電子署名普及に関する活動報告2009

平成22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 21 年度は、これらの成果を踏まえ次の調査検討を行った。

・ 官民連携サービス基盤の検討として、2003 年に作成された「2010 年の市民生活」を踏まえて現状の課題点の整理と今後の展開に向けた提言を行った。また、将来の基盤として必須である「国民 ID」の管理についての検討を行った。

・ 昨年度に引き続き、文書管理に関するアンケート調査を ECOM 会員企業を対象に行い、分析を行った。

・ 文書の長期保存について、PDF 長期署名の調査、署名ポリシー、証明書のビジブル化の検討などを行うとともに、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についても課題を収集し整理した。

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 22 年 3 月

次世代電子商取引推進協議会

目　次

序文

第1部　社会を活性化する官民連携サービス基盤 1

1.　はじめに 3

2.　「2010年の市民生活」と社会基盤 4

2.1　2003年の想定と2010年の現実 4
2.2　社会基盤と電子署名および証明書 10

3.　デジタル社会の官民連携サービス 14

3.1　官民連携サービスへの要求 14
3.1.1　行政サービスのパラダイムシフト 14
3.1.2　官民連携サービスの基本的な考え方 15
3.1.3　社会基盤としてのID管理と個人の属性の扱い 16
3.2　官民連携サービスのための基盤のあり方 17
3.2.1　官民連携サービスのための基盤への要求 17
3.2.2　オーストリアの電子政府法における識別の考え方 19
3.2.3　エストニアの電子政府におけるデータ連携の基盤 20
3.2.4　官民連携サービスの基盤のためのいくつかの考察 23

4.　国民IDに関する整理と提案 25

4.1　IT推進方針の必要性 25
4.2　国民ID導入に関する課題の整理 27
4.3　国民ID管理方式の整理 28
4.4　LINK MODELの導入検討 30
4.4.1　秘密分散技術とは 30
4.4.2　秘密分散技術を用いたID連携テーブル 31
4.5　今後の検討課題 34

第2部　電子文書管理 35

1.　紙・電子文書管理の実態調査結果の概要 37

1.1　調査方法、調査期間 37
1.2　質問内容 37
1.3　回収実績と業種 37

1.4　アンケート結果サマリー……38
1.4.1　全社に関する質問……39
1.4.2　「JSOX 文書」に関する質問……39
1.4.3　「IT インフラ一般」に関する質問……40
1.5　アンケート結果から見る電子文書管理拡大への課題についての考察……40

2.　H21 年度　紙・電子文書管理の実態調査結果の詳細……41

2.1　全社に関する質問……41
2.2　JSOX への取組みについての質問……46
2.3　全社一般についての質問……58

第 3 部　電子署名普及のための標準化提案……61

1.　長期署名プロファイル JIS 改定案……63

1.1　証拠記録の JIS への追加案……63
1.2　その他の JIS 改定案……63

2.　長期署名プロファイル ISO 標準化活動の進捗状況……64

3.　関連技術の標準化動向……65

3.1　PAdES（PDF 長期署名）の概要、経緯、動向……65
3.1.1　PDF 長期署名の経緯と動向……65
3.1.2　PAdES 概要……66
3.1.3　PAdES 仕様概要……69
3.1.4　おわりに……83
3.2　証明書や署名のビジュアル化……83
3.3　暗号アルゴリズムの安全適合性ポリシ……84

4.　電子記録の長期管理ガイドライン……86

4.1　背景……86
4.2　電子記録マネジメント……86
4.3　記録に関するマネジメントシステム標準の動向……89
4.4　電子記録マネジメントコンソーシアム……90

メンバリスト……92

第１部　社会を活性化する官民連携サービス基盤

1. はじめに

電子社会、ネット社会への展望が開けてきた 2000 年前後に、各国で相次いで電子署名法が制定され、電子社会の基盤を整える動きが始まった。日本も先進的な動きをした国の 1 つであった。

その後、ヨーロッパでは、エストニア、オーストリアをはじめ、eID と電子証明書を導入し、電子署名を利活用している国が増えている。アジアでも、韓国のように、およそ 2000 万人が電子証明書を持ち、電子署名を使える環境が整備されている国もある。しかし、日本ではそれ以降、必ずしも普及したといえる状況にはなく、電子署名が電子社会、ネット社会の活性化に貢献しているとは言い難い。

その原因について、基盤整備の問題、法や制度の不備（あるいは不徹底、不十分）が議論されているが、官・民のサービスにおけるベストプラクティスが示されていないことも課題であろう。そして、電子署名や証明書の利用シーンが広がっていくには、利用者、サービス提供者、経営者のそれぞれの視点でこれらの使い方と意義が正しく理解される（決して仕組みの理解ではない）必要があるが、現状十分ではないと思われる。具体的には、電子証明書は単なるパスワードの代替手段であるというような認識が一般的と思われるのはその一例である。そのような状況を払拭しつつ、電子社会、ネット社会のサービスを支える基盤のあり方を考えていく必要がある。昨年、パスポートの不正取得が急増したというニュースがあった。これは旅行会社による代理申請時の確認の甘さを悪用するもので、官民のサービス連携ができていれば防げたことかもしれない。

ID 管理に基づく官の基盤については、欧州の事例を中心に昨年度報告した。今年度は、民間分野、官民連携サービスにおける基盤について考察する。2 章では、電子社会を支える社会基盤の現状について、電子署名等の基盤整備が始まったころの展望と比較しながら、電子化の社会基盤が確立していない状況の原因を考えてみる。3 章では、その現状を踏まえながら、本来の、官民連携を実現する社会基盤のあり方について述べる。4 章では、そのような社会基盤の中核でもある ID 管理基盤の実現方式に関して、一つの案を提起する。

2. 「2010 年の市民生活」と社会基盤

2003 年ごろ、インターネットは社会の通信基盤として定着し、デジタル情報の信頼性確保と本人確認のために、PKI 基盤の構築が進められようとしていた。さらに情報ネットワーク社会が進むと、各サービスの中で、本人性だけでなく、役割や権限を示す属性情報も必要になり、個人の属性情報を安心して登録し、利用できる仕組みの必要性が予想された。

ECOM では H15 年度（2003 年度）報告書『属性情報利用システム　－2010 年の市民生活－』で、2010 年の社会のあるべき姿として、属性情報を活用し、インターネットを利用したさまざまな市民活動のイメージを描き、それを支える基盤として、表 1.2.1 のような「市民社会基盤」を想定した。当時の想像と、ちょうど 2010 年を迎えた今日との差異から、電子社会、ネットワーク社会の基盤の実現性と課題について考えてみる。

表 1.2.1 「2010 年の市民生活」で想定した市民社会基盤（H15 年度報告より）

2010 年の市民社会基盤	具体例
レイヤー1 「属性登録基盤」	証明写真登録局
	団体内権限登録局
レイヤー2 「属性活用共通基盤」	個人属性保証基盤
	システムアクセス権限判別基盤
	公的メールボックス基盤
	匿名電子投票基盤
	ネット行動保証基盤
	本人確認受渡基盤
レイヤー3 「応用サービス」	電子投票・アンケートサービス
	属性提供サービス
	公的電子連絡サービス
	ネット評価・格付け
	ネット試験
	ネット教育

2.1　2003 年の想定と 2010 年の現実

H15 年度（2003 年度）の報告書では、2003 年時点の市民生活における各種手続きの現状と、2010 年のインターネット利用サービスのイメージを想定している。（表中の番号は報告書で記載されている章節項の番号である。6 つの分野に分類し、順序を適宜入れ替えている。）

この 6 つの分野が社会の全体をカバーしているとは限らないが、基盤の状況の変化を推測するケーススタディと考え、今回、H15 年度報告書に対応する形で 2010 年の現状を記述し、その差異

の状況について考察する。

(1) 生活（ライフイベント）

H15 年度報告では、ライフイベントのうち特に出産・育児・結婚を中心に取り上げている。

H15 年度 ECOM 報告		2010 年の現実
2003 年の市民社会基盤	2010 年の市民生活	
2.2.9 出産～保育 ・妊娠届 ・職場休職（育児休業） ・出産 ・保育園入園～職場復帰	1.1.1 「働く母親」支援ポータルサイト ・保育園の空き情報連絡 ・保育園申し込み代行 ・保育園の評価付け ・お迎え代行 ・食材配達	［到達度］：× ・子供手当てなど補助充実化の動きはあるが、インフラ整備面の動きは鈍い ・保育園の空き情報を Web で公開するなど一部サービスは始まっているが、自治体ごとにサービスレベルが異なっている ・出産から保育園手続き、職場復帰の手続きに連携の動きは見られない
（記載なし）	1.1.2 電子自治体と公的メールボックス ・ネットで出生届け ・公的メールボックスに確認メール ・訂正申請	［到達度］：× ・一部の申請以外の電子化は進展していない（大多数の手続きは窓口に行く必要あり） ・「次世代の電子行政サービス基盤の標準モデル※1」でワンストップサービスを目指そうとしている ・公的メールボックスは現在未達成。（国民電子私書箱構想※2で触れられた程度）
2.2.8 結婚 ・結婚相談所入会 ・結婚 ・結婚（引越し含む）手続き	1.1.8 ネットで知り合う ・身分証明ができる出会い系サイト ・属性保証基盤、本人認証システム ・個人情報も交換できる信頼性	［到達度］：△（民間ベースで信頼性の低いサービス） ・SNS などで厳密ではないが類似のサービスが存在。ただしトラブルも多い。 ・結婚相談所では、免許証等でオフラインにより本人確認（さらに独身証明、収入証明も別途行う場合も）が行われるが、出会い系はネットが中心で本人確認なし、メールアドレスのみ

