ISBN978-4-89078-665-7 C2055

電子署名の普及に関する活動報告

平成20年3月

次世代電子商取引推進協議会

電子署名の普及に関する活動報告

平成20年３月

次世代電子商取引推進協議会

序文

ECOM では、2000 年度から、電子署名文書の保存技術に関するガイドラインの作成や各種調査研究を行ってきた。昨年度は、長期署名プロファイルの JIS 原案を作成し、JIS 提案を行うと共に、JIS 原案に基づく長期署名フォーマットを実装する製品や試作品の相互運用性試験を実施した。

JIS 原案に関しては、審議過程で何度か編集上の手直しが行なわれたが、ETSI 仕様を引用規格とした初の JIS 規格として、次の 2 つの規格が 3 月中にも登録される見通しとなった。

- CMS 利用電子署名（CAdES）の長期署名プロファイル：X5092
- XML 署名利用電子署名（XAdES）の長期署名プロファイル：X5093

これらの JIS が発行されることによって、実装者にとっては、相互運用性が確保される実装範囲のガイドとなり、利用者にとっては、相互運用性のある実装の選定が可能になる。

これら 2 つの JIS 規格化されたプロファイルについては、2007 年の春と秋に、約 20 社が参加し各社の実装製品や試作品の相互運用テストを実施し、その動作の確認を行った。相互運用テストに参加して頂いた ECOM 会員各社様、及びテスト用タイムスタンプを無償提供して頂いた、アマノタイムビジネス株式会社様、セイコープレシジョン株式会社様、株式会社 PFU 様、テスト環境整備やテストデータを作成して頂いた、エントラストジャパン株式会社様、日本電気株式会社様、セコム株式会社様にはこの場を借りて再度お礼を申し上げたい。

今年度の電子署名普及の新たな試みとして、業界を超えた課題に関して共通の認識を深め、今後の連携した活動を可能にしていくため、タイムビジネス協議会との共催による「電子署名・タイムスタンプ普及フォーラム」を開催した。また、電子証明書プロファイルの標準化の検討のため、オーストリア等の国民 ID 番号管理制度についての調査を行った。さらに、電子文書の長期保存に関連して、各企業の文書・記録の管理への指針を示すべく、第一段階として各企業における文書管理の実体調査も始めた。

今年度の活動は、会員各位のご協力のもとに、長期保存フォーマットによる相互運用性確保に大いに寄与することができた。本報告書が、電子署名普及促進活動の一端をお伝えできれば幸いである。

平成 20 年 3 月

次世代電子商取引推進協議会

目　次

まえがき

今年度は、文書管理元年といっても過言ではない。国会でも公文書の問題が取り上げられ、省庁連絡会議で公文書保存に関する検討が始まった。最近作成される文書の過半数は電子文書である。電子文書の長期保存は避けては通れない。電子文書の長期にわたる見読性確保や、電子署名の長期にわたる検証可能性の確保は、将来の問題ではなく、現実の問題となっている。内部統制への対応も、電子文書の保管や検索の方法を大きく変えようとしている。国際的な活動状況を見ると、これまでECOMが推奨してきた長期保存形式に一つであるPDFが国際標準として承認された。近々ISO32000 として発行される。

一方、業界の活動を見ると、保険医療福祉情報システム工業会（JAHIS）が、診断書や検査レポートなどの医療文書にする電子署名規格を策定し、タイムビジネス協議会は、電子署先使用権の立証に向けて、「知的財産におけるタイムスタンプ活用ガイド」を発行した。

このような環境のなかで、足掛け 3 年にわたり原案作りと普及啓発を行なってきた長期署名プロファイルが JIS 化されたことは非常に大きな意味を持つ。今後は、署名者の ID や属性との関係を整理しながら、市場に浸透していくことになろう。

本年度は、次ステップに向け、認証公証ワーキンググループと長期署名普及ワーキンググループが合同で活動を行なった。

本年度の活動報告は、3 部構成となっている。各部の概要は次の通りである。

第一部は、今年度の標準化関連活動についてまとめた。

第一部第 1 章では、ETSI との仕様摺り合わせや JIS 化対応など長期署名プロファイルの標準化の経緯などについて、記録を残す意味も含め仔細に紹介している。第 2 章では、JIS 原案に基づくプラグテストの結果を報告している。第 3 章では、ArchiSig など、JIS 案とは異なる長期署名方式の比較検討結果を記している。

第二部は、エストニア、ベルギーなど ID 管理に関する欧州の先進事例について述べると共に、今後のわが国の展望について触れている。

第三部は、内部統制の観点から、文書管理のありかたを調査するための方針や考え方について述べている。また、長期保存媒体に関する最新動向として、磁気テープや光記録媒体の動向についても調査結果を記した。

この分野は、まだまだ課題は山積である。今後とも、一つひとつの課題に取り組んでいく所存である。

第１部　長期署名の国内外の動向

1．標準化

1.1　長期署名プロファイルの JIS 化

平成 18 年度の報告書で、長期署名プロファイル原案を作成し 12 条案件として JIS 提案を行なったところまで報告した。ここでは、その後の審議過程と原案作成元としての対応について述べる。

1.1.1　当初の JIS 原案

JIS 原案作成委員会で作成された原案は、平成 18 年度の報告書「電子文書長期保存ハンドブック」の付録に添付してあるように、次のような構成となっていた。CAdES 版と XAdES 版は同様の構成となっているので、ここでは主に CAdES 版について記す。

当初の JIS 原案のタイトル、本文及び附属書の構成は次のようなものであった。

「暗号メッセージ構文を利用した電子署名（CAdES）の長期署名プロファイルに関する要求事項」

序文
1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 規格適合性
5. 長期署名プロファイル
附属書 A（規定）CAdES のデータ構造と構成要素
附属書 B（参考）参考文献
附属書 C（参考）要素名と ASN.1 表記の対応表
附属書 D（規定）タイムスタンプトークンの構造
附属書 E（参考）PDF/A への長期署名の適用方法
附属書 F（規定）プロファイル適合性宣言

先ず、タイトルであるが、有識者のアドバイスなどにより、日本語であることという条件から CAdES を翻訳したものを適用した。また、関係者以外にも分かるようにということで、プロファイルで留めずにプロファイルの要求事項とした。

引用規格に関しては、JIS 作成ガイドラインに、引用規格は、ISO、IEC、JIS またはそれに順ずるものとの規定があり、ETSI の長期署名仕様 TS 101 733（及び TS 101 933）は、いわゆるデジュア標準ではないことから、附属書 B に参照文献として載せた。

また、用語及び定義については、日本語に訳した用語を載せた。

1.1.2 JIS 化審議過程と最終的な JIS 原案

審議過程で、規格としての言い回しのほか、次の点が指摘された。これは、JIS 規格の作成基準に係わる問題を含んでいることから、長時間に亘って議論された。

①このタイトルからは元となっている CMS 仕様が推測できない

②引用規格が実体と合っていない

③用語定義が実体と合っていない

①と③は、根は同じで、通常用いられている CMS という英語略語を使うか、日本の標準は日本語でという大原則に沿って日本語を使うかとう問題である。結局、CMS は英語ではなく CMS という記号であるという結論になり、「暗号メッセージ構文を利用した電子署名」という表現は「CMS 利用電子署名」となった。更に、プロファイルには要求事項も含まれており、「プロファイルに関する要求事項」という表記は冗長であるということで、「プロファイル」となった。これに伴い、用語定義は暗号メッセージ構文（CMS）ではなく、CMS（暗号メッセージ構文）となった。XAdES に関しても同様に、「拡張可能なマーク付け言語を利用した電子署名」から「XML 利用電子署名」となった。

②に関しては、ISO、IEC、JIS 標準以外は引用しないという従来の運用が、余りにも形式的硬直的であることが議論となり、個別に判断して、ETSI 規格であっても引用規格としてもよいとの判断が下された。この結果、ETSI TS 101 733 を引用規格として掲載し、本来あるべき姿になった。英断に感謝したい。

この結果、JIS 原案は最終的には次のような構成となった。

「CMS 利用電子署名（CAdES）の長期署名プロファイル」

序文
1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 規格適合性
5. 長期署名プロファイル
附属書 A（規定）供給者適合宣言書及び供給者適合宣言書の別紙
附属書 B（参考）CAdES のデータ構造及び構成要素
附属書 C（参考）要素名と ASN.1 表記の対応表
附属書 D（規定）タイムスタンプトークンの構造

1.2 ETSI/ESI との情報交換と仕様調整

ECOM と ETSI（欧州通信規格協会）との実質的なリエゾン関係は平成 17 年度から継続していたが、平成 19 年度から、ECOM は正式に ETSI/ESI のアソシエートメンバとして参加することになっ

た。ETSI/ESI 会議の議題は多岐にわたるが、以下では、ETSI/ESI#17 会議、及び#18 会議で議論された長期署名に関する内容について紹介する。

1.2.1 ETSI/ESI#17 会議

ETSI/ESI#17 会議は、2007 年 7 月 17 日、18 日の両日に、ETSI の本部のあるフランス・ソフィア・アンティポリスで開催された。この会議では、ECOM の長期署名検討体制、JIS 原案概要、2007 年 3 月に実施した Plug Test 結果など、CAdES/XAdES に関する日本の取組み状況の紹介と、CAdES/XAdES の SigningTime の扱いに関する問題提起を行なった。

CAdES/XAdES に関する日本の取組み状況を紹介した結果、ETSI/ESI として次の 2 つの Action Item が設定された。

・ETSI-ECOM プロファイル相互運用ガイドの提示

・PDF への長期署名適用に関する調査報告

また、JIS 原案及び plug test 仕様の英語版提供の要請があり、これに対しては、2007 年 10 月に行なった ECOM の長期保存に関する Web サイトのリニューアルに同期して提供を始めている。

SigningTime は、CMS 署名、CAdES 署名、XAdES 署名で一般的によく使用される属性であるが、これは、署名を行うローカルコンピュータの時計を用いて署名者が主張する署名時刻を表しており、ローカルクロックは誤差が生じたり故意に変更できるものであるため、信頼できる署名時刻とはなり得ない。従って、これを署名対象文書に対するタイムスタンプや署名に対するタイムスタンプと時刻比較することは意味を持たないが、CAdES や XAdES 仕様の Appendix には Informative な情報として、順序としては、時刻の関係が以下の順序でなければならない（Shall）という記述がある。

ContentTimeStamp < SigningTime < SignatureTimeStamp

All/IndividualDataObjectsTimeStamp < SigningTime < SignatureTimeStamp

ECOM の国内実証実験や ETSI との事前実験では、この要件を満たさない署名データを生成する実装も存在していた。日本としては、これらの意味の無い CAdES/XAdES の検証要件を外してもらうべく、両仕様策定のキーパーソン（Nick Pope 氏、Juan Carlos Cruellas 氏）に事前に相談したところ、会議の議題として取り上げられた。

この問題については、

- 指摘された Appendix の記述は Informative なものであり強い要件ではない。
- 比較要件自体を弱い表現に変更してはどうか。
- 署名ポリシの delay 記述ではなく、時間差分の許容範囲とするようにすれば、順序が入れ替わってもかまわなくなる。
- 時間差分の許容範囲の決め方が重要。たとえば、数秒や 10 分といった単位ならば受け入れられるだろうが、1 日やそれ以上となると認めるべきではない。
- メーリングリストでは、署名する機器の時刻管理の監査の観点から、このような時刻比較

の要件を外すべきではない。

などの意見があった。

日本の主張は次の通りである。

- SigningTime は一般的な属性であり、安易に加えられがちだが、検証要件の配慮の不足から実装によっては順序関係を正しく作れない実装も出てくるので、SigningTime 属性自体に注意を要する旨、ノートを追加すべき。
- Appendix の Informative な箇所に検証要件と取れる文書を記述すべきでない。これまで通り順序関係の要件があるとするなら本文にも生成要件として順序を守るような記述を加えるべき。

議論の結果、今後のアクションとして修正案が作成されることとなり、最終的には次のような変更が行なわれた。これは、v1.7.3 の次のバージョンから反映される。

- ETSI TS 101 733 v1.7.3 に基づく RFC 3126 の後継となるインターネットドラフト第 3 版で SigningTime の比較について C.3.6 節で順序に関する記述文言を文書を削除し、「時間差が許可される範囲内であるものとする（shall）。」が追加され、2007 年 11 月、IETF S/MIME Working Group Last Call がを経て 2007 年 12 月 IESG の承認を経た。後継となる RFC は 2008 年 3 月頃公開される予定である。
- IETF インターネットドラフトを反映した ETSI TS 101 733 v1.7.3 の次版となる v1.7.4 のドラフトが 2008 年 1 月に ETSI TC ESI のメーリングリスト内で回覧され、インターネットドラフトの最終版を反映したものとなっている。
- 2008 年 1 月に ETSI TS 101 933 v1.3.2 の次の版の検討を行う STF（Special Task Force）が立ち上がった。この場においても ECOM より SigningTime に関する記述を CAdES と合わせるよう働きかけを行う。

そのほか、CAdES v1.7.3 ベースの IETF インターネットドラフトの状況についてエディタの Nick Pope 氏から報告があった。SHA1 アルゴリズムの危殆化に対応するための新しい属性の別の仕様が IESG の承認を受け最終段階にあり、CAdES はこれに依存しているため、これが策定され次第、CAdES v1.7.3 ベースのインターネットドラフトを更新するとのことであった。CAdES v1.7.3 の RFC 化後は、そこで得られたコメントを再度 ETSI TS 101 733 CAdES の標準へ反映が行なわれる。

なお、旧版の CAdES は RFC 3126 で規定されており、これは Informational RFC であることから、改訂版も恐らく Informational RFC となるものと思われる。

1.2.2 ETSI/ESI#18 会議

ETSI/ESI#18 会議は、2007 年 11 月 6 日、7 日の両日に、フランス・パリにある Bull/SAS の会議室にて開催された。この会議では、これまで ECOM が検討してきた PDF 署名における長期署名の適用方法について紹介すると共に、長期署名プロファイルの JIS 案、及び長期署名に関する ECOM の英語／日本語ウェブサイトの紹介を行なった。

長期署名プロファイルの JIS 案に関しては、長期署名（Long Term Signature）の用語定義が

曖昧との指摘があった。長期とは何処からを指すかが分からないので、証明書の有効期限が切れた後などのように明記した方がよいとのとのことであったが、この定義は日本での共通認識を表したものなので、その旨回答した。また、署名者はオフラインで署名を行うことがあり、常にタイムスタンプが付与できるとは限らないので、ES-T を必須としていることに問題があるとの指摘もあったが、これについては、署名・タイムスタンプ付き文書を作成者から検証者に渡すときのプロファイルであることを追加説明した。

PDF 署名に対する長期署名の適用方法については、PDF 署名における ByteRange に関連する問題点の指摘と具体的な対策は、大変参考になったと感謝された。また、これに関連して、PDF 本体の ISO 化（DIS32000）が話題になり、TC171 での標準化状況に関して情報提供を行なった。

続いて、2007 年 10 月に公開した ECOM プラグテスト Web サイトの紹介を行った。プラグテスト Web サイトは ECOM プラグテストのポータルとして作成したものであり、長期署名フォーマットプロファイルの JIS 原案文書や実証実験のテスト設計書、テストデータをダウンロードすることができる。実際に Web ブラウザで Web サイトを見せながら紹介を行い、プラグテストの参加者一覧やテストの概要、テストケースの概要を示した。国際実験参加のための連絡方法などの問い合わせもあり、Web サイトについて好意的な評価を受けることができた。

そのほか、ERS（RFC 4998 Evidence Record Syntax）と CAdES/XAdES との違いについて調査報告があった。ERS 自体は、「文書がある時点で存在した」という証拠情報を生成し保管するサービスを実現するためのプロトコルの規定であり、サービス提供側は ArchSig 方式が想定されているものの、CAdES/XAdES や他の文書保管サービスも適用可能なものとなっている。LTANS でも ASN.1 文法定義に ArchiveTimeStamp が記載されているが、これは文書保管の証拠情報とすることのできる任意の方式のタイムスタンプである。

ERS について議論にあがった特徴は以下のようなものであった。

- 少ないタイムスタンプで実現できる。
- 検証情報リファレンスに関する情報を含まない。
- TSU（Time Stamp Unit）が危殆化した場合に運用上の懸念がある。
- CAdES の ContentTimeStamp は一つの文書に対してのものだが、ERS は複数の文書に対して行なえる。
- タイムスタンプ更新時の運用に問題がある。
- ERS は Long Term Archiving Service Provider のサービスのための規定であり、CAdES/XAdES は任意のユーザのためのものである。

1.3 PDF/A への長期署名の適用方法

1.3.1 検討の経緯

PDF/A は、電子文書の長期保存に適したファイルフォーマットの一つであるが、PDF/A のみならず PDF で通常用いられている enveloped 形の署名方法においては、アーカイブタイムスタンプ

を PDF 内の署名フィールドに収容できないという問題がある。ECOM では、この解決方法について 2006 年度から検討を進め、当初の JIS 原案では、その解決方法の一つを参考として附属書に付けていた。具体的には、アーカイブタイムスタンプを増分更新で添付ファイルとして格納し、アーカイブタイムスタンプ更新の際は、この添付ファイルを差し替えるという方法である。

この案に対して、PDF/A の所管団体である社団法人日本画像処理マネジメント協会（JIIMA）殿から、次の 2 つの理由から仕様を見直すよう申し入れがあった。

(1) PDF/A（19005-1：2006）では添付ファイルを禁止している。

(2) 添付ファイルの差し替えは、PDF の流儀にそぐわない。

(1)に関しては、PDF/A プロファイルに適合した PDF ファイルに、アーカイブタイムスタンプを増分更新で添付ファイルとして格納すると、その新たな PDF ファイルは、PDF/A プロファイル適合ではないが、長期署名は可能となる。しかし、JIIMA 殿から、「PDF/A ファイルには添付ファイルをつけてはならない」との PDF/A の所管団体としての解釈が提示されたため、関係者との更なる議論と調整が必要との判断から、附属書「PDF/A への長期署名の適用方法」を JIS 原案から削除した。

PDF や PDF/A への長期署名の適用に関しては、引き続き要求もあることから、JIIMA 殿からの申し入れ内容も考慮し、PDF/A への長期署名の適用方法の見直しを行なった。

(1)に関しては、対象を、PDF/A（19005-1：2006）ではなく、PDF 仕様とした。PDF 仕様に関しては、2007 年 12 月に PDF1.7 が ISO の標準として承認されたことから、近いうちに ISO 32000 として発行される。なお、アーカイブ用プロファイルに関しては、PDF/A の次のバージョン（PDF/A-2）が標準化過程にあり、このバージョンでは、添付ファイル禁止の制限は解除されることが決まっている。

(2)に関しては、メタデータの追加などの記録管理の観点から、差し替えではなく増分更新を続ける案も、検討段階では挙がっていたが、実装の容易さを優先した結果であり、再考することとした。

1.3.2 PDF における CAdES-T データ及び CAdES-A データの格納方法

以下に、見直し結果を掲載する。

a) CAdES-T データは、PDF/A 適合ファイルの署名フィールド内に格納し、CAdES-A データは、増分更新により PDF/A 適合ファイルに追加する添付ファイルとして格納する。

注記 この増分更新は PDF 仕様に従うが、PDF/A の適用範囲外にある。

注記 CAdES-T データの代わりに CAdES-BES データ又は CAdES-EPES データを格納し、署名タイムスタンプを付与した CAdES-T データは添付ファイルとして格納しても良い。

b) CAdES-A データを PDF/A 適合ファイルに添付ファイルとして格納する際に、複数回延長処理が施された CAdES-A データを格納しても良い。

c) CAdES データは、バイナリ変換せずにそのまま添付ファイルとする。添付ファイルの MIME タイプは“application/pkcs7-signature”とする。

注記 MIME タイプ“application/pkcs7-signature”に対応するファイル名拡張子は“p7s”

である。

d）長期署名の延長（アーカイブタイムスタンプの再取得）は、添付ファイルとして格納された CAdES-A データに対して行い、更新された CAdES-A データは、元の添付ファイルを格納しているオブジェクトの更新として、PDF 文書に添付する。

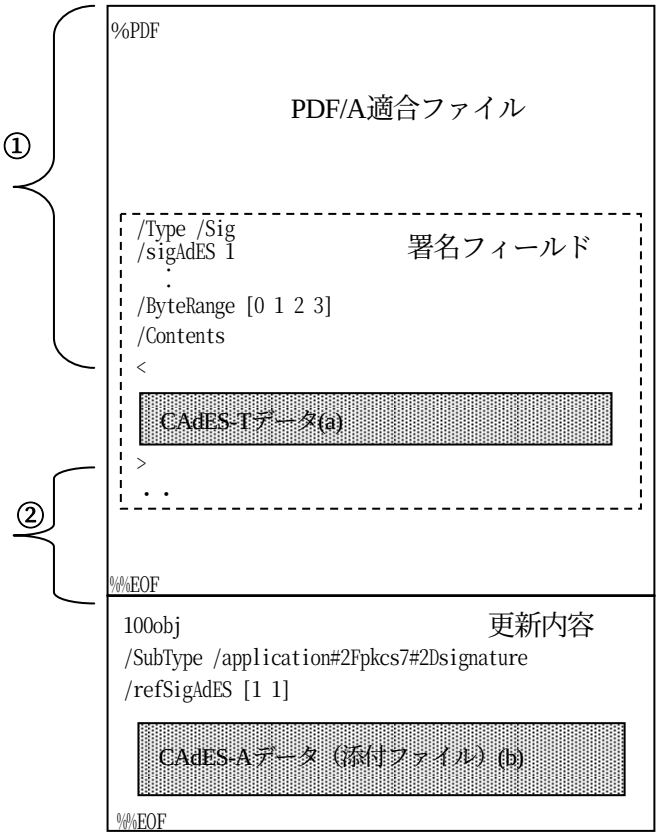
e）署名フィールド内に格納した CAdES-T データのコピーを、添付ファイルとして格納しておいてもよい（増分更新）。もし必要なら、署名フィールド内に“ /sigAdES ”というキー、およびその値に、対象文書に長期署名が施された回数を記述して、この添付ファイルの存在を表示してもよい（例. ” sigAdES 1 ”）

f）添付ファイル格納用の辞書には、2 つの値を持つ“ /refSigAdES ”というキーを記述しても良い。キーの記述例は“ /refSigAdES[a b] ”となり、a は署名フィールド内のキー“ /sigAdES ”の値に対応し、b は長期署名の延長（アーカイブタイムスタンプの再取得）のために CAdES-A をオブジェクト更新した回数を表す（例. “ /refSigAdES [1 2] ”）。

1.3.3 CAdES-A データの格納方法の具体例

(1) 署名対象の PDF ファイルに電子署名を付与し、1 回目のアーカイブタイムスタンプを付与した場合。

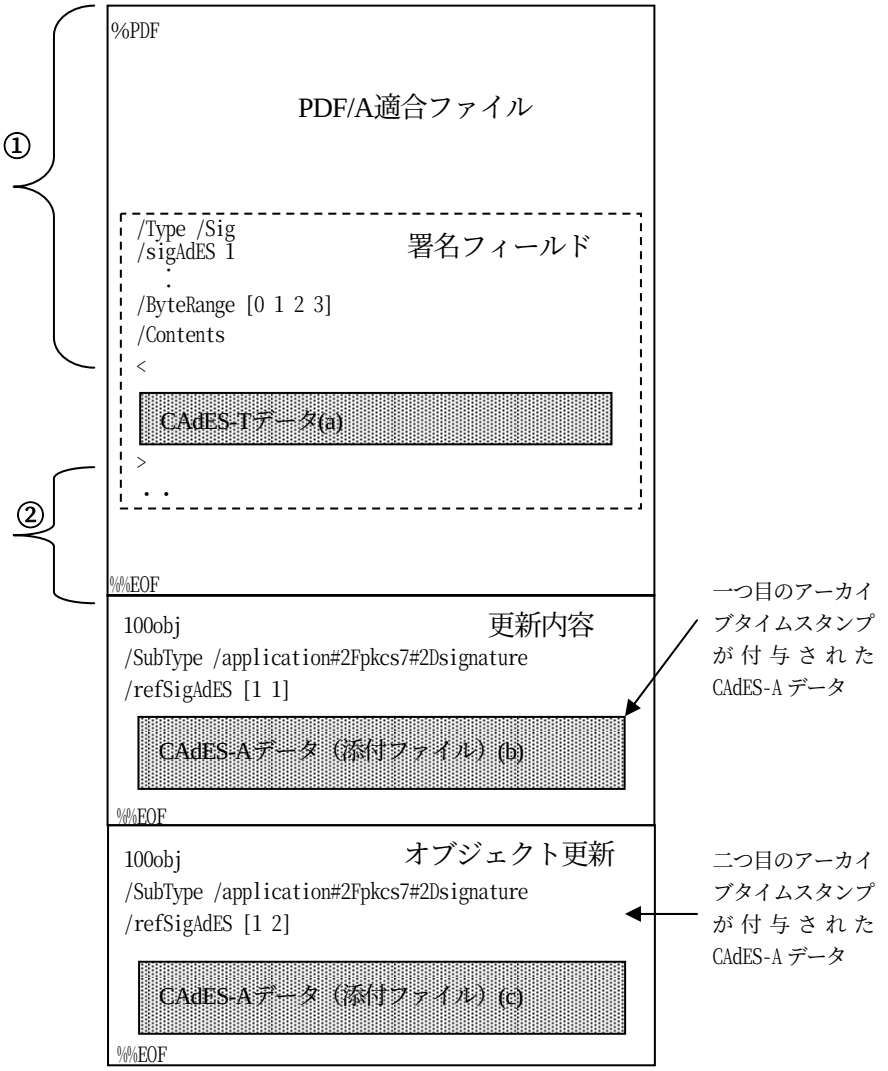
注　以下の記述で①、②はバイトレンジの範囲を示す。



注記　図では、相互参照セクション、トレーラなどは省略している。

図 1.1.1 一回目のアーカイブタイムスタンプ付与時

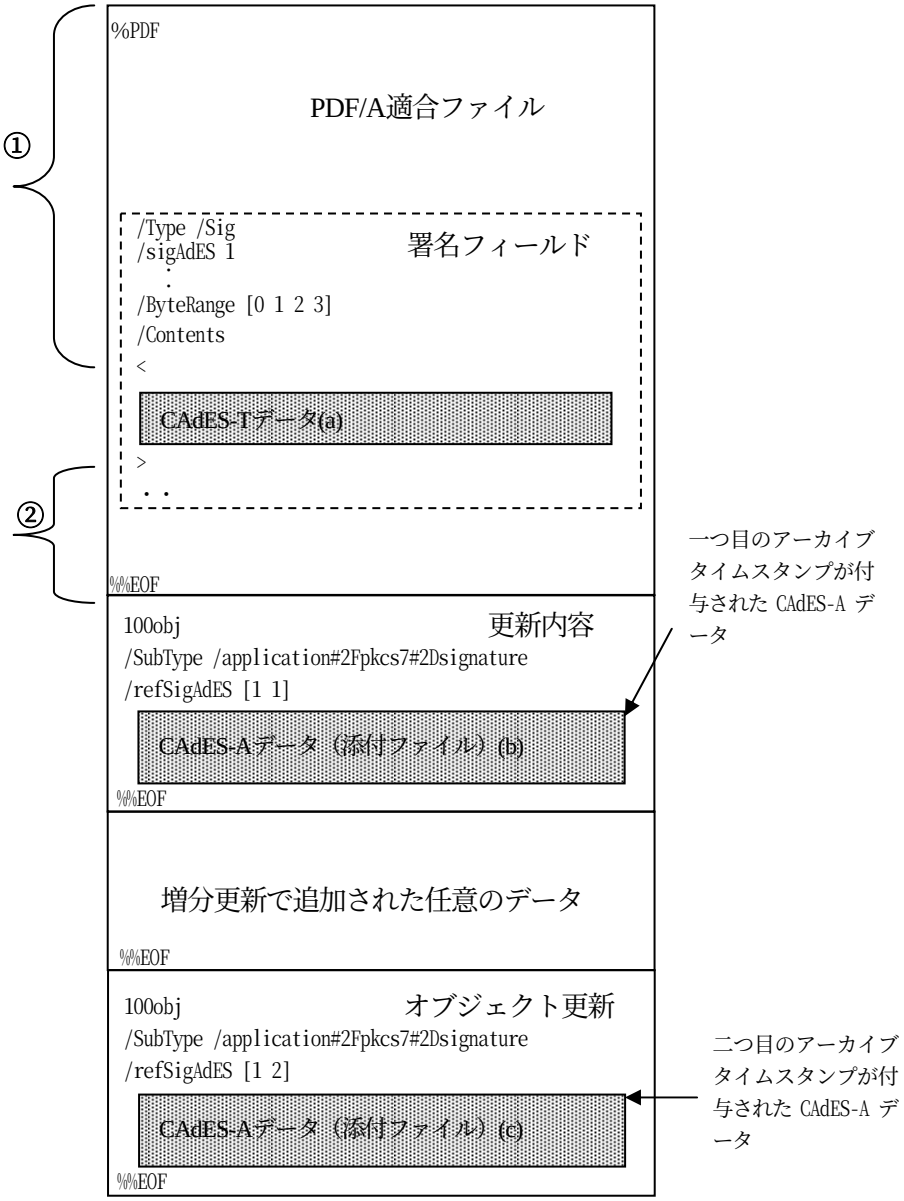
(2) 署名対象の PDF ファイルに電子署名を付与し、2 回目のアーカイブタイムスタンプを付与した場合。



