ISBN978-4-89078-673-2 C2055

電子署名普及に関する活動報告2008

平成21年3月

次世代電子商取引推進協議会

# 電子署名普及に関する活動報告2008

平成21年３月

次世代電子商取引推進協議会

# 序文

次世代電子商取引推進協議会（ECOM）電子署名普及ワーキンググループ（WG）では、平成 12 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。平成 20 年 3 月には ECOM が作成し提案してきた次の 2 つの規格が審査を経て登録された。

・ X5092：2008 CMS 利用電子署名（CAdES）の長期署名プロファイル
・ X5093：2008 XML 署名利用電子署名（XAdES）の長期署名プロファイル

これと並行して、平成 18 年より ECOM は ETSI（欧州通信規格協会）のアソシエイト会員となり、TC ESI（電子署名基盤技術委員会）を舞台に、これらの JIS を国際標準にするための情報交流を進めてきた。

平成 20 年度は、WG 活動としてこれらの成果を踏まえ以下の 3 つのテーマに取り組んだ。

・ 長期署名プロファイルの普及に必要だが、ほとんど未検討の技術項目、例えば「署名ポリシー」など、の洗い出しと整理を行った。

・ 電子商取引のみならず電子記録（電子文書や電子データ）に署名をつけて保存し管理する仕組みは重要である。そこで、紙から電子データへの管理に移行する場合の課題を収集し整理するため、ECOM 会員各社にアンケートによる文書管理の実体調査を行った。

・ 電子署名、認証技術に関係する技術の関連をわかりやすく表現した技術マップを作成する目的で、EU で作成した標準化のための技術マップについて調査検討を行った。

また、国際標準化活動として、ETSI TC ESI および長期署名フォーマットの相互運用実証実験の企画運営のための専門家タスクフォース（ETSI STF351）に参加し技術協力するとともに、ISO/TC154 の総会では JIS の国際標準化提案を行った。

今年度の活動は、会員各位および国内の団体のご協力のもとに進めることができた。特に、文書管理ヒアリング・アンケートに回答頂いた ECOM 会員、ISO での提案に当たってご協力いただいた TC154 国内審議委員会の委員長並びに事務局、磁気テープ装置（MT）に関する最新技術情報をご提供いただいた 電子情報技術産業協会（JEITA）磁気記録媒体標準化専門委員会の皆様、OOXML の長期署名に関する情報をご提供いただいた国立情報学研究所の皆様に感謝する。

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 21 年 3 月

次世代電子商取引推進協議会

# 目　次

# まえがき

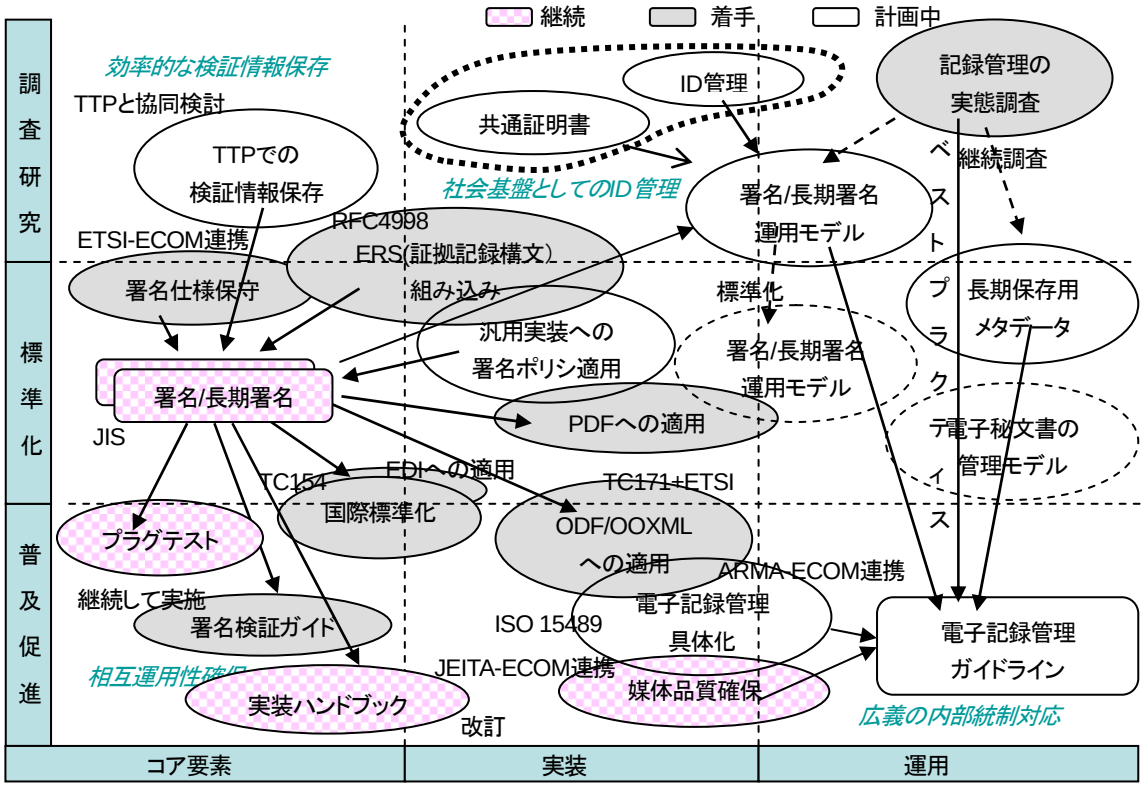
今年度は、電子署名普及活動に大きな前進があった。マイルストーンの国際標準化である。2008年11月にブラッセルで開催されたISO TC171の総会において、JIS規格となった長期署名プロファイルを新作業項目（NWI）として提案したい旨申し出て、ISO化に向けた第一歩を踏み出した。2009年5月にはNWIとして承認される見通しである。電子署名製品の国際的な相互運用性試験では、ECOM有志がETSIの特別タスクフォースに加わって準備を進め、JIS準拠製品の国際的な相互運用性を確認することができた。

長期署名仕様は常に進化しておりフォローは欠かせない。長期署名には幾つかのバリエーションがあり、既にJIS化されている基本的な方法のほかに、複数の文書にまとめて一つのアーカイブタイムスタンプを付与する証拠記録構文（ERS）も出てきた。ERSについてはJISに取り込む方向で検討を進めている。

電子署名利用に関しては、欧州における標準化状況や制度を調査し、マップ化して全体像を把握する作業に取り掛かった。狙いは中長期的な活動の指針作りである。

これ迄繰り返し述べてきたが、長期署名は、署名文書が長期に保存できて意味をもつ。記録媒体の劣化、文書ファイル後方互換性喪失、文書の誤廃棄や散逸から免れ、必要なときはいつでも文書を取り出せなければならないが、具体的な実現方法は各企業とも未だ手探り状況である。電子記録管理のガイドライン作りに向け、関連団体と連携した活動は欠かせない。

下図は、電子記録管理の確立に向けた今後のビジョンを表している。



本年度の活動報告は、3 部構成となっており、各部の概要は次の通りである。

第一部では、電子社会における電子署名と認証基盤の意味や意義を整理すると共に、個人を識別するための ID の管理について、エストニア、デンマーク、スロベニア、オーストリアなどの ID 管理で先行している諸国のモデルを比較し特徴をまとめた。

第二部は、2008 年 11 月に ECOM 会員企業に対して実施した“電子文書管理の実態”に関する調査の概要と分析結果をまとめた。また、従来に引き続き長期保存ストレージの動向について確認結果を付記した。

第三部は、長期署名の検証に関する実装の要点を解説としてまとめるとともに、ODF や OOXL の実装に対する長期署名の適用実験から明らかになった課題をまとめた。また、今後の拡張機能として、信頼点の管理や証拠記録構文（ERS）の導入に関する考察結果を記した。

なお、付録として、長期署名フォーマットの実証実験に関する国際活動、長期署名フォーマットプロファイルの国際標準化活動、PDF 長期署名に関する国際標準化活動など、電子署名普及ワーキンググループの国際標準化活動の記録を掲載した。

一山超えて展望が開けてきた。まだまだ課題は山積であるが、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　電子署名を利活用した安心･安全な電子社会を目指して

# 1. はじめに ― 電子署名をとりまく概況

◇電子署名をとりまく概況

IT（情報技術）は、さまざまな分野の経済成長や社会システムの効率化など社会に欠かすことのできない基盤となりつつある。こうした中、2001 年 4 月に電子署名法が施行されている。この電子署名法は、IT 技術、ネットワーク技術を背景とした本格的な電子社会を、便利で効率的であるのみならず、不正に強く透明性が高い社会を目指した法律として期待されていた。しかし、電子署名法が施行され 8 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」、「電子的な識別（Identification）や認証（Authentication）も含めて電子署名が検討されるべきではないか」、こうしたことが再度検討される必要があるだろう。

電子署名の普及の鍵は、技術的な問題以外にある。「紙と印鑑」の文化から「電子文書と電子署名」の文化へ、まずは、これまでの慣習の壁を越える必要がある。現在の社会は「紙と押印」を前提に非常に長い時間をかけて最適化されてきた。一企業内においても「紙と印鑑」から「電子文書と電子署名」への移行は、業務の本質的な変革が要求される。これが社会全体となると、更に制度も含めた本質的な変革が要求される。電子署名の普及にあたっては、効率的な電子社会へと移行させるために、これまで人々が「最適」と思ってきた実務の意識を変える必要がある。

ユビキタスネットワーク社会においては、無数のデバイスや様々なサービスが連携していく。こうした社会においては、様々な信頼関係や証明、様々な事象の証跡を保存するために、おびただしい数の電子署名が利用されていくと考えられる。これは、現在の電子署名法の適用範囲である自然人が行う電子署名とは限らない。こうした時代においては、「電子署名法」に代わる、新たな枠組みの検討が必要かもしれない。また、IT が社会の基盤となるほどに、法制度との整合性が求められ、技術開発に際しても社会システム化の視点が要求されていることとなろう。

以上を踏まえて、2 章では、電子署名や証明書の役割について改めて整理し、証明書による認証の枠組み（認証基盤）を構築することの意味、意義について説明する。

◇紙が前提の世界の限界

2008 年は、「紙と押印」を前提に最適化された社会の問題も表面化した年であった。以下のふたつの事件は、現在の社会の問題点をよく現している。

- 「元書記官による偽造判決書文」
- 「年金記録の改ざん問題」

「元書記官による偽造判決書文」は、地裁の書記官が、判決書文を偽造することにより振り込め詐欺に使われた口座から不正に預金を引き出したという事件であった。この元書記官は、「戸籍の偽装」、「債権者の偽造」、「口座の偽造」、「凍結解除の判決文の偽造」、「公印の偽造」を行ったとされている。また、「偽りの判決文に押した裁判所の公印は、市販のスタンプ作成キットで作った」と報道されている。市販のスタンプ作成キットで作られた（偽造された）公印が施された（偽造された）「凍結解除の判決文」は、4 つの地方裁判所に送付されたが、偽造が発覚したのは、凍結された口座である被害者からの問い合わせがきっかけだったとされている。これは、書類を送付されてきた地方裁判所は、判決文の真偽を検証する手段を持っていなかった事を意味する。

このように、簡単に偽造できる「押印」は、現社会において、社会の信頼の要として利用されている。実際の信頼は、非常に効率の悪いやり方を併用することにより、辛うじて保っているのが現状ではないだろうか。

「年金記録の改ざん問題」では、コンピュータ上に記録されているデータが改ざんされたと同時に、三文判による（紙の）書類の偽造や、元の証拠となる書類が「証拠が残らないように（紙文書を）シュレッダーで破棄した」とされている。そして記録の改ざんが最も多く行われたのは 10 年以上前とされている。改ざん問題だけではなく、もう少し広い範囲の「年金記録問題」では、長年にわたり、転記ミス等により非常に精度の悪いデータが蓄積されたことにより、収拾がつかなくなっているという深刻な問題がある。

この「年金記録の改ざん問題」を、情報システムの観点から見るに、「非常に効率が悪い」、「透明性に欠ける」、このふたつが問題なのではないだろうか。

こうした「改ざん」の問題を、紙文書から電子文書への移行も踏まえて解決するためには、「電子署名」の適切な利用と普及が欠かせないと考えられる。

◇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する。署名者自身は、その署名に利用する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に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、各種の公的な証明書等の信頼性、すなわち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、現在のところ、この公的

な証明書等の多くは紙文書ということになる。

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、既存の「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いったことは、既存の「社会的信頼の仕組み」に大きく依存する。

「紙と押印」を前提に最適化された社会から、電子文書やデジタルデータがより重要な社会への移行を目指して「社会的信頼の仕組み」自体を、よりIT社会に適合した合理的な仕組みに変革していく動きもある。欧州において情報化社会に対応するためのキーワードの一つに eIDM（electronic identity management）があるが、このeIDMは人や企業の識別を電子的に可能にする基盤を整備し、また、広く利用できる環境を整備しようとするものである。

こうした動向を示すことも念頭におき、3 章の「社会基盤としての ID 管理と電子署名」では、証明書の中に記載されている識別子としてのIDについて「エストニア」「デンマーク」「スロベニア」「オーストリア」の事例をあげて説明している。これらの国々は異なったID管理のモデルを採用しているが、共通していることは、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。

電子署名で利用する証明書は、この証明書が何を証明しているかが重要であり、また、電子署名が施された電子文書などのデジタルデータが長期に渡る証跡として効率的、かつ合理的に利用されるためには、「社会的信頼の仕組み」に基づいたID管理の考え方が重要になる。結局のところ、電子署名が有効に機能するためには、IT社会にふさわしい「社会的信頼の仕組み」を、まず確立する必要がある。

◇今後の社会

4 章では、「今後の認証基盤構築に向けた技術動向」として、「標準化」と「電子文書の長期保存」を取り上げている。ITが社会基盤化する中で、標準化の推進や相互運用性の確保ということの重要さを否定する人は少数であろう。しかし電子署名に関する標準化がわが国で十分進んでいるとは言いがたい状況にある。電子署名の標準化の難しさは、既存の商習慣とのギャップなどから、ビジネスとして利用できる標準を確立することが難しいことにある。こうしたことは、日本国内に限らない。そのため、標準化に対するビジョンの持ち方を含めて「欧州の標準化動向」を説明することにより、我が国の状況を説明することを試みている。

「年金記録の改ざん問題」に対応するための IT の課題は、ひとつは、ID 管理モデルの確立であり、もうひとつは、証拠性のある文書の長期の保存ではないだろうか。4 章のもうひとつのトピックとして「電子文書の長期保存」を取り上げている。ITの基盤化が本質的なものになるためには、「長期に渡るセキュリティ」に対応できる必要がある。「電子文書の長期保存」は、こうした課題に対応する要求であり技術である。

現状の（情報システムや制度の）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を強く引きずっている。電子化に対応する形で登場した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り、必ずしも「今後の社会」に相応しいものになっていないのではないだろうか。

次の時代の IT 技術を駆使した社会を構築するためには、IT 社会に適合した合理的な「社会的信頼の仕組みの再構築」を検討する必要がある。それと同時に、現在の電子署名法を中心とした電子署名の仕組みも見直し「電子署名の再構築」も検討する必要があるだろう。

安心・安全な電子社会を目指し、電子署名の更なる技術開発、法制度の整備などの努力が求められる。

# 2. 電子署名と認証基盤の意味と意義

前章で述べたように、現実社会でも偽造事件があとを絶たない。電子情報は紙と異なり改変が容易であり、今後の電子化の進展を考えると電子社会での偽造防止などに対する電子署名の必要性はますます高まっているといえよう。

一方、電子署名や電子証明書という言葉は一般にも知られるようになってきたが、まだ普及しているとは言えない状況である。これは、その意味や意義、用途が正しく理解されていないことにも原因があるかもしれない。ここではそれらの一般的な説明を行い、次章以降で、基盤として普及するために欠かせない ID との関係、相互運用に必要な標準化の動向について述べる。

## 2.1 電子署名の役割

紙への署名と同様に電子署名には、真正性（完全性）の保証と責任の明示という二つの役割がある。まず前者は、署名により改ざんが検知可能になることから、改ざんを防止する効果と、ある時点で改ざんされていないことを証明できるという効果がある。そのため、契約文書や決裁文書等の重要書類へ署名することにより改ざん防止を図ることや、業務記録やシステムログへ署名することにより、監査等に対する証明性を高めることができる。

後者については、それに誰が署名したかを証明できるため、署名者の責任を明示し、否認を防止する効果がある。契約文書への署名は契約当事者相互の否認防止の意味もある。また、より積極的な意味としては、文責を明示することで署名者の正当性や責任・意志の表明あるいはアピールにつながるものといえる。例えば、公開文書への署名や電子メールに金融機関等が署名を付ける例などが該当すると考えられる。

改ざん防止や否認防止は、紙社会から電子化社会への移行に伴い必然となるものであるが、従来、紙文化で改ざん防止や否認防止のため確立していた業務フローやシステムを変える必要性があり、相応の初期導入コストを伴うこととともに、その署名の受益者が文書を受け取る側であることが、導入・普及の阻害要因となっている一面がある。しかし、現状で電子署名以上に、否認や改ざんを効率よく防止する手段はなく、ペーパーレス社会への移行による業務の効率化と環境問題への貢献という面からトータルのコスト・効率性を発揮できるシーンにおいては、有用な技術であり、いずれ普及するものと考えられる。

一方、非改ざんの証明や文責の表明は、その必要性あるいは効果がまだ十分認知されているとは言えない面はあるが、署名者自身のメリットに繋がることから、積極的なアピールを重視する先進企業や社会的責任のある組織・資格者などから順次導入されていくものと考えられる。

表 1.2.1 電子署名の役割・効果

| 電子署名の役割 | 電子署名の効果 | 用途・対象 | 署名の受益者 |
|---|---|---|---|
| 真正性・完全性の保証 | 改ざん防止 | 保存文書、重要文書など | 文書利用者 |
| | 非改ざんの証明 | 業務記録やシステムログなど | 署名者（社） |
| 責任の明示 | 否認防止 | 契約文書、申請書、Eコマースなど | 文書受領者 |
| | 文責の表明 | 署名付き電子メール、公文書など | 署名者 |

真正性の保証は、対象文書や関係者の範囲が限定的な場合（社内文書の保管や、特定の二者間の契約など)は､サーバによる機械的な署名やクローズドな枠組みの署名で十分な場合もあるが、責任の所在を広く公開する場合は、署名者を証明するオープンな認証基盤が発行する証明書が必要である。逆に言うと、表明する責任の重さ、内容に応じて、適切な証明書（何に基づいて何（IDなど）を証明するか）を選択する必要がある。証明書については次節で述べる。署名により互いに責任を明確化することは、そのコミュニティ内の透明性を上げることになり、安心安全なやり取りを可能とする。反面、透明性はプライバシーとのトレードオフでもあり、社会全般に広く適用するにはプライバシー保護、匿名性を利点とするケースにも配慮し、法的な枠組みと併せて社会基盤としていく必要がある。

## 2.2 電子証明書の役割

署名の責任を明示するため、その署名の公開鍵（正確にはその公開鍵に対応する秘密（私有）鍵）が誰のものであるかを証明する電子証明書（公開鍵証明書）が発行される。つまり電子証明書により署名者の特定ができる。(電子証明書は公開されるものであり、それを所持しているから本人というわけではなく、あくまでも署名と組み合わせて確認して、本人が特定できることに注意しなければならない。)

電子証明書はその使い方により、Authentication（認証）と Certification（認証あるいは証明）の役割を果たす。Authentication は本人性を確認することであり、身分証として提示してその場で確認する行為に相当する。Certification は何らかのことを証明するものであり、特に署名と結びついて、誰がどんな資格で署名したかを後々まで証明することになる。使い方による特徴の差異について下記にまとめる。

表 1.2.2 電子署名の役割・効果

| | Authentication | Certification |
|---|---|---|
| 意味 | 本人性の確認 | 何らかの資格・属性を証明 |
| 主な用途 | アクセス認証 | 署名・否認防止 |
| 署名者の行為 | 受動的 | 能動的 |
| 受益者 | 相手 | 本人 |
| 署名の責任 | 小 | 大 |
| 代替手段 | パスワード等 | 特になし |
| 主な対象者 | 一般人 | 資格者、権限者など |

(1) 認証利用

信頼できる認証局の発行した電子証明書（鍵）を識別の手段として認証（Authentication）に用いることができる。つまり、秘密鍵を持つことを何らかの方法（SSL 等のプロトコルの中で署名）で検証できれば、それが本人確認（人に限らず、機器、サーバシステムなどでもよい）になる。認証（本人確認）はサービス提供側が必要とするものであり、利用者はその求めに応じて証明書を提示し、署名を行う。利用者は、その手続きの過程で署名したという意識もない場合が多い。

単なるアクセス認証であれば、アクセスするものの重要性に応じて、パスワード認証などと使い分けられるが、パスワードは記憶に頼るため、簡易なものを利用したりメモを残してしまうなど漏洩のリスクが大きく、高セキュリティを要するニーズには電子証明書の方が適する。また昨今ニーズの高まっている内部統制のように証跡が重要な場合は、電子署名と組み合わせて利用できる電子証明書が有効であろう。

なお、アクセス時にサービス利用を許可されるかどうかを判定することが「認証」と誤解されやすいが、これは認証された利用者がその権限に応じて、何らかの処理を行えるかどうかを判定すること、すなわち認可（Authorization）であり、認証手段が証明書かパスワードかなどには無関係である。

(2) 署名利用と否認防止

適切に秘密鍵が管理されていれば、本人のみが署名したことが証明される。これは、改ざん防止の効果とともに、文書に対する文責と、否認防止の効果が発生することになる。責任に関して強制力を持つためには､法的根拠を伴うことが重要であり､日本では電子署名法がこれにあたる。

認証の場合と違うのは、認証はサービス提供側が利用者の確認に使うことが多い（その場限りである）のに対し、署名はサービス（情報）提供側が、その内容保証を含めて行い、かつその後の時間経過後も有効なことである。たとえば、電子申請とそれに対する交付、電子契約など、単なるサービスの認可ではなく、行為に証拠性が必要なものは、パスワードなどで代替できるものではなく、電子証明書が有効な領域である。医療分野など、ある資格を持った者（医師など）がその責任において文書を作成する場合なども、電子証明書を持つことの意義が大きいケースであ

る。

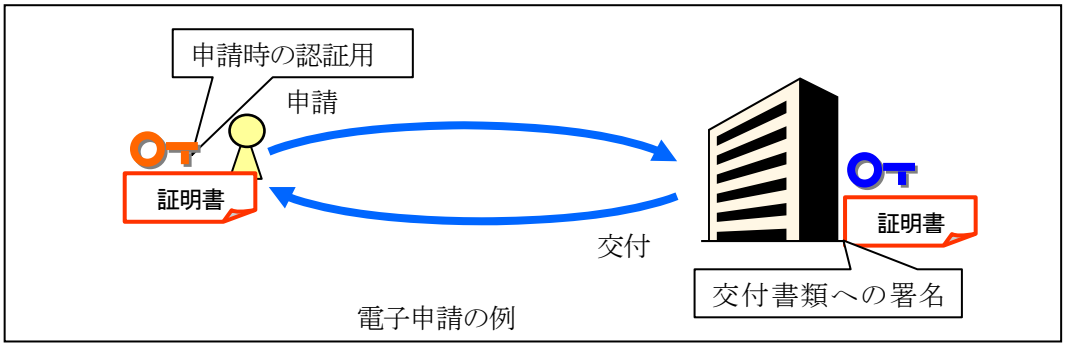



図 1.2.1 証明書の用途の違い

(3) 電子証明書の使い方の事例

認証用も署名（否認防止）用も同じ電子証明書技術ではあるが、目的、効力が異なるため、欧米では、別の鍵と証明書が使われることが多い。実際、フィンランドのFINEIDやベルギーのBELPIC、米国のPIVの場合、下記の表のように1枚のIDカードに異なる鍵と証明書が格納される。否認防止の署名用の鍵は、ひとつの文書の否認防止の署名毎に「カード保有者の同意確認」（User Consent）のためのPINの入力が必要な仕様になっていて、「カード保有者が同意して行う」ものであり、その署名文書等にはカード保有者の責任が生じるということを理解させるようになっている。

一方、日本のJPKI（公的個人認証サービス）では、否認認防止目的の証明書のみが発行されているが、これ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保有者のリテラシーの低下につながるため望ましいことではない。

表 1.2.3 証明書の利用事例

| IC･IDカード | カード保有者の証明書 | 証明書（鍵）の利用に関する説明 |
|---|---|---|
| FINEID／フィンランド | 認証、暗号用の証明書 | 署名操作と暗号分からの復号に使用。PIN1によるカード保有者の認証。 |
| | 否認防止の署名用証明書 | 署名操作のみ。署名操作毎にPIN2による認証が必要。 |
| BELPIC／ベルギー | 認証用の証明書 | 認証（のための署名）に使用する。<br>復号には使用できない（暗号には利用できない）。 |
| | 否認防止の署名用証明書（18歳以上のみ） | 署名操作のみ。署名操作毎にPINによるカード保有者の認証（同意）が必要。 |
| PIV／米国 | 認証用の証明書 | 認証（のための署名）に使用。 |
| | 否認防止の署名用証明書（オプション） | 署名操作のみ。署名操作毎にPINによるカード保有者の認証（同意）が必要。 |
| | 暗号用の証明書（オプション） | 発行者により「鍵」のバックアップがなされる。 |

| | | |
|---|---|---|
| 公的個人認証サービス／日本 | 否認防止の署名用証明書 | 署名操作のみ。<br>否認防止用の証明書のみ発行される。 |

＊独立行政法人　情報処理推進機構（IPA）調査報告書（2007 年 1 月）
「IC・ID カードの相互運用可能性の向上に係る基礎調査」の「シーズ編」より

(4) 日本の法制度の現状

2001 年 4 月に施行された、いわゆる「電子署名法」は、まさに紙に対する押印と同じ効果を電子情報に対して成立させるために電子署名に法的根拠を与えることを狙ったものである。したがって、自然人に対して、否認防止の署名を対象としており、署名法で規定された「特定認証業務」の認証局は否認防止用証明書を発行している。

証明書のコストが高いという議論があるが、これは否認防止を目的として厳しい制約の元で運用する認証局が発行するため、ある意味、当然の結果でもある。証明書の普及やコストの低減を図るためには、否認防止用と認証用は別に発行することも考えられる。

## 2.3　電子証明書と認証基盤

電子署名は印鑑証明の枠組みにたとえて説明されることが多い。その場合、実印が秘密鍵で、印鑑登録証が電子証明書（公開鍵証明書）、それを登録・発行する役所に相当するのが認証局である。つまり、電子署名と証明書も、その署名者が誰であるかを証明書により保証するこのような枠組み（認証基盤）があって初めて有効な手段となる。

ここで、証明書に類するものにおいて重要な点は、発行者が何に基づいて対象者を確認しているか、さらには、対象者の何を証明しているか、ということである。たとえば、住民票は住民の居住（実在）を証明し、社員証や学生証は、ある企業や学校への帰属を証明する。運転免許証は、さらに運転能力を持つことを証明している。何らかの資格証明（医師免許等）も同様である。

同様に電子証明書も、認証局が何らかの基準でその存在や資格を証明している。たとえば公的個人認証サービスの証明書は、住民基本台帳に基づいて、役所の窓口で本人確認を行って発行される。これは国民の存在と居住を証明しており、e-Tax など電子申請の際に本人性の確認に使われる。政府の認証基盤である GPKI は官職を証明するものであり、省庁からの交付文書における署名などに用いられる。サーバ証明書は、認証局がサービス提供者をある基準（認証局によりさまざま）に基づいて判定し、サーバの存在とサービスの正当性を証明している。

このような認証基盤を構築し、電子署名と証明書を導入することの意義と効果を考えてみると、認証基盤はセキュリティの向上に留まらず、コスト・効率性、ユーザビリティ、透明性の確保に効果がある。

表 1.2.4 認証基盤構築の目的

| 分類 | 目的 | 適用例 |
|---|---|---|
| セキュリティ | 従来方式に対するセキュリティ向上 | パスワード認証の代替 |
| コスト面 | 電子化による作業効率アップと、ペーパーレスによるコストダウン | 電子決済、e 文書法対応 |
| 利便性 | 従来方式に対する操作性・運用性の向上 | 証明書による認証方式の統一・シングルサインオン |
| 透明性 | アカウンタビリティ、証明性の向上 | メール、文書、証拠記録等への署名 |

コスト面では認証基盤の導入運用コストはかかるものの、電子化推進によるトータルのコスト効果を評価する必要がある。利便性としては、パスワード方式と比較するとシステムが多くなった場合にパスワードを適切に使い分け、頻繁に更新するという運用負担を軽減する効果が期待される。また、これらはワンタイムパスワードなどでも解決できるかもしれないが、透明性の確保は、署名と証明書方式のみの効果である。このような基盤により安心安全なネットワークコミュニティが形成されると、それを前提とした新たなサービス（例えば、より信頼性の高い SNS のようなサービス）の創生も期待される。

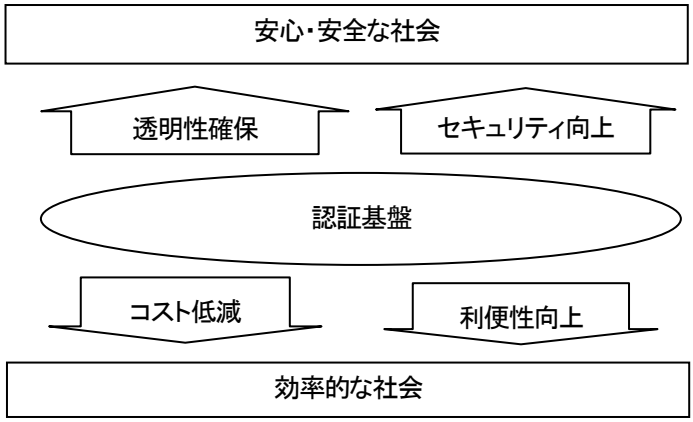



図 1.2.2 認証基盤のもたらす社会的効果

認証の枠組みは企業内や業界、大学などの組織単位のものから、国単位の社会基盤まで様々な単位で構築されうるものである。それぞれの組織内においては、認証対象を識別するために通常何らかの ID を用いており、認証基盤としては、ID 管理と組み合わせて構築される必要がある。国レベルでの ID 管理と認証基盤のあり方については次章で述べる。

# 3. 社会基盤としてのID管理と電子署名

## 3.1 ID管理モデル

電子署名、認証（Authentication）に利用する証明書には、概ね利用者（署名者、認証要求者）が識別できる情報が記載されている。公的個人認証サービス（JPKI）においては、識別情報として「住基4情報」が記載されている。しかし、多くの国の電子政府などで利用されている証明書の場合、何らかの個人を識別するための国レベルのIDが記載されている事例が多い。逆にJPKIにように「住所」が記載されている事例はほとんど見受けられない。

非常に広範囲に連携させる情報システムを考えた場合、証明書に記載されるIDが公的な登録に基づくものであれば、この証明書を利用して署名された電子文書は、法的な意味も含め責任の所在などを合理的に示せることになる。そしてサービス提供者側においてIDに基づく、誤りの少ない合理的でかつ（IDの照合も含めた）自動的なデータ処理を可能にする。「責任の所在なども合理的に示す」ことと「自動的なデータ処理を可能にする」このふたつは、行政・公共サービス等の人や企業に対するサービスの効率性と透明性の双方を提供することになる。

証明書に記載されるIDについてもうひとつ重要な観点に、行政サービスにおけるバックオフィスの連携や、官民連携がある。公的な登録に基づくIDが適切に利用できれば、個人や企業のための組織を越えた情報（個人情報、企業情報）の利活用が可能になる。一方、個人情報等が容易に結合できることから、個人を監視するために利用されるのではないかという危惧も生じる。こうしたことは、個人情報保護法等との関係も注意深く考察される必要がある。

電子署名の利用ということに関して言えば、多くの場合において、電子署名が施された電子文書は証跡として長期に保存される必要がある。この時、長期に保存という要件からも、証明書に記載されるIDは、より普遍的なものが望ましい。

国レベルのID管理には、いくつかの考え方がある。オーストリアの産官学によるITセキュリティセンターであるA-SIT[1]では、図 1.3.1に示すとおりID管理モデルを以下の3つに分類している。

[1] A-SIT http://www.a-sit.at/

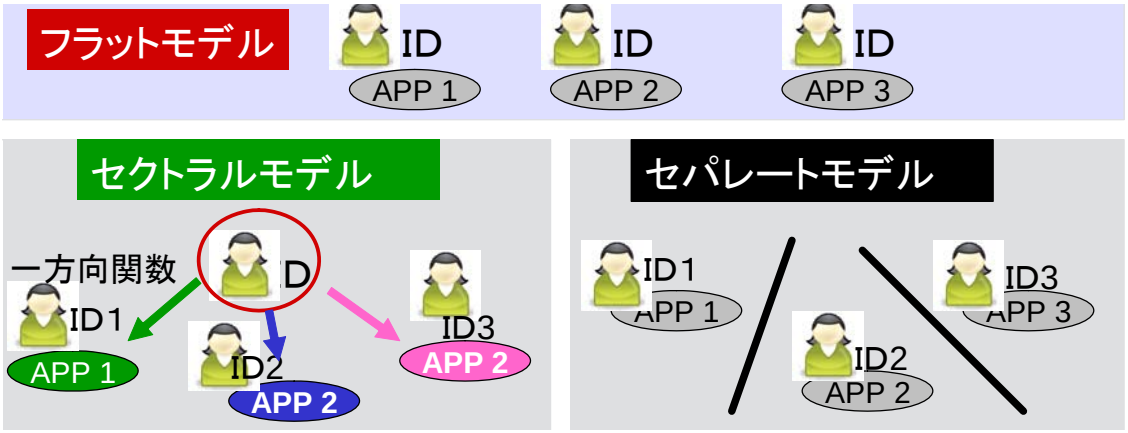



図 1.3.1 ID 管理モデルの種類

(1) フラットモデル (FLAT MODEL)

複数のサービス (APP1、APP2、APP3) に同じ ID を使う。つまり個別のサービスに依存しない汎用的な ID を使うモデルである。欧州のエストニア、ベルギー、デンマーク等のいくつかの国はこのモデルを採用している。エストニア、ベルギーでは電子身分証明 (eID) が全国民に配布されているが、この eID に格納されている署名用証明書と認証用証明書には、この ID が記載されている。

エストニアの例では、生まれると「性別」、「生年月日」、「4 桁の番号」からなる 11 桁の国民 ID がつけられる。多くの個人のデータは、この国民 ID に関連付けられて記録されるため、行政・公共サービス間で個人情報を連携することが容易にできる。例えば、行政・公共サービスで何らかの手続き等の際、既に他の組織で登録した情報は、再度入力を求められることはないといったことが実際に行われている。

(2) セパレートモデル (SEPARATED MODEL)

セパレートモデルは、サービス (APP1、APP2、APP3) 毎に ID (ID1、ID2、ID3) をつける方法である。各サービスの情報は、それぞれの持つ ID により管理されているため、単純に情報を連携させることはできない。また、サービス毎に ID 発行のコストがかかるという欠点もある。一方、個人情報を保持する行政機関などは、自分の権限を越えて個人情報を収集することが困難なため、行政が「国民を監視」しているという嫌疑を受け難いと言える。しかし、行政・公共サービスにおけるバックオフィスの連携は、時代の要請でもあり、このセパレートモデルであっても様々な情報の連携が求められている。何のポリシーもなく情報の連携を進めると、至る所で ID 間のマッピング情報を持つことになり、また ID の流用が脈略なく利用されるといったことが起きる可能性もある。

(3) セクトラルモデル (SECTORAL MODEL)

サービス (APP1、APP2、APP3) 毎に異なる ID (ID1、ID2、ID3) を使うが、それらの ID は一つの基本となる ID から派生させる方式である。このセクトラルモデルは、オーストリアで採用され

ている ID 管理モデルであり、まだ、事例としては少ない。セパレートモデルと同様、各サービス（ないし各セクター）の組織は、自分の権限を越えて個人情報を連携することが困難になるが、セパレートモデルと違い、ひとつの ID が、様々なサービス（ないしセクター）で利用でき、サービス毎の ID 発行のコストがかからない。

以上で説明した「フラットモデル」「セパレートモデル」「セクトラルモデル」は、それぞれ利点と欠点がある。こうした利点と欠点が認識された上で、様々な法制度（例えば個人情報保護法）との関係が整理される必要がある。次節以降では、それぞれの ID 管理モデルと発行している証明書の事例を説明する。「フラットモデル」では、エストニアとデンマークの事例、「セパレートモデル」では、スロベニアの事例、「セクトラルモデル」ではオーストリアの事例を取り上げている。

## 3.2 エストニア

エストニアは、欧州の中で非常に先進的な電子政府を推進している国として知られている。特に、全国民に配布された eID（電子身分証明書）と、X-ROAD と呼ばれる情報交換基盤の二つが有名であり、この eID と X-ROAD を基盤として様々な行政サービスが提供されている。この eID を利用し、世界で初めて国政レベルの選挙において「インターネット投票」が実施されている。また、2011 年には、新たに整備されているモバイル ID（携帯を利用した署名と認証）による国政選挙の投票を認める法案が可決されている。こうしたインターネット投票、モバイル ID には、電子署名が利用されている。そして、この電子署名に利用される証明書にはエストニアの国民 ID が記載されている。

エストニアでは、前述したとおり 11 桁の国民 ID が利用されている。エストニアにおける ID 管理モデルは、この国民 ID を利用した「フラットモデル」ということになる。各サービスの個人情報はこの国民 ID に関連付けられて記録されるためサービス間で個人情報を容易に連携することができる。

エストニアにおいては、多くのサービスが X-ROAD に接続されているが、図 1.3.2 に示すようにフラットモデルの ID 管理をベースにした情報連携を行っている。

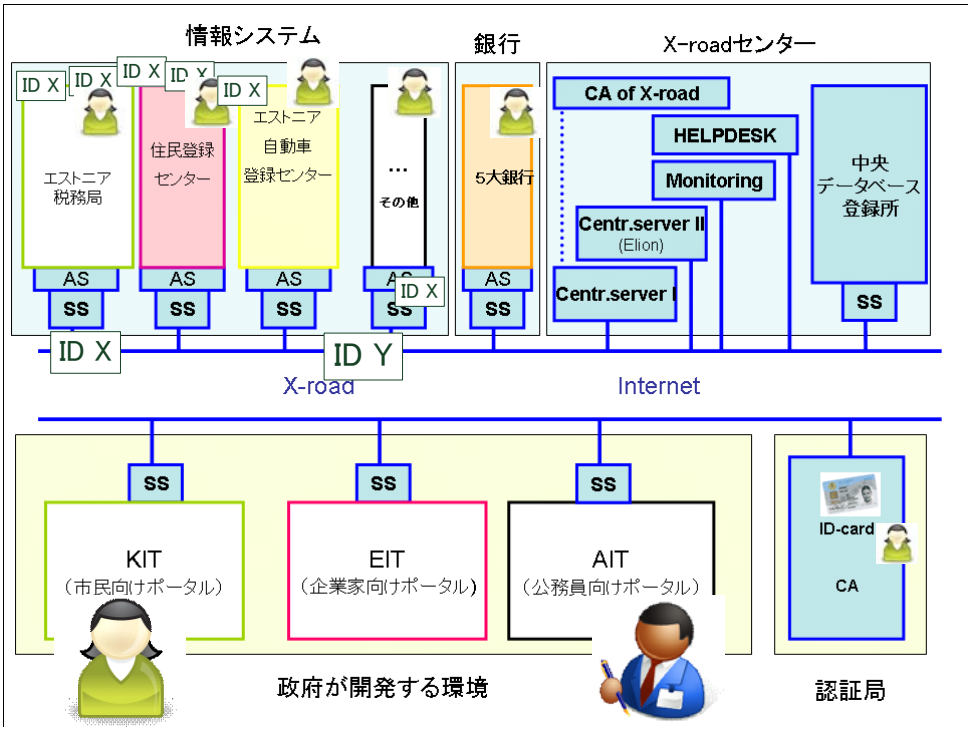



図 1.3.2 フラットモデルの ID 管理をベースにした情報連携モデル

エストニアでは、こうした X-ROAD のような情報連携を前提とした電子政府を、「行政中心のサービではない国民中心の行政サービス」と称している。

国民 ID を管理しているのは、内務省の管轄にあるエストニア市民権・移民委員会（CMB）である。CMB は、エストニア国民および在留外国人への身分証明書の発行に責任を負う政府機関であり、国民からの eID の申し込みも受け付けている。

eID と eID に格納されている（電子）証明書は、エストニアの 2 つの主要な銀行および 2 つの通信会社によって設立された「証明書発行センター」（SK）が発行している。