■『働く母親』支援ポータルサイト

少子高齢化による労働人口減少等の背景から、「働く母親」の労働環境の改善には、高い社会的要請が寄せられているところであり、オンデマンドにかつ柔軟な支援を実現するための仕組みが求められている。その実現には、企業、行政、病院等による横断的な連携が必要であり、官民共通の認証基盤、社会基盤を必要とするところであるが、行政は依然としてサービス創出よりも認可業務中心の対応に終始し、「働く母親」の支援実現に対する一貫したビジョンがみえてこない。子供手当てや、高校授業料無料化などの子育て支援が進みつつあるが、企業内保育所の義務化や、幼保一体化などの大胆な施策が必要との意見がある。

■電子自治体と公的メールボックス

行政サービスの効率化や利便性向上の目的から、電子的な社会基盤の中核として電子自治体の実現は長い間求められ続けているところであり、各省庁で様々な検討や実証実験が行われ、また一部の先進的な自治体で各種サービスの電子化が試みられてきたものの、全国的な大きな流れにつながっていない。省庁を横断した推進機関がない、あるいはうまく機能してこなかったことや、国民感情として、電子化による情報漏えいやプライバシ保護に対する懸念が十分に払拭されてい

※1 http://www.kantei.go.jp/jp/singi/it2/nextg/pdf/granddesign.pdf　などを参照
※2 http://www.kantei.go.jp/jp/singi/it2/epo-box2/houkoku1.pdf　などを参照

ないことによる世論の盛り上がりの欠如などを原因として挙げる声がある。

■ネットで知り合う

「出会い系」、「婚活」などのサービスがネット上で広く展開されている。現状のネット上のサービスでは、本人確認に対する厳密な保証の根拠が乏しく、またそこまでのニーズもない。ただし、個人情報や本人確認をめぐるトラブルは多く報告されており、個人情報の管理基準や、ガイドラインの整備を求める声がある（開示レベルや、それに付随するメリット、デメリット、補償策など)。

(2) 申請・申告

H15 年度報告では、海外旅行と確定申告が取り上げられている。

H15 年度 ECOM 報告		2010 年の現実
2003 年の市民社会基盤	2010 年の市民生活	
2.2.1 海外旅行 ・パスポート申請 ・ビザ ・国際予防接種 ・国外運転免許 ・国際学生証 ・海外旅行保険	1.1.3 海外旅行申請サイト ・住民 IC カードで会員登録 ・鍵チケットで確認 ・証明センター（写真の転送） ・本人確認受け渡し認定	［到達度］：× ・パスポートの電子申請サービスは実現された（住基ネットにより、住民票の写しが不要となった）ものの、その後、利用率の低迷を理由に廃止 ・旅行会社では本人確認なしか、パスポートを確認（申請が電子化されていないので、本人確認不要。）
2.2.4 確定申告 ・医療費控除 ・住宅ローン控除 ・サイドビジネスの申告	（記載なし）	［到達度］：△（一部） ・e-Tax が開始され、徐々に利用者が増えているがまだ広く普及しているとはいえない。(公的個人認証サービス利用の敷居が高い・・・手数料、証明書入手・設定の煩雑さなど)

■海外旅行申請サイト

パスポートの電子申請サービスの停止理由となった利用率低迷の原因として、電子化や住基ネットの利用が手段でなく目的化されてしまい、使い勝手や利用条件のハードルの高さ、行政サービス間の連携等について、十分な考慮が行われたかの検証が必要。

■確定申告

H15 年度報告書では 2010 年の姿は描かれていないが、H16 年より国税電子申告・納税システム e-Tax がサービス開始されている。税額控除の特典により利用率の向上が見られるものの、本特典が 1 回限りの施策であることや、申請部分のみが電子化されているのみで、医療費控除や住宅ローン控除等のための申告額算出の過程においては、依然として行政サービス間の連携はできておらず、さらなる利用率の向上とその定着に向けた課題を指摘する声がある。

(3) 社会参加

H15 年度報告では、投票を中心に取り上げられている。

H15 年度 ECOM 報告		2010 年の現実
2003 年の市民社会基盤	2010 年の市民生活	
2.2.2 住民投票 ・住民投票条例の請求 ・投票 ・開票	1.1.4 地方政治参加 ・地方議会の住民参加議案採決システム ・インターネットで議会中継 ・ネット投票（匿名投票）	［到達度］：△（一部） ・電磁記録投票法（条例を定めた自治体で行われる地方選挙に限定）施行 ・一部自治体にて投票所での電子投票機による電子投票を実施 ・インターネットによる議会中継は実現
（記載なし）	1.1.12 アンケート、住民投票 ・電子投票システム ・匿名投票 ・各家庭にブロードバンド環境 ・投票用共同端末 （マンション組合、企業内評価用など）	［到達度］：△～○ ・ブロードバンド環境の普及、ポイント付与などを使ったネットアンケートサービス（企業利用がほとんど）の提供などは進展しているが、電子投票システムはほとんど普及していない ・02 年の区分所有法改正に伴い、マンション管理組合は、パソコンやインターネットを利用した電磁的方法により、議決権の行使や、規約・議事録の作成、保管などが可能になった

■地方政治参加

選挙については、開票作業の迅速化や実施コストが時として課題に挙げられることはあるものの、不在者投票制度の充実等により、必ずしもネットや電子投票の実現を要請する声は高まっておらず、また、これを推進する母体も見えていない。その実現に向けては、極めて高い本人確認や情報保護のための基盤が求められることから、基盤となるサービスの継続的な信頼感、安定感の醸成も求められる。

■アンケート、住民投票

ブロードバンド環境の普及もあり、ネットを通じて、マンション組合における住民や、企業における顧客の意見や評価をタイムリーかつ低コストに収集し、施策や商品作りに反映させようという活動は、広く行われるようになっている。上記の選挙と比べて、厳密な本人確認は必ずしも必要ではないところも普及の要因であるとの声がある。

(4) 起業・ビジネス

H15 年度報告では、NPO や会社の設立が取り上げられている。

H15 年度 ECOM 報告		2010 年の現実
2003 年の市民社会基盤	2010 年の市民生活	
2.2.6 NPO 設立 ・認証手続き ・登記手続き ・設立届出	1.1.5 NPO 設立 ・団体への評価システム（第三者評価組織） ・ネット申込み	［到達度］：△（一部） ・内閣府の電子申請システムで申請 ・法人の登記申請等は印紙税削減目的にて利用拡大 ・評価システムは見当たらないが、必要性は認識
2.2.5 店舗開業 ・開業手続き ・青色申告申請 ・税務申告	1.1.8 店舗開業、会社設立の手続き ・公的ポータルサイトから書式ダウンロード ・身分証を添えて送信（代行送信） ・許認可の申請	［到達度］：△（一部） ・各種申請や e-Tax による税務申告などが一部電子化されている

■NPO 設立、店舗開業、会社設立の手続き

特別に電子化することのメリットは見いだせない状況であり、基盤サービス構築につながる特

別な動きはない。

(5) 消費活動

H15 年度報告では、車の購入とネットショッピングが取り上げられており、ネットによる消費活動と分類した。

H15 年度 ECOM 報告		2010 年の現実
2003 年の市民社会基盤	2010 年の市民生活	
2.2.3 自動車購入 ・運転免許取得 ・車庫証明取得 ・新規登録	1.1.6 ネットで購入 ・自動車の販売サイト ・メーカの違いを越えて検索 ・ネットで注文	[到達度]：△（かなり実現しているが連携は未） ・ネットでの購入サービスは実現。 ・自動車保有関係手続のワンストップサービスも提供されているが普及はまだ（使い勝手には難）
2.2.10 電子商取引（開業～取引） ・ネットショッピング	（記載なし）	[到達度]：○（ただし、信頼性は低い？） ・電子消費者契約法（2001 年）等の後押しもあり、ネットショッピング等のオンライン取引は順調に増加 ・本人確認などの問題は、ネットのみではなく、電話やFAX、郵便等でも問題を抱えており必ずしもネットに特化した問題ではない ・信頼度レベル（どうすれば安全なのか）の検討は不十分

■ネットで購入

自動車のような高額な商品についてもネットで売買されることが特別なことではなくなっている。ただし、依然として消費活動にかかわるトラブルは多数発生しており、自動車保有関連の手続きに代表されるような消費活動と行政サービスとを連携させた利便性向上を推進する動きも弱く、新設された消費者庁が推進役となりうるのでは？との期待もある。

