成者 A が、それを確かに作成したという事実（本人性）を第三者に対して証明することも、上記と同様に困難である。

(2) 完全性の保証が困難

紙媒体の文書と比べると、電子文書は改竄の検出が困難である。例えば、電子メールやフロッピーディスク等で受け取った電子文書 M に対して改竄が行われていないという事実（完全性）を検証することは困難である。

さて、上記のような問題を解決し、電子文書の「本人性」と「完全性」を保証するものとして、前節で述べた「電子署名」が期待されている。図 1-3に、電子署名[5] が施された電子文書（以下、電子署名文書）の「本人性」と「完全性」を検証する仕組みを示す。

「本人性」と「完全性」の検証プロトコル

(1) A は作成した電子文書からハッシュ関数 H を用いてハッシュ値を生成する。

[5] 電子署名の生成方法には、電子文書に対して直接生成する場合のほか、電子文書からハッシュ値を計算し、そのハッシュ値に対して生成する場合もある。ここでは、ハッシュ値に対して電子署名を生成する場合をとりあげる。

(2) A は(1)のハッシュ値に対し自分の秘密鍵を用いて電子署名を生成する。

(3) A は電子文書に電子署名とあらかじめ認証局から発行された証明書を添付し、これを電子署名文書として B に送る。

(4) B は受け取った電子署名文書から電子文書を取出し、ハッシュ関数 H を用いてハッシュ値を生成する。

(5) B は認証局が提供する失効リストをもとに、証明書が有効であるか否かを検証する。

(6) B は電子署名文書に添付されている証明書から A の公開鍵を取出す。

(7) B は A の公開鍵を使って電子署名文書に添付されている電子署名を検証し、ハッシュ値を得る。

(8) (4)で生成したハッシュ値と(7)で得たハッシュ値とを比較する。

(9) ２つのハッシュ値が一致した場合、A の秘密鍵で電子署名が生成されたこと（本人性）および電子文書が途中で第三者によって改ざんされていないこと（完全性）が確認できる。

(10) (9)においてハッシュ値が一致しなかった場合、本人性および完全性は立証できないことになる。

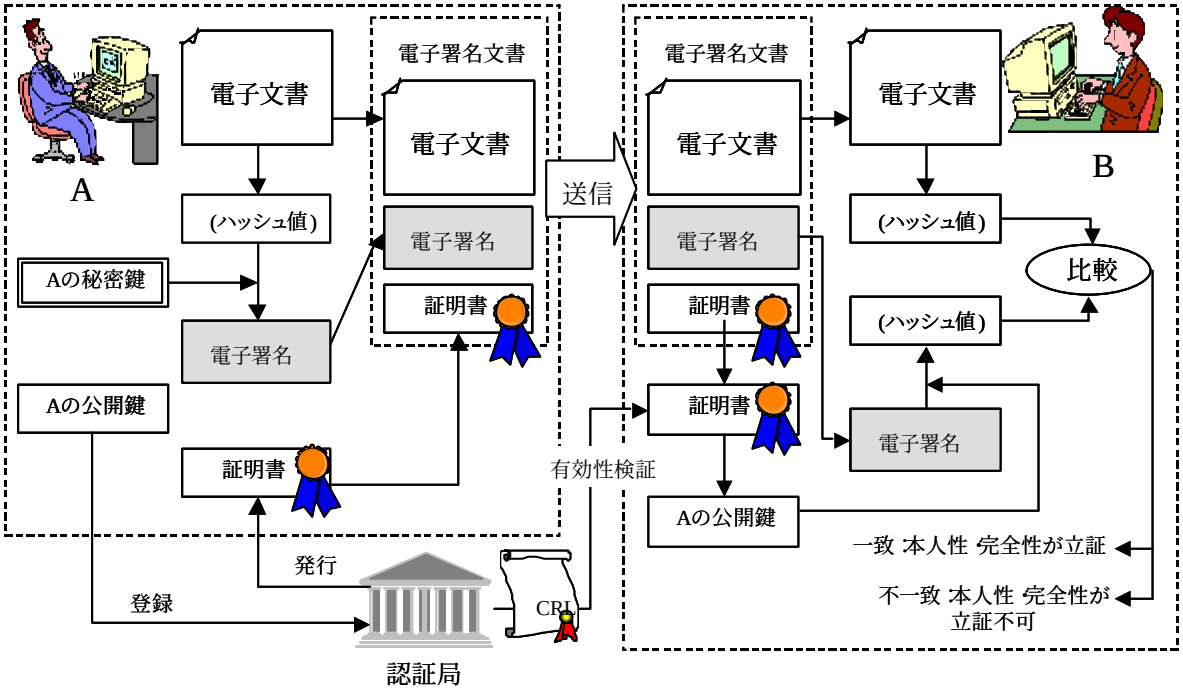

図 1-3 電子署名文書の 本人性」と完全性」の検証

これにより、電子署名が施された電子文書（電子署名文書）の「本人性」および「完全性」の検証を行うことが可能となる。

2　電子署名長期保存に対する要件［3］

2.1　デジタル署名の問題点

前章で述べたように、公開鍵証明書に基づく電子署名－デジタル署名－を用いることにより電子文書の真正性（本人性及び完全性）を確保することができる。また、デジタル署名の有効性が、公開鍵証明書によって裏付けられることも述べた。つまり、デジタル署名によって電子文書の真正性を確保するためには、デジタル署名に用いる秘密鍵に対応する公開鍵証明書が有効でなければならない。

ところが本来、公開鍵証明書は次にあげる制約を伴う。

- 公開鍵証明書には有効期限が必ず存在する
- 公開鍵証明書には失効が発生する可能性がある

また、デジタル署名自体も次の制約を持つ。

- デジタル署名の基礎になる暗号技術は脆弱化して破られる可能性がある

上記の３つの制約は、長期保存を考える場合、いずれもデジタル署名の有効性の判断に大きな影響を与える。以下、各制約がデジタル署名の有効性に与える影響について記す。

2.1.1　公開鍵証明書の有効期限

公開鍵証明書（X.509）は、基本領域として証明書有効期間（Validity）を記載する領域を持つ。この領域は公開鍵証明書が有効となる日時と有効性を喪失する日時を規定するものであり、必ず設定しておかなければならない。公開鍵証明書が有効である期間は、2.1.2節で述べる失効が発生しない限り、この領域に示された期間となる。有効期間の長さは認証局のポリシーによって決定されるが、一般的には数ヶ月乃至数年の範囲である。

図 2-1は公開鍵証明書の有効期間とデジタル署名生成時期による署名の有効性の関係を示す図である。この図に示すように、公開鍵証明書の有効期間外にその証明書に基づく署

名を生成した場合、有効なデジタル署名とは見なされない。つまり、公開鍵証明書の有効期間外に生成されたデジタル署名では、電子文書の真正性を確保することは出来ない。

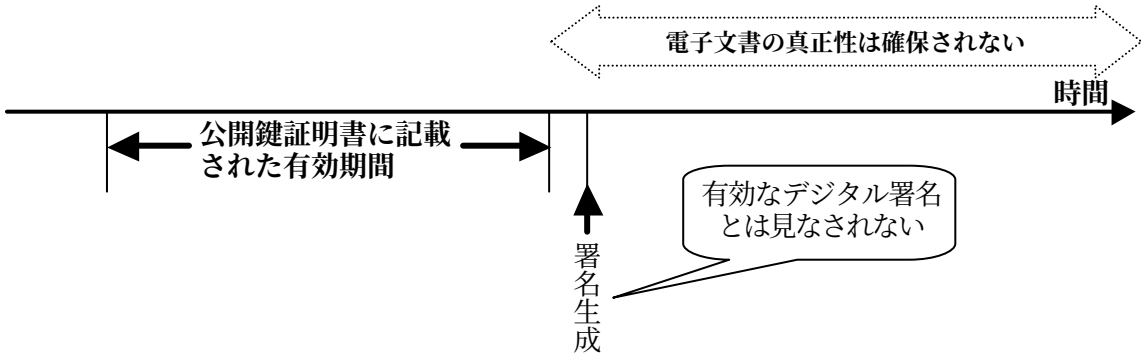

図 2-1 証明書有効期間とデジタル署名の関係(1)

デジタル署名の生成を公開鍵証明書の有効期間内に行った場合について図 2-2に示す。このとき、失効がないと仮定すれば、公開鍵証明書の有効期間内の署名検証に対しては「有効」と判断される。ところが、有効期限を過ぎた後に検証すると、通常、「無効」と判断されることになる。これは、公開鍵証明書の有効期間後においては、秘密鍵が漏洩しないように厳密に管理あるいは破棄されることを保証できないためである。つまり、生成された当初は有効であったデジタル署名であっても、電子文書の真正性を確保できる期間は公開鍵証明書の有効期間内に制限されることになる。

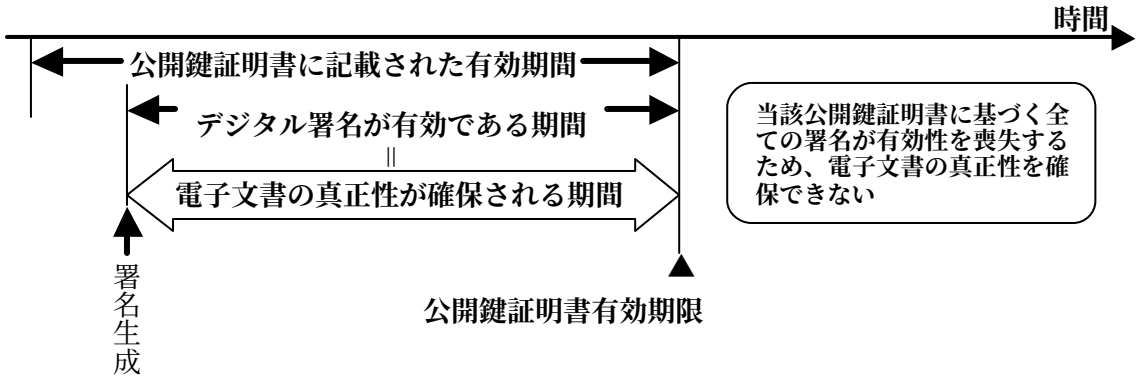

図 2-2 証明書有効期間とデジタル署名の関係(2)

生成された署名が有効期間内に生成されたものか否かを判断することは可能であろうか？有効期間を過ぎても、その署名が有効期間内に生成されたものであることが確認でき

れば（失効はないと仮定）その署名が生成時点で有効であったことが確認でき、それをもって有効期限を過ぎた時点でもその署名を有効であると見なすこと、すなわち、その署名によって電子文書の真正性が確保されていると見なすことも可能であると考えられる。

CMS（Cryptographic Message Syntax: IETF RFC2630）［4］の署名データフォーマットでは、属性データとして署名生成時刻（Signing Time）を設定できるようになっている。ところがこの値が正確であることは保証されておらず、この値を頼りにその署名が有効期間内に生成されたか否かを確認することはできない。通常は有効期間以前に署名が生成されることはないと仮定すると、有効期限に達する前であれば署名は有効期間内に生成されたと見なすことができるが、有効期限を越えてしまうと、その署名が有効期間内に生成されたものであるか、有効期限を過ぎてから生成されたものであるかを区別することはできなくなってしまう。従って現在のデジタル署名の枠組みのみでは、有効期間を超えてしまうと、署名生成が有効期間内に行われたか否かを判断することさえできなくなってしまう。

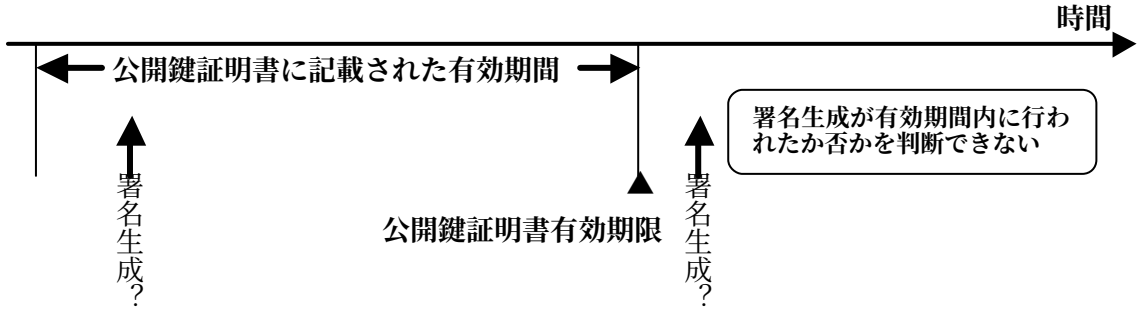

図 2-3 証明書有効期間とデジタル署名の関係(3)

ここまで公開鍵証明書の基本領域として規定されている証明書有効期間についてのみ取り上げてきたが、標準拡張領域ではデジタル署名の生成に用いる秘密鍵（Private Key）の使用期間を規定できるようになっている。しかし標準仕様ではこの領域の使用を推奨されていないためここでは言及しないこととする。