表 1.3.1 に証明書に記載される主体者名を示す。また図 1.3.3 では、実際のエストニアの署名用の証明書を表示された例を示す。

表 1.3.1 エストニアの証明書の主体者名

| 項目 | 説明 | 事例 |
|---|---|---|
| CountryName | 国コード | EE |
| O（Organisation） | 証明書タイプ | ESTEID |
| OU（Organisational Unit） | 証明書の種類 | [‘authentication’,‘digital signature’] |
| SN（Surname） | | ‘Kaxxx’ |
| G（GivenName） | | ‘Juxxx’ |
| Serialnumber | 国民 ID（11 桁）が記載される | ‘3701112xxxx’ |

| | | |
|---|---|---|
| CN　(CommonName) | 名前と国民 ID (11 桁) が連結されて記載される。 | '3701112xxxx, Kaxxx, Juxxx' |


**図 1.3.3 エストニアの署名用証明書**

表 1.3.1、図 1.3.3 で分かるように、証明書の主体者名（識別名）にエストニアの国民 ID が記載されている。証明書が更新されても、証明書に記載されるエストニアの国民 ID は変わらない。一方、住所のような変更される可能性が高い情報は、証明書には記載されていない。

署名用の証明書以外に認証用の証明書が eID に格納されるが、この認証用の証明書には、政府が割り当てた、カード所有者の公的な電子メールアドレスも含まれている（firstname.lastname_NNNN@eesti.ee という形式。NNNN は 4 つの乱数)。このアドレスは、それ以降の証明書または eID の発行でも変更されず、その利用者の「生涯の」アドレスであることが保証される。また、このアドレスとカード上の認証用の証明書を使用すると、利用者は自分の電子メールへのデジタル署名や暗号化も可能になる（証明書を使用した電子メールの暗号化や署名は、各種の電子メール・アプリケーションの標準の機能である)。この認証用の証明書を利用した電子メールへの電子署名には法的拘束力はないが、これによって、送信者の正当性に関する認証が受信者に提供される。

エストニアにおいては、国民 ID が広く利用できることを前提に、個人に対して利便性の高いサービスが提供されている。一方、個人情報等が容易に結合できることから、政府が個人を監視するために利用されるのではないかという危惧に対応する必要になる。また、国民 ID これ自体の（個人）情報としての扱いも明確にする必要がある。表 1.3.2 にエストニアの個人情報保護法（Personal Data Protection Act）により示されている個人情報の区分を示す。

表 1.3.2 エストニアの個人情報の区分

| 情報区別 | 情報内容 | データ収集の制約 |
|---|---|---|
| 個人情報 | 名前、ID<br>等 | 特になし（名前、ID は公開されている？） |
| 私的個人情報<br>private personal data | 1) 家庭生活の詳細を明らかにする情報、<br>2) 社会扶助または社会福祉の給付申請を示す情報<br>Etc… | 情報保護監察局へ通知する必要がある。 |
| 機密個人情報<br>sensitive personal data | 1) 政治的意見または宗教的もしくは哲学的信条を示す情報（ただし、法律で規定された手続きに基づいて登録された私法上の法人の構成員であることに関する情報はこの限りでない）<br>2) 民族的または人種的起源を示す情報<br>Etc… | 情報保護監察局の許可が必要 |

国民 ID などの ID 自身は、重要な個人情報とはしていない一方で、ID に関連付けられる情報については、その収集に関して日本の個人情報保護法よりも厳しい制度となっている。ID は、様々な情報システムで利用できなければ、個人に対して利便性の高いサービスを提供することは困難になるが「エストニアの個人情報保護法」では、ID の扱いにも次の様に言及している。

| |
|---|
| 第 16 条　個人識別コードの処理に対する許可<br>個人識別コードの処理が国際協定、法律または規則により規定される場合は、情報主体の同意を得ることなく、かかる個人識別コードを処理することが認められる。 |

X-ROAD を中心に行政サービスにおいても、市民自身が、自分の個人情報に対して公務員等がアクセスしたことの履歴を参照できる機能を提供している。このように ID 自体ではなく、ID に関連付けられる情報を守るための制度や情報システムが整備されていると言える。

以上のようにエストニアにおいて国民 ID は、隠すべき情報としては扱われておらず公共財的な情報に近い。実質的に身元を容易に証明できる eID（電子身分証明書）が全国民に発行され、また民間での利用制限も無いため、国民 ID が公知であっても ID 詐称などの被害は抑えられることにも関係があると考えられる。

参考

住基カードの普及策はエストニアの国民 ID カードに学べ
http://itpro.nikkeibp.co.jp/article/COLUMN/20070423/269245/
「IT 立国エストニア―バルトの新しい風」
前田陽二／内田道久　著　　ISBN978-4-86330-019-4

Personal Data Protection Act

http://www.legaltext.ee/text/en/X70030.htm

eID Interoperability for PEGS / NATIONAL PROFILE ESTONIA

http://ec.europa.eu/idabc/servlets/Doc?id=31526

エストニアの個人情報保護法 Personal Data Protection Act Passed 12 February 2003

http://www.legaltext.ee/text/en/X70030.htm

## 3.3 デンマーク

デンマークは、すぐれた福祉の先進国として広く知られているが、電子政府においても、国連の電子政府調査でランキング第2位という充実したサービスを提供している。

デンマークでは10桁の国民番号である中央住民登録番号（CPR番号）を約40年前に導入しており、非常に幅広く利用されている。例えば、課税処理等もCPR番号を利用している。CPR番号は、生年月日部分（6桁）と誕生日番号（3桁）とチェック桁（1桁）の10桁の数字で構成されている。このCPR番号は、福祉省管轄のCPR Bureauという機関が管理を行っている。

デンマークの電子政府で利用される証明書を発行する認証局は、OCES（Public Certificate for Electronic Service）プロジェクトにより科学技術イノベーション省と契約した TDC（旧国営電信電話会社：Tele Denmark）が運用している。

表 1.3.3デンマークの証明書の主体者名に証明書に記載される主体者名を示す。また図 1.3.4では、実際のOCESの証明書を表示した例を示す。

**表 1.3.3 デンマークの証明書の主体者名**

| 項目 | 説明 | 事例 |
|---|---|---|
| CountryName | 国コード | DK |
| O（Organisation） | 証明書の種類<br>（法人向け証明書では、法人名） | 'Ingen organisatorisk tilknytning' |
| Serialnumber | Qualifier PID：Concatenated with serial number. See DS 843-1 Person-specific Identification Numbers（PID） | PID：9208-2001-3-279815395 |
| CN（CommonName） | Last and first names | Test Tester |

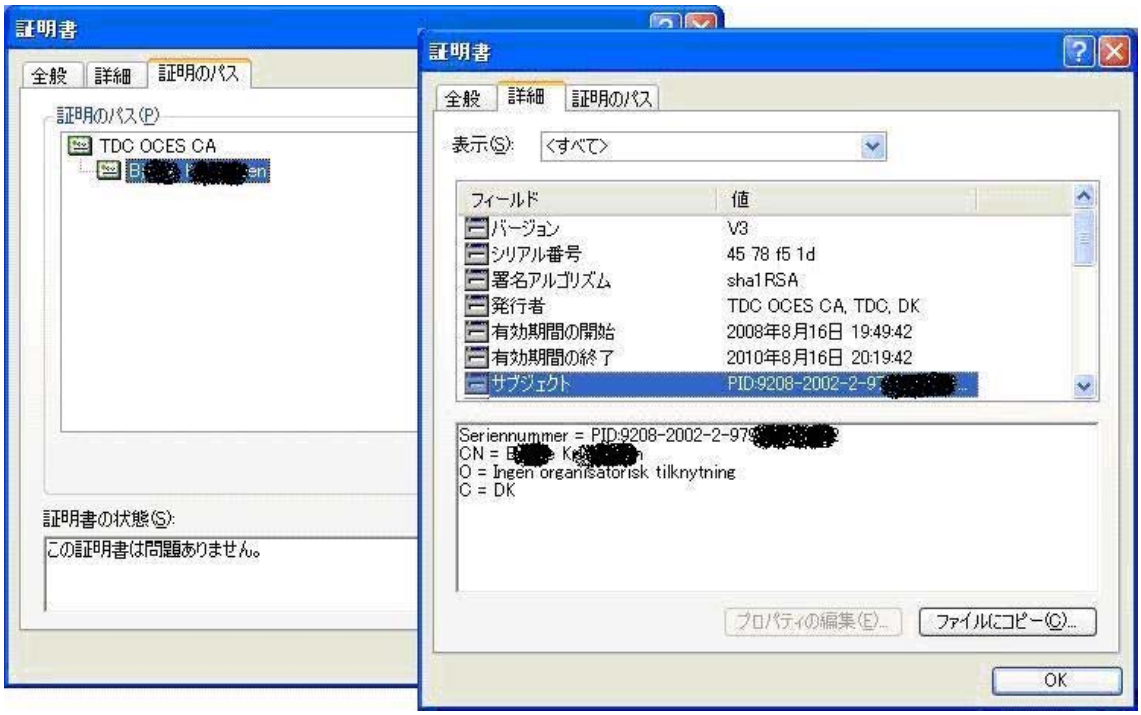



図 1.3.4 デンマークの兼用証明書（combined certificate）

表 1.3.3、図 1.3.4 で分かるように証明書には、CPR 番号は記載されておらず代わって PID（Person-specific Identification Numbers）が記載されている。この証明書に記載される PID から CPR 番号の変換は、認証局のサービスとして提供されており、法的に CPR 番号を利用できる「行政機関」「公共機関」であれば、このサービスを利用できる。また、民間であっても「証明書利用者の同意」があれば、変換サービスを利用することができるとされている。

デンマークの電子政府では、2008 年 10 月にマイページという国民一人ひとりに個別化したサービスの提供を始めている。PID が記載された証明書が広く配布さていること、情報を提供する行政機関のデータが PID から一意に変換される CPR 番号を中心にデータベース化していること、このふたつがマイページのようなサービスを可能にしていると考えられる。

参考

デンマークにおけるデジタル署名の普及に向けた取り組み（NTT データ・デジタルガバメント）
http://e-public.nttdata.co.jp/f/repo/384_e0605/e0605.aspx
デンマークの社会保険ワンストップ・サービス（NTT データ・デジタルガバメント）
http://e-public.nttdata.co.jp/f/repo/583_e0810/e0810.aspx
北欧の電子政府に学ぶ
http://itpro.nikkeibp.co.jp/article/COLUMN/20081027/317824/
Certificate Policy for OCES personal certificates
https://www.signatursekretariatet.dk/pdf/ca/Final%20Etsi%20OCES-CP%203.0%20personal%20certificates_eng.pdf

eID Interoperability for PEGS / NATIONAL PROFILE DENMARK
http://ec.europa.eu/idabc/servlets/Doc?id=31525

## 3.4 スロベニア

スロベニアは、2007 年の欧州電子政府サービスランキングで 2 位の評価を得ている。既に、個人向け、企業向けの個別化したサービスも提供している。

スロベニアでは、全てのサービスに共通化した ID は持っておらず、個人の場合は、以下の 3 つの ID が利用されている。

- 個人登録番号（PRN：Personal Registration Number）
- 納税者番号（Tax Number）
- 健康保険番号（Health Insurance Number）

法人の場合は、以下の二つの ID を持っている。

- 識別番号（Identification Number）
- VAT 番号（VAT Number）.

個人登録番号（PRN）は、スロベニア内務省により管理される「スロベニア中央住民登録」において一意識別可能な番号として登録されている。この個人登録番号（PRN）は、13 桁の数字であり最初の 7 桁は、生年月日（DDMMYYY）、続いて「登録簿」のラベルを示す“50”、続く 3 桁は、性別も含む（男性のための 000-499 と女性のための 500-999）に同日に生まれる人のための連続番号となっている。最後の 13 桁目は、チェック桁となる。

納税者番号（Tax Number）は、国税庁（Tax Administration）により管理される「納税者登録簿」により一意識別可能な番号として登録されている。最初の 7 桁は乱数により採番され 8 桁目は、チェック桁となる。この納税者番号（Tax Number）をプライマリキーとして管理される「納税者登録簿」には、個人登録番号（PRN）も含まれる。

健康保険番号（Health Insurance Number）は、全てのスロベニアの市民に、保健省の下部機関であるスロベニア健康保険協会（HIIS）により発行される。健康保険番号は、9 桁の数字から構成されている。スロベニアでは、IC カード化された「スロベニア健康保険カード」が 2000 年から利用されている。また、2008 年には、PKI にも対応した新しい「スロベニア健康保険カード」プロジェクトが開始されている。

以上の様に、スロベニアにおいて完全な汎用 ID は存在せず、ID 管理モデルは、セパレートモデルを採用していると言える。しかし、個人登録番号（PRN）は、健康保険、税以外の分野（セクター）において汎用的に利用されている ID であるとも言えるかもしれない。

スロベニアにおいては、電子署名に利用されるクォリファイド証明書を発行している認証局が 5 つ存在する。ここでは、総務省（Ministry of Public Administration）が管理する認証局について説明する。総務省は、公務員に証明書を発行する SIGOV-CA と、自然人、法人に証明書を発行

するSIGEN-CAの二つの認証局を運営している。表 1.3.4にスロベニアのSIGEN-CAの発行する証明書に記載される主体者名を示す。また図 1.3.5では、SIGEN-CAの発行する証明書を表示した例を示す。

**表 1.3.4 スロベニアの証明書の主体者名**

| 項目 | 説明 | 事例 |
|---|---|---|
| CountryName | 国コード | SI |
| O (Organisation) | | state-institutions |
| OU (Organisational Unit) | CAの名前 | sigen-ca |
| OU (Organisational Unit) | 発行対象（自然人）であることを示す。 | individuals |
| Serialnumber | 認証局（SIGEN-CA）が管理する「シリアル番号」 | 246445951nnnn |
| CN (CommonName) | 個人名が記載される | xxxx xxxxx |


**図 1.3.5 スロベニア SIGEN-CA の証明書**

SIGEN-CAが発行する自然人のための個人証明書には、個人登録番号（PRN）、納税者番号は、直接記載されていない。代わって証明書には、個人の名前と認証局自体が管理する（電子証明書固有の）シリアル番号が記載されている。そして認証局（SIGEN-CA）は、この「シリアル番号」と

「個人登録番号（PRN)」、「納税者番号（Tax Number)」のマッピングをデータベースに保持している。

認証局は、シリアル番号から、「個人登録番号（PRN)」、「納税者番号」に変換するサービスを提供しているが、これには、スロベニアの個人情報保護法に従う必要があるとされている。変換するサービスが利用可能になるものには、「法制度に基づくもの」と、「個人の同意に基づくもの」がある。SIGEN-CA では、法人向けの証明書も発行しているが、この場合は、識別番号（Identification Number)、VAT 番号（VAT Number）が直接記載されている。

スロベニアにおいては、こうした「個人登録番号（PRN)」、「納税者番号」に変換可能なシリアル番号が記載された証明書を前提に、個人向け、企業向けの個別化したサービスを提供している。個人の場合は、e-Remainder と呼ばれている異なる行政機関が発行する免許書、証明書などの期限切れを知らせるサービスを提供しており、次に My e- Archive と呼ばれる、行政とのやり取りを保管するサービスが提供されようとしている。企業向けの個別サービスでは、“one-stop shop”と呼ばれている企業の起業から、企業の様々な活動、更に廃業までオンラインでサポートするサービスを提供している。

eID Interoperability for PEGS / NATIONAL PROFILE SLOVENIA
http://ec.europa.eu/idabc/servlets/Doc?id=31547
one-stop shop
http://www.epractice.eu/cases/eVEMSlovenia

## 3.5 オーストリア

オーストリアは、2007 年に欧州電子政府サービスランキングで 1 位の評価を得ている。このオーストリアは「セクトラルモデル」と名付けられた ID 管理モデルを採用しているが、この「セクトラルモデル」は、オーストリアの「電子政府法(E-Government Gesetz:The Austrian E-Government Act)」に基づいている。電子政府法は、オーストリアの電子政府関連法規の中核であり、2004 年 3 月 1 日に施行され、2008 年 1 月 1 日に最初の改正が行われている。この法律は電子政府のサービスに関わる法制上の原則を示し、電子政府のサービスを提供する全ての行政機関相互のより緊密な協働を可能とするための連携の機会を提供している。電子政府法において定められている「市民カード」、「セクター固有（sector-specific）個人識別（ssPIN)」および文書の電子配布等の電子政府に関わる多くの仕組みは民間における利用も可能としている。

オーストリアにおいては、3 つのレベルの個人を識別する ID（ZMR-Zahl、SourcePIN、ssPIN）が発行されている。

(1) 国民登録番号（ZMR-Zahl）

オーストリアでは、出生後すぐに国民登録機関（CRR：Central Register of Residents）に登録される。この時、CRR により ZMR-Zahl が発行される。この ZMR-Zahl の利用には、制約があり、広く利用されている訳ではない。電子政府等では、後述するように ZMR-Zahl を元にした SourcePIN、ssPIN が利用される。

このほかに、会社を登録する商業登記機関（CR：Commercial Register)、団体登録機関（RA：Register of Associations)、それに、在オーストリア外国人はその他登録機関(supR:Supplemental Registers）に登録される。これらの機関でも、CRR と同様に、登録された企業や団体、外国人に対して（SourcePIN、ssPIN）が発行される。

(2) SourcePIN

SourcePIN は、オーストリアの個人情報保護法（Federal Data Protection Act）により設立された「データ保護委員会」の管理の元、ZMR-Zahl を Triple DES でスクランブルして生成される。Triple DES の「暗号鍵」もまた、「データ保護委員会」で管理される。こうすることにより、SourcePIN から ZMR-Zahl、ZMR-Zahl から SourcePIN を類推することが出来なくしている。作成された SourcePIN は、非公開情報であり、本人の「市民カード」にのみ格納される。「市民カード」は、オーストリアの「電子政府法」で定義された論理的な媒体になる。

(3) ssPIN (Sector-specific IDs)

ssPIN は、各セクターのサービス（アプリケーション）で実際に利用される ID となる。サービスを提供するセクターには、セクターID が割りつけられる。ssPIN は、SourcePIN とこのセクターID をつなぎ合わせた値に対して、ハッシュ関数により得られた固定長の数値列（ハッシュ値）から計算される。このように、ひとつの ID（SourcePIN）から、セクター毎の ID（ssPIN）を生成して利用するのがセクトラルモデルの特徴となっている。

オーストリアのセクトラルモデルにおいては、ssPIN 生成のために各公共機関によるデータ活用を国の活動分野毎に指定する必要があるが、そのため法規制である「電子政府セクター範囲設定規制（eGovernment Sectors Delimitation Regulation)」が存在する。この「電子政府セクター範囲設定規制」により活動分野を定義し、各分野にセクターID を指定している。現在 26 のセクターが定義されているが、セクターの例としては、「税」、「健康」等がある。図 1.3.6 に sourcePIN、ssPIN、セクターの関係を示す。

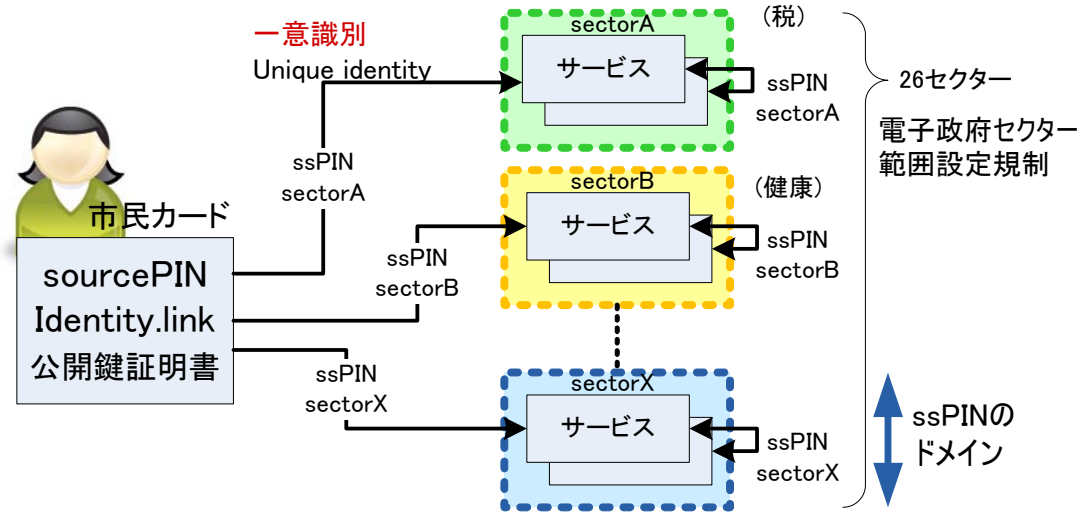



図 1.3.6 sourcePIN, ssPIN とセクターの関係

ssPIN を生成するも基になる SourcePIN は、オーストリアの「市民カード」に格納される。「オーストリア電子政府法」において「市民カード」は、特定のデバイスではない「論理ユニット」であることが明記されており、例えば、携帯電話等も実際に利用している。オーストリアのセクトラル方式においては、セクターを越えた個人情報の連携を行うためには、「データ保護委員会」が管理する「Triple DES の暗号鍵」が必要になるが、これは法律に基づく場合においてのみ利用が可能である。この場合でも、一意な識別が可能なため連携に曖昧性はない。

市民カードには、署名に利用する証明書と鍵が格納される。表 1.3.5、オーストリアの市民カードの証明書に記載される主体者名を示す。また図 1.3.7 では、実際の証明書を表示した例を示す。

表 1.3.5 オーストリアの証明書の主体者名

| 項目 | 説明 | 事例 |
|---|---|---|
| CountryName | 国コード | AT |
| O (Organisation) | | Hauptverband österr. Sozialversicherungs. |
| OU (Organisational Unit) | | VSig |
| CN (CommonName) | First name(s) + Surname | |

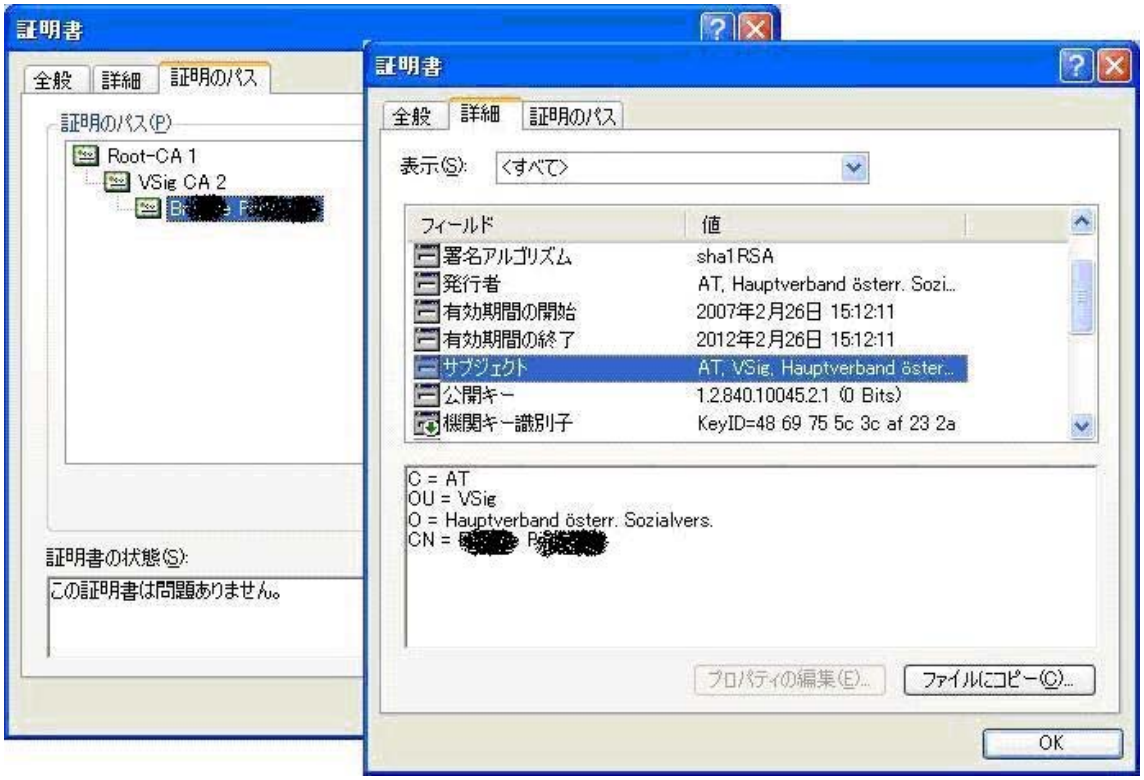



図 1.3.7 健康保険証カードの署名用証明書

この証明書の記載内容自体には、ID が含まれていない。代わって Identity.link を呼ばれる署名ファイルが SourcePIN、名前と生年月日と証明書の公開鍵の関係を証明している。この Identity.link 市民カードに格納されている。

参考

漏えい被害を限定的に抑制――オーストリアの国民 ID 番号

http://itpro.nikkeibp.co.jp/article/COLUMN/20080125/292090/

eID Interoperability for PEGS / NATIONAL PROFILE AUSTRIA

http://ec.europa.eu/idabc/servlets/Doc?id=31519

Administration on the Net / The ABC guide of eGovernment in Austria

http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19394

## 3.6 ID 管理モデルと証明書の関係の考察

表 1.3.6 に各国の ID 管理モデルと証明書の関係を示す。また、図 1.3.8 に ID 管理モデルに対応する「登録機関」「認証局」「個人や企業」「サービス」の関係を示す。

表 1.3.6 各国の ID 管理モデルと証明書の関係

| 国 | ID 管理モデル | ID と ID 管理の主体 | 認証局 | 証明書に記載される ID 情報 |
|---|---|---|---|---|
| エストニア | フラットモデル | 内務省の管轄にあるエストニア市民権・移民委員会（CMB）が 11 桁の国民 ID を発行している。 | エストニアの 2 つの主要な銀行および 2 つの通信会社によって設立された「証明書発行センター」 | 11 桁の国民 ID |
| デンマーク | フラットモデル | 福祉省管轄の CPR Bureau という機関が、10 桁の国民番号（CPR 番号）を約 40 年前に導入している。 | 科学技術革新省と契約した TDC（旧国営電信電話会社：Tele Denmark）が運用している。 | CPR 番号に変換可能な Person-specific Identification Numbers（PID） |
| スロベニア | セパレートモデル | ・個人登録番号（PRN）は、スロベニア内務省<br>・納税者番号（Tax Number）は、国税庁（Tax Administration）<br>・健康保険番号（Health Insurance Number）は、スロベニア健康保険協会（HIIS） | 総務省が運営する公務員に証明書を発行する SIGOV-CA と、自然人、法人に証明書を発行する SIGEN-CA その他民間認証局も存在する。 | 認証局（SIGEN）が管理する「シリアル番号」。この「シリアル番号は、個人登録番号（PRN）、納税者番号（Tax Number）と関係付けられている。 |
| オーストリア | セクトラルモデル | 国民登録機関（CRR：Central Register of Residents）発行する国民登録番号（ZMR-Zahl）がある。ただし「国民登録番号（ZMR-Zahl）」の利用には法的な制約があり、そのまま利用する訳ではない。 | 民間の認証局である A-TRUST<br>または、<br>社会保険本部 | 「名前」のみ。<br>公開鍵証明書の「公開鍵」と SourcePIN の関係を証明した Identity.link という XML 署名ファイルが利用される。 |

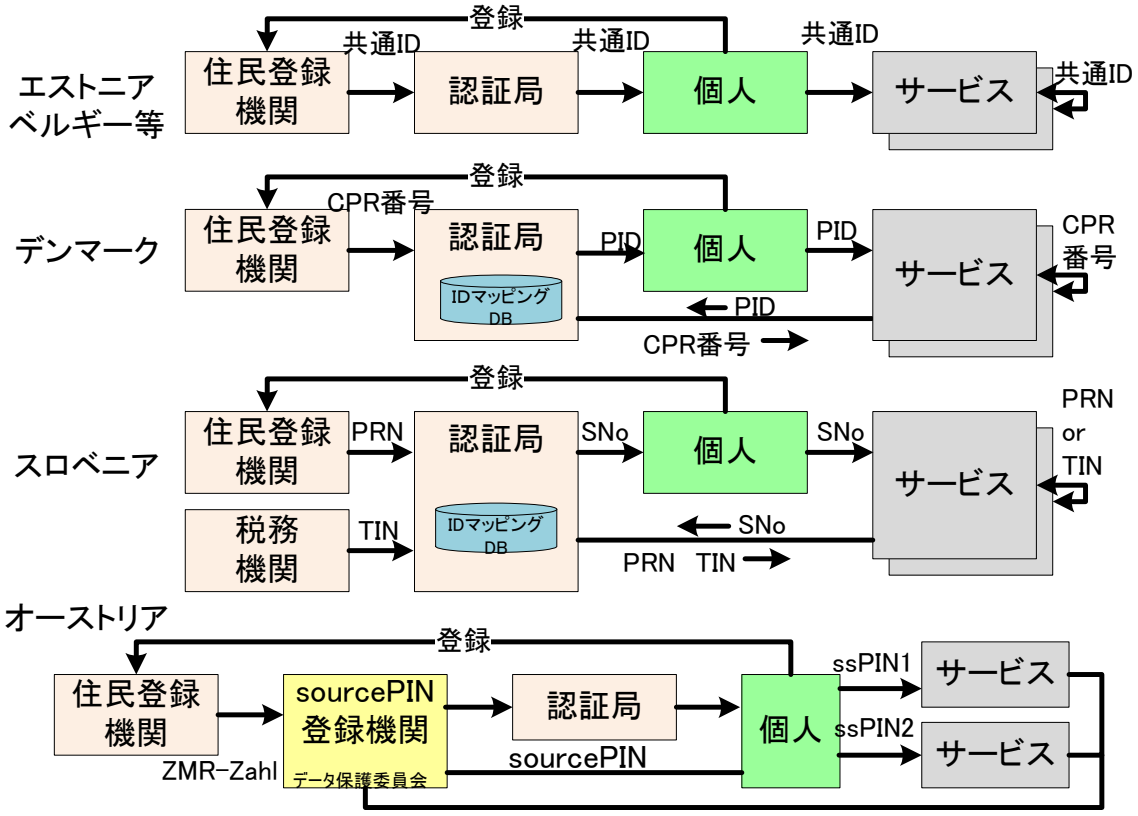



図 1.3.8 ID 登録機関、認証局、個人、サービスの関係

これまでの各国の事例において示したように、公的な登録に基づく ID が適切に利用できれば、個人や企業ための組織を超えた情報（個人情報、企業情報）の利活用が可能になる。一方、個人情報等が容易に結合できることから個人を監視するために利用されることを防ぐことも十分に考慮される必要がある。これまでの事例でも示されているように、基本的な考え方としての「ID 管理モデル」と個人情報保護法などの制度が連動して検討される必要がある。

一般的に「証明書」は、認証局が証明書を発行し、証明書の利用者（個人、企業、代理人）がサービスにおいて電子署名や認証（Authentication）に利用するものとして理解されている。例えば電子政府においても「電子署名」や「認証」は、フロントエンドとしての電子政府で利用されるものといった認識のみで利用されている。しかし、これまでの事例にある先進的な電子政府を推進している国においては、バックオフィスの連携も含めたもっと広い範囲おける IT 化、電子化を実現するために存在することが分かる。図 1.3.9 に、公的な登録機関、認証局、証明書利用者、署名文書を受け付けるサービスの関係の例を示す。

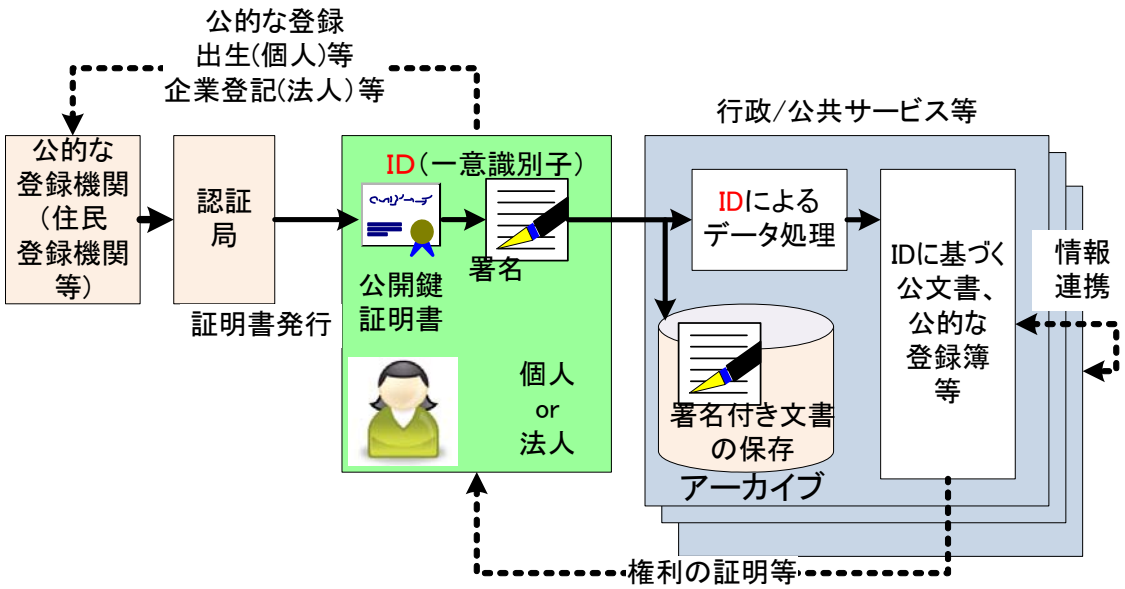



図 1.3.9 ID と証明書とサービスの関係

電子証明書の本質は、個人や企業のアイデンティティを電子データとして証明（Certify）することに大きな意味があるが、これは一時的なものではないことに注意する必要がある。ID 管理モデルと、この ID 管理モデルに従った ID の付与、この ID と人や企業を結びつける公開鍵証明書等は、フロントエンドとしての電子政府というよりは、バックオフィスの連携も含めて考えられる必要がある。更に、よく考慮されたシステム（法制度、官民連携の情報システム）が構築できれば、社会全体としての、人や企業に対するサービスの効率性の向上に決定的な影響を与える可能性があり、また、同時に透明性も確保できる可能性がある。

実際、ここで紹介した電子政府の先進国では、「バックオフィスの連携」が進んでいる。これは、ひとつは行政の効率化のためであり、もうひとつは、エストニアの電子政府で言われているような「サービス利用者中心」の行政システムへの移行がある。こうしたバックオフィスの連携に関する成功の鍵は、「ID 管理の確立」ではないだろうか。また、「サービス利用者中心」の意味は「サービス対象者」の管理方法の確立なしには、考えられない。但し「管理」は、「国民の監視」ではないことも示される必要がある。

「フラットモデル」「セパレートモデル」「セクトラルモデル」の 3 つの ID 管理モデルは、それぞれ、利点と欠点がある。どの ID 管理モデルであれ、その欠点をカバーする施策が必要になる。ID 管理モデルとそのポリシーが曖昧なまま個別のシステムが構築されていくと、バックオフィスの連携が出来ない、もしくは連携すると非常に脆弱なシステムになってしまう可能性が高い。

ID 管理モデルの明確化と、その ID 管理モデルにおける ID に関するポリシーの確立は、個人情報などをバックオフィスにおいて連携させるための基礎を形成することになるだろう。

# 4. 今後の認証基盤構築に向けた技術動向

## 4.1 欧州の標準化動向と我が国の状況の比較

電子署名に関係する標準化は、様々な組織において行われている。しかし、電子署名は、電子署名法などの法的な枠組みとの関係が強く、これまでの IT に関連した標準化の課題と異なる側面の課題を持っている。法的な枠組みは、単に電子署名法という枠にはとどまらず、さまざまな制度との関連がある。わが国で言えば、2005 年に施行された通称 e 文書法なども非常に関係が深い。電子署名の普及という観点からは、法的な枠組みや商習慣との関連を考慮したビジネスで利用できる電子署名の標準化が求められている。

欧州においては、情報化社会を推進するというビジョンのもと電子署名の標準化が進められている。実際に、現在の世界的な電子署名の標準化もまた、欧州が中心的な役割を果たしている。こうしたことから、まず「欧州における標準化動向」を説明した上で日本における電子署名の標準化との関係を考察する。

欧州においては、1999 年から欧州電子署名標準化イニシアティブ (EESSI : European Electronic Signature Standardisation Initiative) の下で、欧州の標準化団体である欧州標準化委員会 (CEN : European Committee for Standardisation) と欧州電気通信標準化機構 (ETSI : European Telecommunications Standards Institute) により、指令の要件に基づいて電子署名に関する一連の標準が作成されてきた。こうした方針は、現在まで継続されており、これにより欧州においては、現在の日本における電子署名の標準よりも、充実した標準化文書が存在する。

しかし、その欧州においても「電子署名」は、必ずしも広く利用されているとは言い難い状況にある。そのため標準化に対する見直しも行われ 2008 年 11 月には、「European Action Plan on e-signatures and e-identification」が公表されている。この「European Action Plan on e-signatures and e-identification」の公表の 1 年前には、欧州の「電子署名の標準化に関する調査報告書 (Study on the standardisation aspects of e-signatures)」が公開されている。この報告書では、現在の欧州での電子署名の標準化の問題を分析し、「標準化」に関する提案を行っている。この提案が「European Action Plan on e-signatures and e-identification」にも取り込まれている。

この「電子署名の標準化に関する調査報告書」において示されている欧州における電子署名の標準化の成果物を図 1.4.1 に示す。

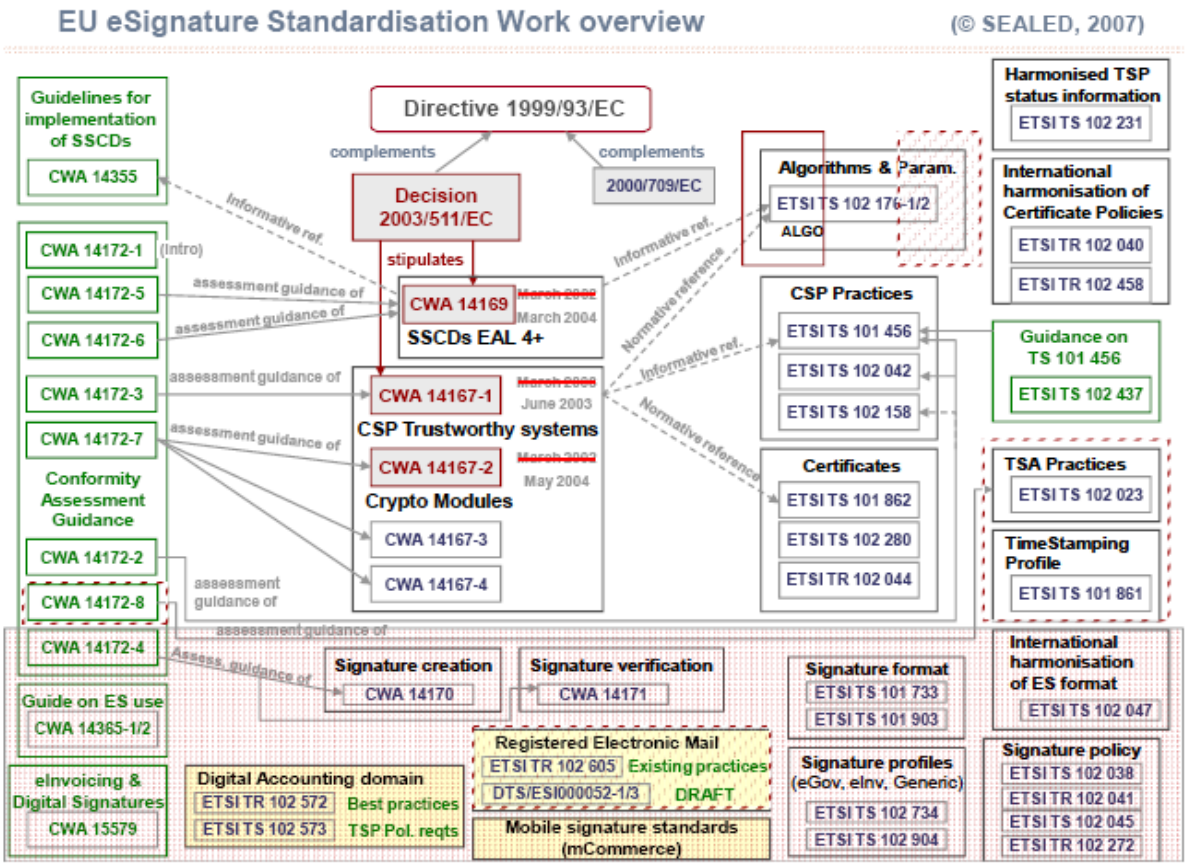



Figure 5: Current eSignature standardisation deliverables grouped per ES product categories