■電子商取引（開業～取引）

2010 年の姿は描かれていないが、ブロードバンドの普及や、利便性の向上により、ネットショッピングやネットオークション等はすでに市民生活に深く入り込んでいる状況であるといえる。しかしながら、当初より課題とされている本人確認手段は、その多くがパスワードレベルの認証を利用するにとどまっており、それによるリスクは、消費者あるいはサービス提供者（企業等）が一定量を受容することで成り立っている状況であるといえる。厳密な本人認証は必要とされてはいるものの、電子商取引においては、費用対効果が厳しく問われるところであり、本人認証手段も例外ではなく､安心して電子商取引を利用可能となる低コストは認証手段が求められている。

(6) 教育・試験

H15 年度報告では、運転免許と大学教育関連が取り上げられている。

H15 年度 ECOM 報告		2010 年の現実
2003 年の市民社会基盤	2010 年の市民生活	
（記載なし）	1.1.7 運転免許試験 ・ネットで受験 ・本人確認受け渡し	[到達度]：×（ほとんどナシ） ・運転免許ではないが、試験会場にてコンピュータ（ネット）で受験する形態の資格試験はいくつか存在（漢検など）するものの普及には至らず。

H15 年度 ECOM 報告		2010 年の現実
2003 年の市民社会基盤	2010 年の市民生活	
（記載なし）	1.1.10 大学の検索・選択 ・IC カード認証（生徒の証明） ・評価機関の評価（学生/企業から大学の評価、教官の評価）	［到達度］：△（一部） ・IC カード（学生証）を利用して、証明書による認証や教室への入退室、生協との連携などを実現している事例あり ・評価の収集は行われているところもあるが方式は不明
2.2.7 大学入学～留学 ・入学試験 ・入学手続き ・奨学金 ・奨学金（留学関係） ・留学（渡航）	1.1.11 遠隔教育と単位交換 ・連携大学間単位交換制度 ・遠隔授業、e-ラーニング（海外含む）	［到達度］：△ ・一部大学による講義のネット公開、遠隔授業、単位交換などを実現している例あり（厳密に本人確認できているかは不明） ・単位交換制度、e-ラーニングも海外や社会人大学を中心に普及してきている（内容もより充実）

■運転免許試験

入学試験や各種資格試験等における申込みのネット化は普及している．しかしながら、本人確認の電子的基盤がないため、本人確認は、基本的に会場における写真と公的書類による確認が主となっている。

■大学の検索・選択

一部の先進的な大学おいては、IC カード学生証などを本人確認の核として積極的に活用する取り組みが行われているものの、全体としては、大学における IT 化は進んでいない（コストの問題か）。評価については、ネットを通じて効率的かつ匿名性を確保しながら収集する取り組みが一部で見られるものの、公平な基準作りが難しいという課題の声がある。

■遠隔教育と単位交換

一部の大学では、講義のネット公開や遠隔授業およびそれによる単位交換などが実施されている例があるが、そこでの本人確認の精度は、ある程度の割り切りをもって推進されているものと考えられる。

(7) まとめ

以上、6 つのカテゴリで 2003 年度に想定した 2010 年における市民生活像と現実との差異について比較、分析を行った。

所感としては、行政系については、電子署名・証明書の基盤が部分的に導入されつつあるが、サービス間の連携には取り組めていない状況であり、民間系については、サービスとしてニーズのあるところは電子化、ネット化が進んでいるが、本人確認の厳密性や安全性は軽視、あるいはサービス上受容しなければならないリスクとして扱われている状況と言える。例えば、サービスとしては 2003 年時点では予想されなかったもの（YouTube や Twitter など）が出現し、民間のみならず、場合によっては行政も利用する一種の基盤となってきているが、あくまでも厳密な本人確認を必要としない分野だからとも言えるであろう。

2003 年当時は、証明書発行基盤さえあれば、各種認証への利用が広まっていくと考えられていたかもしれないが、現実には、サービスはメリットがあれば多少の認証リスクを負ってでも普及

していく。逆に真に認証を必要とする場面には、ある程度信頼性の高い実在証明に基づき、各種サービスで共通に使えるアイデンティティを証明する基盤（例えば現実社会の免許証のようなもの）でなければ、適用は難しいということかもしれない。

2.2 社会基盤と電子署名および証明書

前節で分かるように、本人確認、属性確認のための基盤は、ほとんど整備されていない状況である。官・民の電子サービス、ネットサービスがより発展するには、官の本人確認基盤が民間分野でも連携できることや、民間での本人確認、属性確認の基盤のあり方が整理されることが１つの条件になると考えられる。

電子証明書と電子署名は、本人性や属性などを証明し、結果を保証する手段として適しており、社会基盤の重要な要素になるはずである。しかし冒頭に述べたように、一般には電子証明書や署名に対する理解は十分ではなく、必要性が認識されていないのかもしれない。それらの意味を再確認した上で、どのような基盤が必要とされるかについて、利用シーンから考えてみる。

(1) 電子証明書と電子署名に対する認識

電子証明書と電子署名について、例えば次のように認識されていることが多いのではないかと思われる。

- ✓ 証明書はパスワードに代わる認証手段である
- ✓ 証明書はコピーされると成りすまされたり個人情報が漏洩する
- ✓ 証明書の取得は面倒で、使いにくい
- ✓ 署名しても見えないので効果がわからない
- ✓ 署名はメリットがないので使い道がない

これらは一面では正しい部分もあるが、それが全てではないという意味では、ありがちな誤解であるともいえる。

① パスワードの代わり

証明書は、パスワードより強い認証手段として説明され、アクセス認証に利用されることが多いのは事実であろう。なりすましするためのキー情報(パスワード方式ではパスワードそのもの、証明書（PKI）方式では秘密鍵）を推測することが、パスワード方式よりも証明書方式のほうが一般に困難であることから、総合的にパスワードより強度が高いのは確かである。但しキー情報を安全に保管するなど適切な運用がなされる前提は同じである。また、バイオ認証ともよく比較され、バイオ認証のほうがより厳密であるという考え方もあるが、それぞれ特長があり、用途・目的によって使い分けるべきであろう。バイオ認証は生体そのものを認証するには優れるが、逆に模造される危険があることや法人や機器には使えないこと、変更の効かない個人情報であることにも注意が必要である。何よりも証明書がパスワードやバイオ認証と決定的に違うのは、認証だけでなく、署名ができることにある。

② 個人情報が不安

証明書はコピーされたり、見られたりすると問題が生じるというのは、単純な誤解であろう。証明書自体は公開される情報でありコピーもできるが、秘密鍵を別に所有していることに意味があり、IC カードなどの耐タンパな処理能力のあるデバイスを持っていることが重要である。証明書に記載する情報は認証局（サービス）のポリシーや証明書の用途によるが、一般には公開できない個人情報は記載すべきでないと考えられる。背番号制を連想されるケースもこの認識の延長と考えられるが、証明書が、必ずしも一意の（個人を特定しやすい）背番号を要求しているわけではない。もともと各業務システムや分野毎に何らかの識別子（ID）が付与されて、一元的に管理されており、その範囲で証明書を導入することは、現状と何ら変わることはない。分野をまたがって証明書を導入する場合も、それらの ID を容易に結合させない仕組みが、すでにいくつかの国で実現されている。また、証明書が 1 枚である必要はなく、むしろ証明される事柄（属性）や用途によって、信頼性のレベルなども異なり、複数あるほうが自然であろう。

③ 取得が面倒で使いにくい

証明書（署名）は実印相当なので、高価で取得が面倒であり、使いにくいという評判は、現状の仕組みや制度によるところが大きい。実印相当と位置づけているのは電子署名法の用途の場合であり、それなりの信頼性を求めたためである。必ずしもすべての用途に実印が必要なわけではないが、それに代わるより簡易な制度が制定されていないことが課題である。ただ、何らかの本人確認は必要であり、証明書の信頼度に応じた手続きは許容されるべきである。また、使いにくさは、IC カードリーダの設定の手間など個々のシステムの問題もあり、徐々に改善されていくと期待したい。証明書は期限があるため面倒というイメージもあるが、パスワードも本来は定期的に変えるべきであり（パスワードの推測容易性を考慮すると証明書よりも短い周期での変更が求められる）、そこに本質的な差はない。

④ 署名結果が見えない

電子署名は、署名対象のデータに添付される形で利用され、暗号化のように情報に変化を加えるものではないため、見た目に分かりにくく、効果が実感しにくいのも事実であろう。これはビューワなどアプリケーションが普及することで解消されていくと期待したい。第 3 部で述べるように証明書のビジュアル化の検討も始まっている。