2.1.2 公開鍵証明書の失効

公開鍵証明書には、有効期間内にはあるが何らかの理由により信頼しないこととするために「失効」というメカニズムが用意されている。失効が生じる原因としては、秘密鍵の

危殆化、あるいは氏名等の重要な属性情報の変更などが挙げられる。失効は認証局が発行する失効リストによって関係者に公開される。

公開鍵証明書の有効期間内であり、かつ失効後に生成されたデジタル署名の有効性を図示すると図 2-4のようになる。公開鍵証明書の有効期間内であっても、失効後に生成されたデジタル署名は有効なデジタル署名とは見なされない。つまり、公開鍵証明書の失効後に生成されたデジタル署名では、電子文書の真正性を確保することはできない。

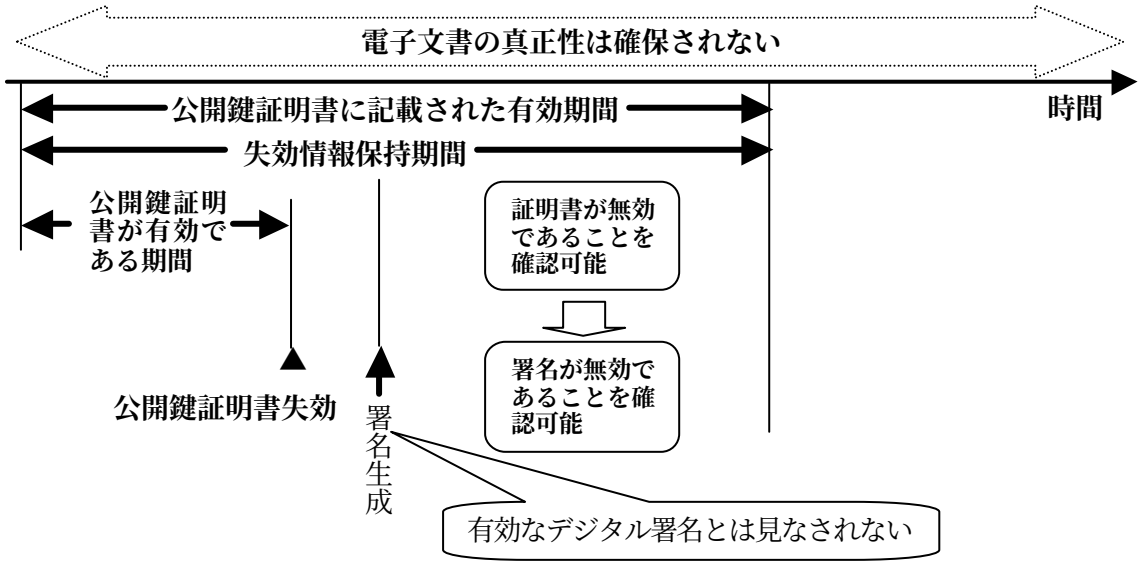

図 2-4 証明書失効とデジタル署名の関係(1)

公開鍵証明書の有効期間内であり、かつ失効前に生成されたデジタル署名の有効性を図

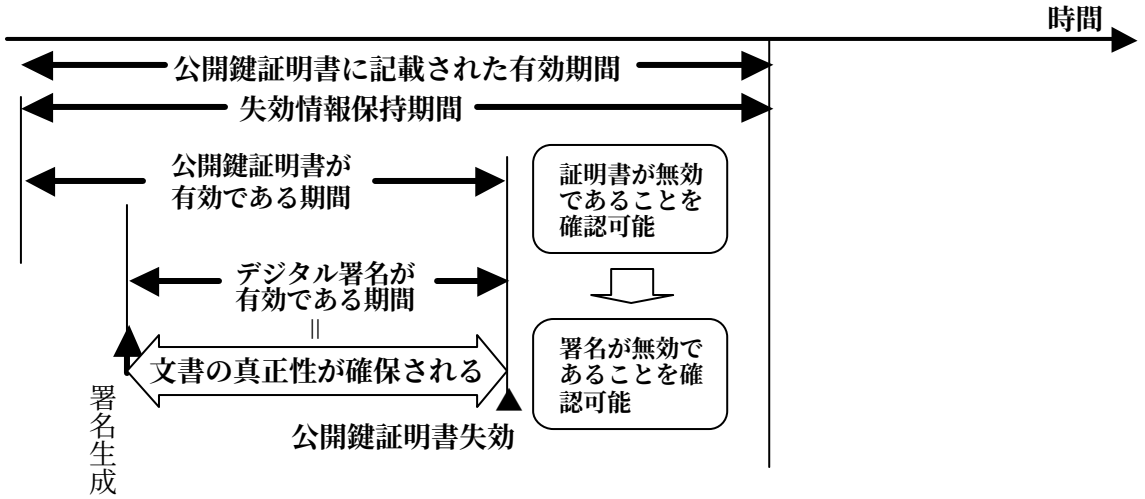

図 2-5 証明書失効とデジタル署名の関係(2)

示すると図 2-5のようになる。失効が発生すると失効前に生成された署名の有効性は失われる。つまり、生成された当初は有効であったデジタル署名であっても、電子文書の真正性を確保できる期間は公開鍵証明書が失効するまでの期間に制限されることになる。

では、生成時点でのデジタル署名の有効性を後から確認することは可能であろうか？前節で述べたとおり、署名に示された時刻を信用することができないとすると、署名が失効前に生成されたか失効後に生成されたかを判断できないため、生成時点での有効性を確認することはできない。証明書の失効時刻に関しては、認証局に信頼を置く限り、認証局の発行する失効情報を参照することにより、知ることができる。従って、もしも信頼できる署名生成時刻が得られた場合、署名が失効前に生成されたか否かを判断することが可能である。ところが有効期限を過ぎた証明書に関する失効情報は削除するのが一般的である。そのため、有効期限を過ぎてしまうと、その証明書がいつ失効したか、そもそも失効があったのか否かさえ判断できなくなってしまう（図 2-6）。

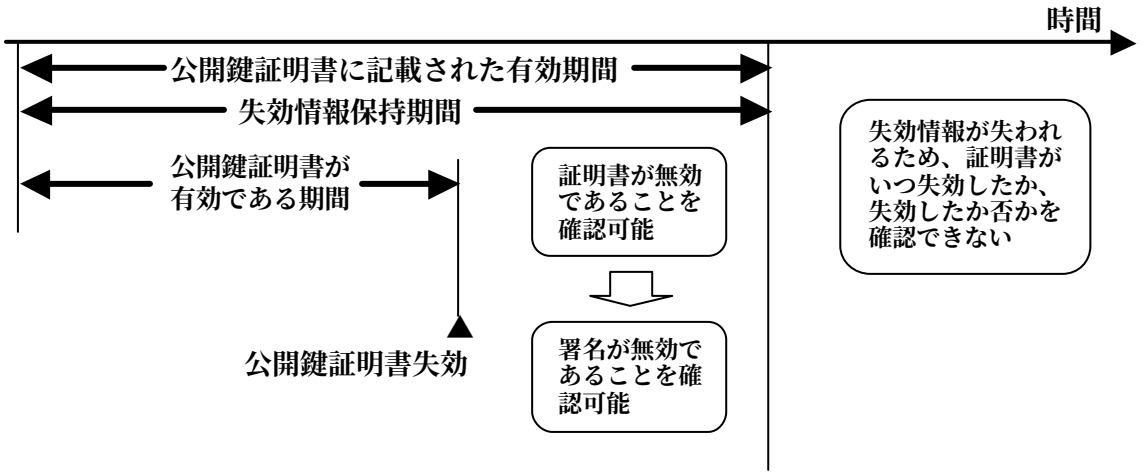

図 2-6 証明書失効とデジタル署名の関係(3)

2.1.3 デジタル署名が基礎とする暗号技術の脆弱化

現在のデジタル署名がよりどころとしているハッシュ関数や公開鍵暗号は、情報理論的に完全な安全性が保証されるものではなく、その安全性は離散対数問題や素因数分解の計算量的な困難性に基づいている。従って、技術が進歩することによって、現在用いられているハッシュ関数や公開鍵暗号が脆弱化し、デジタル署名が容易に偽造されてしまうよう

になる可能性がある。一旦脆弱化した暗号技術に基づくデジタル署名は、偽造されたものと区別ができなくなるため、有効性を失うと考えるのが自然である。通常は、公開鍵証明書に対して技術動向を勘案して十分な安全性を保てるような有効期間を設けているため、有効期間内に脆弱化して破られることは考えにくい。ところが、電子署名文書の長期保存を考える場合は、脆弱化についても考慮しておく必要がある。

2.2　真正性を長期にわたって保証するための要件

前節で述べた制約を整理する。

1. デジタル署名の検証時点での有効性の判定：
   (1) 公開鍵証明書の有効期間を過ぎている場合、デジタル署名は無効となる
   (2) 公開鍵証明書が失効している場合、デジタル署名は無効となる
2. デジタル署名生成時点での有効性の確認：
   (1) 公開鍵証明書の有効期限を越えると、生成時点でのデジタル署名の有効性は判断できない
   - 署名に示された時刻を信用できないため
   - 失効情報が失われるため

   (2) 公開鍵証明書が失効すると、生成時点でのデジタル署名の有効性は有効期間内においても判断できない
   - 署名に示された時刻を信用できないため

   (3) デジタル署名が基礎とする暗号技術が脆弱化して破られると、生成時点でのデジタル署名の有効性は確認できない
   - デジタル署名が偽造される可能性があるため

これらの制約はいずれも、有効であったデジタル署名の有効性が時間の経過によって失われることを示す。電子文書の真正性を考える場合、公開鍵証明書が有効である期間を過ぎた後にその時点でデジタル署名が有効であるか否かを判断することが問題となるのではなく、デジタル署名生成時点に有効であったか否かが問題となる。デジタル署名生成時点での有効性が確認できれば、その時点での電子文書の真正性が確認できたことになり、長

期間経過した後にも生成当時の有効性が確認できることをもって、電子文書の真正性を長期にわたって確保できると見なすことができる。

デジタル署名生成時点での有効性を確認する際の主な障害は、署名生成時刻が保証されないことと失効情報が失われることである。これに対処するためには、デジタル署名生成後、有効性の失われる前の時点で、そのデジタル署名の有効性を検証できる客観的なデータを揃え、それらを改竄ができないことが保証されるある種の安全な領域に保存する方法が考えられる。また、署名生成時刻や有効性が失われていない時点の検証データであることを保証するためには、信頼できる時刻[6]を対象データと結び付けた形で与えるような安全なタイムスタンプ[7]が必要となると考えられる。

デジタル署名の有効性を検証できる客観的なデータとは、デジタル署名の検証に用いる通常のデータであり、デジタル署名を生成したエンドエンティティから信頼する認証局に至るパス上の公開鍵証明書のセットと、それらの失効情報のセットなどである。

これらのデータを安全な領域、すなわち物理的な不正アクセスおよび論理的な不正アクセスを防ぐことができると考えらる改竄のできない領域に保存する（図 2-7）。

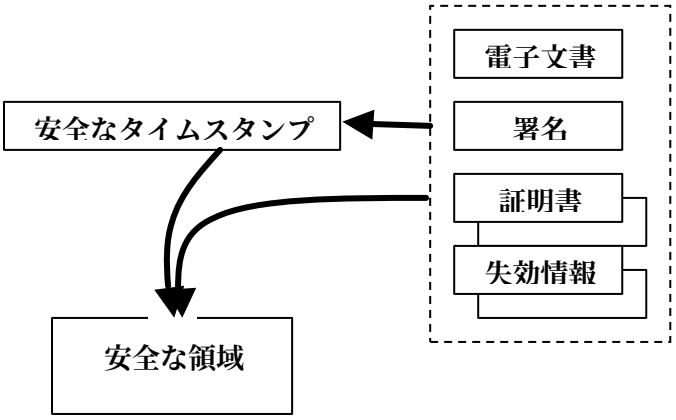

図 2-7 電子署名文書長期保存の概念

すると、有効期間等の制約を超えた時点においても、安全な領域に確保された情報を用い

---

[6] 厳密に正確な時刻とは限らないが、ある誤差範囲内であることが保証された時刻

[7] 不正行為を行う可能性の低いタイムスタンプの発行機関が発行するタイムスタンプ、またはタイムスタンプの生成に利用されるハッシュ関数の安全性の低下が考えられにくい場合のタイムスタンプ等を安全なタイムスタンプと呼ぶ。