図 1.4.1 電子署名製品のカテゴリーごとにまとめられた現在の電子署名の標準化の成果物

我が国において、電子署名に関連する標準化は、非常に限定されているのに対して、欧州における電子署名の標準化は、非常に多岐に渡っていることが分かる。日本における図 1.4.1 に相当するものを示すことは、実質的にできない。図 1.4.1 の標準化成果物に対応して我が国に存在する標準文書に近いものは、例えば、以下のものがある。

表 1.4.1 日本における電子署名に関連した標準

| 項目 | 内容 |
|---|---|
| 署名フォーマット | ECOM のメンバーが中心となって策定した「JIS X 5092：2008 CMS 利用電子署名（CAdES）の長期署名プロファイル」、「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」がある。 |
| タイムスタンプ関係 | 日本データ通信協会による、「タイムビジネス信頼・安心認定制度」の認定基準として実質的な標準化が行われている。 |
| 認証局の基準 | 電子署名法の特定認証業務認定制度において認定する認証局の基準が存在する。 |

| | |
|---|---|
| 暗号アルゴリズム | CRYPTREC が電子政府推奨暗号リストを作成して公表している。 |
| 暗号モジュールの基準 | JCMVP (Japan Cryptographic Module Validation) |

欧州の電子署名に関連した標準化と比較すると、単発的で、標準化を進める組織間の連携も少なく、用語等も統一もなされていない状況にある。「電子署名の標準化に関する調査報告書」は、欧州における標準化の課題を整理しているが、いくつかの課題は、我が国における状況にも当てはまるものがある。

欧州における電子署名は、「クォリファイド電子署名」、「アドバンスド電子署名」などに分類されている。「クォリファイド電子署名」は、我が国で言えば、概ね電子署名法の認定認証局が発効する証明書を使った署名に相当する。

調査報告書では、これまで標準化の中心にあった「クォリファイド電子署名」について、「要件が多く、したがってコストも高いため開発が難しい場合がある」としている。そして、ビジネスで要求される標準について、「質の高い実装」と「最高レベルの相互運用性」を提供するものを必要としている。ここで「質の高い実装」とは、「最高の質ではないが、コストベネフィットと対象ビジネス分野での適切なリスク軽減の点で適切な質のもの」としている。「クォリファイド電子署名」に対して、これまで標準化が推進されてこなかった「アドバンスド電子署名」は、「質の高い実装」を提供できる可能性があるが、相互運用性が低いという点を指摘している。こうしたことから、「European Action Plan on e-signatures and e-identification」では、「アドバンスド電子署名」の標準化に関する計画も盛り込まれている。

日本においては、欧州ほど電子署名に関する標準化は進んでいないが、やはり似た状況もある。「電子署名法」の認定認証局の認定基準は、多くの要件があり「最高の質」を求めている。そのため、電子署名が利用されるべき多くの領域において、コストベネフィットも考慮されたベストプラクティスを提供している訳ではないところがある。GPKI を中心とした政府の PKI は、相互運用性を考慮しているが、「電子署名法」レベルのものしか使えない。ところが、現在の「電子政府」は、「最高の質」だけを求められている訳ではなく、「適切なリスク軽減の点で適切な質」のものも求められている。ビジネスにおいても、ベストプラクティスが求められているが、「最高の質」の「電子署名法」の認定認証局の認定基準は、多くの場合必要なく、従って「電子署名法」はビジネスに役に立っていない面がある。

こうしたことは、「電子署名法」が検討されていた 2000 年頃という時期にも関係している。この頃は、「ベストプラクティスとしての情報セキュリティ」「適切なリスク軽減」等は、ほとんど認識されておらず、そして、その後も見直しがなされていなかったと言える。

我が国において、標準化文書が存在せず、欧州において盛んに標準化が進められているものに、モバイル署名がある。「電子署名の標準化に関する調査報告書」においても、電子署名の（将来の）実装に関して、期待される有望な技術としてモバイル・ワイアレス技術が上げられている。表 1.4.2 に ETSI が標準化を行ったモバイル署名に関する標準化文書を示す。

表 1.4.2 日本における電子署名に関連した標準

| 標準 | タイトル |
|---|---|
| ETSI TR 102 203 | ビジネスと機能の要件 |
| ETSI TS 102 204 | Web サービスインターフェース |
| ETSI TR 102 206 | セキュリティフレームワーク |
| ETSI TS 102 207 | モバイル署名におけるローミングの仕様 |

モバイル署名は、現在、北欧の国々、スロベニア、トルコ等で展開が図られている。トルコにおいては、モバイル署名が様々な用途で利用できるような環境が整備されつつある。トルコの電子政府等においても税務申告をモバイル署名で行うパイロットプロジェクトが進行している。

参考

http://ec.europa.eu/information_society/eeurope/i2010/esignature/

## 4.2 電子文書の長期保存

(1) 情報資産の増大とポータビリティ

電子化、IT 化の進展とともに、電子文書などの情報資産は質、量ともに増大を続けている。また、コンプライアンスの要求の高まりから、重要な情報は、改ざん等の脅威から保護しながら、保存すべき期間も長くなる傾向にある。一方で、技術の進歩のためシステムは遠からず更改時期を迎え、従来システム内で管理されていた情報資産は、移行を余儀なくされる。

そこで、電子署名技術により、完全性と責任の所在を情報（データ）自身に付加することで、データの独立性、システム非依存を可能とすることが重要になってくる。すなわち、データにポータビリティを持たせることにより、システムからの独立や、システム間の移行が容易となる。

(2) 保存期間の延長とタイムスタンプ

電子署名は、完全性と責任の所在を保証することはできるが、時刻に関する証明機能がないことと、署名の暗号技術に有効期限があることが、長期保存にあたって問題となる。この問題に対しては、タイムスタンプ技術を組み合わせて再署名を行う長期署名の技術がある。この技術により、システムのライフサイクルとは独立に長期にデータを保存することができるようになる。

(3) 文書保存の現状と標準化動向

技術的には電子署名とタイムスタンプにより長期の保存が可能となるが、その規定や運用が標準化されていなければ、いずれ互換性がなくなったり、再利用ができなくなり、保存された意味がなくなってしまう。長期間の保存、組織を超えた広域の流通・利用に対応するためには、基盤と標準化は必須条件と言える。これに対応するため、次世代電子商取引推進協議会（ECOM）では「ECOM 長期署名フォーマット」を策定している。ECOM においては、欧州の標準化機関である ETSI

（欧州通信規格協会）と協力して仕様を作成し、JIS 化の作業を進めてきた。さらに、ISO 化を働きかけ、標準仕様を広く普及させる活動を進めるとともに、この仕様に基づいた相互運用性テストの実施、さらには運用モデルを検討している。真に電子化社会を実現するには、下図に示すように電子署名・ID 管理・タイムスタンプの社会基盤とともに、実際にデータの長期保存を可能とする運用の枠組みを構築する必要がある。

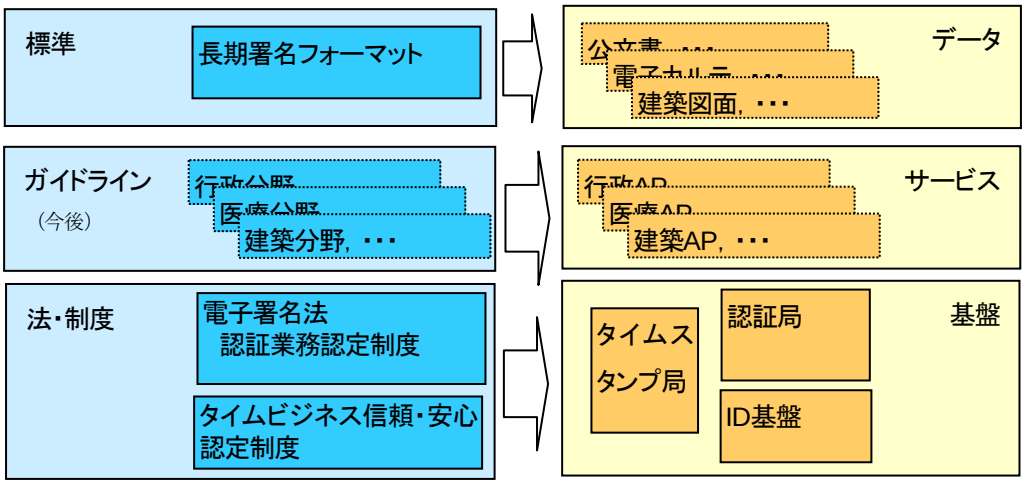



図 1.4.2 長期保存を実現する社会の枠組み

# 第２部　電子文書管理

ECOM として、民間企業の文書・記録の管理への指針を示すべく、第一段階として、ECOM 会員企業における紙・電子文書管理の実態調査を行った。

また、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なった。

# 1. 紙・電子文書管理の実態調査

本実態調査は、電子署名を含む電子記録管理システムの導入を推進するための記録管理規則の雛形の作成、導入ガイドラインの作成を目標とし、民間企業における紙及び電子での文書管理の実態を把握するため、アンケート形式で実態調査を行った。使用したアンケートについては、アンケート項目・内容精査等について、記録管理の専門団体である ARMA 東京支部と記録管理学会の協力を頂いた。

本アンケートでの文書管理の調査事例としては、業種、業態に拘わらず、多くの企業が保有しているものとして、H20 年度から本番を迎えている金融商品取引法（JSOX 法）で、使用する文書を取り上げた。

## 1.1 調査方法、調査期間

ECOM 会員企業に郵送によりアンケートを送付し、郵送にて回収した。

調査期間は 2008 年 11 月 25 日から 12 月末日までである。

## 1.2 質問内容概要

表 2.1.1 に示す 3 つの分類で、アンケートを依頼した。その狙いは、次の通りである。

- 「全社」：各社の文書管理に関する規則・ルールの整備状況の確認。
- 「JSOX 文書」：具体的な文書管理の事例として、JSOX で使用する文書について、その管理方法について、「紙」、「電子」の取扱いの違いを含めた確認。
- 「IT インフラ一般」：各社の電子ファイルの管理システムの状況と業務の電子化状況の確認。

表 2.1.1

| No. | 種別 | 質問概要 |
|---|---|---|
| 1 | 全社 | 文書管理に関する全社的な組織、ルールに関して |
| 2 | JSOX 文書 | JSOX 文書の管理、利用に関して |
| 3 | IT インフラ一般 | 文書管理に関する IT インフラに関して |

## 1.3 回収実績と業種

ECOM 会員企業 111 社にアンケートを依頼し、表 2.1.2 に示すように 27 社から回答を頂いた。

回答頂いた企業の業種については、表 2.1.3 に示すように、「情報」、「電力」、「通信」、「サービス」、「自動車・自動車部品」、「商社」、「その他金融」であった。

表 2.1.2

| | 送付件数 | 回収件数 | 回収率 |
|---|---|---|---|
| 理事会員 | 8 | 2 | 25% |
| A 会員 | 43 | 13 | 30% |
| B 会員 | 60 | 10 | 17% |
| 不明 | | 2 | |
| 総数 | 111 | 27 | 24% |

表 2.1.3

| No | 業種 | 回収社数 | No | 業種 | 回収社数 |
|---|---|---|---|---|---|
| 1 | 情報 | 9 | 5 | 電気機器 | 2 |
| 2 | 電力 | 5 | 6 | 自動車・自動車部品 | 1 |
| 3 | サービス | 3 | 7 | 商社 | 1 |
| 4 | 通信 | 2 | 8 | その他金融 | 1 |

## 1.4 質問内容とアンケート結果集計

質問内容の詳細とアンケート結果の集計については、付録 B-1 に記載する。

アンケート項目毎に、回答社数は異なることから、各集計表には回答社数を記載する。

## 1.5 企業における記録管理の「期待する姿」と「現実の姿」の推定

前記アンケートを実施するに先立って、本 WG にて、質問事項に関連しての民間企業での記録管理のあり方について「期待する姿」の検討と「現実の姿」の推定を行ったので、付録 B-2 に紹介する。

## 1.6 アンケート結果における問題点

アンケート結果から、民間企業の記録管理において、特に問題となると考える点を示し、その理由について推定する。さらに、今後制定を計画している「民間企業の記録管理のガイドライン」への盛込み事項等を対策として、検討する。

ただし、本アンケート結果は実査を行ったものではないので、「会社規則上、ルールが制定されていなくても、現場レベルでは、自主的に綿密な管理を行っていることもある。」、「また、その逆もありえる。」、「問題の発生理由についても、今回は推定であるので、各社に事情を確認しなければ、正確にはわからない。」ということは、読者には、ご留意頂きたい。事実関係の正確な確認のため、次年度以降、追加アンケートを行うなどして、実際の理由を確かめ、対策検討を行う必要がある。

### 1.6.1 「全社」における問題点

(1) 問1. CIOの有無

・アンケート結果）CIOの有無が文書管理ルールや具体的な管理方策に影響していない。

・問題点）CIO の有無に関係なく、文書管理ルールやその具体的な管理方策に企業間で差がある。

・推定理由）CIOの職務の範囲に、文書管理ルール、運用の徹底が入っていない。

・対策方針案）「民間企業の記録管理のガイドライン」に、「CIO の職務責任に、文書管理ルールの設定、その運用の徹底」を含める。

(2) 問2、問4　文書管理ルール、具体的な規程内容

・アンケート結果）「情報セキュリティ規程」、「個人情報管理規程」の制定率は高い。一方、「保管ファイル台帳の作成」、「ファイル管理者の設定」等　紙文書での管理運用を行うための基本的なルールを制定していない会社が6割ある。

・問題点）「紙」を適切に管理するルールを保有しない企業が多い。

・推定理由）会社が新しいなどの理由で、紙文書管理の基本事項について認知していない。

・対策方針案）紙文書管理が今後継続して必要な企業向けに、「民間企業の記録管理のガイドライン」に、紙文書の基本的な管理ルールを入れる。

(3) 問6. 電子文書管理ルール(1)

・アンケート結果）検索用データベース（メタデータ管理など）整備のルールが不十分である。

・問題点）検索に手間取る。メンテナンスが困難。いわゆる電子文書の「ごみ箱化」を招く。

・推定理由）メタデータ管理などの検索用データベースの重要性は十分理解されているものの、いざ、メタデータ等を登録しようとすると、操作性・効率のよい登録ツールが見当たらない。

・対策方針案）本WGとして、メタデータ入力の手間を減らすツールの必要性を示し、ITベンダの開発を促す。

(4) 問6. 電子文書管理ルール(2)

・アンケート結果）紙文書管理、電子文書管理ともに「文書廃棄記録の義務付け」ルールを設定している会社は少ない。

・問題点）廃棄対象文書がそのまま残存するリスクが高まる。米国企業または、米国政府との裁判が起きた場合、e-Discovery 法の適用を受ける可能性がある。米国コールマン／モルガン・スタンレー事件のように、存在しないとした文書（メール）が後に発見されたケースで、多額の賠償金を課せられた事例もある。

・推定理由）わが社に限って当事者になることはないという経営層の思いが、判断を鈍らせており、文書廃棄の重要性を認知していない。また、使いやすいツールの普及が遅れている。

・対策方針案）「民間企業の記録管理のガイドライン」に、「文書廃棄記録の義務付け」のルールを入れ、国内企業への啓蒙を図る。

### 1.6.2 「JSOX 文書」における問題点

(1) 問 4. 社内の原本管理方法、問 6. 監査法人からの紙提出要請

・アンケート結果）監査法人から紙提出を求められている企業が 8 割に達している。また、原本管理について、紙とファイルサーバを併用しているケースが 3.5 割あった。

・問題点）原本は電子であるにかかわず、監査法人提出用だけ紙で保管、提示している可能性がある。紙運用を継続すると運用コストが上がり、紙の使用枚数、CO2 消費が増加し、今後のグリーン対応の流れに逆行することになる。

・推定原因）監査法人の提示に紙を要求されることから、保管する原本まで紙である必要があると誤解している可能性がある。

・対策方針案）監査法人の要求内容を正確に確認する必要がある。少なくとも、原本、閲覧物、提出物などに分けての確認が必要である。保管まで紙にする必要があるとしている場合は、その理由について、監査法人との会話により、その根源になっているものを明らかにする。

(3) 問 7. 紙への押印

・アンケート結果）紙を原本としている場合でも押印している比率は 6 割に留まり、審査・承認等の多段承認をしている企業は 1、2 社と少なかった。

・問題点）押印されていないと保管している紙が原本であるという証拠性（いわゆる真正性）が低くなる。また、多段の承認印　がないと上長が確認したエビデンスが残らない。

・推定原因）企業内で、紙運用における証拠性について基本要件についての認知度が低い

・対策方針案）「民間企業の記録管理ガイドライン」に紙運用での証拠性を保持した運用方法について、紹介する。

(4) 問 10、問 11、問 12　紙保管時のアクセス管理

・アンケート結果）「入退出簿なし」4～5 割、「施錠なし」2～3 割、「アクセス管理簿なし」8 割であり、アクセス管理ルールが不十分なケースが多かった。

・問題点）保管している紙原本の紛失、すり替え、改ざんなどのリスクが高い。

・推定原因）紙原本の紛失、すり替え、改ざんのリスクが、経営者に認知されていない。

・対策方針案）「民間企業の記録管理ガイドライン」に、紙での原本管理におけるすり替え、改ざん防止リスクについて、記載するとともに、リスクを低減する管理手法について、紹介する。

### 1.6.3 「IT インフラ一般」に対しての結果

(1) 問 1. 情報共有手段の利用状況

・アンケート結果）「全社共有サーバを全面的もしくは大部分使用している」企業が、8 割あるものの、「部門共有サーバの使用を全面的もしくは大部分使用している」企業もほぼ同程度ある。文書管理システム使用の企業は 3 割に留まっている。

・問題点）部門共有サーバを利用すると管理対象が多くなり、全社としての文書管理ルールの

徹底が難しい。また、ファイルサーバ主体の情報共有では文書管理ルールの設定などの運用を徹底することが困難である。

・推定原因）部門管理サーバが増え、管理対象が増えることによるコスト増、リスク増が経営者に認知されていない。文書管理システムを使用すると登録が面倒、システム価格が高いというイメージがユーザ部門にある。

・対策方針案）「民間企業の記録管理のガイドライン」に、「CIO の職務責任に、文書管理ルールの設定、その運用の徹底」を含めることで、部門管理サーバ使用によるコスト増、リスク増を CIO から経営者に説明できるようにする。また、文書管理ソフトの登録作業等の操作性アップ、価格低減については、文書管理ソフト開発各社に改善をお願いする。

## 1.7　アンケート結果から見る電子署名の利用拡大について

アンケート結果から見た電子署名の利用拡大に向けての今後の課題について、以下に示す。

(1)　「JSOX 文書」問 8. 電子データの原本性確保

・アンケート結果）JSOX 文書に「電子署名」、「PKI に基づくタイムスタンプ」を利用している企業は 1 社のみ。

・今後の課題）「電子署名」、「PKI に基づくタイムスタンプ」の利用実例の収集を行い、ユーザ企業への紹介を行っていく必要がある。

(2)　「IT インフラ一般」問 2. 電子化が進んでいる業務

・アンケート結果）旅費申請・清算、経費清算・勤怠管理、人事関連申請、備品購入申請など多くの業務で、電子化が進んでいる。稟議書、決裁書は一番遅れているもののそれでも 6 割である。

・今後の課題）会社内の業務の電子化が進んでいることから、「電子署名」、「PKI に基づくタイムスタンプ」の利用シーンを増やすことができる可能性がある。今後は、これら業務への「電子署名」、「PKI に基づくタイムスタンプ」適用ベストプラクティスについて調査する必要がある。

# 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・装置の長期保存性の動向にについて説明する。

尚、最近は省エネルギーニーズも高まっており、長期保存においても今後は保存性だけではなく、エネルギー使用量も選択のファクターとなってくるであろう。磁気ディスクを使用したRAIDシステムにおいても、利用していない RAID グループの磁気ディスクの回転を停止する MAID（Massive Arrays of Inactive Disks）機能を持つ省エネタイプの機種も増えて来ている。

## 2.1 長期電子媒体動向

### 2.1.1 磁気テープの動向

これまでテープ保存寿命については、メーカ独自の評価であり、且つ、評価方法・評価内容などが非公開であった。このため、一般ユーザから見た場合に、業務用の長期保存に利用できるか否かについて判断しかねる状況であった。この状況を打開するため、、2006年、ECOMから財団法人電子情報技術産業協会（JEITA）磁気記録媒体標準化専門委員会に、第3者でのテープ寿命評価とその公開を申し入れた。JEITA　磁気記録媒体標準化専門委員会では、媒体寿命評価SWGを立ち上げ、テープ寿命の加速試験を実施、2008年8月、本WGに説明を頂いた。

一般ユーザ向けには、2008年9月に、JEITA殿のホームページにて、「データテープメディア寿命評価」として以下のURLで公開された。

http://home.jeita.or.jp/is/committee/tech-std/std/com02.html

以下にその概要を引用、紹介します。[1]

(1) 試験対象メディア

- LTO　第3世代
- メディアメーカは5社:イメーション(株)、ソニー(株)、TDK(株)、日立マクセル(株)、富士フイルム（株）

(2) 加速試験条件

55℃　160日間（25℃　保管時　15.4年に相当）

(3) 試験結論

全メディアメーカの製品とも劣化は進まず、明確な寿命推定は出来なかったが、25℃で15年程度の保管では顕著なエラーレートの上昇もなく、全く問題ない安定した製品であることが確認できた。尚、システムの寿命、OS及びソフトウェアの互換性を考慮すると安全かつ安心して、一つのフォーマット媒体にデータを保管する目安は10年と考えられ、10年以上の長期保管するユーザにおいては、10年を目安にデータを移行することを推奨する。

今回のJEITAの結論に関して、本WGからの留意点を以下に示すので、ご参考にして頂きたい。

(1) LTO　第3世代であれば、10年を目安に保管できることがわかった。

(2) どの種類のテープでも共通ではなく、テープ種別やメーカが異なる場合は再度試験が必要。

(3) 今回の試験は、設置環境の良いデータセンタのような場所を想定し、保管時温度25℃を仮

定しているが、これより温度が高くなると寿命は短くなる。テープを長期保存に使用する場合は、温度管理が重要である。

### 2.1.2 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、長期保存の観点からは、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。最近は、データ移行の手間を軽減する機能を保有したRAIDシステムも多く出てきており、磁気ディスクベースでの長期保管の負担も軽減されてきている。

コンプライアンスの観点からは、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。

### 2.1.3 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。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を採用が望ましい。

このため、国内の光ディスクの普及推進を行っている CDs21 ソリューションズ（会長：中島平太郎、事務局：東京都品川区）は、米国の光ストレージ推進団体 OSTA（OpticalStorage Technology Association 米国カリフォルニア）と合同で、長期保存対応か否かを識別する試験方法の国際標準化を進めていたが、2008 年 1 月 13 日、ISO（International Organization for Standardization：国際標準化機構）/IEC（InternationalElectro technical Commission：国際電気標準会議）により正式に国際規格として承認され、規格番号は“ISO/IEC 10995”と決定した。

これにより、これまで、ユーザレベルでは、長期保存性をもったDVDの判別が困難であったが、今後は、この規格を遵守した媒体を使用すれば、長期保存性が担保されるようになってくる。

尚、ブルーレーザを使用したBlu-Ray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、まだ、拙速の感がある。

引用・参考文献

[1] 財団法人電子情報技術産業協会（JEITA）磁気記録媒体標準化専門委員会「データテープメディア寿命評価」

# 付録　B－1　紙・電子文書管理の実態調査　アンケート　集計結果

## 1. 全社に関する質問

【組織に関して】

問1　貴社はCIOを設けていますか。

| 回答内容 | 回答数 | 比率（%） |
|---|---|---|
| 1. はい | 12 | 44% |
| 2. いいえ | 12 | 44% |
| 3. 回答なし | 3 | 11% |
| 回答社数 | 27 | |

分析・補足）CIOを設けている会社は4.5割であった。特に、電力業界にCIOを設けている会社が多い傾向があった。

以下の質問への回答について、CIOを設けている会社といない会社の差異はなかった。

【全社的な文書管理ルールに関して】

問2　全社に適用される文書管理ルールにどのようなものがありますか。

| 回答内容 | | 回答数 | 比率 |
|---|---|---|---|
| 1. | 文書取扱い規程 | 22 | 81% |
| 2. | 文書整理・分類基準 | 15 | 56% |
| 3. | 文書保管・保存基準 | 21 | 78% |
| 4. | ファイル（紙文書）管理規程 | 11 | 41% |
| 5. | 機密文書管理規程 | 20 | 74% |
| 6. | 個人情報管理規程 | 24 | 89% |
| 7. | 示達・通達文書規程 | 14 | 52% |
| 8. | 電子文書管理規程 | 11 | 41% |
| 9. | 電子媒体取扱い基準 | 16 | 59% |
| 10. | 情報セキュリティ管理基準 | 24 | 89% |
| 11. | その他 | 0 | 0% |
| 12. | 回答なし | 1 | 4% |
| 回答社数 | | 27 | |

分析・補足）殆どの企業で、個人情報管理規程、情報セキュリティ規程を設けている。文書取扱い規程、文書保管・保存基準、機密文書管理規程が次いで8割と多い。一方、ファイル（紙文書）管理規程、電子文書管理規程を設定している企業は4割と低い。

問3　イントラネットで社内の人が見られるように公開していますか。

| 回答内容 | | 回答数 | 比率 |
|---|---|---|---|
| 1. | はい | 24 | 89% |
| 2. | どのルールも公開していない。 | 0 | 0% |
| 3. | 一部公開している。 | 2 | 7% |
| 4. | 回答なし | 1 | 4% |
| 回答社数 | | 27 | |

分析・補足）殆どの企業9割で、イントラネットでのルールの公開を実施している。

問4　問2のルールの中での具体的な規程内容

| 回答内容 | | 回答数 | 比率（%） |
|---|---|---|---|
| 1. | 保管ファイル台帳の作成 | 11 | 41% |
| 2. | ファイル管理者の設定 | 13 | 48% |
| 3. | ファイル分類基準 | 11 | 41% |
| 4. | ファイル背表紙記入基準 | 7 | 26% |
| 5. | 文書登録台帳の作成 | 11 | 41% |
| 6. | 文書保管・保存基準 | 24 | 89% |
| 7. | 文書廃棄基準 | 24 | 89% |
| 8. | 文書廃棄記録の義務付け | 7 | 26% |
| 9. | 回答なし | 1 | 4% |
| 回答社数 | | 27 | |

分析・補足）文書保管・保存基準、廃棄基準については殆どの企業で準備されているものの、保管ファイル台帳の作成、ファイル管理者の設定、ファイル分類基準、文書登録台帳については、対応している会社は4～5割と少なめであった。ファイル背表紙や文書廃棄記録の義務付けについての実施企業は3割と少なかった。

【電子文書の管理について】

問5　ファイルサーバや文書管理システムなどのアクセス権、ユーザグループについて管理ポリシー／ルールなどが決まっていますか。

| 回答内容 | | 回答数 | 比率（%） |
|---|---|---|---|
| 1. | はい | 22 | 81% |
| 2. | いいえ | 3 | 11% |
| 3. | 回答なし | 2 | 7% |
| 回答社数 | | 27 | |

分析・補足）殆どの企業で、管理ポリシー／ルールを決定している。

問6　問5で、規程している規則の中に以下のルールは入っていますか。
尚、紙ベースでのファイルをフォルダと称することとします。

| 回答内容 | | 回答数 | 比率（%） |
|---|---|---|---|
| 1. | フォルダ一覧表の作成（データベース化） | 9 | 41% |
| 2. | フォルダ管理者の設定 | 13 | 59% |
| 3. | フォルダ分類基準 | 8 | 36% |
| 4. | 文書保管・保存基準 | 11 | 50% |
| 5. | 文書一覧表の作成（データベース化） | 7 | 32% |
| 6. | 文書廃棄基準 | 10 | 45% |
| 7. | 文書廃棄記録の義務付け | 5 | 23% |
| 8. | 回答なし | 5 | 23% |
| 問5　回答“1”の社数 | | 22 | |

分析・補足）フォルダの管理者の設定については8割と設定率が高いが、その他の事項については、設定率が低くなっている。特に、文書廃棄記録の義務付けを行っている企業は3割と低い。尚、文書廃棄記録の義務付けを行っている企業は他の項目についても全て設定している傾向がある。

問7　アクセス権設定は誰が行いますか。

| 回答内容 | | 回答数 | 比率（%） |
|---|---|---|---|
| 1. | 全て情報システム部門 | 7 | 26% |
| 2. | 情報システム部門が各部門毎に、親フォルダを割当、その下を各部門の管理者が実施 | 12 | 44% |
| 3. | 情報システム部門が各部門毎に、親フォルダを割当、その下を各部門で実施 | 3 | 11% |
| 4. | その他 | 1 | 4% |
| 5. | 回答なし | 4 | 15% |
| 回答社数 | | 27 | |

分析・補足）全てを情報システム部門で設定している企業が3割あった。各部門の責任で実施している企業が6.5割で、その内の8割が各部門の管理者が管理を実施している。

問8　近年、原本を紙から電子情報に変更した業務がありますか。

| 回答内容 | | 回答数 | 比率（%） |
|---|---|---|---|
| 1. | ある | 6 | 22% |
| 2. | ない | 18 | 67% |
| 3. | 回答なし | 3 | 11% |
| 回答社数 | | 27 | |

分析・補足）紙から電子情報への変更をおこなった企業は2.5割と少なかった。

問8-1、2、3
問8で「はい」と回答された方に、質問します。
その具体的な業務内容、切り替え時期、切り替え理由
回答）業務内容としては「給与明細配布」、「経理処理」、「役員会資料配布」、「パソコン利用申請」など、切り替え時期は2007/後半から2008/前半であった。切り替え理由は、「JSOX対応」ではなく、「業務効率改善」、「ペーパレス化」、「システム更改に伴う見直し」であった。

## 2. JSOXへの取組みについての質問

【会社区分】

問1　JSOX対象会社ですか。

| 回答内容 | | 回答数 | 比率 |
|---|---|---|---|
| 1. | JSOX、及び米SOX対象上場企業 | 3 | 12% |
| 2. | JSOX対象上場企業 | 12 | 48% |
| 3. | 上場準備中 | 1 | 4% |
| 4. | JSOX又は米SOX対象上場企業の関連会社 | 4 | 16% |
| 5. | 上記に当てはまらない | 5 | 20% |
| 回答社数 | | 25 | |

問2　貴社の内部統制整備の準備状況についてお聞かせください。

| 回答内容 | | 回答数 | 比率 |
|---|---|---|---|
| 1. | 取組みを実施していない | 0 | 0 |
| 2. | 取組み準備中 | 1 | 6% |
| 3. | 取組み中 | 6 | 35% |
| 4. | ほぼ対応済み | 10 | 59% |
| 回答社数 | | 17 | |

問3　問2で、2～4を回答された方に質問します。

| 回答内容 | | 回答数 | 比率 |
|---|---|---|---|
| 1. | 文書化パイロットプロジェクト実施済み | 18 | 100% |
| 2. | 文書化作業全社展開済み | 17 | 94% |
| 3. | 整備状況評価パイロットプロジェクト実施済み | 17 | 94% |
| 4. | 整備状況評価全社展開済み | 16 | 89% |
| 5. | 運用テストパイロットプロジェクト実施済み | 17 | 94% |
| 6. | 運用テスト全社展開済み | 16 | 89% |
| 7. | 有効性評価パイロットプロジェクト実施済み | 12 | 67% |
| 8. | 有効性評価全社展開済み | 8 | 44% |
| 回答社数 | | 18 | |

【文書保管区分】

問4　社内の原本の保管方法を教えてください。

【上段：回答数、下段：比率】

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 紙 | 10 | 8 | 14 | 10 | 14 |
| | | 59% | 57% | 88% | 63% | 88% |
| 2. | ファイルサーバ | 9 | 5 | 2 | 5 | 3 |
| | | 53% | 36% | 13% | 31% | 19% |
| 3. | 汎用文書管理システム | 0 | 0 | 0 | 0 | 0 |
| | | 0% | 0% | 0% | 0% | 0% |
| 4. | J-SOX用文書管理システム | 7 | 6 | 1 | 4 | 2 |
| | | 41% | 43% | 6% | 25% | 13% |
| 4-1. | いわゆる汎用文書管理ソフト | 1 | 1 | 0 | 1 | 0 |
| | | 6% | 7% | 0% | 6% | 0% |
| 4-2. | 市販J-SOX専用機能付き文書管理ソフト | 3 | 2 | 1 | 1 | 0 |
| | | 18% | 14% | 6% | 6% | 0% |
| 4-3. | 自社独自文書管理ソフト | 3 | 2 | 1 | 2 | 1 |
| | | 18% | 14% | 6% | 13% | 6% |
| 5. | その他 | 0 | 0 | 0 | 0 | 0 |
| | | 0% | 0% | 0% | 0% | 0% |
| 電子データ保管（No.2～No.4） | | 16 | 11 | 3 | 9 | 5 |
| | | 94% | 65% | 18% | 53% | 29% |
| 回答社数 | | 17 | 14 | 16 | 16 | 16 |

分析・補足）文書化の3点セットについては、紙での管理が6割、ファイルサーバでの管理が5割、JSOX用文書管理システムでの管理が4割であった。紙、ファイルサーバの両方で管理しているケースも3.5割あった。整備状況／運用テストのテスト報告書については、紙での管理は6割と多く、JSOX用文書管理システムの使用比率は整備状況において、2.5割、運用テストでは1割と文書化3点セットよりは低い普及率であった。整備状況／運用テストのエビデンスでは紙での管理が9割を占めている。

問4-1　J-SOX用文書管理システムをご利用の方に質問します。

以下の機能はご利用でしょうか。

| 回答内容 | | 回答数 | 比率 |
|---|---|---|---|
| 1. | 承認機能（決裁機能） | 4 | 57% |
| 2. | 文書作成、テスト等工程の進捗報告・確認機能 | 4 | 57% |

| | | | |
|---|---|---|---|
| 3. | テスト実績、テスト結果、評価判定の Web 入力 | 3 | 43% |
| 4. | テスト実績、テスト結果、評価判定の一覧表示 | 4 | 57% |
| 回答社数 | | 7 | |

問5　監査法人への提示方法

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3 点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 紙提出 | 13 | 11 | 12 | 11 | 12 |
| | | 72% | 79% | 86% | 79% | 86% |
| 2. | システム画面 | 1 | 1 | 1 | 1 | 1 |
| | | 6% | 7% | 7% | 7% | 7% |
| 3. | 電子ファイル | 7 | 3 | 2 | 3 | 2 |
| | | 39% | 21% | 14% | 21% | 14% |
| 回答社数 | | 18 | 14 | 14 | 14 | 14 |

分析・補足）監査法人にシステム画面、電子ファイルを提示しているケースはあるが、監査法人には紙で、提示している企業が 7～9 割である。

問6　監査法人から紙提出を求められていますか。

| 回答内容 | 回答数 | 比率 |
|---|---|---|
| 1. はい | 8 | 80% |
| 2. いいえ | 2 | 20% |
| 回答社数 | 10 | |

分析・補足）8 割の企業が監査法人から紙提出を求められている。

【原本作成】

問7　紙を原本としている場合押印していますか。

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3 点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 書類への押印有り | 6 | 5 | 5 | 6 | 5 |
| | | 60% | 63% | 36% | 60% | 36% |
| 2. | 書類への審査・承認等多段押印有り。 | 2 | 0 | 1 | 0 | 1 |
| | | 20% | 0% | 7% | 0% | 7% |
| 3. | 回答なし | 4 | 3 | 9 | 4 | 9 |
| | | 40% | 38% | 64% | 40% | 64% |
| 問4　紙原本　回答社数 | | 10 | 8 | 14 | 10 | 14 |

分析・補足）文書化3点セット、整備状況／運用テストのテスト報告書については6割の企業が押印をしている。整備状況／運用テストのエビデンスについては、押印している企業の割合は3.5割と少ない。さらに審査・承認等の多段の押印を行っている企業は1、2社程度と少ない。

問8　電子データを原本としている場合、原本性の確保にはどこまでの手段を講じていますか。

【上段：回答数、下段：比率%】

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | ワークフロー履歴 | 6 | 4 | 1 | 3 | 1 |
| | | 38% | 36% | 33% | 33% | 20% |
| 2. | 電子署名 | 1 | 1 | 0 | 1 | 0 |
| | | 6% | 9% | 0% | 11% | 0% |
| 3. | PKI に基づくタイムスタンプ | 1 | 1 | 0 | 1 | 0 |
| | | 6% | 9% | 0% | 11% | 0% |
| 4. | その他 | 2 | 2 | 2 | 1 | 1 |
| | | 13% | 18% | 67% | 11% | 20% |
| 5. | 回答なし | 8 | 5 | 8 | 5 | 3 |
| | | 50% | 45% | 267% | 56% | 60% |
| 問4　電子データ原本　回答社数 | | 16 | 11 | 3 | 9 | 5 |

分析・補足）原本性確保の手段として、ワークフロー履歴を挙げている会社が3～4割、電子署名、PKIを挙げている会社は1社に留まった。JSOX文書管理システムを使用の場合、ワークフロー履歴を挙げることが多い。

【紙保管】

問9　紙保管している文書・エビデンスを集中管理していますか。分散管理していますか。

【上段：回答数、下段：比率】

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 事務局集中管理 | 8 | 8 | 9 | 8 | 10 |
| | | 62% | 80% | 60% | 73% | 67% |
| 2. | 部署別等分散管理 | 5 | 2 | 6 | 3 | 5 |
| | | 38% | 20% | 40% | 27% | 33% |
| 回答社数 | | 13 | 10 | 15 | 11 | 15 |

分析・補足）事務局に集中管理している企業が6割～8割と多い。その中でも整備状況／運用テ

ストのテスト報告書は7割～8割と高率になっている。

問10　保管場所への入退出管理

【上段：回答数、下段：比率】

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 入退出簿あり | 8 | 6 | 6 | 6 | 6 |
| | | 67% | 60% | 46% | 60% | 43% |
| 2. | 入退出簿なし | 4 | 4 | 7 | 4 | 8 |
| | | 33% | 40% | 54% | 40% | 57% |
| 回答社数 | | 12 | 10 | 13 | 10 | 14 |

分析・補足）入退出簿で管理しているのは、文書化3点セット、整備状況／運用テストの報告書については、6～7割、整備状況／運用テストのエビデンスについては、4～5割とやや低くなっている。

問11　保管キャビネトもしくはファル棚には施錠していますか。

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 施錠あり | 11 | 7 | 10 | 8 | 10 |
| | | 79% | 70% | 67% | 73% | 67% |
| 2. | 施錠なし | 3 | 3 | 5 | 3 | 5 |
| | | 21% | 30% | 33% | 27% | 33% |
| 回答社数 | | 14 | 10 | 15 | 11 | 15 |

分析・補足）施錠ありの企業が7割であった。

問12　保管キャビネトもしくはファイル棚の施錠管理簿はありますか。

【上段：回答数、下段：比率】

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | アクセス管理簿あり | 3 | 2 | 3 | 2 | 3 |
| | | 21% | 20% | 20% | 18% | 20% |
| 2. | アクセス管理簿なし | 11 | 8 | 12 | 9 | 12 |
| | | 79% | 80% | 80% | 82% | 80% |
| 回答社数 | | 14 | 10 | 15 | 11 | 15 |

分析・補足）アクセス管理簿を使用している企業は2割（2～3社）に留まっている。

【電子保管】

問13　電子保管している文書・エビデンスを集中管理していますか。分散管理していますか。

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 全社集中管理 | 14 | 8 | 5 | 9 | 3 |
| | | 88% | 89% | 100% | 90% | 75% |
| 2. | 部署別等分散管理 | 2 | 1 | 1 | 1 | 1 |
| | | 13% | 11% | 20% | 10% | 25% |
| 回答社数 | | 16 | 9 | 5 | 10 | 4 |