⑤ 署名のメリットがわからない

メリットを感じにくいのは紙での署名と同様で、本来署名は、相手が否認防止の担保を取る用途が多いため、一般人が自ら望んで行うケースは少ない。むしろ相手（多くの場合サービス提供側）のメリットであるため、サービス提供側がその負担で導入することを考えてもよいと思われる。また本人が自ら署名を必要とするのは、社会的責任のある立場や資格を有する者であり、そういった層の義務と責任（noblesse oblige）として普及していくべきであろう。政治家がインターネット上で情報発信する場合の影響力の大きさを考えても当然のことと考えられる。

(2) 電子証明書と電子署名の適用領域

上記のとおり、証明書は単なる ID/パスワードの代わりではない。何かを証明していることと、それを保証する仕組みがあることが重要である。つまり、住民登録（実在性）や何らかの資格属性を審査して証明していることと、それを認定した機関（認証局）の署名が付いていることである。例えるなら、保証付きの ID と言えるかもしれない。通常の ID/パスワードと違い、何かのアプリケーションに限定される必要もない。

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発行されるため、そこに住所をおく住民であることを証明する証明書であるが、どういう人物か、経済力支払い能力がどうかなどは証明しない。クレジットカードが使われるような領域には、金融機関が何らかの与信に基づいて発行する証明書のほうが有用かもしれない。また、社会生活上は、単なる住民であるより、何らかの肩書きが重要な場面も多く、資格の証明や企業・組織などの団体の証明書の方が価値があるケースも想定される。1 人が何枚かの証明書を持ち、目的に応じて使い分けることが必要かもしれないが、現状ではまだ、使い分けの基準や証明能力のレベルについて共通認識にはなっていない。

電子署名をすることは、①改ざん防止、②存在証明、③文責、④否認防止の意味がある。①②は自然人の署名である必要はなく、機械の署名でもかまわない。③④は誰が何に署名するかが重要であり、署名者の保証や意志が、署名対象に込められる。③は、署名者が積極的に内容を保証する場合が多く、④は逆に相手側が署名者の否認を防止するため強制的に署名させる意味合いが強い。日本では特に文責を主張する③の用途は少なく、署名者の望まない④のケースが多いことが、電子署名の普及を妨げる 1 つの要因かもしれない。なお、任意の電文に署名させて本人確認を行う処理は、認証（Authenticationn）であり、利用者は、一般的な「署名」の意識は持たない。

以上のことから、公的な証明や何らかの資格・属性に基づく電子証明書は、官民の連携など複数のサービスで使える ID になりうる。さらに、その場限りの認証ではなく、後々、事実の確認や意志の確認を必要とする場面や、情報そのものに意志や文責を付与したい場合には、証明書と署名が必須と言えるだろう。

(3) 市民生活における証明の対象と利用シーン

H15 年度報告にあるように「市民生活」の中で本人性や属性・資格を提示するようなシーンが、いつどのような頻度で発生するかを考えてみる。

図 1.2.1 にあるように、ライフイベントや年中行事において本人確認を行う際には、公的な証明が必要となることが多い。しかしこれらの場面は日常的にあるわけではなく、普段は必要性を実感しにくい。従って、何かのイベントに直面して急に必要性を実感することになる。その際、手続きが複雑なために取得を諦めたり、公的証明に対するマイナスイメージが形成されている可能性がある。これに対しては、例えば、出生または成人と同時に必ず付与される欧州のような仕組みがあれば、利便性が飛躍的に高まり、利用シーンも増えると思われる。

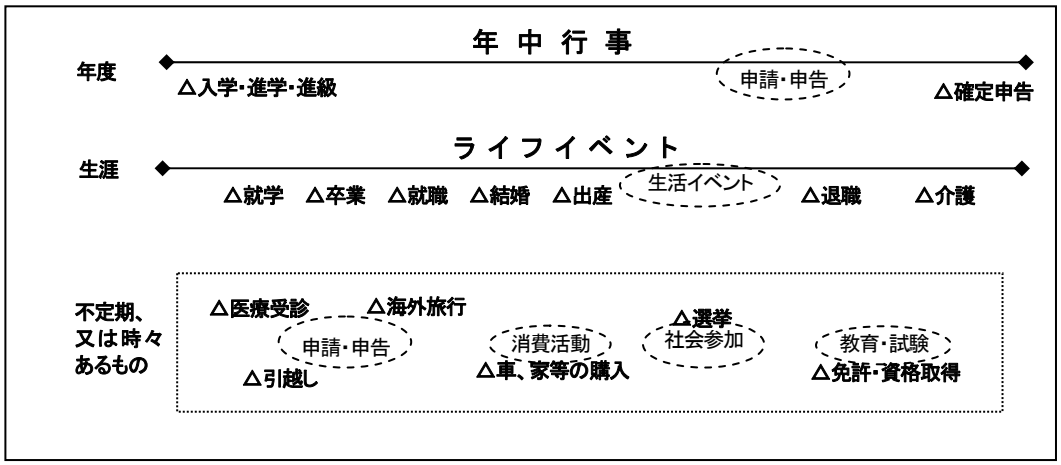


図 1.2.1 本人確認等を必要とするイベントの例

一方、日々必要性を感じるのは、図 1.2.2 のように、何らかの組織に属する証明や資格の証明である。これは何らかのサービスを提供・享受する場合、住民登録に基づく実在証明だけでなく、資格や権利を証明する必要がある場合が多いことによる。しかも利用頻度が高いことから、より柔軟に証明書を発行可能であることが求められるだろう。例えば、公的な証明による本人確認に基づいて、民間の資格証明を発行するとか、連携の仕組みも必要になると考えられる。特に、企業など ID 管理基盤やユーザ DB が整備されている環境では証明書発行にも馴染みやすく、資格やサービスの利用許可などを表す証明書を発行することにより、一種の社会基盤となるかもしれない。

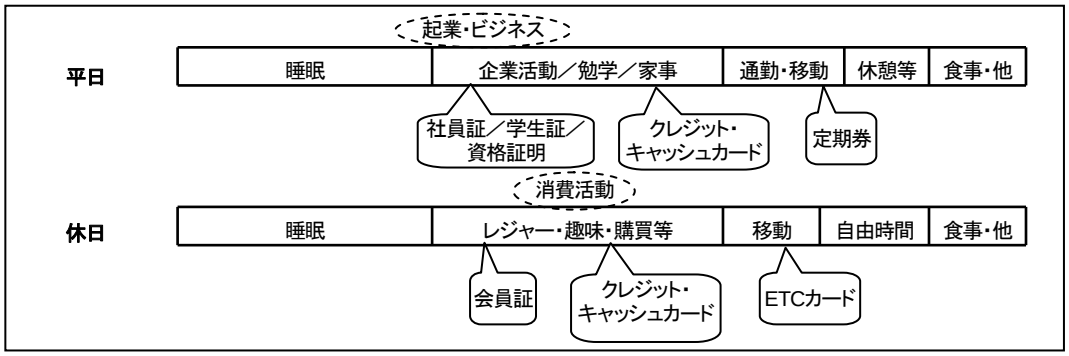


図 1.2.2 一日のパターンと証明事項の例

これらを踏まえて、官民のサービスに使える社会基盤が整備されていくことが期待される。

3. デジタル社会の官民連携サービス

3.1 官民連携サービスへの要求

3.1.1 行政サービスのパラダイムシフト

行政機関は、住民情報、戸籍情報、資格情報、許認可情報、登記情報等の様々な信頼のおける登録情報（個人情報、企業情報）を保持しており、これらの情報は社会を動かす重要な役割を担っている。これらの情報は、民間おいても信頼の拠り所として広く利用されている。

このような登録情報は、デジタル技術もネットワークもない時代から「紙の台帳」という形で存在していた。現在では、これらの多くがコンピュータにより管理されデータベース化されているが、名前としては「住民基本台帳」「土地・家屋台帳」等といった「紙の台帳」時代を連想させる名前で管理されている。実際に名前だけでなく現状の日本のシステムは、デジタル技術もネットワークもない時代の「紙台帳」を前提としたシステムから大きく変わっている訳ではないように見受けられる。

「紙台帳」を前提とした場合、その登録には、物理的に台帳がある役所に出向いて登録を申請する必要があった。出向く必要があるため「紙台帳」は地域に分散しており、台帳のインデックスとなる識別情報は、地域に依存した形で発番され管理されていた。こうした「紙台帳」を前提としたシステムは現在においても様々な形で継承されている。例えば、企業情報の最もプリミティブな情報となる「商業登記簿」は、こうした「紙台帳」の時代のシステムを基本的には継承している。

「紙台帳」にある情報を、ある別の組織に対して示したい場合、台帳がある役所に出向いて、台帳にある情報に基づいた「紙の証明書」を発行してもらう必要があった。例えば、住民票、印鑑証明書、戸籍謄本、登記簿謄本などがこうした「紙の証明書」類になる。こうした仕組みは制度化され、世の中でごく当たり前に、何の疑問もなく利用されている。現状の日本の電子政府では、こうした証明書の取得がオンラインで可能という方向にはある。しかし、基本的な仕組みは、「紙台帳」を前提とした仕組みからほとんど変わっていないように見受けられる。