注記 図では、相互参照セクション、トレーラなどは省略している。

図 1.1.2 2 回目のアーカイブタイムスタンプ付与時

(3) 署名対象の PDF ファイルに電子署名を付与し、1 回目のアーカイブタイムスタンプを付与した後、任意の情報が増分更新で追記された後、既に付与されている CAdES-A を延長する場合。この場合、長期署名フォーマットで長期間保証されるのは①②部分の署名対象データのみとなる。増分更新で追記された部分を保証したい場合は、再度電子署名を付与する必要がある。

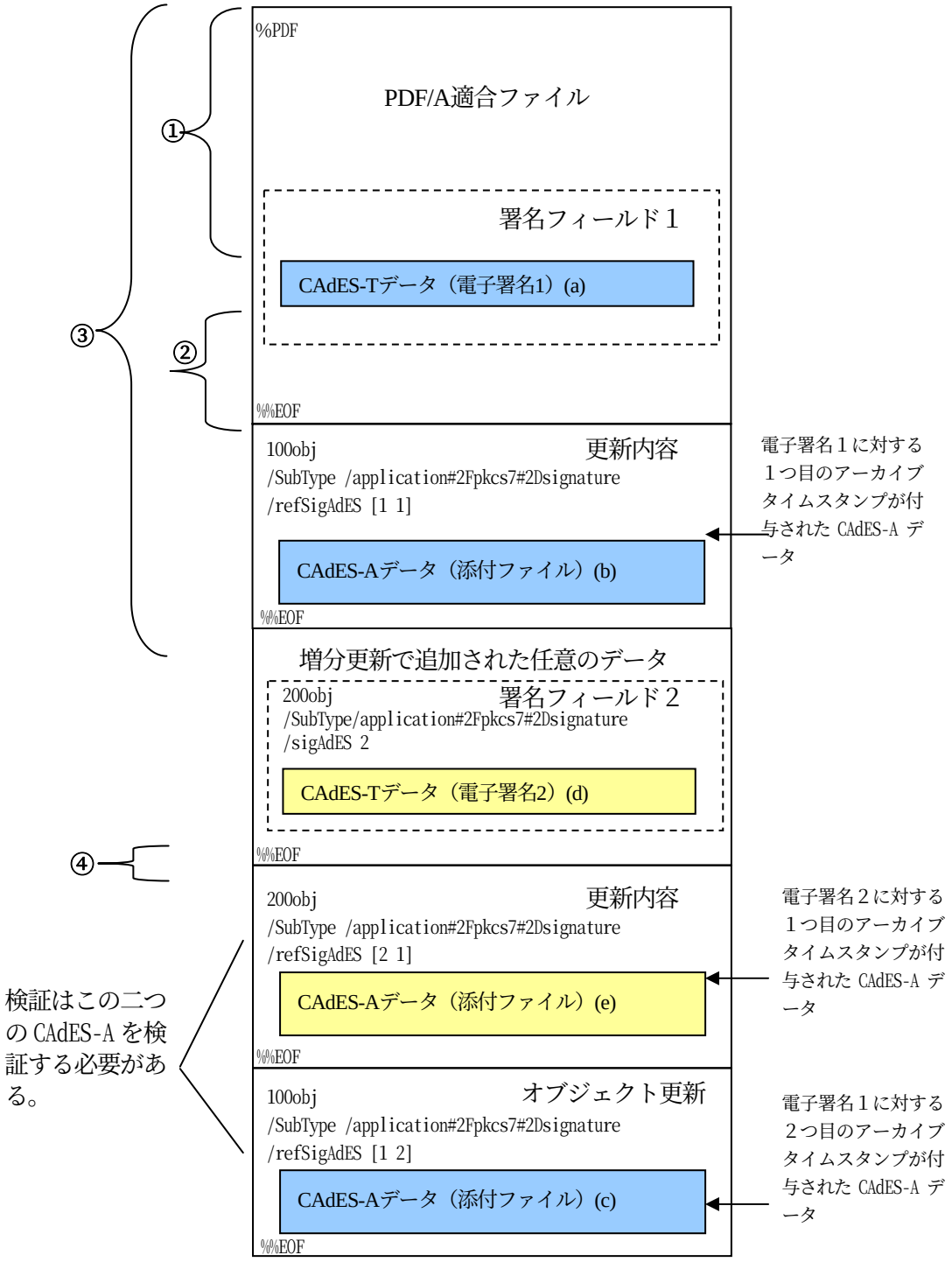


注記　図では、相互参照セクション、トレーラなどは省略している。

図 1.1.3 2 回目のアーカイブタイムスタンプ付与時

（任意のデータが増分更新で追加された場合）

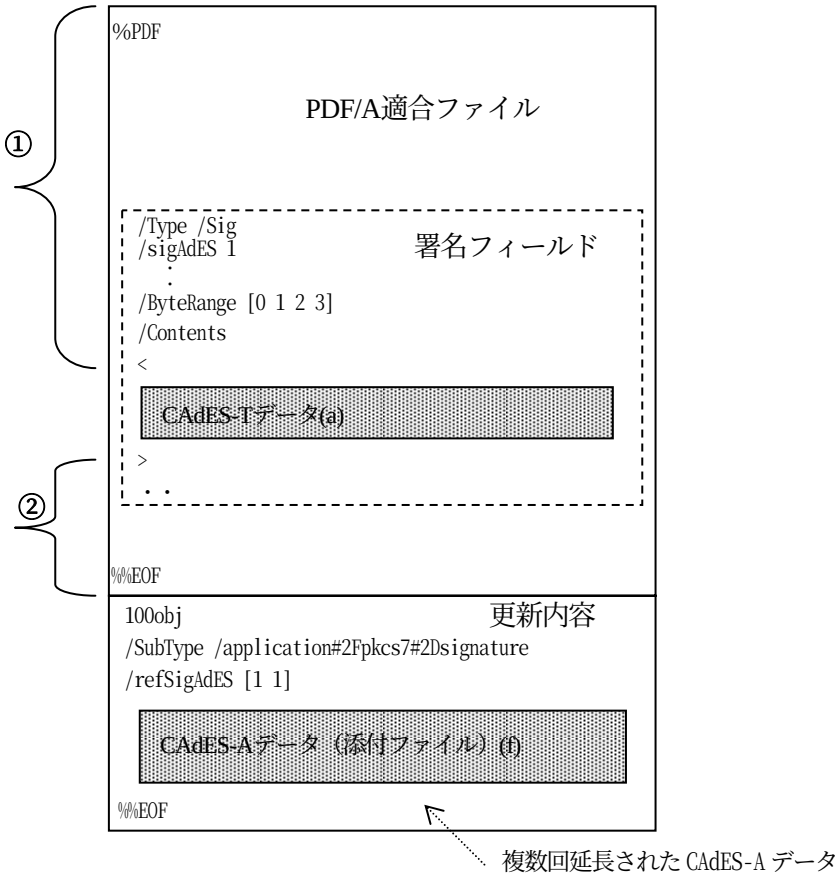
(4) 署名対象の PDF ファイルに電子署名 1 を付与し、1 回目のアーカイブタイムスタンプを付与した後、任意の情報が増分更新で追記された場合の署名延長の方法。増分更新で追記された情報に電子署名を付与すると署名対象は③④となる。この状態で署名を延長する場合、その後ろに電子署名 2 に対して一つ目のアーカイブタイムスタンプを付与した CAdES-A データを添付する。電子署名 1 をさらに延長したい場合は、電子署名 1 に対する二つ目のアーカイブタイムスタンプを付与した CAdES-A データをオブジェクト更新で追記することになる。



注記　図では、相互参照セクション、トレーラなどは省略している。

図 1.1.4 任意のデータが増分更新で追加された場合の複数の署名を延長する場合

(5) 電子署名１を付与した署名対象の PDF ファイルに、複数回署名延長された CAdES-A データを格納する場合。電子署名１を付与した署名対象の PDF ファイルと、CAdES-A データとを DB や文書管理サーバ等のシステムで別々のデータファイルとして管理し、システムからの取出し時に PDF ファイルに CAdES-A データを格納する等の運用で利用されることが考えられる。



注記 図では、相互参照セクション、トレーラなどは省略している。

図 1.1.5 署名対象の PDF ファイルに、複数回署名延長された CAdES-A データを格納する場合

a）検証時は、各電子署名（ここでは、図 1.1.4 の電子署名 1 と電子署名 2）に関する最新の CAdES-A データをそれぞれ検証する必要がある。

b）長期署名を延長して行く際に、タイムスタンプトークンの証拠情報をタイムスタンプトークン内に格納する必要がない場合は、図 1.1.4 の再度の CAdES-A データ(c)は不要になる。すなわち、最後に付与された電子署名を延長していけばよい。ただし、最後の電子署名（図 1.1.4 では、電子署名 2）を付与する前にその他の電子署名の CAdES-A データが添付されていること。また、最後の電子署名以外の電子署名に対応する CAdES-A データの一番外側のアーカイブタイムスタンプは、最後の電子署名に対する CAdES-A データに含まれる署名タイムスタンプの時刻で検証することが要件となる。

2. プラグテスト

2.1 はじめに

次世代電子商取引推進協議会（ECOM）では、2004 年 CAdES/XAdES 長期署名フォーマット[1][2]の普及に伴い日本国内での相互運用性を確保する目的でフォーマットの最小限の要件として ECOM プロファイル[3][4]を定め、その翌年 2005 年に ECOM プロファイルの準拠性を確認するための相互運用実証実験[5]を行った。2006 年には ECOM プロファイルに基づき関係団体ならびに有識者が集まり CAdES/XAdES プロファイルの JIS 原案[6][7]を作成し、2008 年 3 月にはこれが JIS として制定される見通しである[10][11]。その間、着実に国内外における CAdES/XAdES の実装が増えており、2007 年度、国内外の CAdES/XAdES の実装を持つ 21 の組織が集まり標準仕様ならびに JIS 原案の相互運用性ならびに標準準拠性を確認するため実証実験「ECOM CAdES/XAdES Plugtest 2007」を実施した。本報告書では、この実証実験の概要について報告する。

2.2 テスト概要

テストは CAdES/XAdES で規定されたフォーマットのうち、異なる組織間で交換されることが多く、JIS 原案における要件ともなっている CAdES-T、XAdES-T、CAdES-A および XAdES-A フォーマットを対象とし、CAdES/XAdES を規定する基礎となる標準と、このうち最小限の要件を定めた JIS 原案に対する準拠性ならびに相互運用性を確認することを目的とし、以下の 2 種類のテストを実施した。

- 共通データ検証機能標準準拠性テスト（2007 年 1 月～3 月）
  実証実験事務局で事前に作成した ES-T、ES-A フォーマットの署名データ、検証情報を用い、これが正しい署名か、そうでないかを期待値通り正しく検証する機能を有しているかを確認するテスト。署名値やハッシュ値の不一致、証明書の失効、期限切れなど無効な署名データの検証も含まれている。

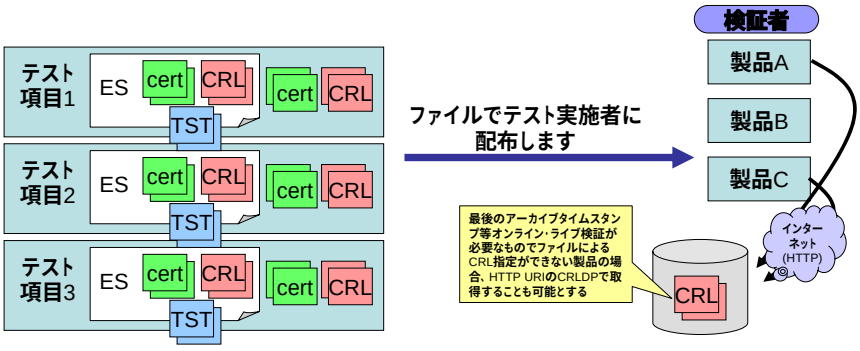


図 1.2.1 共通データ検証機能標準準拠性テストの方法

- 署名生成・検証相互運用性テスト（2007 年 10 月～12 月）
  各参加者の持つ実装により、テスト用タイムスタンプ局を用いてテスト仕様書の要件にあった ES-T、ES-A フォーマットの署名を生成し、これを他の実装が正しく検証できるか、生

成・機能の相互運用性を確認するテスト。

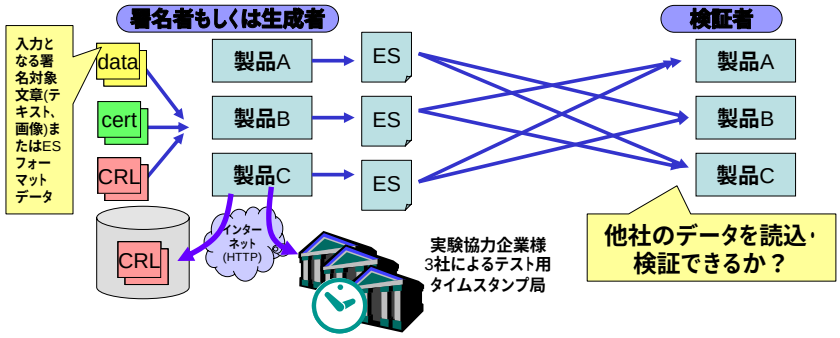


図 1.2.2 署名生成・検証相互運用性テストの方法

JIS の長期署名フォーマットプロファイルには供給者適合宣言書（文献[10][11]附属書 A を参照）というチェックシートが含まれている。これは、署名のどの要素の生成および検証をサポートしているのか、導入側が参考にできるようにするための情報である。本実験では参加者に供給者適合宣言書の提出を依頼した。

実験に際し、国内外向けの実証実験用のウェブサイトを整備した[8]。テストの方法、内容、テストケースなどを定めたテスト仕様書やテストデータは日本語版および英語版の双方がウェブサイトよりダウンロード可能である。テスト内容の詳細については、ウェブサイトの資料の方を参照されたい。

実証実験に参加した組織とそれらの実装は以下の以下の通り。

表 1.2.1 参加組織一覧

組織および実装の名称（五十音順　全 23 組織）	提供種別	用途種別	CAdES	XAdES	国際実験	事前実験
RSA セキュリティ株式会社						
RSA BSAFE e-文書法対応ライブラリ（version 1.3）	製	開				
エントラストジャパン株式会社						
CAdES Add-on for Entrust/IAIK Java Toolkit （build 20071124）+Jython Scripts	試	開	○		○	
XAdES Add-on for Entrust/IAIK Java Toolkit （build 20071207）+Jython Scripts	試	開		○	○	○
関電システムソリューションズ株式会社						
XAdES 長期署名ライブラリ for .NET V2.2	製	開				

サートラスト株式会社 WebSign/FileSign/SignVerifier Ver3.3.0.7	試	ソ	○			
株式会社スカイコム SkyPDF Tools for ArchivingSignature（Version 1.6）	製	ソ	○			
大日本印刷株式会社 SecureStarXML3.0 for Java	試	開		○		
セコム株式会社 セコム長期署名ライブラリ（バージョン 1.4.5）＋テスト用サンプル実装（ver 0.9）	製	開	○	○		
株式会社帝国データバンク TDB 長期署名ライブラリ V0.5	試	開	○			
東北インフォメーション・システムズ株式会社 TOiNX XML 長期署名モジュール（仮称）バージョン 1.0	試	開		○		
日本電気株式会社 PDF 長期署名プラグイン version2.1＋プロトタイプ PKI サーバ/Carassuit 原本保管サーバ Version 3.0	試 製	ソ 管	○	 ○	○ ○	 ○
株式会社日本電子公証機構 JN＋（電子署名・タイムスタンプ付与／検証ソフト）長期署名オプション	試	開	○			
株式会社ハイパーギア HG/PscanServPro 長期保存署名対応版 Ver0.9.1	試	管	○			
株式会社 PFU 長期署名ライブラリ（Build：1.0.10.30）	試	開	○		○	
ビーパークテクノロジー株式会社 DocStamper Version2.0/ESChecker Version2.0	製	ソ	○		○	
富士ゼロックス株式会社 ArcSuite 2.3 原本性保証オプション	製	管		○	○	
三菱電機株式会社　情報技術総合研究所 CMS 長期署名ライブラリ Ver 3.0 XML 長期署名ライブラリ Ver 1.0	試 試	開 開	○	 ○	○ ○	
三菱電機インフォメーションシステムズ株式会社 三菱署名延長システム MistyGuard <EVERSIGN> V3.00（改版予定品）	製	管	○			
有限会社ラング・エッジ Le-XAdES Library Ver0.98f+XAdEStool クライアントβ40（テスト用ツール）	製	開		○		

株式会社リコー 長期署名ライブラリ Ver 0.1	試	開	○			
カタルーニャ工科大学（スペイン）	製	開		○		○
A-SIT／グラッツ工科大学（IAIK）（オーストリア）	製	開		○		○
Safelayer Secure Communications, S.A.（スペイン）	製	開	○	○	○	
Cryptolog International（フランス）	製	開	○	○	○	

凡例：
提供種別：「製」：製品、「試」：試作品・プロトタイプ
用途種別：「開」：開発ツールキット、「ソ」：生成・検証ソフト、「管」：文書管理システム
国際実験：ECOM CAdES/XAdES Plugtest 2007 国際実験グループによる実証実験
事前実験：ETSI-ECOM XAdES Plugtest 事前実験（ETSI XAdES Plugtest 2008 の事前準備として）

また、テスト用タイムスタンプ局、テスト設計、テストデータ作成について以下の企業に御協力頂いた。

表 1.2.2 協力企業一覧

テスト用タイムスタンプ局提供（五十音順）
- アマノタイムビジネス株式会社
- セイコープレシジョン株式会社
- 株式会社 PFU

テスト設計、テストデータ作成（五十音順）
- エントラストジャパン株式会社
- セコム株式会社
- 日本電気株式会社

2.3 テスト結果

署名生成・検証相互運用性テストの生成・検証機能の各テスト項目におけるテスト結果は以下の通りであった。

表 1.2.3 CAdES 署名生成・検証相互運用性テスト集計結果

CAdES生成・検証相互運用性テスト 参加組織名(五十音順)		RSAセキュリティ		エントラストジャパン		サートラスト		スカイコム		セコム		帝国データバンク		NEC		日本電子公証機構		ハイパーギア		PFU		ピーバークテクノロジー		三菱電機		三菱電機インフォメーションシステムズ		JIS要求レベル
実装の提供形態(SDK/生成検証アプリ/文書管理システム)		SDK		SDK		アプリ		アプリ		SDK		SDK		アプリ		SDK		文管		SDK		アプリ		SDK		文管		
製品 / 試作品 区分		製品		試作		製品		製品		製品		試作		試作		製品		製品		試作		製品		試作		製品		
生成 / 検証		生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	
CAdES-T 基本テスト	ON-T-BASIC-ATTACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
	ON-T-BASIC-DETACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
CAdES-T タイムスタンプ局テスト	ON-T-TSA-AMANO-ATTACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-T-TSA-PFU-ATTACHED	○	○	○	○	○	○	○	○	○	○	−	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-T-TSA-SEIKO-ATTACHED	○	○	○	○	○	○	○	○	○	○	−	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
CAdES-T オプショナル属性テスト	ON-T-ATTR-SIGNINGTIME	−	−	○	○	○	−	−	○	○	−	−	−	−	○	○	−	−	○	−	−	○	−	○	○	×	○	任意選択
	ON-T-ATTR-EPES-RFC3125	−	−	○	○	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	要別途
	ON-T-ATTR-SIGNERLOCATION	−	−	○	○	−	○	−	○	○	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	要別途
	ON-T-ATTR-SIGNERATTRIBUTES-CLAIMED	−	−	○	○	−	−	−	○	○	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	要別途
	ON-T-ATTR-CONTENTHINTS	−	−	○	○	○	−	−	○	○	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	要別途
	ON-T-ATTR-COMMITMENTTYPEINDICATION	−	−	○	○	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	要別途
	ON-T-ATTR-CONTENTTS-CLAIMEDTIME	−	−	○	○	−	−	−	○	○	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	要別途
	ON-T-ATTR-CONTENTREFERENCE	−	−	○	○	−	−	−	○	○	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	要別途
	ON-T-ATTR-CONTENTIDENTIFIER	−	−	○	○	−	−	−	○	○	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	要別途
	ON-T-ATTR-COUNTERSIGNATURE	−	−	○	○	−	○	−	○	○	−	−	−	−	−	−	−	−	−	−	−	○	○	○	−	−	任意選択
	ON-T-ATTR-ESSCERTV2	−	−	○	○	○	○	○	○	○	○	○	○	○	○	○	○	−	−	○	○	○	○	○	○	○	○	任意選択
CAdES-A 基本テスト	ON-A-BASIC-A1-ATTACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-A-BASIC-A1-DETACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-A-BASIC-A2-ATTACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-A-BASIC-A3-ATTACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
CAdES-A オプショナル属性テスト	ON-A-ATTR-A1-ARCTSV1-ATTACHED	−	−	○	○	−	−	−	○	○	−	−	−	−	−	−	−	−	−	−	○	−	○	−	−	−	−	任意選択
	ON-A-ATTR-A1-TIMESTAMPEDCERTSCRLS	−	−	○	○	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	要別途
	ON-A-ATTR-A1-ESCTIMESTAMP	−	−	○	○	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	要別途
生成時のTSA証明書パス検証情報の格納方法		UA		F		F		UA		UA		F		UA		UA		UA		UA		UA		F		F		

表 1.2.4 XAdES 署名生成・検証相互運用性テスト集計結果

XAdES生成・検証相互運用性テスト 参加組織名(五十音順)		エントラストジャパン		関電システムソリューションズ		TOINX		NEC		富士ゼロックス		三菱電機		ラングエッジ		JIS要求レベル
実装の提供形態(SDK/生成検証アプリ/文書管理システム)		SDK		SDK		SDK		文管		文管		SDK		SDK		
製品 / 試作品 区分		試作		製品		試作		製品		製品		試作		製品		
生成 / 検証		生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	
XAdES-T 基本テスト	ON-T-BASIC-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	
	ON-T-BASIC-DETACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
	ON-T-BASIC-ENVELOPED	○	○	○	○	○	○	○	○	-	-	○	○	○	○	
XAdES-T タイムスタンプ局テスト	ON-T-TSA-AMANO-ENVELOPING	○	○	−	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-T-TSA-PFU-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-T-TSA-SEIKO-ENVELOPING	○	○	−	○	○	○	○	○	-	-	○	○	○	○	任意選択
XAdES-T オプショナルプロパティテスト	ON-T-PROP-SIGNINGTIME	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-T-PROP-EPES-FREEXML	○	○	○	○	○	○	○	○	-	-	-	-	-	-	要別途
	ON-T-PROP-EPES-TR102038-V111	○	○	○	○	○	○	○	○	-	-	-	-	-	-	要別途
	ON-T-PROP-SIGNERPRODUCTIONPLACE	○	○	○	○	○	○	○	○	-	-	○	○	-	-	要別途
	ON-T-PROP-SIGNERROLE-CLAIMED	○	○	○	○	○	○	○	○	-	-	○	○	-	-	要別途
	ON-T-PROP-DATAOBJECTFORMAT	○	○	−	−	○	○	-	-	-	-	○	○	-	-	要別途
	ON-T-PROP-COMMITMENTTYPEINDICATION	○	○	○	○	○	○	-	-	-	-	○	○	-	-	要別途
	ON-T-PROP-ALLDATATS-CLAIMEDTIME	○	○	−	○	○	○	-	-	-	-	-	-	-	-	要別途
	ON-T-PROP-INDVDATATS-CLAIMEDTIME	○	○	−	○	○	○	-	-	-	-	-	-	-	-	要別途
	ON-T-PROP-COUNTERSIGNATURE	○	○	○	○	○	○	-	-	-	-	○	○	-	-	任意選択
	ON-T-PROP-SIGNINGCERTIFICATE	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
XAdES-A 基本テスト	ON-A-BASIC-A1-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-A-BASIC-A1-DETACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-A-BASIC-A1-ENVELOPED	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-A-BASIC-A2-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-A-BASIC-A3-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
XAdES-A オプショナルプロパティテスト	ON-A-PROP-A1-REFS	○	○	○	○	○	○	○	○	-	-	○	○	-	−	任意選択
	ON-A-PROP-A1-REFS-REFSONLYTS	○	○	−	○	○	○	○	○	-	-	-	-	-	−	要別途
	ON-A-PROP-A1-REFS-SIGANDREFSTS	○	○	−	○	○	○	○	○	-	-	-	-	-	−	要別途
生成時のTSA証明書パス検証情報の格納方法		F		F		F		F		F		F		FS		