分析・補足）全社集中管理している企業が8～9割

問14　アクセス管理はどのレベルで行っていますか。

【上段：回答数、下段：比率】

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | アクセス権設定 | 16 | 11 | 5 | 9 | 5 |
| | | 100% | 100% | 100% | 100% | 100% |
| 2. | アクセス権ログ保管 | 6 | 3 | 1 | 2 | 1 |
| | | 38% | 27% | 20% | 22% | 20% |
| 3. | アクセスログ監査 | 0 | 0 | 0 | 0 | 0 |
| | | 0% | 0% | 0% | 0% | 0% |
| 回答社数 | | 16 | 11 | 5 | 9 | 5 |

分析・補足）アクセス権限の設定はおこなっているが、アクセスのログ管理を行っている会社は文書化3点セットで、4割、整備状況／運用テストの報告書、エビデンスで2割であった。その監査については実施している会社はなかった。

問15　集めたJSOX文書やエビデンスを社内の業務改善検討や、社外へのCSR等のPRに利用できるように、参照や加工ができるようにしてありますか。

| 回答内容 | 回答数 | 比率（%） |
|---|---|---|
| 1. はい | 8 | 44% |
| 2. いいえ | 10 | 56% |
| 回答社数 | 18 | |

分析・補足）4～5割の企業で他に活用するようにしている。

問16　問15で、「はい」と回答した方に質問します。
どのように利用していますか。
回答）業務改善に向けた検討用とするものが多かった。

## 3. 全社一般についての質問

問1　情報共有手段の利用状況について教えてください。

【上段：回答数、下段：比率】

| | 全く利用していない | 一部利用している | 大部分が利用している | 全面的に利用している |
|---|---|---|---|---|
| 部門ファイルサーバ | 2 | 3 | 5 | 12 |
| | 9% | 13% | 22% | 52% |
| 部門文書管理システム | 4 | 9 | 1 | 4 |
| | 17% | 39% | 4% | 17% |
| 全社共有サーバ | 5 | 2 | 4 | 14 |
| | 22% | 9% | 17% | 61% |
| 文書管理システム（ECM等も含む） | 2 | 7 | 0 | 7 |
| | 9% | 30% | 0% | 30% |
| 回答社数 | 23 | | | |

ECMとはEnterprise Content Managementシステムの略です。

分析・補足）「全社共有サーバを全面的もしくは大部分使用している」企業が、8割ある。一方で、「部門共有サーバの使用を全面的もしくは大部分使用している」企業もほぼ同程度あり、全社共有サーバと部門共有サーバが併用されている企業が多い。文書管理システム使用の企業は3割に留まり、ファイルサーバでの情報共有が主体となっている。

問2　以下の業務の中で、電子化が進んでいるものを教えてください。

| 回答内容 | | 回答数 | 比率 |
|---|---|---|---|
| 1. | 旅費申請・清算 | 18 | 86% |
| 2. | 経費清算 | 18 | 86% |
| 3. | 勤怠管理・勤怠申請 | 20 | 95% |
| 4. | 人事関連申請 | 14 | 67% |
| 5. | 備品購買申請 | 15 | 71% |
| 6. | 稟議書、決裁文書 | 13 | 62% |
| 回答社数 | | 21 | |

分析・補足）勤怠管理・勤怠申請については殆どの会社で電子化が済んでいる。
旅費精算・申請、経理精算についても電子化率が高く、電子化率は8.5割、ついで、備品購入申請、人事関連申請が7割となっている。稟議書、決裁書は一番遅れているもののそれでも6割である。

# 付録　B－2　紙・電子文書管理の実態調査　アンケート

## 「期待する姿」と「現実の姿の推定」

4．全社に関する質問

【組織に関して】

問1．貴社はCIOを設けていますか。

① 期待する姿：CIOは文書管理にも責任を持ち、CIOが設置されている企業は、文書管理に関するルール・規程さらにはその具体的な運用内容についてもルール化している。

② 現実の姿の推定：CIO 設置の有無は、文書管理ルール、規程さらにはその具体的内容の整備に関連していない。

【全社的な文書管理ルールに関して】

問2　全社に適用される文書管理ルールにどのようなものがありますか。

| 項番 | 回答選択肢 |
|---|---|
| 1. | 文書取扱い規程 |
| 2. | 文書整理・分類基準 |
| 3. | 文書保管・保存基準 |
| 4. | ファイル（紙文書）管理規程 |
| 5. | 機密文書管理規程 |
| 6. | 個人情報管理規程 |
| 7. | 示達・通達文書規程 |
| 8. | 電子文書管理規程 |
| 9. | 電子媒体取扱い基準 |
| 10. | 情報セキュリティ管理基準 |
| 11. | その他 |

① 期待する姿：項番1～10のルールまたは規程については何らかの形で保有している。

② 現実の姿の推定：個人情報管理規程は全ての企業が保有している。機密文書管理規程、情報セキュリティ管理基準についても8割程度は保有している。しかしながら、これらの運用に関連する電子文書・電子媒体に関する項番8、9については、2割程度しか保有しない。

問3　イントラネットで社内の人が見られるように公開していますか。

① 期待する姿：9割以上の企業が、イントラネットで規則・ルールを公開している。

② 現実の姿の推定：同上

問4　問2のルールの中での具体的な規程内容

| 項番 | 回答選択肢 |
|---|---|
| 1. | 保管ファイル台帳の作成 |
| 2. | ファイル管理者の設定 |
| 3. | ファイル分類基準 |
| 4. | ファイル背表紙記入基準 |
| 5. | 文書登録台帳の作成 |
| 6. | 文書保管・保存基準 |
| 7. | 文書廃棄基準 |
| 8. | 文書廃棄記録の義務付け |

①　期待する姿：項番1～8の具体的な規程を所有する。

②　現実の姿の推定：殆どの企業で、項番6、7を設定しているが、他の項目については5割程度、特に、項番8については、設定している企業は稀である。

【電子文書の管理について】

問5　ファイルサーバや文書管理システムなどのアクセス権、ユーザグループについて管理ポリシー／ルールなどが決まっていますか。

①　期待する姿：これらの管理ポリシー、ルールを設定する。

②　現実の姿の推定：殆どの企業がなんらかの形で、これらのポリシー、ルールを設定している。

問6　問5で、規程している規則の中に以下のルールは入っていますか。
尚、紙ベースでのファイルをフォルダと称することとします。

| 項番 | 回答選択肢 |
|---|---|
| 1. | フォルダ一覧表の作成（データベース化） |
| 2. | フォルダ管理者の設定 |
| 3. | フォルダ分類基準 |
| 4. | 文書保管・保存基準 |
| 5. | 文書一覧表の作成（データベース化） |
| 6. | 文書廃棄基準 |
| 7. | 文書廃棄記録の義務付け |

①　期待する姿：全てをルールまたは規程にしている。

②　現実の姿の推定：項番2は殆どの企業で、制定しているものの、他の項目については、制定している会社は少ない。

問7　アクセス権設定は誰が行いますか。

| 項番 | 回答選択肢 |
|---|---|
| 1. | 全て情報システム部門 |

| | |
|---|---|
| 2. | 情報システム部門が各部門毎に、親フォルダを割当、その下を各部門の管理者が実施 |
| 3. | 情報システム部門が各部門毎に、親フォルダを割当、その下を各部門で実施 |
| 4. | その他 |

① 期待する姿：会社の業種などに左右されるが項番 1 または項番 2 のいずれかで、アクセス権の設定を実施する。

② 現実の姿の推定：殆どの企業が項番 1 または項番 2 で、アクセス権設定を実施しているものの、項番 3 で、実施している企業が少数ある。項番 3 では、部門内でアクセス権の設定の仕方に属人的な差が出る可能性が残る。

問 8　近年、原本を紙から電子情報に変更した業務がありますか。

問 8-1、2、3

問 8 で「はい」と回答された方に、質問します。

① 期待する姿：JSOX を契機に、原紙を紙から電子情報に変えた業務がある。

② 現実の姿の推定：同上

## 5. JSOX への取組みについての質問

【文書保管区分】

問 4　社内の原本の保管方法を教えてください。

| 項番 | 区分 | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3 点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 紙 | | | | | |
| 2. | ファイルサーバ | | | | | |
| 3. | 汎用文書管理システム | | | | | |
| 4. | J－SOX 用文書管理システム | | | | | |
| 4-1. | いわゆる汎用文書管理ソフト | | | | | |
| 4-2. | 市販 J-SOX 専用機能付き文書管理ソフト | | | | | |
| 4-3. | 自社独自文書管理ソフト | | | | | |
| 5. | その他 | | | | | |

① 期待する姿：原本の管理は「紙」ではなく、項番 2～4 の電子管理を全面的に使用する。できれば、JSOX 用文書管理ソフトを使用する。

② 現実の姿の推定：「紙」を原本としている企業も半数近くは残存している。

問5　監査法人への提示方法

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 紙提出 | | | | | |
| 2. | システム画面 | | | | | |
| 3. | 電子ファイル | | | | | |

①　期待する姿：「システム画面」または「電子ファイル」での提示

②　現実の姿の推定：「紙」での提出が殆ど

問6　監査法人から紙提出を求められていますか。

①　期待する姿：「紙」での提出は求められていない。

②　現実の姿の推定：殆どの企業が「紙」での提出を求められている。

【原本作成】

問7　紙を原本としている場合押印していますか。

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 書類への押印有り | | | | | |
| 2. | 書類への審査･承認等多段押印有り。 | | | | | |

①　期待する姿：「紙」原本には押印がある。できれば、上長承認までの多段の押印をしている。

②　現実の姿の推定：殆どの企業で押印している。上長承認まではされていないことも多い。

問8　電子データを原本としている場合、原本性の確保にはどこまでの手段を講じていますか。

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | ワークフロー履歴 | | | | | |
| 2. | 電子署名 | | | | | |
| 3. | PKIに基づくタイムスタンプ | | | | | |
| 4. | その他 | | | | | |

①　期待する姿：3 点セット、テス報告書については、ワークフロー履歴の実施が望ましい。エビデンスについては、電子署名、PKIによるタイムスタンプまでが望ましい。

②　現実の姿の推定：ワークフロー履歴を活用しているケースは半数程度、電子署名、PKI によるタイムスタンプについては殆ど活用されていない。

【紙保管】

問9　紙保管している文書・エビデンスを集中管理していますか。分散管理していますか。

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 事務局集中管理 | | | | | |
| 2. | 部署別等分散管理 | | | | | |

①　期待する姿：全て、事務局集中管理

②　現実の姿の推定：半数は部署別等分散管理

問10　保管場所への入退出管理

問11　保管キャビネトもしくはファル棚には施錠していますか。

問12　保管キャビネトもしくはファイル棚の施錠管理簿はありますか。

①　期待する姿：「保管場所への入退出管理」、「保管キャビネトもしくはファル棚の施錠」、「施錠管理」これら全ての管理している。

②　現実の姿の推定：「保管場所への入退出管理」は5割程度、「保管キャビネトもしくはファル棚の施錠」は9割程度、「施錠管理」は3割程度の実施である。

【電子保管】

問13　電子保管している文書・エビデンスを集中管理していますか。分散管理していますか。

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | 全社集中管理 | | | | | |
| | | | | | | |
| 2. | 部署別等分散管理 | | | | | |
| | | | | | | |

①　期待する姿：全て、全社集中管理

②　現実の姿の推定：殆どの企業が全社集中管理を実施

問14　アクセス管理はどのレベルで行っていますか。

| | | 文書化 | 整備状況 | | 運用テスト | |
|---|---|---|---|---|---|---|
| | | 3点セット | テスト報告書 | エビデンス | テスト報告書 | エビデンス |
| 1. | アクセス権設定 | | | | | |
| 2. | アクセス権ログ保管 | | | | | |
| 3. | アクセスログ監査 | | | | | |

① 期待する姿：全ての会社で、アクセス権の設定、アクセスログの保管、アクセスログ監査を実施している。

② 現実の姿の推定：全ての会社で、アクセス権の設定は行っている。アクセスログの保管まで行っているのは半数、アクセスログ監査の実施は少ない。

## 6. 全社一般についての質問

問1　情報共有手段の利用状況について教えてください。

| | 全く利用していない | 一部利用している | 大部分が利用している | 全面的に利用している |
|---|---|---|---|---|
| 部門ファイルサーバ | | | | |
| 部門文書管理システム | | | | |
| 全社共有サーバ | | | | |
| 文書管理システム（ECM 等も含む） | | | | |

ECM とは Enterprise Content Management システムの略です。

① 期待する姿：部門ファイルサーバ、部門文書管理システムは全く利用しない。全社共有サーバ、ECM 等を含む全社用の文書管理システムを全面的に利用する。

② 現実の姿の推定：部門ファイルサーバ、部門文書管理システムを一部利用している。全社共有サーバについては、大部分が利用している。ECM 等を含む全社用の文書管理システムは、一部利用に留まっている。

問2　以下の業務の中で、電子化が進んでいるものを教えてください。

| 項番 | 回答選択肢 |
|---|---|
| 1. | 旅費申請・清算 |
| 2. | 経費清算 |
| 3. | 勤怠管理・勤怠申請 |
| 4. | 人事関連申請 |
| 5. | 備品購買申請 |
| 6. | 稟議書、決裁文書 |

① 期待する姿：全ての業務が電子化されている。

② 現状の姿の推定：定型化されていることが多い項番 1～5 は電子化率 8 割程度、稟議書、決裁文書については、非定型であることから電子化が進んでおらず、3 割程度

# 第３部　署名仕様

ECOM では長期署名フォーマットのプロファイルの標準化活動を進めており、2008 年 3 月にはそのプロファイルを原案とする JIS 規格「JIS X 5092：2008 CMS 利用電子署名（CAdES）の長期署名プロファイル」、「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」が制定された。これらの JIS 規格の制定により、長期署名フォーマットのさらなる利用促進が期待できる。長期署名フォーマットが普及するとともに、実運用において次のような問題がますます顕在化すると考えられる。

- 相互運用性の問題
  正しく実装・運用するためには JIS 規格が参照する規格書を併せて理解する必要がある。参照する規格を誤解なく全て理解することは労力を要する。各実装間で仕様の解釈に食い違いが発生してしまう可能性がある。
- 文書フォーマットとの適合性
  実際に長期署名フォーマットを使用する場合には、例えば XML や PDF といった文書フォーマットへ組み込み使用したいケースも多いと考えられる。長期署名フォーマットと文書フォーマットの仕様の適合性が課題となる。

相互運用性の問題に対して、ECOM では相互運用性実証実験の実施や、技術解説を報告書としてまとめるなどの活動を行ってきた。平成 18 年度の報告書「電子文書長期保存ハンドブック」は開発者が長期署名フォーマット規格の全容を理解する助けとなるように作成したものである。今回はハンドブックを補間するものとして、実際に利用する場合に直面するであろういくつかの留意点に対して考察を行っている。1 章では、特に長期署名フォーマットの検証に焦点をあて、最低限必要であると考えられる検証項目をまとめている。さらに、長期署名の時刻順序を考慮した証明書のパス検証の考察を加えている。また、長期署名フォーマットにおける証明書の信頼点や失効情報の管理について 2 章で考察している。

文書フォーマットの適合性については､ODF と OOXML の実装に対して XAdES の適用実験を行い、その実験により明らかになった課題を 3 章でまとめている。PDF については、本報告書の付録に PDF 長期署名の標準化活動の記録を掲載しているので参照されたい。

また、長期署名に関連する規格として ERS（Evidence Record Syntax）が新たに登場した。アーカイブタイムスタンプを付与する別の方法であり、JIS 規格との適合性を今後検討する必要があるだろう。4 章では ERS の概要を紹介し、JIS 規格への導入案を述べる。

# 1. 長期署名の検証とパス検証についての考察

## 1.1 目的と概要

ここでは参考例として長期署名の ES / ES-T / ES-A における検証プロセスに関して簡単にまとめる。長期署名の検証で必要となる主な検証事項を 1.2 節でまとめる。長期署名を含む電子署名を検証する際には、公開鍵証明書（以下、証明書）の認証パスの構築と検証が必要となる。1.3 節では長期署名における認証パスの検証について時刻の順序関係に着目して考察する。証明書の

認証パスの構築や検証の詳細はここでは触れない。認証パスの具体的な検証方法は RFC 5280（旧版は RFC 3280）/ RFC 2560 にて標準規格化されているので参照されたい。

## 1.2 長期署名の検証

ここでは長期署名の検証に必要な最低限の項目について記述する。

### 1.2.1 概要

長期署名の署名フォーマットは以下の形式に分けられる。

| 形式 | 説明 |
|---|---|
| ES | 署名者に関する情報と署名データを格納した形式 |
| ES-T | 署名時刻を担保する署名タイムスタンプを付与した形式 |
| ES-C | 署名検証の為の一連の証明書と失効情報に対する参照情報を付与した形式 |
| ES-X Long | 署名検証の為の一連の証明書と失効情報を格納した形式 |
| ES-A | 署名データやタイムスタンプ、検証情報等を保護する為にアーカイブタイムスタンプを付与した形式 |

これらの形式のうち、ES-C と ES-X Long は ES-A を生成する過程の形式と考え、ここでは ES / ES-T / ES-A の 3 形式の検証プロセスに関して簡単に項目をまとめる。なお詳しいプロセスや検証内容に関しては長期署名フォーマット CAdES/XAdES の標準規格やハンドブック/ガイドブックを参照すること。

### 1.2.2 ES（電子署名）の検証

ES の検証では以下の項目を検証する。各項目の検証順序は問われない。

| |
|---|
| 1）署名データ形式の検証<br>データ形式の正しさを検証する以下のすべてを確認する。<br>・正しいデータ構造であること。<br>・プロファイルで規定されている必須要素をもつこと。<br>・バージョン番号の整合性。 |
| 2）署名者の証明書の検証<br>署名者の証明書の有効性を RFC 5280 に倣い検証する。現在時刻での有効性を確認する。<br>・署名者の証明書に対して認証パスの構築と検証を行う。 |
| 3）署名者の署名の検証<br>署名に改ざんがないことを検証する<br>3-1）値の整合性の検証<br>以下のすべてを確認する。<br>・署名対象文書と、そのハッシュ値を照合する。<br>・署名値を署名者の証明書に含まれる公開鍵により検証する。<br>3-2）識別情報の整合性の検証<br>・署名者の識別情報と証明書が一致することを確認する。 |

### 1.2.3 ES-T の検証

ES-T の検証では以下の項目を検証する。検証の項目には 1.2.2 節の ES の検証の内容を含む。各項目の検証順序は問われない。

| |
|---|
| 1）署名タイムスタンプの検証<br>適切なタイムスタンプであることを検証する。以下の工程からなる。<br>1-1）署名タイムスタンプを発行した TSA の証明書の検証<br>以下のすべてを確認する。<br>・TSA 証明書に対して認証パスの構築と認証パスの検証を行い、検証時点における証明書の有効性を確認する。<br>・TSA 証明書の鍵使用目的が適切である事を確認する。<br>1-2）署名タイムスタンプを発行した TSA の署名の検証<br>・TSA 証明書の公開鍵を用いてタイムスタンプトークンの署名値を検証する。<br>1-3）署名タイムスタンプとタイムスタンプ対象との整合性検証<br>・タイムスタンプトークンの MessageImprint とタイムスタンプ対象となるデータを照合する。 |
| 2）署名タイムスタンプが示す時刻における ES の検証<br>署名時刻に基づき ES の検証を行う。以下の工程からなる。<br>2-1）署名時刻における ES の検証<br>署名タイムスタンプが示す時刻を想定して「1.2.2.ES（電子署名）の検証」を実施する。<br>署名タイムスタンプが示す時刻において署名者の証明書が有効である事を確認する。<br>2-2）ES の信頼点の正当性の確認<br>信頼点が適切なものであるか確認する（※1）。 |

署名者の証明書や署名タイムスタンプの TSA 証明書の検証については 1.3 節で考察しているので参照のこと。

### 1.2.4 ES-A の検証

ES-A の検証は以下の項目を検証する。検証の項目には 1.2.3 節の ES-T の検証の内容を含む。各項目の検証順序は問われない。

| |
|---|
| 1）最新のアーカイブタイムスタンプの検証<br>適切なタイムスタンプであることを検証する。以下の工程からなる。<br>1-1）最新のアーカイブタイムスタンプを発行した TSA の証明書の検証<br>以下のすべてを確認する。<br>・TSA 証明書に対して認証パスの構築と認証パスの検証を行い、検証時点における証明書の有効性を確認する。<br>・TSA 証明書の鍵使用目的が適切である事を確認する。<br>1-2）最新のアーカイブタイムスタンプを発行した TSA の署名の検証<br>・TSA 証明書の公開鍵を用いてタイムスタンプトークンの署名値を検証する。 |

| |
|---|
| 1-3）最新のアーカイブタイムスタンプとタイムスタンプ対象との整合性検証<br>・タイムスタンプトークンの MessageImprint とアーカイブタイムスタンプの対象となるデータを照合する。 |
| 2）前世代～過去のアーカイブタイムスタンプの検証（存在する場合のみ）<br>検証対象となるアーカイブタイムスタンプに対し、一世代後の（一世代新しい）アーカイブタイムスタンプが示す時刻を想定して、「1）最新のアーカイブタイムスタンプの検証」と同様の検証を実施する。<br>2-1）アーカイブタイムスタンプを発行した TSA の証明書の検証<br>一世代後のアーカイブタイムスタンプが示す時刻において、検証対象となるアーカイブタイムスタンプの TSA 証明書の検証（有効性の確認等）を行う。<br>2-2）アーカイブタイムスタンプを発行した TSA の署名の検証<br>2-3）アーカイブタイムスタンプとタイムスタンプ対象との整合性検証<br>2-4）アーカイブタイムスタンプの信頼点の正当性の検証<br>信頼点が適切なものであるか確認する（※1）。 |
| 3）アーカイブされている証明書や失効情報に対する有効性の確認<br>適切な検証情報がアーカイブされている事を確認する。最も古いアーカイブタイムスタンプが示す時刻と比較して失効情報やその失効情報を検証するための証明書が適切なものであるかを確認する。失効情報の署名に用いられた証明書の有効性を検証する時、その信頼点となる証明書が適切なものである事を確認する。 |
| 4）署名タイムスタンプの検証<br>4-1）アーカイブ時刻における署名タイムスタンプの検証<br>最も古いアーカイブタイムスタンプが示す時刻を想定して「1.2.3.ES-T の検証」の「1）署名タイムスタンプの検証」を実施する。最も古いアーカイブタイムスタンプが示す時刻における TSA 証明書の有効性を確認する。<br>4-2）署名タイムスタンプの信頼点の正当性の確認<br>信頼点が適切なものであるか確認する（※1）。 |
| 5）署名タイムスタンプが示す時刻における ES の検証<br>5-1）署名タイムスタンプが示す時刻を想定し、4）で有効性が確認された検証情報により「1.2.2.ES（電子署名）の検証」を実施する。<br>5-2）ES の信頼点の正当性の確認<br>信頼点が適切なものであるか確認する（※1）。 |
| 6）時間的整合性の確認<br>上記のうち時間的整合性確認で抜けている部分の整合性の確認<br>署名タイムスタンプの時刻、アーカイブタイムスタンプの時刻に対して、時刻の整合性を確認する。 |

署名者の証明書、署名タイムスタンプやアーカイブタイムスタンプの TSA 証明書の検証については 3 節で考察しているので参照のこと。

（※1）信頼点の正当性の確認について

証明書のパス検証では信頼点となる証明書が重要な起点となる。この信頼点となる証明書が意図したものであるかどうかを確認するためには、例えば、認証局自体が提供する情報や公的な文書など信頼できる第三者機関によって提供される情報との照合を行うことが考えられる。しかし、長期署名のように署名作成から長い時間が経過するものを想定したとき、検証時点においてこれらの情報を取得することが困難で、信頼点として適切なものかどうか判断できなくなる可能性もありえる。このようなリスクに備えるためには、例えば、あらかじめ署名ポリシーとして信頼点に関する情報を記載しておき適切な管理下に置いておくことや、信頼できる第三者機関で過去の証明書に対して識別可能な情報を管理しておきそれらの情報と照合する等といった方法が考えられる。その場合にも、将来の暗号やハッシュ関数の危殆化に対して適切な対策を行うことが求められる。信頼点の管理に関する手法や運用方法の指針等は別途検討する必要がある。第2章の考察を参照のこと。

## 1.3 長期署名におけるパス検証の考察

### 1.3.1 概要

電子署名を検証するには、署名に使われた秘密鍵に対応した公開鍵を持つ証明書により、署名値が正しい事を確認した後で、その証明書に関して認証パスを構築して、更に認証パスを検証する必要がある。

① 認証パスの構築：署名者の証明書（EE証明書）と信頼点となる自己署名証明書の間を、証明書の発行者名（Issuer Name）・署名（Signature）・認証局鍵識別子（Authority Key Identifier）を利用して確認しつつ辿る事で認証パスを構築する。

② 認証パスの検証：①で構築した認証パス中の各証明書に対して有効期間の確認、失効有無の確認、認証局証明書か否かの確認、証明書ポリシーの確認等を行う。失効確認においては、失効情報自体の署名に用いられた証明書の有効性の検証をして、その信頼点となる証明書が適切である事を確認する。

認証パスの単純な例として階層型モデルを紹介する。

図 3.1.1のように署名者と検証者が信頼点を共有する単独PKIドメインにおける単純な階層型のモデルである。Microsoft社のIE等において使われているWebモデルでは図 3.1.2のように信頼点をリストにして保持しており、これらの複数の信頼点を署名者と検証者が共有する事になるので認証パスに関しては、単独の信頼点モデルの場合と同様の考え方になる。

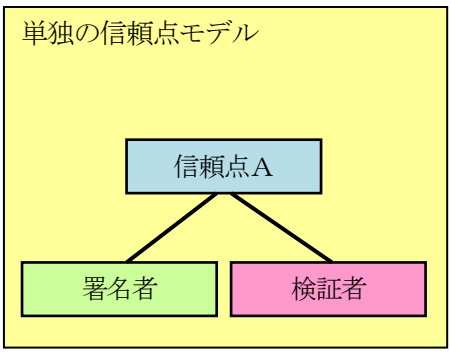



図 3.1.1 単独の信頼点のモデル

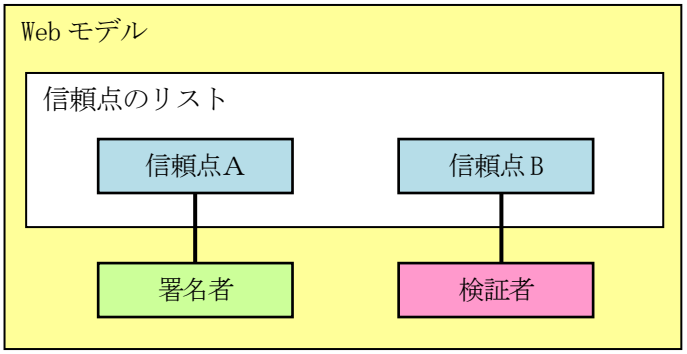



図 3.1.2 Web モデル

図 3.1.3 は 2 階層と 3 階層の階層型モデルの認証パスを例示したものである。信頼点となる認証局から中間認証局を経て多段の構成になることがある。検証者は検証者が信頼点とする証明書から署名者の証明書までの認証パスを構築しその有効性を確認するための検証を行う。認証パスの構築では署名者証明書から信頼点に向かって構築しても、信頼点から署名者証明書に向かって構築しても同じパスになる。

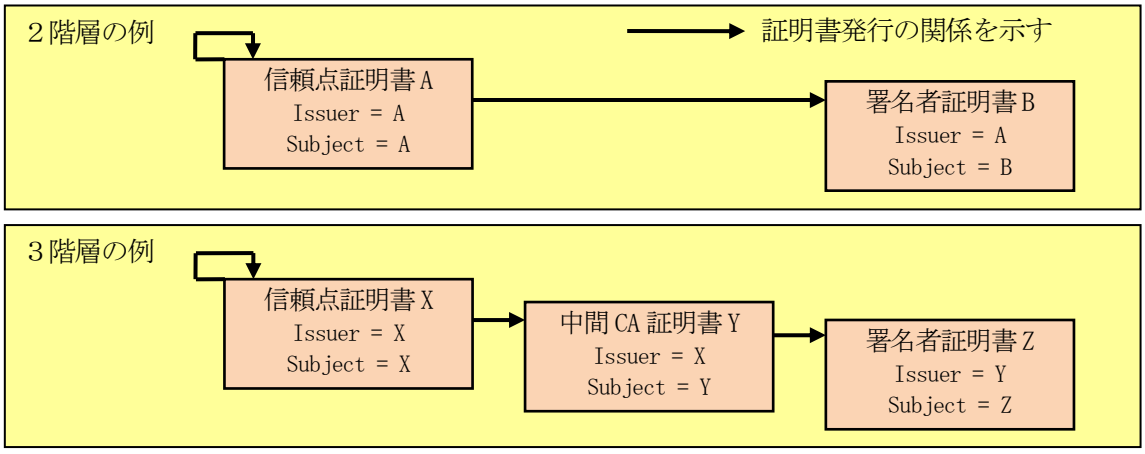



図 3.1.3 階層構造による認証パスの例

電子認証（Authentication）用途での証明書検証では認証用の署名データ生成から検証までの時間的な差異は少なく、検証時刻（現在時刻）での証明書の有効性を確認できればよい。しかし、署名データを保存し時間が経過した後にも真正性を示すことを目的とした電子署名では、署名データを生成した時点において証明書が有効であったことを示す必要がある。長期署名フォーマットでは署名タイムスタンプやアーカイブタイムスタンプによって、署名の生成日時や検証情報（証明書や失効情報）の収集日時が証明可能であり、これらの時刻を基準にして適切な証明書検証を行う必要がある。

### 1.3.2　パス検証における時刻の扱い（ES-T のケース）

ES-T の形式では以下の証明書を検証する必要がある。

・署名者の証明書

・署名タイムスタンプの TSA 証明書

検証者は署名者の証明書、署名タイムスタンプの TSA 証明書について自身の信頼点までの認証パス検証を行うことになる。

ここでは簡単な例として階層型モデルを取り上げ、証明書パス検証における時刻パラメータの扱いについて基本的な考え方を示す。

署名生成から署名タイムスタンプ付与、署名検証の時間的な関係を図 3.1.4 に示す。

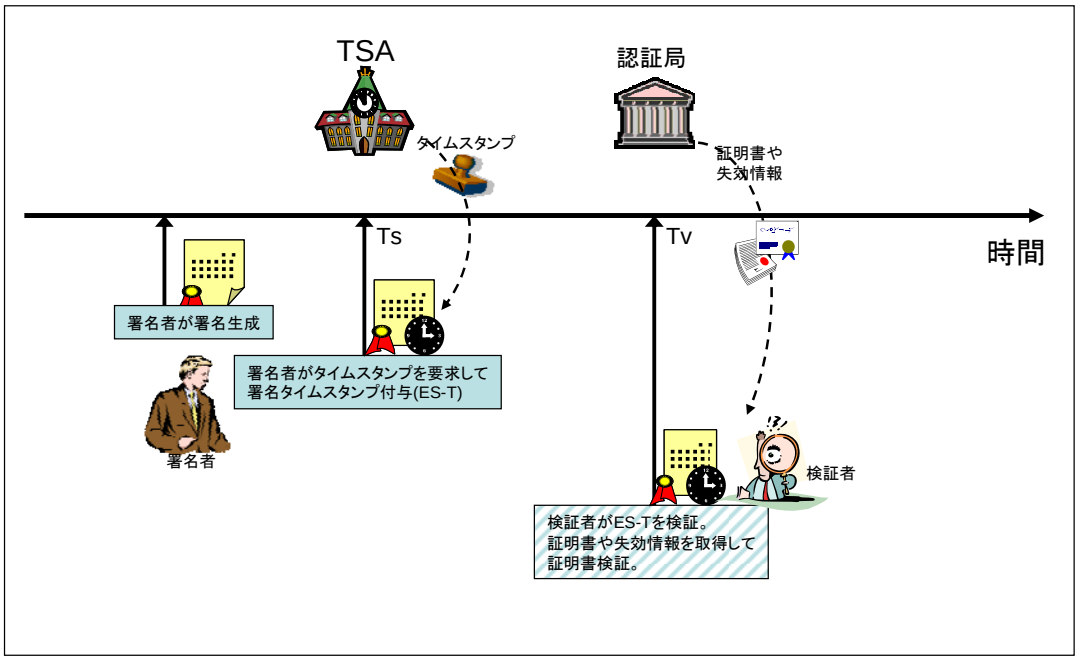



図 3.1.4 ES-T 生成・検証の時間的な関係

署名者の証明書は図 3.1.5 のようにシンプルな階層型モデルとし、失効リストは証明書を発行した認証局から直接発行される例を考える。署名タイムスタンプの TSA 証明書も同様のモデルと

する。

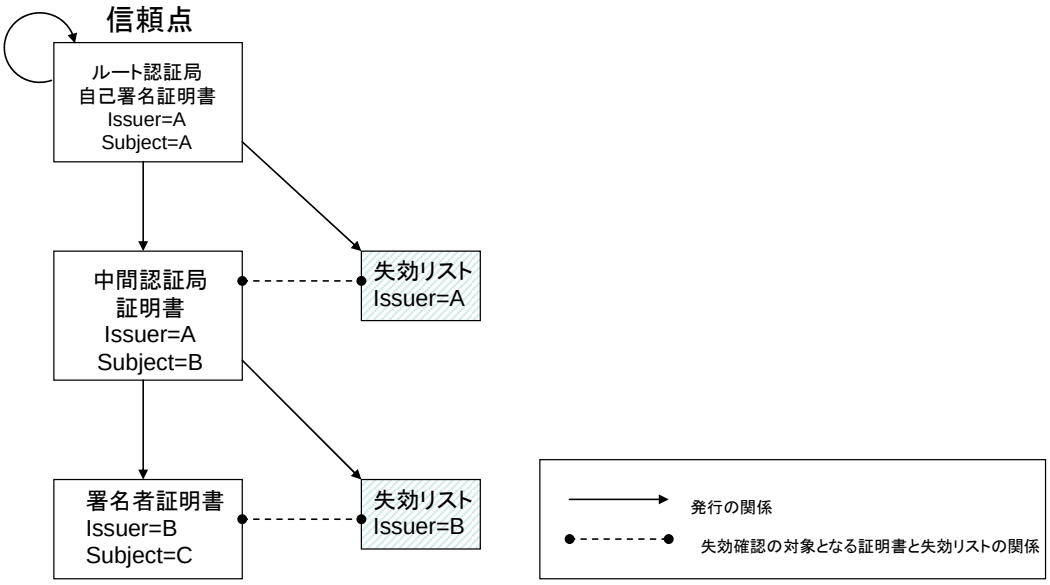



**図 3.1.5 証明書発行モデル**

証明書の検証において時刻のパラメータに関係あるものは以下のものが考えられる。

a) 認証パス上の証明書の有効期限の確認

b) 認証パス上の証明書の失効確認（失効時刻の確認）

c) 失効リストに付与された署名を検証するための証明書の有効期限・失効確認

d) 失効リストの発行時刻の適切さの確認

失効リストの発行時刻の適切さの確認では次のようなケースが考えられる。

- 有効期限切れ証明書に対する失効リストの扱い
  失効されている証明書であっても有効期限が切れた証明書については、以降に発行される失効リストからその失効状態を削除する運用を行う認証局もある。そのような場合、失効確認の対象となる証明書の有効期限を考慮して、取得した失効リストが受け入れられるものかどうかを判断する必要がある。
- 失効リストへ反映される猶予期間の考慮
  認証局への失効申請から失効リストへ失効状態が反映されるまでの時間的な猶予を考慮したうえで、失効リストの発行時刻と署名時刻を比較して、取得した失効リストが受け入れられるものかどうかを判断する。

失効リストの発行時刻の適切さの判断は認証局の運用ポリシーにも依存するものである。具体的な方法についてはここでは触れないものとする。

署名者証明書の検証において、認証パス上の証明書は署名が生成された時点、すなわち署名タイムスタンプの時刻（Ts）における有効性が確認できればよい。一方、その証明書の失効確認に