行政サービスにおける申請主義は、「紙台帳」が前提だった時代において、行政機関が社会のオーソリティとしての行政サービスを行うために必要な仕組みだったと考えられる。そして、日本の電子政府は、こうした仕組みをそのままの形で電子化するという発想で展開してきた。ところが、先進的な電子政府を実現しつつある国においては、こうしたレガシーな仕組み自体が根本から見直されつつある。根本的に見直された仕組みを土台に行政サービス自体も申請主義からプッシュ型へ変化しつつある。例えば、韓国においては、戸籍制度が廃止され、印鑑登録制度も廃止されようとしている。これらは、行政機関のバックオフィス連携、官民連携を前提とした法制度に置き換わろうとしている。欧州における先進的な電子政府においても同様の動きがある。これらの行政サービスのパラダイムシフトとも言える動きには、行政サービス、および行政機関の本質的な変革が必要になる。

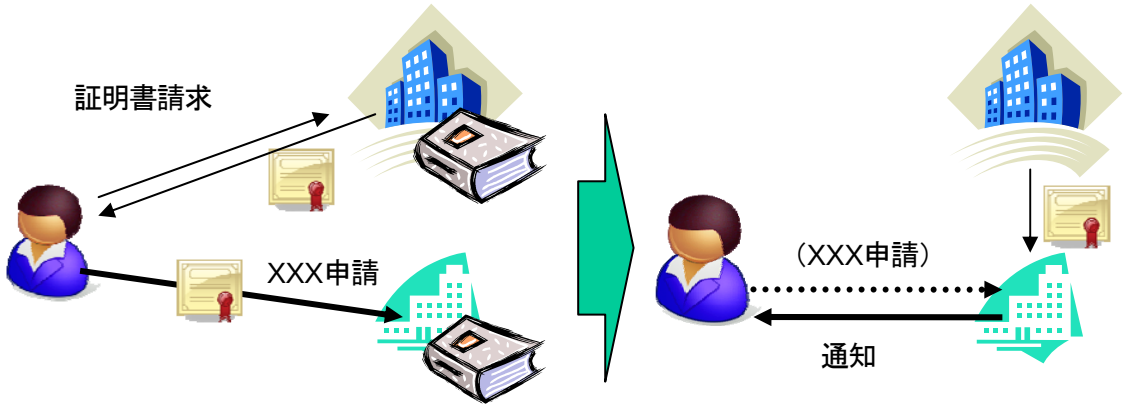


図 1.3.1 行政サービスのパラダイムシフト

3.1.2　官民連携サービスの基本的な考え方

現状の行政サービスにおける申請主義は、デジタル技術もネットワークもない「紙の台帳」を前提とした時代のシステムに由来していると考えられる。こうした申請主義から脱却して、プッシュ型の行政サービスに移行するためには、これまでの法制度や慣習にとらわれない、行政サービスのパラダイムシフトが必要になる。具体的にプッシュ型の行政サービスを実現するためには、行政機関のバックオフィス連携、官民連携が必要になる。こうしたことは、様々な行政機関、公共機関、民間組織に散らばった個人情報が、個人自身にとって有効活用されることより効率性の高い社会を実現するだけでなく、透明性の高い社会を作る上でも重要だと考えられる。

行政機関のバックオフィス連携、官民連携の基本的な仕組みは、ふたつの組織間での個人情報の移動になる。個人情報の移動には、行政機関が持つ社会のオーソリティとして保持している情報、例えば、住民情報、登記情報等の個人情報を、個人の意思に従って、行政機関から民間組織へ、または、登録情報として民間組織から行政組織へ引き渡すこと等が考えられる。こうした組織間の個人情報の移動は、制度的にも明確にされ、こうした制度に基づいた情報システムが構築される必要がある。

これまでの申請主義の行政サービスにおいては、個人が紙文書である個人情報を自分自身で物理的に組織間を移動させていた。また、自分自身が直接的に関与して個人情報の名寄せを行っていたことになる。こうしたことは、行政機関のバックオフィス連携、官民連携の実現により、利用者の利便性と、行政機関の高い効率性が期待できる。一方、理由が明確でない個人情報の移動が行われると行政機関による恣意的な個人情報の名寄せと見なされる。

一般論として、「ふたつの組織間での個人情報の移動」は、個人情報保護法等に従った形で行われるべきある。個人情報の移動は、通常、以下の二つの場合が考えられる。

(1) 法律で定められた個人情報の移動
(2) 個人の同意に基づいた個人情報の移動

逆の見方をすると「法律で定められたもの」「個人の同意に基づくもの」以外の個人情報の移動は禁止されるべきであり、また、不正な個人情報の移動を監視する枠組みが必要になる。

ここでは、2010 年 3 月時点で、内閣官房国家戦略室で検討されている「社会保障・税に関わる番号制度」の背景のひとつである納税について少し考察する。雇用者である企業は、被雇用者である従業員に源泉徴収票を発行する。これは企業が従業員に発行する給与支払い証明となる。納税者である個人は、確定申告に、雇用者から受け取ったこの源泉徴収票を確定申告の添付書類として税務署に提出する。納税者本人は、収入に関する情報以外にも、医療費控除や住宅ローン控除等の証明も添付書類として税務署に提出する。電子政府では、こうした添付書類の扱いが常に問題になっているが、こうした添付書類を揃える作用は、納税者本人自身による個人情報の名寄せ作業だと考えられる。

こうした申告、すなわち申請主義の仕組みをプッシュ型の仕組みに変更しようとした場合、雇用者である企業が、企業が保持する個人情報である個人の源泉徴収票を、個人の識別子を明確にした電子データで直接的に税務署に提出する。また、控除となる医療費や住宅ローンを受け取る組織も同様に電子データで直接的に税務署に提出する。これが一種の官民連携サービスだと考えられる。

この時、雇用者が被雇用者の源泉徴収票の電子データを税務署に提出しなければならないという法制度になれば、この個人情報の移動は、「(1) 法律で定められたもの」になる。また、被雇用者が、源泉徴収票を添付する代わり雇用者から転送するように依頼した場合は、この個人情報の移動は、「(2) 個人の同意に基づくもの」になる。納税者本人は、医療費控除や住宅ローン控除等の証明も含め、個人経由で申告書類（添付書類）とするのではなく、官民連携で渡された情報を元に税務署が申告書類を作成する。次に、納税者は税務所が作成した申告書の内容の確認を行う。こうしたプッシュ型の納税サービスを提供している海外事例は多数存在する。

韓国では、電子レセプトが日本にくらべ非常に普及している。電子レセプトの情報は、納税者の医療控除のデータとしても利用されているようである。納税者の利便性を高めるとともに、医療費請求の透明化も役立っている。

この場合は、民間組織から行政機関への個人情報の移動になるが、多くの行政サービスでは、行政機関から、民間組織等への個人情報の移動になる。いずれにせよ、個人情報が、個人にとって適切に利用されることが重要なポイントになる。

こうしたシステムを構築する際の課題は、納税者本人と、その本人に関係する組織が、納税者本人を一意に識別できるシステムの構築にある。多くの場合、識別のための「番号」があるだけでは、効率的で安全なサーヒスは提供できない。

「番号」等と個人（または、Identity）を結び付けるのが電子証明書の役割になる。2008 年度の報告書にある「社会基盤としての ID 管理と電子署名」では、こうしたシステムの事例を紹介している。

3.1.3 社会基盤としての ID 管理と個人の属性の扱い

2008 年度の ECOM の報告書にある「社会基盤としての ID 管理と電子署名」では、先進的な電子政府を実現している欧州 4 カ国（エストニア、デンマーク、スロベニア、オーストリア）の事例を紹介している。ここでは、行政機関のバックオフィス連携の基本的な仕組みの背景にある各国の ID 管理の仕組みと、その ID 管理を前提とした電子的な本人確認、そして電子署名の意義を解

説している。行政機関のバックオフィス連携や官民連携を実現する上で、社会基盤としての ID 管理は、必要不可欠なものだと考えられる。

社会基盤としての ID 管理が重要となっている背景には、デジタル技術やネットワークが、既存の社会の仕組みに対してアドホックに利用されていた時代から、デジタル技術やネットワークの利用を前提とした社会への移行がある。申請主義の行政サービスの世の中では、法的な裏付けが必要な個人の資格、権利等は、「免許書」「許可証」「権利書」といった物理的な所持による証明で示されてきた。しかしデジタル技術やネットワークの利用を前提とした社会に移行する中、個人の資格、権利等は、法的な意味での「識別」された個人の属性情報として扱われる時代に移っている。