凡例:
○: 合格:当該テスト項目の生成/検証の結果に相互運用性上の問題が無い
×: 不合格:当該テスト項目の生成/検証の結果に相互運用性上の問題がある
−: 実装が当該テスト項目の生成/検証の機能を提供していない
製品: 有償、無償を問わず2008年までに製品などの形で提供予定の実装
試作品: 社内の試作目的で開発された実装、又は2008年内に提供予定のない実装
SDK: 開発ツールキットまたはライブラリとして提供
アプリ: 独立した署名生成・検証ソフトウェアとして提供
文管: 文書管理システムまたはその一部となるサーバーシステムとして提供

CAdES 共通データ検証機能標準準拠性テストの各テストケースにおけるテスト結果は以下の通りであった。

表 1.2.5 CAdES 共通データ検証機能標準準拠性テスト集計結果

テストケース	RSAセキュリティ	エントラストジャパン	サートラスト	スカイコム	セコム	帝国データバンク	NEC	日本電子公証機構	ハイパーギア	PFU	ビーバークテクノロジー	三菱電機	三菱電機インフォメーションシステムズ	リコー	テストケース内容
OFF-T-1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	有効である一般的な内包署名のES-Tを読み込める
OFF-T-2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の期限切れを扱える
OFF-T-3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の失効を扱える
OFF-T-4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の認証パス検証を正しく行える
OFF-T-6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-TのSignerInfoの署名値の改竄を検知できる
OFF-T-7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-Tの署名タイムスタンプのトークンのSignerInfoの署名値改竄を検知できる
OFF-T-8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-TのMessageDigestのハッシュ値の改竄を検知できる
OFF-T-9	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-Tの署名タイムスタンプのトークンのMessageDigestのハッシュ値改竄を検知でき
OFF-T-OP-11	–	○	○	○	○	○	○	○	–	○	○	○	○	○	ESSSigningCeritificateV2属性においてSHA-256であるES-Tフォーマットを扱える
OFF-T-OP-12	–	○	○	○	○	○	○	○	–	○	○	○	○	○	ESSSigningCeritificateV2属性においてSHA-512であるES-Tフォーマットを扱える
OFF-T-OP-13	–	○	–	○	○	–	○	○	–	–	○	○	○	○	カウンタ署名を付したES-Tフォーマットを扱える。
OFF-A-3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ETSI TS 101 733 v1.7.3に基づく内包署名の第一世代のES-Aを扱える
OFF-A-4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ETSI TS 101 733 v1.7.3に基づく分離署名の第一世代のES-Aを扱える
OFF-A-5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ETSI TS 101 733 v1.7.3に基づく内包署名の第二世代のES-Aを扱える
OFF-A-6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ETSI TS 101 733 v1.7.3に基づく分離署名の第二世代のES-Aを扱える

XAdES 共通データ検証機能標準準拠性テストの各テストケースにおけるテスト結果は以下の通りであった。

表 1.2.6 XAdES 共通データ検証機能標準準拠性テスト集計結果

テストケース	エントラストジャパン	関電システムソリューションズ	大日本印刷	TOINX	NEC	富士ゼロックス	三菱 電機	ランクエッジ	テストケース内容
OFF-T-1	○	○	○	○	○	○	○	○	有効である一般的な内包署名のES-Tを読み込める
OFF-T-2	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の期限切れを扱える
OFF-T-3	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の失効を扱える
OFF-T-4	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の認証パス検証を正しく行える
OFF-T-6	○	○	○	○	○	○	○	○	ES-TのSignerInfoの署名値の改竄を検知できる
OFF-T-7	○	○	○	○	○	○	○	○	ES-Tの署名タイムスタンプのトークンのSignerInfoの署名値改竄を検知できる
OFF-T-8	○	○	○	○	○	○	○	○	ES-TのMessageDigestのハッシュ値の改竄を検知できる
OFF-T-9	○	○	○	○	○	○	○	○	ES-Tの署名タイムスタンプのトークンのMessageDigestのハッシュ値改竄を検知できる
OFF-T-10	○	○	○	○	○	○	○	○	detached署名のES-Tを扱える
OFF-A-1	○	○	○	○	○	○	○	○	enveloping署名の第一世代のES-Aを扱える
OFF-A-2	○	○	○	○	○	○	○	○	detached署名の第一世代のES-Aを扱える
OFF-A-3	○	○	○	○	○	○	○	○	enveloping署名の第二世代のES-Aを扱える
OFF-A-4	○	○	○	○	○	○	○	○	detached署名の第二世代のES-Aを扱える

以上、署名生成・検証相互運用性テストと共通データ検証機能標準準拠性テストを集計した結果、参加者実装の合否判定結果は以下となった。

表 1.2.7 CAdES 総合合否判定結果

CAdESテスト総合合否判定結果 参加組織名(五十音順)	RSA セキュリティ		エントラストジャパン		サートラスト		スカイコム		セコム		帝国データバンク		NEC		日本電子公証機構		ハイパーギア		PFU		ビーバークテクノロジー		三菱電機		三菱電機インフォメーションシステムズ		リコー	
生成 / 検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証
CAdES-Tの基本機能の提供	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	–	○1
CAdES-Tのオプション機能の提供	–	–	○	○	○	○	○	○	○	○	○	○	○	○	○	○	–	–	○	○	○	○	○	○	○	○	–	–
CAdES-Aの基本機能の提供	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	–	○1
CAdES-Aのオプション機能の提供	–	–	○	○	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	○	–	–	–	–	–	–	–

表 1.2.8 XAdES 総合合否判定結果

XAdESテスト総合合否判定結果 参加組織名(五十音順)	エントラストジャパン		国際システムソリューションズ		大日本印刷		TOiNX		NEC		富士ゼロックス		三菱電機		ランダエッジ	
生成 / 検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証
XAdES-Tの基本機能の提供	○	○	○	○	-	○1	○	○	○	○	○	○	○	○	○	○
XAdES-Tのオプション機能の提供	○	○	○	○	-	-	○	○	○	○	-	-	○	○	○	○
XAdES-Aの基本機能の提供	○	○	○	○	-	○1	○	○	○	○	○	○	○	○	○	○
XAdES-Aのオプション機能の提供	○	○	○	○	-	-	○	○	○	○	-	-	○	○	-	-

凡例
○ 合格:生成/検証の結果に標準準拠性並びに相互運用性上の問題が無い
○1 合格:共通データ検証テストのみ実施した結果、検証機能に問題が無い
× 不合格:生成/検証の結果に標準準拠性もしくは相互運用性上の問題がある
－ 非サポート:実装が該当する生成/検証の機能を提供していない

基本機能に合格していれば、その実装は CAdES/XAdES 署名の生成または検証において JIS 原案の CAdES/XAdES プロファイルの要件を満たしていると言え、参加した全ての実装がテストに合格した。

個々のテスト項目に関する結果詳細や実装間でのテスト結果、参加者に提出を依頼した JIS プロファイルの供給者適合性宣言書の集計結果はウェブサイト[8]で公開予定の別紙で示す。

2.4 国際実験の状況

ECOM では、ウェブサイトから問い合わせのあった CAdES/XAdES の実装を有する海外企業 2 社と日本国内有志企業 7 社で実証実験を実施中である。テスト内容は署名生成・検証相互運用性テストのみとし、2007 年 11 月から 2 月末までの期間で行う。テスト結果については実験終了後、別紙としてウェブサイト[8]上で公開する予定である。

また、昨年度より ECOM では ETSI TC ESI にて CAdES/XAdES プラグテストを実施するよう働きかけを行なってきた。2007 年 1 月から 3 月にかけて準備として ETSI 側よりスペインのカタルーニャ工科大、オーストリアの A-SIT、日本電気、エントラストジャパンの 4 組織で XAdES に関する事前実験を行った。ECOM 側よりコストや時間などの面からテストは欧州に集まって行わずリモートでもできることを主張し、事前実験は電話会議、メールなどを活用しリモートで行われた。そしてようやく、2008 年 3 月 3 日から 7 日の期間 ETSI の主催で XAdES REMOTE Interoperability Plugtest[9]が実施される運びとなった。2 月 15 日現在、企業、大学、政府機関を含む欧州 25 組織、日本 1 組織が参加する予定である。ECOM からは、継続的に CAdES と XAdES のテストの両方の共催を呼びかけてきたが XAdES のみしか実現に至らなかったことは残念に思う。

2.5 考察と課題

本節では、実証実験により得られた知見、相互運用上の課題、テスト内容に関する課題について述べる。

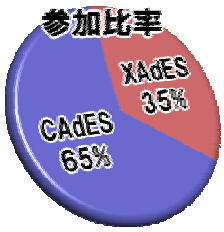
2.5.1 実験結果に見る日本国内の実装の傾向

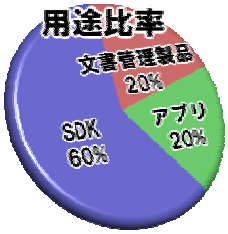
生成・検証相互運用テストでは、JIS 原案の要件に含まれるかどうかにかかわらず、実装がどのような機能を持っているのかを客観的に知ることができるよう配慮した。集計された結果により、日本国内における CAdES/XAdES の実装の傾向が伺える。

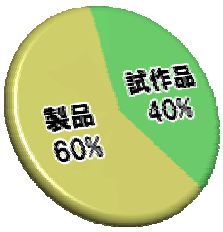
表 1.2.9 CAdES/XAdES 国内実装の傾向

参加した実装の内訳

国内実験に参加した実装の比率としては、CAdES がやや多く、開発ツールキットに基づく実装が多かった。また、製品としての参加が半数を超えている。

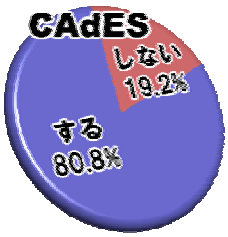


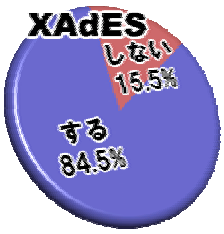




JIS の任意選択の要素をサポートするか

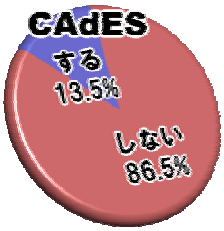
任意選択とは JIS 原案の標準のみでオプションとして利用することが可能な属性もしくはプロパティであり、JIS に準拠する生成者の実装が追加の規定抜きで使用することができる。これに対し、80%以上の実装が生成・検証をサポートしていることがわかった。

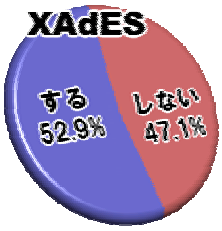




JIS の要別途規定の要素をサポートするか

要別途規定とは ETSI の標準では要素が規定されているものの、利用方法、検証方法に詳しい言及が無いため追加の規定なしには利用してはならない属性もしくはプロパティである。XAdES の 5 割に対し、CAdES では実装している比率が極端に少ない。CAdES では JIS に準拠するための最低限の実装を行うケースが多いようだ。

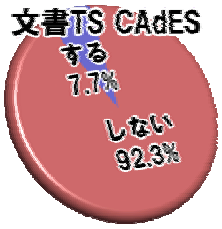


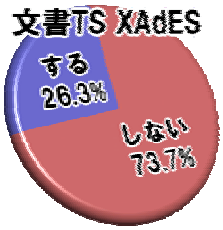


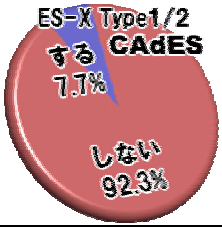
ASN.1 構造と XML との比較で、XAdES の方が要素の追加に柔軟に対応しやすいのかもしれない。

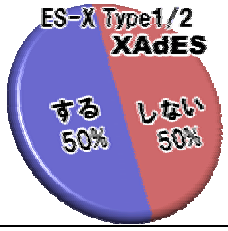
要別途規定のタイムスタンプをサポートするか

JIS で要別途規定となっている署名前に署名対象文書に対し直接付与する ContentTimeStamp, AllDataObjects TimeStamp などのタイムスタンプの属性およびプロパティのサポート率は予想通り、かなり低いものであった。また、署名や検証参照情報にタイムスタンプを付与する ES-X Type 1 および Type2 の CAdES-C TimeStamp や SigAndRefsTimeStamp 属性およびプロパティについては、CAdES では 1 社しかサポートしていないが、XAdES では半数の実装がサポートしていた。

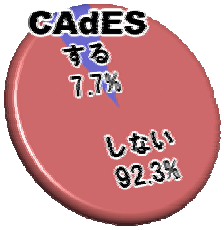


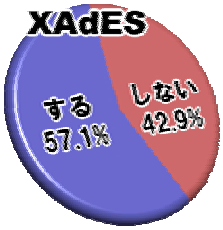






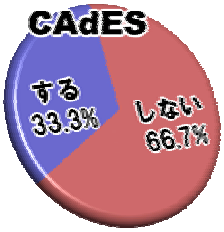
署名ポリシをサポートするか

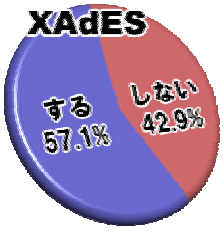




他の要別途規定の比率と同程度のサポート状況で、日本国内で署名ポリシを利用するには、ハードルが高いことが伺える。数値的には XAdES では使いやすいように勘違いされるかもしれないが、XML 署名ポリシは ETSI 技術標準ではなく技術報告に留まり、スキーマ定義の誤りがあるまま、改訂がされていないなど利用上の障壁はある。

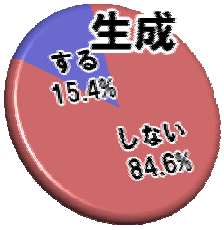
カウンタ署名をサポートするか

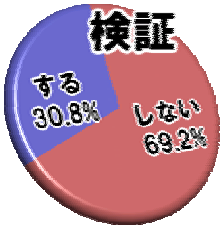




CAdES の場合、元の標準である CMS で提供する機能で、JIS では任意選択になっているものの対応する実装は 3 割に留まった。また、XAdES においては XML 署名が持つ任意の対象に対し明示的に署名できる機能により XAdES の CounterSignature プロパティを使用しなくてもカウンタ署名は実現できるが 6 割近くが実装している。

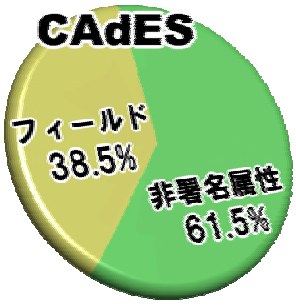
RFC 3126 CAdES ArchiveTimeStampV1 をサポートするか

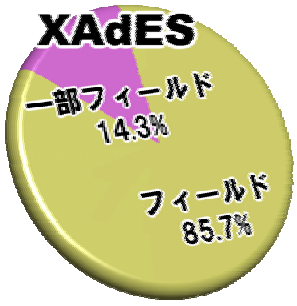




RFC 3126 が公開されて 7 年であるが、既に V1 形式を検証できる実装は 30%程度である。数 10 年といったスパンで電子文書を保存することを考えると、少なくとも検証についてだけでも過去のバージョンのフォーマットを検証する機能を提供し続けることは重要であり、将来の継続的なフォーマットサポートが危惧される。XAdES についても同様にバージョン間の非互換性の問題を抱えている。

どこに署名生成者は TSA 証明書検証情報を格納するか





特にアーカイブタイムスタンプを付与する場合、タイムスタンプの検証情報をどのように保管するかは重要な問題である。長期署名フォーマットでは署名データ単体で検証が可能な事から、タイムスタンプトークンに含めておいた方が管理しやすい。参加企業の実装はその 100%がトークンに格納する方法をサポートしており、CAdES ではトークンの CertificateValues など非署名属性に格納する方法、XAdES ではトークンの CMS 構造の certificates フィールドに格納する実装の方が多い。XAdES で署名者証明書検証情報の格納領域に TSA 証明書の検証情報を格納する実装もあった。一方、検証については、どこに格納されていても 100%の実装が正しく検証することができた。

2.5.2 CAdES/XAdES 実装の陥りやすい相互運用性上の誤り

今回 2007 年の実験は前回 2005 年の実験[5]に続いて二度目の実験であり 44%が前回も参加していたり、過去のテストデータをウェブサイト上で公開したりしているため、2007 年の実験では大きな相互運用性上の問題は起きなかった。細かな障害は発生したものの、多くの参加者が実験期間中に修正版を実装し問題解決している。

そこで本節では、実験期間中に起きた実装の誤りによる障害事例を述べる。実装上陥りやすい誤りを示すことにより、今後新規に参入する組織が長期署名フォーマットの実装をする際の参考に資すれば幸いである。

- CAdES で起きやすい誤り
  - アーカイブハッシュ対象が BER であることを想定していないためのハッシュ不一致
    アーカイブタイムスタンプのハッシュ対象である CMS SignedData の eContent、certificates、crls および SignerInfo 中の unsignedAttrs が ASN.1 DER でなく BER を利用可能であることを想定していないためにハッシュ値の不整合を起こしているケースがあった。BER は不定長の OCTET STRING 表現ができ、SET OF 構造をソートしないという特徴があるため、BER、DER の違いに注意する必要がある。
  - signedAttrs の要素がソートされていない
    RFC 3852 で規定されているように CMS SignedData では signedAttrs が ASN.1 DER でエンコードされるため、属性要素を格納する SET OF 構造はソートされなければならない。
  - CompleteRevocationRefs の要素の対応関係の誤り
    CompleteRevocationRefs の要素は CompleteCertificateRefs の要素と対応関係があるように格納しなければならないが、一つの要素の複数の CRL 参照情報を格納しているケースがあった。
  - CompleteCertificateRefs の OtherCertID の issuerSerial の不足
    OtherSigningCertificate 属性を定めた ASN.1 シンタックスの中で、OtherCertID の issuerSerial はオプションとなっているが、CompleteCertificateRefs の中で使用する場合には必須なので注意が必要である。
- XAdES で起きやすい誤り
  - XMLDSIG の Id 属性の重複、不足、入れてはならない場所での使用
    Id 属性は XML ドキュメント中で要素を一意に特定するためのものであり、既存の XML ドキュメントを追加や内包するような場合属性値が重複しないようにしなければならない。また、XAdES においてはスキーマの定義上、要素によって Id 属性が必須であったり、入れてはならない要素があったりするので注意しなければならない。
  - SignedProperties を参照する Reference の Type 属性の値の誤り
    この Type 属性の値は“http://uri.etsi.org/01903#SignedProperties”のように決まっているがそうでないケースがあった。
  - Reference に XPath が使われていると対応できない

これは誤りではないが、Reference に XPath もしくは XPointer の表現が使われていると対応できない実装がある。可能であれば Id により参照した方が相互運用性は高い。

- CAdES/XAdES に共通の起きやすい誤り
  - ◆ TimeStampToken がミリ秒以下の分解能を持つ場合正しくデコードできない
    日本国内の時刻認証事業者はミリ秒の精度でタイムスタンプを発行している事業者が多いが、ミリ秒以下の精度で発行する事業者もある。ミリ秒以下の GeneralizedTime を想定していないために、時刻の比較でエラーとなる実装があった。
  - ◆ 検証したい時刻よりも古い CRL、OCSP が格納されているケース
  - ◆ 検証情報、検証参照情報の不足
    署名生成時に検証に必要な証明書、CRL、およびこれらの参照情報が不足しているために検証に失敗するケースがあった。
  - ◆ TSA 証明書検証情報の格納方法の対応／非対応による検証失敗
    これは誤りではないが、タイムスタンプトークンの TSA 証明書を検証する際に、検証情報はファイルで提供されたりトークンに格納されたりしているが、検証側の実装が、ある格納方法に対応していないために検証に失敗するケースがある。
  - ◆ 失効情報の猶予期間
    失効情報を利用する際に猶予期間を厳密に見る実装と、そうでない実装があるので、注意が必要である。
  - ◆ SigningTime と TimeStamp 属性の順序関係の不整合
    CAdES および XAdES の仕様ではコンテントに対するタイムスタンプ、SigningTime および署名タイムスタンプの順序関係が規定されている。この順序に従わないデータを生成しているために検証エラーとなるケースがある。

2.5.3 タイムスタンプトークンに関する相互運用性上の課題

CAdES および XAdES は、タイムスタンプを用いた署名フォーマットであり、タイムスタンプ局より取得したタイムスタンプトークンを定められた位置に格納するといった処理を行う。今回の実証実験では、日本国内の認定制度による時刻認証認定事業者 3 社に協力を仰ぎ、テスト用に準備された、ほぼ実サービスと同じプロファイルのタイムスタンプ局を使用した。一部の実装において、以下の問題が発生した。

- 時刻監査証の格納場所に関する問題
  時刻認証局（TSA）の機器と時刻配信局（TA）の時刻差を監査した結果を X.509 V2 属性証明書の形式で発行する製品があり、国内の事業者でもタイムスタンプトークンにこの時刻監査証（TAC）を含める実装がある。TAC は V2 属性証明書であるが、タイムスタンプトークンの V1 属性証明書の格納領域に入れているため読み込みエラーになるなどの障害が起きるケースがあった。
- 時刻監査証の整数型フィールドにおける ASN.1 エンコーディングの問題
  ある事業者のタイムスタンプトークンには、TA より発行された ASN.1 INTEGER のエンコーディングに誤りのある TAC が含まれており、そのため読み込み時にエラーになる実装

があった。

- トークンの PKCS#1 署名値のパディングの問題
  実サービスと同じテスト用タイムスタンプ局で利用するタイムスタンプを発行する製品において、PKCS#1 署名に厳密に従っていないものがあり仕様に基づき厳密に検証した場合、タイムスタンプトークンの署名値が一致しないというケースがあった。PKCS#1 のパディング中のダイジェストアルゴリズムのパラメーターを含めるか、含めないかという問題であり、詳細は ECOM の昨年度の報告書（文献[12] 200p）でも述べている。Java などで提供される署名 API では、検証においては相互運用性もしくは後方互換性のためパラメーターの有無に関わらず検証成功としているようだ。ちなみにタイムスタンプサーバーの製品ベンダーからは 2006 年 9 月にこの問題に対する修正[13]が出ている。

署名の生成、延長、検証における相互運用性確保のためには、実装者側は処理の過程で、タイムスタンプトークンの ASN.1 エンコーディングを変更しないことが求められる。また、TA 並びに TSA においては標準に準拠しない箇所の修正が必要となる。TAC は属性証明書であるから一般には検証は不可欠である。その意味内容、提供手段、署名検証者による検証の必要性、検証する側の検証要件について明らかにすると共に長期保存の対象とすべきか、どのように保存する必要があるかについて議論の必要がある。

2.5.4 CAdES/XAdES における SigningTime の時刻比較

CAdES および XAdES においては SigningTime とタイムスタンプ要素との時刻の比較の検証要件（文献[1] C.3.6 および[2] G.2.2.16）が定められており、コンテンツに対するタイムスタンプ、SigningTime、署名タイムスタンプの順序でなければならないとしている。時刻が全て厳密に正確ならば論理的にこのような順序であることが保証されるが、SigningTime は署名を付与する機器のローカル時刻に基づく時刻であるため調時が正確でなかったりすると、往々にして時刻の順序関係が前述の検証要件を満たさないこととなる。

SigningTime は CMS 署名や S/MIME 署名メールにおいて一般的な属性であり、頻繁に使われるが、署名デバイスは必ずしもオンラインの環境で NTP 等により調時できるとは限らないため順序関係の要件を満足するのは非常に難しい。そこで、ETSI TC ESI 会議や IETF S/MIME ワーキングループの議論の場で、SigningTime の比較の要件を緩和することを ECOM より提言し、2008 年上旬には公開される RFC 3126 の後継となる CAdES の RFC では「前後関係は問わず、ある事前に取り決められた範囲内であることを確認する」というような表現に変更された。同様に、2008 年に改定される ETSI TS 101 733 v1.7.4 でも同様に反映される。XAdES においても同様の改定がなされるよう ECOM より提言を継続する。

2.5.5 CAdES/XAdES に関連するセキュリティ勧告

CAdES 署名に直接関連するセキュリティ勧告としては、現状把握している限りにおいて、OpenSSL や Microsoft CryptoAPI に関する脆弱性報告のみであり、報告から数年が経過していることから概ねの実装が対策を施していると思われる。

一方、XAdES においては、2007 年 6 月に XML 署名に関してセキュリティ勧告[14]があった。XML

署名では Reference 要素や KeyInfo の RetrievalMethod 要素の中に Transform 要素を含むことができ、この中では XML スタイルシートを記述することができる。過去の Apache Xalan に基づく XSLT の実装では、extension を有効にしていた場合スタイルシートの中で任意の Java クラスのメソッドを実行ができるようになっていたため、攻撃者がコマンド実行や DoS 攻撃を受ける可能性がある。署名検証よりも前にこれらの処理が行われることが多いため、送信者が不特定であったり、中間者が XML メッセージの改竄ができたりするような環境では確認が必要である。Microsoft 系の実装でも独自の拡張によりスクリプト（msxsl：script）を実行やコマンドが実行できる可能性があるので、調査ならびに確認が必要である。

2.5.6 将来に向けた標準仕様の改定案

実証実験を踏まえ、サービス側、実装側で対処するのではなく、CAdES、XAdES のみならず CMS、XMLDSIG などの標準仕様そのものを変更が望まれる箇所があった。これを今後の課題としてまとめる。

- ETSI TS 101 733 XAdES
  - ◆ 名前空間にバージョンが含まれている問題

    XAdES の規定する XML 要素は XML の名前空間を持っているが、これは“http://uri.etsi.org/01903/v1.3.2#”のようにバージョン番号を含んだ表現となっている。XAdES は 2～3 年毎に改定されているが、その度に名前空間が変っている。XAdES の実装では名前空間が変わると、基本的には実装を分ける必要があり、今回の実験参加した実装も、そのほとんどが最新版の v1.3.2 のみにしか対応しない実装がほとんどであり、前回実験のバージョンをサポートするものは無かった。この事は、XML 署名文書を長期保存する上で重大な問題である。10 年後、20 年後、過去のバージョンの XAdES を検証できない可能性が非常に高いのである。バージョンの差異によって生成、検証のアルゴリズムが変わる場合に名前空間を分けることは重要だが、XAdES のバージョンの違いで個々の要素の処理内容には変更が無いようなバージョン更新が多い。今後は、名前空間のバージョンを変更しないか、含めずに、要素の構造や処理内容に変更があった場合には、別の名前の要素として（例　SigningTime, SigningTimeV2）仕様追加し、将来的に後方互換性をある程度保証できるような仕様にしなければならないと考える。
  - ◆ タイムスタンプトークンの検証情報格納領域の追加