用いられる失効リスト自身に対する有効性は失効リストを取得した時点、すなわち検証時刻（現在時刻 Tv）が基準となる（図 3.1.6）。

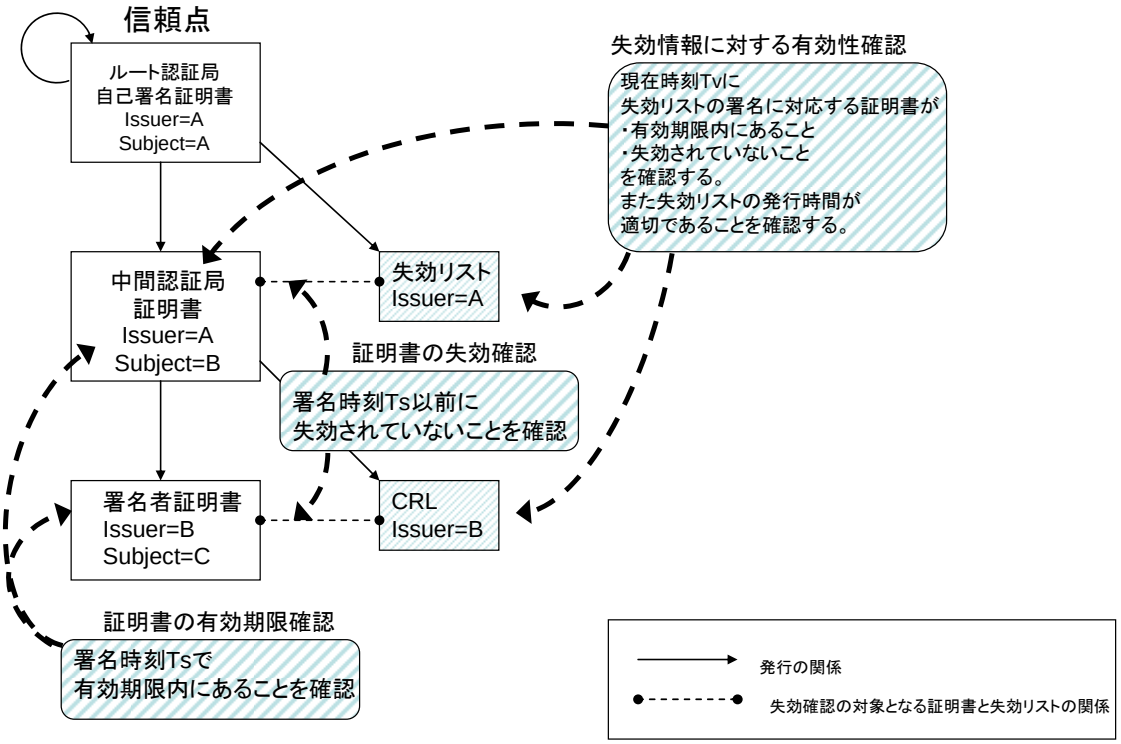



図 3.1.6 ES-T における署名者証明書検証の基準となる時刻

署名タイムスタンプの TSA 証明書については全て現在時刻（Tv）での有効性を確認すればよい（図 3.1.7）。

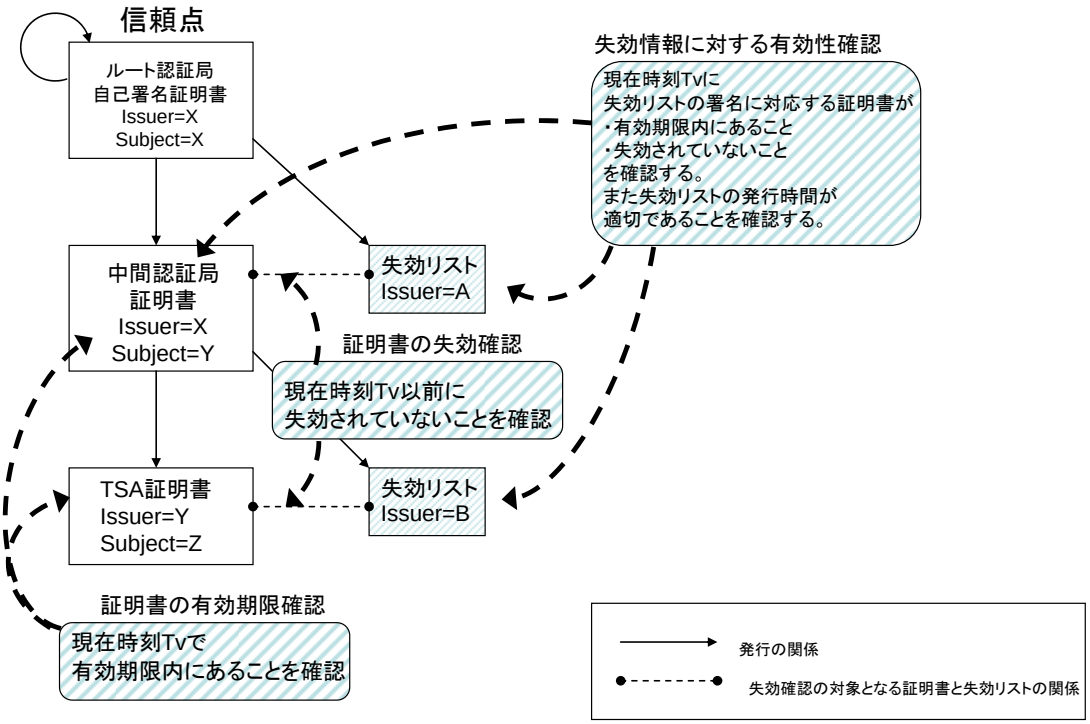



図 3.1.7 ES-T における署名タイムスタンプ TSA 証明書検証の基準となる時刻

図 3.1.8 は ES-T 生成の過程と ES-T 検証で用いる時刻パラメータの関係を示したものである。

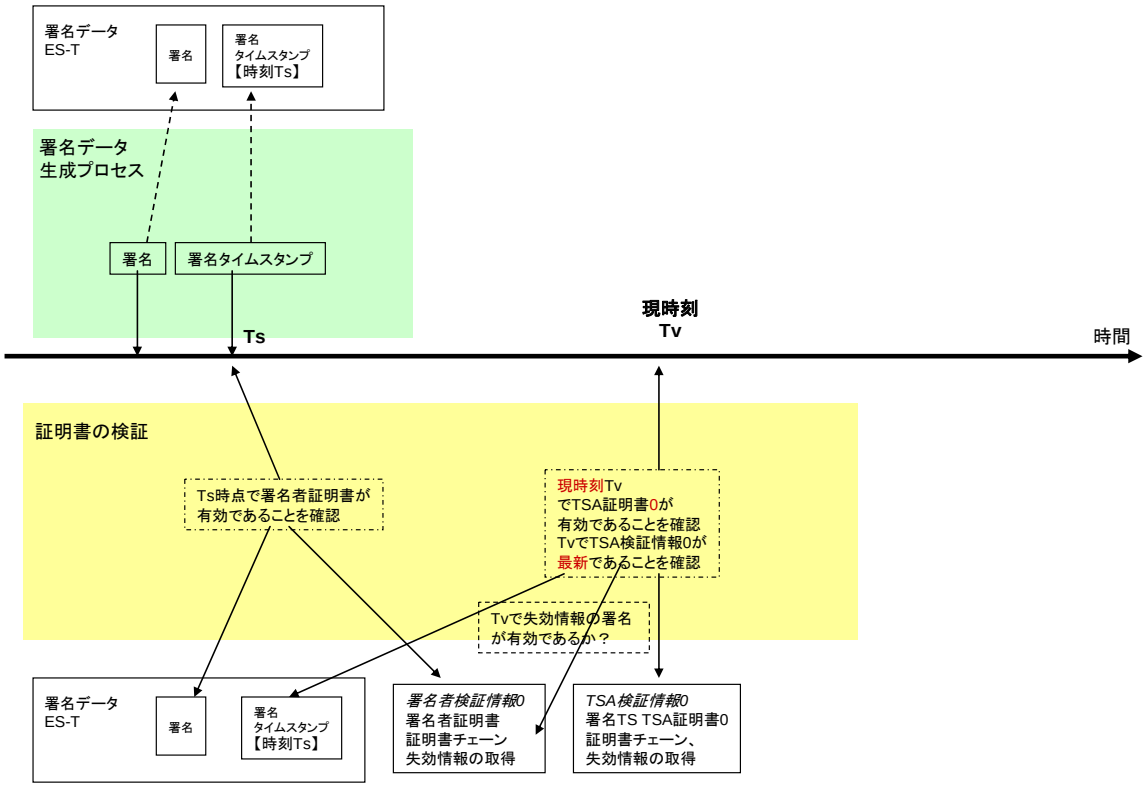



図 3.1.8 ES-T 生成と検証の関係

ES-T 検証における証明書検証での基準となる時刻の考え方を表 3.1.1 にまとめる。

表 3.1.1 ES-T における証明書検証の基準となる時刻

| | 信頼点までの認証パス上の証明書の有効期間、失効時刻 | 失効リストに付与された署名に対する証明書の有効性 |
|---|---|---|
| 署名者の証明書 | 署名タイムスタンプ時刻 Ts で有効であることを確認する。 | 失効リストを取得した検証時刻（現在時刻 Tv）で有効であることを確認する。 |
| 署名タイムスタンプの TSA 証明書 | 検証時刻（現在時刻 Tv）で有効であることを確認する。 | 検証時刻（現在時刻 Tv）で有効であることを確認する。 |

図 3.1.5 のシンプルな発行モデルでは失効リストの署名を検証する証明書は署名者証明書の認証パス上の証明書と一致している。証明書発行時に付与される署名と失効リストの発行時に付与される署名では、用いられる秘密鍵が異なるケースもある。例えば、認証局が鍵更新を行うケースがあり、これについては 1.3.4 節で紹介する。また、失効情報が証明書を発行した認証局とは別の主体から発行されるケースもある（1.3.5 節で紹介する OCSP がその一例である）。

### 1.3.3 パス検証における時刻の扱い（ES-A のケース）

ES-A の検証において、署名者の証明書、署名タイムスタンプや過去のアーカイブタイムスタンプの TSA 証明書の検証は、過去に収集した証明書や失効情報を用いて検証を行う。

ここでは ES-A のアーカイブタイムスタンプによって保護された証明書や失効情報を検証に用いることを想定する。

ES-A 生成と検証の時間的な関係を図 3.1.9 に示す。

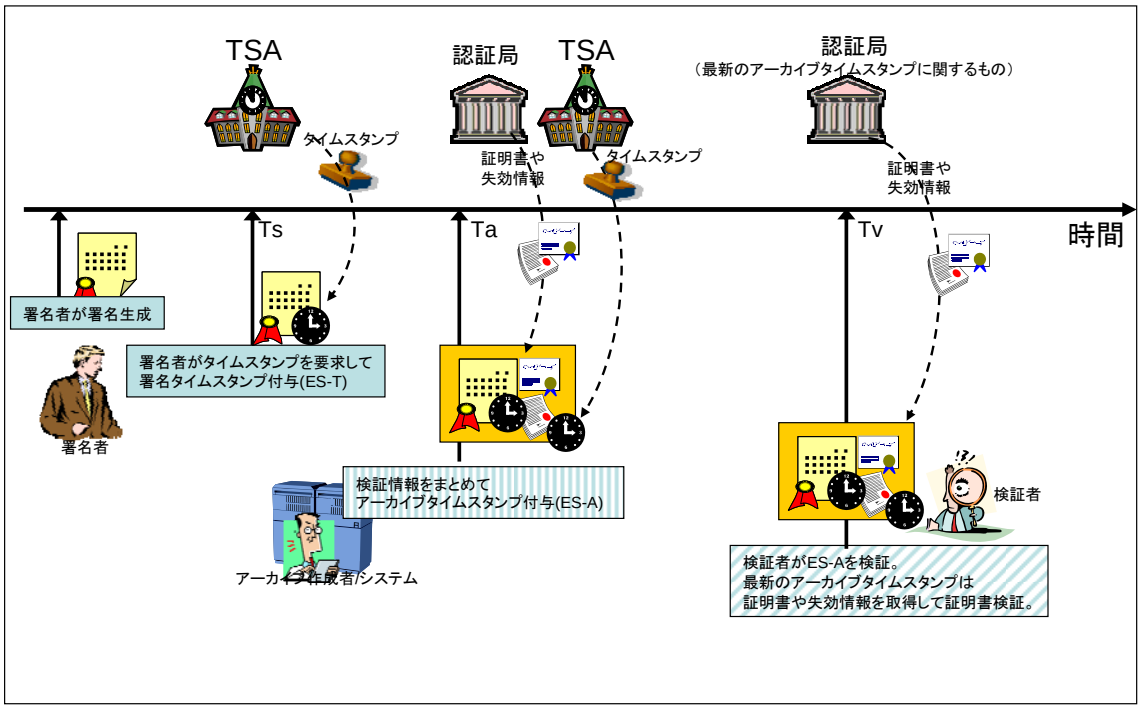



図 3.1.9 ES-A 生成・検証の時間的な関係

ES-A の生成過程の概要は次のようになる（図 3.1.10 の上段を参照のこと）。

1. 署名者が署名を生成し、署名タイムスタンプを付与する（ES-T 生成）。
2. アーカイブを作成する者もしくはシステムが ES-T を検証し、署名者証明書と署名タイムスタンプの TSA 証明書の検証に必要な証明書や失効情報を格納してアーカイブタイムスタンプを付与する（ES-A の生成）。
3. 署名文書の保存期間がアーカイブタイムスタンプの有効な期間を超える場合には、アーカイブ作成者もしくはシステムが ES-A を検証したうえで、最後のアーカイブタイムスタンプの検証に必要な証明書と失効情報を格納して、新たなアーカイブタイムスタンプを追加する（ES-A の更新）。必要に応じてこのアーカイブタイムスタンプの付与を繰り返し、複数世代のアーカイブタイムスタンプが存在する状態になる。

ES-A における証明書の検証では上記の生成過程の時間順序を考慮して検証を行う。

検証が必要な証明書をまとめると以下のようになる。

- 署名者の証明書
  検証に必要な証明書や失効情報が最初のアーカイブタイムスタンプによって保護されている。
- 署名タイムスタンプの TSA 証明書
  検証に必要な証明書や失効情報が最初のアーカイブタイムスタンプによって保護されている。

・ 過去のアーカイブタイムスタンプの TSA 証明書
検証に必要な証明書や失効情報が次の世代のアーカイブタイムスタンプによって保護されている。
・ 最新のアーカイブタイムスタンプの TSA 証明書
検証に必要な証明書や失効情報は検証時点において取得可能なものを使用する。

過去にアーカイブされた証明書や失効情報を使って認証パスを構築し検証する場合には、署名生成やアーカイブ生成当時において合意のあった信頼点を基点とすることになる。アーカイブの作成から検証まで長期間にわたることが考えられ、これらの信頼点が検証する時点において受け入れられる適切なものであるかは別途確認する必要がある。信頼点の管理に関する手法や運用方法の指針等はここでは範囲外とする。

図 3.1.10 は ES-A 生成の過程と ES-A 検証で用いる時刻パラメータの関係を示したものである。

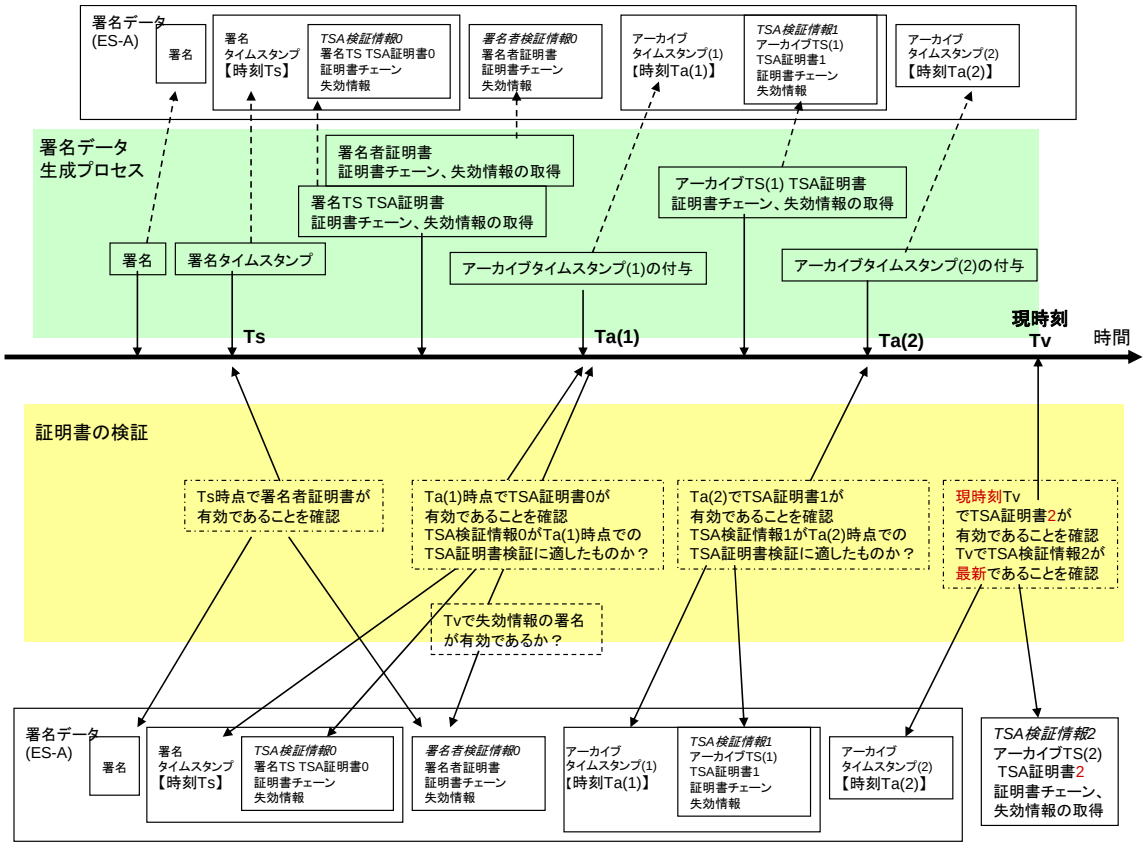



図 3.1.10 ES-A 生成と ES-A 検証の関係

署名者証明書や署名タイムスタンプの TSA 証明書の検証は 1.3.2 節の ES-T 検証のケースの基本的な考え方を踏襲したものである。1.3.2 節における ES-T の検証時刻を最初のアーカイブ時刻 Ta（1）と考えればよい。

過去のアーカイブタイムスタンプの TSA 証明書については、前述の ES-A 生成過程を考慮すれば、次の世代のアーカイブタイムスタンプが付与された時間での有効性を確認することになる。

最新のアーカイブタイムスタンプの TSA 証明書は、検証時刻（現在時刻）での有効性を確認する。

ES-A 検証における証明書検証での基準となる時刻の考え方を表 3.1.2 にまとめる。

**表 3.1.2 ES-A における証明書検証の基準となる時刻**

| | 信頼点までの認証パス上の証明書の有効期間、失効時刻 | 失効リストに付与された署名に対する証明書の有効性 |
|---|---|---|
| 署名者の証明書 | 署名タイムスタンプ時刻 Ts で有効であることを確認する。 | 最初のアーカイブタイムスタンプ時刻 Ta（1）で有効であることを確認する。 |
| 署名タイムスタンプの TSA 証明書 | 最初のアーカイブタイムスタンプ時刻 Ta（1）で有効であることを確認する。 | 最初のアーカイブタイムスタンプ時刻 Ta（1）で有効であることを確認する。 |
| 過去のアーカイブタイムスタンプ（n 世代）の TSA 証明書 | 次の世代のアーカイブタイムスタンプ時刻 Ta（n+1）で有効であることを確認する。 | 次の世代のアーカイブタイムスタンプ時刻 Ta（n+1）で有効であることを確認する。 |
| 最新のアーカイブタイムスタンプの TSA 証明書 | 検証時刻（現在時刻 Tv）で有効であることを確認する。 | 検証時刻（現在時刻 Tv）で有効であることを確認する。 |

### 1.3.4 リンク証明書を用いた検証

#### 1.3.4.1 リンク証明書の概要

信頼点の自己署名証明書は有効期限やその他の理由で、いずれ更新する必要を生じる。この時に信頼点となる自己署名証明書の新旧 2 つを並存させる場合がある。並存している期間は信頼点となる 2 つの自己署名証明書が存在するが、新旧どちらの自己署名証明書を信頼点としている場合にも他方も信頼できる仕組みがリンク証明書により実現される。リンク証明書が発行されるか否かは認証局の運用ポリシーによる。

リンク証明書は旧（Old）自己署名証明書の秘密鍵で新（New）自己署名証明書の公開鍵に署名した NewWithOld リンク証明書と、その逆に新（New）自己署名証明書の秘密鍵で旧（Old）自己署名証明書の公開鍵に署名した OldWithNew リンク証明書の、2 種類がある。同様に旧（Old）自己署名証明書を OldWithOld 証明書、新（New）自己署名証明書を NewWithNew 証明書と呼ぶ。

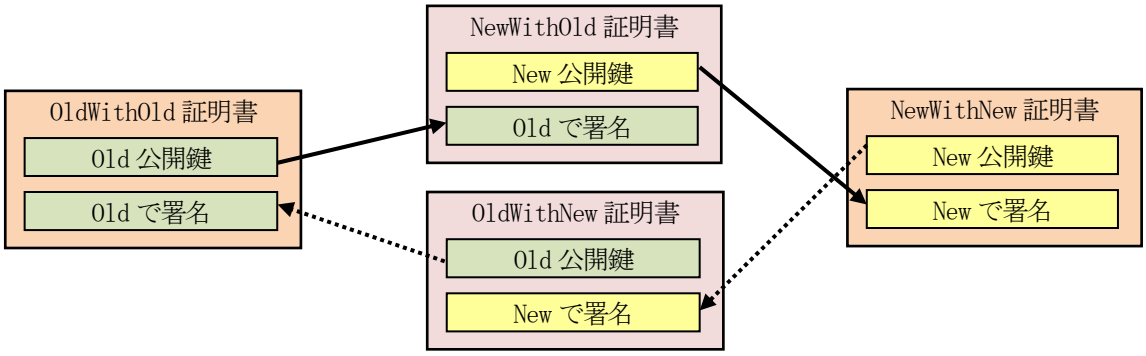



**図 3.1.11 リンク証明書と新旧ルート証明書の関係**

① 旧（Old）自己署名証明書が信頼点の場合に新（New）自己署名証明書の有効性を確認
1-1 OldWithOld 自己署名証明書の公開鍵で、NewWithOld リンク証明書の署名を検証
1-2 NewWithOld リンク証明書の公開鍵で、NewWithNew 自己署名証明書の署名を検証
1-3 NewWithNew 自己署名証明書は信頼できる

② 新（New）自己署名証明書が信頼点の場合に旧（Old）自己署名証明書の有効性を確認
2-1 NewWithNew 自己署名証明書の公開鍵で、OldWithNew リンク証明書の署名を検証
2-2 OldWithNew リンク証明書の公開鍵で、OldWithOld 自己署名証明書を署名を検証
2-2 OldWithOld 自己署名証明書は信頼できる

このようにリンク証明書を用いることができれば新旧いずれかの自己署名証明書を信頼点にすることで認証パスを構築することができる。

リンク証明書は OldWithNew と NewWithOld で有効期間が異なる。RFC4210「Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)」の「4.4. Root CA Key Update」で表 3.1.3 のように定めている。政府認証基盤（GPKI）相互運用性仕様書も同様に定められている。

**表 3.1.3 リンク証明書の有効期間**

| | 有効期間の開始 | 有効期間の終了 |
|---|---|---|
| OldWithNew | 旧鍵ペアが生成された時間 | 旧自己署名証明書が期限切れとなる時間 |
| NewWithOld | 新鍵ペアが生成された時間 | この認証局の全てのエンティティが新自己署名証明書を取得する日時（遅くとも旧自己署名証明書の有効期限まで） |

### 1.3.4.2 リンク証明書と時刻の関係

認証局が鍵更新を行った場合のシナリオとして図 3.1.12 のようなケースが考えられる。

1. 署名者は認証局（Old）より証明書を発行される。
2. 署名者は 1. で与えられた秘密鍵で署名を生成する。
3. 検証者は 2. の署名を検証する。この時点で認証局は鍵更新が行われており、
   1. の証明書に対する失効状態は認証局（New）が発行する失効リストで確認する。

認証局の鍵更新が行われても認証局（Old）から発行された秘密鍵や証明書が利用できなくなるわけではないため、鍵更新が行われるタイミングとしては 2. の前後どちらもありえる。

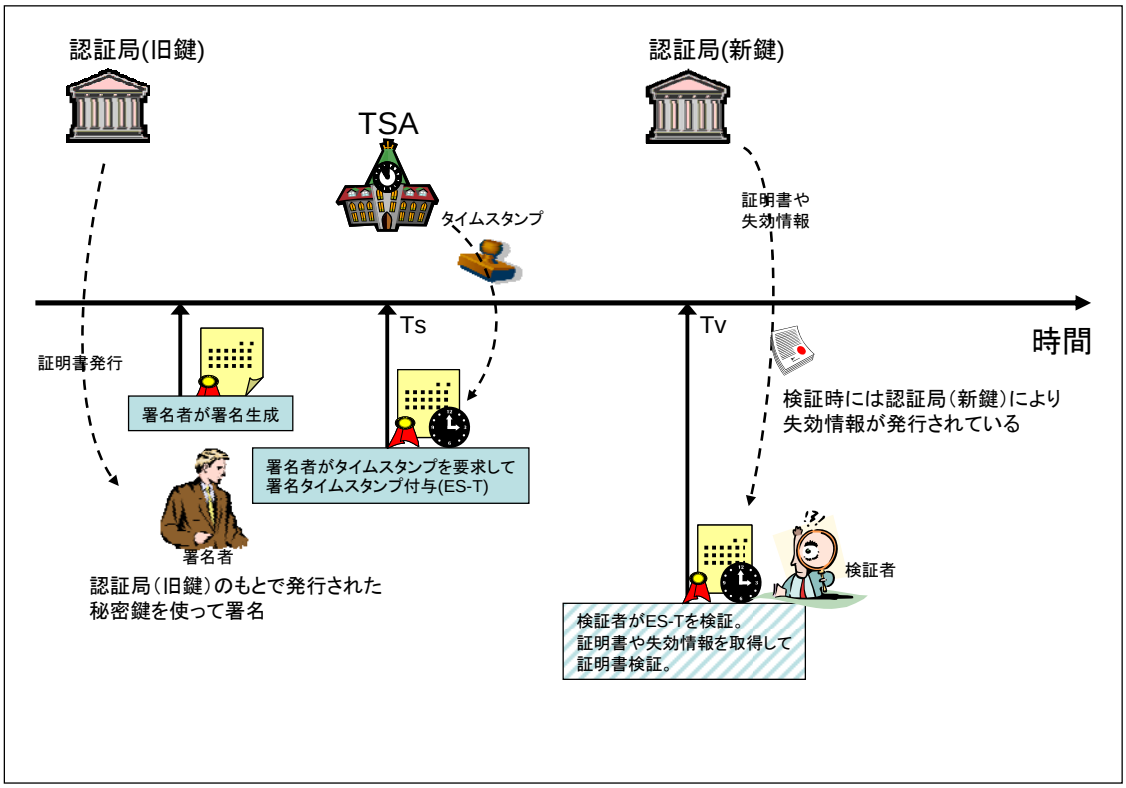



図 3.1.12 認証局の鍵更新と署名検証

1.3.4.1 節で述べたように、認証局によりリンク証明書が発行される場合には、検証者は認証局（Old）か認証局（New）のいずれか一方を信頼点として認証パスを構築することができる。例として図 3.1.13 のような信頼点となるルート認証局が鍵更新を行うモデルを考える。このような状態にある署名データ（ES-T）を検証者が検証するケースを考える。

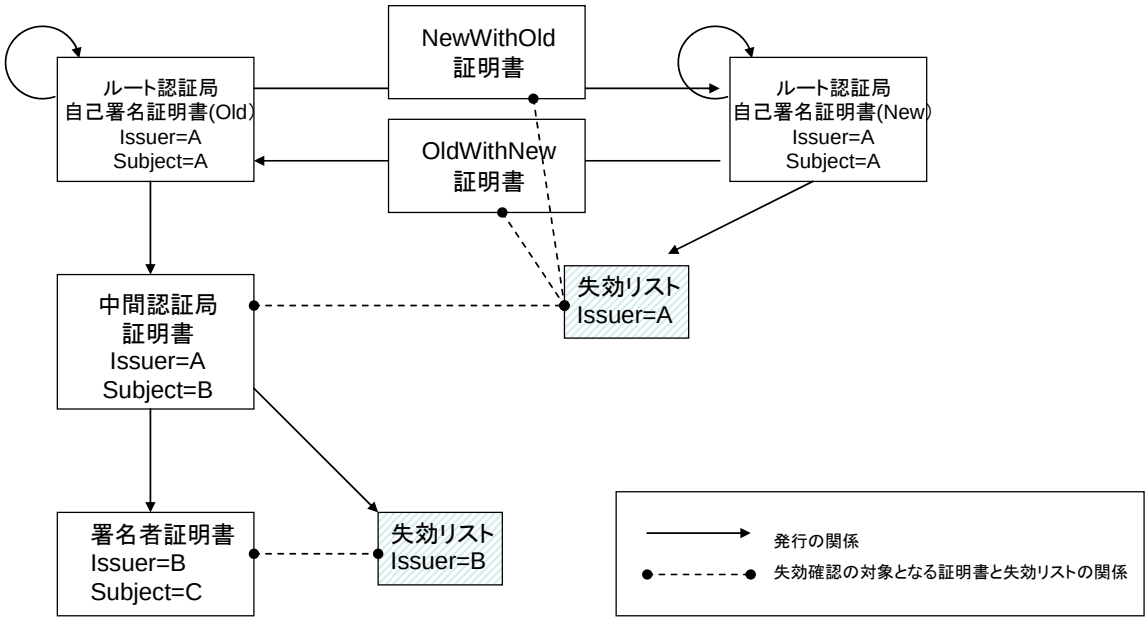



図 3.1.13 リンク証明書を用いたモデルの例

リンク証明書が介在しても基本的な考え方は表 3.1.3 と同様である。図 3.1.14 は認証局(Old)を信頼点に入れた場合である。この場合は信頼点となる認証局（Old）から署名者証明書までの認証パスは図 3.1.13 のモデルと同様である。この認証パス上の証明書の有効性は署名タイムスタンプの時刻（Ts）を基準に考えればよい。失効リストに付与された署名を検証するときには、NewWithOld 証明書によって認証局（Old）との繋がりを確認することができる。失効リストに付与された署名の有効性は、失効リストを取得して検証を行う時刻（現在時刻 Tv）を基準に考えればよい。

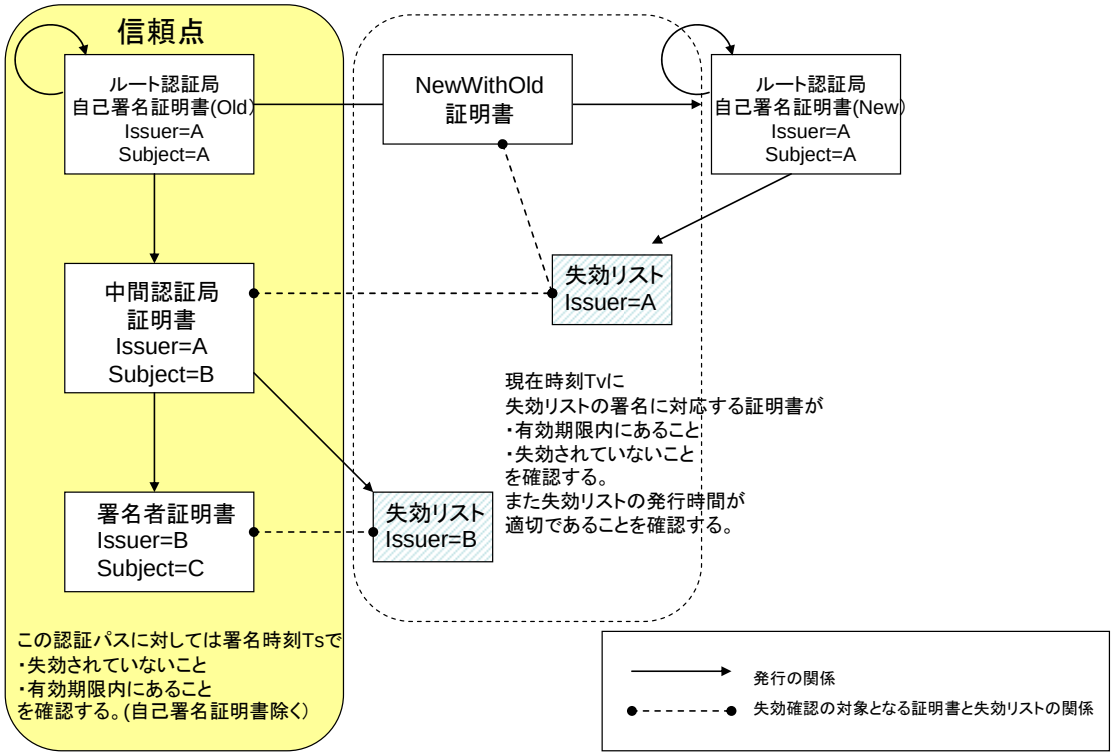



図 3.1.14 認証局（Old）を信頼点とした場合（ES-T の検証）

図 3.1.15 は認証局（New）を信頼点においた場合である。この場合は信頼点から署名者証明書までのパスは OldWithNew 証明書を含んだ形となる。認証パス上の証明書も同様に署名時刻（Ts）での有効性を確認する。表 3.1.3 に示すように OldWithNew 証明書の有効期間は旧鍵ペアが存在した時点から開始するため、署名時刻の時点で有効期間内（開始時刻以降）にある。このケースでも失効リストに付与された署名の有効性は、失効リストを取得して検証を行う時刻（現在時刻 Tv）を基準に考えればよい。

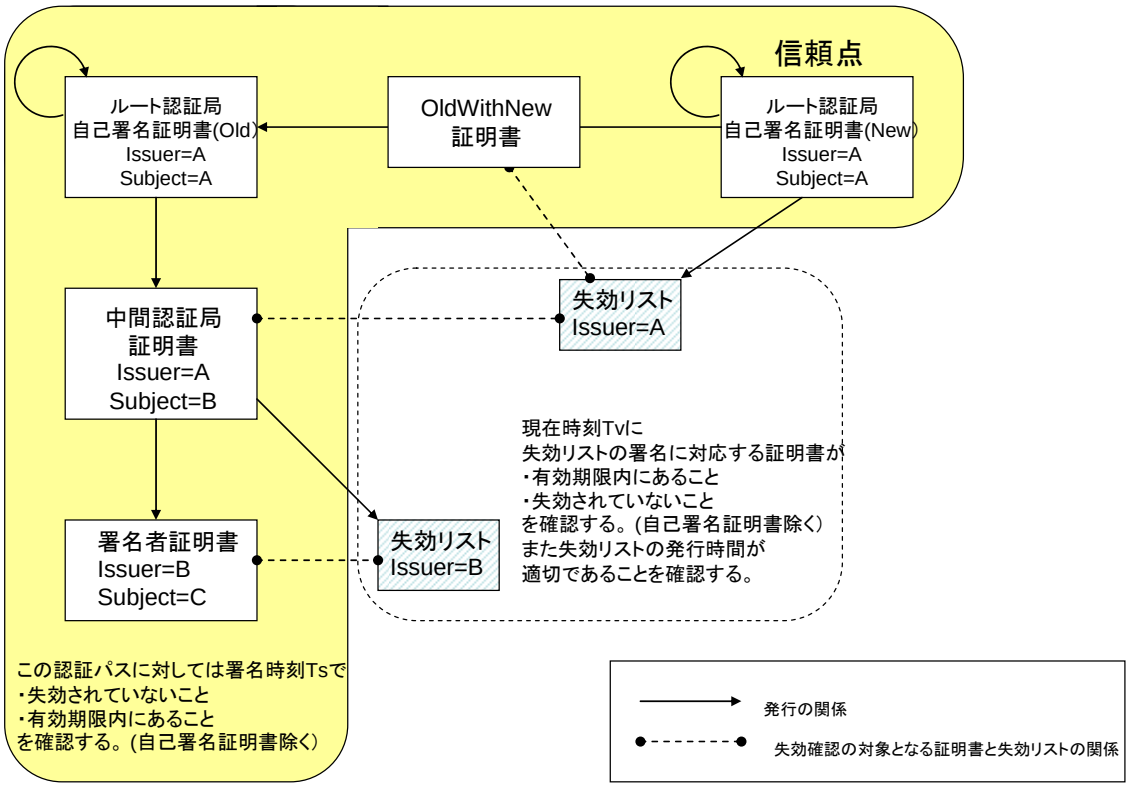



図 3.1.15 認証局（New）を信頼点とした場合（ES-T の検証）

署名タイムスタンプの TSA 証明書に関して認証局の鍵更新が行われた場合でも考え方は同様である。表 3.1.1 のように現在時刻 Tv における有効性を確認する。

ES-A の検証において、アーカイブされているリンク証明書を用いて検証する場合にも、これまでの考察と同様に扱うことができる（表 3.1.2 参照）。

### 1.3.5 より複雑なモデルの例

これまでの考察は階層型モデルのシンプルなモデルを例示した。ここではより複雑なモデルの例としてブリッジ認証局を使った相互認証モデルと OCSP を使ったモデルを紹介する。

これらのモデルでのパス構築は複雑になるが、検証において基準となる時刻の考え方はこれまで述べた基本的な考え方と同様である。

#### 1.3.5.1 ブリッジ認証局を使った相互認証モデル

署名者と検証者が異なる PKI ドメインに属して信頼点も異なっている場合に、ブリッジ認証局（BCA）を使って信頼点同士が相互認証する場合の認証パスの構築について考える。信頼点同士が直接相互認証するモデルもあるがここでは説明を省く。各信頼点とブリッジ認証間はお互いに相互認証証明書を発行する。図 3.1.16 の例ならば、信頼点 A を持つ検証者が、信頼点 C を持つ署名者の証明書 C-1 から信頼点 A までの認証パスを構築できる。

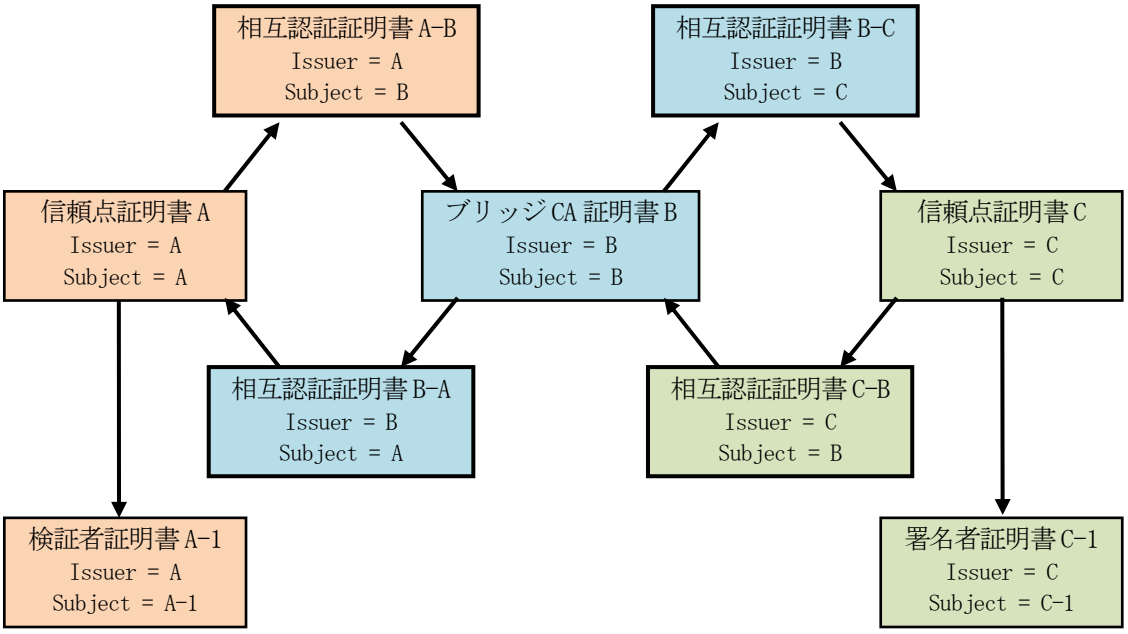



**図 3.1.16 ブリッジ認証局を使った相互認証の例**

図 3.1.16 の例において署名者の EE 証明書 C-1 から、検証者の信頼点である自己署名証明書 A までの認証パスは図 3.1.17 のようになる。

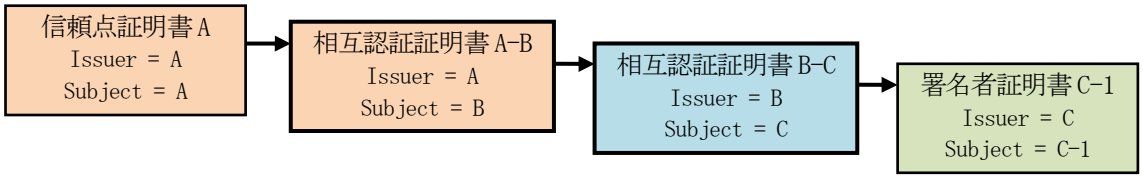



**図 3.1.17 認証パスの例**

なお、信頼点証明書 C やブリッジ認証局の証明書 B の自己署名証明書を含む場合もある。

### 1.3.5.2 相互認証モデルとリンク証明書

図 3.1.16 の例においてブリッジ認証局が二世代の自己署名証明書を持つ場合に、署名者の信頼点 C がブリッジ認証局の新（New）自己署名証明書と相互認証を、検証者の信頼点 A がブリッジ認証局の旧（Old）自己署名証明書と相互認証をしているケースを考える。同じ世代のブリッジ認証局の自己署名証明書を使った場合の、図 3.1.17 の例と比較すると、リンク証明書（NewWithOld）が認証パスに増える事になる。

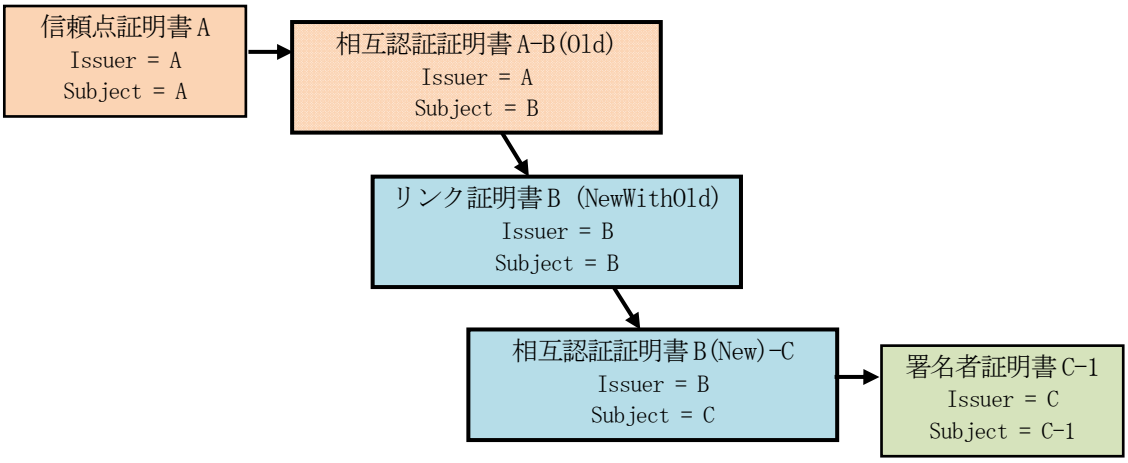



図 3.1.18 リンク証明書を含んだ認証パスの例

このようにブリッジ認証局と相互認証証明書を使った異なる PKI ドメイン間での認証パス構築に、複数世代の証明書が加わるとかなり複雑な認証パス構築が必要である。

### 1.3.5.3 OCSP を用いた検証

OCSP（オンライン失効情報問合せプロトコル）を用いた失効確認を行う場合には、OCSP レスポンスの署名に利用される秘密鍵と対応する証明書の種類によって大きく 3 つのモデルがある。

1）CA 直接信頼：検証対象の証明書と同じ認証局の秘密鍵で署名。
2）CA 間接信頼：検証対象の証明書と同じ認証局が発行した OCSP レスポンダ用の秘密鍵で署名。
3）VA 直接信頼：検証局（VA）が別途発行した秘密鍵で署名。