てデジタル署名の生成時点での有効性が確認できる。このことは即ち、前述したように、電子文書の真正性が長期にわたって確保されることを示す（図 2-8）。

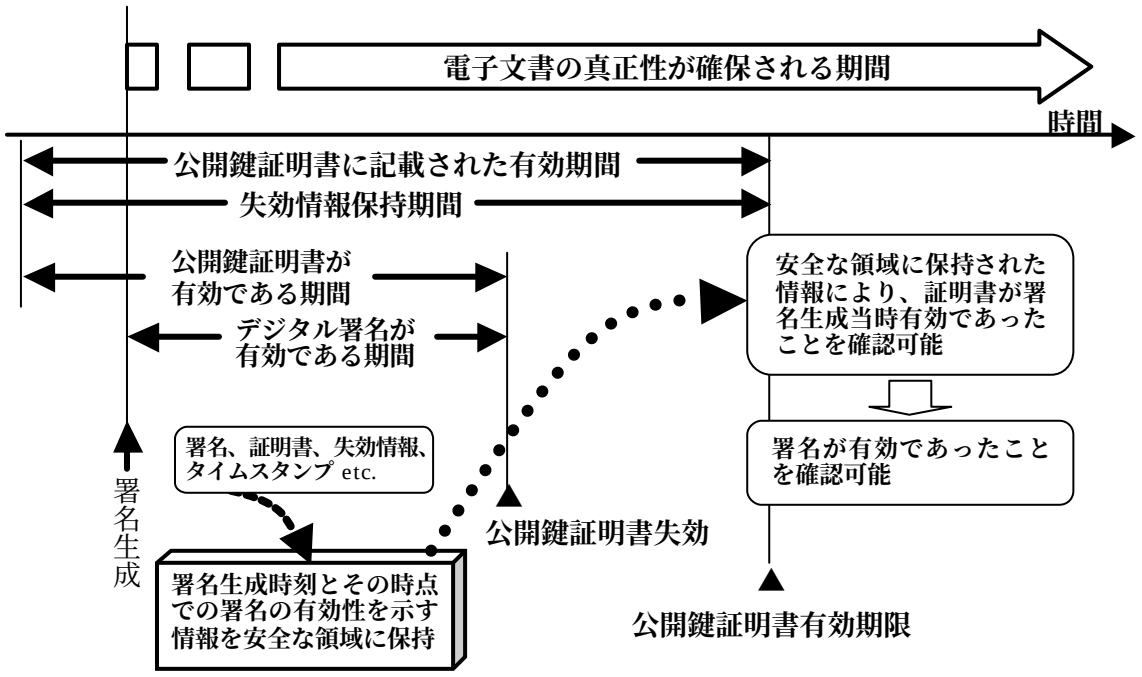

図 2-8 電子署名文書長期保存の効果

安全な領域に格納する方法には、次にあげるものがある。

- 格納されたデータの改竄ができないことを保証する原本性保証システムに格納する
- これらのデータに対して有効期間の長いデジタル署名を生成する
- これらのデータのハッシュ値を新聞等のメディアに公開する

また、安全なタイムスタンプには、次にあげるものがある。

- 原本性保証システムにデータを格納する際に生成するログにつけられた時刻
- IETF で標準化が進められているデジタル署名に基づく(ＰＫＩに基づく)タイムスタンプや Surety.com 社の提供するハッシュに基づく(ＰＫＩに基づかない)タイムスタンプなど

ただし、「安全な領域」及び「安全なタイムスタンプ」の安全性に関しては次の点に注意すべきである。

- デジタル署名をベースとする場合、前節までで述べた制約をそのまま引き継ぐこととなる。安全性を長期にわたって確保するためには、時期を見て安全な領域への再格納、安全なタイムスタンプの再取得が必要になる。
- ハッシュをベースとする場合も、脆弱化に備えるため、その時点でより安全とされる技術を用いて再度、領域への格納やタイムスタンプの取得が必要となる。
- 耐タンパなハードウェアをベースとする原本性保証システムを利用する場合、安全性を客観的に判断することは困難であるため、まずその安全性に対する基準（FIPS140-1のような）や認定制度が必要となる。技術の進歩による脆弱化が懸念される場合は、上記と同様に最新の技術を用いたより安全な技術を再適用することが必要となる。

電子文書の真正性を長期にわたって保証するために、上記のアプローチとは異なる方法として電子文書をそのまま預かるような公証サービスを利用することも考えられる。これは従来の公証サービスと同様、電子文書そのものを公証人の権威や社会的信頼という安全な領域に保存するものである。

3 電子署名長期保存技術

電子署名文書長期保存のためには、公開鍵証明書の有効期限切れ・失効、またはデジタル署名が基礎とする暗号技術の脆弱化後も署名の有効性を検証する方法が必要となる。

本章では、各種プロトコルや保存フォーマットを提案している要素技術、それら要素技術を組み合わせた実装システムについて述べる。また、署名時刻や署名の真正性を保証する公証サービス、電子署名文書を保存する原本性保証システムや、電子文書を預けられる公証サービスなどについて述べる。

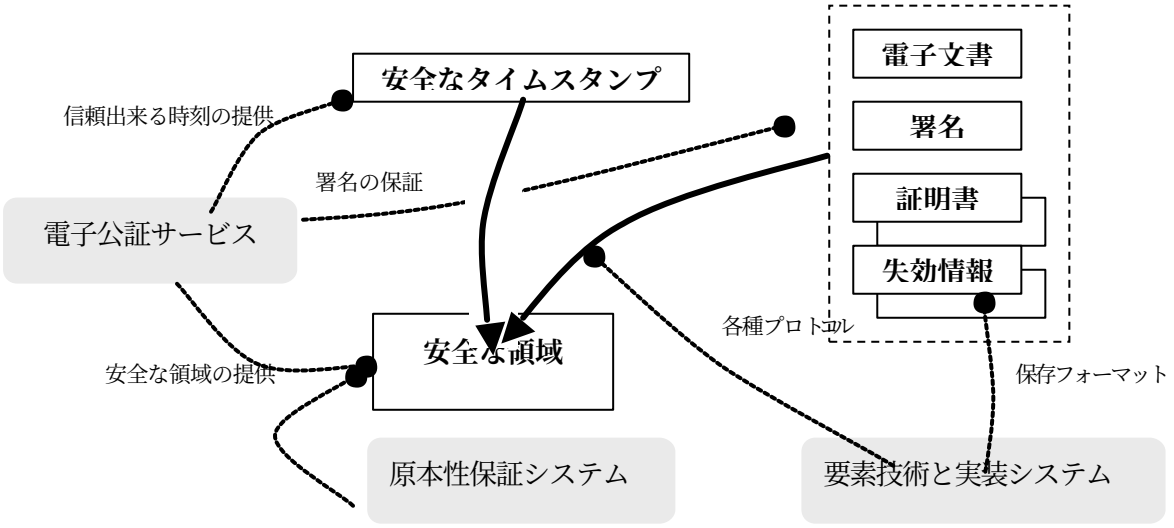

図 3-1 電子署名長期保存技術の概要

3.1 要素技術と実装システム例

電子署名が施された電子文書は、アルゴリズム、鍵、その他の暗号機能の脆弱化により、長期間の保存に絶えられないと危惧されていた。しかし、従来の紙ベースである文書から電子文書への移行の必要性が高く要求されるようになり、電子署名文書の長期保存を可能にするための基盤技術が各団体等で検討されてきた。今日では標準プロトコルやその応用技術が報告され、更にそれらの技術を利用したシステムの実験がなされるなど、実用化に向けた環境が整備されてきている状況である。

ここでは、電子署名文書の長期保存に利用できる要素技術と、それらの技術を用いた実装システム例について述べる。紹介する内容は次の通り。

1. 要素技術
   - ETSI ES 201 733 Electronic Signature Formats
   - Data Validation and Certification Server Protocols（RFC3029）
   - Time Stamp Protocol
   - ヒステリシス署名
2. 実装システム例
   - 長期保存文書のための電子署名期限延長技術開発

●(ＩＰＡプロジェクト：「電子政府情報セキュリティ基盤技術開発に係る公募」採択テーマ)

3.1.1 ETSI ES 201 733 Electronic Signature Formats

ETSI ES 201 733 Electronic Signature Formats［5］は、電子商取引における情報保護および信頼構築のための重要な要素である電子署名(電子署名トークンの書式と署名ポリシーの書式)の標準仕様をＥＴＳＩ(European Telecommunications Standards Institute)が規定するドキュメントである。

この電子署名の標準仕様は、次を目的に作成されている。

- Ｂ、Ｃ、Ｇ間のさまざまなトランザクションに適用可能であること
- 環境(スマートカード、ＧＳＭ ＳＩＭカード、その他の署名プログラムなど)に独立であること

また、この標準の特徴として、長期間正当性を維持できる形式を定めていることがあげられ、また、そのためにタイムスタンプオーソリティなどの信頼のおける第三者サービスを利用している。

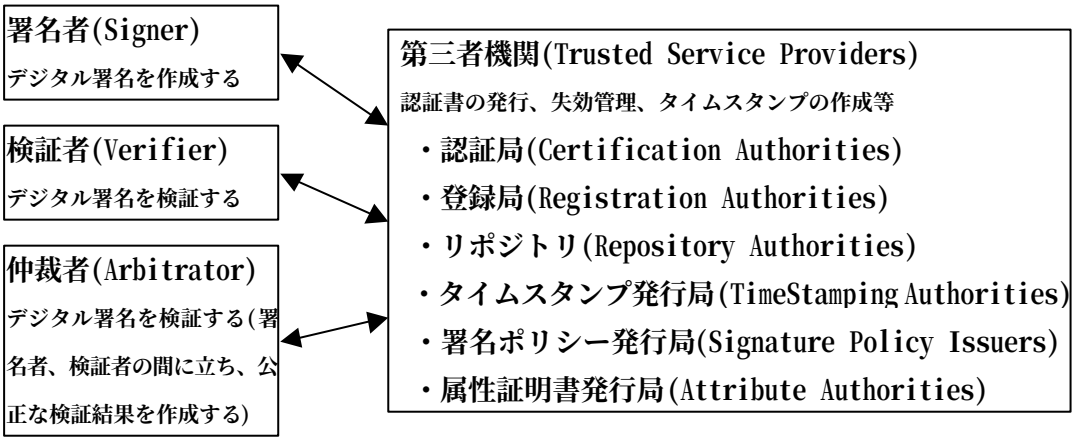

図 3-2 esformatsの構成

本仕様はＩＥＴＦにも提案されインターネットドラフトとなっており、Ｓ／ＭＩＭＥワーキンググループで検討中である。

3.1.1.1 電子署名データと検証データ

電子署名データは次のデータを含む。

- 署名ポリシー(the signature policy)
- 署名されたユーザ・データ(the signed user data)
- デジタル署名(the digital signature)
- 署名者によって提供される署名されたその他の属性(other signed attributes provided by the signer)

電子署名を検証するための検証データは次のデータを含む。

- 証明書(certificates)
- 失効状態の情報(revocation status information)
- ＴＳＰから得た信頼できるタイムスタンプ(trusted time-stamps from Trusted Service Providers(ＴＳＰ))

3.1.1.2 検証データの形式

検証データの形式を以下に示す。

(1) 電子署名：ＥＳ(the Electric Signature)

署名者によって提供されるデジタル署名と他の基本的情報を含む。

(2) タイムスタンプ付きＥＳ：ＥＳ－Ｔ(the ES with Time stamp)

長期間にわたる有効性を提供する最初のステップとしてタイムスタンプをＥＳに加えたもの。

(3) 完全な検証データ付きＥＳ：ＥＳ－Ｃ(the ES with Complete validation data)

電子署名の有効性を示すデータ(つまり失効状態情報)の完全な集合へのリファレンスをＥＳ－Ｔに加えたもの。

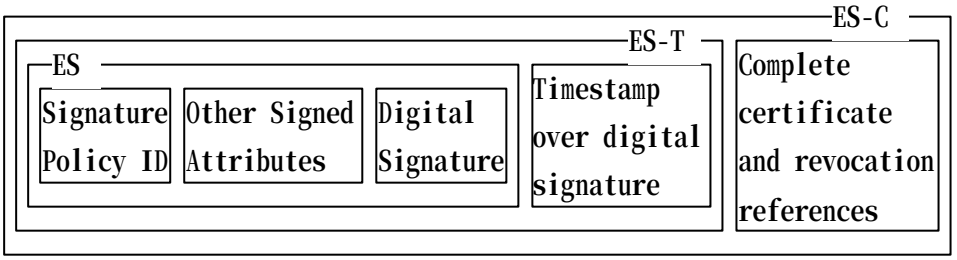

図 3-3 ES、ES―T、ES―C

検証者が次のデータにアクセスできない時のために、証明書と失効情報の値をＥＳ－Ｃに付加し、ＥＳ－Ｘ ｌｏｎｇ(the ES with extended Validation data)に拡張できる。

- 署名者の証明書
- 完全な証明書パスを構成する全てのＣＡ証明書
- ＥＳ－Ｃで参照される全ての失効状態情報

また、証明書チェーンにおいて使われるＣＡ鍵が危殆化される危険があるときに対処するため、検証データにタイムスタンプを付加する。その方法は次の２通りある。

- ＥＳ(ＥＳ－Ｃ)の全ての検証データに対するタイムスタンプを付加する(ＥＳ－Ｘ Ｔｙｐｅ１)
- 完全に利用される個々のリファレンス・データに対するタイムスタンプを付加する(ＥＳ－Ｘ Ｔｙｐｅ２)