    タイムスタンプトークンを検証するのに必要な証明書や失効情報は長期署名フォーマットの中に含めてアーカイビングした方が、署名データ単体で検証できるため望ましい。しかしながら、CAdES/XAdES ではトークンの検証情報の格納の属性やプロパティを持たないため、現在では仕方なくトークンの CMS SignedData 構造の中に格納している。トークン自体が証拠情報であるため、意図しない改ざんを防止する意味でも本来なら手を加えずそのまま格納しておくことが望ましい。そのためにも、タイムスタンプトークンの検証情報を格納する領域に関する規定を追加することが望ましい。XAdES の実装者は、この問題がなければタイムスタンプ以外で CMS SignedData を細か

く扱う必要が無いので、特に XAdES においてトークン検証情報の格納用のプロパティの追加が強く求められる。

- ETSI TS 101 733 CAdES
  - ◆ ArchiveTimeStamp の計算方法に関する注釈の曖昧性

    CAdES の ArchiveTimeStamp のハッシュ対象となる非署名属性群の ASN.1 エンコーディングについて ETSI TS 101 733 v1.7.3 では以下のような記述がある。

> 6.4.1 Archive time-stamp attribute definition
> NOTE 5：Whilst it is recommended that unsigned attributes are DER encoded it cannot generally be so guaranteed except by prior arrangement.
> （訳）非署名属性は DER でエンコードされることが推奨されるが、事前の調整がある場合を除いて、一般にそのようには保証できない。
> -- 出典：ETSI TS 101 733 v1.7.3

    CAdES の元となっている CMS SignedData の仕様では、CMS 自体は DER ではなく BER エンコーディングであり、非署名属性群もまた属性要素がソートされない BER エンコーディングでよい。この注釈自体、仕様の不整合を生じてまで誰が DER を推奨しているのか明らかではないし、本来正しいはずの BER が、例外であるような印象を受ける。実験参加者の中にも非署名属性群が DER であることを想定した実装があり相互運用性に問題があった。eContent、certificates, crls など他のハッシュ対象も BER エンコーディングでよいことから、非署名属性群についてのみこのような制限を加えるのは適切でない。この注釈を修正し、非署名属性が BER であることを踏まえた実装を行う必要があることを明記する必要がある。
  - ◆ タイムスタンプトークンの検証情報の格納用属性の追加

    CAdES についても XAdES と同様にトークンの検証情報の格納用の属性が望まれる。
- IETF RFC 3852 CMS
  - ◆ OCSP 応答を格納するための OID の規定

    CMS SignedData の RevocationInfoChoices では、CRL やその他の任意の形式の失効情報を格納することができる。OCSP 応答を格納したい場合、その他の形式を利用するわけだが、現状 RFC では OCSP 応答の形式であるということを特定するためのオブジェクト識別子（OID）の規定が無い。例えば、タイムスタンプの検証情報が OCSP のみでしか提供されない場合に備え、早期にこの OID の規定を追加する必要がある。
- W3C XMLDSIG
  - ◆ 名前空間にバージョン（年月）が含まれている問題

    前述の名前空間による後方互換性の問題は、XAdES だけでなく、XML 署名（XMLDSIG）についても同じ問題である。XMLDSIG の現行バージョンは“http://www.w3.org/2000/09/xmldsig#”のような名前空間となっている。将来にわたって現行の XMLDSIG の名前空間に対応した実装が存在し続けられるか懸念される。何らかの対策、方針が必要であると考える。

以上の点は、ETSI TC ESI、IETF S/MIME WG、W3C を通じて今後、継続的に提言を続けていく必要がある。

2.5.7 CAdES/XAdES 実証実験内容に関する今後の課題

今回の実証実験を踏まえた残課題をまとめる。

- 共通データ検証機能標準準拠性テストのテストケースの充実
  テストデータの準備期間が十分でなかったことから 2005 年に実施したテストと比較してテスト項目数ベースで 25%程度減っている。また、CAdES と比較して XAdES の方が、よりテストケースが少ない。今回実施した生成・検証相互運用性テストで利用したツールを用いて相互運用性テストのテスト項目程度にテスト内容を充実させることが望まれる。OCSP に関するテストなども必要である。
- XAdES 共通データ検証機能標準準拠性テストのテストケース
  近年、SHA1 ハッシュアルゴリズムの危殆化が危惧されているが、XML 署名においては CMS と比較してアルゴリズムの移行が遅れており、対応する実装が少ないようである。一つにアルゴリズム URI の登録機関が明確でない点もあるかと思う。長期保存の観点から SHA2 を用いた署名のテストは急務であると考える。また、Enveloped 署名、署名ポリシなどのテストも必要となるだろう。
- 後方互換性を確認するテスト
  CAdES、XAdES の長期署名フォーマットの実装が現れてほんの数年であるが、CAdES では ArchiveTimeStamp V1 と V2 があったり、XAdES では仕様のバージョン毎に名前空間が異なるなど後方互換性の問題が懸念される。今回の実証実験では、現時点で最新の仕様のみに準拠し、過去の版をサポートしない実装が多かったようだ。少なくとも署名検証だけでも過去の版のテストケースを提供しておく必要がある。

2.6 謝辞

本実証実験を実施するにあたり快く無償でテスト用 TSA を提供して頂いたアマノタイムビジネス株式会社様、セイコープレシジョン株式会社様、株式会社 PFU 様、また、時刻監査証（TAC）に関し情報提供頂いたセイコーインスツル様に心より感謝の意を表します。

2.7 参考文献

[1] ETSI TS 101 733 V1.7.3 (2007-01) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), Jan 2007, ETSI

[2] ETSI TS 101 903 V1.3.2 (2006-03) XML Advanced Electronic Signatures (XAdES), Mar 2006, ETSI

[3] CMS 長期署名プロファイル、2005 年 8 月、次世代電子商取引推進協議会（ECOM）、http://www.ecom.jp/report/electronic_signatures/CMSformat.pdf

[4] XAdES 長期署名プロファイル、2005 年 8 月、次世代電子商取引推進協議会（ECOM）、http://www.ecom.jp/report/electronic_signatures/XAdESLong-TermSignatureFormatProf

ile_V0.6pub_.pdf
[5] 長期署名フォーマット相互運用性実験報告書、平成18年3月、電子商取引推進協議会　セキュリティワーキンググループ
[6] 暗号メッセージ構文を利用した電子署名（CAdES）の長期署名プロファイルに関する要求事項JIS原案、2006年12月、次世代電子商取引推進協議会（ECOM）、http://www.ecom.jp/report/JIS_CAdES_Profile.pdf
[7] 拡張可能なマーク付け言語を利用した電子署名（XAdES）の長期署名プロファイルに関する要求事項JIS原案、2006年12月、次世代電子商取引推進協議会（ECOM）、http://www.ecom.jp/report/JIS_XAdES_Profile.pdf
[8] ECOM CAdES/XAdES Plugtest 2007ウェブサイト、2007年10月、次世代電子商取引推進協議会（ECOM）、http://www.ecom.jp/LongTermStorage/interoptest2007.html
[9] Plugtest Portal for Electonic Signature 3 - 7 March 2008、2007年11月、ETSI、http://www.etsi.org/plugtests/XAdES/XAdES.htm
[10] 日本工業規格（JIS）JIS X 5092：2008　CMS利用電子署名（CAdES）の長期署名プロファイル、2008年、日本規格協会
[11] 日本工業規格（JIS）JIS X 5093：2008　XML署名利用電子署名（XAdES）の長期署名プロファイル、2008年、日本規格協会
[12] 電子文書長期保存ハンドブック、平成19年3月、電子商取引推進協議会　セキュリティワーキンググループ、http://www.ecom.jp/results/results18.html
[13] nCipher DSE 200 Release Notes、2006年9月、nCipher PLC、http://active.ncipher.com/documentation/nCDSE/win/user/dse_rnot.txt
[14] XML Digital Signature Command Injection, iSEC Partners Security Advisory - 12 Jul 2007、2007年6月、iSEC Partners、Inc.、http://www.isecpartners.com/advisories/2007-04-dsig.txt

3．長期署名方式の比較

3.1　目的

デジタル署名の有効性を長期間にわたって検証可能とする方式（長期署名方式）には、長期署名フォーマットを用いた方式以外にもいくつかの方式が提案されている。ここでは、その代表的な方式として、

(1) ArchiSig 方式

長期署名フォーマットにおける ES-X（署名データに署名タイムスタンプ及び検証情報を付与したデータ）をハッシュツリーによってリンクし、ツリーの頂点にのみアーカイブタイムスタンプを付与する方式。

(2) ヒステリシス署名による方式

（方式 1）署名者の署名としてヒステリシス署名を利用する方式。

（方式 2）ES-X に保存用サーバのヒステリシス署名を付与する方式。

(3) SecureSeal による方式

長期署名フォーマットのタイムスタンプとして SecureSeal のタイムスタンプを利用する方式。（標準の長期署名フォーマットでは、RFC3161 準拠のタイムスタンプを利用する。）

の 4 方式を取り上げ、長期署名フォーマットによる方式と比較する。

なお、『デジタル署名の有効性を長期間にわたって検証可能とする』とは、デジタル署名が作成された時点において、それが有効であったことを確認可能とすることであり、その要件は図 1.3.1 の通りである（詳細は「電子署名文書長期保存に関するガイドライン（2002/3)」等を参照のこと)。

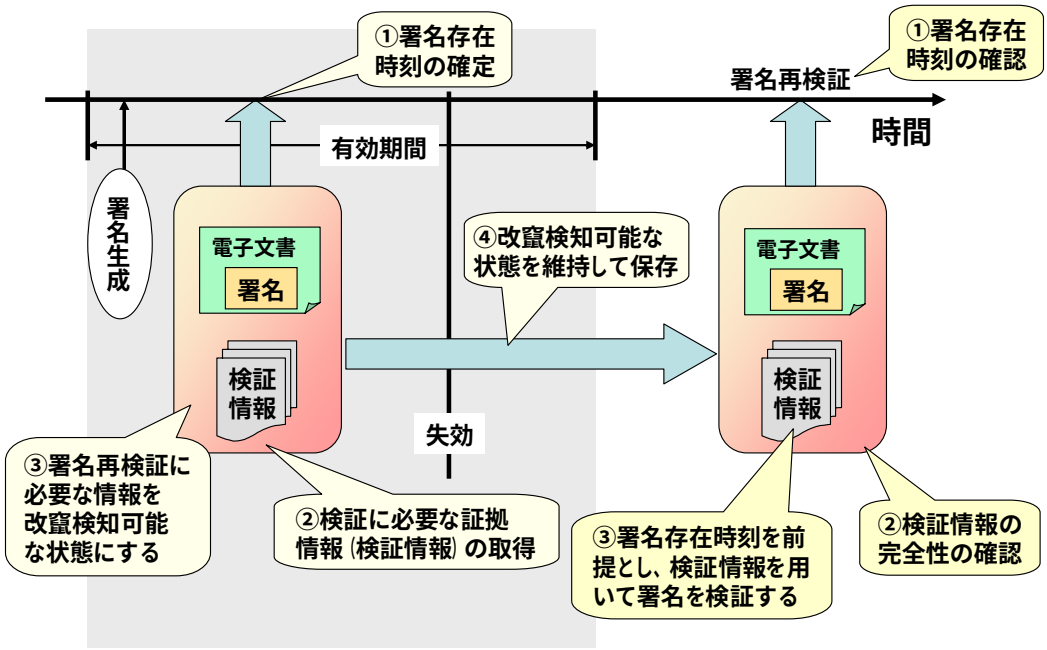


図 1.3.1 長期署名の要件

各方式の対応状況は次の通りである。

① 署名存在時刻の確定。

長期署名による方式、ArchiSig 方式、ヒステリシス署名による方式 2、SecureSeal による方式ともに、署名値に対してタイムスタンプを付与することにより、署名存在時刻を担保している。ヒステリシス署名による方式 1 では、署名記録を刊行物に掲載することにより公開するか、タイムスタンプを付与することにより、署名存在時刻を担保している。

② 検証に必要な証拠情報の取得。

長期署名による方式、ArchiSig 方式、ヒステリシス署名による方式 2、SecureSeal による方式ともに、トラストアンカまでの証明書及びそれらの失効情報を署名データに関連付けて保持している。ヒステリシス署名による方式 1 では、署名データに関連付けるための既定の手段は提示されていない。

③ 署名再検証に必要な情報を改ざん検知可能な状態にする。

長期署名による方式、ArchiSig 方式、SecureSeal による方式では、アーカイブタイムスタンプにより、署名文書や検証情報等の全体を改ざん検知可能な状態にしている。ヒステリシス署名による方式 2 では、サーバのヒステリシス署名を付与することにより、当該情報を改ざん検知可能な状態にしている。ヒステリシス署名による方式 1 では、全体に対して統一した手段により改ざん検知可能とはしておらず、(証明書や失効情報に付与された認証局の署名など) 個別の手段に依存している。

④ 改ざん検知可能な状態を維持して保存する。

長期署名による方式、SecureSeal による方式では、アーカイブタイムスタンプを重ねて取得することにより、改ざん検知可能な状態を維持している。ArchiSig 方式では、アーカイブタイムスタンプの更新とハッシュツリーの更新により、同様の効果を得ている。ヒステリシス署名による方式 1、2 では、既定の手段は提示されていない。

3.2 各方式の概要

本節では、長期署名フォーマットによる長期署名方式を含め、5 つの方式の概要をまとめる。

(1) 長期署名フォーマットによる方式

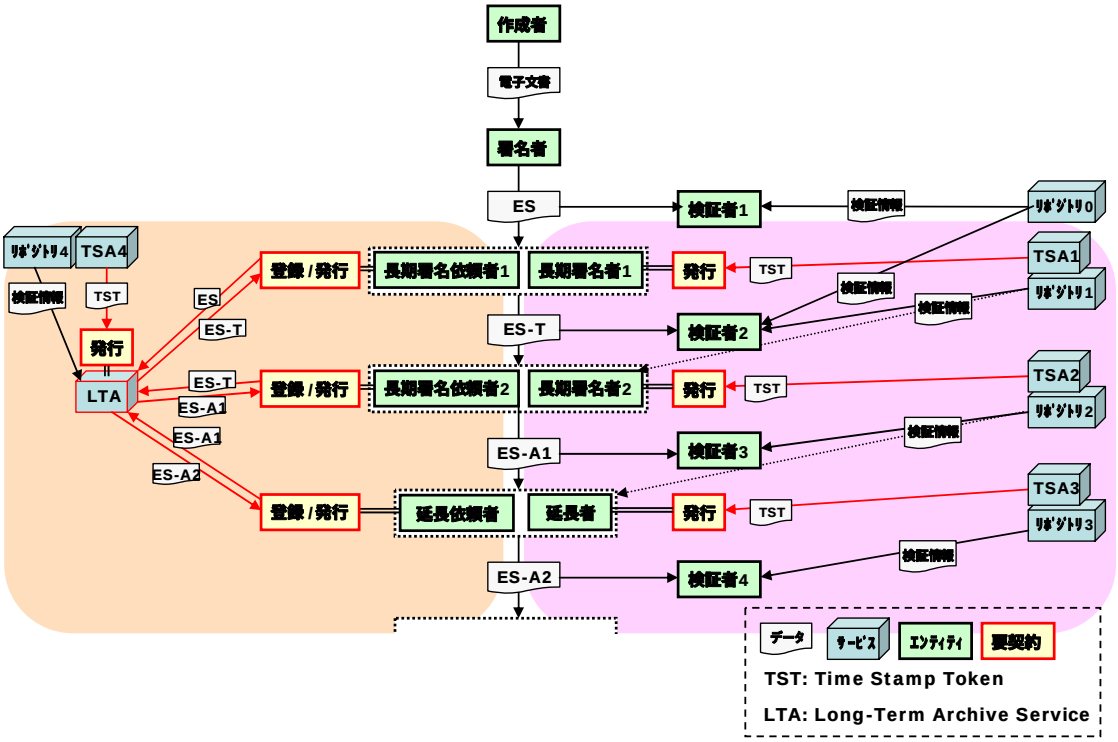


図 1.3.2 長期署名フォーマットによる方式

図 1.3.2 は、長期署名フォーマットによる長期署名方式における生成と検証の様子を示したものである。延長処理を長期保存サービス（LTA）に依頼する場合と、自ら実施する場合とでそれぞれ左右に分けて示している。

作成者が作成した電子文書に対して、署名者が署名を生成・付与し、ES を作成する。検証者 1 が ES を検証するときには、署名者証明書を発行した認証局のリポジトリ 0 から検証情報（認証パス及び失効情報）を取得する。

ES-T を得るには、長期署名者 1 が TSA1 より署名タイムスタンプを取得して自ら ES-T 形式のデータを構築するか、長期署名依頼者 1 が LTA に ES を登録し、ES-T 形式のデータの構築を依頼する。この際、長期署名者 1 は TSA1 と、長期署名依頼者 1 は LTA との契約が必要である。検証者 2 が ES-T を検証するときには、署名者証明書を発行した認証局のリポジトリ 0 及び TSA1 あるいは TSA1 に証明書を発行した認証局のリポジトリ 1 から、それぞれ署名者証明書に関する認証パスと検証情報、及びタイムスタンプの証明書に関する認証パスと検証情報を取得し、自ら検証処理を行う。なお、LTA から ES-T を取得するために通常は LTA との契約を要する。

ES-A1 を得るには、長期署名者 2 が TSA2 よりアーカイブタイムスタンプを、リポジトリ 0 から署名者証明書の認証パス及び失効情報を取得して自ら ES-A 形式のデータを構築するか、LTA に長期署名依頼者 1 が ES を、長期署名依頼者 2 が ES-T を登録して ES-A 形式のデータの構築を依頼する。検証者 3 が ES-A を検証するときには、TSA2 あるいは TSA2 に証明書を発行した認証局のリポジトリ 2 からアーカイブタイムスタンプの証明書に関する認証パスと検証情報を取得し、自ら検証処理を行う。延長者及び延長依頼者が ES-A2 を得る手順、検証者 4 が ES-A2 を検証する手順は

ES-A1 の場合とほぼ同様である。

上記において、各エンティティは同一であっても異なっても構わない。自ら延長したデータを中途から LTA に委託することも可能であるし、LTA に委託して得たデータを中途から自らで延長することも可能である。長期署名者及び延長者は TSA との契約を要する。長期署名依頼者及び延長依頼者は LTA との契約を要する。検証者なんら契約を伴わずに自ら検証を実施することができる。

(2) ArchiSig 方式

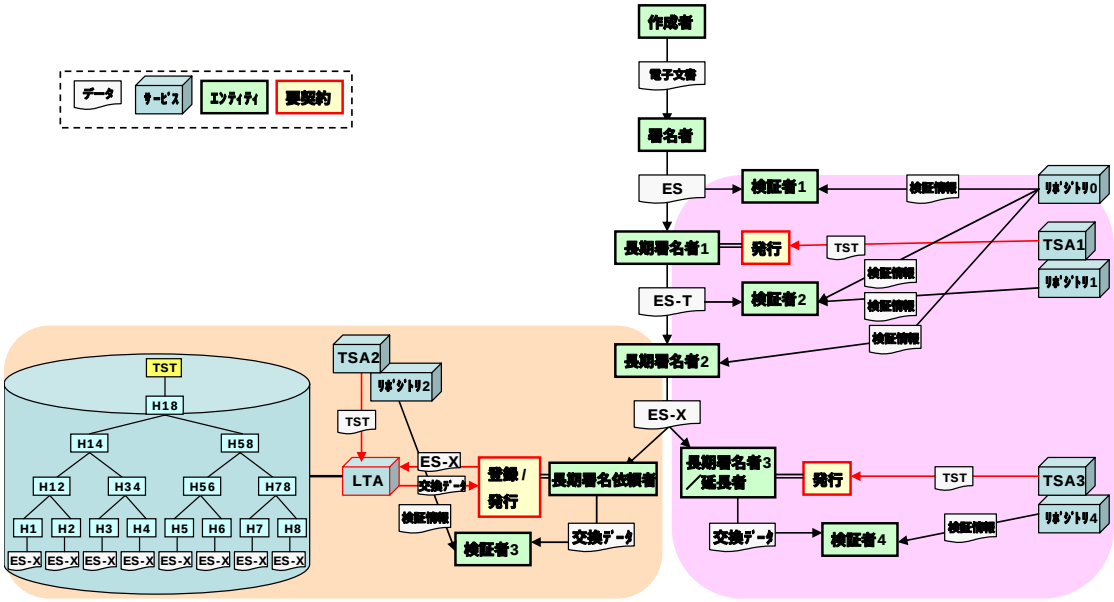


図 1.3.3 ArchiSig 方式

図 1.3.3 は、ArchiSig 方式における生成と検証の様子を示したものである。延長処理を LTA に依頼する場合と、自ら実施する場合とでそれぞれ左右に分けて示している。

ES-T の生成及び検証は長期署名フォーマットによる方式と同様である。ただし図では ES-T の生成に LTA を利用するケースを省略してある。

ES-X を生成するためには、長期署名者 2 が署名者の公開鍵証明書を発行した認証局のリポジトリ 0 より検証情報を取得し、ES-X 形式のデータを構築する。

LTA に長期署名生成を依頼する場合、長期署名依頼者が ES-X あるいはそのハッシュ値を LTA に登録する。LTA では、登録されたデータからハッシュツリーを構築する。アーカイブタイムスタンプの更新等の延長処理も LTA が実施する。

長期署名の生成処理や延長処理を自ら実施する場合、対象となる ES-X のデータを含むハッシュツリーを構築し、その頂点のハッシュ値に対するタイムスタンプを取得する（ここまでが長期署名の生成処理)。このタイムスタンプが有効期間を終える前に、タイムスタンプに対して新たな

タイムスタンプを取得する（延長処理）。ハッシュツリーのハッシュが脆弱化しない限り、この方法で延長処理を継続できる。ハッシュの脆弱化に対しては、脆弱化前にハッシュツリーの更新（登録データごとに、データ本体、ハッシュツリーのハッシュの一部、アーカイブタイムスタンプ等に対して新たなアーカイブタイムスタンプを生成）を実施する。

長期署名依頼者がLTAより得た交換形式のデータあるいは長期署名者3あるいは延長者から得た交換形式のデータ（登録データ本体、ハッシュツリーの一部のハッシュ値、アーカイブタイムスタンプ等を含むデータ）を検証するときには、前者に対してはリポジトリ2から、後者に対してはリポジトリ3から検証情報を取得して、自ら実施する。

上記において、各エンティティは同一であっても異なっても構わない。ただし、ハッシュツリーを同一のエンティティが保持し続ける必要がある。延長者はTSAと、長期署名依頼者はLTAとの契約を要する。検証者なんら契約を伴わずに自ら検証を実施することができる。

(3) ヒステリシス署名による方式

（方式1）署名者の署名としてヒステリシス署名を利用する方式

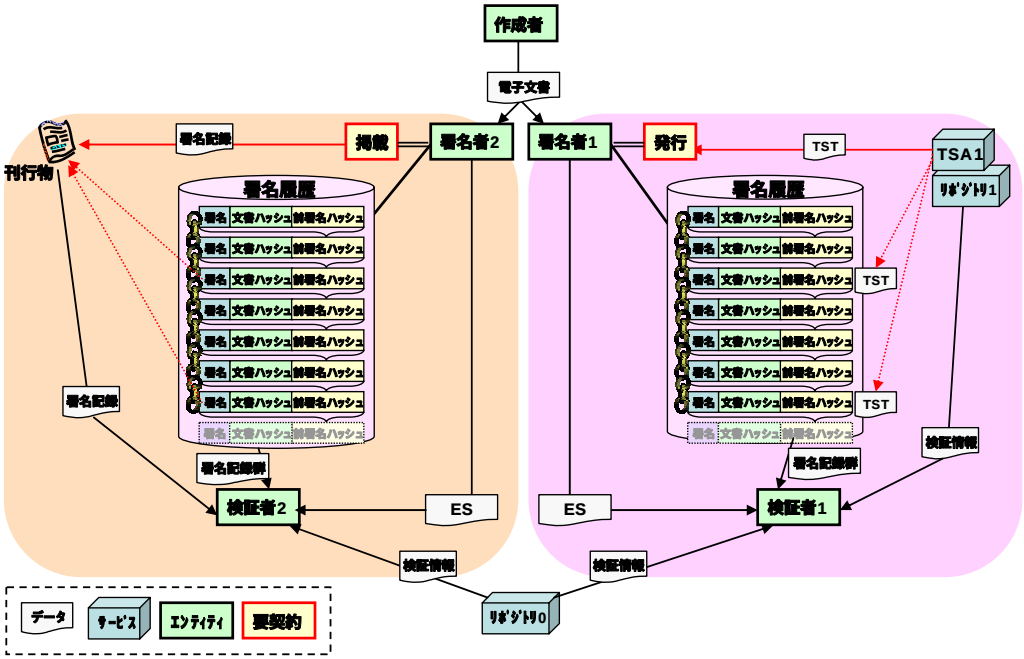


図 1.3.4 ヒステリシス署名による方式1

図 1.3.4 は署名者の署名としてヒステリシス署名を利用する方式における生成と検証の様子を示したものである。署名記録を刊行物に掲載して公開する場合と、署名記録に対するタイムスタンプを取得する場合とで、それぞれ左右に分けて示している。

作成者が作成した電子文書に対して、署名者 1、2 がヒステリシス署名生成の方法に従って署名を生成・付与し、ESを作成する。ヒステリシス署名に用いるハッシュが危殆化しない限り、ES

の有効性は確認可能となる。

検証者 1、2 が署名者の公開鍵証明書の有効期間内に ES を検証するときには、署名者証明書を発行した認証局のリポジトリ 0 から検証情報を取得し、通常の署名検証の方法に従って検証する。

署名者の公開鍵証明書の有効期限を過ぎて ES を検証するときには、検証者 1 の場合、ES に相当する署名記録とそれ以降に作られた署名記録を TST が添付された署名記録まで集めた署名記録群、TST、TST の検証情報、署名者証明書の検証情報を取得する。検証者 2 の場合、ES に相当する署名記録とそれ以降に作られた署名記録を刊行物に掲載された署名記録まで集めた署名記録群、その署名記録が掲載された刊行物、署名者証明書の検証情報を取得し、自ら検証する。

上記において、各エンティティは同一であっても異なっても構わない。ただし、署名履歴を検証者に開示する必要がある。また、有効期限後には署名者証明書の検証情報がリポジトリ 0 から削除される場合があるので、何らかの形で事前に取得して安全に保存しておく必要がある。延長者は、TSA あるいは刊行物の出版社との契約を要し、刊行物に掲載する方法を採用した場合、検証者はその刊行物を入手する必要がある。