CA（認証局）直接信頼モデルの例を図 3.1.19 に示す。

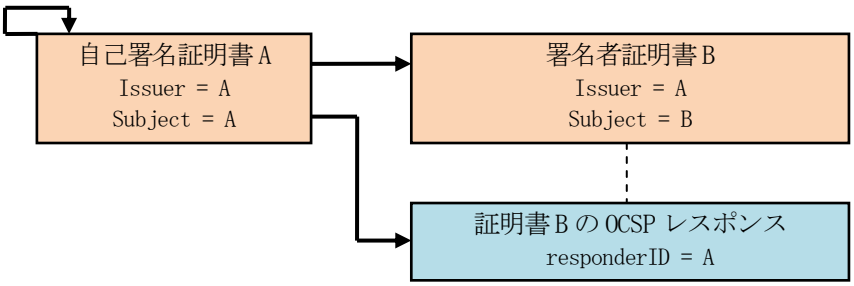



図 3.1.19 CA 直接信頼モデル

次に信頼点となる自己署名証明書に対応する秘密鍵を使って署名された、OCSP レスポンダ専用の秘密鍵を使う CA 間接信頼モデルの例を図 3.1.20 に示す。

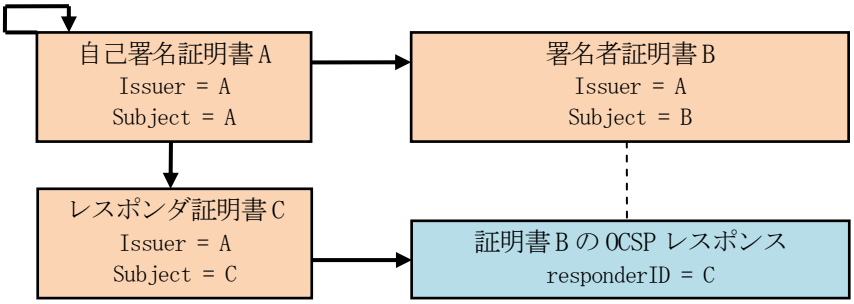



図 3.1.20 CA 間接信頼モデル

OCSP レスポンダが全く別の自己署名証明書に対応した秘密鍵により署名する VA（検証局）直接信頼モデルの例を図 3.1.21 に示す。この例ではレスポンダ証明書 D は自己署名証明書としている。

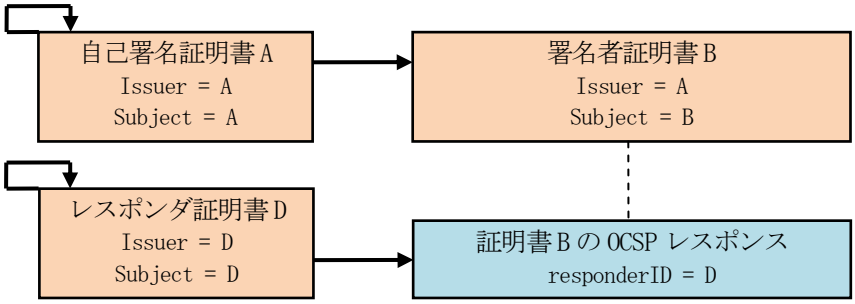



図 3.1.21 VA 直接信頼モデル

OCSP の場合は OCSP レスポンスへの署名に使われる秘密鍵に対応した証明書の有効性の確認をどうするかと言う問題がある。その証明書の拡張部に id-pkix-ocsp-nocheck 等を設定する事で確認しない方法や、別途 CRL により確認する方法等が選択できるので、レスポンダ証明書の内容を確認する必要がある。

## 2. 長期署名における検証情報の管理について

長期署名に用いる長期署名フォーマット CAdES/XAdES では、署名者の証明書から信頼点までに至る認証パス上の証明書及び信頼点を除く各証明書に対する失効情報（CRL あるいは OCSP レスポンスなど）を検証情報として格納でき、これらの検証情報を用いて検証を行うことによって長期署名の正当性を主張できる。

このときの運用上の課題として次の 2 点を取り上げる。

(1) 信頼点に関する課題

(2) 検証情報に関する課題

### 2.1 信頼点に関する課題と対策案

長期署名の検証においては、長期署名フォーマット内に格納されている信頼点が正当なものであったことを確認する必要がある。検証時点に有効な信頼点（例えば、最新世代のアーカイブタイムスタンプ署名の信頼点）は、その時点で活性化されている認証局（CA）等 TTP のリポジトリを参照することによって正当性を主張できる。ところが検証時点に活性化していない過去の信頼点の正当性を主張するためには、次に述べる信頼点偽装の脅威を回避するために、TTP が過去の信頼点を保存し、参照可能としておく等の対策が必要となる。

#### 2.1.1 信頼点偽装の脅威

長期署名フォーマットには、過去の署名やタイムスタンプを検証するための証明書や失効情報を、ルートの証明書を含めて全て格納することができる。従って、長期署名に含まれるルート証明書を信頼点とみなし、各種タイムスタンプが示す時刻を検証時刻と見立てることにより、長期署名に含まれる情報だけを利用して、過去の署名やタイムスタンプの有効性を検証できる。

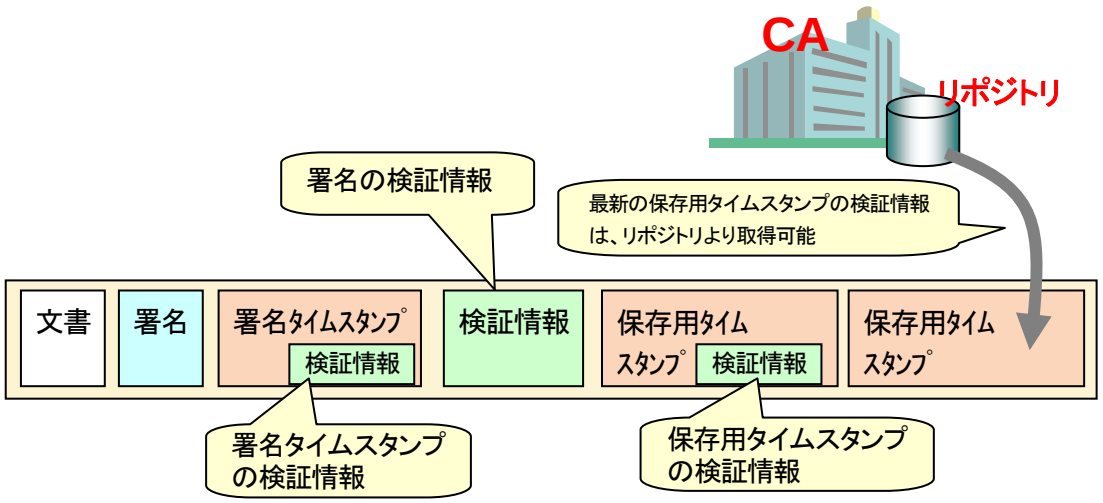



図 3.2.1 長期署名と検証情報

しかしここで、長期署名に格納されたルート証明書を信頼点とみなして信用しても良いもので

あろうか？　実はここには致命的な脅威が潜んでいる。

証明書には、公開鍵に加え、証明書の発行者（CA）や保持者の情報や有効期間をはじめ、各種属性情報を含まれており、それらの全体に対して発行者である CA が署名を施すことにより、公開鍵と属性との関係を保護している。ルート証明書は、自己の公開鍵を含む各種属性情報に対し、その公開鍵に対応する自己の秘密鍵で署名を施す自己署名証明書となっており、それを信頼の起点である信頼点とみなすことが多い。

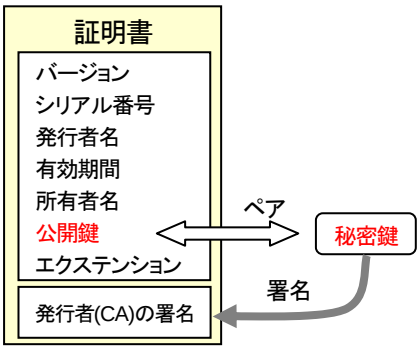



図 3.2.2 自己署名証明書

このとき、現時点で有効である自己署名証明書を偽造することはおよそ不可能である。それは、CA が所有する秘密鍵を他者が得ることができない（厳密な運用管理、耐タンパ H/W による鍵管理、公開鍵アルゴリズムの安全性などによる）ため、証明書への正当な署名が施せないからである。ところが、正当な認証局以外のものが新たに鍵ペアを生成し、公開鍵のみが異なり、他の属性情報が全て正当な証明書と同一であるような証明書を作成することは可能である。このような行為を証明書の偽装と呼ぶこととする。こうしてできた 2 つの証明書を比較すると、一見しただけでは真偽の判断は不可能で、偽装を見破るには、内部に含まれる公開鍵のデータを根拠として区別する以外に方法はない。

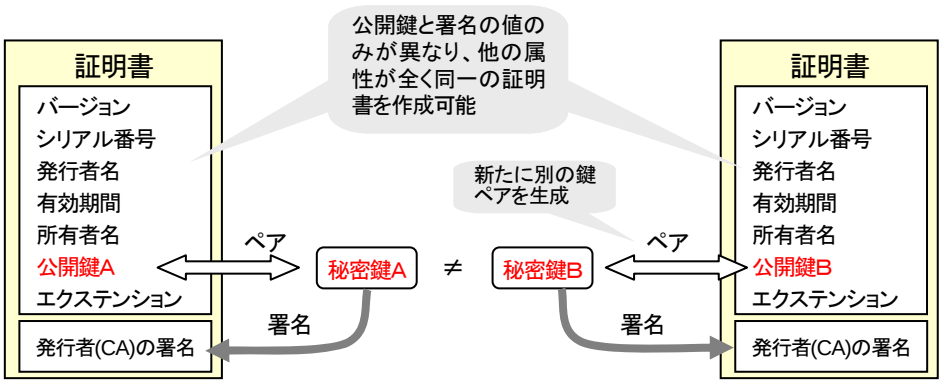



図 3.2.3 証明書の偽装

偽装したルート証明書と対応する秘密鍵を利用し、更に、サブ CA 証明書、タイムスタンプ局（TSA）用証明書、署名者用証明書等を次々と偽装することが可能である。つまりそれぞれの偽装された証明書により、TSA や署名者になりすまして署名を生成することが可能となるのである。

このようなお膳立てのもと、次の手順で長期署名を組み立てることを考える。

(1) 文書をすり替え、署名者になりすまして署名を付与する。

(2) TSA になりすまして偽の署名値に対して T1 の時刻を持つ署名タイムスタンプを生成する。タイムスタンプの場合も証明書同様、署名値や証明書以外の各種属性値は正当なものと全く同一とすることができる。

(3) 署名者の偽装した検証情報、タイムスタンプの偽装した検証情報を生成し、長期署名に格

納する。このとき必要となる失効情報も偽物を容易に生成できる。

(4) TSA になりすまし、(1)～(3)の情報に対して T2 の時刻を持つ保存用タイムスタンプを生成する。

(5) 保存用タイムスタンプの偽装した検証情報を格納し、最新の保存用タイムスタンプを、現存する正当な TSA より取得し、付与する。

上記の手順により生成した偽造長期署名と正当な長期署名との相違は、文書、署名値、タイムスタンプに含まれるハッシュ値、証明書に含まれる公開鍵情報等のみであり、どちらも過去の署名やタイムスタンプの検証を長期署名に含まれる検証情報のみを頼りに検証した場合、有効であると判断されてしまう。つまり、元の文書を都合の良いように偽造できてしまうのである。

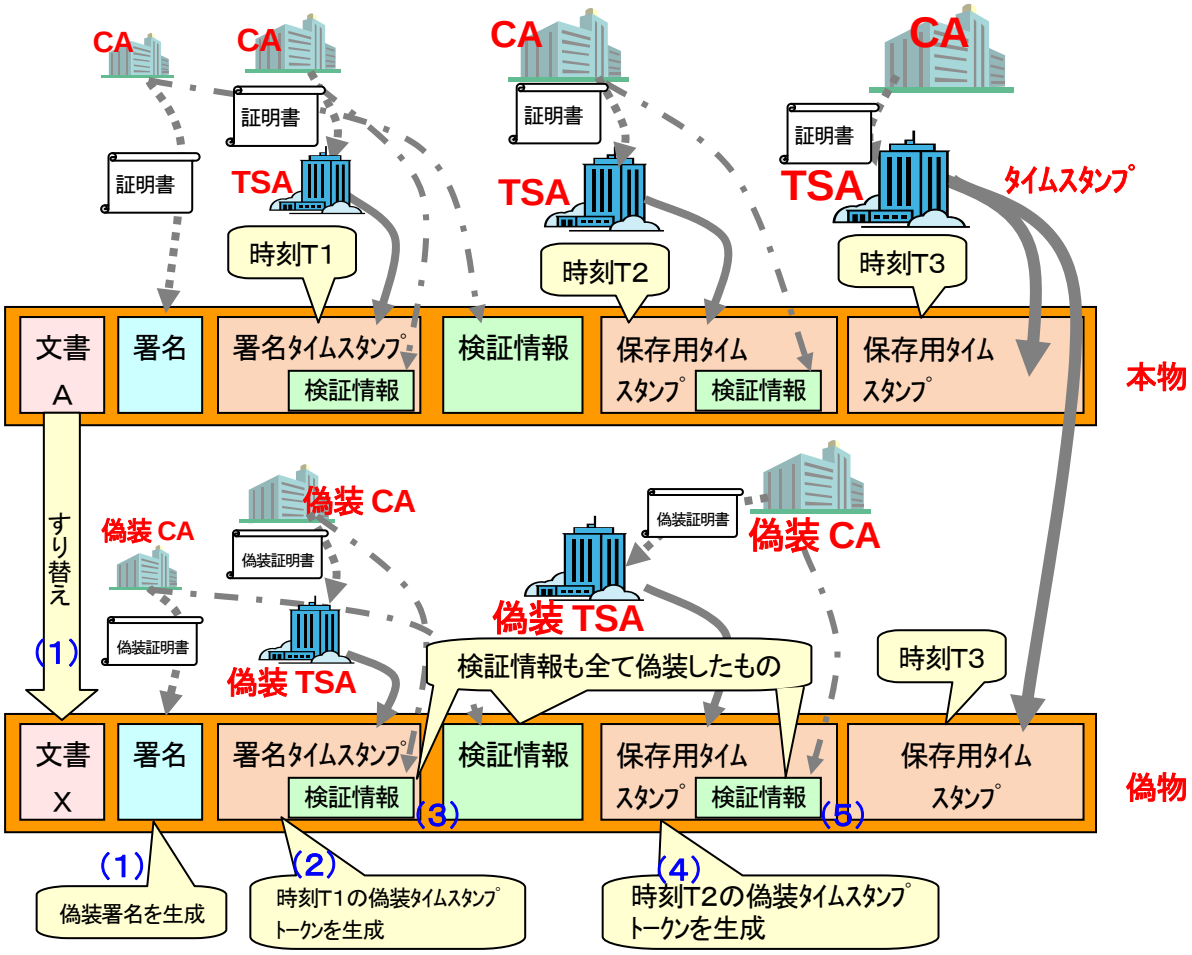



図 3.2.4 長期署名の偽造

### 2.1.1.1 信頼点偽装への対策

このような脅威に対処するためには、当時の正当な信頼点となる CA がどの秘密鍵を利用していたかを確認することである。長期署名に付与された最新の保存用タイムスタンプは、現存する正当な TSA より発行されたものであるため、正当な TSA が公開するリポジトリから獲得した検証情報を基に検証処理を行うことにより、その正当性は保証される。保証されたタイムスタンプに

含まれる時刻（上図の場合、T3 に相当）において、前世代の保存用タイムスタンプを発行した TSA やその TSA に証明書を発行した CA の秘密鍵は厳密に保護されている。従って、前述したような偽装は可能であるが、必ず鍵は異なってしまうはずである。従って、当時の証明書あるいは公開鍵の値を参照し、長期署名に格納されている値と照合すれば良い。

信頼点が偽装されたものでないことを自身で確認するためには、自己責任において正当な証明書や公開鍵を保存しておくことで対処できる。しかし、多くの場合がそうであるように、客観的に信頼点の正当性を説明する必要があるときには、信頼のおける機関が信頼のおける方法によって、それらの情報を保存し、公開する仕組みが必要となる。

この問題への対策の試みとして、電子認証局会議では参加各認証局のフィンガープリント（自己署名証明書のハッシュ値）を書籍（第 8 回電子署名・電子認証シンポジウム検討資料集）にまとめて掲載して出版し、国会図書館に納本した。信頼のおける方法で信頼点を公知化することにより、信頼点の偽装を見分けることが可能となる。ただしこの方法では、数十桁（SHA-1 を利用した場合、40 桁）の 16 進数で表示されたフィンガープリントの値を目視で確認する必要があり、誤認を引き起こす可能性を否定できない。

利便性と確実性を考えると、検証処理を実施する際にオンラインで信頼点を照合できることが望ましい。その場合、信頼のおけるリポジトリで歴代の信頼点を保管・公開し、対象となる信頼点の有効期間を考慮した標準的な手順でアクセスできるような仕組みがあるとよい。また、歴代の信頼点を保管・公開する「信頼のおけるリポジトリ」を提供する機関も予め定義しておくことが望ましい。

そのような機関としては、署名者証明書や TSA の証明書を発行した認証局が第 1 の候補となる。ただし、認証局が業務を廃止することも考えられ、その場合の対処も必要となる。このような場合に備え、信頼点に係る業務を継承するための何らかのルールが必要で、他の認証局への継承、電子認証局会議等の認証局関連の任意団体への継承、公的な機関への継承などをルール化すべきである。また、TSA の信頼点の場合、（財）日本データ通信協会のタイムビジネス認定センターへの継承が適当かもしれない。保管・公開機関の案を次表に示す。

**表 3.2.1 信頼点の保管・公開機関案**

| 署名者証明書 | TSA 証明書 |
|---|---|
| 署名者証明書を発行した認証局 | TSA 証明書を発行した認証局 |
| 廃業された業務を引継いだ認証局 | 廃業された業務を引継いだ認証局 |
| 電子認証局会議等の認証局関連の任意団体 | TSA |
| 信頼点の保管・公開のために新設された公的機関 | タイムビジネス認定センター |
| | 信頼点の保管・公開のために新設された公的機関 |

### 2.1.2　失効情報に関する課題と対策案

長期署名フォーマットの中に格納すべき失効情報の発行時期や取得時期が問題となる場合がある。それは、署名検証において、認証局が失効申請を受けてから実際に失効情報に反映させるための期間：猶予期間（grace period）を考慮する必要があるからである（ECOM「電子文書長期保存ハンドブック」2007年3月，p.162-p.163)。十分な猶予期間が経過した後に取得した失効情報を利用しないと、正しく失効状態が反映されていない可能性がある。

長期署名フォーマットにおいては、署名の生成時刻は署名タイムスタンプの示す時刻を根拠とするが、その時刻を基点に十分な猶予期間を見て取得した失効情報を長期署名フォーマットに格納する必要がある。

このような失効情報に関する問題の一例を次に示す。

A社で部門責任者（署名者）が3月31日で退職。30日に認証局に失効申請したが失効情報への反映まで1週間かかった。一方、A社の長期署名システムにおける猶予期間の設定は3日であった。このため、失効申請後の署名、例えば4月1日に生成された退職した元部門責任者の署名に対して、失効の反映される前の4月4日に発行された失効情報が長期署名フォーマットに格納される。つまり、実際には失効している署名であるにもかかわらず、検証すると有効と判断される長期署名となってしまう。

このとき問題となるのは、猶予期間に明確な定量的な定義がないことである。また定義するとしても、実際の運用においてどのくらいの期間を猶予期間として見ておけばよいのかが不明な場合が多い。

この課題への対策案を次に示す。

(1) 認証局がCP/CPSで最大「猶予期間」を公開し、長期署名システムはその期間後に失効情報を取得して長期署名フォーマットに格納する。利用者は最大「猶予期間」を考慮し、失効申請を行う。上記の例において最大「猶予期間」を1週間とすれば、このような不整合は生じない。しかし、失効情報への実際の反映にかかる時間が最大「猶予期間」を超えるような場合へのリスクは依然として残る。

(2) 利用者が予め希望失効日指定の上、失効申請を行っておく。例えば上記の場合、十分な猶予期間を見込んで4月1日を希望失効日とする失効申請を行っておけば、4月1日には失効が反映された失効情報を発行することができるため、不整合が生じることはない。ただし多くの場合、認証局側の業務の変更が必要となる。また、予期せず失効が発生するようなケースには対応できない。

(3) 失効情報を信頼のおける機関が永年にわたり保管し、公開する。これは、失効点の保管・公開と同様の考え方である。ほとんどの場合において、証明書の有効期間を超えてしまうと失効情報は認証局から発行されなくなり、入手が困難となる。2.1.1.1で示した信頼点の場合と同様に、信頼のおける機関が失効情報を保管・公開することが保証されていると、各自が長期署名フォーマット内に失効情報を格納しておく必要はなく、検証時に必要な失効情報を信頼のおける機関から入手して利用すればよい。この場合、猶予期間の問題が解消されることはもちろん、署名タイムスタンプも不要となる。署名タイムスタンプは長期署名フォーマット内に格納された失効情報の発行時期の正当性を確認するためのもので

あるためで、単に署名の存在時刻を証明するためにはアーカイブタイムスタンプの付与で十分である。保管・公開するのに適当な機関は信頼点の場合と同等と考えてもよいであろう。ただし、失効情報として保管するデータが失効リストという形式が良いのか、また失効を問い合わせるプロトコルが OCSP という形式がよいのかについては検討の余地があるであろう。長期署名検証のための過去の証明書の失効状態について問い合わせる新たな仕組みを検討する必要があるかもしれない。

上記 3 案を示したが、(1)と(2)は決定的な解決策とはならないように思われる。(3)は失効情報に関する本節で示した課題を根本的に解決できる可能性があると思われるが、実運用における各エンティティの負荷や、失効情報の保存形式や問合せプロトコルなど、更に詳細に検討する必要がありそうである。

# 3. ODF と OOXML におけるデジタル署名の XAdES 長期署名化の考察

## 3.1 概要

### 3.1.1 ODF と OOXML

文書ファイルフォーマットも ISO による規格化が進んでいる。オフィス系の文書ファイルフォーマットとしてはマイクロソフト社提案の OOXML（Office Open XML）が今年（2008 年）ISO29500 標準として承認された。一方それよりも早く OpenOffice.org 陣営の ODF（OpenDocument Format）は 2005 年に ISO26300 標準として承認されている。両フォーマットは XML を基本フォーマットとして採用している為に、電子署名の仕様においても XML 署名（W3C 勧告）を採用している。両フォーマット共に含まれる XML や付属ファイルを 1 つのファイルに ZIP 方式によりまとめている点等の多くの共通点も見られる。ここでは、ODF と OOXML の XML 署名を単純に長期署名 XAdES（XML Advanced Electronic Signatures）に置き換えてみてその結果から今後必要と思われる長期署名拡張の可能性を考察する。

OOXML の電子署名に関する仕様に関しては Final Draft 版の仕様書から「Part2：Open Packaging Conventions」の「12. Digital Signature」を参照した。ODF では電子署名の仕様が「OpenDocument 1.2」にて記述される予定だが、実際にテストを行った時点ではまだ仕様として公開されていなかった。しかしながら OpenOffice.org 2.0 以降において既に電子署名が可能であるので、実際に電子署名を行って仕様を確認した。

### 3.1.2 XML 署名と長期署名 XAdES

ODF と OOXML に関して述べる前にまず XML 署名と長期署名の 1 つである XAdES に関する関係をまとめる。XAdES は 2008 年に「JIS X5093 XML 署名利用電子署名（XAdES）の長期署名プロファイル」として承認された。その名前が指すように XAdES はベースとして XML 署名を利用している。従って XAdES ファイルは、長期署名に関係する検証を除けば、XML 署名としても検証が可能となる。今回はまず ODF と OOXML のワード形式文書ファイルの XML 署名部を XAdES に置き換え、ODF は OpenOffice.org で、OOXML は MS-Office2007 の標準機能により XML 署名として検証が可能かどうかを調査した結果をまとめている。

XAdES は XML 署名をベースにしているが、最初の署名時には長期署名用の Object 要素を入れておく必要がある。この為に既に単純に XML 署名されたファイルを後から XAdES 化する事はできない。従って ODF も OOXML も長期署名化する為には、まず XAdES-BES として署名する必要がある。これは OpenOffice.org や MS-Office2007 の機能としては提供されていないので、今回のテスト用に XAdES-BES として署名が可能なツールを開発して利用している。

## 3.2 ODF と OOXML の署名機能比較

### 3.2.1 共通している点

ODF も OOXML も画像等の情報を除き、XML 形式のファイルにより文章や見栄えに関する情報を保持している点は全く同じである。更にそれらのファイルを ZIP 圧縮により 1 つのファイルにまとめている点も同じである。XML 署名として見た場合に 1 文書ファイルに対して、複数の署名を並列に付与できる点も同じである。このように両フォーマットの基本的なコンセプトは非常に似通っている。

### 3.2.2 異なっている点

ODF も OOXML も XML フォーマットは採用しているが、その中の構造（スキーマ）は全く異なっている。ここではオフィス文書としての差異は議論しないで、電子署名部において異なっている点を簡単にまとめる。

OOXML では仕様として、PDF 文書の可視署名と不可視署名のように、外観を備えた目に見える署名欄を持つ電子署名と非表示の電子署名の 2 種類が選択できる。ODF では現在はまだ目に見える可視署名のような電子署名はサポートしていない。本資料中では単純に電子署名の部分のみを比較したいので、OOXML においても非表示の電子署名を対象とする。

#### 3.2.2.1 署名ファイルと複数署名

最初に署名を付与すると、ODF では META-INF フォルダ下に documentsignatures.xml と言うファイルが、OOXML では_xmlsignatures フォルダの下に sig1.xml と言うファイルが作成される。

OOXML では複数署名を付与して行くと、順番に sig2.xml , sig3.xml , …と順番に数字が増えたファイルが追加生成されて行く。sigN.xml のルート要素は XML 署名の Signature 要素となっており、1 ファイル 1 署名になっている。

ODF では複数署名を付与してもファイルは最初の documentsignatures.xml だけで新たにファイルは生成されない。documentsignatures.xml のルート要素は document-signatures 要素となっており、そのルート要素の下に署名が付与される度に XML 署名の Signature 要素が増えて行く。つまり ODF では 1 ファイル複数署名の形式になっている。

#### 3.2.2.2 署名対象ファイルの指定方法

ODF では署名対象ファイルは単純に Signature/SignedInfo パスの下に必要な数だけ Reference 要素を並べて Detached 形式で指定される。これは XML 署名の W3C 規格中に「2.1 Simple Example」として説明がされている形式である。

OOXML では ODF のような単純な形式では無く、Object 要素と Manifest 要素を使った間接的な

署名対象の指定形式を使っている。まずSignature/SignedInfo/Referenceの1つとしてManifest要素を含むObject要素(OOXMLでは特別なId属性“idPackageObject”を付けて「Package-Specific Object」と呼んでいる）が指定される。次にSignature/Object/Manifestの下に、更にReference要素をDetached形式で並べて最終的な署名対象ファイルを指定している。署名対象ファイルは2段階のReferenceにより指定がされる。これはXML署名のW3C規格中に「2.3 Extended Example (Object and Manifest)」として説明がされている形式である。

#### 3.2.2.3 付属情報

ODFでは署名日時をXML署名標準のSignatureProperty要素の下にdate要素として埋め込む事ができる。OpenOffice.org による検証では署名日時は埋め込まなくても検証エラーにはならず、正常と判定されるが、署名日時が「0000/00/00 00:00:00」と表示されてしまう。

OOXMLでは署名日時を「Package-Specific Object」の中にSignatureProperty要素を持ち、その下にOOXML独自定義のSignatureTime要素の下に持つ。MS-Office2007では、OOXMLの仕様により独自定義可能とされている「Application-Specific Object」中に、署名目的のSignatureComments 要素を含んでいる。「Application-Specific Object」の中には他にも署名をした際のMS-Officeのバージョン番号や画面の解像度等の各種付属情報を含める事ができ、実際にMS-Office2007では多数の情報が保存される。

## 3.3 ODFの長期署名化テスト

ODFの電子署名はOpenOffice.orgの2.0以降において、ファイルメニュー下の「デジタル署名」により付与する事ができる。ここではODF標準のXML署名ファイルをXAdES長期署名ファイルに入れ替えて、XML署名として検証がされるかどうかを確認する。

ODFの電子署名の詳細な仕様は入手できなかった。その為にOpenOffice.org 2.0でシンプルなワープロ形式にデジタル署名を付与した場合にどのファイルが署名対象となっているかを調査した。

| ファイル・フォルダ名 | 署名対象 | 概要 |
|---|---|---|
| layout-cache | ○ | バイナリのキャッシュ情報 |
| content.xml | ○ | ドキュメント本体データ |
| meta.xml | ○ | 作成者や時間等のメタデータ |
| settings.xml | ○ | 設定情報データ |
| styles.xml | ○ | スタイル情報データ |
| mimetype | × | ドキュメントのタイプ |
| Pictures¥ | --- | 画像用フォルダ |

| | | |
|---|---|---|
| Pictures¥*.* | ○ | ドキュメント中の各種画像ファイル |
| Configurations2¥ | --- | 不明：情報無し |
| Thumbnails¥ | --- | サムネール用フォルダ |
| Thumbnails¥thumbnail.png | × | サムネール画像 |
| META-INF¥ | --- | メタ情報用フォルダ |
| META-INF¥manifest.xml | × | 目録情報データ |
| META-INF¥documentsignatures.xml | × | デジタル署名データ（標準名） |

署名対象かどうかは生成されたデジタル署名データ“documentsignatures.xml”中の Reference タグで判断している。この結果から今回の長期署名化テストにおいては以下項目を署名対象にしている。

| |
|---|
| 1）ルートフォルダ直下にある“layout-cache”ファイル。 |
| 2）ルートフォルダ直下にある拡張子が“.xml”のファイル全て。 |
| 3）Pictures フォルダ下にある全てのファイル。(Pictures フォルダが無い場合あり) |
| 4)“documentsignatures.xml”中の Object/SignatureProperties/SignatureProperty 要素。(署名日時用) |
| 5)“documentsignatures.xml”中の Object/QualifyingProperties/SignedProperties 要素。(長期署名用) |

テストの為に別途この仕様にて長期署名を付与し、長期署名検証が可能なテストツールを開発して利用した。

### 3.3.1 ODF の長期署名化サンプル

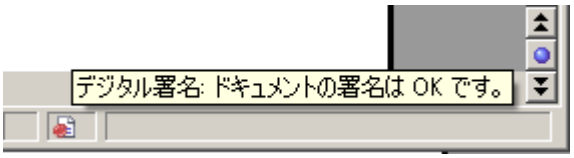
```
<document-signatures>
  <Signature Id="Id">
    <SignedInfo Id="Id-Si-8">
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference Id="Id-Ref-1" URI="content.xml">
        <Transforms><Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/></Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>KJA9nLpoUGXdKHGwEFOhdOGa1gc=</DigestValue>
      </Reference>
      <Reference Id="Id-Ref-2" URI="meta.xml">
        <Transforms><Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/></Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>GdawuL8wlLZ/BCXdl6XBgBnRdpE=</DigestValue>
      </Reference>
      <Reference Id="Id-Ref-3" URI="settings.xml">
        <Transforms><Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/></Transforms>
```

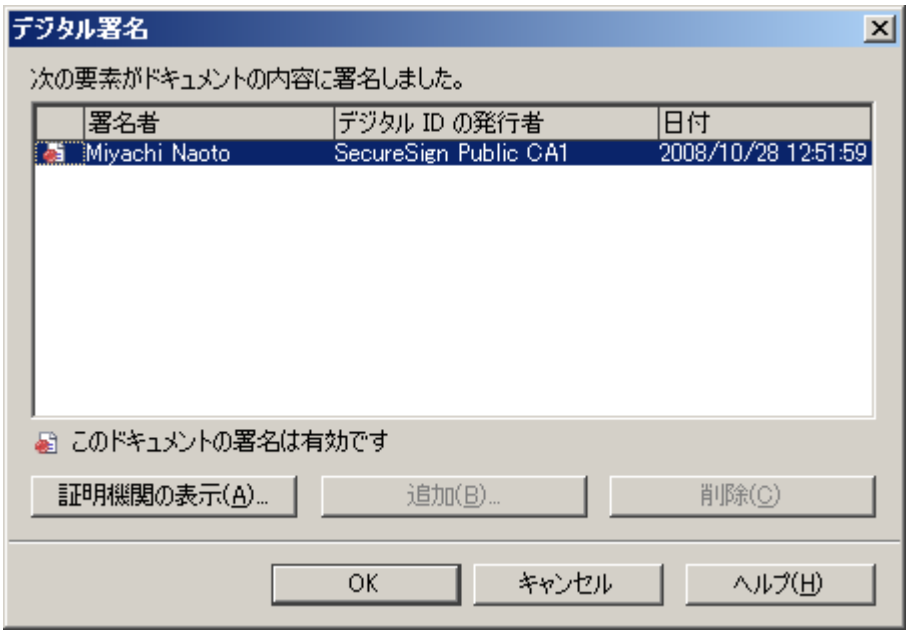
```
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>O6PXfJ9tOPE4znAgOM36K7ojeDA=</DigestValue>
      </Reference>
      <Reference Id="Id-Ref-4" URI="styles.xml">
        <Transforms><Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/></Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>77nAw4qOEqzhefHzKwwdvfYMWCA=</DigestValue>
      </Reference>
      <Reference Id="Id-Ref-7" URI="#Id-Sp-5">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>j9/IHYC7WjcsStlOVI3cqtrQtpg=</DigestValue>
      </Reference>
      <Reference Id="Id-Ref-12" URI="#Id-Sp-11" Type="http://uri.etsi.org/01903#SignedProperties">
        <Transforms><Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/></Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>RFOijWiaA3iZVdoHLIw4AXLKzqg=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue Id="Id-Sv-9">ZA6WsGpuaO7FLmlQ.....CEQAm/95SfIO+6c=</SignatureValue>
    <KeyInfo Id="Id-Key-10">
      <X509Data>
        <X509Certificate>MIIDlDCCAv2gAwIBAgI.....KSFNH6DtkojDRA3G/EBWcE=</X509Certificate>
      </X509Data>
      <KeyValue>
        <RSAKeyValue>
          <Modulus>urHtAraFHxXUB6drWZe/1......MKJ4ybnBzOpUInfsJ7lNSYs=</Modulus>
          <Exponent>AQAB</Exponent>
        </RSAKeyValue>
      </KeyValue>
    </KeyInfo>
    <Object Id="Id-Obj-6">
      <SignatureProperties>
        <SignatureProperty Id="Id-Sp-5" Target="#Id">
          <dc:date>2008-10-28T12:51:59</dc:date>
        </SignatureProperty>
      </SignatureProperties>
    </Object>
    <Object Id="Id-XAdES-Object">
      <QualifyingProperties Target="#Id">
        <SignedProperties Id="Id-Sp-11">
          <SignedSignatureProperties>
            <SigningTime>2008-10-28T03:51:59Z</SigningTime>
            <SigningCertificate>
              <Cert>
                <CertDigest>
                  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <DigestValue>OSKEwLpv9YKcO75wYMyUwzXU1TI=</DigestValue>
                </CertDigest>
                <IssuerSerial>
                  <X509IssuerName>CN=TEST, O=TEST ORG, C=JP</X509IssuerName>
                  <X509SerialNumber>5400365494282747904</X509SerialNumber>
                </IssuerSerial>
              </Cert>
            </SigningCertificate>
```

```
            <SignaturePolicyIdentifier>
              <SignaturePolicyImplied/>
            </SignaturePolicyIdentifier>
          </SignedSignatureProperties>
        </SignedProperties>
        <UnsignedProperties>
          <UnsignedSignatureProperties>
            <SignatureTimeStamp Id="Id-STS-1">
              <EncapsulatedTimeStamp
Id="Id-ESTS-1">MIIMdgYJZI......eRe5REvbmA=</EncapsulatedTimeStamp>
            </SignatureTimeStamp>
          </UnsignedSignatureProperties>
        </UnsignedProperties>
      </QualifyingProperties>
    </Object>
  </Signature>
</document-signatures>
```

### 3.3.2　OpenOffice.org による検証結果

3.3.1 の長期署名サンプルをセットした ODF ファイルを OpenOffice.org 2.0 以降で読み込んでみたところ、正常に XML 署名として署名検証がされドキュメントを開く事ができた。




長期署名用の情報を追加した XML 署名であっても問題なく XML 署名として検証が可能である事が確認できた。

### 3.3.3 ODF の長期署名化に関する考察

ODF の XML 署名の仕様は非常に素直な XML 署名仕様と言える。また本来の署名対象以外に長期署名用の独自の署名対象（Object 要素）を追加しても OpenOffice.org 2.0 ではエラーにならず、正常に検証できた。このことより ODF 仕様（正確には今回は OpenOffice.org 2.0 仕様）でのデジタル署名は XAdES による長期署名に入れ替えても大きな問題は無いと考えられる。

OpenOffice.org に長期署名と検証が可能なモジュールが提供できるならば、今回の長期署名化のテストの仕様により標準で長期署名対応の ODF を実現できる可能性が高い。しかし組み込みモジュールとして実現するにはオープンソースのプロジェクトである OpenOffice.org のライセンスに合致したオープンソースの長期署名ライブラリが必要になる点が問題になりそうである。ODF 長期署名を別モジュールとして提供するのであればライセンスの問題は無くなるが、この場合には OpenOffice.org 本体では XML 署名としての検証のみが可能となる。

#### 3.3.3.1 署名日時に関する考察と要望

OpenOffice.org 2.0 では表示する署名日時を独自の date 要素から取得している。長期署名対応として考えた場合に、もし署名タイムスタンプが付与された XAdES-T 形式であればタイムスタンプ日時を署名日時として表示して欲しいと考える。また署名タイムスタンプが無く date 要素も無い場合には、XAdES の SigningTime 要素の日時を参照して表示して欲しい。

## 3.4 OOXML の長期署名化テスト

OOXML の電子署名は MS-Office 2007 以降において、「配布準備」下の「デジタル署名の追加」により付与する事ができる。ここでは OOXML 標準の XML 署名ファイルを XAdES 長期署名ファイルに入れ替えて、XML 署名として検証がされるかどうかを確認する。

OOXML の Final Draft 版の仕様書から「Part2：Open Packaging Conventions」の「12. Digital Signature」によると XML 署名の署名対象となるのは「Package-Specific Object」と「Application-Specific Object」の 2 種類の Object 要素となる。

| 種類 | Package-Specific Object | Application-Specific Object |
|---|---|---|
| 目的 | パッケージ内の署名対象を指定する。<br>Manifest と SignatureProperties の要素が必要。 | アプリケーション独自の要素を設定する。 |
| 数 | 1 つのみ | 複数指定可能 |
| Id | “idPackageObject”（固定） | 任意指定可能 |

「Package-Specific Object」は XML 署名であっても長期署名であっても共通と考えられる。従って今回のテストでは MS-Office 2007 にて生成された「Package-Specific Object」と同じ内容とした。「Package-Specific Object」から参照されている署名対象は種類が多く、更に独自の

Transform である RelationshipTransform (http://schemas.openxmlformats.org/package/2006/RelationshipTransform) を使った参照もあった。OOXML 独自の RelationshipTransform 変換に関しては別途説明を行う。

「Application-Specific Object」は標準にて MS-Office 用の Object が追加されている。今回のテストでは長期署名用の Object も追加している。長期署名用 Object も「Application-Specific Object」の 1 つとして扱われることを期待した。以上より、XML 署名の基本的な参照先としては 3 つの Object を設定した。

| -- | 種類 | Id | 内容 |
|---|---|---|---|
| 1 | Package-Specific Object | “idPackageObject” | OOXML パッケージ内の署名対象を指定。 |
| 2 | Application-Specific Object | “idOfficeObject” | MS-Office 関連情報と署名日時 |
| 3 | Application-Specific Object | 独自生成 | 長期署名用 |