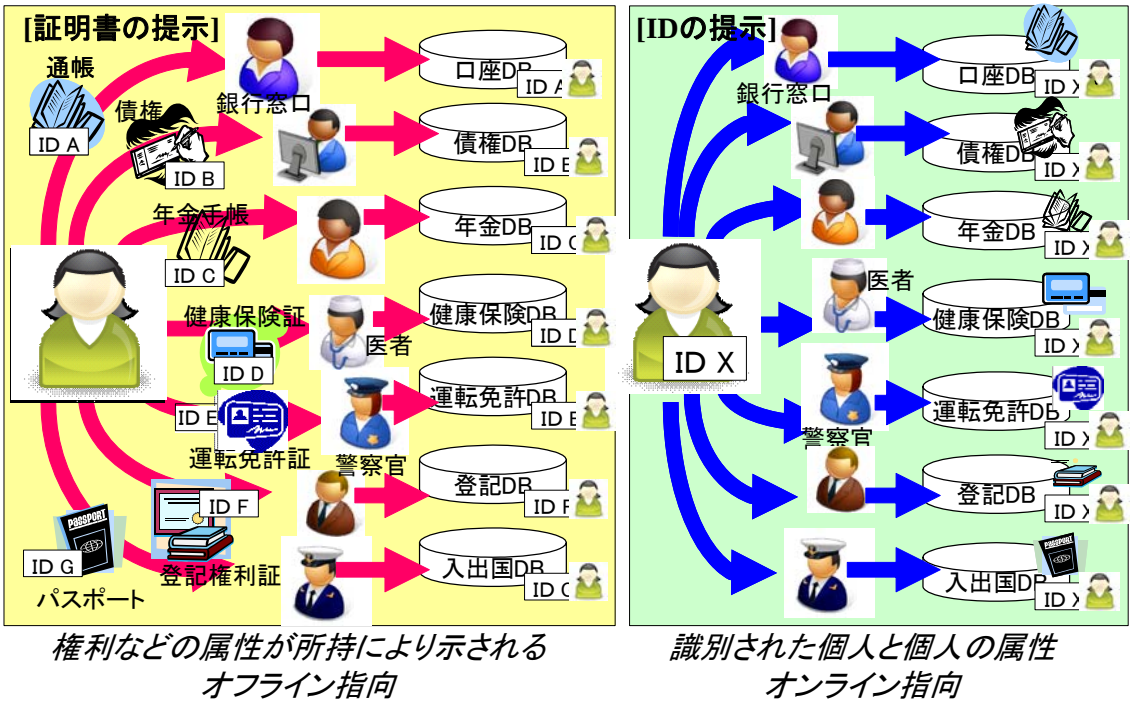


図 1.3.2 識別された個人の属性への移行

3.2 官民連携サービスのための基盤のあり方

3.2.1 官民連携サービスのための基盤への要求

日本の電子政府の現状として、情報通信の基盤は整備されたが、電子申請などの利用率が上がらない等、利活用が進んでいないといった報告がなされている。しかし、前節で説明した通り、現状の日本の社会の仕組みは、デジタル技術もネットワークもない時代の「紙台帳」を前提としたシステムの影響を強く残しているままであり、申請主義の行政サービスの上で社会の慣習が出来上がってしまっている。そのためプッシュ型の行政サービス、更に民間も含めた「官民連携サービス」に対応した基盤ということに関しては、制度的にも情報システム的にも、まったく未整

備といって良い状況なのではないだろうか。

こうした状況にあって、直接的なサービスとしての官民連携サービスを実現しようとすると、個別の官民連携サービスのシステムの構築が非常にコスト高なものになってしまう可能性が高い。また、行政機関による恣意的な個人情報の名寄せが防げない、名寄せが疑われるといったことも起き得る。そして、こうしたことが本質的な電子化が遅らせる結果となる。

それではプッシュ型の行政サービスや官民連携サービスを可能にするための、どのような法制度の整備と、情報基盤の整備が必要なのだろうか。官民連携サービスへの要求から、以下のようなものが考えられる。

(1) 個人情報連携のための個人の一意識別
(2) 個人の身元証明
(3) 個人情報の移動の原則の確立
(4) 個人情報を連携させるための情報交換基盤

「(1) 個人情報連携のための個人の一意識別」は、「社会保障・税に関わる番号制度」等で議論されている番号制度の話になる。こうした番号は、行政機関や民間組織の情報システムの構築に決定的な影響があるにも関わらず、曖昧にされてきたところがある。

「(2) 個人の身元証明」は、「番号」等の個人の一意識別子と個人（または、Identity）を結び付けるための仕組み、そのための基盤の話になる。個人の一意識別子としての「番号」は、効率性を高めるが、安全なサービスを実現するには、提供するサービスのリスクに応じた「(2) 個人の身元証明」のセキュリティレベルが重要になる。これには認証基盤と言われるようなものが重要になるが、公的個人認証サービス（JPKI）等が、こうした役割を果たすと考えられる。しかし JPKI についても「(1) 個人情報連携のための個人の一意識別」の議論がされないまま構築されたところに問題がある。JPKI につては利便性などの批判もあるが、こうしたことは、電子政府ガイドライン検討会のセキュリティ分科会の報告書にまとめられている。

「(3) 個人情報の移動の原則の確立」は、個人情報保護法などの課題になる。プッシュ型の行政サービスでは、個人情報が組織を超えて移動される。一方で、行政機関による恣意的な個人情報の名寄せを防ぐ必要がある。現在の日本では、行政機関を監視する第 3 者機関が存在しないといった課題がある。

「(4) 個人情報を連携させるための情報交換基盤」に関しては、エストニアの X-ROAD、ベルギーのクロスロードバンク、韓国の行政情報共同利用センターなどの事例がある。このような情報交換の基盤は、(1), (2), (3)に関連する法制度と情報基盤が整備されて初めて機能すると考えられる。

以上の 4 つの項目は、関連性を持っている。これらの関連性が十分に理解された上でバランスのよい実装がなされる必要がある。これらを考察するため、ここでは、世界でも最もプッシュ型の行政サービスや官民連携サービスのための基盤が整備されつつあると考えられるエストニア等の事例などを踏まえて、そのあり方を考察する。

3.2.2　オーストリアの電子政府法における識別の考え方

デジタル技術もネットワークもない時代の「紙の台帳」の時代においては、行政サービスにおいて、個人情報の移動は、個人が紙文書を自分自身で物理的に転送していた。この際の本人確認などの多くの作業は、「目視」による確認で行われてきた。目視による作業により、本人が紙に書いた住所の情報の曖昧性等などを許容してきた。しかし、こうしたことを行政機関のバックオフィス連携においてデジタルデータの交換という形で行う場合、「曖昧性」を極力排除する必要がある。その中でも重要なのが個人の一意識別になる。個人が一意識別された上で、様々な関係、属性が、曖昧さがなく電子的に証明することができれば、効率性、透明性が高い社会システムが構築できることになる。

個人の一意識別の考え方を明確にしているものに「オーストリアの電子政府法」がある。「オーストリアの電子政府法」では、電子政府のサービス対象者の「一意識別」と個人情報を電子的に扱う際の原則を明確にしている。

◇「一意識別（Unique identity)」
データ主体者が他のすべてのデータ主体者から誤りなく識別されることを可能にする、一つまたは複数の特徴による特定人（データ主体者、本条7号）の指定。
◇「履歴識別（Recurring identity)」
一意識別（Unique identity）によらずに、以前の出来事（以前の提出行為など）の参照により人の認識を可能にする方法での特定人（データ主体者、本条7号）の指定。
◇一意識別と履歴識別
「2000年データ保護法」（中略）秘密性に保護権益が存在する個人データへのアクセス権（「2000年データ保護法」第4条1号）が付与されるのは、アクセス要求者が一意識別（Unique identity）され、その要求の真正性（Authenticity）が確認された場合に限る。かかる確認は、電子的に証明されうる形態で提供されなければならない。履歴識別（Recurring identity）のみが可能な場合、アクセスが許可されるのは、アクセス要求者が当該識別を使用して自ら提供した個人データに関するものに限る。

「オーストリアの電子政府法」では、電子政府のサービス対象者である「オーストリア在住のオーストリア国民」、「オーストリア在住の外国人」、「海外のオーストリア人」を一意に識別できることを要求している。デジタル技術やネットワークの利用を前提とした社会においては、法的な裏付けが必要な個人の資格、権利等が「一意識別された個人」の属性情報として扱われる方向にあるが、組織間での個人情報の連携を曖昧のないものにするためにも個人の一意識別は大きな意味を持つ。「オーストリアの電子政府法」は、サービス対象者の一意識別の要求を明確に定義している。オーストリアの電子政府は、このような制度に基づいて構築されていることは言うまでもない。

我が国においても、内閣官房国家戦略室で検討されている「社会保障・税に関わる番号制度」等は、本来ならば、電子政府の構築が始まる前に検討されるべきだったであろう。

3.2.3　エストニアの電子政府におけるデータ連携の基盤

行政サービスのバックオフィス連携、更に官民連携を実現した先進事例としてエストニアの事例がある。エストニアにおける、これらの連携のための情報システムの中心はX-Roadと呼ばれているデータ交換システムになる。このX-Roadは、「ふたつの組織間での個人情報の移動」のための基盤だと考えると理解しやすい。