（方式 2）ES-X にサーバのヒステリシス署名を付与する方式

図 1.3.5 は ES-X にサーバのヒステリシス署名を付与する方式における生成と検証の様子を示したものである。長期署名生成処理を自ら実施する場合と、LTA に委託する場合とで、それぞれ左右に分けて示している。なお、署名記録を刊行物に公開する方法については省略してある。

ES-X を生成するまでの方法は ArchiSig 方式の場合と同等である。

LTA に長期署名生成処理を依頼する場合、長期署名依頼者が ES-X あるいはそのハッシュ値を LTA に登録する。LTA では、登録されたデータに対して LTA のヒステリシス署名を生成する。

長期署名生成処理を自ら実施する場合、長期署名者が対象となる ES-X に対して長期署名者自身あるいはサーバのヒステリシス署名を生成する。また適当な間隔で、署名履歴中の署名記録に対するタイムスタンプを取得し、署名記録とともに保存する。ヒステリシス署名が有効期間を終えるまで ES-X を取り込むことができ、ヒステリシス署名のハッシュが危殆化しない限り、署名者の署名の有効性を検証可能にできる。

検証者 3、4 が ES の有効性を検証する場合、ES-X に加え、ES-X に対応する署名記録からそれ以降に作られた署名記録を、TST が添付された署名記録まで集めた署名記録群、TST、TST の検証情報（図中ではこれらをまとめて HSVD と表している）を取得し、自ら検証する。署名記録を刊行物に公開する方法を採用した場合、ES に相当する署名記録とそれ以降に作られた署名記録を刊行物に掲載された署名記録まで集めた署名記録群、その署名記録が掲載された刊行物を取得し、自ら検証する。

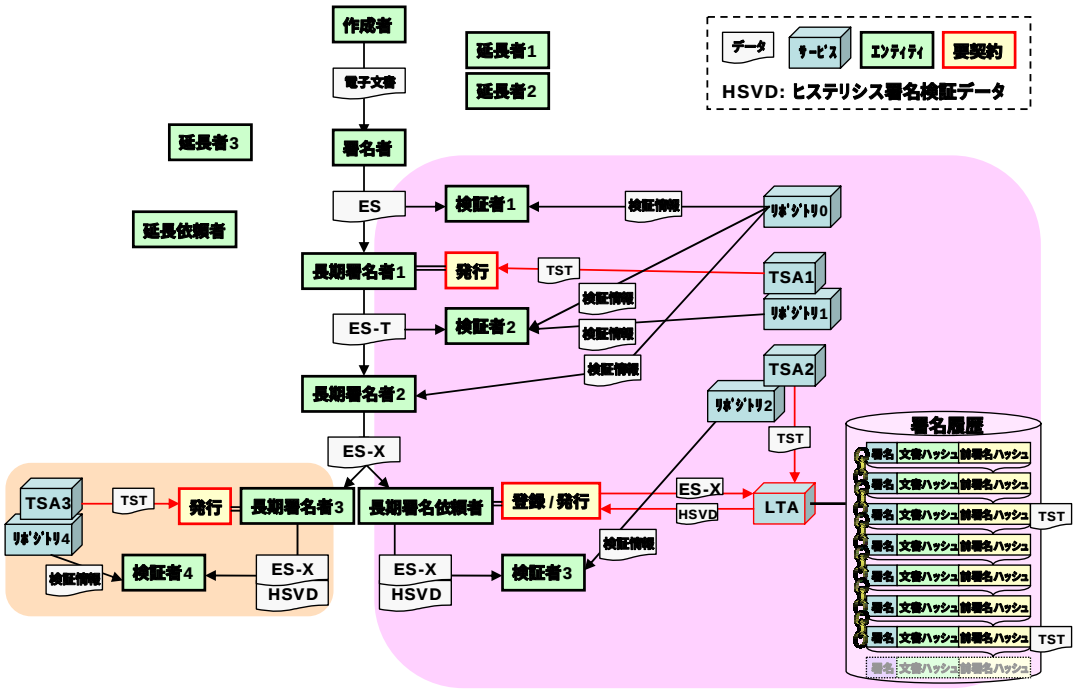


図 1.3.5 ヒステリシス署名による方式 2

上記において、各エンティティは同一であっても異なっても構わない。長期署名者は、TSA あるいは刊行物の出版社との契約を要し、刊行物に掲載する方法を採用した場合、検証者はその刊行物を入手する必要がある。

(4) SecureSeal による方式

図 1.3.6 は、長期署名フォーマットのタイムスタンプとして SecureSeal を用いた長期署名方式における生成と検証の様子を示したものである。長期署名の生成及び延長処理を依頼する場合と、自ら実施する場合とでそれぞれ左右に分けて示している。

ES-T、ES-A1、ES-A2 の生成方法は、TST の形式が異なるだけで、長期署名フォーマットによる方式とほぼ同等である。ただし、ES-T、ES-A1、ES-A2 の検証において、TST の検証を自ら実施することはできず（TST に否認防止措置が施されておらず、かつ検証者が刊行物に掲載されている情報と TST との関連を確認できないため）、TSA に依頼し、検証結果を取得する必要がある。

上記において、各エンティティは同一であっても異なっても構わないが、検証者は TSA との契約者である必要があるため、通常は長期署名者あるいは延長者と同一となる。

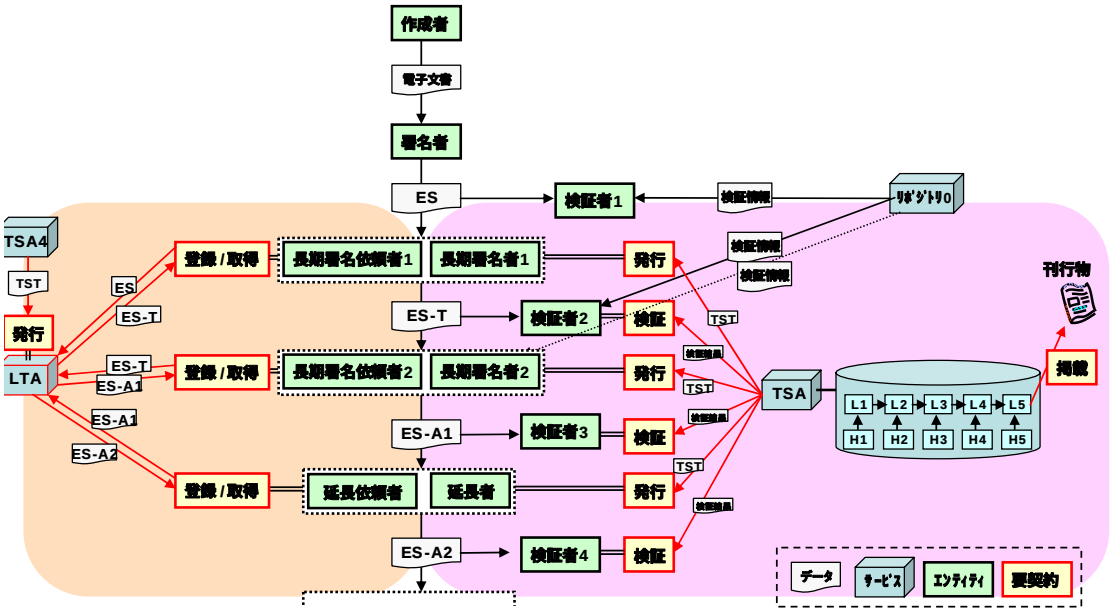


図 1.3.6 SecureSeal による方式

3.3 各方式の比較

項目ごとに各方式を比較した結果を次表に示す。

	長期署名フォーマット	ArchiSig	ヒステリシス署名(方式 1)	ヒステリシス署名(方式 2)	SecureSeal
長期署名方式概要	長期署名フォーマットにおいて署名タイムスタンプ及びアーカイブタイムスタンプに RFC3161 のタイムスタンプトークンを利用する。	ES-X のハッシュ値をツリー状にハッシュ計算を重ねることによってリンクし、頂点のハッシュ値に対してアーカイブタイムスタンプを重ねる。	署名者の署名としてヒステリシス署名を利用する。定期的に一部の署名記録につき、公開／タイムスタンプ取得する。	ES-X あるいはそのハッシュ値に対して、サーバのヒステリシス署名を生成する。定期的にヒステリシス署名の一部の署名記録につき、公開／タイムスタンプ取得する。	長期署名フォーマットにおいて署名タイムスタンプ及びアーカイブタイムスタンプに「SecureSeal のタイムスタンプトークン」を利用する。
署名者	不特定	不特定	ヒステリシス署名利用者	不特定	不特定
署名生成の手数	通常の署名生成と同様	通常の署名生成と同様	ヒステリシス署名生成 (署名履歴生成)	通常の署名生成と同様	通常の署名生成と同様
長期署名者	TSA 利用者 署名者と別人でも可	TSA 利用者 署名者と別人でも可	ヒステリシス署名利用者 刊行物掲載契約者／TSA 利用者 署名者自身	ヒステリシス署名利用者 刊行物掲載契約者／TSA 利用者 署名者と別人でも可	SecureSeal 利用者 署名者と別人でも可

	長期署名フォーマット	ArchiSig	ヒステリシス署名(方式 1)	ヒステリシス署名(方式 2)	SecureSeal
長期署名生成の手数	署名タイムスタンプの取得、ES-T の生成、検証情報の取得、ES-X の生成、アーカイブタイムスタンプの取得、ES-A の生成 ※処理時間は、署名数に比例。例えば、10,000 署名／日であれば、20,000 個のタイムスタンプ取得が必要。	署名タイムスタンプの取得、ES-T の生成、検証情報の取得、ES-X の生成、ハッシュツリーの構築、アーカイブタイムスタンプの取得、ArchiSig ES-A の生成、検証者への交換形式データの提供 ※処理時間は頂点のハッシュの数に比例。例えば、10,000 署名／日で、一日分を 1 つのハッシュツリーとした場合、1 日 10,000 個の署名タイムスタンプと 1 個アーカイブタイムスタンプの取得で良い。	署名履歴の生成、検証者への署名履歴の提供、署名記録の刊行物への掲載／署名記録に対するタイムスタンプの取得 ※一部の署名記録に対して実施。処理時間は署名数に関係なく一定。例えば、10,000 署名 / 日で、毎日公開であれば、10,000 署名に 1 個の公開手続で良い。	署名タイムスタンプの取得、ES-T の生成、検証情報の取得、ES-X 生成、署名履歴の生成、署名履歴の検証者への提供、署名記録の刊行物への掲載／署名記録に対するタイムスタンプの取得 ※署名記録公開は、一部の署名記録に対して実施。処理時間は、署名数に関係なく一定。例えば、10,000 署名 / 日で、毎日公開であれば、10,000 個に 1 個の公開手続で良い。	署名タイムスタンプとして SecureSeal タイムスタンプの取得、ES-T の生成、検証情報の取得、ES-X 生成、アーカイブタイムスタンプとして SecureSeal タイムスタンプの取得、ES-A の生成 ※処理時間は、署名数に比例。例えば、10,000 署名／日であれば、20,000 個のタイムスタンプ取得が必要。
長期署名検証者	不特定	交換形式のデータの入手に制限がなければ不特定	署名履歴が公開されていれば不特定 そうでなければ署名者自身	署名履歴が公開されていれば不特定 そうでなければ署名者自身	SecureSeal 利用者 署名者と別人でも可
長期署名検証の手数	ES-X の検証、アーカイブタイムスタンプの検証	交換形式のデータの取得、ES-X の検証、頂点に至るハッシュリンク（reduced hash tree）の検証、アーカイブタイムスタンプの検証	署名の検証、公開された／タイムスタンプを付与された署名記録に至るハッシュリンクの検証、公開された／タイムスタンプの付与された署名記録の照合／検証	ES-X の検証、サーバ署名の検証、公開された／タイムスタンプを付与された署名記録に至るハッシュリンクの検証、公開された／タイムスタンプの付与された署名記録の照合／検証	ES-X の検証、アーカイブタイムスタンプの検証依頼 ※署名タイムスタンプとアーカイブタイムスタンプに用いられる「SecureSeal のタイムスタンプトークン」の検証は TSA に依頼し、発行された検証結果を確認する
延長時期	アーカイブタイムスタンプの有効期限に至る前	①アーカイブタイムスタンプの有効期限に至る前 ②ハッシュが脆弱化する前	なし		アーカイブタイムスタンプの有効期限に至る前

	長期署名フォーマット	ArchiSig	ヒステリシス署名(方式 1)	ヒステリシス署名(方式 2)	SecureSeal
延長者	不特定	ArchiSig 運用者	なし		SecureSeal 利用者 署名者、長期署名生成者と別人でも可
延長の手数	ES-A の主要な情報に対する新たなタイムスタンプの取得	①タイムスタンプの更新(アーカイブタイムスタンプに対する新たなタイムスタンプの取得) ②ハッシュツリーの更新(すべてのデータオブジェクトに対する交換形式のデータをノードとした新たなハッシュツリーの構築と頂点のハッシュ値に対するアーカイブタイムスタンプの取得)	なし		ES-A の主要な情報に対する新たな SecureSeal タイムスタンプの取得
トラストアンカ	署名者の証明書のルート証明書、タイムスタンプの証明書のルート証明書	署名者の証明書のルート証明書、タイムスタンプの証明書のルート証明書	署名者の証明書のルート証明書、公開された署名記録／タイムスタンプの証明書のルート証明書		署名者の証明書のルート証明書、公開されたリンク情報の代表値
証拠として提出すべきデータ	・ES-A (署名対象データを含む)	・ES-X (署名対象データを含む) ・ reduced hash tree+関連するすべてのアーカイブタイムスタンプ	・署名対象データ ・ヒステリシス署名データ ・署名履歴 ・公開された署名記録／タイムスタンプ	・ES-X (署名対象データを含む) ・ヒステリシス署名データ ・署名履歴 ・公開された署名記録／タイムスタンプ	・ES-A (署名対象データを含む) ・公開されたリンク情報の代表値 ・公開されたリンク情報と ES-A に含まれる SecureSeal タイムスタンプ間のリンク情報
可搬性	ES 、 ES-T 、 ES-C 、 ES-X 、 ES-A 形式で交換可能 受取ったデータを継続して延長処理可能	ES-X 、 reduced hash tree, 関連するすべてのアーカイブタイムスタンプをパッケージ化して交換可能 受取ったデータを新たなデータオブジェクトとして延長処理可能	(・有効期間内であれば、ES、または、ES-T 形式で交換可能) (・有効期限切れの場合の) 交換形式は未定義		ES 、 ES-T 、 ES-C 、 ES-X 、 ES-A 形式で交換可能 ただし、検証には TSA との契約が必要 受取ったデータを継続して延長処理可能

	長期署名フォーマット	ArchiSig	ヒステリシス署名(方式 1)	ヒステリシス署名(方式 2)	SecureSeal
特定システムへの依存度	長期署名の生成、検証、延長ともシステム非依存	長期署名の検証はシステム非依存。生成、延長はハッシュツリーを管理するシステムに依存。	長期署名の生成、検証ともシステムに依存。(有効期間内であれば、検証はシステム非依存。)		長期署名の生成、検証、延長とも TSA に依存。
公開鍵暗号アルゴリズム脆弱化のインパクト	既定の延長処理として、脆弱化前に新たなタイムスタンプを取得する必要あり。	既定の延長処理として、脆弱化前にタイムスタンプを更新(新たなタイムスタンプを取得)する必要あり。	タイムスタンプを用いる場合、脆弱化前に対処を要する。		なし
ハッシュアルゴリズム脆弱化のインパクト	既定の延長処理として、脆弱化前に新たなタイムスタンプを取得する必要あり。	既定の延長処理として、脆弱化前にハッシュツリーを更新(ハッシュツリーを新たな安全なハッシュ関数で再構築)する必要あり。	脆弱化前に対処を要する。		・アーカイブタイムスタンプのハッシュの脆弱化に対しては、既定の延長処理として、脆弱化前に新たなアーカイブタイムスタンプを取得する。 ・TSA のハッシュリンクのハッシュの脆弱化に対しては、脆弱化前に対処を要する。
廃業のインパクト	TSA の廃業:検証に影響なし。他の TSA に移行可能。 LTA の廃業:最新の ES-A を入手し、他の LTA に登録可能。	TSA の廃業:検証に影響なし。他の TSA に移行可能。 LTA の廃業:交換形式のデータを入手し、他の LTA に登録可能。ただし、個々のデータサイズは増大。	TSA の廃業:検証に影響なし。他の TSA に移行可能。 LTA の廃業:交換形式が未定義であり、他の LTA への移行は比較的困難。		TSA の廃業:検証サービスが提供されなくなるため、ユーザに検証手段が提供される必要あり。例えば、検証に必要な情報(リンク情報)が開示など。他の TSA に移行可能。 LTA の廃業:最新の ES-A を入手し、他の LTA に移行可能。
コスト要因	タイムスタンプ取得	タイムスタンプ取得	署名記録公開／タイムスタンプ取得		・タイムスタンプ取得 ・タイムスタンプ検証

	長期署名フォーマット	ArchiSig	ヒステリシス署名(方式 1)	ヒステリシス署名(方式 2)	SecureSeal
契約先	署名者:署名者証明書発行 CA 検証者:なし 長期署名生成者、延長者:TSA 長期署名依頼者、延長依頼者:LTA	署名者:署名者証明書発行 CA 検証者:なし 長期署名生成者、延長者:TSA 長期署名依頼者、延長依頼者:LTA	署名者:署名者証明書発行 CA 検証者:署名履歴が公開されていれば契約不要。公開されていない場合、署名者から署名履歴を入手する必要有。 長期署名生成者:公開先の出版社等／TSA 長期署名生成依頼者:LTA		署名者:署名者証明書発行 CA 検証者:TSA(SecureSeal) 長期署名生成者、延長者:TSA(SecureSeal) 長期署名依頼者、延長依頼者:LTA
主な用途	・利用者や組織を限定しない雑多な種類の文書の保存 ・個人や組織間で交換される文書の保存	・利用者や組織を限定しない雑多な種類の文書の保存 ・頻繁に交換の生じない文書の保存 ・暗号化を要する文書の保存	・署名者自身による文書の保存	・組織内で管理する文書の保存	・特定の利用者や組織向けのサービスに伴う文書の保存
主な特徴	・検証は標準的 PKI 技術のみで可能。 ・長期署名の生成や再延長の実施者に制約がなく、可搬性が大きい。 ・署名毎にアーカイブタイムスタンプを要するため、タイムスタンプのコストが比較的大きくなる。	・アーカイブタイムスタンプのコストは、ハッシュツリーでまとめるデータオブジェクトの数を増やすことにより、低減することができる。 ・ハッシュの脆弱化が見込まれるときの対応コストは大きくなる。 ・交換するときのデータサイズは比較的大きくなる。	・タイムスタンプのコストが抑えられる。 ・検証者に署名履歴を提示する必要がある。 ・ハッシュ脆弱化への対処手段が未定義。		・タイムスタンプの有効期間が比較的長いため、再タイムスタンプのコストを抑えられる。 ・検証を自ら実施することができず、検証を依頼できるのは TSA との契約者に限られる。
標準化動向	・ETSI、IETF、JIS などの標準化が最も進んでいる。	・IETF の LTANS のワーキンググループで標準化作業中。	ー		・SecureSeal タイムスタンプは ISO/IEC 18014-2 に準拠している。長期署名方式としての標準化作業はない。

3.4 比較項目の解説

本節では、3.3 に示した比較項目表を解釈する上で、特に注意を要するものについて解説を加える。

(1) 長期署名と延長について

長期署名の生成は、検証情報を含む署名文書を改ざん検知可能な状態にするまでとし、延長

処理は、その処置の脆弱化に対処する処置を呼ぶこととする。ただし、延長処理の結果生成されたデータの検証のことも本表では長期署名の検証としている。

(2) トラストアンカ

PKI で定義される「電子署名の検証を行う際の検証者によって信頼された信用の起点となるCA の証明書」のみでなく、署名やタイムスタンプの有効性を確認するうえで信頼すべきその他のデータ。検証者に対して否認できない手段でかつ誤認のないように提示されることが前提。

(3) 証拠として提出すべきデータ

署名の有効性を判断するために、長期署名とトラストアンカとの関係の安全性を形式的な手段で確認するために必要な全データ。

(4) 可搬性

長期署名の生成、延長、検証等の各処理において、他のエンティティに対して個々の署名データあるいは長期署名データを移行や交換できるかどうかについて。

(5) 特定システムへの依存度

システムが管理している長期署名の全部あるいは一部について、長期署名の生成、延長、検証等の各処理及びそれに付随する処理を、他のシステムに移行することが容易であるか否かについて。

(6) 公開鍵暗号アルゴリズム脆弱化のインパクト

署名者による署名、証明書／失効情報／タイムスタンプ等の署名に用いられる公開鍵アルゴリズムが脆弱化した場合の影響及び対策。

(7) ハッシュアルゴリズム脆弱化のインパクト

署名者による署名、証明書／失効情報／タイムスタンプ等の署名、ハッシュツリーやタイムスタンプ等に用いられるハッシュアルゴリズムが脆弱化した場合の影響及び対策。

(8) 廃業のインパクト

TSA、LTA の廃業が、長期署名の検証や移行に与える影響。

(9) コスト要因

長期署名の生成や延長処理に伴う、主な外部的コスト要因。データの維持管理にかかるような内部的コストには言及していない。

(10)契約先

署名者、検証者、長期署名生成者、延長者、長期署名生成依頼者、延長依頼者にとって必要な外部委託先。

(11)主な用途

各方式にとって最も適していると考えられる用途。

第２部　電子署名利用環境の再構築に向けて

1．欧州の先進事例

欧州では、1999 年 12 月に発令された「EU 電子署名指令[1]」以来、各国において電子署名を IT 社会における基盤とすべく、様々な取り組みがなされてきた。現在の状況は欧州においても、必ずしも順調に電子署名が普及しているとは言いがたい。しかし、その中でも電子署名が社会の基盤として成立する兆しがある国や分野が出てきた。

欧州の国々の電子署名法のモデルは、「規制モデル[2]」と言われている。この規制モデルは、これは証明書発行などに一定の基準があるが、欧州の大陸法の国々は一般的に、電子署名法に関して高い基準を設定している。高い基準は証明書発行等のコストにも、一定のコストを要求することから、技術的観点、ビジネス的な観点からだけでは、電子署名を普及させることは難しい。制度的にも、電子署名に求められるセキュリティレベルに合わせた適度な強制力が必要になると考えられる。また、電子署名はある程度普及することにより、初めて基盤としてその威力を発揮することができると考えられる。このことからも制度や施策などによる立ち上げが重要になる。

本稿では、欧州において基盤として電子署名の普及が図られているエストニア、ベルギー、オーストリア、ドイツの 4 つの国の事例を紹介している。エストニアやベルギーの場合、国自体がコンパクトであり、地域で電子署名を普及されることにより様々な業界分野を横断して電子署名を利用しようとしている。このためにエストニア、ベルギーでは、全国民に電子身分証明書（eID カード）を配布することにより、電子署名、および、電子認証を社会の基盤としての確立を図っている。一方、オーストリアにおいては、IT 社会の基盤として IT 社会に相応しいアイデンティティ管理を実現した上で､特定の IC カード等のハードウェアに依存しない形で電子署名の普及を図っている。

業界分野での普及を考える場合、普及が可能な業界分野は、電子署名が、何らかの法制度による規制との関係がある場合が多い。規制が多い分野の典型として、医療や、製薬などの分野がある。英米法体系で市場モデルの電子署名法を採用している米国においても、医療や、製薬といった分野においては、多くの規制が存在する。そのため、これらの分野においての IT 化、電子文書化においても、規制が存在する。その規制に、ある基準を満たした電子署名が利用への強制力が働く。電子署名の普及には、こうした適度な強制力が必要だと考えられる。本報告書では、ドイツの医療分野の例を取り上げている。ドイツにおいては、医療従事者の身分証明書と、被保険者の健康保険証に関して PKI に対応した IC カード化を推進している。この IC カードを利用した電子署名、電子認証を基盤として医療情報システムを国レベルで最適化しようとしている。

1.1　エストニア

エストニアは人口約 135 万人であり、バルト諸国の一番北にある九州より少し広い程度の国である。1991 年にソビエト連邦から独立後、政治的判断で ICT に力を注ぐことを決め、市民もそれを支持した。1994 年以降国家予算の 1%を継続的に ICT に投資している。エストニアでは ICT 基

[1] EU 電子署名指令
[2] http://www.japanpkiforum.jp/shiryou/esign_k/2004_e-sign_report.pdf

盤を整備することにより、電子政府などの開発経費の拡大を防ぐ方針を取った。基盤の主なものとしてeIDカードとX-Roadがある。電子署名の普及としては、このeIDカードを中心に様々な取り組みがある。

(1) eIDカード

2002年よりeIDカードが発行され、15歳以上の市民全員が所持を義務づけられている。長期外国人滞在者もこのカードを受け取ることができる。2008年1月時点で、約100万枚が発行されている。

図 2.1.1 エストニアeIDカード

eIDカードの表側には、カード所有者の写真とともに、以下の項目が印字されている。

・カード所有者の氏名
・カード所有者の国民ID番号
・カード所有者の生年月日
・カード所有者の性別
・カード所有者の市民権の有無
・カード番号
・カードの有効期限

カードの裏側には、以下の項目が印字されている。

・カード所有者の出生地
・カード発効日
・その他、居住許可に関する項目等
・機械で読取り可能な形式で印刷された、上記の裏表に印字されたデータ

eIDカード内（ICチップ）には、写真と（手書きの）署名を除く上記情報と、認証用と否認防止の署名用の2種類の電子証明書が格納されている。証明書には、氏名とカード所有者の国民ID番号が記入されている。この国には認証局はひとつだけであり、発行された証明書の相互運用性については問題ない。カードは10年有効だが、電子証明書は有効期限が3年である。カードの取得費用は、約10ユーロである。2007年より、カードと証明書の有効期限が両方と

も 5 年に変更になる予定とされている。

なお、エストニアでは国民 ID 番号は誕生時に決まり生涯その番号を使う。国民 ID 番号は、性別（1 桁）、生年月日（6 桁）、シリアル番号（4 桁）の 11 桁で構成される。国民 ID 番号はカードに印字されるなど公開されていて、個人で秘密にしておくものではなく社会的な情報と考えられている。

(2) X-Road

X-Road は分散する各種データベースを高いセキュリティを確保して接続して利用するために、エストニアで開発されたデータ交換基盤である。セキュリティを確保するために、IC カードを用いた認証を必ず行うことと、さまざまな情報システムがセキュリティ・サーバ（SS）を介して通信する点である。SS はすべてのメッセージをログに保存する特殊なファイヤーウォールであり、いつだれが利用したのかを保存することができる。データベースはアダプタ・サーバ（AS）に接続され、メッセージ形式の変換を行う。