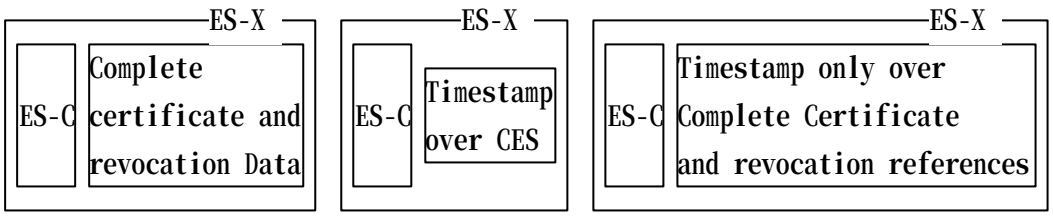

図 3-4 ＥＳ－Ｘ long, ES－Ｘ Type1、ES－Ｘ Type2

更に、ＥＳ－Ｃが生成された時点で利用されたアルゴリズム、鍵、その他の暗号機能が脆弱化または以前生成されたタイムスタンプに対する証明書が失効する前に、署名データ、ＥＳ－Ｃ、その他の付加情報(ＥＳ－Ｘ)に対するタイムスタンプを順次生成し、付加していくことにより長期間署名を有効にするデータ形式をＥＳ－Ａ(the ES with Archived validation data)と呼ぶ。

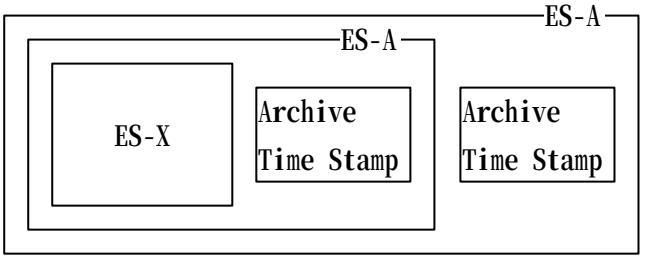

図 3-5 ＥＳ－Ａ

3.1.1.3 仲裁

条件により、仲裁に用いる検証用データが異なる。

1. 仲裁者がＥＳ－Ｃで参照される署名者の証明書、相互認証書、ＣＲＬまたはＯＣＳＰレスポンスの場所を知っている。
2. 証明書チェーン上のどの鍵も危殆化していない。
3. ＥＳ－Ｃが生成された時点の暗号処理は仲裁が行われる時点で破られていない。

１～３が満たされているとき	：ＥＳ－Ｃ
１が満たされないとき	：ＥＳ－Ｘ ｌｏｎｇ
２が満たされないとき	：タイムスタンプ付きＥＳ－Ｘ(ＥＳ－Ｘ Ｔｙｐｅ１またはＥＳ－Ｘ Ｔｙｐｅ２)
１と２が満たされないとき	：タイムスタンプ付きＥＳ－Ｘおよび ＥＳ－Ｘ ｌｏｎｇ
３が満たされないとき	：ＥＳ－Ａ

3.1.1.4 検証プロセス

電子署名の検証結果は、次の値を取りうる。

- 有効(valid)
- 無効(invalid)
- 検証不能(incomplete verification)

その他、検証により次の検証データを出力することもありうる。

- 署名のタイムスタンプ(a signature time stamp)
- 完全な検証データ(the complete validation data)
- アーカイブ検証データ(the archive validation data)

3.1.2 Data Validation and Certification Server Protocols

Data Validation and Certification Server Protocols(ＤＶＣＳ)[6]はTrusted Third Party(ＴＴＰ)で、ある時点での要求者のデータ所有を証明したり、デジタル署名文書(公開鍵証明書も含む)の署名検証を行ったりする。その結果を証明するものとしてＤＶＣＳの署名の付いた時刻入りの「データ検証証明書(ＤＶＣ)」を応答として発行する。

応答として得られた「データ検証証明書(ＤＶＣ)」は、ある時点でのデータの所有またはデジタル署名の正しさを証明するものとして使われる。このＤＶＣの検証は、同じＤＶＣＳの署名検証要求プロトコルを使ってＤＶＣＳに問合わせることで行うことができる。ＤＶＣＳは、否認防止支援のサービスや、ＤＶＣＳにデータのアーカイブ機能を含めて証拠記録機関として使うこともできる。

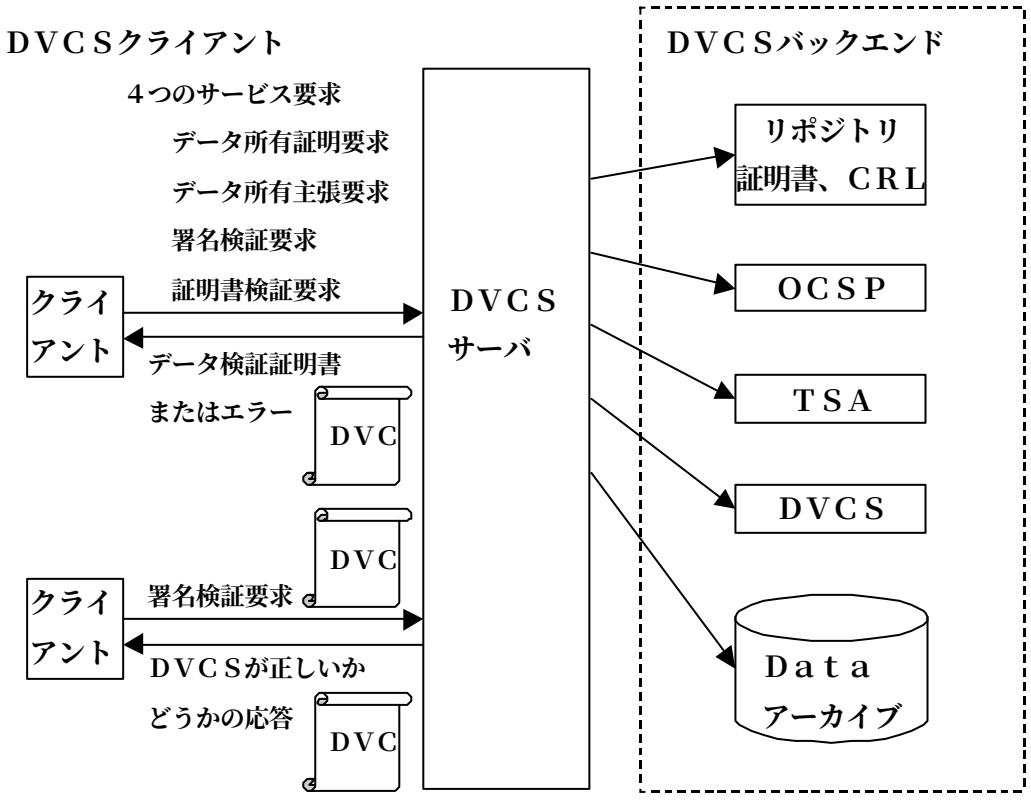

図 3-6 DVCS概要

本技術は、ＩＥＴＦで規定されるＲＦＣ３０２９「Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols」からの引用であり、詳細については原文を参照のこと。

3.1.2.1 ＤＶＣＳの機能要件

ＤＶＣＳは一般的なデータの有効性と認証のサービスを行う Trusted Third Party(ＴＴＰ)で、次のような４つのサービスを提供する。

- データ認証
  - ＣＰＤ　：データ所有の認証(任意データ)
  - ＣＣＰＤ：データ所有申請の認証(データのハッシュ値：内容は問わない、ＴＳＰと同様なサービス)
- 署名文書の検証
  - ＶＳＤ　：デジタル署名文書の検証(パス検証と失効情報の検証を含む)
  - ＶＰＫＣ：公開鍵証明書の検証(パス検証と失効情報の検証を含む)

ＤＶＣＳの機能要件を以下に示す。

1. ＤＶＣＳはそのサービスとポリシーに従って、データ検証証明書(ＤＶＣ)としての署名付き応答(ＣＭＳ署名)を返す。どのような内容をＤＶＣに含めるかはポリシーにより定められる(関連証明書、ＣＲＬ、およびＯＣＳＰ、ＴＳＡ、他のＤＶＣＳの応答など)。
2. ＤＶＣには署名文書であるかないか、または証明書が有効であったか、データが有効であったかどうかを示す。エラーの場合はその理由を返す。
3. ＤＶＣに単純増加のシリアル番号を付ける。
4. ＤＶＣに時刻情報を付けるかタイムスタンプトークンをつける。
5. ＤＶＣＳの証明書に署名用拡張鍵目的を付けたＤＶＣＳの書名鍵でＤＶＣに署名する、そしてこの署名の属性にこの証明書の参照を含める。
6. ＤＶＣを発行する前に自身の署名鍵の有効性を確認する、エラーの場合はＤＶＣを発行してはならない。

3.1.2.2 ＤＶＣＳトランザクション

ＤＶＣＳプロトコルはクライアント／サーバのプロトコルで、クライアントはデータ認証要求または署名文書(あるいは公開鍵証明書)の検証をＤＶＣＳに要求する。ＤＶＣＳは要求を検証しその応答をデータ検証証明書(ＤＶＣ)として返す。エラーの場合はその理由を返す。

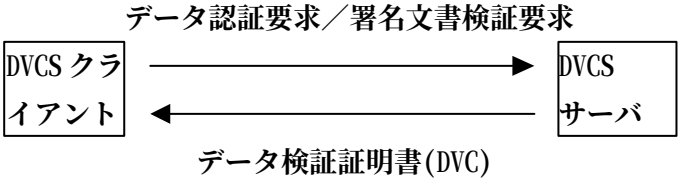

図 3-7 DVCSのトランザクション

要求者はＤＶＣＳの応答であるＤＶＣに対して、時間、ＤＶＣＳの名前、要求への対応、署名、および状態、サービスポリシーなどを検証すべきである。ＤＶＣが正しければ、ＤＶＣＳの証明書が有効かどうかはアプリケーションが検証する。

3.1.2.3 ＤＶＣＳ要求とＤＶＣＳ応答

クライアントからのＤＶＣＳ要求は次のデータを含む。

- サービスタイプを指定するＤＶＣＳ要求情報(requestInformation)
- 対象となる認証または検証のデータ(data)
- ＩＤ情報(transactionIdentifier)

ＤＶＣＳ要求情報にはサービスタイプの指定の他に、オプションとして要求時間、要求者名、要求ポリシー、ＤＶＣＳサーバ名、データの所在場所の指定がある。

サービスタイプには、次の値を指定することができる。

- データ所有の認証(任意データ)：ｃｐｄ
- デジタル署名文書の検証(パス検証を含む)：ｖｓｄ
- 公開鍵証明書の検証(パス検証と失効情報の検証)：ｃｐｋｃ
- データ所有申請の認証(データのハッシュ値：ＴＳＰと同様)：ｃｃｐｄ

サーバからのＤＶＣＳ応答は次のデータを含む。

- 認証または検証結果(dvReqInfo)
- 要求データのハッシュ値(messageImprint)
- 認証または検証時間(responseTime)
- ＤＶＣＳ応答状態(dvStatus)
- ＤＶＣＳポリシー(policy)
- 証明書チェーン(certs)

3.1.2.4 送受信のプロトコル

ＤＶＣＳメッセージに関して、特定の送受信メカニズムは定めない。以下のものを使うことができる。

１．ＨＴＴＰまたはＨＴＴＰＳによるＤＶＣＳプロトコル

２．Ｅメールを利用したＤＶＣＳプロトコル

3.1.3 Time Stamp Protocol ［7］、［8］

タイムスタンプサービスは特定時刻より前にデータが存在していた証拠を供給し、否認防止サービス[ＩＳＯＮＲ]をサポートするための基礎として利用することができる。タイムスタンプにおいては幾つかのプロトコルが報告されているが、ここではＩＥＴＦ ＰＫＩＸにおいて検討が進められているタイムスタンププロトコルを紹介する。このプロトコルは、サービスを提供する Time Stamp Authority(ＴＳＡ)に送られる要求フォーマットと返される応答フォーマットを規定する。