エストニアでは、2001年頃に、行政機関のバックオフィス連携を行った上で電子的な行政サービスの提供を行うことが決定され、その目的を達成する手段としてX-Roadの構築がなされた。同時期の2001年当時、日本における電子政府の方針は「既存の手続きをすべて電子化する」というものだった。これは、デジタル技術もネットワークもない時代の「紙の台帳」を前提とした申請主義の行政サービスの全面的な電子化ということになる。2001年当時のエストニアと日本の電子政府の方針は、このように全く異なるものだった。

エストニアに　おける先進的な電子政府の背景に以下のようなものがある。

- 既存の「インフラ、法制度、慣習、権益」等のしがらみが少ない
- 柔軟な法制度
- 国策として情報通信技術による経済発展を目指したトップダウンな情報通信技術施策をぶれなく続けてきた
- 1991年に独立回復、2004年EU加盟といった時代背景の中、（時代的にも）情報通信技術を前提に国つくりが行われてきた
- 国がコンパクト（人口　135万人）

(1)「個人情報を連携させるための情報交換基盤」であるX-Road

X-Roadには、様々な個人情報を保持する行政機関だけでなく、公共的なサービスを提供するテレコム、銀行、ヘルスケア等の民間（プライベートセクター）にも接続されている。

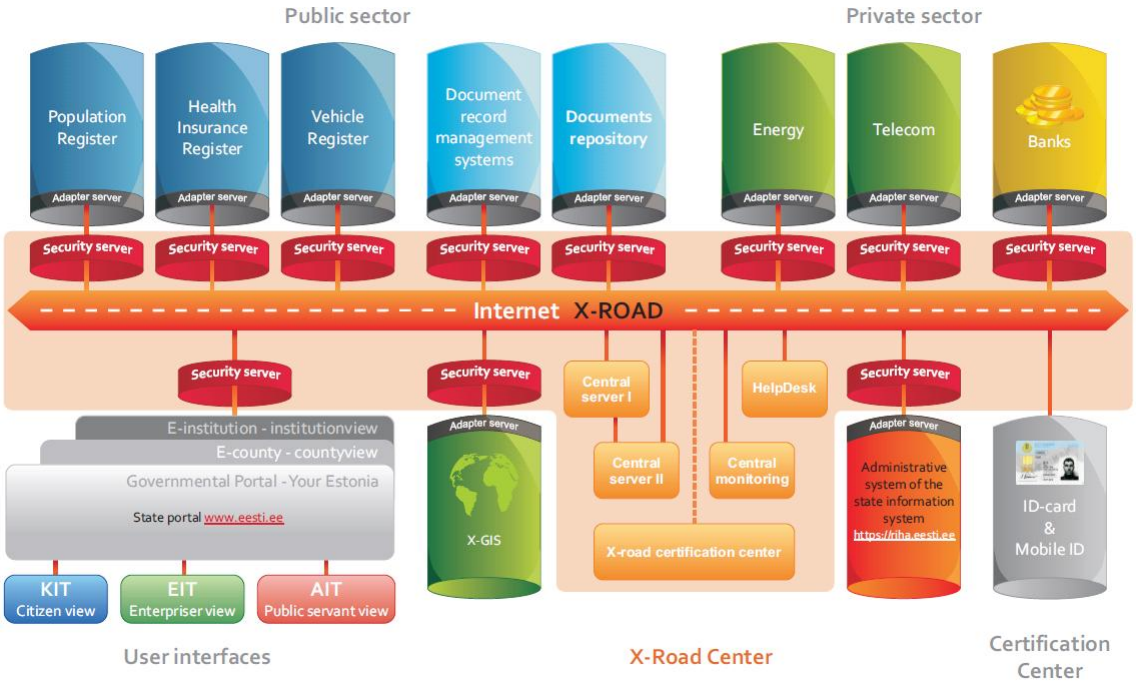


図 1.3.3 エストニアの X-ROAD

(2) 「個人情報連携のための個人の一意識別である」国民 ID

2008 年度の ECOM の報告書にある「社会基盤としての ID 管理と電子署名」では、欧州 4 カ国の事例の中でエストニアの事例も紹介している。エストニアでは、11 桁の国民 ID がある。

(3) 「個人の身元証明」する国民 ID カードとモバイル ID

国民 ID と氏名を証明する手段として、国民 ID カードがあるが、この国民 ID カードには、電子的に国民 ID と氏名を証明するための電子証明書が格納されている。日本の公的個人認証サービスの電子証明書では、住基 4 情報が格納されているが、この住基 4 情報には住所も含まれている。それに対してエストニアの国民 ID カードに格納されている電子証明書には、住所は含まれない。「住所」は、識別された個人の属性、すなわち国民 ID により識別された属性として扱われる。こうした属性の参照は、本人の許諾同意に基づく場合や、法的な裏付けのある権限者から行われる。

国民 ID カードは、運転免許証や健康保険証の代替にもなっている等、様々に利用されているが、欠点としては、住基カードと同様に、その利用にカードリーダ・ライタが必要になるといったことがある。エストニアにおいては、国民 ID カード以外に、現在はモバイル ID の展開を行っている。このモバイル ID では、携帯電話の SIM に名前と国民 ID を証明する電子証明書が格納されている。このモバイル ID は、基本的には、PC と組み合わせて利用するものだが、カードリーダ・ライタなしに、国民 ID カードと、ほぼ同様の機能を提供している。

エストニアでは 2005 年に国民 ID カードを利用した世界で初めてインターネット投票が行われ、その後も 2007 年、2009 年にもインターネット投票が行われている。モバイル ID での投票を可能とする法律も可決し、2011 年から行われるとされている。

(4) 「個人情報の移動の原則の確立」のための個人情報保護法

個人情報の取り扱いに関する基本的な枠組みは、エストニアの個人情報保護法により定められている。エストニアは、EU の加盟国であり、EU の「データ保護指令」に準拠した個人情報保護法を施行している。そのため、個人情報の扱いに関する第三者機関として、「個人情報保護監察局」が存在する。この「個人情報保護監察局」が、「個人情報の移動」に関して大きな役割を果たしている。

エストニアのプッシュ型の行政サービスにおいて「ふたつの組織間での個人情報の移動」は、X-ROAD を介して行われている。X-ROAD では、個人情報の本質的なオーナである個人は、自分の個人情報に誰がいつアクセスしたかという履歴情報を自分で調べることができる仕組みを持っている。不正なアクセスは、訴えることが出来る。また異なる機関の持つ個人情報のデータベースの関連付けは、「個人情報保護監察局」の許可が必要とされている。

エストニアの個人情報保護法では、機微な個人情報の収集については、個人情報保護監察局の許可が必要など、日本の個人情報保護法よりも厳しい面がある。

その一方、名前と国民 ID の扱いについては寛容なところがある。日本においては、「番号」等の漏洩が問題視される傾向にあるが、エストニアの国民 ID は、公共財的な扱いになっており、実質的にも公開されている。これは、国民 ID、モバイル ID という国民 ID を証明する強力な手段が提供されていることに起因している。

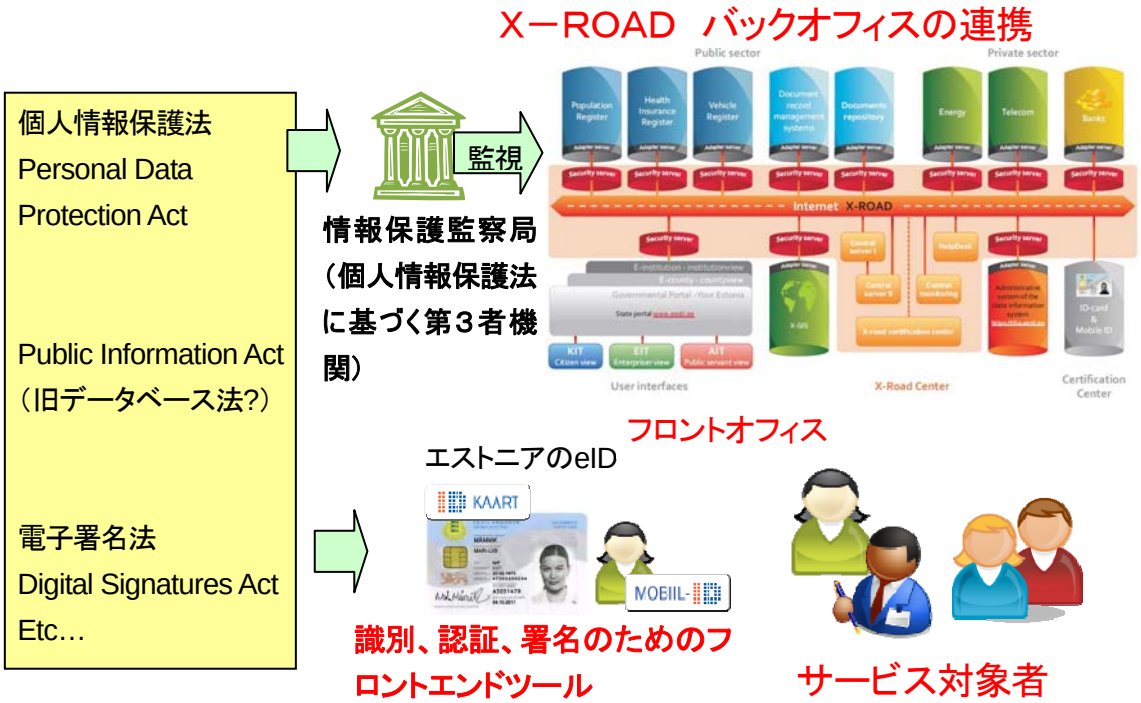


図 1.3.4 エストニアの電子政府の概観

3.2.4　官民連携サービスの基盤のためのいくつかの考察

(1) 不正な個人情報の移動を監視する枠組

個人情報を扱う行政機関のバックオフィス連携や官民連携を推進するためには、その個人情報の扱いを明確にする必要がある。特に、個人情報の連携が、行政機関による個人の不正な監視や、恣意的な個人情報の名寄せにつながることを防ぐ必要がある。連携する個人情報は、「法律で定められたもの」「個人の同意に基づくもの」とした場合、これら以外の不正な個人情報の移動を監視する枠組みが必要になる。