電子証明書を用いて本人認証することにより、市民は政府が管理する個人情報システムにアクセスすることができ、個人の登録情報を見ること、及び自分の登録情報をいつ誰がアクセスしたかを確認することができる。

X-Road を用いた一般的な e ガバメント・アーキテクチャーの概要を図 2.1.2 に示す。

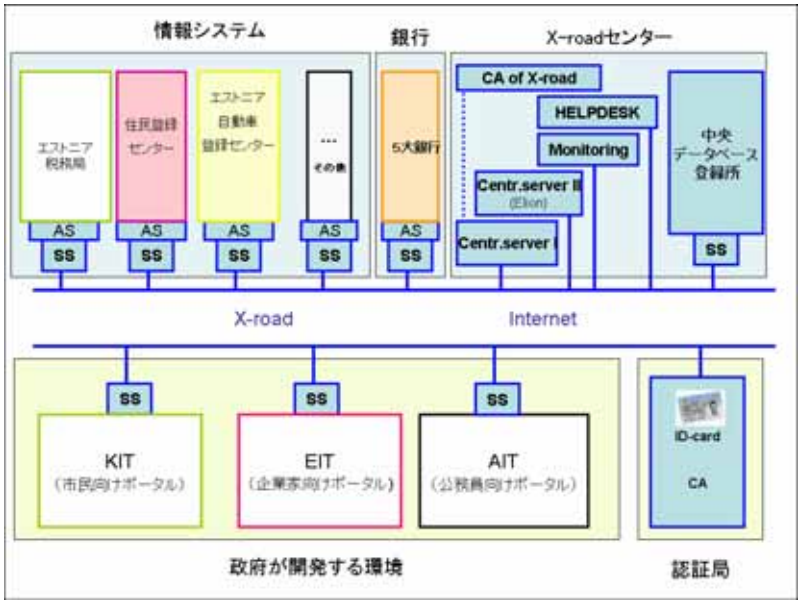


図 2.1.2 X-Road

(3) OpenXAdES と DigDOC

エストニアにおける技術面からの電子署名の取り組みに、オープンソースプロジェクトである OpenXAdES[3]がある。このプロジェクトでは、XML ベースの長期署名フォーマットである Xades

[3] http://www.openxades.org/

（XML Advanced Electronic Signatures）の生成と検証を行なうミドルウェアのオープンソースによる実装を行なっている。OpenXAdES は、オープンソースのミドルウェアとして広く配布することにより、電子署名、および、タイムスタンプを施した電子文書の相互運用性を確保している。またミドルウェアの OpenXAdES をベースとした DigDOC という署名ソフトウェアも広く配布されている。

◇エストニアのカードによるサービス

eID カードの利用場面としては、公共乗り物の運賃支払い、運転免許証の代用、e バンク、電子政府の利用など、日々市民が利用するサービスがある。その代表的なサービスを紹介する。

(1) 電子投票（e-Vote）

2005 年 10 月に、世界で初めて国の規模の選挙でインターネットを用いた投票を実施した。その後 2007 年 3 月に国政選挙でも同様のインターネットを用いた投票を実施された。投票には、eID カードによる認証（Authentication）と電子署名が利用されている。

投票は、不在者投票期間に実施した。セキュリティの確保のため、投票内容は選挙管理委員会の公開鍵で暗号化し、選挙管理委員会はプライベート鍵で復号する。この方法により、投票者の認証と投票内容の漏洩（選挙管理委員会以外の人が投票内容を見る）を防いでいる。2005 年 10 月では、インターネットで投票した人の割合は有効投票の中の 1.85%（9287 名）であり、その後の 2007 年 3 月では、5.4%（30.275 人）となっている。このインターネット投票に関する詳細な調査報告書が公開されているが、この報告書によると、2005 年にインターネット投票した人は、2007 年にもインターネット投票を行なっている。こうした人々は、インターネット投票を契機に電子署名を利用していくと考えられている。

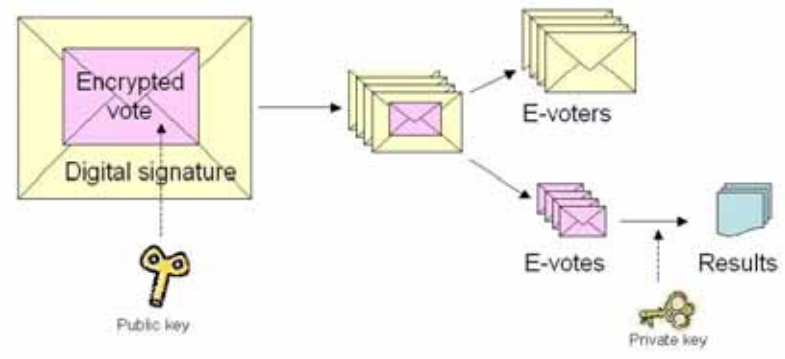


図 2.1.3 e-Vote の概要

(2) e-Democracy

議会が運営する、市民の意見を汲み上げるしくみである。登録すれば誰でもが参加することができる。テーマをあげ、3 週間議論して政府に提案するかどうかを投票する。このときも、電子署名をつけて投票する。提案が決まった場合は、2 週間以内に関係省庁に送り、1 ヶ月以

内に回答が返される。

◇まとめ

エストニアでは、IT による経済発展を目指していることもあり、トップダウン政策と法制度の柔軟な対応により、PKI を電子署名と認証の基盤として機能させることにより、地域の中での全体最適の実現に PKI を有効に活用する利用する傾向がある。

柔軟な法制度も、非常に重要な要素だと考えられる。電子署名が有効に働く領域は、「責任の所在」の明確化が必要な、何らかの規制が重要な役割を果す分野になる。こうした規制が重要な分野ほど、硬直化した従来の法制度が、電子化を遅らせる原因となっていると考えられる。エストニアのような法制度の柔軟な対応が可能な国や地域ほど、電子署名が普及する可能性が高いと考えられる。

エストニアの電子署名法[4]には、タイムスタンプも含まれる。電子署名にタイムスタンプも付与するとこにより、証拠性の高い電子文書の保存が可能となる。

参考文献

[1] The Estonian ID Card and Digital Signature Concept -Principle and Solutions 2003, 6
[2] The National Election Committee E-Voting System Overview - Tallinn 2005 - http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf
[3] Report for the Council of Europe Internet voting in the March 2007 Parliamentary Elections in Estonia http://www.eudo.eu/download/Report_Evoting_Estonia_for_the_CoE_2007.pdf

1.2 ベルギー

ベルギーは、人口 1 千万人強の国であり、人口と面積ともに日本の約 12 分の 1 の国である。注目されているのは、欧州の人口1千万人以上の国ではじめて国民全員が公開鍵証明書を含むeIDカードを所持することを決めた。2009 年までに 12 歳以上の国民全員に、これまでの紙の国民カードから全て eID カードに切り替わる予定である。

eID カードの立案などは、ベルギー連邦政府の Fedict が行なっている。Fedict は 2001 年の 3 月に設立され電子政府の推進を主な責務とする政府機関である。組織としては、約 100 名からなり、電子政府戦略の立案や連邦の各省庁の IT 部門の情報設備投資を横通しして、連邦政府共通に係わる標準化やガイドラインの作成や共通基盤の構築など IT 関連の課題を解決する部署である。

ベルギー市民用の eID カードは、2008 年 1 月現在、既に 600 万枚発行されている。用途として、データの入力のほか認証や電子署名にも使われる。

eID カードの券面に印刷されている情報は以下のとおりである。

・名前／クリスチャンネーム

[4] エストニアの電子署名法の日本語訳が、「電子署名法の在り方と 電子文書長期保管に関する現状調査」http://www.japanpkiforum.jp/shiryou/esign_k/2004_e-sign_report.pdf にある。

・国籍
・誕生日及び出生地
・性別
・eID カード発行場所
・eID カードの開始日と終了日
・eID カードの種別とカード番号
・所有者の写真
・所有者のサイン
・国民 ID 番号
（生年月日が 6 桁、性別及び番号が 3 桁、チェックデジットが 2 桁の 11 桁からなる）

図 2.1.4 ベルギーの eID

eID カード内（IC チップ）には写真を含む券面情報が格納される他、以下の情報が格納されている。
・プライベート鍵
・二つのカード所有者証明書
・信頼点の自己署名証明書
・カード所有者の住所（住所は変わる可能性があるので、券面には印刷しない）

電子証明書の有効期限は、カードそのものと同じく 5 年間である。国民は 10 ユーロ（約 1650 円）負担する必要がある。この間住所の変更があった場合、カード内のデータを書き換える（券面には住所は印刷されていない）。

電子政府サービスについては、連邦政府、地方政府とも、多くの電子政府サービスが提供されている。税務申告なども 150 万人以上が利用していてこれは、全体の 30%にあたる。

次に CA の構成図を下記に示す。

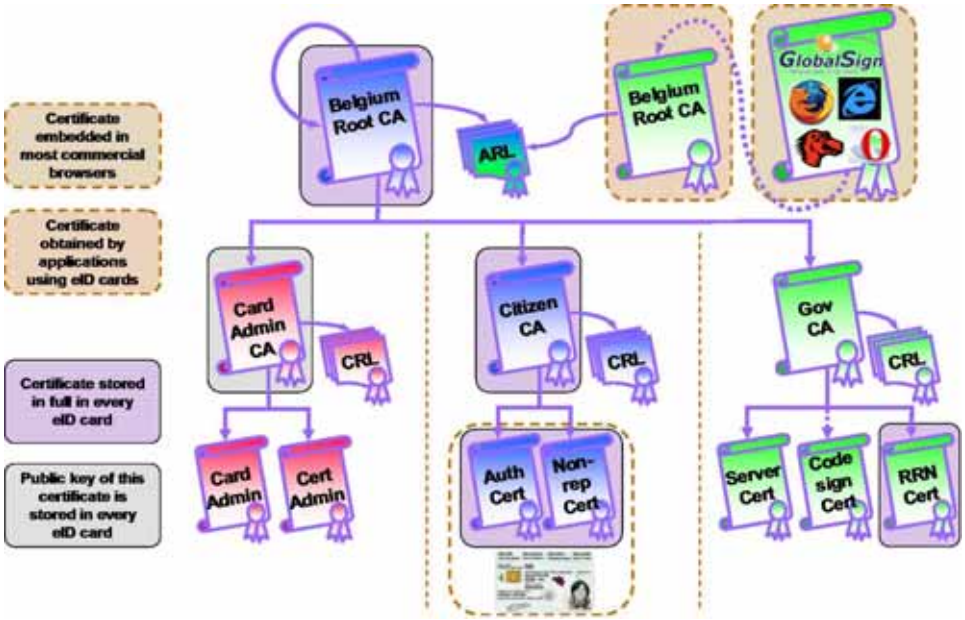


図 2.1.5 eID カード CA 構成図

ベルギーのルート認証局は、カード管理のための認証局や、政府関係のサーバ証明書なども発行している政府認証局（Gov. CA）など、いくつかの認証局に CA 証明書を発行している。ルート認証局の自己署名証明書は、カード所有者の信頼点として eID に格納されるが、このルート認証局自体も、商用認証局である GlobalSign から CA 証明書が発行されている。

ルート認証局の下位認証局である市民認証局は、「否認防止用の証明書」および「認証用の証明書」の 2 つのカード所有者の電子証明書を発行している。ベルギーの eID のような欧州の電子身分証 IC カードは、IAS すなわち Identification、Authentication と electronic Signature と言ったコンセプトで仕様が作成されている。eID カードは、電子認証（Authentication)、電子署名（electronic Signature)、に利用できるものだが、その使い分けを明確にしている。例えば、ベルギーの eID では、カードに格納される（否認防止の）署名用の証明書は、18 歳以上に発行されている。責任能力の観点から 18 歳以下の国民には、IAS の「S」を提供していない。否認防止の署名は「責任の所在」を示すので責任能力が必要なる。

ベルギーの eID の場合、否認防止の署名のプライベート鍵は、1 回の否認防止の署名操作、つまりひとつの文書の否認防止の署名毎に「カード所有者の同意確認」(User Consent）のための PIN の入力が必要な仕様になっている。正当なカード所有者の認証（Authentication）時の認証用のプライベート鍵の利用は、カード所有者に不利益をもたらすことはない。認証（Authentication）をするのはサービス提供者側であり、カード所有者が認証されるためにプライベート鍵を使うことにより責任が生じると言うことはない。これに対して否認防止の署名は、「カード所有者が同意して行う」ものであり、この署名には、その署名文書等にはカード所有者

の責任が生じるということを理解する必要がある。署名時の「カード所有者の同意確認」のための PIN の入力には、図 2.1.6 のようなダイアログが表示される。

図 2.1.6 電子署名のダイアログ

ベルギー政府が公認している eID カードを利用するミドルウェアやアプリケーションの多くが、オープンソースソフトウェアとして公開されている。これは、BELPIC 自体の仕様がオープンであることにも関係している。

参考文献

[1] The Belgian Electronic Identity Card (Overview)
www.cosic.esat.kuleuven.be/publications/article-769.pdf
[2] IC・ID カードの相互運用可能性の向上に係る基礎調査
http://www.ipa.go.jp/security/fy18/reports/ICID/index.html

1.3 オーストリア

オーストリアは、人口 830 万人の国であるが、電子署名を積極的に普及させようとしている国の一つである。オーストリアの電子署名法は、行政手続に関する署名に関して、電子署名は法的に認められることを示した。行政手続に関する署名は全て電子署名の要求を満たす必要性がないが、適正なセキュリティレベルで運用されなくてはならないと定めている。オーストリアにおいては、2004 年に施行された電子政府法が、電子署名に必要な識別（Identification）に特徴がある。

また、電子政府推進の為、1999 年 5 月、オーストリア財務省、オーストリア国立銀行、グラーツ工科大学により非営利団体 A-SIT が設立された。A-SIT の使命はセキュリティ関する指針、手引きの作成や電子政府推進のためのコンサルティングなどであるが、市民カード（Bürgerkarte）の導入および暗号方式の評価を行っている。また、A-SIT は電子署名の証明書を提供する権限を持った唯一の団体とである。

- オーストリアの市民カード

オーストリアの電子政府の基本的な要素は市民カード（Bürgerkarte）である。この市民カードのコンセプトは「否認防止の署名」と「認証（Authentication)」機能を持つことである。これにより市民は、電子公共サービスにアクセスし、行政手続を行うことができる。この市民カード（Bürgerkarte）の特徴は、全ての市民に同じカードを所持させるのではなく、次の媒体に機能を持たせることができることにある。よって、どの媒体を利用するかは、完全に市民が選択することができる。主な例は次の通りである。

・ 電子健康保険カード「e-card」

図 2.1.7 オーストリアの電子健康保険カード

全オーストリアで普及キャンペーンが行われ、2005 年 11 月、紙ベースの医療証明書から変更された。この IC カードには、所有者の氏名、所属、生年月日、社会保険番号などの行政データが含まれる。

・ 銀行クレジットカード
・ 携帯電話

また、電子政府を促進する為、首相府はすべての基本ソフトウェアおよび、必要なライセンスの無償提供を行っている。

- オーストリアの ID 管理

市民カードで利用されている ID カードの管理方式は次の通りである。

オーストリアの ID 管理方式の特徴は 3 レベルの国民 ID 番号（ZMR-Zahl、SourcePIN、ssPIN）を連携して使うことである。以下は The Austrian E-Government Act に公開されている。[1]

① ZMR-Zahl

出生後 CRR（Central Register of Residents）に登録される。この時点で、CRR の内部ルールに従った番号がつけられる。この番号は公開される番号であり、一生変わらない。同様に、在オーストリア外国人は supR（Supplemental Registers）に登録される。また、企業は CR（Commercial Register）に、団体等は RA（Register of Associations）に登録されて番

号がつけられる。

② sourcePIN

ZMR-Zahl を基にした暗号処理を行うことにより、ID（SourcePIN：sPIN）を得る。この番号は市民カードに格納され、本人以外は知ることはできない。また、sPIN から ZMR-Zahl を推定することはできない。この処理は、政府のデータ保護委員会（DSK）のもとで実施される。（他の番号も同様の処理が行われる）

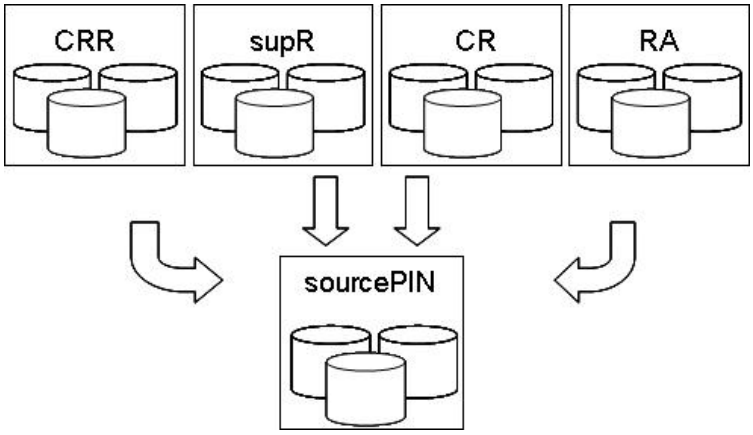


図 2.1.8 sourcePIN 作成の流れ

③ ssPIN（Sector-specific IDs）

ssPIN が実際にアプリケーションで使われる ID である。sPIN と各アプリケーションに振られた SectorID を合成した上でハッシュ処理を施すことにより ssPIN を得る。これは、利用する毎に発生して利用する。なお、ssPIN から sPIN を推定することはできない。

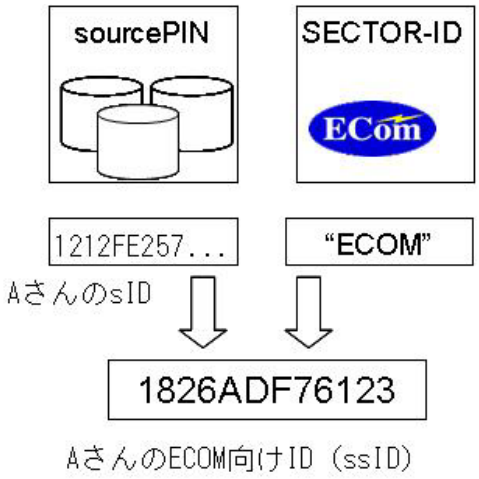


図 2.1.9 ssPIN の生成

このようなしくみにすることにより、アプリケーション毎にことなる ID を利用することができ、不正なアクセスをしにくくするとともに、政府のデータ保護委員会（DSK）の許可を得ることにより、たとえば納税申告の場合など、関連する情報を統合利用して、把握した情報を納税者に提示することができる。

参考文献

[1] The Austrian E-Government Act
http://www.stammzahlenregister.gv.at/documents/e-government-act_federal_law_gazette_part_i_no_10_2004.pdf

1.4 ドイツ

保健医療福祉分野では、世界的に医療記録等の重要な個人情報の電子化が進みつつあるが、この電子化された医療記録を中心に医療機関の連携などを行う EHR（Electronic Health Record）の実現が、先進各国の医療の情報化の目標になりつつある。このような EHR を推進するためには、医療に関連した電子文書の作成に電子署名が非常に重要になる。また、社会保障制度の重要な一翼を占めている保健医療福祉分野は、非常に高額な公的な資金も投入されており、その高い透明性が求められているという点においても医療文書の責任者としての医療従事者の電子署名が重要になる。

保健医療福祉分野の電子署名の整備は、特に社会保障制度が成熟している欧州で先行している。例えば、フランスやドイツなどでは、医師や薬剤師に対して電子署名や電子認証に対応した医療従事者身分証書 IC カードを配布している。このことにより診療記録や電子処方箋への署名を行える環境を整備し医療の情報化、電子化を進めている。また、全被保険者の健康保険証を PKI 対応した IC カード化し、被保険者自身が自分の健康情報にアクセスを可能にするなどといったプロジェクトが進行している。こうしたプロジェクトの目標は、国レベルでの医療全体に関して、IT 技術を駆使して全体最適化することにより、医療費の削減を目指したている。こうした全体最適化のためには、広域のセキュリティや長期にわたる電子文書の保存、更に高い透明性や、標準化されたセキュリティ技術が必要になり、そのための電子署名の利用がある。

- 電子健康保険カード（「健康カード」）

  ドイツでは、2005 年 6 月 27 日付「法定健康保険組合近代化法」に基づき、健康保険組合は、従前の健康保険被保険者カードを「健康　カード」（電子健康保険カード）に置き換えるよう義務付けられた。

- ドイツの国家 e 健康プログラム

  ドイツの国家 e 健康プログラムは、8,000 万枚の被保険者向け IC カード（PDC）、37 万枚の医療従事者向け IC カード（HPC：Health Professional Card）をベースに 2,200 の病院、100,000 の一般開業医、21,000 の薬局と 200 の健康保険組合をつなごうとしている。

  大部分の他の欧州の国と対照的に、ドイツはセキュリティ基盤の整備の解決から始めるほう

を選んでいる。

- 電子処方箋

ドイツの国家ｅ健康プログラムで実現を予定しているものに電子処方箋がある。電子処方箋では、HPC による電子処方箋への署名と、PDC による、電子処方箋の暗号化と復号が利用される。

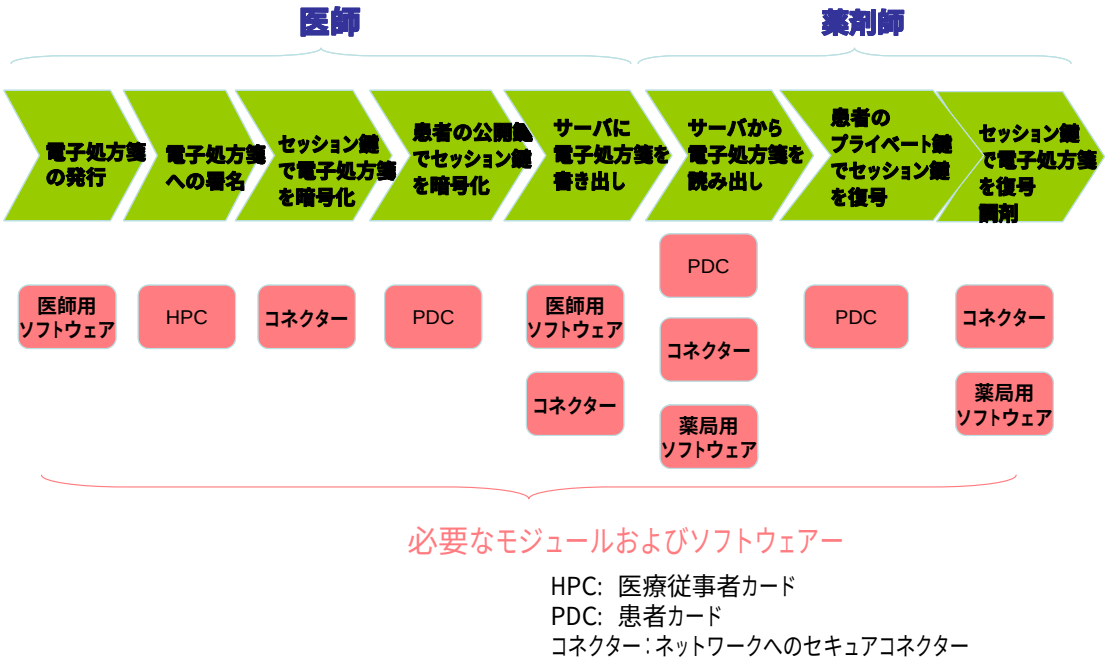


図 2.1.10 ドイツの電子処方箋

医師は、患者のために（電子）処方箋と発行するが、処方箋に対して自分の HPC を使い電子署名を施す。その署名が付された電子処方箋を患者のカード（PDC）に格納された公開鍵を利用して暗号化を施し、その暗号化を施した電子処方箋を外部のサーバに送付する。このとき、患者の PDC には、電子処方箋のチケット番号が書き込まれる。

薬局では、患者の PDC に書き込まれたチケット番号から暗号化された電子処方箋をサーバから取り出す。暗号化された電子処方箋を復号するには、この患者の PDC に格納されている暗号用の証明書に対応したプライベート鍵を使う。薬局では、このようにして医師が署名をした患者の電子処方箋を受領することができる。

ドイツのｅ健康プログラムでは、電子処方箋の実現により、個々の患者の薬の相互作用（薬の副作用）などを自動的に検出でき、このことにより大きな費用削減ができるとしている。

[1] Health Systems Relying on Smart Cards
http://www.cenetec.gob.mx/archivoscenetec/Seminario_AplicacionesBandaAncha_para_e-Salud/Presentaciones/17_Klaus_Vedder_Seguridad_en_Smartcards.swf

2．わが国における今後の展望

日本においては、2001 年 4 月に電子署名法が施行された。この電子署名法が施行されて、7 年経過したが、現状において電子署名法に基づく電子署名が十分に普及しているとは言い難い状況にある。電子署名法が検討されてきた 2000 年当時からしても、IT 技術は社会の基盤として深く浸透しつつある。それにも関らず電子署名が利用されている領域は、まだ、かなり限定的である。こうしたことの理由のひとつに 2001 年に施行された現在の電子署名法は、完璧を求めすぎているところがあるのかもしれない。

電子署名法の認定認証局の認定基準は非常に厳しく、また、証明書の発行に対する制約も大きい。一般論として、セキュリティに完璧はなく、セキュリティに完璧を求める程に現実的なコストや利便性から乖離してしまう。電子署名法についても同じことが言える。

電子署名に要求されるセキュリティも含め、「そもそも電子署名とは何か」、「電子署名がどういった領域に利用されるべきなのか」、「電子署名という範囲だけの検討でよいのか」、こうしたことが再度検討される必要があるだろう。ここでは、検討すべき課題とその展望について記述する。

2.1　電子署名と電子認証の使分け

「欧州の先進事例」で紹介したエストニアとベルギーの電子身分証明書は、一般的に eID と呼ばれている。「ベルギー」の事例でも紹介したように、この eID は、IAS すなわち Identification、Authentication と electronic Signature と言ったコンセプトで仕様が作成されている。そして証明書は、認証（Authentication）用と（否認防止用のための）電子署名（electronic Signature）用のために別々の証明書は発行されており、1 枚のカードで双方の利用できる仕様になっている。当然のことながら、認証と電子署名の使い分けも明確にしている。