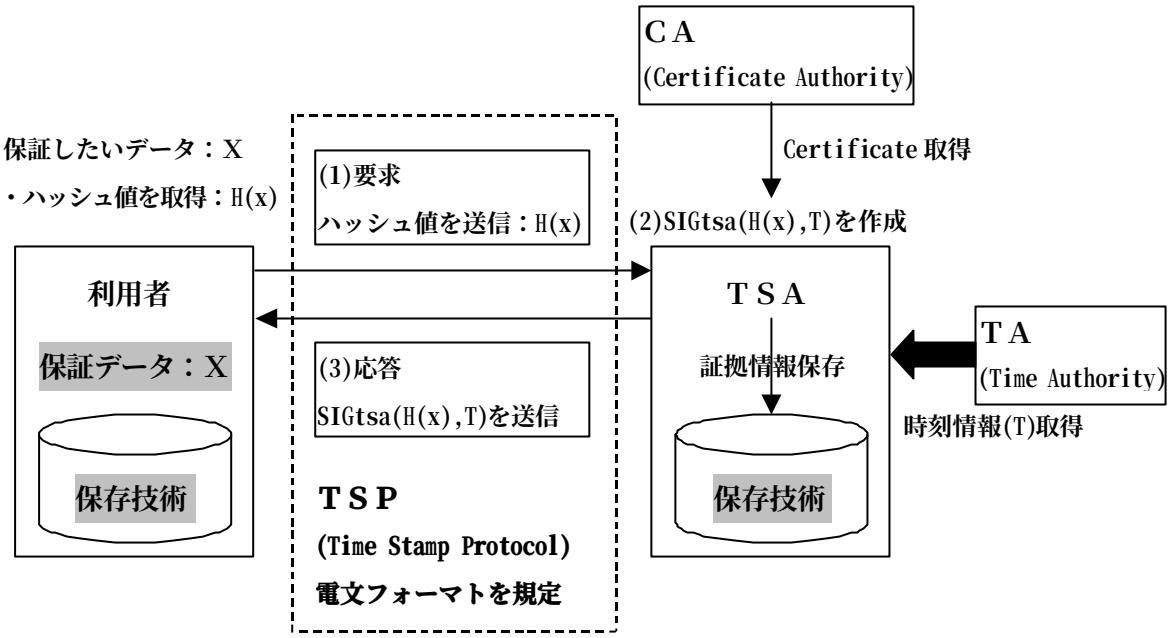

図 3-8 TSP概要

本技術は、ＩＥＴＦのＰＫＩＸで検討されているインターネットドラフト「Internet X.509 Public Key Infrastructure Time Stamp Protocol（ＴＳＰ)」からの引用であり、詳細については原文を参照のこと。

3.1.3.1 ＴＳＡの必要条件

ＴＳＡは特定時刻にデータが存在していたことを示すためにタイムスタンプトークンを生成する Trusted Third Party(ＴＴＰ)である。

ＴＳＡの必要条件を以下に示す。

１．信頼された時間源を使う。
２．各タイムスタンプトークンに信頼された時間値を含む。
３．新たに生成された各タイムスタンプトークンにユニークな整数値を含む。
４．要求者から正当な要求を受けることでタイムスタンプトークンを生成する。
５．トークン作成におけるセキュリティポリシーをユニークに表示するための要件を、各タイムスタンプトークンに含む。
６．データのハッシュ値表現にのみタイムスタンプを押す、すなわち、ＯＩＤでユニークに認識される一方向性ハッシュ関数のデータに押印する。
７．一方向性ハッシュ関数のＯＩＤを調べ、ハッシュ値の長さがハッシュアルゴリズムと一致することを証明する。
８．(前項で述べたように、長さをチェックする以外に)タイムスタンプされた内容を調べない。
９．タイムスタンプトークンに要求者のいかなる身元確認も含まない。
１０．この目的の為に排他的に生成された鍵を使って各タイムスタンプトークンを署名し、対応

している証明書に表示されている鍵の所有権を持つ。

１１．要求者によって拡張フィールドの使用を要求された場合、ＴＳＡが拡張フィールドをサポートしているならば、タイムスタンプトークンに付加情報を含む。拡張フィールドをサポートしていないならば、ＴＳＡはエラーメッセージを応答しなければならない。

3.1.3.2 ＴＳＡトランザクション

このメカニズムの最初のメッセージとして、要求者がＴＳＡに要求(後で定義される TimeStampReq を含む)を送ることでタイムスタンプトークンを要求する。二つ目のメッセージとして、ＴＳＡは要求者に応答(後で定義される TimeStampResp を含む)を送ることで返信する。

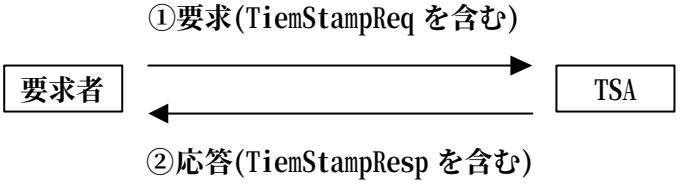

図 3-9 TSAトランザクション

応答を受け取ると、要求者はタイムスタンプトークンのデジタル署名の正当性を検証しなければならい。特に、タイムスタンプされたものがタイムスタンプを要求したものと一致していることを検証しなければならない。要求者はタイムスタンプトークンがＴＳＡの正しい身元証明書、正しいデータ押印、そして正しいハッシュアルゴリズムＯＩＤを含んでいることを検証しなければならない。

3.1.3.3 要求と応答

タイムスタンプの要求は次のデータを含む。

- ハッシュアルゴリズムＯＩＤとタイムスタンプされるデータのハッシュ値(messageImprint)
- タイムスタンプトークンを規定するＴＳＡポリシー(reqPolicy)

タイムスタンプの応答は次のデータを含む。

- タイムスタンプの要求に対する応答状態(status)
- ＴＳＡがタイムスタンプを生成した時刻を含むタイムスタンプトークン(timeStampToken)

タイムスタンプトークンにはタイムスタンプの他に、ＴＳＡポリシー、ＵＴＣ時間における時差、ＴＳＡの名称がある。

3.1.3.4 送受信のプロトコル

ＴＳＡメッセージに関して、特定の送受信メカニズムは定めない。以下のものを使うことができる。

１．Ｅメールを利用したタイムスタンププロトコル

２．ファイルベースプロトコル

３．ソケットベースプロトコル
４．ＨＴＴＰによるタイムスタンププロトコル

3.1.3.5 セキュリティの考慮

ＴＳＡサービスを設計するとき、タイムスタンプトークの正当性や信用に影響を及ぼす次の考慮が必要である。

１．ＴＳＡの信用
２．ＴＳＡの秘密鍵管理
３．ＴＳＡの署名鍵の長さ
４．応答時間の条件
５．タイムスタンプトークン生成時の参照データ
６．要求メッセージの再生

3.1.4 ヒステリシス署名 ［9］、［10］、［11］

ヒステリシス署名とは、電子データに施された電子署名が当該利用者が生成したものなのか、あるいは不正者によって偽造されたものなのかということを判別するために、電子署名の生成履歴を当該利用者にも変更困難な形で安全に保管し、事後になっても署名の正当性を確認可能とする技術である。

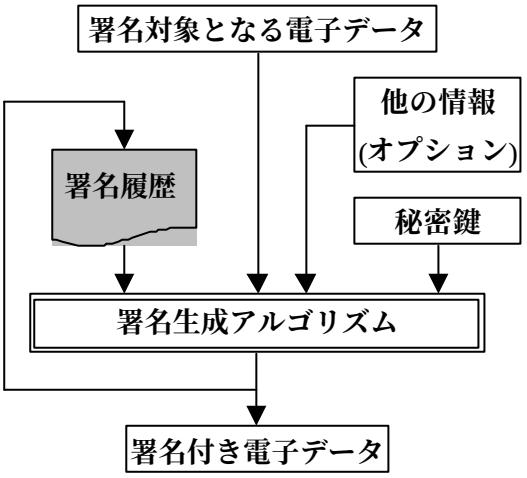

図 3-10 ヒステリシス署名概要

不正者Ｂが「利用者Ａの過去の電子署名α」を偽造するためには、電子署名αを生成して以降の全ての電子署名を整合的に偽造することが必要となる。すなわち、利用者は自己の署名履歴を調停者に提示することによって、当該利用者が生成した個々の電子署名の現在に至るまでの順序関係を示すことで、それ以外の電子署名を生成していないことを証明できる。

最新の署名には、署名履歴管理ＩＣカード(*1)の使用開始時からの全ての署名履歴が影響を及ぼしている為、署名履歴が正しく連鎖している事を確認することで署名検証をすることができる。

*1：アクセス制御機能、鍵管理機能、署名機能、署名履歴管理機能を持つ。

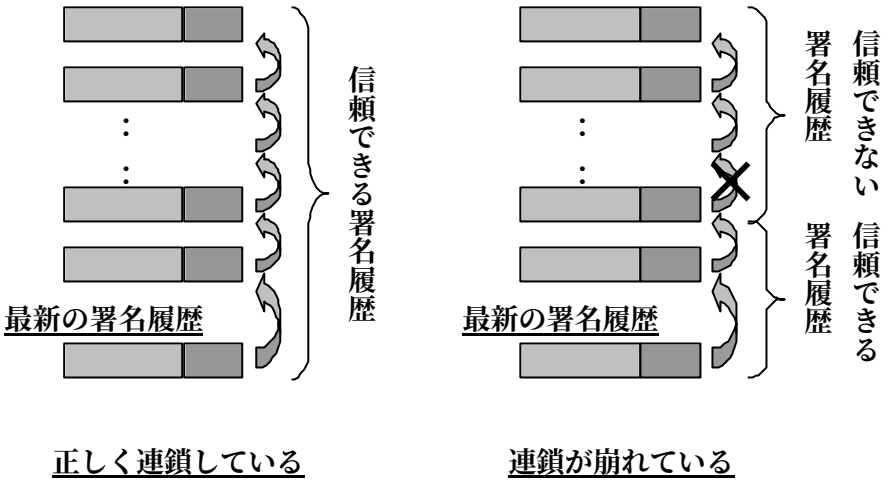

図 3-11 署名履歴の検証

3.1.4.1 署名履歴の要件

署名履歴を生成するにあたり、その要件を以下に示す。

1. 利用者は、署名履歴の中に記載されないような手段で自己の電子署名を正しく生成することができない。
2. 利用者が生成した電子署名に対するログは、署名履歴の中にすべて記載される。
3. 利用者の署名履歴は、利用者自身も含めて誰にも変更することができない。
4. 署名履歴に何らかの変更が加えられた場合には、事後になってもその事実が正しく検証できる。

3.1.4.2 履歴交差プロトコル

ヒステリシス署名においては、各利用者の署名履歴を交差させることで改竄を著しく困難にすることができる。

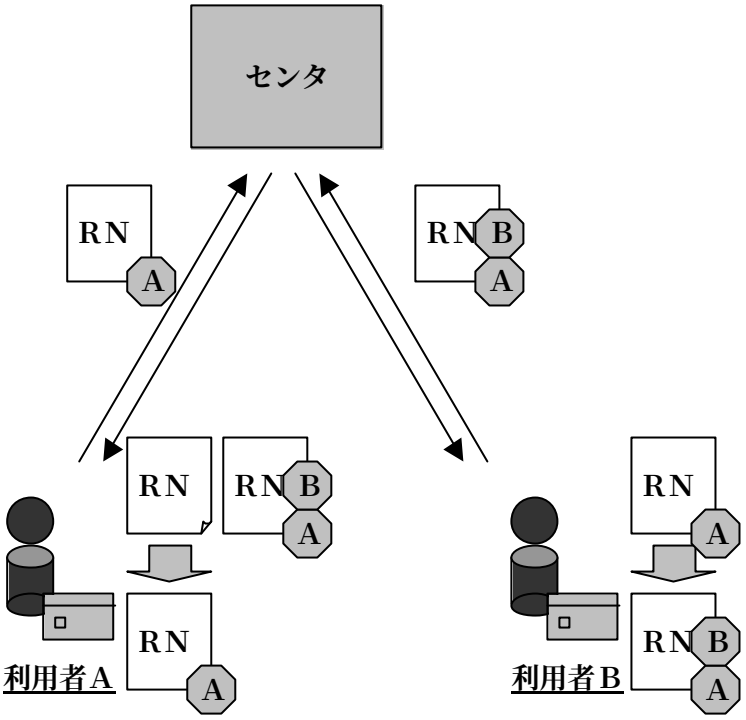

図 3-12 履歴交差プロトコル概要

1. 利用者Aは乱数を生成して電子署名を施し、当該乱数に対する署名結果を署名履歴に含ませる。
2. 利用者Aは署名付き乱数をセンタに送付する。
3. センタはランダムに選択した利用者Bに利用者Aから送られてきた署名付き乱数を送付する。
4. 利用者Bはセンタから送られてきた署名付き乱数に電子署名を施し、当該データに対する署名結果を署名履歴に含ませる。
5. 利用者Bは二者署名付き乱数をセンタに返送する。
6. センタは利用者Bから返送されてきた二者署名付き乱数を利用者Aに送付する。