テストの為に別途この仕様にて長期署名を付与し、長期署名検証が可能なテストツールを開発して利用した。

### 3.4.1 OOXML の長期署名化サンプル

```
<Signature Id="idPackageSignature">
  <SignedInfo Id="idPackageSignature-Si-3">
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference Id="idPackageSignature-Ref-1" URI="#idPackageObject"
        Type="http://www.w3.org/2000/09/xmldsig#Object">
      <Transforms><Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/></Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>dU1oUlEs5n2huPV0oeBxCnPbhFw=</DigestValue>
    </Reference>
    <Reference Id="idPackageSignature-Ref-2" URI="#idOfficeObject"
        Type="http://www.w3.org/2000/09/xmldsig#Object">
      <Transforms><Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/></Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>xZOW9jDPVeJHjZ9f1wMJonhYhDU=</DigestValue>
    </Reference>
    <Reference Id="idPackageSignature-Ref-7" URI="#idPackageSignature-Sp-6"
        Type="http://uri.etsi.org/01903#SignedProperties">
      <Transforms><Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/></Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>1ewVQ5OKIMU+Vcja6hx6b/chwf0=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue
```

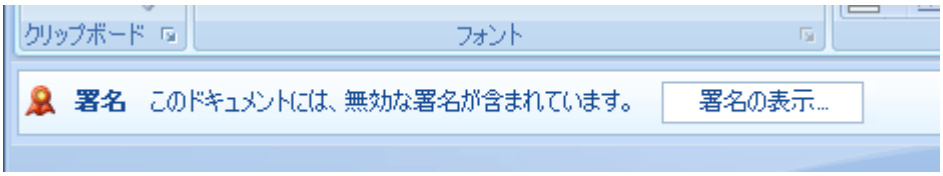
```
Id="idPackageSignature-Sv-4">d3svvBwLuesp6mK/S......DlqgrTC+/onwlcs=</SignatureValue>
  <KeyInfo Id="idPackageSignature-Key-5">
    <X509Data>
      <X509Certificate>MIIDlDCCAv2g......FNH6DtkojDRA3G/EBWcE=</X509Certificate>
    </X509Data>
    <KeyValue>
      <RSAKeyValue>
        <Modulus>urHtAraFHxXUB6drW......J4ybnBzOpUInfsJ7lNSYs=</Modulus>
        <Exponent>AQAB</Exponent>
      </RSAKeyValue>
    </KeyValue>
  </KeyInfo>
  <Object Id="idPackageObject">
    <Manifest>
      <Reference
          URI="/_rels/.rels?ContentType=application/vnd.openxmlformats-package.relationships+xml">
        <Transforms>
          <Transform
Algorithm="http://schemas.openxmlformats.org/package/2006/RelationshipTransform">
            <mdssi:RelationshipReference SourceId="rId1"/>
          </Transform>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>1vWU/YTF/7t6ZjnE44gAFTbZvvA=</DigestValue>
      </Reference>
      <Reference URI="/word/_rels/document.xml.rels?
ContentType=application/vnd.openxmlformats-package.relationships+xml">
        <Transforms>
          <Transform
Algorithm="http://schemas.openxmlformats.org/package/2006/RelationshipTransform">
            <mdssi:RelationshipReference SourceId="rId3"/>
            <mdssi:RelationshipReference SourceId="rId2"/>
            <mdssi:RelationshipReference SourceId="rId1"/>
            <mdssi:RelationshipReference SourceId="rId5"/>
            <mdssi:RelationshipReference SourceId="rId4"/>
          </Transform>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>zAGOXkhww/vsV8M3Agd0/+AHFYw=</DigestValue>
      </Reference>
      <Reference URI="/word/document.xml?
ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.document.main+xml">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>V8w/ettXsE3Xm+9bDUXxpQf380g=</DigestValue>
      </Reference>
      <Reference URI="/word/fontTable.xml?
ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.fontTable+xml">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>avBMPJLJQE4LnLawd0hrJgKo7A4=</DigestValue>
      </Reference>
      <Reference URI="/word/settings.xml?
ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.settings+xml">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>TCj0Q1LHssxSbFrNgjFvkJhJDP4=</DigestValue>
```

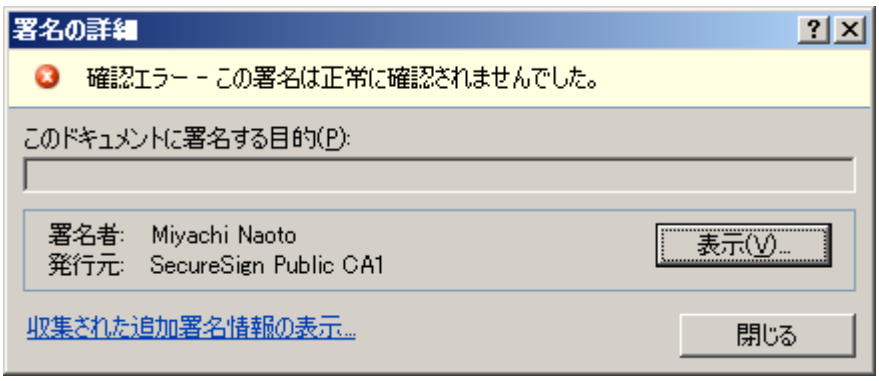
```
      </Reference>
      <Reference URI="/word/styles.xml?
ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.styles+xml">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>1kunkUW3bF/09KfcfFszvGuMAE8=</DigestValue>
      </Reference>
      <Reference URI="/word/theme/theme1.xml?
ContentType=application/vnd.openxmlformats-officedocument.theme+xml">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>njId7TpxXaw3lGZC2bqGy6DvWRw=</DigestValue>
      </Reference>
      <Reference URI="/word/webSettings.xml?
ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.webSettings+xml">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>lsJpQUi3QcTiTVvBBf6+hbXAN/o=</DigestValue>
      </Reference>
    </Manifest>
    <SignatureProperties>
      <SignatureProperty Id="idSignatureTime" Target="#idPackageSignature">
        <mdssi:SignatureTime>
          <mdssi:Format>YYYY-MM-DDThh:mm:ssTZD</mdssi:Format>
          <mdssi:Value>2008-11-06T12:30:46Z</mdssi:Value>
        </mdssi:SignatureTime>
      </SignatureProperty>
    </SignatureProperties>
  </Object>
  <Object Id="idOfficeObject">
    <SignatureProperties>
      <SignatureProperty Id="idOfficeV1Details" Target="#idPackageSignature">
        <SignatureInfoV1>
          <SetupID/>
          <SignatureText/>
          <SignatureImage/>
          <SignatureComments/>
          <WindowsVersion>5.1</WindowsVersion>
          <OfficeVersion>12.0</OfficeVersion>
          <ApplicationVersion>12.0</ApplicationVersion>
          <Monitors>1</Monitors>
          <HorizontalResolution>1024</HorizontalResolution>
          <VerticalResolution>768</VerticalResolution>
          <ColorDepth>32</ColorDepth>
          <SignatureProviderId>{00000000-0000-0000-0000-000000000000}</SignatureProviderId>
          <SignatureProviderUrl/>
          <SignatureProviderDetails>9</SignatureProviderDetails>
          <ManifestHashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</ManifestHashAlgorithm>
          <SignatureType>1</SignatureType>
        </SignatureInfoV1>
      </SignatureProperty>
    </SignatureProperties>
  </Object>
  <Object Id="idPackageSignature-XAdES-Object">
    <QualifyingProperties Target="#idPackageSignature">
      <SignedProperties Id="idPackageSignature-Sp-6">
        <SignedSignatureProperties>
          <SigningCertificate>
            <Cert>
```

```
            <CertDigest>
              <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <DigestValue>OSKEwLpv9YKc075wYMyUwzXU1TI=</DigestValue>
            </CertDigest>
            <IssuerSerial>
              <X509IssuerName>CN=TEST, O=TEST ORG, C=JP</X509IssuerName>
              <X509SerialNumber>5400365494282747904</X509SerialNumber>
            </IssuerSerial>
          </Cert>
        </SigningCertificate>
        <SignaturePolicyIdentifier>
          <SignaturePolicyImplied/>
        </SignaturePolicyIdentifier>
      </SignedSignatureProperties>
    </SignedProperties>
    <UnsignedProperties>
      <UnsignedSignatureProperties>
        <SignatureTimeStamp Id="idPackageSignature-STS-1">
          <EncapsulatedTimeStamp Id="idPackageSignature-ESTS-1">
            MIIPcAYJKoZIhvcNAQcC.....Q8oKllSIyQWOSc=
          </EncapsulatedTimeStamp>
        </SignatureTimeStamp>
      </UnsignedSignatureProperties>
    </UnsignedProperties>
  </QualifyingProperties>
 </Object>
</Signature>
```

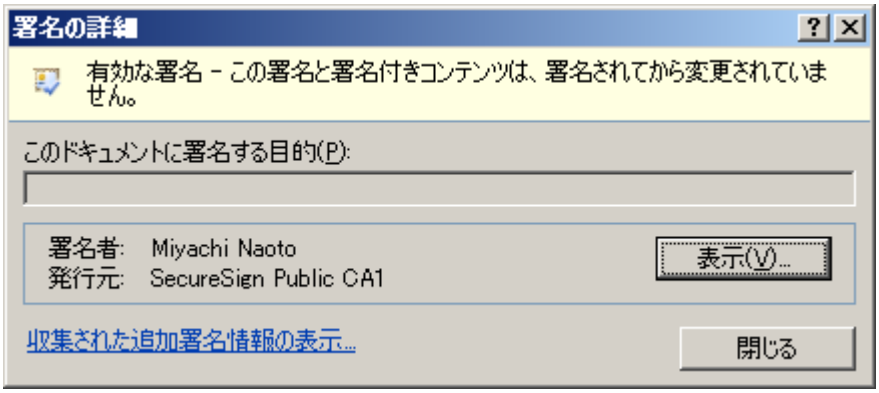
### 3.4.2　MS-Office 2007 による検証結果

3.4.1.の長期署名サンプルをセットした OOXML ファイルを MS-Office 2007 で読み込んでみたところ、残念ながら正常に署名検証がされず無効となってしまった。



同じテストツールにて長期署名部を省くと正しく検証されるようになる。




このことより長期署名用の Object 要素を追加した場合には MS-Office 2007 ではエラーになる事がわかった。長期署名用の Object 要素もただ追加するだけならエラーにならない事から Reference 要素の Type 属性が長期署名用の「Type="http://uri.etsi.org/01903#SignedProperties"」となっている事か、Object 要素以外を Reference 指定している事が問題なのかもしれない。しかし OOXML 仕様書の「Application-Specific Object」の箇所には Type 属性に関する記述や Reference 先の要素に限定がないので明確な仕様違反とは言えないようにも思える。

### 3.4.3 RelationshipTransoform 変換

XML 署名では Reference 要素の属性として Transform (変換) 要素をセット可能になっている。ODF 署名では XML 署名標準の Transform 要素だけであるが、OOXML 署名では独自の変換である RelationshipTransform が仕様として設定されている。これは「Package-Specific Object」内の Manifest 要素内に定義されている Reference 要素にて指定されている。OOXML では Relationship 署名対象 (拡張子が ".rels" のファイル) に対し、Transform 要素として ReleationshipTransform 変換の後で XML 正規化変換 (c14n 変換) を行うことが指定されている。拡張子が ".rels" のファイルも内部は XML となっているので、この 2 つの変換を順次適応してハッシュ計算対象の XML 情報を取得する。RelationshipTransform を使った変換は大雑把に言って以下の手順で良い。

| |
|---|
| 1) 必要な Relationship 要素を対象となる .rels より取り出す<br>Transform 要素の SourceId 属性で指定されていない Relationship 要素は削除する |
| 2) 名前空間プレフィックス等があれば削除する<br>MS-Office 2007 で生成されたファイルは最初から名前空間プレフィックスを含んでいない |
| 3) Relationship 要素で省略されている属性情報を追加する<br>通常 TargetMode 属性が省略されているので補う (OOXML 仕様書説明に記載が無い) |
| 4) Relationship 要素を Id 属性により並べ替え (ソート) する |

5) XML 正規化を実施する
余分な余白削除や Id をアルファベット順に並べたり名前空間の処理をする

3) の TargetMode 属性を付けなければならない点が OOXML 仕様書に記載が無く、試行錯誤により解析をした。本来なら仕様書の手順として明記しておくべき項目であろう。この変換をおこなった結果を以下に示す。なお以下は見やすくする為に改行や空白を加えてあるが実際には改行や空白は入らない。

```
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship
    Id="rId1"
    Type="http://schemas.openxmlformats.org/package/2006/relationships/digital-signature/signature"
    Target="sig1.xml"/>
</Relationships>
```

変換前

```
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship
    Id="rId1"
    Target="sig1.xml"
    TargetMode="Internal"
    Type="http://schemas.openxmlformats.org/package/2006/relationships/digital-signature/signature">
  </Relationship>
</Relationships>
```

変換後

### 3.4.4 OOXML の長期署名化に関する考察

OOXML の XML 署名の仕様は独自の拡張や形式も拡張されており、良く言えば仕様が明確ではあるが半面長期署名のような拡張に対する柔軟性が少ないとも言える。OOXML の仕様書を読む限りでは長期署名の Object を「Application-Specific Object」として入れられるようにも思える。しかし実際には MS-Office 2007 において長期署名を行った OOXML ファイルはエラーとなっている。

MS-Office 2007 標準機能の開発はマイクロソフト社しか行えない。出来る事なら長期署名 XAdES の仕様も許すような実装を次期 MS-Office には強く期待をしたい。できれば長期署名の拡張をきちんと OOXML の仕様として取り入れて欲しい。それまで拡張モジュールとしてアドインやプラグインのような形式で長期署名を実現する事は可能ではある。しかしその場合には MS-Office 2007 本体では XML 署名としての検証もエラーになってしまう。

#### 3.4.4.1 署名日時に関する考察と要望

MS-Office 2007 では表示する署名日時を、「Package-Specific Object」の中の独自の SignatureTime 要素から取得している。長期署名対応として考えた場合に、もし署名タイムスタンプが付与された XAdES-T 形式であればタイムスタンプ日時を署名日時として表示して欲しい。

また署名タイムスタンプが無く SignatureTime 要素も無い場合には、XAdES の SigningTime 要素の日時を表示して欲しい。

## 3.5 まとめ

本来 OOXML や ODF へ長期署名を組み込む場合には、まず ISO 仕様として長期署名仕様を採用して貰い、しかるのちに MS-Office や OpenOffice.org 等のアプリケーションにて実装をして貰う手順を踏むべきである。しかしながら長期署名仕様として既存の XML 署名との互換性を実現できるのであればより良い仕様となると考えて今回のテストと考察をおこなった。

ISO 標準となった PDF (Portable Document Format) フォーマットにおいて、次期仕様では長期署名の検討が開始されている。しかし PDF フォーマットの電子署名ではバイナリ形式の為に ByteRange により署名範囲と署名データ格納の範囲が決められている制約がある。この為に PDF の長期署名仕様には工夫が必要となると考えられる。

今回のテスト結果から、ODF に関してはおそらく素直に XML 署名の拡張として長期署名仕様を実現できそうであり、OOXML に関しても少し MS-Office での検証に問題があったが、最初から長期署名を意識した仕様を検討すれば比較的容易に長期署名仕様が実現できるのではないかと考える。今後両フォーマットにおいて ISO 標準仕様として長期署名 XAdES 仕様が正式に採用されることを期待したい。

### 3.5.1 参考文献


「ETSI TS 101 903 v1.3.2 (2006-03) XML Advanced Electronic Signatures (XAdES)」

「電子文書長期保存ハンドブック　平成 19 年 3 月」(ECOM)

「電子文書保存のしくみと実務 第 2 版」ISBN978-4-502-96730-6

「XML 署名利用電子署名 (XAdES) の長期署名プロファイル」(ECOM)
http://www.ecom.jp/LongTermStorage/data/jis/Long_term_signature_profiles_for_XAdES(jp).pdf

「Office Open XML - Part2: Open Packaging Conversions 」
http://www.ecma-international.org/news/TC45_current_work/TC45_available_docs.htm

「Open Document Format for Office Applications (OpenDocument) v1.1」
(注意：現在は電子署名未対応の 1.1 までが公開済み)
http://www.oasis-open.org/specs/index.php#opendocumentv1.1

「国立情報学研究所 OpenXML 長期署名システム設計書 (概要/詳細)」
http://www.langedge.jp/pub/doc/NII-OpenXml-XAdES-Outline.pdf
http://www.langedge.jp/pub/doc/NII-OpenXml-XAdES-Detail.pdf

「Office Open XML Formats 入門」ISBN978-4-8399-2582-6

## 4. ERS の JIS 長期署名プロファイルへの導入案

RFC4998 として規定される ERS（Evidence Record Syntax）は、RFC3161 のタイムスタンプ等を利用して、電子データの存在時刻や非改ざん性を長期にわたって証明するためのデータ、すなわちエビデンスレコードの構文である。

ERS の特徴は、ハッシュツリーを利用することにより、複数の電子データに対する証明を少数のタイムスタンプでカバーできることである（図 3.4.1）。また、タイムスタンプの更新やハッシュツリーの更新により、単一のタイムスタンプの有効期限を越えた長期にわたる証明が可能となる（詳細は RFC4998 を参照いただきたい）。これらの特徴から、大量の文書を長期にわたって管理・保存する場合にタイムスタンプ取得に係るコストや運用の手間を大幅に軽減できることが予想される。

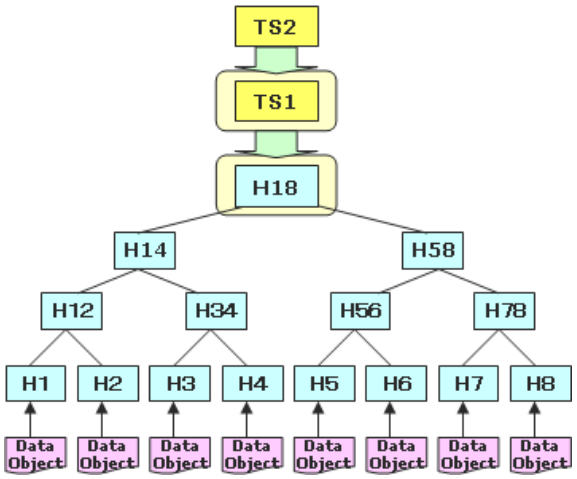



図 3.4.1 ERS におけるタイムスタンプの付与

複数のデータオブジェクトをハッシュツリーで関連付け、ルートのハッシュツリーにのみタイムスタンプ（TS1）を付与することで、すべてのデータオブジェクトの存在証明と非改ざん証明を実施。TS1 の有効期限が切れる前に TS2 を付与すること（タイムスタンプの更新）により、証明期間を延長可能

対象とする電子データには制約はないため、長期署名フォーマットにおける検証情報までを含めた ES-X Long のデータを証明対象のデータ、すなわちデータオブジェクトとすることが可能である。こうすることにより個々の署名ごとにアーカイブタイムスタンプを取得する必要がなくなる。エビデンスレコードは、こうして全体に付与されたタイムスタンプと個々のデータオブジェクトとの関係（ハッシュのリンク関係）をデータオブジェクトごとに縮約ハッシュツリー（reduced hash tree）として保存しているため（図 3.4.2）、エビデンスレコード内の情報を利用することで、個々のデータオブジェクトの存在と非改ざん性を証明することができる。これはつまり、長期署名フォーマットにおけるアーカイブタイムスタンプと同様な効果を得られることを意味する。また、その構造を見れば判るように、長期署名フォーマットにおける現行のアーカイブタイムスタンプの代わりにエビデンスレコードを格納することは、技術的に何ら問題ない。

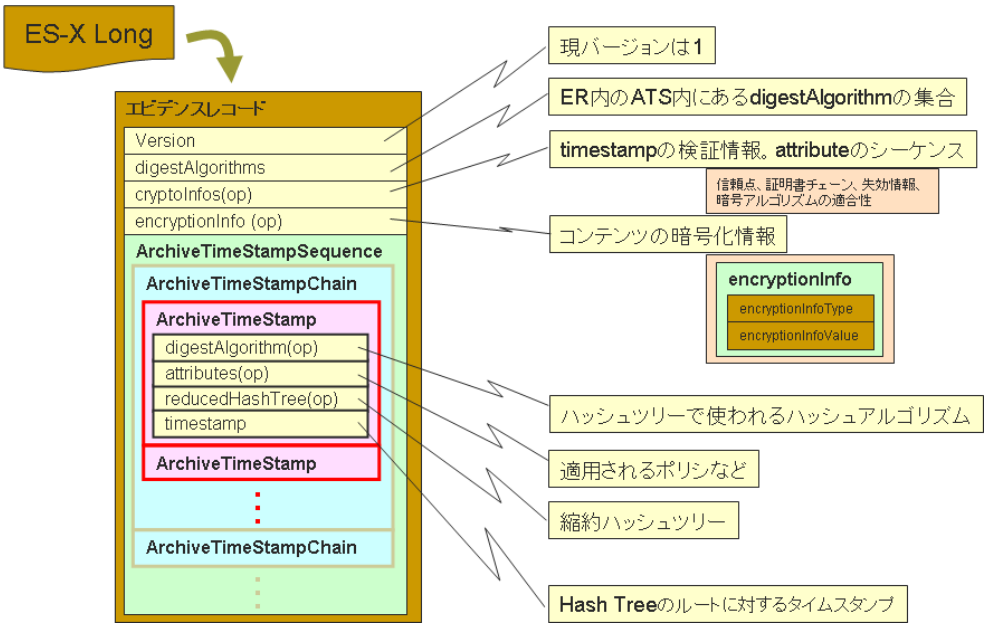



図 3.4.2 エビデンスレコードの構造

そこで本節では、現行の JIS 長期署名プロファイル（JIS X 5092、JIS X 5093）にエビデンスレコードを導入する際の改定案を示す。

## 4.1 JIS X 5092 の改定案

JIS X 5092 の改定案を次に示す。

(1) 3.25 として次を追記。

**3.25 証拠記録 (evidence record)**

データの存在時刻を特定可能とし、改ざんを検知可能とするための、タイムスタンプを含む証拠情報の集まり。

**注記** IETF RFC 4998 で定義されている。

(2) 表 6 に証拠記録を追記。

**表 6－追加される非署名属性**

| 要素 | 要求レベル |
|---|---|
| 全証明書参照情報群 | 必す |
| 全失効参照情報群 | 必す |
| - CRL 形式の失効参照情報群 | 任意選択 |
| - OCSP 形式の失効参照情報群 | 任意選択 |
| - 他の形式の失効参照情報群 | 要別途規定 |
| 属性証明書の参照情報群 | 要別途規定 |
| 属性失効情報の参照情報群 | 要別途規定 |

| | |
|---|---|
| 証明書群 | 必す |
| - 証明書 | 任意選択 |
| - CA 等による証明書の保管 | 要別途規定 |
| 失効情報群 | 必す |
| - CRL による失効情報 | 任意選択 |
| - 基本 OCSP 応答 | 任意選択 |
| - 他の失効情報 | 要別途規定 |
| - CA 等による失効情報の保管 | 要別途規定 |
| CAdES-C データへのタイムスタンプ | 要別途規定 |
| タイムスタンプが付与された証明書及び失効情報に関する参照 | 要別途規定 |
| （改ざん検知を可能とする情報） | 必す |
| - アーカイブタイムスタンプ id-aa-48 | 任意選択 |
| - アーカイブタイムスタンプ id-aa-27 | 任意選択 |
| **- 証拠記録 id-aa-er** | **任意選択** |
| - タイムマークなどその他の方式 | 要別途規定 |

(3) 付属書として次を追記。

# 附属書 X
# （規定）
# 証拠記録の構造

**序文**

この附属書は、長期署名における証拠記録の構造に関する要求事項を規定する。

## D.1 準拠する仕様

この規格における証拠記録は RFC4998 の仕様に準拠する。

## D.2 構成要素の要求レベル

証拠記録の各要素に対する要求レベルは**表 X.1** に従う。

**表 X.1－証拠記録の各要素に対する要求レベル**

| 要素 | 要求レベル | 条件又は値 |
|---|---|---|
| 証拠記録の版数 | 必す | 1 |
| ダイジェストアルゴリズム識別子群 | 必す | |
| 暗号関連情報群 | 要別途規定 | |
| 暗号化情報 | 要別途規定 | |
| - 暗号化情報の種別 | 要別途規定 | |
| - 暗号化情報の値 | 要別途規定 | |

| | | |
|---|---|---|
| アーカイブタイムスタンプチェーン群 | 必す | |
| - アーカイブタイムスタンプ群 | 必す | |
| - アーカイブタイムスタンプ | 必す | |
| - ダイジェストアルゴリズム識別子 | 任意選択 | |
| - 属性群 | 要別途規定 | |
| - 縮約ハッシュツリー | 任意選択 | |
| - 部分ハッシュツリー | 任意選択 | |
| - タイムスタンプトークン | 必す | |

## 4.2 JIS X 5093 の改定案

JIS X 5093 の改定案を次に示す。

(1) 3.21 として次を追記。

**3.21 証拠記録 (evidence record)**

データの存在時刻を特定可能とし、改ざんを検知可能とするための、タイムスタンプを含む証拠情報の集まり。

**注記** IETF RFC 4998 で定義されている。

(2) 表 5 に証拠記録を追記。

**表 5 追加される非署名対象の署名プロパティ要素**

| 要素又は処理方式 | 要求レベル |
|---|---|
| 全証明書参照情報群 | 任意選択 a) |
| 全失効情報参照情報群 | 任意選択 a) |
| - CRL 形式の失効情報参照情報 | 任意選択 |
| - OCSP 形式の失効情報参照情報 | 任意選択 |
| - 他の失効情報参照情報 | 要別途規定 |
| 属性証明書参照情報群 | 要別途規定 |
| 属性失効情報参照情報群 | 要別途規定 |
| 署名及び参照情報に対するタイムスタンプ | 要別途規定 b) |
| - *非分離型* | 必す |
| - *分離型* | 要別途規定 |
| 参照情報に対するタイムスタンプ | 要別途規定 b) |
| - *非分離型* | 必す |
| - *分離型* | 要別途規定 |
| 証明書群 | 必す |
| - カプセル構造化された証明書 | 任意選択 |
| - 他の証明書 | 要別途規定 |

| | |
|---|---|
| - CA 等による証明書の保管 | 要別途規定 |
| 失効情報群 | 必す |
| - CRL による失効情報群 | 任意選択 |
| - OCSP による失効情報群 | 任意選択 |
| - 他の失効情報群 | 要別途規定 |
| - CA 等による失効情報の保管 | 要別途規定 |
| 属性証明書群 | 要別途規定 |
| 属性失効情報群 | 要別途規定 |
| (改ざん検知を可能とする情報) | 必す |
| - アーカイブタイムスタンプ | 任意選択 |
| - *非分離型* | 必す |
| - *分離型* | 要別途規定 |
| **- 証拠記録 id-aa-er** | **任意選択** |
| - タイムマークなどその他の方式 | 要別途規定 |
| 異なる版の非署名対象の署名プロパティ | 要別途規定 |

(3) 付属書として 4.1(3)で示した内容を追記。

## 4.3 参考文献

[RFC4998] “Evidence Record Syntax (ERS)”, 2007/8

# 付録：電子署名普及ワーキンググループにおける国際標準化活動

署名普及ワーキンググループでは、下部組織として国際標準化委員会を設置し以下の国際標準化活動を推進してきた。本節ではこれらを報告する。

(1) ETSI ESI とのXAdESおよびCAdESの実証実験のための協力体制
(2) JIS長期署名フォーマットプロファイルの国際標準（ISO）化に向けた活動
(3) PDF長期署名の標準化に向けた活動
(4) ETSI ESI会議へのアソシエートメンバーとしての参加・意見交換

# 1. 長期署名フォーマットの実証実験に関する国際活動

欧州通信規格協会（ETSI, www.etsi.org）の電子署名基盤技術委員会（TC ESI）が規定しIETF RFCやW3Cの標準としても公開されている長期署名フォーマットであるXAdESとCAdESについて、ECOM署名関連のワーキンググループでは2005年頃より長期署名の仕様の改定や相互運用実験について協力関係を育んできた。ECOMはこれまで日本において、インターネット上でどこからでも参加できる2回のXAdESとCAdESの世界初のリモートプラグテストを実施してきた。当初、ETSIで開催される携帯電話通信（3G)、署名、ITSなどの全てのプラグテストがフランス・ソフィアアンチポリスのETSI本部に集って実施する対面テストしか実施した経験が無かったため、リモートプラグテストについては懐疑的だったがECOMからのETSI ESIへの継続的な説明、説得により2007年2月には欧州2組織（UPC、IAIK)、日本2組織（日本電気、エントラストジャパン）により事前実験が実施され、ETSIにおける初のリモートプラグテストの実現可能性が日欧で確認された。

この日欧事前実験の経験を踏まえ、一般組織の参加を募り ETSI でリモートプラグテストを実施するためにETSIにおいて技術専門家作業部会STF-351 Interoperability framework for XML Advanced Electronic Signatures（XAdES）が組織されECOMからもボランティアとして貢献した。
http://portal.etsi.org/stfs/STF_HomePages/STF351/STF351.asp
http://xades-portal.etsi.org/pub/STF-351_presentation.shtml

STF-351では、2008年度に2回の長期署名フォーマットの実証実験を行うにあたり次の会議を行った。
・2回の対面会議（2008年8月東京、2009年2月バルセロナ）
・14回の電話会議（2009年1月21日までの期間において）
・2008年8月、東京におけるセミナーの実施

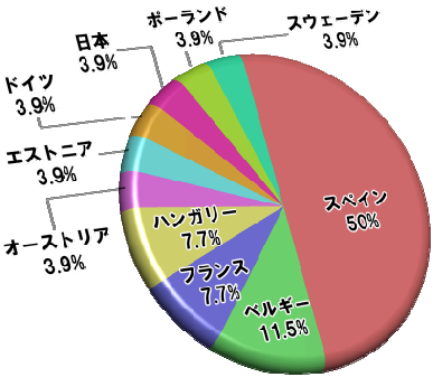
## 1.1 ETSI STF-351 メンバーと役割

ETSI STF-351のメンバーとそれぞれの役割を以下に示す。

| 氏名(略号)・所属・ | 役割 |
|---|---|
| Juan Carlos Cruellas Ibarz (JC)<br>スペイン カタロニア工科大学 教授 | STF リーダー・XAdES テストケース設計・XAdES 失敗系テストデータ生成・テストケース記述言語設計・欧州委員会およびETSI 向け報告書作成 |
| Peter Kremer (PK)<br>フランス ETSI | STF 事務局・プラグテスト事務局・実験ポータルサイトの構築・対ETSI ESI 報告 |
| Konrad Lanz (KL)<br>オーストリア A-SIT, IAIK グラーツ工科大学 | XAdES テストケース設計・実験ポータルサイトの構築 (CA, OCSP, LDAP, TSP) |
| Gregory Sun (GS)<br>マカオ Macau Post | ボランティアメンバー・ドキュメントレビュー |
| 前田陽二 (YM)<br>日本 ECOM | ボランティアメンバー・日本側事務局・ECOM-ETSI セミナーの国内調整 |
| 漆嶌賢二 (KU)<br>日本 エントラストジャパン | ボランティアメンバー・XAdES テストケース設計・XAdES 失敗系テストデータ生成・CAdES テストケース設計・CAdES 失敗系テストデータ生成・ECOM-ETSI セミナーのSTF 内調整と運営・日本向けの実験参加者用ヘルプデスクの運営と対応 |

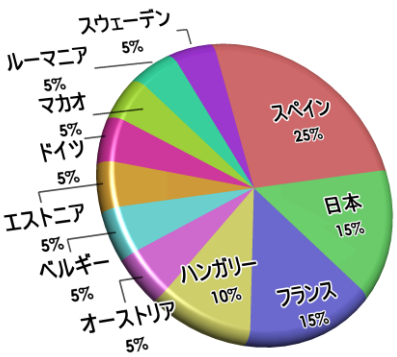
## 1.2 ETSI 1st Remote XAdES Plugtests（2008 年 3 月）

日欧 4 組織による事前実験の経験を踏まえ、ETSI が主催する第一回の XAdES リモートプラグテストが 2008 年 3 月 3 日～7 日の日程で開催され、日欧 10 カ国、26 組織の実装が参加した（参加内訳は右表）。日本からは 1 社が参加している。まだ、STF-351 の発足前のテストであり生成検証テストのみしか行わず、署名者証明書は参加者が全て同じものを使っていた。実験用タイムスタンプ局についてはソフトウェアベースのものを実験用に立ち上げ、以降の実験でも同じものが使用されている。




## 1.3 ETSI 2nd Remote XAdES Plugtests（2008 年 9 月）

ETSI STF-351 が発足後初めての XAdES リモートプラグテストが 2008 年 9 月 8 日～14 日の日程で開催され、日欧 11 カ国、20 組織の実装が参加した（参加内訳は右表）。日本からは日本電気、三菱電機情報技術総合研究所、エントラストジャパンの 3 社が参加し、その他アジア圏からマカオ



郵政局が参加した。このテストではPKI環境が整備され、参加者毎に証明書を発行し、OCSP、LDAPなどのサービスも利用できるようになった。また、署名を交換し生成・検証するテストの他に、誤りのある署名を正しく検証できるかという失敗系の検証テストが追加された。

## 1.4　ETSI 3rd Remote XAdES/CAdES Plugtests（2009年2月）

2009年2月16日～27日の日程でXAdESとCAdESに関するリモートプラグテストが開催される予定となっている。ETSIにおけるCAdESのプラグテストは初の開催となる。当初よりECOMではこれまで二回のXAdES/CAdES国内実証実験の経験から、ETSI ESI会議においてXAdESに加えCAdESの実証実験の共催を要望してきたが、ようやく今回のテストで結実したものである。CAdES のテスト手順はETSI 2nd Remote XAdES Plugtestsの手順を踏襲している。CAdESのテストケース設計、テストデータの提供については、ほぼECOMからのボランティアによるものである。

## 1.5　ECOM-ETSI Advanced Electronic Signature Seminar 2008, Tokyo Japan

2008年8月18日、長期署名フォーマットやこれに関連する標準の主要エディタであるSTFのメンバーが日本に来る機会に、スペイン、オーストリア、マカオにおける長期署名フォーマット、デジタルタイムスタンプ、署名技術の動向を紹介してもらうと共に、長期署名フォーマットやREM（レジスタードメール）、PDF署名、OASIS拡張署名サービス（DSS-X）などの標準化動向について解説してもらうセミナー「ECOM-ETSI Advanced Electronic Signature Seminar 2008, Tokyo Japan」を実施した。ECOMとETSIによる初の試みのジョイントセミナーとなった。講演内容および講演者は以下の通りであった。

| |
|---|
| (1) XAdES/CAdES present and future. XAdES/CAdES and related standards in Spain<br>Universitat Politecnica de Catalunya(Spain), Juan Carlos Cruellas Ibarz 教授 |
| (2) XMLDSIG Status and new Developments, XAdES and the OASIS-DSS AdES-Profile<br>A-SIT, IAIK, Technische Universitat Graz(Austria) Konrad Lanz 氏 |
| (3) PKI and Time Stamping Services in Macau and global communities<br>マカオ郵政局（マカオ）孫君煬（Gregory Sun）氏（都合により欠席・前田研究員代読） |
| (4) ETSI XAdES/CAdES リモートプラグテストの参加方法<br>エントラストジャパン株式会社 漆嶌賢二 |

参考：

ECOMホームページ

ECOM-ETSI Advanced Electronic Signature Seminar 2008, Tokyo, Japan

http://www.ecom.jp/seminar/workshop01.html

## 1.6 会議記録

| 表題, 日時, 参加者 | 議題 |
|---|---|
| 第1回電話会議<br>2008.04.28 17-19<br>KU,KL,GS,YM,PK,JC | ・ETSI と STF-351 メンバーとの NDA<br>・ドキュメント共有(FTP)について<br>・メーリングリストについて |
| 第2回電話会議<br>2008.05.02 17-19<br>KU,KL,GS,YM,PK,JC | ・実験に向けた作業項目の洗い出し<br>（ポータル,PKI,TSP,LDAP,ML）<br>・PKI インストール |
| 第3回電話会議<br>2008.05.12 17-19<br>KU,KL,GS,YM,PK,JC | ・PKI の DN や LDAP に関する調整<br>・対面会議の日程調整<br>・実証実験の回数・日程・XAdES/CAdES の決議<br>回数は2回（2008.09 に XAdES のみ, 2009.02 に XAdES/CAdES）<br>・OCSP と CRL（発行周期）の決議<br>・テストケース記述言語について<br>・LDAP の公開について |
| 第4回電話会議<br>2008.05.30 17-19<br>KU,KL,GS,PK,JC | ・STF の作業スケジュールの確認<br>・XAdES 実験ポータルサイトの準備状況<br>署名用証明書、鍵、署名ポリシファイル等の入力ファイル群のドラフト<br>・対面会議の日程調整 |
| 第5回電話会議<br>2008.06.06 17-19<br>KU,KL,PK,JC | ・欧州委員会 EC/EFTA への STF 活動報告書のレビュー<br>・XAdES 実験ポータルの準備状況<br>CA,OCSP の稼動確認<br>・東京における対面会議について<br>欧州メンバーの出張予算申請（EC/EFTA）<br>・対面会議と AdES セミナーの併催について |
| 第6回電話会議<br>2008.06.13 17-19<br>KU,KL,GS,PK,JC | ・第二回実験の日程について（要報告書提出との日程調整）<br>EC/EFTA 提出の STF 活動最終報告書のドラフト期限は 2009 年 3 月 10 日<br>・プラグテスト案内文の作成<br>・XAdES 実験ポータルの準備状況<br>ユーザ認証（Basic 認証）の稼動確認、実験チャット<br>パスワード保護されるコンテンツの確認<br>・Java における Basic 認証のコードの共有（参加者に公開） |

| | |
|---|---|
| 臨時対面会議<br>2008.06.25 13-17<br>KU,YM,PK,JC | 場所：ETSI 本部（フランス ソフィアアンチポリス）<br>・ETSI ESI Meeting in Sofia Antipolice, France 後、臨時会議<br>・CA, TSP の動作確認<br>・前回テストのコンテンツを移動し、9 月テスト用の<br>コンテンツを準備<br>・テストの構成（成功系署名の交換（Positive）と、失敗系署名の検証（Negative））<br>・テストケースドラフトに関する KU からのコメントの反映<br>・東京で開催する AdES セミナーの調整<br>ECOM からのセミナーの計画の提示（アジェンダ、会場費用）<br>・KL は電話参加 |
| 第 7 回電話会議<br>2008.06.30 17-19<br>KU,KL,PK,JC | ・AdES セミナーin Tokyo<br>・ECOM 案の承認<br>・プラグテストの内容・参加方法について KU より紹介<br>・セミナー講演内容に関する調整<br>・ポータルの SSL 化について（否決）<br>・XAdES テストケースのレビュー |
| 第 8 回電話会議<br>2008.07.08 17-19<br>KU,KL,PK,JC | ・AdES セミナーin Tokyo セミナー資料の期限<br>・テストケースレビュー<br>・ポータルの準備状況の確認 |
| 第 1 回対面会議<br>2008.08.14-15<br>KU,KL,YM,PK,JC | 場所：東京（機会振興会館 ECOM 会議室）<br>・実験ポータルの説明と動作確認<br>TSP,OCSP 等で Basic 認証ができないユーザに対し、<br>登録 IP による認証無し制御<br>・AdES セミナーの講演スライドのレビュー<br>・ETSI に対する活動報告書のレビュー<br>・9 月実験のスケジュール<br>・事前に電話会議による実験説明会を行う<br>・実験方法に関する調整事項<br>・失敗系テストの個別テストケースの採択と署名生成分担 |
| 2008.08.18 | ECOM-ETSI Advanced Electronic Signature Seminar 2008, Tokyo Japan の開催 |
| 第 9 回電話会議<br>2008.08.27 17-19<br>KU,KL,PK,JC | ・東京対面会議のラップアップ<br>・実験説明会のスケジュールと内容の調整<br>・時間節約のため日本からの参加者向けに別途説明会は不要<br>・実験ポータルの準備状況<br>・テストケース定義ファイルのレビュー |

| | |
|---|---|
| 2008.09.08-14 | ETSI 2nd Remote XAdES Plugtests の実施 |
| 第 10 回電話会議<br>2008.10.15 17-19<br>KL, PK, JC | ・実験報告書の作成についての議論<br>・テストで得た参加者コメントの集計<br>・2009 年 2 月のテスト<br>・CAdES についての準備<br>・XAdES 仕様 改善点（案）の確認 |
| 第 11 回電話会議<br>2008.10.29 17-19<br>KL, PK, JC | ・実験報告書のドラフトレビュー<br>・XAdES 仕様 改善点（案）の確認<br>・ETSI Security Workshop における AdES Seminar の<br>開催（案）のレビュー |
| 第 12 回電話会議<br>2008.11.21 17-19<br>GS, PK, KL, JC | ・今後の作業分担案の議論（特に CAdES） |
| 第 13 回電話会議<br>2009.01.09 17-19<br>KU, KL, GS, PK, JC | ・今後の作業分担案の議論<br>・ECOM からの要望<br>・参加者とテスト結果の部分公開<br>・ECOM からのボランティア貢献作業の明記・公開<br>・次回対面会議（案）2009.02.02-03 in Barcelona, Spain<br>UPC Residence に宿泊（要至急予約）<br>・CAdES Testcase Definitions のレビュー依頼<br>・前回テストの問題点の議論（XLN データの誤り、属性証明書） |
| 第 14 回電話会議<br>2009.01.21 17-19 | ・CAdES テストケースのレビュー<br>・属性証明書の問題(KU) |
| 第 2 回対面会議<br>2009.02.02-03 | 場所：カタロニア工科大学（スペイン、バルセロナ） |
| 2009.02.16-27 | ETSI 3rd Remote XAdES/CAdES Plugtests の実施 |