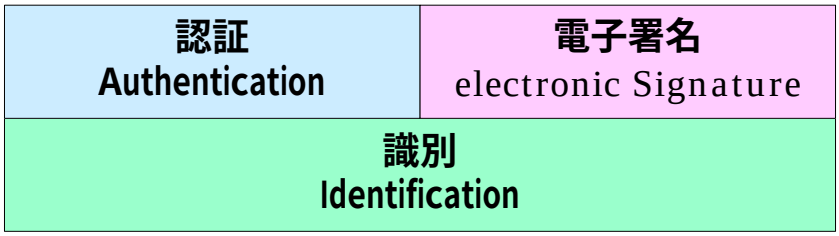


図 2.2.1 IAS

これに対して、日本の公的個人認証サービス（JPKI）では、否認認防止目的の証明書のみが発行されている。従って、JPKI の発行する証明書を、認証（Authentication）として利用すべきではない。否認防止目的のプライベート鍵を安易に責任の生じない認証（Authentication）として利用することは、責任が生じる署名に対するカード所有者のリテラシーの低下につながる可能性がある。

このような状況に対して、2007 年 5 月、総務省の「公的個人認証サービスの利活用のあり方に

関する検討会[5]」から公表された「公的個人認証サービスの利活用のあり方に関する検討会　論点整理[6]」では、「電子署名」と「オンライン上の認証」の違いについて整理した上で「認証用途の電子証明書の発行」についての検討がなされている。これは、「電子署名」と「オンライン上の認証」の違いについて認識されないまま、電子政府が構築されてきたという裏返しでもある。

認証と電子署名の双方の証明書を発行すること自体が、直ちに電子署名の普及につながるという訳ではないが、「電子署名とオンライン上の認証の違い」といった基本的な認識ない、また、電子署名に対する様々な誤解があるままで、電子署名が適切に利用されるといったことは考えにくい。

電子署名用の証明書の発行に関しても、ひとつ重要な論点がある。エストニアとベルギーも、カード所有者にふたつの証明書を発行しているが、その証明書を発行している認証局は同一の認証局である。これに対して、日本の電子署名法は、「誤認防止」という理由から、電子署名法の認定認証局は、電子署名以外の用途の証明書を発行することを実質的に禁止してされている。これは、ビジネス上の大きな制約になっている。

PKI は、CA 証明書などの発行により様々な信頼関係（Trust Model）を形成する。電子署名法に閉じた「誤認防止」の考え方は、様々な信頼関係を結ぶことを困難にしている。電子署名は、現在の電子署名法の枠組みの中だけではなく、電子認証（Authentication）やタイムスタンプ等も含め、IT 戦略の枠組みとして再構築されるべきである。

2.2　電子署名とタイムスタンプの統合と電子文書保存

電子署名を施す文書は、基本的に保存されるべき文書であり、その時刻証明などは、重要な意味を持つ。タイムスタンプサービスの主な方式のうちのひとつは、時刻が何らかの形で保証されたサーバが行う電子署名によって実現される。つまりタイムスタンプ自体も電子署名により実現された技術と言える。こうしたことからも、電子文書の証拠性を確保には、電子署名、タイムスタンプの双方が適切に利用されるのが合理的だと考えられる。技術だけではなく、制度面においても、電子署名とタイムスタンプは、関連付けられるべきである。実際、欧州の電子署名法には、欧州の先進事例で紹介したエストニアのようにタイムスタンプと取り込んだ例が少なくない。図 2.2.2 に、エストニアにおける、電子署名法、証明書を発行する認証局、時刻証明を行うタイムスタンプ局（TSA）などの関係を示す。

[5] http://www.soumu.go.jp/menu_03/shingi_kenkyu/kenkyu/kojin_ninsho/index.html
[6] http://www.soumu.go.jp/s-news/2007/pdf/070522_1_si2.pdf

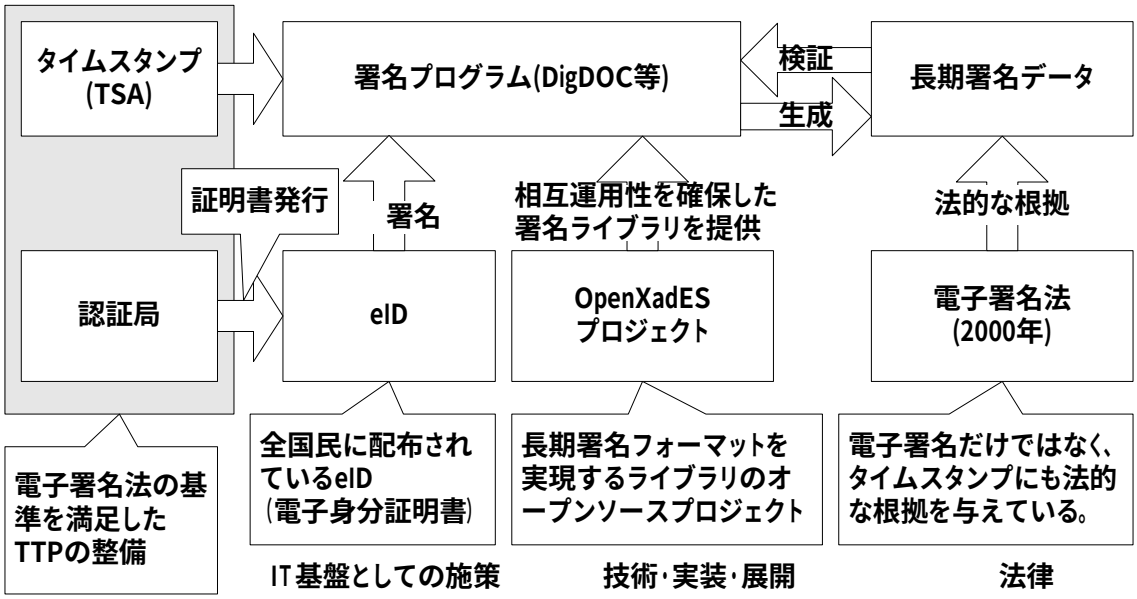


図 2.2.2 エストニアの電子署名とタイムスタンプ

エストニアにおいては、制度面から電子署名法が、「証明書を発行する認証局」、「時刻証明を行うタイムスタンプ局（TSA）」を支えており「長期署名データ」に法的な根拠を与えている。IT 施策としては、全国民に配布される eID が、誰もが電子署名を利用する環境を提供している。また技術面からは、電子署名とタイムスタンプを利用した長期署名フォーマットを実現するオープンソースのライブラリの実装・展開により、相互運用性を確保した署名・タイムスタンプ環境を提供している。エストニアのような国は、既存の法制度等のしがらみや、その法制度等から生じる既存の権益などの影響がすくない。そのため比較的、IT 社会に適応した法制度を構築しやすいと言える。

現時点の日本においては、「長期署名データ」が必要とされる分野は、紙文書保存に大きく依存しているのが現状ではないだろうか。過去から存在する法制度等のしがらみや、この法制度等から生じる権益の確保などが、様々な電子化を阻害している可能性がある。

タイムスタンプによる時刻証明は、公証人による確定日付の付与と同様の機能を、IT 技術を駆使して実現したものとも言える。しかし、その効力が電子署名のように法制化され広く認められている訳ではない。タイムスタンプによる時刻証明は、公証人による確定日付の付与にくらべ、非常に低コストで、かつ自動的に行うことが可能なので、社会全体としての大きなコスト削減が可能になる。紙文書から電子文書への移行の中で、電子署名とタイムスタンプが適切に利用されるべきである。

2.3 適度な強制力

電子署名法における認定認証局の認定制度等は、証明書発行等に対して高い基準を設定している。この高い基準は、一定のコストを要求する。そのため技術的観点、ビジネス的な観点からだけでは、電子署名を普及させることは難しい。制度的にも、電子署名に求められるセキュリティレベルに合わせた適度な強制力が必要になると考えられる。また、電子署名はある程度普及する

ことにより、初めて基盤としてその威力を発揮することができると考えられる。このようなことからも制度や施策などによる立ち上げが重要になる。

情報セキュリティ分野等において、これまでの法制度で影響力が大きかったものに「個人情報保護法」がある。これは、法律の施行により強制力が働いたため非常に影響力が大きかった。逆に「電子署名法」「e 文書法」は、電子署名や、電子文書での保存を強制したものではない。現状維持でよいとすると、これらは利用されない。普及を促がすためには、何らかの強制力やインセンティブが検討される必要がある。

適度な強制力により、電子署名が社会基盤として成立すれば、その電子署名の基盤の上で様々な展開が可能になる。実際、韓国における電子署名は、適度な強制力により、実際に機能する社会基盤となりつつある。そして、様々な分野で電子署名が利用されつつある。

日本において、電子署名が普及した分野に行政機関による電子入札がある。電子入札は、入札を行なう行政機関が、入札に対して電子入札を強制させることにより普及した。電子入札が、電子署名を必須としたため電子署名も普及した。こうした業界においては、電子入札の次に更に高い否認防止性が求まれる電子契約においても電子署名を容易に利用することができる。同様なことは、社会全体にも言える。電子署名は、利用者に広く普及して初めて基盤としての役割を果す。電子署名が基盤として機能することは、社会全体に対しての透明性と効率の双方を提供することになる。

今後、「適度な強制力」により、電子署名が普及する可能性のある分野として、保健医療福祉分野がある。保健医療福祉分野では、医療記録等の重要な個人情報の電子化が進みつつある。この電子化された医療記録を中心に医療機関の連携などを行う EHR（Electronic Health Record）の実現が、先進各国の医療の情報化の目標になりつつある。このような EHR を推進するためには、情報のセキュリティ確保や本人確認及びその資格と属性認証等が、非常に重要になる。また、社会保障制度の重要な一翼を占めている保健医療福祉分野は、非常に高額な公的な資金も投入されており、その高い透明性が求める。

保健医療福祉分野における電子署名の利用環境の整備は、特に社会保障制度が成熟している欧州で先行している。「欧州の先進事例」では、ドイツの事例を取り上げている。このドイツの事例やフランスでは、医師や薬剤師に対して PKI に対応した身分証書 IC カードを配布し、診療記録や電子処方箋への署名を行える環境を整備し医療の情報化、電子化を進めている。また、全被保険者の健康保険証を PKI 対応した IC カード化し、被保険者自身が自分の健康情報にアクセスを可能にするなどといったプロジェクトが進行している。こうしたプロジェクトの目標は、国レベルでの医療全体に関して、IT 技術を駆使して全体最適化することにより、医療費の削減を目指したものである。こうした全体最適化のためには、広域のセキュリティや長期にわたる電子文書の保存、更に高い透明性や、標準化されたセキュリティ技術が必要になり、そのための電子署名の利用がある。

強制力を働かせることに関しては、異論はあるだろう。しかし、現在の紙文書で最適化された社会から、法制度や慣習、既存の権益等を乗り越えて、電子文書で最適化された社会への移行を促すためには、適度な強制力は必要になるだろう。

2.4　社会的信頼の仕組みの再構築

電子署名が施された電子文書は、その電子文書の責任者や内容を合理的に証明にする。署名者自身は、その署名に利用した証明書により明確になる。そして、公開鍵証明書を発行する認証局は、証明書に記載されたエンドエンティティを証明すること、すなわち誰に証明書を発行したか関して責任を持つことになる。ここで、証明書の発行コストの本質は、証明することのコストになる。この「証明することのコスト」と「証明の信頼性」は、様々な公的な証明書等の信頼性などの既存の法制度等の社会システムに大きく依存している。そして、この公的な証明書等の多くは紙文書ということになる。このような社会システムを「社会的信頼の仕組み」と表現することにする。

「欧州の先進事例」で紹介した、エストニア、ベルギーは、国民 ID が存在し、発行される証明書は、この国民 ID を証明している。国民 ID に関する議論は、欧州においても様々な議論があるようであり、「欧州の先進事例」で紹介したオーストリアでは、別のアプローチを取っている。しかし、エストニア、ベルギーとオーストリアで共通しているのは、IT 社会にふさわしい「社会的信頼の仕組み」を構築しようとしている点にある。

電子署名の技術のおおもとにある PKI を理解する重要なキーワードに、信頼関係モデル（Trust model）、信頼点（Trust point）などがある。この「信頼」自体は、IT 技術で実現できるものというよりは、「社会的信頼の仕組み」に依存する。PKI の場合、信頼関係をマシンリーダブルな標準化された証明書で表しコンピュータによる自動処理を可能にする。この場合、社会において何が信頼できるかと言ったことは、「社会的信頼の仕組み」既存に大きく依存する。

現在、日本では、（仮称）社会保障カード、社会保障番号の議論が進んでいる。海外、特に欧州における社会保障カードと類似したカードは PKI 対応となりつつある。日本においても新しい社会保障カードが実現してとすれば PKI 対応のカードとなるだろう。なぜ PKI かということに関して、PKI は広く仕様をオープンにしてもセキュリティを保てる仕組みが可能であり、そのため幅広い標準化なされた技術であるということが言える。また、公的機関は従来から様々なヒューマンリーダブルな紙文書を使った証明書の発行を行ってきたが、コンピュータの処理を前提とした場合、電子化された証明書を使うのが合理的であり、電子化された証明書の標準として PKI がある。

以上のように、IT 社会にふさわしい「社会的信頼の仕組み」には、PKI が大きな役割を果たすと考えられる。日本の JPKI も、IT 社会にふさわしい「社会的信頼の仕組み」の構築を目指したものとかもしれない。しかし、欧州の eID のコンセプトの IAS の I と A に関して、もっと考慮されるべきであろう。特に、I（Identification）の「識別」に関して「欧州の先進事例」のオーストリアの電子政府法に見られるような、根本的な取り組みがなされていないところに問題があるのではないだろうか。JPKI では、住民基本台帳にある基本 4 情報を証明しており、これが実質的な識別のための項目となっている。こうした事例は、海外では、ほとんど見受けられない。

この「識別」を根本的に見直して IT 社会にふさわしい「社会的信頼の仕組みの再構築」を検討する必要があるかもしれない。オーストリアの取組は、そのように見える。現状のシステムは、IT 技術もネットワークもない時代の紙文書を前提としたシステムである。現状の電子署名法にしても、紙文書に対する法制度をそのまま電子文書に適用しようとするものである。これらは、IT

技術の面からは様々な不都合も出てきた状況にあると言える。次の時代の IT 技術を駆使した社会にふさわしい社会システムのために「社会的信頼の仕組みの再構築」、「電子署名の再構築」を検討する必要があるだろう。

参考

「PKI をめぐる社会的動向」
プロフェッショナル・セキュリティ・レビュー　ISBN：978-4-7561-5103-2

第３部　内部統制における文書管理

「金融商品取引」（いわゆる、JSOX 法）の 2006 年 8 月制定を受け、2008 年 4 月から、3 月決算の上場企業を皮切りに、JSOX 法の対象となる。JSOX 法に関連して、「財務報告に係わる内部統制の評価及び監査に関する実施規準」も公開されているが、文書・記録の管理は各企業の判断に委ねたところが多い。このため、ECOM として、各企業の文書・記録の管理への指針を示すべく、第一段階として、各企業における文書管理の実態調査を計画した。

企業、官公庁、自治体を取り巻く環境は、「情報公開法」、「PL 法」、「個人情報保護法」、「ISO19000」、「ISO14000」、「会社法　内部統制」などの CSR が厳しくなってきており、順次、これらへの文書・記録の管理への指針の拡大を図って行く予定である。

また、内部統制文書の保管期間は 5 年以上、通常の会計関係資料は 7 年間の保管義務があることから従来に引き続き長期保存ストレージの動向についても確認を行っていく。

1．文書管理の実態調査計画

各企業の文書管理の実態調査を行うに当たって、ARMA 及び ARMA から紹介頂いた記録管理学会とその進め方を協議した。記録管理学会では、製造業 12 社の法務部、研究部、総務部などに対し、インタビュー調査を行い、全社的な文書管理ルール、文書管理ルールの運用、監査体制などのヒヤリングを行っている。[1]

その結果、文書管理のためのルール作りといった基本的な事項にも改善の余地が多いことが判明している。

本 WG では、JSOX に視点をおいて、主に、各企業の内部統制事務局へのヒヤリングを通じて、問題点の把握に努めていく。JSOX の評価上は文書管理の仕方自体は対象となっていない。しかしながら、評価の元となるエビデンス・文書を記録・管理していくのは文書管理であり、その重要性は極めて高い。

表 3.1.1 に記録管理学会の調査で判明した文書管理ルール、管理ルール運用上の課題を紹介する。

JSOX のエビデンスとなる文書・記録も同様の管理状況にあることが推定できる。

手作業での文書管理には運用上の限界があるため、電子化による運用品質の確保の推奨をしていきたいと考える。

表 3.1.1 製造業企業に対する文書管理に関するインタビュー結果抜粋[1]

No	分類	質問事項	判明した課題
1	文書管理ルール	会社全体若しくは企業グループ全体に適用される文書ルールにはどのようなものがありますか。	全社的文書管理ルール・その他近年の法的自主規制に対応するものはあるが、形骸化している。外資系は記録保持スケジュールが厳密に運用されている
2		保存すべき文書の全社的な種類・分類	全社基準は形骸化。外資系では記録保持スケジュールが厳密に運用されている。

3		実際に保存資料の調査で頼りになる部署はどこですか。	技術文書については、技術管理部署・図書室にある。その他については、事業場単位
4	ルールの運用	保存文書の保存・廃棄の選別はどのようにしていますか？	部署長の権限で保存／廃棄が決まる。
5		保存文書の処分（廃棄日）記録はありますか。	処分記録を確認できない。
6		組織変更での継承は確実ですか。	組織変更や引越しで廃棄される可能性が高い。
7		部署内で使う文書の存在が、部署外から容易にわかりますか。	他部署の状況はわかりずらい。人づてに聞かないとだめというのが現実。
8	監査体制	文書管理ルールの承認や整合性はどのようにチェックしていますか。	事業場ルールが優先し、全社基準は形骸化。外資系では本国の承認が必要。

2．長期保存ストレージの最新動向

本章では、長期保存用途に使用する電子媒体・装置の動向及びそれらの特徴について記す。

JSOX 法の保管期限が 5 年以上を目安としていることから、概ね 5 年を超える保存期間を長期保存と称する。10 年、30 年等の保存に際しては、媒体の保存寿命とは別に、読出し装置の提供期間などを考慮し、ユーザ側として、媒体・装置間で、データ移行を行うマイグレーション計画を立案しておくことを推奨する。

2.1　長期電子媒体動向

2.1.1　光ディスク動向

民生用の Wtrite DVD/CD については、メーカや型式の差により媒体の保存寿命は大きく異なっている。このことについては、製造メーカとは異なる財団法人　コンテンツマネジメント協会のような機関によって、各社の DVD 媒体の保存寿命の実力調査、測定方法の検討などが行われている[2]。媒体の保存寿命はメーカ、媒体種別により大きく異なるので、データの長期保存には、安定した長期保存性をもった光ディスクの採用が望ましい。

現在のところ個々の製品について、その保存寿命を確認するには、メーカに問い合わせるしか見分ける手段はない。別の動きとして、米国の光ディスクの標準化団体である OSTA（Optical Storage Technology Association）とテラバイト光メモリ研究推進機構（略称　Terabyte Optical Memory Consotium TBOC）では、30 年の寿命を持つ媒体のテスト規格を策定し、ユーザの長期保存ニーズに答えようと DVD の ISO 規格化の推進を行っている。

適合媒体には、ロゴマークも付与することを検討している。これは、従来から ECOM が光ディ

スクメーカに要望していた事項であり、早期の ISO 化を期待する。

また、本規格を先取りした DVD 媒体、対応 DVD ドライブの販売も開始されている。

ブルーレーザを使用した Blu-Ray、HD DVD は現在のところ民生対応を主としており、業務用の保存媒体として採用するには時期的に拙速の感がある。

2.1.2 磁気テープの動向

これまでのテープ保存寿命は、メーカ独自の評価であり、評価方法・評価内容などが非公開であり、DVD に比べると一歩遅れた取り組みに見えた。ECOM からは、昨年（2006 年度)、これらのユーザへの公開の必要性を財団法人電子情報技術産業協会（JEITA）磁気記録媒体標準化グループ殿に申し入れている。

今年度、同グループから、媒体寿命評価 SWG を 2006 年秋に、新設し、情報処理用磁気テープの寿命予測について、媒体メーカ（イメーション（株)、ソニー（株)、TDK（株)、日立マクセル（株)、富士写真フイルム（株））を中心に検討を進めているとの説明があった。同 SWG の活動方針を以下に紹介する。

(1) 現在、主流のシステムである LTO G3 媒体を用い、参加媒体メーカが協働して具体的な保存データを取得する。
(2) システムの寿命、OS 及び Application ソフトウェアの互換性寿命等を考えると、ユーザが安全かつ安心して、一つの媒体にデータを保管して貰える目安は 10 年と考えられることから、媒体として、10 年以上の保存は問題ないことを確認する。
(3) 10 年以上の長期に渡り、データを保存する必要があるユーザに対しては、10 年を目安に新しいシステムにデータをコピーすることを推奨する。

尚、使用環境温度は 25℃であり、コンピュータマシンルームでの使用を想定していると推定する。

2.1.3 磁気ディスクの動向

磁気ディスクの使用にあたっては、障害対応の観点から、RAID の使用は最低限必要である。

また、一般に、磁気ディスク及びそれを組み込んだ RAID システムの装置寿命は 5 年程度であり、データ移行計画を立てておく必要がある。

内部統制、コンプライアンスの観点から、上位システムからデータの保存期間を設定し、その間のデータの更新、削除を許可しないタイプ（一種の WORM ストレージ）の RAID システムの販売機種も増えてきている。例として、EMC の Centera、日立製作所の Hitachi Contents Archive Platform、NetApp 社 Filer SnapLock などがある。

このようなシステムにおいては、保管期間が装置寿命を超える場合、なんらかのデータ移行手段を備えていることが必要である。当 WG としても次年度はこの観点での調査を進めて行く。

2.1.4 長期保存におけるストレージの選定に関する考察

上記、ストレージ動向を踏まえ、現状での長期保存に適したストレージを表 3.2.1 に示す。

光ディスクは可搬性重視の用途に、磁気テープ、磁気ディスクはコンピュータ室でのデータの

集中保存用途に用途が分かれてきている。

表 3.2.1 長期保存に適したストレージ

No	媒体・装置種別		RAW		メカ的、電気的リスク対応	WORM タイプ	可搬性	保存・保管期間	想定使用環境
			書込み品質チェック	ディフェクト管理					
1	長期保存用光ディスク（ISO 化推進中）	DVD-RAM	○	○	△媒体面露出	×	◎	30 年	一般事務室
2	磁気テープ	LTO	○	○	△ヘッド接触	△	○	10 年	コンピュータマシン室
3	磁気ディスク	RAID	○	○	○冗長化でカバー	×	×	5 年	コンピュータマシン室
4	WORM 型磁気ディスク	RAID	○	○	○冗長化でカバー	○	×	5 年	コンピュータマシン室

また、各ストレージの特性（容量、アクセス時間、転送速度、消費電量、コスト）を比較して表 3.2.2 に示す。昨今は、環境側面もあり、消費電力も注目されている。

導入コスト面からすると光ディスクは優位であり、スモールオフィスやデータ交換に向いていると考えられる。データ量が多い場合は、磁気ディスク、磁気テープライブラリなどが向いているが、磁気テープライブラリは磁気ディスクに比べ、アクセス速度が遅いので、超大容量でアクセス頻度の低いデータ群への適用が考えられる。

尚、磁気ディスク RAID については、バックアップは必須であり、バックアップ装置として、磁気ディスク RAID を使用する場合と磁気テープライブラリを使用するケースがある。

災害対応などを考えると、バックアップデータの遠隔地保管を行っておくことを推奨したい。

表 3.2.2 長期保存に適したストレージの特性比較

No	媒体･装置種別		容量	アクセス時間	転送時間	消費電力	コスト
1	長期保存用光ディスク	DVD-RAM	小	小	小	小	小
2	磁気テープ	LTO	中	中	大	小	中
3	磁気テープライブラリ	LTO	大	大	大	小	大
4	磁気ディスク（WORM 型含む）	RAID	大	小	大	大	大

引用・参考文献

[1] 山崎久道・黒済晃・伊藤充「わが国に文書管理の現状と課題に関する考察－製造企業に対するインタビュー調査を通して－」記録管理学会 2006 年　研究大会、レコード・マネジメント No.52、pp.48～75（2006）

[2] コンテンツマネジメント協会「長期保存のための光ディスク媒体の開発に関するフィージビリティスタディ報告書－要旨－」2007 年 3 月

付　録

オーストリア電子政府法

オーストリア電子政府法

公共団体との電子通信促進規定に関する連邦法

(Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz – E-GovG)

2004 年オーストリア連邦法令官報第 1 部第 10 号で公告された法律第 1 編

2004 年 3 月 1 日施行

目次

第 1 章

法律のねらいおよび目的

1. (1) 本連邦法は、法的に関連する電子通信の促進を目的とする。公共団体への提出行為時に、公共団体との電子通信は、多様な通信手段間[YM1]における選択自由の原則を考慮して促進されるべきである。

(2) 第 1 条の規定の目的の達成に向けて、法的保護の強化ために、自動化されたデータ処理の使用増加に伴う危険に対処する特別の技術手段が生み出されるものとし、他の防止手段による適切な保護措置が提供されていないところの実装がなされるものとする。

(3) 本連邦法の目的の実現に関して、遅くとも 2008 年 1 月 1 日までに、手続きの情報または電子的サポートを提供する公式インターネット・サイトを、ワールドワイド・ウェブへのアクセスに関する国際標準に準拠した方法（障害者による制約のないアクセスを含む）で確実に構築する措置が講じられるものとする。

第 2 章

公共団体との電子通信における識別および認証

定義

2. 本法律の本章において、以下の定義を適用する。

1. 「識別(Identity)」 他者から区別するためにとりわけ適したデータ（具体的には、氏名、出生日、出生地だけでなく、例えば企業名や（英）数字表示など）による特定人（データ主体者、本条 7 号）の指定。

2. 「一意識別(Unique identity)」 データ主体者が他のすべてのデータ主体者から誤りなく識別されることを可能にする、一つまたは複数の特徴による特定人（データ主体者、本条 7 号）の指定。

3. 「履歴識別（Recurring identity）」 一意識別(Unique identity)によらずに、以前の出来事（以前の提出行為など）の参照により人の認識を可能にする方法での特定人（データ主体者、本条 7 号）の指定。

4. 「識別行為（Identification）」 身元の確認または認識に必要な過程。

5. 「真正性（Authenticity）」 言明者または行為者と称する者が実際の実行者であるという意味における、意図または行為の言明の真正性。

6. 「認証（Authentication）」 真正性（Authenticity）の確認または認識に必要な過程。

7. 「データ主体者（Data subject）」 法律関係または経済関係の目的で識別された自然人、法人またはその他団体、機構。

8. 「ソース識別番号（sourcePIN）」 自然人、法人およびその他データ主体者の識別に使用される番号であり、誤りなく識別対象データ主体者を特定しうるもの、さらに自然人の場合には、（民間）セクター用個人識別子(ssPIN)（第 9 条および第 14 条）を生成する基礎となるもの。