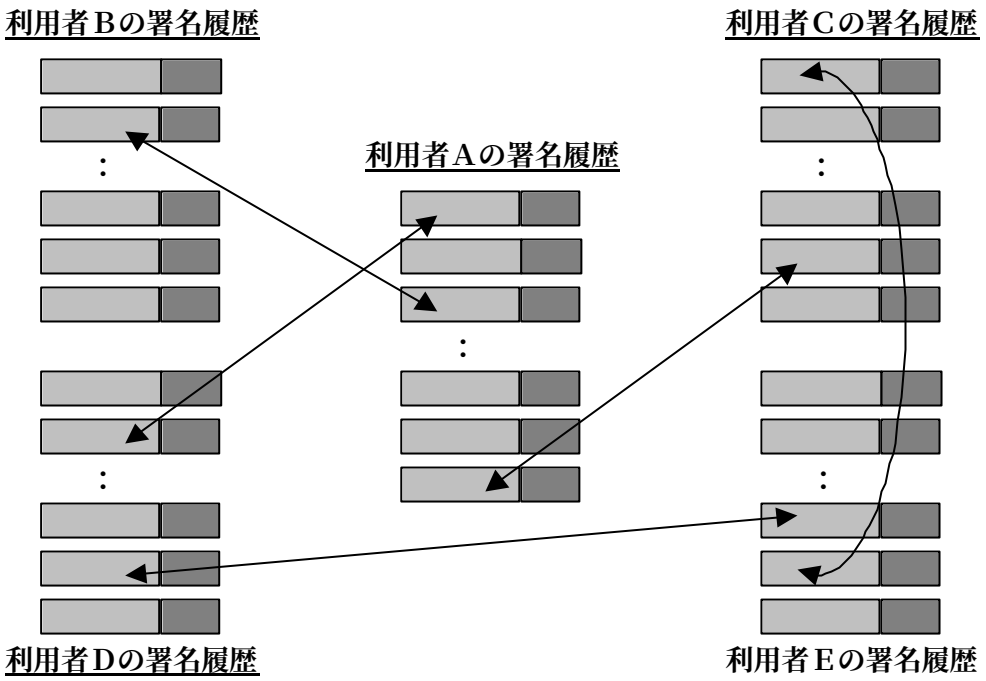

図 3-13 履歴交差している署名履歴

署名履歴の中に他の利用者と履歴交差を行った部分があれば、当該交差相手の署名履歴を確認することによって、欠落した履歴データ以前に署名されたものの真偽も検証可能となる。

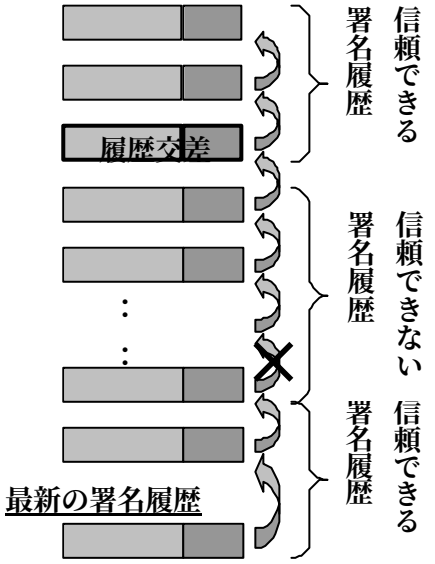

図 3-14 履歴交差の検証

3.1.5 長期保存文書のための電子署名期限延長技術開発（ＩＰＡプロジェクト：「電子政府情報セキュリティ基盤技術開発に係る公募」採択テーマ）

「電子政府情報セキュリティ基盤技術開発－長期保存文書のための電子署名期限延長技術開発」プロジェクトで採択されたデジタル署名の有効性延長技術方法である。

デジタル署名に用いた証明書の有効性が失われる前に、そのデジタル署名データに対して新たな証明書に基づくデジタル署名を生成し、元の証明書の有効性を保証するデータと、それらに対するタイムスタンプデータを Trusted Third Party(ＴＴＰ)から獲得して組み合わせることにより延長署名データを作成し、元のデジタル署名データから次々に延長して生成した延長署名データを延長署名系列としてデータベースにより管理する。

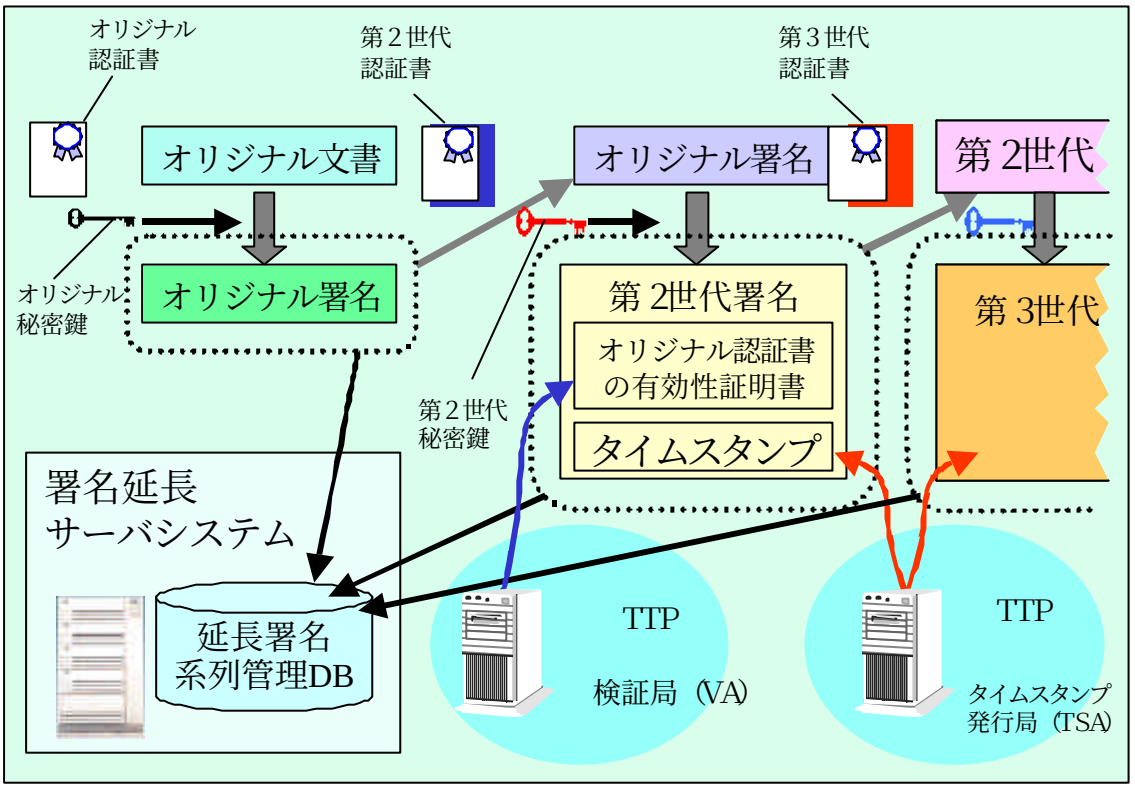

図 3-15 署名延長技術概要

3.1.5.1 署名延長技術の要件

署名延長技術を開発する上での要件を以下に示す。

1. 単なる電子署名の付替えではなく、オリジナル電子署名の有効性を維持できること。
2. 第三者の電子署名の期限延長を可能とすること。
3. 第三者による延長署名検証を可能とすること。
4. ＰＫＩに基づく標準的な技術で実現できること。

3.1.5.2 システム構成

署名延長技術のシステム構成を以下に示す。

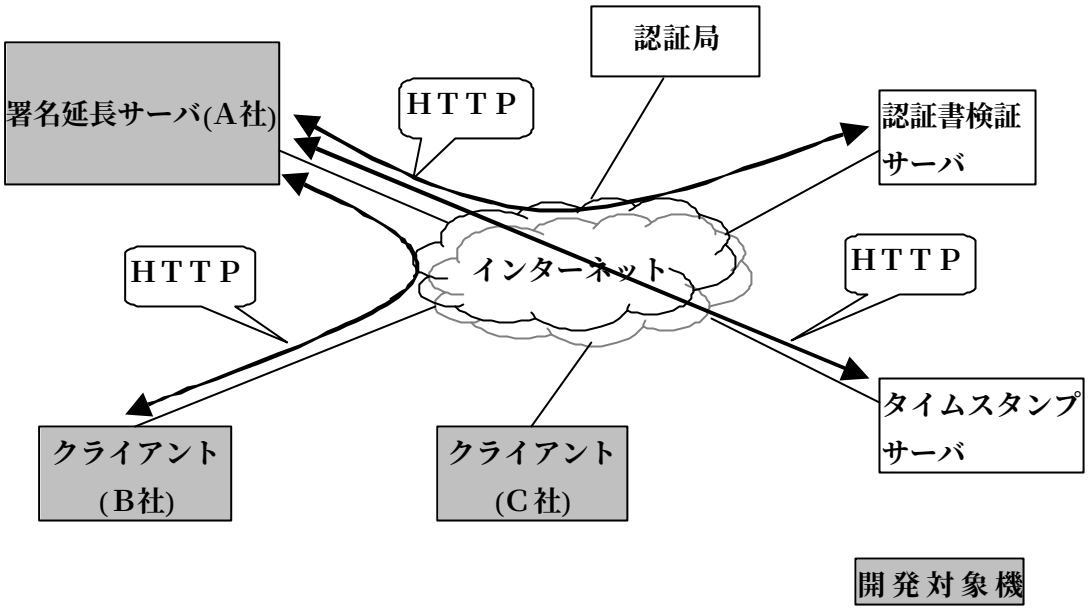

図 3-16 システム構成

署名延長サーバは以下の機能を有する。

- 延長署名生成機能：署名から延長署名と署名系列を生成
- 延長署名管理機能：署名系列を管理
- 延長署名自動生成機能：署名期限から自動的に署名を延長
- サーバ問合わせ機能：認証書検証サーバや、タイムスタンプサーバへの問合わせ

クライアントは以下の機能を有する。

- 延長署名検証機能：延長署名の正当性を検証

3.1.5.3 安全性・信頼性の根拠

本方式による安全性・信頼性の根拠は、ＴＴＰにより発行される証明書の有効性を保証するデータとタイムスタンプデータの正当性に依存する。それらには各ＴＴＰによるデジタル署名が施されており、正当性を保証している。

3.1.5.4 管理の容易性

署名延長は、オリジナルの署名者自ら実施する必要がなく、第三者によるサービスとして実現できる。そのため、署名の有効期間を延長したい者(署名者本人とは限らない)が署名延長サービスに依存することにより、管理を任せることができる。また、署名の有効期間を延長したい者が署名延長サーバを運用する場合でも、延長署名の生成や延長署名系列の管理はシステムが行うため、管理は容易である。

ただし、管理する延長署名系列が増加するとＴＴＰに高負荷をかけることになる。

3.1.5.5　検証の容易性

有効な証明書に基づく電子文書の真正性の検証のためには署名データの検証を行う。この場合、標準的な署名検証処理が利用できれば良い。

また、有効性の失われた有効な証明書に基づく電子文書の真正性の検証を行う場合、延長署名系列の検証を行う。この時、延長署名系列は署名延長システムのデータベースに保存されており、遠隔にオンラインで転送することが可能である。

また、延長署名系列に含まれるデジタル署名(ＰＫＣＳ＃７準拠)、タイムスタンプ(ＩＥＴＦ Internet X.509 Public Key Infrastructure Time Stamp Protocol 準拠)、証明書の有効性証明書(Online Certificate Status Protocol － ＯＣＳＰ(ＲＦＣ２５６０)準拠)は標準に準拠するものであるため、標準的なＰＫＩ環境により検証可能である。

また、延長署名は、一つの電子文書に対する署名毎に生成されるため、延長署名系列が膨大になることはない。

3.2　　原本性保証システム

電子署名文書の長期保存に必要となる、改竄できない安全な領域を実現する技術の一つとして原本性保証システムについて調査した。電子文書の原本性保証ガイドライン及びシステムの事例について説明する。

3.2.1　電子文書の原本性保証ガイドライン

「電子文書の原本性保証ガイドライン」（平成１２年３月財団法人ニューメディア開発協会）［12］において、電子文書の原本性確保要件及び対策がまとめられている。これは総務庁が平成１１年４月にまとめた「共通課題研究会中間報告」［13］をもとに検討が行われ、原本性保証システムの導入を検討する行政および民間の機関において活用されることを目的として作成されたものである。

原本性とは、電子的な文書として保存することが確定された後、紙文書と同様に管理・利用できる状態にあることであって、法的な意味での「原本、謄本・抄本」などを区別することではないとされ、完全性、機密性、見読性の３つの要件が挙げられている。対策には、組織体制、アクセス管理、記録媒体及びバックアップ、ウィルス対策、見読対策、その他が含まれ、必須とオプションに分けて以下に示す項目が挙げられている。

必須	電子文書の保存・管理についての責任及び権限を明確化するため、管理責任者等を定めること
必須	電子文書を保存・管理するためのシステムにアクセスする者を ID、パスワード等によって識別し、認証すること
必須	電子文書を記録した媒体は、保管場所を定め、施錠して保管し、保管場所からの搬出入及び授受は管理記録を整備して行うこと
	電子文書保存・管理システムに対するアクセスを監視すること
	電子文書保存・管理システムに対するアクセスを記録すること
必須	電子文書保存・管理システムには、電子文書の内容・性格に応じて、アクセス権限を設定すること。
必須	電子文書の保存、参照、更新、複写及び廃棄の日時並びに実施者を記録するログを取得し、保存すること。当該ログは、安全な場所及び媒体に一定期間保存すること
	電子文書の更新履歴（削除した内容、追加入力した内容等）が確認できること。当該更新履歴は、安全な場所及び媒体に一定期間保存すること
	更新前の電子文書についても、必要に応じ一定期間保存すること
	電子文書の盗難、漏洩等に備えるとともに、改竄等を防止するため、必要に応じて電子文書を暗号化して保管すること
	必要に応じ改竄検出機能を有する電子署名を電子文書に施して保管すること
	システムタイマーの設定・変更等の作業履歴が確認できること。当該作業履歴は安全な場所及び媒体に一定期間保存すること
必須	電子文書のバックアップを定期的に行い、当該バックアップを適切に保管すること
必須	電子文書を記録した媒体及びそのバックアップについては､定期的に保管状態及びデータの内容が正常であるか否かの点検を行うこと。
必須	外部から入手した電子文書は、ウィルスチェック後に利用すること
必須	電子文書の出力に必要な電子計算機、プログラム、通信関係装置、ディスプレイ、プリンタ等を備え付け､いつでも必要な場合には電子文書をディスプレイの画面及び書面に出力することができるようにすること
必須	電子文書保存・管理システムの保守、点検、改造等は計画的に行い、当該行為の期間