## 2. 長期署名フォーマットプロファイルの国際標準化活動

2008年3月に発行された長期署名プロファイルに関するJIS規格（JIS X 5092, JIS X 5093）のISO標準化に関しては、提案先候補のTCやISO/IEC JTC1下のSCに打診していたが、最終的に、TC154に提案することが決まった（2008年9月のTC154国内委員会で決定）。これを受け、TC154メンバ国への具体的な提案活動が開始された。

### 2.1 長期署名国際標準化の中長期スコープ

長期署名は、署名文書が長期に保存できて意味をもつ。記録媒体が将来に亘って読み出せること、文書ファイルが将来も後方互換性をもって読み出せること、文書そのものが適切に管理され、意図的あるいは過失による誤廃棄や散逸から免れること、必要なときはいつでも検索して取り出せることなどが前提となる。従って、長期署名を定着させるためには、長期署名の視点でこれらの活動に積極的に関与し牽引役を果たして行かなければならない。

図 付.2.1 は、長期署名の観点から中長期的どのような活動に係わるべきかを示している。現在の立ち位置は、長期署名プロファイルのJIS規格が発行され、ISO標準化に向けた日本からの提案活動が始まったところである。これを契機に、今すぐにでも積極的に係わる必要がある活動は2つある。一つ目は、文書や帳票フォーマットへのISO標準の長期署名の組み込みである。具体的には、PDF、オフィス文書、電子データ交換（EDI）構文などへの長期署名の組み込みである。EDIについては、TC154への長期署名標準化提案の一環に組み込まれている。PDFについては、PDFのISO化（ISO 32000-1）に伴い2008年9月からISO/TC171/SC2/WG8（議長は米国）とETSIが連携して仕様策定作業を始めている。この活動に対しては、今後制定されるISO標準の長期署名プロファイルを参照するよう仕向けなければならない。オフィス文書（ODF/OOXML）に関しては一部でボランタリ活動が始まっており、今後の活動をウォッチする必要がある。

今すぐにでも積極的に係わる必要がある活動の二つ目は、長期署名の運用モデルの策定である。長期署名の普及には何等かのリファレンスが必要であり、リファレンスにはメタデータ、即ち、長期署名を維持するための説明や指示書が欠かせない。このメタデータは、文書そのものの長期保存のためのメタデータと整合がとれていることが望まれる。

これらの活動は、結果的に電子記録管理ガイドラインの策定そのものにほかならない。

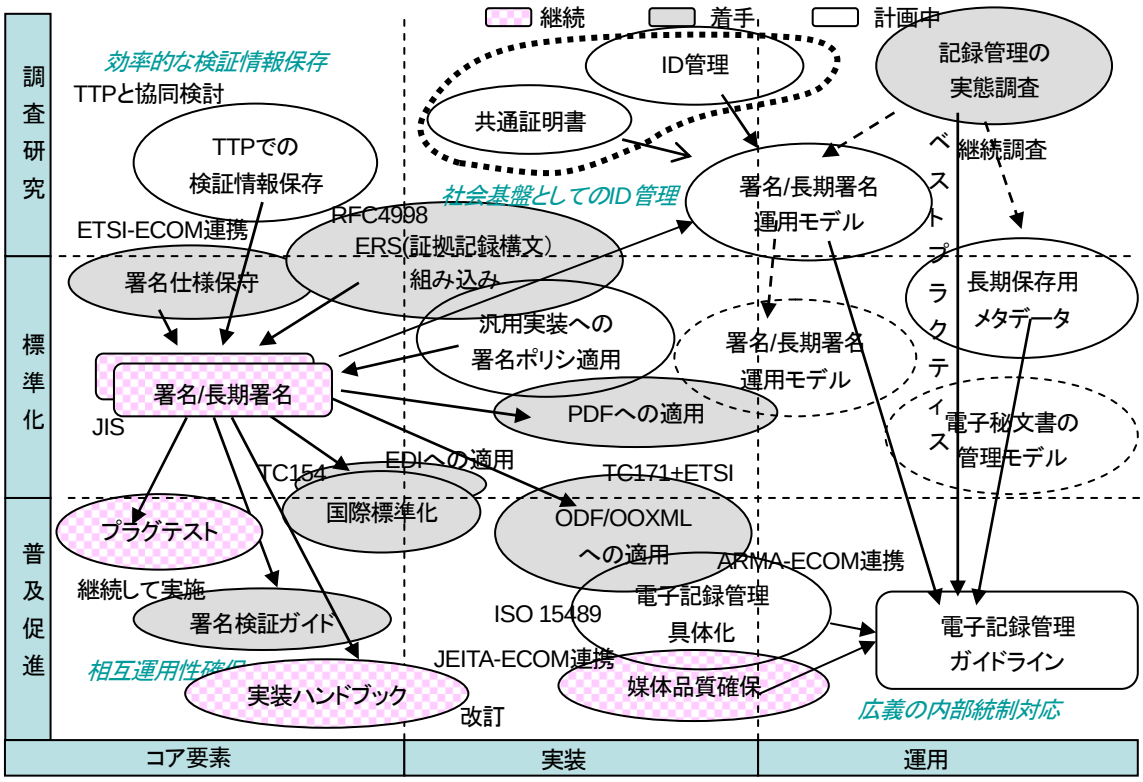



図 付.2.1 長期署名国際標準化の中長期スコープ

## 2.2 ETSI 長期署名プロファイルとの棲み分け

CAdES/XAdES に関するプロファイルは 2 系統存在する。1 つは JIS として制定された長期署名プロファイル（以降、JIS プロファイルと云う）であり、もう 1 つは ETSI が策定したプロファイル（以降、ETSI プロファイルと云う）である。現在、JIS プロファイル及び ETSI プロファイルとして次の仕様がある。

JIS X 5092　CAdES 長期署名プロファイル

JIS X 5093　XAdES 長期署名プロファイル

ETSI TS 102 734 V1.1.1　Profiles for CAdES based on TS 101 733 (2007-02)

ETSI TS 102 904 V1.1.1　Profiles for XAdES based on TS 101 903 (2007-02)

JIS プロファイルは、CAdES-T/XAdES-T 及び CAdES-A/XAdES-A のように時間軸のプロファイルであるのに対して、ETSI プロファイルは電子政府、e インボイス、ベースラインのようなドメイン別のプロファイルである。従って、結論から言えば JIS プロファイルと ETSI プロファイルは、競合関係ではなく補完関係にある。つまり、組み合わせて使うことができる。

(1) 複数プロファイル組み合わせ時の整合化

CAdES-A と e インボイスのように、JIS プロファイルと ETSI プロファイルを組み合わせて使う時、一方が必須要素 (M) でもう一方が選択要素 (O) など各要素の要求レベルが競合することが考えられる。この件に関して ECOM は、ETSI の会議のなかで組み合わせ時の整合化ルールを提案し、問題がないことを示した。

複数プロファイル組み合わせ時の整合化の基本的な考え方は次の通りである。

①正規化規則と整合化規則を作る

②各プロファイルを正規化して重ね合わせる

③整合化規則を適用する

④必要なら対立する要求を調整する

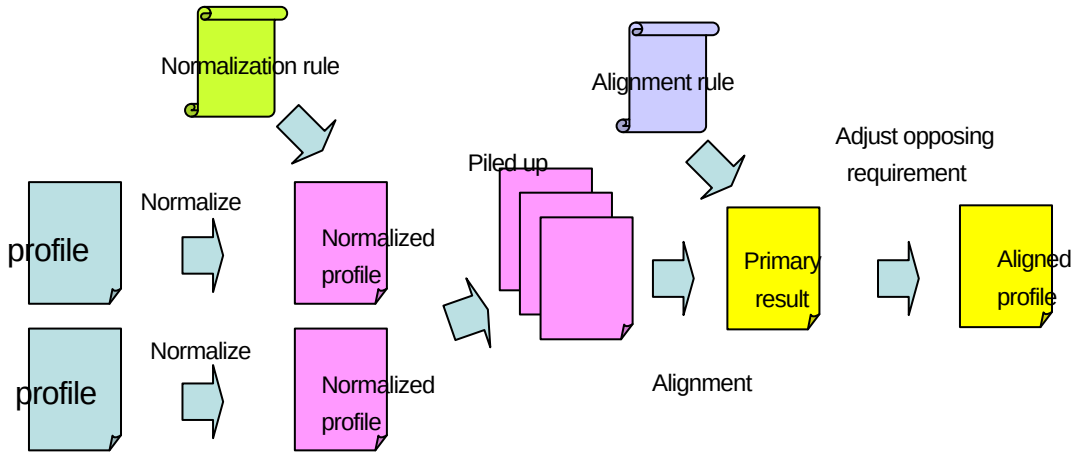



図 付.2.2 複数プロファイル組み合わせ時の整合化

(2) 正規化規則

サービスと実行要素に対する各々の要求レベルを表 付.2.1 に示す shall、should、may、shouldnot、shallnot の 5 つのキーワードで表現する。キーワードの定義は RFC2119 に従う。

表 付.2.1 正規化のキーワード

| KEY WORDS | MEANING (RFC2119) |
|---|---|
| MUST<br>REQUIED<br>SHALL NOT | the definition is an absolute requirement of the specification. |
| SHALL<br>SHOULD<br>RECOMENDED | there may exist valid reasons in particular circumstances to ignore a particular item. |

| | |
|---|---|
| MAY<br>OPTIONAL | an item is truly optional. |
| SHOULD NOT<br>NOT RECOMENDED | there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful. |
| MUST NOT<br>SHALL NOT | the definition is an absolute prohibition of the specification. |

(3) 整合化規則

整合化規則を表 付.2.2 に示す。ここで、マトリックスの交点が整合化結果である。一方が shall、もう一方が shallnot の場合は整合化に失敗する。shall と shouldnot, should と shouldnot, should と shallnot の組み合わせは、個別調整の対象である。

図 付.2.3 に整合化規則の適用例を示す。

**表 付.2.2 整合化規則**

| | Shall | Should | May | Should not | Shall not |
|---|---|---|---|---|---|
| Shall | Shall | Shall | Shall | Shall | － |
| Should | － | Should | Should | May | Should not |
| May | － | － | May | Should not | Should not |
| Should not | － | － | － | Should not | Should not |
| Shall not | － | － | － | － | Should not |

| TS 102 734 | 生成 | 検証 |
|---|---|---|
| SigningCertRef | shall | shall |
| ESS SigningCert | should | shall |
| ESS SigningCert V2 | may | shall |

| JIS X 5092 | 生成 | 検証 |
|---|---|---|
| SigningCertRef | shall | shall |
| ESS SigningCert | may | may |
| ESS SigningCert V2 | may | may |

整合化結果

| TS 102 734 | 生成 | 検証 |
|---|---|---|
| SigningCertRef | shall | shall |
| ESS SigningCert | should | shall |
| ESS SigningCert V2 | may | shall |

**図 付.2.3 整合化規則の適用例**

## 2.3 ISO/TC154 総会（ベルギー）

| | |
|---|---|
| 表題 | ISO/TC154 Prenary Meeting |
| 場所 | ベルギー ブリュッセル WCO（世界税関機構）本部ビル Room E3.27<br>Rue du Marche’30, Brussels, Belgium |
| 日時 | 2008 年 11 月 25 日 12:00 ～ 2008 年 11 月 26 日 14:00 |
| 参加者 | ISO/TC154 国内委員会（伊藤委員長、鬼頭副委員長）<br>NEC 木村、エントラスト 漆嶌 |
| 議題概要 | ・新しい ISO/TC154 議長の就任に伴う全作業項目の状況確認<br>・EDIFACT, UN/CEFACT の用語の統一に関する報告<br>・新しい作業項目提案、各国の関連活動紹介<br>・欧州での ebXML の利用紹介<br>・トランザクション証拠情報としての長期署名プロファイル（日本）<br>・中国での利用状況紹介 |

ISO/TC154 は電子データ交換の基盤技術である EDI の標準化に係る技術委員会であり、日本情報処理開発協会（JIPDEC）が国内審議委員会の事務局となっている。TC154 で扱われる電子商取引の基本プロトコルは従来型メッセージベースの UN/EDIFACT と XML に基づく ebXML がある。そのどちらも電子署名が可能であるがトランザクションの電子的な記録を長期に渡り保管する必要がある。

そこで電子署名普及 WG では、TC154 国内審議委員会を通じて TC154 の総会にて UN/EDIFACT や ebXML の記録保管にも応用できる長期署名フォーマットプロファイルに関する新しいワークアイテムの提案を行った。総会での趣旨説明概要は以下の通りである。

・EDI（UN/EDIFACT や ebXML）においてもトランザクションの記録保存は重要。
・UN/EDIFACT および ebXML は電子署名をサポートしている。
・しかしながら、使用する証明書の有効期限、失効の問題から長期には保存できない。
・UN/EDIFACT および ebXML のメッセージの電子的長期保存を可能にする
　長期署名フォーマットプロファイルの標準化をワークアイテムとして提案
・JIS として既に同プロファイルは公開済みであり、これに基づいた国際標準とする。
・同プロファイルは電子商取引以外でも金融、医療などにも適用可能な基礎となる。

趣旨説明後、参加各国からは好意的なコメントが寄せられ、特に興味を持った米国、中国に対しては資料等の情報を提供した。既に P メンバーの賛成確保のため動いており 2009 年以降、策定作業を進めていくこととなった。これも一重に経済産業省 森田様、伊東国内審議委員長、ISO の事務局である猿橋様の多大なるご助言、ご尽力の賜物であり、ここに感謝の意を表したい。

## 2.4　TC154 における長期署名標準化スケジュール

TC154 全体会議での長期署名プロファイル標準化提案の事前説明により、現在提案段階に進んでいる。今後のスケジュールは図 付.2.4 の通りである。

現時点の TC154 の P メンバ（投票権をもつメンバ国）は、アルジェリア（IANOR)、オーストラリア（SA)、ベルギー（NBN)、ブルガリア（BDS)、中国（SAC)、Czech Republic（CNI)、デンマーク（DS)、フランス（AFNOR)、ドイツ（DIN)、イタリア（UNI)、日本（JISC)、韓国（KATS)、オランダ（NEN)、ロシア（GOST R)、セルビア（ISS)、スイス（SNV)、アメリカ（ANSI)、イギリス（BSI)、ベトナム（TCVN）の 19 ケ国である。

NP 投票では 5 ケ国以上の賛成票が必要なことと、主要国の賛同は欠かせないことからアメリカ、ドイツ、ベルギー、オランダ（事務局)、イギリス、フランス、スイス（議長）の代表には個別に賛同依頼を送付した。

予備段階（PWI、Preliminary Work Item）
　　標準化項目の検討
提案段階（NP、New Work Item Proposal）
　　標準化範囲などを検討、NP 投票
作成段階（WD、Working Draft）
　　WD 作成
委員会段階（CD、Committee Draft）
　　委員会で審議し 3 ケ月の CD 投票。
照会段階（DIS、Draft International Standard）
　　DIS の登録と回付。5 ケ月の DIS 投票。

**図 付.2.4 標準化の段階**

**（出典：http://www.hido.or.jp/ITS/TS/TSF/4_iso.html）**

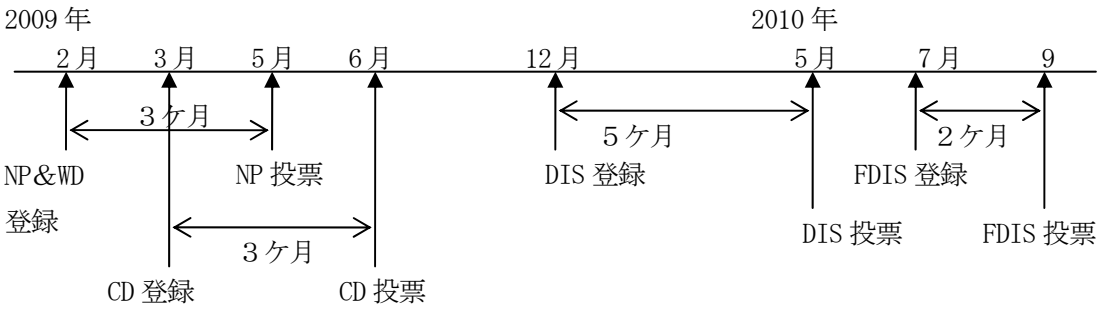



**図 付.2.5 TC154 における長期署名標準化スケジュール**

# 3. PDF 長期署名に関する国際標準化活動

## 3.1　PDF 長期署名の課題と WI 32000-2 の設定

アドビ社が開発した PDF 仕様には PDF1.6 から独自の署名仕様が含まれている。2007 年 1 月、PDF 仕様は国際標準化を狙ってアドビ社から AIM に移管された。署名仕様に関しては、ISO 32000-1 の原案となった PDF1.7 から CAdES/XAdES などの外部で定義された署名プラグインを組み込むことが可能になったが、実装の観点からは多くの課題が残されたままであった。具体的には、複数署名の方式、アーカイブタイムスタンプ付与時のタイムスタンプや検証情報の格納場所、署名プラグイン名の登録方法などが挙げられる。

これらの課題は、2006 年末から PDF/A（ISO19005-1、PDF の長期保存プロファイル仕様）の標準化を進めている ISO TC171 SC2 WG5 で認識され、署名問題を解決するチームを立ち上げようという動きにあった。その一方で、PDF1.7 仕様が TC171 事務局提案によりファストトラックで（つまり、仕様内容の審議なしで）ISO 化の投票にかけられた。投票の結果、CAdES の開発者であるデニス・ピンカス（AFNOR）から、独自署名仕様に問題があるとのとの理由で反対投票がなされ、2008 年 2 月に投票結果調整会議（Ballot Resolution Meeting）が開催された。長時間に亘る調整の結果、PDF1.7 仕様に一切手を加えないパート 1 と、独自署名仕様の CAdES/XAdES への置き換えやそのほかの機能拡張を行ったパート 2 とに分けることで合意され、2008 年 7 月に ISO 32000-1 が発行された。パート 2 については、WI 32000-2 として審議が始まったところである。

## 3.2　PDF 署名に関する ISO-ETSI 連携

パート 2 のための、CAdES/XAdES をベースとした PDF 署名仕様の開発は、PDF の標準化を行っている TC171 と CAdES/XAdES を開発した ETSI とが連携して原案を作成することになったことから（誰が音頭を取ったかは不明）ETSI 内に PDF 署名の専門家タスクフォース（STF）が設けられた。この STF は、ETSI 仕様としての PDF 署名仕様の開発と、ISO への提案を目的としている。STF のメンバは、ISO からはアドビ社のローゼンタール、ETSI からは CAdES 担当のニック・ポープ、XAdES 担当のジュアン・カルロスなどである。STF の議長は ETSI メンバでアドビ社のマーク・ストラットが務めている。なお、ETSI 仕様だけで漏れなく標準をカバーするために、前者には、既存の PDF 署名が含まれる。

STF における検討スケジュールは、次の通りである。

フェーズ 1　2008 年 12 月　PDF1.7 仕様互換の PDF 署名プロファイル

フェーズ 2　2009 年 6 月　CAdES/XAdES ベースの PDF 署名プロファイル

フェーズ 3　2010 年 6 月　視覚インタフェース仕様（visible signatures and interfaces）

ECOM は、先行して PDF の長期署名課題の検討を進めてきており（2006 年度報告書参照）、主要課題について検討結果を ETSI に入力し賛同を得た。以下にその概要を示す。

(1) 複数署名の方式

署名付き文書に対して署名を行う“従来の PDF 署名の方式”に限定するか、CAdES の複数署名（複数 SignerInfo、カウンタ署名）も可能にするかに関して、ECOM の結論として、CAdES 導入の狙いは、PDF の文化を尊重し且つ署名を長期にわたって検証できるようにすることであるから、従来の PDF 署名の方式に限定する（複数 SignerInfo、カウンタ署名は使わない）ことを提案した。

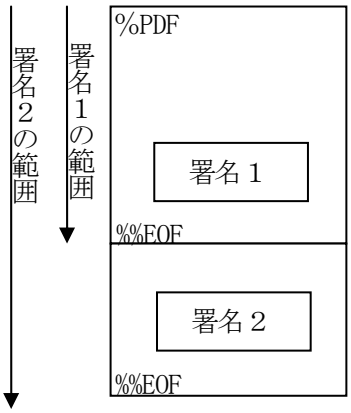



**図 付.3.1 従来の PDF 署名の方式**

(2) アーカイブタイムスタンプの格納

証明書、失効情報、アーカイブタイムスタンプの挿入によって、ハッシュ範囲を示すバイトレンジパラメタが正しい値を示さなくなる。予め大きな領域を確保しておくべきかについて、ECOM の結論として、何十年も先のサイズの予測は困難であり、更新された CAdES データは添付ファイルとして増分更新により付加することを提案した。

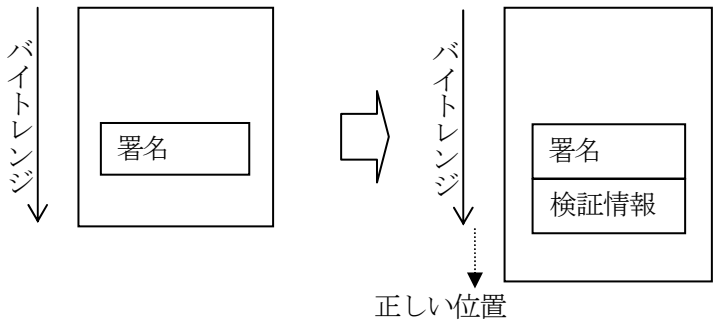



**図 付.3.2 バイトレンジが示すハッシュ範囲**

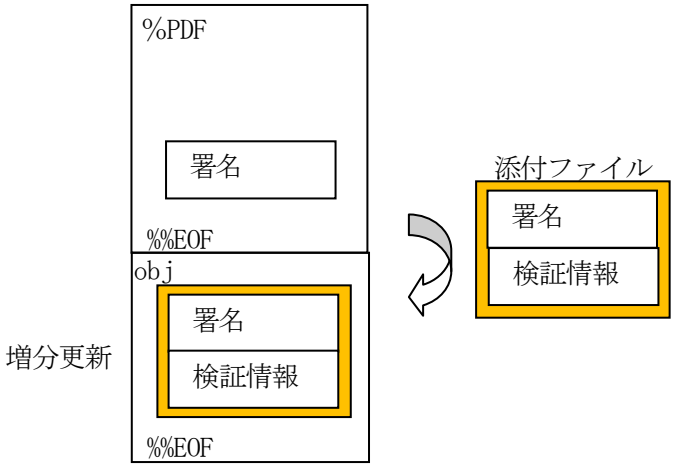



**図 付.3.3 添付ファイルによる解決案**

(3) 署名辞書と CAdES データのマッピング

複数の署名や複数世代のアーカイブタイムスタンプが存在する場合は、CAdES データと署名辞書との対応付けが必要となる。このため、各署名辞書に名前を付け CAdES データを格納する添付ファイル用辞書からこれを参照可能にすることを提案した。

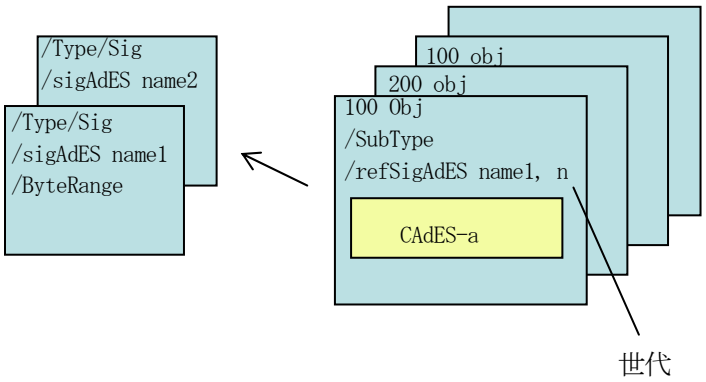



**図 付.3.4 署名辞書と CAdES データのマッピング**

(4) PDF 用署名のプロファイリングの考え方

ECOM では、PDF 用の署名仕様は CAdES、XAdES 両方を準備すべきか一方だけにすべきか、またそのプロファイルはどうあるべきかに関して議論してきた。その結論として、PDF 長期署名は CAdES だけにすべきであり、プロファイルとしては、署名を長期に亘って検証できるようにするという目的から CAdES-T と CAdES-A の両方を定義し、オプショナル要素は極力制限すべきであるとの提案を行った。本章の末尾に ETSI に提案した PDF 用プロファイルを載せる。

## 3.3　TC171 北京会議と今後のスケジュール

| | |
|---|---|
| 表題 | ISO TC171/SC2/WG8 |
| 場所 | 中華人民共和国 / 北京　友誼賓館会議棟 |
| 日時 | 2008 年 10 月 27 日（月）～9 月 29 日（水） |
| 参加者 | 米国、英国、ドイツ、日本、中国など 16 名 |
| 議題概要 | ・WI 32000-2 審議 |

WG8 は、DIS32000 投票後の投票解決調整会議に伴って設立され、議題項目は WI32000-2 に対する拡張機能である。議長はアドビのプロダクトマネージャの Nora Calvillo、WG の技術顧問は PDF の考案者である同じくアドビの Jim King である。参加者の内訳は、米国、英国、ドイツ、日本、中国などの各国、及び ISO 事務局であった。中国はホスト役であったこともあり 5 名が参加していた。米国、英国、ドイツから拡張機能の提案があり、特に米国からは 100 ページを超える寄書が提出され多数の拡張機能提案があった。

署名に関しては、P エントリ、LockDocument エントリ、AppearanceFilter エントリのカテゴリ見直しが提案された。特に反対意見は出なかった。

> 備考：P” エントリは、署名文書に対する変更を制限し変更を一切認めず、フォーム入力のみ認める、フォーム入力に加えて注釈の作成・削除・変更を認める、を選択可能にする。このエントリはオプショナルで、エントリ無し（デフォルト）は従来どおり。

その他、署名とは直接関係ないが米国から AES256 及び UNICODE ベースパスワードアルゴリズムの追加提案があり、反対意見は特になかった。

会議中に、PDF の互換性・規格適合性とは何かについて何度も議論が繰り返された。結局、どのビュアでも同じに見えるようにすること（つまり、ビュアを通して見える結果が基準である）ということで落着した。

この会議では、ETSI の STF の検討結果を反映した提案はなかったが、この会議のエディタであり STF メンバのローゼンタールによると、2009 年 4 月にドイツで開催される TC171/SC2/WG8 にインプットされる見通しとのことであった。また、署名ポリシに関しては日本からの提案を期待しているとのことであった。

参考　ETSI に提案した PDF 署名のプロファイル案

M：例外なく実装が要求される

O：任意

X：特段の理由がない限り実装すべきではない

CAdES-T

| SignedData | Required level |
|---|---|
| CMSVersion | M |
| DigestAlgorithmIdentifiers | M |
| EncapsulatedContentInfo | M |
| eContentType | M |
| eContent | - |
| CertificateSet (Certificates) | O |
| Certificate | O |
| AttributeCertificateV2 | X |
| OtherCertificateFormat | X |
| RevocationInfoChoices (crls) | O |
| CertificateList | O |
| OtherRevocationInfoFormat | X |
| SignerInfos | M |
| single | M |
| parallel | X |

| SignerInfo | Required level |
|---|---|
| CMSVersion | M |
| SignerIdentifier | M |
| IssuerAndSerialNumber | M |
| SubjectKeyIdentifier | M |
| DigestAlgorithmIdentifier | M |
| SignedAttributes | M |
| SignatureAlgorithmIdentifier | M |
| SignatureValue | M |
| UnsignedAttributes | M |

| SignedAttributes | Required level |
|---|---|
| ContentType | M |
| MessageDigest | M |
| SigningCertificateReference | M |
| ESS SigningCertificate | O |
| ESS SigningCertificate v2 | M |
| OtherSigningCertificate | X |
| SignaturePolicyIdentifier | O |
| SigningTime | O |
| ContentReference | X |

| | |
|---|---|
| ContentIdentifier | X |
| ContentHints | X |
| CommitmentTypeIndication | X |
| SignerLocation | X |
| SignerAttribute | X |
| ContentTomestamp | X |

| UnsignedAttributes | Required level |
|---|---|
| CounterSignature | X |
| *Trusted signing time* | M |
| SignatureTimeStamp | M |
| *Time Mark etc.* | X |
| CompleteCertificateReferences | O |
| CompleteRevocationReferences | O |
| CompleteRevRefs CRL | M |
| CompleteRevRefs OCSP | M |
| OtherRevRefs | X |
| Attribute certificate references | X |
| Attribute revocation references | X |
| CertificateValues | O |
| CertificateValues | M |
| *Storage of the certificate by CA* | O |
| RevocationValues | O |
| CertificateList | M |
| BasicOCSPResponse | M |
| OtherRevVals | X |
| *Storage of the revocation Info by CA* | O |
| CAdES-C-timestamp | X |
| Time-stamped cert and crls reference | X |
| *Archiving* | X |
| ArchiveTimestamp | X |
| ArchiveTimestamp v2 | M |

CAdES-A

| SignedData | Required level |
|---|---|
| CMSVersion | M |
| DigestAlgorithmIdentifiers | M |
| EncapsulatedContentInfo | M |
| eContentType | M |
| eContent | - |
| CertificateSet (Certificates) | O |
| Certificate | O |
| AttributeCertificateV2 | X |
| OtherCertificateFormat | X |

| | |
|---|---|
| RevocationInfoChoices (crls) | O |
| CertificateList | O |
| OtherRevocationInfoFormat | X |
| SignerInfos | M |
| single | M |
| parallel | X |

| SignerInfo | Required level |
|---|---|
| CMSVersion | M |
| SignerIdentifier | M |
| IssuerAndSerialNumber | M |
| SubjectKeyIdentifier | M |
| DigestAlgorithmIdentifier | M |
| SignedAttributes | M |
| SignatureAlgorithmIdentifier | M |
| SignatureValue | M |
| UnsignedAttributes | M |

| SignedAttributes | Required level |
|---|---|
| ContentType | M |
| MessageDigest | M |
| SigningCertificateReference | M |
| ESS SigningCertificate | O |
| ESS SigningCertificate v2 | M |
| OtherSigningCertificate | X |
| SignaturePolicyIdentifier | O |
| SigningTime | O |
| ContentReference | X |
| ContentIdentifier | X |
| ContentHints | X |
| CommitmentTypeIndication | X |
| SignerLocation | X |
| SignerAttribute | X |
| ContentTomestamp | X |

| UnsignedAttributes | Required level |
|---|---|
| CounterSignature | X |
| *Trusted signing time* | M |
| SignatureTimeStamp | M |
| *Time Mark etc.* | X |
| CompleteCertificateReferences | M |
| CompleteRevocationReferences | M |
| CompleteRevRefs CRL | M |
| CompleteRevRefs OCSP | M |
| OtherRevRefs | X |

| | |
|---|---|
| Attribute certificate references | X |
| Attribute revocation references | X |
| CertificateValues | M |
| CertificateValues | M |
| *Storage of the certificate by CA* | O |
| RevocationValues | M |
| CertificateList | M |
| BasicOCSPResponse | M |
| OtherRevVals | X |
| *Storage of the revocation Info by CA* | O |
| CAdES-C-timestamp | X |
| Time-stamped cert and crls reference | X |
| *Archiving* | M |
| ArchiveTimestamp | X |
| ArchiveTimestamp v2 | M |

# 4. その他の国際標準化活動

ECOM は、定期的に欧州通信規格協会（ETSI）の電子署名基盤技術委員会（TC ESI）のアソシエートメンバーとなっている。本節では署名普及 WG の参加した会議の報告を行う。

## 4.1 ETSI ESI#20 Meeting, Sofia Antiplice

| | |
|---|---|
| 表題 | ETSI ESI#20 Meeting, Sofia Antipolice |
| 場所 | フランス ソフィアアンチポリス ETSI 本部 |
| 日時 | 2008 年 6 月 24 日 9:00 ～ 2008 年 6 月 25 日 17:00 |
| 参加者 | NEC 木村、ECOM 前田、エントラスト 漆嶌 |
| 議題概要 | ・STF 318 Registered E-Mail (REM) の状況報告<br>・STF 351 ETSI Remote XAdES/CAdES Plugtest の状況報告<br>・XAdES と CAdES の整合性と仕様改定について<br>・ISO 32000-1 PDF 1.7 での CAdES・XAdES の利用のための新 STF<br>・長期署名プロファイルの ECOM 提案の説明 |

PDF の CAdES 利用については、今回初めて米 Adobe より PDF 署名の設計のコアメンバが ESI 会議に参加し、ISO TC 171 と ETSI ESI のメンバが協調した新しい STF（専門家技術部会）を立ち上げることとなった。NEC 木村氏が AdES と PDF との増分更新による AdES 署名付与方法を紹介し好意的な意見を得た。

Julien Stern 氏から XAdES および CAdES において、現状認識されている仕様上の問題点、課題をまとめている。どのように解決するかについては、Stern 氏が情報共有サイトを立ち上げ、その上で今後有識者（有識者メンバ：Nick Pope, Denis Pinkas, Juan Carlos Cruellas, 漆嶌賢二, Julien Stern）がディスカッションすることとなった。

また､NEC 木村氏は ECOM の提案による長期署名フォーマットの汎用プロファイルの説明を行い、特に異論がなければこれを日本から ISO 提案する予定であることを説明した。

## 4.2 ETSI ESI#21 Meeting, London

| | |
|---|---|
| 表題 | ETSI ESI#21 Meeting, London |
| 場所 | イギリス ロンドン Adobe London Regents Park |
| 日時 | 2008年9月24日 9:00 ～ 2008年9月25日 17:00 |
| 参加者 | NEC 木村 |
| 議題概要 | ・PDF署名<br>・ETSI Plugtest<br>・CAdES仕様改訂<br>・証明書パス構築・検証<br>・次期会期の議長、副議長選出 |

PDF署名に関して、STF364（Advanced Electronic Signatures for PDF）リーダのMarc Straatから検討状況の報告があった。STF活動を3フェーズに分け、フェーズ1（～2008/12）は現状のPDF署名の範囲、フェーズ2（～2009/6）はCAdES、XAdESによる長期署名、フェーズ3（～2010/6）は可視表現の仕様化を行う。また、CAdES、XAdESの棲み分けは、従来のPDF文書に対してはCAdES、XFAやFormsに対してはXAdESを適用し、フェーズ1は、2008年11月10日に最初のドラフトが回覧されることが報告された。報告に対して、Denis PinkasからPDFには署名ポリシが必要との意見が出されたが、意図が十分には伝わらず議論には至らなかった。

Plugtestに関しては、STF351リーダのJuan Carlos Cruellasから実施状況の報告があった。この中で、テスト環境整備に関してECOMからの多大な協力があったとの感謝の言葉があった。今回のPlugtestで挙げられた問題点は、XAdESの次の版に反映させる予定であるとの説明があった。また、8月18日に東京で開催されたECOM-ETSIワークショップの内容について報告があり、今後も度々このようなワークショップを開催したいこと、また、ECOMのPlugtestのWebサイトを引き合いに出し、ETSIのPlugtestもこのようなサイトを提供したらどうかとの提案があった。

Peter Ryber等から出されCAdES仕様の問題指摘に対しては、Julien Sternから改訂案の説明が行われたが、CAdESの著者であるDenis Pinkasから、後方互換性のない更新はすべきでないこと、どの属性にどの検証情報を入れるか明記していないのは、それらの検証情報をそこに入れるべきではなく、別に保管すべきものと考えているとの発言があった。本件は別途議論することとなった。また、Peter Ryberから証明書パス構築・検証に関する詳細規定の提案があり、MLで検討することとなった。この仕様に関しては賛否両論があることから、ESI#22でETSI仕様とするか否かを審議し、ETSI仕様とする場合は来年3月を目標とすることになった。

任期切れに伴うESIの議長、副議長の選出は、それぞれRiccardo GenghiniおよびErnst Giessmannが再選された。任期は2009年～2010年の2年間である。

## 4.3 ETSI ESI#22 Meeting, Bilbao

| | |
|---|---|
| 表題 | ETSI ESI#22 Meeting, Bilbao |
| 場所 | スペイン ビルバオ　Hotel Izenpe Hesperia Zubialde |
| 日時 | 2008年11月25日 9:00 ～ 2008年11月26日 17:00 |
| 参加者 | ECOM 前田陽二 |
| 議題概要 | ・STF 318 Registered E-Mail (REM) の今後の計画について紹介<br>・STF 351 ETSI Remote XAdES/CAdES Plugtestの9月に行ったXAdESのプラグテストの報告と2月に行うXAdES/CAdESの計画紹介<br>・ISO 32000-1 PDF 1.7でのCAdES・XAdESの利用のためのTS案の紹介<br>・ここ10年に行われた電子署名関連の標準化活動の紹介と今後の標準化テーマの紹介 |

参加者はRiccardo Genghini議長他22名であり、ECOMからは前田が参加した。

STF 351 (Interoperability framework for XML Advanced Electronic Signatures (XAdES) Specialist Task Force) が2008年9月に実施したXAdES (XML Advanced Electronic Signatures) のプラグテストの報告書について、ETSI事務局のPéter Krémer氏より説明が行われた。また、2009 年 2 月に予定されている XAdES 及び CAdES (Cryptographic Message Syntax Advanced Electronic Signatures) のプラグテストに向けた計画の報告があった。

今後の進め方については以下についての質問があった。

- 参加者へのテスト結果等の情報のフィードバック方法
- 実験結果のXAdESへのフィードバック

事務局からは踏み込んだ回答はなかった。

CAdES フォーマットの現状の問題点の列挙と改訂については、会議の前にメールベースで討論を行いECOMからも問題提議を行ったが、今回の会議の席上では議論の進展は無かった。

# 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 |
| 副主査 | 溝上　卓也 | 日立ソフトウェアエンジニアリング株式会社 |
| 幹　事 | 佐藤　雅史 | セコム株式会社 |
| 幹　事 | 政本　廣志 | 日本電信電話株式会社 |
| 委　員 | 高尾美由紀 | みずほ情報総研株式会社 |
| 委　員 | 橋本　正一 | 日本電信電話株式会社 |
| 委　員 | 宮地　直人 | 有限会社ラング･エッジ |
| オブザーバ | 西川　康男 | ARMA JAPAN |

メンバ（五十音順）（上記以外）

| 役　割 | 氏　名 | 所　属 |
|---|---|---|
| 幹　事 | 後藤　　淳 | 日本電気株式会社 |
| 委　員 | 戸田　安彦 | 株式会社NTTデータ |
| 委　員 | 勝岡　義博 | 株式会社NTTデータ |
| 委　員 | 保倉　　豊 | グローバルフレンドシップ株式会社 |
| 委　員 | 川城　三治 | グローバルフレンドシップ株式会社 |
| 委　員 | 上畑　正和 | セイコーインスツル株式会社 |
| 委　員 | 和田　宗樹 | 株式会社帝国データバンク |
| 委　員 | 石原　達也 | 東芝ソリューション株式会社 |
| 委　員 | 今井　秀和 | 株式会社PFU |
| 委　員 | 小池　正通 | 富士ゼロックス株式会社 |
| 委　員 | 三原　　真 | 富士ゼロックス株式会社 |
| 委　員 | 松山　博美 | 富士通株式会社 |
| 委　員 | 田村　雅之 | 三菱電機株式会社 |
| 委　員 | 中村　克己 | 三菱電機情報ネットワーク株式会社 |
| オブザーバ | 高塚　　肇 | NTTソフトウェア株式会社 |

電子署名普及に関する活動報告 2008

平成 21 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
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