9. 「sourcePIN 登録」 データ主体者の一意識別(Unique identity)に使用される登録であり、ソース識別番号(sourcePIN)の生成（必要な場合）に使用される技術要素を含む。

10. 「市民カード」 異なる技術要素で実行されたか否かに無関係な論理ユニットであり、電子署名を、識別リンク（identity link）（第 4 条 (2) 項）ならびに関連セキュリティ・データおよび機能に加えて、代理に関する既存データと結合する。

識別(Identity)および真正性（Authenticity）

3. (1) 「2000 年データ保護法（Datenschutzgesetz 2000）」（BGBl. I[7] 1999 年第 165 号）の第 5 条 (2) 項の意味における公共セクター管理者との電子通信において、「2000 年データ保護法」第 1 条 (1) 項の意味における秘密性に保護権益が存在する個人データへのアクセス権（「2000 年データ保護法」第 4 条 1 号）が付与されるのは、アクセス要求者が一意識別(Unique identity)され、その要求の真正性（Authenticity）が確認された場合に限る。かかる確認は、電子的に証明されうる形態で提供されなければならない。履歴識別（Recurring identity)のみが可能な場合、アクセスが許可されるのは、アクセス要求者が当該識別を使用して自ら提供した個人データに関するものに限る。

(2) そのほか、人の識別行為（Identification）を公共セクター管理者との通信で要求することができるのは、そのことが管理者の正当な権利に優先して必要とされる場合、とりわけ、法によって管理者に任命された職務の実行に不可欠な要件である場合に限る。

「市民カード」機能

4. (1) 市民カードは、公共セクター管理者が構築した市民カード使用の技術環境の手続きにおいて、提出行為人の一意識別(Unique identity)、および電子的提出行為の真正性（Authenticity）確認の役割を果たす。

(2) 市民カードの正当な所有者である自然人の一意識別(Unique identity)は、当該者の市民カードで識別リンク（identity link）の方法により実行される。すなわち、sourcePIN 登録機関（第 7 条）は、電子署名によって、市民カードで所有者と識別された自然人が一意識別(Unique identity)のために特定のソース識別番号（sourcePIN）を割り当てられたことを確認する。代理の場合における識別に関しては、第 5 条を適用する。

(3) 識別リンク（identity link）は、sourcePIN 登録機関、または当該機関に代わる他の機関もしくは他の適切な団体（第 5 条に基づき制定される規則で、より詳細に規定する）が市民カードに入力する。団体の適否は、要件とされる技術およびその使用に必要な専門技能の有無、ならびに法的枠組順守の信頼性の有無に基づき評価される。

(4) 市民カードを使用した提出行為の真正性（Authenticity）は、市民カードに含まれる電子署名によって確認される。

(5) 必要に応じて、第 1 条から第 4 条の細則は、所管連邦大臣の同意で制定される連邦首相規則に規定される。連邦州（*Länder*）および地方自治体（地方自治体連合および市町村連合（*Gemeindebund* および *Städtebund*）で代表される）は、当該規則制定前に協議を受けなければならない。

市民カードと代理

5. (1) 代理人による提出行為に市民カードを使用する場合、代理人の市民カードに代理の許可の証明が入力されなければならない。これは、以下の場合に行われる。

1. sourcePIN 登録機関が既存の代理権限の証拠を提示された場合、または法定代理の場合に、sourcePIN 登録機関が、代理人による申請に応じて、代理人の市民カードに本人の sourcePIN および代理権の存在（関連情報や有効期間を含む）の証明を入力する場合。

2. 特に代理権の証明を要さない職業代理人（*berufsmäßige Parteienvertretung*）の場合に、sourcePIN 登録機関が、代理人の市民カードに、電子的に証明されうる形態で、職業代理人としての行為権限を有するという事実の証明を入力する場合。それらの場合において、本人は、第 10 条 (2) 項に従って電子的に識別される。

(2) 第 4 条 (3) 項は、第 1 条で必要とされる市民カードの入力に準用する。

(3) 地方自治体が当該業務を提供する場合、この目的の権限を特に与えられた職員（*Organwalter*）は、要求があれば、職権にかかわらず、自己の実質的および組織的権限にかかわりなく、市民カードが使用可能な手続きにおいて、要求者のために申請書を提出することができる。申請は、職員の市民カードを使用して提出しなければならず、申請当事者は、第 10 条 (2) 項に従って電子的に識別される。市民のために申請を提出する職員の一般的権限は、職員の市民カードの署名用の証明書から明白でなければならない。一方、市民から出された特定の指示は、書面による申請の謄本の形で文書化され、「1991 年行政手続き一般法（Allgemeines Verwaltungsverfahrensgesetz 1991）」第 14 条に従い当該自治体に保管される。

[7] 「BGBl.」とは Bundesgesetzblatt（オーストリア連邦法令官報）の略称。

ソース識別番号(sourcePIN)

6. (1) 当事者は、市民カードのソース識別番号（sourcePIN）によって一意識別(Unique identity)される。

(2) 中央住民登録（CRR）に登録を要する自然人については、ソース識別番号(sourcePIN）は、当該個人の中央住民登録の登録番号（CRR 番号）（BGBl. 1992 年第 9 号掲載「1991 年登録法（Meldegesetz 1991）」第 16 条 (1) 項）から派生されるものとし、強力な暗号を使用して保護されなければならない。CRR への登録を要しない自然人のソース識別番号(sourcePIN）は、補助登録（第 4 条）の登録番号に基づくものとする。ソース識別番号(sourcePIN）生成のための CRR 番号の使用は、「1991 年登録法（Meldegesetz 1991）」第 16 条 a における中央住民登録データの使用とはみなされない。

(3) 法人、およびその他自然人以外については、ソース識別番号(sourcePIN）は、商号登記の登記番号（BGBl. 1991 年第 10 号掲載「商号登記法（Firmenbuchgesetz）」第 3 条 1 項）、中央団体登記の登記番号（ZVR 番号）（BGBl. 2002 年第 66 号掲載「2002 年団体法（Vereinsgesetz 2002）」第 18 条 (3) 項）、または補助登録で割り当てられた登録番号（第 4 条）とする。

(4) 中央住民登録、商号登記または団体登記に登録を要さない者は、自らの申請により、または第 10 条 (2) 項が適用される場合にはデータ・ファイル管理者の要求で、sourcePIN 登録機関（第 7 条）によって、一意識別(Unique identity)の電子的確認を目的として補助登録に登録される。自然人の場合には、これは、「1991 年登録法（Meldegesetz 1991）」第 1 条 (5a) 項の意味における識別データと同等のデータの証明が提供されることを条件とし、その他のデータ主体者の場合には、法的に有効な名称など法的存在の証明が提供されることを条件とする。この補助登録は、自然人部門とその他のデータ主体者部門とに分けられる。他人の代理人として行為する公共団体についてもまた、自然人以外のデータ主体者に関する補助登録の部門に入力することができる。補助登録への登録に必要なデータ証明の提出先とすることができる国内または国外の団体、および市民カードに識別リンク（identity link）を入力する権限を有する団体は、第 4 条 (5) 項に基づき制定される連邦首相規則に規定する。さらに、当該規則は、補助登録の登録に関して身元を証明するため、および代理の証明を入力するために、sourcePIN 登録機関および当該機関に指示された団体に連絡することによって生じた費用について、支払われるべき範囲を定める。公共団体（*Gebietskörperschaften*）は、いかなる場合においても、かかる費用の支払義務を免除される。

(5) 第 3 条に基づき要求されるデータ証明が提供されない場合、履歴識別（Recurring identity)を確認する目的に限定して、要求者は、sourcePIN 登録機関から代用 sourcePIN の提供を受けることができる。代用 sourcePIN は、当該人に関するデータ（氏名、出生日および出生地または証明書の一連番号など）に基づき生成され、全体として当該人を十分に識別しうることが求められる。番号は、代用 sourcePIN として認識することが可能でなければならない。

(6) ソース識別番号(sourcePIN）（自然人の場合には強力な暗号を使用）および代用ソース識別番号(sourcePIN）（自然人の場合にはデータのハッシュ値および追加的に強力な暗号を使用）を生成するために sourcePIN 登録機関が適用する数学アルゴリズムは、sourcePIN 登録機関が決定し、使用される暗号鍵を除いて、インターネット上で公開しなければならない。

sourcePIN 登録機関

7. (1) sourcePIN 登録機関はデータ保護委員会であり、データ・ファイルへの登録の方法によりその職務を遂行する。

(2) 補助登録の維持、ソース識別番号(sourcePIN）の生成、ならびに第 4 条、第 9 条および第 10 条が適用される手続きの実施において、sourcePIN 登録機関は、自然人に関する限りにおいては連邦内務省の業務、その他すべてのデータ主体者に関する限りにおいては連邦財務省の業務と連携を図るものとする。sourcePIN 登録機関としてのデータ保護委員会と、業務提供者としての連邦内務省または財務省との間の職務配分を決定する詳細規定は、データ保護委員会との協議後、連邦内務大臣または連邦財務大臣との同意により、連邦首相規則に規定される。

データ・ファイルにおける一意識別(Unique identity)

8. 公共セクター管理者のデータ・ファイルにおいて、市民カードスキームのフレームワークにおいて自然人の識別を表示することができるのは、セクター用個人識別子(ssPIN)（第 9 条）の形態に限られる。自然人以外の者に関しては、ソース識別番号(sourcePIN）を一意識別(Unique identity)のために保存することができる。

セクター用個人識別子(ssPIN)

9. (1) セクター用個人識別子(ssPIN)は、関係自然人のソース識別番号(sourcePIN)から派生される。識別目的での当該識別子の使用は、個人識別子が使用されるデータ・ファイルによって行われる連邦活動の当該部門に限定される(セクター用個人識別子(ssPIN))。データ・ファイルが割り当てられる連邦活動の具体的な部門は、第17条(2)項1号から3号または(3)項が適用されない限りにおいて、「2000年データ保護法(Datenschutzgesetz 2000)」第17条(2)項6号で規定されている「標準およびモデル・データ処理規則(Standard- und Muster-Verordnung)」におけるそれぞれのデータ・ファイル登録の登録で明示される。

(2) セクター用個人識別子(ssPIN)を生成するために、連邦活動の部門は、関連する状況が確実に同一部門内に含まれるような方法で、また、同一地域内で矛盾するデータ使用(「2000年データ保護法(Datenschutzgesetz 2000)」第6条(1)項2号)を防止するように、範囲を定められる。それらの地域の詳細および範囲は、連邦首相規則で決定する。連邦州(*Länder*)および地方自治体(地方自治体連合および市町村連合で代表される)は、当該規則制定前に協議を受ける。

(3) ssPINを生成するために適用する数学アルゴリズム(ソース識別番号(sourcePIN)および部門コードを使用したハッシュ機能)は、sourcePIN登録機関が決定し、使用される暗号鍵を除いて、インターネット上で公開しなければならない。

セクター用個人識別子(ssPIN)の生成

10. (1) 個人のssPINは、公共セクター管理者が構築した市民カード使用環境で電子的手続きにおいて、市民カードを使用して生成されるものとする。

(2) セクター用個人識別子(ssPIN)を、市民カードを使用せずに生成することができるのは、sourcePIN登録機関による場合に限り、これが認められるのは、公共セクター管理者のデータ・ファイルにおけるssPINに基づく一意識別(Unique identity)が、「2000年データ保護法(Datenschutzgesetz 2000)」に従って個人データを処理または伝送するために必要とされる場合に限る。これには、とりわけ、行政協力、データ主体者の要求によるデータ取得、または職業代理人による公共団体への提出の場合が含まれる。要求を行う団体が権限者として行為する権限を有さない部門のssPIN要求の場合(外部ssPIN)、または職業代理人によるssPIN要求の場合、第13条(2)項に従って暗号化されたssPINに限って利用可能とされる。

(3) 第2条に基づく職業代理人に関するセクター用個人識別子(ssPIN)の提供費用の支払いもまた、第4条(5)項に基づき制定される規則を適用する。

通信におけるセクター用個人識別子(ssPIN)の開示

11. セクター用個人識別子(ssPIN)は、データ主体者または第三者に対する通信の中に含むことはできない。同一の対象に関して、かかる通信を管理者の記録に対応させることは、参照番号など他の手段で図られるものとする。

自然人のソース識別番号(sourcePIN)の保護

12. (1) ソース識別番号(sourcePIN)が公衆データ(商号登記番号、中央団体登記番号など)でない限り、その秘密性は、以下の市民カードスキームの基準による特別な保護に従う。

1. CRR番号から派生し、自然人のソース識別番号(sourcePIN)として使用される番号は、市民カード内に限り、また、識別リンク(identity link)関連または代理権限の事実提示目的に限り、恒久的に記録することができる。

2. 自然人のソース識別番号(sourcePIN)は、要求があれば必ず、sourcePIN登録において生成される。ただし、それらは、生成および即時処理に必要な期間を超過して保存されてはならない。

3. ssPIN生成目的で自然人のソース識別番号(sourcePIN)を使用した場合、生成過程外でソース識別番号(sourcePIN)を保存することはできない。

4. 民間セクター管理者は、ソース識別番号(sourcePIN)に基づく民間セクターPINの生成(第14条)を実行することはできない。

(2) ソース識別番号(sourcePIN)をセクター用個人識別子(ssPIN)の生成のために使用することができるのは、以下の場合に限る。

1. データ主体者が自己の市民カードを使用して協力する場合。その都度、データ主体者は、適宜、市民カード機能の電子的活性化について通知を受けなければならない。

2. データ主体者の協力を得ずに、sourcePIN 登録機関が第 10 条および第 13 条 (2) 項の細則に従って使用する場合。

個人識別子の保護強化

13. (1) セクター用個人識別子(ssPIN)は、ソース識別番号(sourcePIN) から不可逆的に派生させて生成される。連邦活動は透明性を有するものであるため、これは、公共団体を代表する職員としての活動に関連してのみ使用されるセクター用個人識別子(ssPIN)には適用しない。

(2) 第 10 条 (2) 項に基づき、データ主体者の一意識別(Unique identity)を目的とした sourcePIN 登録機関へのセクター用個人識別子(ssPIN)の要求が許可される場合、sourcePIN 登録機関は、外部 ssPIN (すなわち、要求当事者が権限者資格を有さない部門の ssPIN) に関しては、暗号化された形態に限って ssPIN を利用可能とすることができる。かかる暗号化の形態は、以下を確実にするものでなければならない。

1. 自己のデータ・ファイルにおいて、復号化された形態での ssPIN の使用が許される管理者だけが、それを復号できること (第 3 条)。

2. 要求当事者が知識を有さない追加的可変データが暗号化基盤に包含された結果、ssPIN が、暗号化された形態においてであっても、データ主体者に関するいかなる情報も供給できないこと。

(3) セクター用個人識別子(ssPIN)を暗号化されていない形態でデータ・ファイルに保存することができるのは、第 9 条 (2) 項に従い成立する規則に従ってデータ・ファイルが割り当てられる部門向けコードを、ssPIN を生成するために利用した場合に限る。

第 3 章

民間セクターにおける市民カード機能の使用

民間セクター用個人識別子

14. (1) 民間セクター管理者との電子通信 (「2000 年データ保護法 (Datenschutzgesetz 2000)」第 5 条 (3) 項) において自然人を識別するために、市民カードを使用して、データ主体者のソース識別番号(sourcePIN) および部門コードとしての管理者のソース識別番号(sourcePIN) から生成されたハッシュ値から、特定の番号を派生させることができる (民間セクター用個人識別子、民間セクターPIN)。これは、民間セクター管理者が、市民カードが使用可能であり、かつ管理者のソース識別番号(sourcePIN) を民間セクターPIN 生成用の部門コードとして利用可能な技術環境を構築することを条件とする。

(2) 民間セクター管理者は、自己のソース識別番号(sourcePIN) を部門コードとして使用して生成した民間セクター用個人識別子に限って、保存および使用することができる。

ソース識別番号(sourcePIN) および個人識別子の保護の保証

15. (1) 民間セクター用個人識別子を生成できるのは、市民カードに基づいてデータ主体者の協力が得られる場合に限り、その都度、データ主体者に、それらの機能の電子的活性化について適宜通知しなければならない。

(2) データ主体者のソース識別番号(sourcePIN) は、民間セクターPIN の生成中いつでも、市民カード機能によって、民間セクター管理者に提供しないことができる。ただし、データ主体者が使用する識別リンク (identity link) の正確性の電子的証明は、「1991 年登録法 (Meldegesetz 1991)」第 16 条 (1) 項に基づく中央住民登録所にアクセス要求を提出することによって可能である。

第 4 章

データの電子的確認

自営業者の経済活動に関する情報

16. (1) 自営業活動の性質、および当該活動のための職業的要件の充足についての電子的確認は、「連邦財務法典 (Bundesabgabenordnung)」第 114 条 (2) 項に基づく文書登記所から得ることができる。

(2) 公共セクター管理者が関与する手続きにおいて、第 1 条で言及するデータの確認が要求される場合は、データ主体者自身が文書登記所によって電子的に署名されたコピーを提出することによって、それを提供すること

ができる。または、データ主体者の要求に応じて、管理者が文書登記に電子的にアクセスすることによって、それを入手することができる。かかるデータ取得の法的要件が充足される場合、公のルートを通じて確認を得ることが認められる。

個人の地位および国籍に関するデータ

17. (1) 個人の地位および国籍に関して中央住民登録に保存されたデータの正確性が、地方登録機関による適切な文書（標準文書）の検査で確認された場合、当該地方機関はその旨中央住民登録所に通知しなければならず、データ確認の事実は、適切な電子的に判別可能な形態で中央住民登録に記録される。データ主体者は、適切な文書を提出することによって登録機関に登録データの正確性の証明を提供した場合、住民登録手続き外であっても、かかる情報の入力を要求することができる。

(2) 他の機関が、手続きにおける予備問題として、登録データである個人の地位または国籍に関するデータの正確性を判断しなければならない場合、当該機関は、当事者がデータ取得に同意すること、または公的ルートを通じての当該取得が法律で認められていることを条件として、そのことについて中央住民登録所に電子的要求を提出することができ、その要求は、「登録法（Meldegesetz 1991）」第 16 条 a (4) 項に従って取り扱われる。

(3) データ主体者は、以下によって、確認された登録データの電子的有用性を利用することができる。

1. 第 1 条の意味における標準文書の提出が必要とされる手続きにおいて、中央住民登録所に要求したデータ取得に同意すること。または、

2. 電子的に公式署名（第 19 条）され、個々の登録データの正確性が確認された旨記載された登録の確認を、中央住民登録所に要求すること。

その他のデータ

18. 公共団体または公権力を付与された者は、自己の権限または管理領域内で保存するデータの電子的確認を発行する準備ができている範囲を、インターネット上で公開しなければならない。公的ルートを通じたデータの取得が法律で認められていない場合において、個人データに言及する確認を発行することができるのは、当事者本人、またはデータ主体者の同意を有する第三者に対するものに限る。

第 5 章

電子記録保存の特性

公式署名

19. (1) 公共団体の電子署名たる公式署名は、「署名法（Signaturgesetz）」の意味における電子署名であり、その特性は、署名用の証明書における適切な属性によって示される。

(2) 公式署名は、文書が公共団体から発せられたものであるという事実の認識を容易にする役割を果たす。それゆえ、かかる署名の使用は、第 3 条規定の詳細条件に従い、公共団体が電子的に署名するとき、または公共団体が交付する文書を作成するときに限定される。

(3) 公式署名は、公共団体がインターネット上で自己のものとして安全な形態で公開する画像によって、電子版文書に表示される。画像に加え、電子版文書にはまた、署名の実効値とともに、少なくとも一連番号ならびに証明書サービス提供者の名称および国名を示さなければならない。文書全体の表示を署名が確認できる形態に変換することによって、署名を確認することが可能でなければならない。表示から電子文書を検索するために必要な追加情報も同様に、文書の発行者によって安全な形態でインターネット上に公開されなければならない。

印刷出力物の証明力

20. 書面印刷された公共団体の電子文書は、文書が公式署名され、かつ、文書の電子版を復元することによって印刷書式においても署名を確認することが可能である場合、真正であると推定される。そのために、文書には、復元可能である旨を記載し、印刷文書を電子的形態に再変換する手順および適用可能な検証メカニズムを説明したインターネット上の情報源への参照を含まなければならない。

電子記録の提出

21. (1) 公共団体が他の公共団体への記録の提出を求められた場合、かつ、それらの記録が電子的に生成および承認された場合、提出義務は電子的な原本に遡って適用される。これは、とりわけ、完全に電子的に操作された

ファイル処理および管理システムで保存された記録に適用する。文書は、標準書式で提出されなければならない。

(2) 標準書式とは、文書の保管が想定される期間において、第三者の観点からも可能な限り最高の可読性を保証する、利用可能な最新技術を使用した電子書式である。

(3) 電子記録の提出先の公共団体が、電子配信サービス機関に自己あての通信を受領する権限を与えた場合において、とりわけ提出の証明が必要とされる場合において、記録は、当該機関へも提出することができる。この場合において、配信サービス機関のサーバーから文書が検索可能である旨の通知が電子配送された翌日に、文書を提出したとみなされることを条件として、「文書事業法（Zustellgesetz）」第 3 章を準用する。

第 6 章

罰則

ソース識別番号(sourcePIN)、セクター用個人識別子(ssPIN)または公式署名の使用禁止事項

22. (1) ある行為が、裁判所の管轄に属する刑事犯罪を構成しない限りにおいて、または行政違反に関するその他の規定でより重い刑罰を伴わない限りにおいて、以下の者は、地方行政機関の科す罰金 EUR 20 000 以下の行政違反に処する。

1. 違法にデータ主体者の個人データを入手するために、第 2 章および第 3 章の規定に反して、自然人のソース識別番号(sourcePIN) またはセクター用個人識別子(ssPIN)を使用目的で入手した者。

2. 他の民間セクター管理者のセクター用個人識別子(ssPIN)を、権限なく保存または使用した者。

3. 民間セクターの他の管理者に、「2000 年データ保護法（Datenschutzgesetz 2000）」第 8 条が禁止する方法で、自己のソース識別番号(sourcePIN) から派生した民間セクター用個人識別子を提供した者。

4. データ主体者の登録住所に関するデータを第三者に供給するために、民間セクター用個人識別子を使用した者。

5. 第 19 条 (2) 項に違反して公式署名を使用した者、または使用を企てた者。

(2) 第 1 条の意味における行政違反に関連して入手した目的物について、没収（「1991 年行政違反法（Verwaltungsstrafgesetz 1991）」第 10 条、第 17 条および第 18 条）を科すことができる。

(3) 違反地の公共団体は、本条 1 号および 2 号に基づく決定を行う地域管轄権を有する。

第 7 章

暫定条項および最終条項

言語上の平等な取扱い

23. 自然人に言及する本条項の用語が男性形のみで表現されている場合、それらは男性および女性に平等に適用する。

施行

24. 本連邦法は、第 6 章を除き、2004 年 3 月 1 日から施行する。第 6 章は 2005 年 1 月 1 日から施行する。

暫定条項

25. (1) 2007 年 12 月 31 日まで、管理上の署名もまた、市民カード機能に関連して使用され、安全な署名と同様に取り扱われる。管理上の署名とは、それらが必ずしも、安全な署名の作成に使用されるデータの生成および保存の条件すべてを充足しない場合、および必ずしもクォリファイド証明書（Qualified Certificate）に基づかない場合であっても、許容される使用目的の範囲内で、十分な安全性を提供する署名をいう。本連邦法のために、管理上の署名が実現すべき安全および組織条件は、連邦首相規則に規定する。

(2) 憲法以下の法律が、公権力（*Hoheitsverwaltung*）を行使する公共団体との通信において安全な電子署名の使用を明示的に要求する場合、第 1 条で言及する暫定期間の終了までは、管理上の署名が使用された場合であっても、当該条件は充足されたとみなされる。

規則の制定および施行

26. 本連邦法に基づく規則（および改正規則）は、規則によって実行される法規定の公布翌日から施行する。ただし、規則は、当該法規定より前に施行することができない。

参照

27. 本連邦法において他の連邦法に参照がなされた場合、それらの法律は、該当時点における有効な法律に適用される。

実施

28. 以下の機関は、本連邦法を実施する権限を有する。

    1. 第 4 条 (5) 項に関しては、他の所管連邦大臣の同意を得て任務を行う連邦首相。

    2. 第 7 条 (2) 項に関しては、自然人のソース識別番号(sourcePIN) に関する業務の場合は連邦内務大臣の同意、自然人以外のソース識別番号(sourcePIN) に関する業務の場合は連邦財務大臣の同意を得て任務を行う連邦首相。

    3. 第 9 条 (2) 項に関しては、連邦首相。

    4. 第 15 条 (2) 項の最終文および第 17 条に関しては、連邦内務大臣。

    5. 第 16 条に関しては、連邦財務大臣。

    6. 残余に関しては、当該実施が連邦政府または連邦州（*Länder*）政府の管轄でない限りにおいて、所管連邦大臣。

メンバリスト

事務局

前田　陽二	次世代電子商取引推進協議会

顧問（五十音順）

大山　永昭	東京工業大学
菅　　知之	関西大学
平田　健治	大阪大学大学院
辻　　秀一	東海大学
松本　　勉	横浜国立大学大学院
米丸　恒治	神戸大学大学院

編集メンバ（五十音順）

役　割	氏　名	所　属
主　査	木村　道弘	日本電気株式会社
副主査	漆嶌　賢二	エントラストジャパン株式会社
副主査	松本　　泰	セコム株式会社
副主査	宮崎　一哉	三菱電機株式会社
幹　事	榎本　　尚	エヌアイシー・インフォトレード株式会社 （旧　花王インフォネットワーク株式会社）
幹　事	後藤　　淳	日本電気株式会社
幹　事	佐藤　雅史	セコム株式会社
幹　事	溝上　卓也	日立ソフト株式会社
委　員	石原　達也	東芝ソリューション(株)
委　員	小林　信博	三菱電機株式会社
オブザーバ	西川　康男	ARMA

メンバ（五十音順）（上記以外）

役　割	氏　名	所　属
委　員	今井　秀和	株式会社 PFU
委　員	斉藤　　聡	株式会社リコー
委　員	高橋　健蔵	NTT データ株式会社
委　員	戸田　安彦	NTT データ株式会社
委　員	中村　克巳	三菱電機情報ネットワーク株式会社
委　員	橋本　正一	日本電信電話株式会社
委　員	林　　良一	NTT コミュニケーションズ株式会社

電子署名の普及に関する活動報告

平成 20 年 3 月発行

発　行　　次世代電子商取引推進協議会

発行所　　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園三丁目 5 番 8 号
機械振興会館　3 階
TEL：03(3436)7500

この資料は再生紙を使用しています。