	中における電子文書の保護措置を講ずること
必須	停電、誤切断等による電子文書の消失、破壊等を防止するため、無停電電源等の必要な措置を講ずること
	プログラムのバックアップを行い、適切に保存すること
	原本・謄本・抄本等の区別をする場合、これらを混同することがないようにすること

3.2.2 原本性保証システムの事例

装置またはシステムの構造・機能等により電子文書の原本性を保証するために各種の形態が可能であるが、その一例として「原本性確保支援システム Trusty Cabinet V1」（リコー）について説明する。原本性保証を実現するための主な機能は以下の通りである。

1. 原本管理機能

- 原本データと各種履歴については改竄検知用データを付与し、改竄の有無を判別可能。（保存文書の改竄の有無をチェックするのにハッシュ関数を利用する。文書と暗号化したハッシュ値はセットにして保存する。暗号化の秘密鍵は、利用者はもちろん管理者にもわからないようにプログラム中に格納されている。）
- 保存データには作成日時や保存期限などの属性情報を付与して管理。
- 保存データへ更新処理を行うと装置内で自動的に原本の版管理を行う。

2. アクセスコントロール

- 保存装置を利用するクライアントシステムへアカウントを発行し、クライアントシステム側で管理・認証。
- 保存データへのアクセスコントロールは、Read Write、Read Only の２つ。エンドユーザごとのアクセスコントロールはクライアントシステムが設定・管理。
- 保存データへの操作と装置への操作は全て自動的に履歴を保存（管理者の操作も履歴に残り、管理者でも履歴の改竄は不可能）。

3. 記録媒体及びバックアップ

- 保存データを可搬媒体(CD-R)へ書き出し、媒体識別番号を付与して管理が可能（原本の所在は保存装置内部で管理）。
- 保存装置内部のデータは自動的にミラーリングし、また外部記憶装置へバックアップを作成可能。

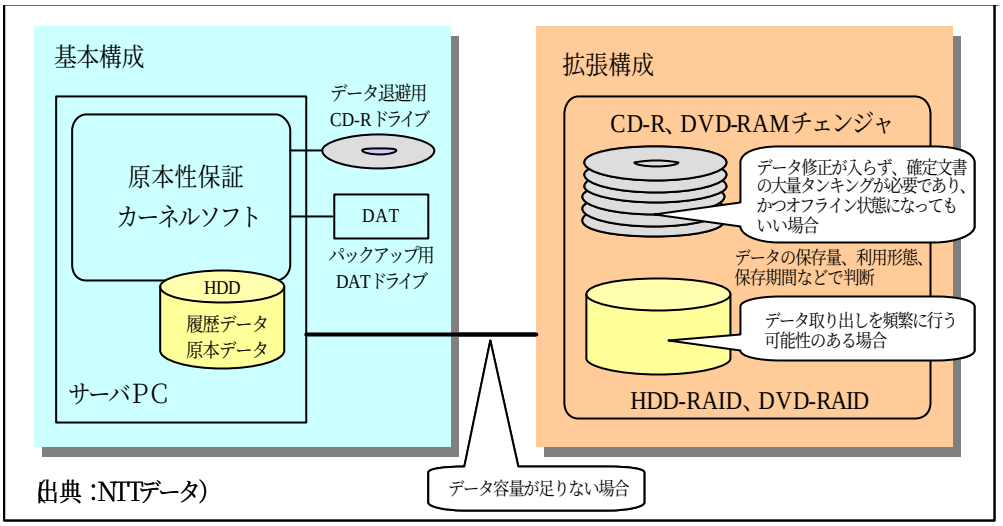

図 3-17 原本性確保支援システム Trusty Cabinet V1 の構成概要

3.3　　電子公証サービス

電子公証は、電子認証とならんで電子申請・企業間取引・電子文書長期保存等を支えるプラットフォームであり、一般的には「第三者（TTP: Trusted Third Party）による、電子的記録の原本性を保証するサービス」として捉えられている。しかしながら、実際に電子公証という言葉が何を指すかについて、立場により解釈が異なる部分がある。

例えば ECOM では、過去の報告書において電子公証を次のように定義している（H10.5 「電子公証システムガイドライン」の成果の概要、より引用 ）。

『（前略）取引当事者間の信頼性確保の視点から「“ 誰が（と） ”、“ 何を ”、“ 何時 ” 電子的交流を行ったかを証明する仕組み」であるとした。』

このような解釈を元に、公証制度の範囲外において行われるもの（民間が提供するサービス）も電子公証に含める、という位置づけが ECOM においてはされてきた。一方、公証制度を実質運営する法務省は、民間の提供する電子公証について以下のように述べている。

『民間の企業がその情報収集能力を利用して収集した情報に基づいて，契約に基づいて一定の事項を証明することは，法律用語としての公証ではない。（後略）』（H9.3「電子取引法制に関する研究会中間報告書」より抜粋）

このように、電子公証という言葉持つ意味にはいくつかの解釈が存在しているが、それらの共通部分のみを抽出すると以下のような要件が残る。

- 電子的記録の非改竄を保証し、証拠能力を担保するための一要素
- 非改竄の保証は、当事者ではなく第三者によって行われる
- 電子公証の提供者が誰であるかは、特に問わない

3.3.1　電子公証の概要　[14]

電子公証のシステム構成は、第三者である電子公証センタと、それを利用するユーザから成り立っている。

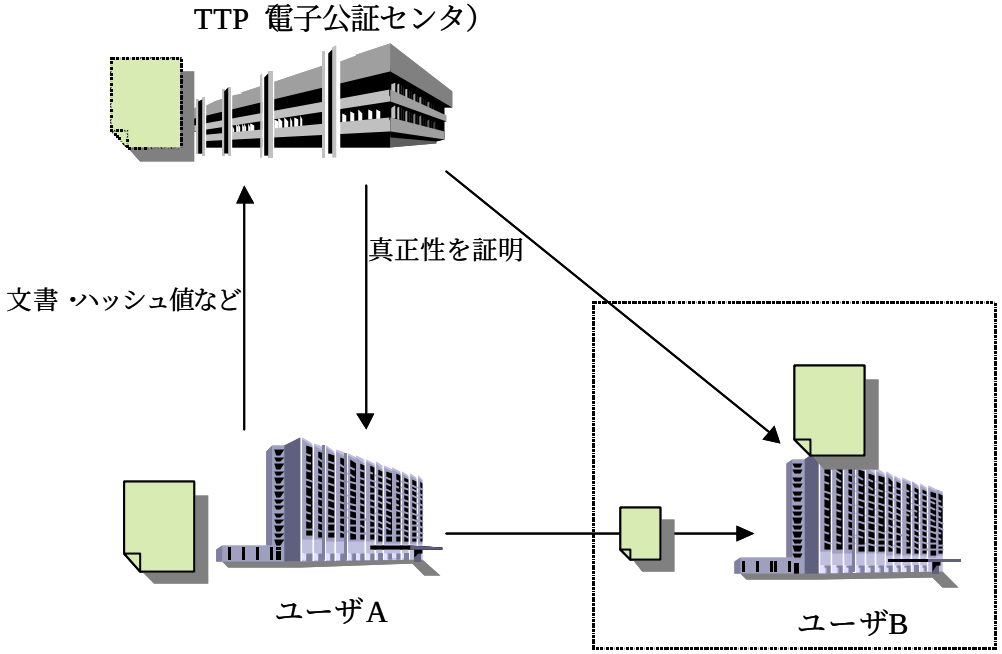

図 3-18 電子公証システムの構成

ユーザの手元にある電子的記録は、TTP によってその真正性が保証される。真正性を保証する方式はいくつかあるが、代表的な方式として

- ユーザが TTP に電子的記録を預け、TTP でその記録を厳密に保管・管理する。
- 電子的記録をユーザの手元に留めておき、TTP には真正性の保証に必要となるデータ（ハッシュ値など）のみを送信する。

という 2 種類が挙げられる。

また、「電子的記録の真正性を保証する」という行為について、その意味するところは以下の２つに大別することができる。

- 文書を作成する過程が真正であることを保証する（形式主義）。
- 文書内容の真正を保証する（実質主義）。

形式主義は、通常作成名義の真正を保証することを意味し、民事訴訟法第 228 条の第４項「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する。」などに関わる考え方であると言えよう。

これに対し、実質主義は文書内容の真正性を問うものであり、文書が成立する過程が真正であっても内容が不実である場合、その文書は真正なものと見なさない。例えば、遺言目的で公正証書を作成しようとする場合、遺産の相続対象が法的に無効な場合（猫とか犬など）は発行されない。一部の例外を除き、この考え方は専ら公文書に対して適用される。従って、実質主義に基づいた公証はその対象が公文書でない限り困難であり、オフラインの世界では「私的な目的で作成する契約書などに対して内容の真正性を保証する場合、公証役場において公正証書を作成する。」ということが行われる。同様に、実質主義に基づいた電子公証についても、国による公証制度の枠組みに則って行われることになる（3.3.2 電子公証サービスの事例の 1.電子公証（法務省）を参照）。

一方ユーザの立場から見ると、電子公証システムには以下のような役割を果たすことが期待さ

れている。

１．自ら保管する記録の真正性を担保

２．自組織外に送信・提出する記録の真正性を担保

３．文書の存在時刻証明（時刻認証）

４．アーカイブサービスの一環として利用

1 の形態は、文書が外部に送られることなく、もっぱら自組織内に蓄積されていく利用方法である。企業の研究開発部門で蓄積されている実験レポート、医療機関における電子カルテに対する公証サービスの利用などが、この形態に相当すると言える。この場合、公証の対象となるデータは基本的に組織外に公開できない、極めて機密性の高いものであることが多く、そのため TTP に電子的記録そのものを送る形は一般的に取りにくい。

対照的に、2 の形態は複数組織間でやり取りされるデータの真正性を保つ目的であり、電子メールから EDI におけるトランザクションまで、幅広い利用形態が想定される。TTP に文書を預けるか否かはケース次第であるが、例えば米国においては証券取引委員会(SEC)規則において、証券会社-顧客間でやり取りされる電子的記録そのものについて、第三者による保存が義務付けられている。

3 は文書の存在時刻の証明に重きをおく利用形態であり、従来の紙による文書管理では、公証人役場の確定日付や郵便局の消印の利用がこれに相当する。通常、電子的記録の作成（存在）時刻を証明することは困難であるが、電子公証サービスを利用することにより「該当文書がその日付にその形で世の中に存在していたこと」を客観的に証明することが可能になる。特に、米国では特許制度として先発明主義（出願日ではなく発明日を基準時として採用する制度）を採用している関係上、企業における知的財産権に関わる文書管理に公証サービスを利用しているケースが多い。

4 はアーカイブサービスの一環として公証サービスを利用する形態であり、文書そのものを TTP に預ける形となる。ユーザから見ると、他組織によって運用されているアーカイブサービスまたはバックアップサービスを利用しており、そのうち重要な文書についてはアーカイブサービス提供者によって真正性が確保されている、という状態である。

3.3.2　電子公証サービスの事例

国内で利用可能な（もしくはまもなく利用可能になる）電子公証サービスとして、法務省の電子公証サービスと、(株)NTT データの電子文書証明サービス SecureSeal の概要を以下に記す。

3.3.2.1　電子公証サービス（仮称）（法務省）

(1) 現在の状況

法務省の電子政府サービスとして現在開発中であり、Step-1 は「譲渡性預金（CD：negotiable certificate of deposit）の譲渡の際の通知・承諾のための確定日付保証」のために使われる。平成 13 年度早々に運用開始を予定している。CD は、金融機関が短期の資金調達に用いるものである。

(2) システム仕様

Step-1 の仕様では年間 20 万件の利用が予定されており、文書全体を保管する（１件あた

り平均１ＭＢ）。システムの利用者は「企業」のため法人登記を元にした電子証明書により申請を行う。その文書に対し指定公証人名簿を元にした電子証明書により、署名（公証人が契約を保証）される。企業・公証人の電子証明書の有効期限は１年である。
今後は、法人登録申請の電子化（現在 350 万登録）、CD 以外には「船荷証券」の取り扱いなどを予定している。

(3) 文書保存（保証）期間

２０年保存。

(4) 長期保存に対する対策

文書はシステム側にて厳重保存されている。システムは２重化されているが、ロケーションの２局化はない。保存電子文書の長期保管について「災害対策」「記録メディアの検討」などさらなる詳細な各種要件は、今後の課題にするとのことである。

(5) 参考文献

「登記インターネット（月刊）」 発行販売 社団法人 民事法情報センター

(6) その他

「公正証書（遺言や離婚協議書など）」への適用は、利用者（一般市民）の電子証明書に対する解決方法が未定なため、今後検討する予定である。法務省には利用者の台帳が無いので、単独でのシステム化は不可能である。利用する電子証明書に関する方針は特に無く、認可を受けた民間認証局の証明書でも、自治省の証明書でも何でも良いとの見解である。一方、実際の利用シーンについては、完全オンライン化するには現行の法律に「遺言を関係者集めて読み上げること」などが規定されているため、これをメールにして良いなどの法律変更を伴わなければならない。

3.3.2.2 電子文書証明サービス SecureSeal（NTT データ）[15]

(1) 現在の状況

2000 年 4 月よりサービスを開始している。電子カルテシステムやデジタルコンテンツ管理システムにおいて、「原本性保証機能」としてシステムに組み込んだ形で提供されている。利用料金は、2000 件／月からで 24 万円／月。一件あたり 120 円だが、NTT データでは小売りはしていない。北米 Surety.com 社（SecureSeal の開発元）でも、サービス形態として小口対応メニューは無いが、リセーラによる小口サービスがある。

(2) システム仕様

利用者は専用の端末ソフトにより、保存したい電子文書のハッシュを生成し、「SecureSeal」センタへ登録する。するとセンタから「SecureSeal 証明書（X.509 電子証明書ではない）」が発行される。SecureSeal 証明書には、登録文書のハッシュの他に時刻情報や、SecureSeal センタにおける同時刻に発生したハッシュを統合した SHV（Super Hash Value）などが含まれる。文書の検証は、登録時と同じ手順でハッシュ生成したものがセンタに登録されていたものと同値であるか確認することで実現される。
SecureSeal センタでは、管理しているハッシュの改竄が無いことを証明するため、一週間分の SHV のハッシュを新聞紙面（日本では日経産業新聞。毎週金曜日）に公開している。

(3) 文書保存（保証）期間

文書そのものの保存は行わない。文書の原本性を保証した「ハッシュ（SHV）」の保存を毎 0.1 秒ごとに行っている。SHV は全て保存し、文書の検証目的でオンライン参照できるようになっている。サービスの制約として「保存期間」は設定されておらず、SHV はこのサービスが継続される限り未来永劫保存することになっている。

(4) 長期保存に対する対策

現在のハッシュサイズは 288bit だが、将来この長さが危険になった場合はサイズの延長が必要になる。その具体的な方法（登録文書のハッシュを新しいハッシュ値で取り直す）は特許になっている。

4 付録

4.1 用語集

本中間報告で使用されている主要な用語の一部を、以下に概説する。

1. 公開鍵暗号システム（Public Key Cryptosystem）
   関連した2つの鍵(公開鍵と秘密鍵)を使用する非対称暗号方式(asymmetric cryptographic algorithm)の一つであり、一方の鍵(公開鍵)で暗号化したデータは他方の鍵(秘密鍵)でのみ復号化できるようになっているシステム。2つの鍵は、公開鍵が与えられても、秘密鍵を導き出す事が計算上不可能な特性を持つ。
2. 公開鍵（Public Key）
   公開鍵暗号システムにおける鍵ペアのうちの一つで、通信相手等の他人に知らせて利用してもらうための鍵。
3. 秘密鍵（Private Key）
   公開鍵暗号システムにおける鍵ペアのうちの一つで、他人には知られないように秘密にしておく鍵。
4. 鍵ペア（Key Pair）
   公開鍵暗号システムにおける公開鍵及びそれに対応する秘密鍵。
5. 共通鍵（Secret Key）
   発信者と受信者が同一の暗号鍵を使用してデータの暗号化と復号化を行う対称暗号方式(symmetric cryptographic algorithm)における鍵。
6. 公開鍵基盤（Public Key Infrastructure）
   公開鍵暗号システムを用いて情報システムやコミュニケーションシステムのセキュリティを確保するための一連の技術およびサービス。
7. 認証（Certification）
   個人、法人、装置等を対象として、証明書を生成するプロセス。
8. 本人確認（Identification & Authentication）
   個人、法人、装置等の認証対象者に関する情報が真正であることを審査する行為。
9. 証明書（Certificate）
   認証対象者の識別情報と公開鍵とが対応していることを証明するデジタル文書。認証対象者の識別情報、その公開鍵、鍵の利用目的・範囲、発行認証局名などが含む一連の情報に、認証局のデジタル署名を付加したもの。従って、厳密には公開鍵証明書であるが、本書では曖昧さがない限り単に証明書という。
10. 証明書の発行（Certificate Issuance）
    証明書を生成し、証明書に登録された申請者に対し、その内容を通知する行為。

11. 証明書の失効（Certificate Revocation）
    証明書の有効期間内に、秘密鍵が危殆した場合、あるいは氏名等の重要な属性情報に変更が生じた場合に証明書を無効にする行為。
12. 証明書の一時失効（Certificate Suspension）
    証明書の有効期間中に一時的に証明書を失効させる行為。
13. 失効リスト（Certificate Revocation List＝CRL）
    失効した証明書のリスト。通常認証局によるデジタル署名が付される。
14. 認証局（Certification Authority＝CA）
    証明書の発行、開示、失効もしくは一時失効等のサービスを行なう信頼された個人または法人。
15. 登録局（Registration Authority＝RA）
    証明書の発行や失効のプロセスにおいて、本人確認などの一部機能を認証局の承認を受けて行う個人または法人。登録局は、証明書や失効リストの生成は行わない。
16. リポジトリ（Repository）
    証明書や失効リスト等を保管し、証明書利用者等に対してこれらの開示や配布もしくは検索等のサービスを提供するシステム。
17. 証明書加入者（Certificate Subscriber）
    認証局から証明書の発行を受けた者。本書では特に区別が必要な場合を除いて、単に「加入者」という。
18. リライングパーティー（Relying Party）
    取引等において証明書を利用する場合、証明書を受け取って、それを信頼して行動する者。加入者ばかりでなく非加入者も含まれる。本書では特に区別が必要な場合を除いて、単に「信頼者」という。
19. 証明書利用者（Certificate User）
    証明書加入者及び証明書信頼者などの証明書を利用する者。本書では特に区別が必要な場合を除いて、単に「利用者」という。
20. 証明書ポリシー（Certificate Policy）
    認証局のサービス・運用等に関する方針や規定、基準。
21. 認証局運用規定（Certification Practice Statement＝CPS）
    証明書ポリシーに基づいて、認証の実施における手続き、遵守事項などを文書化したもの。利用者等の認証局の外部者に開示されるもの。
22. 事務取扱要領（Operation Manuals）
    認証局運用規定に基づいて、認証局内部における実務を詳細に規定したもの。
23. 危殆化（Compromise）
    秘密鍵や関連機密情報等が、盗難や漏洩、第三者による解読等によってその機密性を失ったか、あるいはその可能性があること。

24. デジタル署名（Digital Signature）
署名対象データのハッシュ値(データを数学的な操作によって一定の長さに縮小させたもの。ハッシュ値から元のデータは再現不可能)に対して、秘密鍵で暗号化したもの。デジタル署名の検証は、デジタル署名を公開鍵で復号化した値と元のデータのハッシュ値とを照合することで可能。デジタル署名は、当該秘密鍵の保有者のみが生成できることから文字による署名と同等の効果が推定される。
25. 電子署名（Electronic Signature）
間違い無く本人である事を証明する電子的なデータ。デジタル署名と同義で使われる事が多いが、広義ではアナログ署名を電子データにしたものも含む。
26. 暗号モジュール（Cryptographic Module）
暗号鍵等の生成、保管、利用などにおいて、セキュリティを確保する目的で使用されるソフトウェア、ファームウエア、ハードウェアあるいはそれらを組み合わせた装置。

4.2　　参考文献

今回検討を進めるにおいて参考とした文献を以下に示す。文書によってはﾊﾞｰｼﾞｮﾝが更新されることがあるので、注意を要する。（ＵＲＬは 2001 年 3 月現在）

1．行政文書の管理方策に関するガイドラインについて（平成 12 年 2 月 25 日　各省庁事務連絡会議申合せ）http://www.somucho.go.jp/gyoukan/kanri/gaido.htm

2．「電子帳簿保存法」とその対応（株式会社さくら総合研究所）
http://www.sakura.co.jp/sir/report/r_consul/19990201.htm

3．　IETF　Electronic Signature Formats for long term electronic signatures
http://www.ietf.org/internet-drafts/draft-ietf-smime-esformats-03.txt

4．　IETF RFC2630「Cryptographic Message Syntax」
http://www.itac.gr.jp/rfc/rfc2630.txt

5．　ETSI TS 101 733 V1.2.2 (2000-12) Electronic Signature Formats
http://www.etsi.org/sec/ts_101733v010202p.pdf

6．　IETF RFC3029「Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols 」http://www.imc.org/rfc3029

7．　IETF Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)
http://www.ietf.org/internet-drafts/draft-ietf-pkix-time-stamp-13.txt

8．宇根 正志、松浦 幹太、田倉 昭　デジタルタイムスタンプ技術の現状と課題
http://www.imes.boj.or.jp/japanese/kinyu/2000/kk19-b1-4.pdf

9．松本勉 他，暗号ブレイク対応電子署名アリバイ実現機構（その１）－コンセプト概要－，情報処理学会ＣＳＥＣ研究会，２０００年３月

10．洲崎誠一 他，暗号ブレイク対応電子署名アリバイ実現機構（その２）－詳細方式－，情報処理学会ＣＳＥＣ研究会，２０００年３月

11．洲崎誠一，ヒステリシス署名と証拠性基盤，電子情報通信学会 ２０００年ソサイエティ大会パネル討論「量子・物理暗号とソフトウェア暗号の協調と未来展望」，２０００年１０月

12．財団法人ニューメディア開発協会「電子文書の原本性保証ガイドライン」他（平成 12 年 3 月）http://www.nmda.or.jp/nmda/soc/sie/index.html

13．総務庁　共通課題研究会中間報告－電子文書の原本性確保方策を中心として－（平成 11 年 4 月）http://www.somucho.go.jp/gyoukan/kanri/990413.htm

14. 公証制度に基礎を置く電子公証制度の導入について（法務省）
http://www.moj.go.jp/MINJI/minji24.html

15. 電子文書証明サービス（Secure　Seal）
http://210.144.76.11/index2.html

16．　Final Report of the EESSI Expert Team (20th July 1999)
http://www.ict.etsi.org/eessi/Final-Report.pdf

IETF：Internet Engineering Task Force

ETSI：European Telecommunications Standards Institute

EESSI：European Electronic Signature Standardization Initiative

5 メンバーリスト

事務局

菅　　知之　　電子商取引推進協議会　主席研究員
紙田　政典　　電子商取引推進協議会　主席研究員
米倉　早織　　電子商取引推進協議会　主席研究員

顧問

松本　　勉　　横浜国立大学

リーダー

木村　道弘　　日本電気株式会社
宮崎　一哉　　三菱電機株式会社

ＴＦ５メンバー(編集メンバー)

No.	氏名	会社名
1	藤川　真樹	綜合警備保障株式会社
2	磐城　洋介	ＮＴＴコムウェア株式会社
3	野村　　進	ＮＴＴコミュニケーションズ株式会社
4	鈴木　邦康	株式会社ＮＴＴデータ
5	鈴木　優一	エントラストジャパン株式会社
6	宍倉　勝仁	シャチハタ株式会社
7	畠山　京子	情報処理振興事業協会
8	高橋　征広	日本電気オフィスシステム株式会社
9	橋本　正一	日本電信電話株式会社
10	高山　聡一郎	株式会社日立製作所
11	田中　美樹	株式会社日立製作所
12	洲崎　誠一	株式会社日立製作所
13	小村　昌弘	富士通株式会社

ＳＷＧ３メンバー（上記以外）

No.	氏名	会社名
1	市来　丈彦	株式会社エヌジェーケー
2	河田　悦生	ＮＴＴドコモ株式会社
3	関野　公彦	ＮＴＴドコモ株式会社
4	風間　博之	株式会社ＮＴＴデータ
5	保倉　　豊	グローバルフレンドシップ株式会社
6	高崎　政嗣	グローバルフォーカス株式会社
7	岡　　誠	ソニー株式会社
8	星野　　理	株式会社帝国データバンク

9	中原　　康	株式会社東芝
10	藤岡　直美	日本アビオニクス株式会社
11	田吹　隆明	日本ボルチモアテクノロジーズ株式会社
12	小野　千秋	株式会社日本システムディベロップメント
13	小暮　貢次郎	日本信販株式会社
14	野口　雄治	日本認証サービス株式会社
15	塚田　孝則	日立ソフトウェアエンジニアリング株式会社
16	飯塚　光二	富士重工業株式会社
17	船越　　亘	株式会社富士通総研
18	大木　直人	三菱マテリアル株式会社

平成１３年３月発行
発行：電子商取引推進協議会
東京都江東区青海２－４５
タイム２４ビル１０階
Tel　03-5500-3600
E-mail　info@ecom.or.jp