EU の「データ保護指令」に準拠した個人情報保護法を施行している国では、個人情報保護に関する第三者機関が存在する。また、官民の境目がないオムニバス方式の個人情報保護法を施行している。第三者機関は、行政機関のバックオフィス連携、官民連携における、不正な個人情報の移動を監視する役割を果たしている。オムニバス方式の個人情報保護法は、個人情報の官民連携を矛盾なく行うことができると考えられる。

現状の日本においては、第三者機関は存在しない。特に、多くの個人情報が、個人の意思に関係なく集まる行政機関を監視するための第三者機関が存在しない。個人情報の具体的な取り扱いは、業種毎の民間を監督する管轄官庁毎に定められている。こうした枠組みは、個人情報の行政機関のバックオフィス連携や官民連携を困難にする可能性がある。

(2) 利用者の同意確認の仕組み

行政機関のバックオフィス連携、官民連携により、様々の行政機関、公共機関、民間組織に散らばった個人情報を、個人自身にとって有効活用するためには、個人情報の扱い、個人情報の移動に関して「個人の同意確認を取る仕組み」が極めて重要になる。同意確認が曖昧だと、個人にとっての個人情報の利活用と、行政機関による恣意的な個人情報の名寄せの区別がつかなくなる。

重要な同意確認を電子的に行うための合理的な手段は、同意文書への個人の電子署名になる。電子署名まで要求される必要のない軽微な同意確認も含め、利用者の同意確認の仕組みの整備が非常に重要になる。

(3) 代理の仕組み

個人の識別の問題を明確した上で、「代理の仕組み」を確立する必要がある。基本的には、個人と代理人の関係が、電子的に証明されるべきである。代理人は、法的な裏付けがある資格者（法定代理人）、公務員、親権者が考えられる。親権者に関しては、親権者であること自体も、電子的な証明ができるべきである。

韓国においては、2008 年に戸籍が廃止され、代わって「家族関係登録法」が施行されている。「家族関係登録法」では、韓国における個人の識別子である「住民登録番号」により、家族関係を登録、証明する体系になっている。親権者が、代理者となる場合、親権者であることが、電子的に曖昧さがなく証明できる必要があるが、「家族関係登録法」により、こうしたことが可能になったと言える。

[参考文献]

(1) 欧州の政府系 PKI と ID 管理
http://www.jnsa.org/seminar/2009/0624/data/06_matsumoto.pdf
「エストニア」「デンマーク」「スロベニア」「オーストリア」の欧州の 4 カ国の電子政府先進国における「ID 管理」と、ID 管理に基づく「データ連携」の比較を行っている

(2) ECOM の 20 年度報告書
電子署名普及に関する活動報告 2008 - 1,751KB
http://www.ecom.jp/results/h20seika/H20results-14.pdf
第 1 部　　3　社会基盤としての ID 管理と電子署名

(3) 電子署名普及に関する活動報告 2007
http://www.ecom.jp/results/h19seika/h19results-14.pdf
付録：オーストリアの電子政府法

(4) 電子政府ガイドライン作成検討会　セキュリティ分科会報告書
http://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf

(5) Electronic identity management in Estonia between market and state governance
http://www.springerlink.com/content/dx707750g1p41vux/
エストニアにおける個人情報の扱いについて言及している

4. 国民 ID に関する整理と提案

将来の少子化社会に対応するには行政コストを下げる必要があり、国民の要求に対応するには行政サービスを増強する必要がある。この相反する要求に対応するためには IT 技術を用いた行政の自動化（AA：Administrative Automation（注：ECOM が定義した用語で一般に使われているものではない））を進めることが必須である。この 10 年、世界各国では電子政府あるいは電子行政の名の下で AA が推進されてきた。日本においても 2001 年に IT 戦略本部が立ち上り、電子政府の実現に向けた活動が始まってから約 10 年を経たが、一部のサービスを除き電子政府の利用拡大の見通しはたたず、今後の IT 戦略は混沌としたまま方向性を失っているように見える。これは、「IT 推進のポリシー」や「IT 社会基盤のフレームワーク」など IT 推進方針に関する検討が不十分なままになっているためと考えられる。

このような状況のため、「IT 社会基盤のフレームワーク」の重要な技術要素である国民 ID 管理技術（国民に関する情報に番号を付けて管理する技術）についての方針が決まらず、公的機関の各セクタ（個人情報の管理単位）が管理している個人情報を、セクタを超えて利用しあうことができない。たとえば、国民の納税額を決めるにしても、本人の所得情報は税務署等税務関連セクタが保有しており、医療控除や扶養控除を行うためには、他のセクタが保管する医療や扶養に関する個人情報を入手して納税額を決める必要がある。その場合、各セクタが持つ個人情報が同一人物のものであることを認証するため、個人情報と国民 ID を対応付けて管理する必要がある。

この「行政機関がセクタ毎に保管する個人情報の連携の仕組み」の導入について、すなわち、電子行政フレームワークの基盤技術のひとつと考えられる国民 ID 管理技術の必要性について、多くの人によって論じられるようになってきている。

日本において、この国民 ID の仕組みをこれまで導入できていない主な理由としては、国民の不安に対して、十分な説明ができていないことが挙げられる。

たとえば、電子化及び国民 ID の導入により、他人に知られたくない個人情報（宗教、家族血縁、職歴、病歴、など）が広く世の中に出回ってしまう心配や、政府が個人情報を容易に集約できるようになるため、集約した個人情報を国民を管理するために使用する心配があるが、その不安を取り除く対応方法の説明や議論がほとんどない。

そこで、本章ではこれらの議論を進め、まず国民の不安を整理し、その不安に対応できる新たな個人 ID 管理のしくみを提案する。

4.1 IT 推進方針の必要性

国内における IT 戦略の議論は、国民を巻き込んで進めるべきで、国民の理解を得ないで進めては、出来上がったシステムは結局使われないものになってしまう。そのいい例が住民基本台帳ネットワークである。そこで、IT 推進計画をわかりやすく説明していく必要がある。エストニアを例にとると、電子政府推進のステップは図 1.4.1 の IT システム階層に示すように以下の 3 段階からなる。

(1) IT 推進ポリシー

日本においても、だれが、なぜ、何のために、どのように IT を推進していくのかのポリシー

を分かりやすく説明する必要がある。情報ポリシーの例としてエストニア情報ポリシーの原則を「エストニア情報社会戦略 2013」[EST01] より抜粋して紹介する。

① エストニアにおける情報社会の発展は、公共部門が主導する形で、この原則にしたがい進むべき方向を戦略的に選択する。

② 情報社会は、公共部門、民間部門および第三セクタの間の協力に基づいた、調整された方法で開発される。

③ 公共部門は賢明な顧客であり、公共調達において、革新的な実現方法に可能な限りの自由が残されることを保証する。

④ 情報社会は、すべてのエストニア国民のために開発される。その一方で、特殊なニーズを持つ社会的なグループへの差別の廃止、地域の発展、および地域の自主性の強化に特別の注意を払う。

⑤ エストニアの言語および文化の一貫性が保証される。

⑥ EU や世界のその他の地域で起きている動向を考慮に入れる。さらに、エストニアは、アクティブなパートナーとして自身の体験を他の国々と共有すると共に、他の国々からも学ぶ。

⑦ 公共部門は、既に存在している技術（eID カード、データ交換層 X-Road など）を利用し、IT 技術開発の重複を避ける。

⑧ 公共部門はビジネス・プロセスを再構成して、一般市民、企業、および公共団体から 1 回データを収集するだけで、あらゆるサービスが実現できるようにする。

⑨ 公共部門は異なるハードウェアおよびソフトウェア・プラットフォームを同等に取り扱い、自由に無償で利用できるオープンな標準（オープンスタンダード）を使用して情報システムの相互運用性を保証する。

(2) IT の基盤のフレームワーク

電子政府にとどまらず、日本として IT の基盤のフレームワークを決めることは重要である。特にユーザにとっては、サービスごとにユーザインタフェースが異なったり、認証や署名方式が違ったのでは、とても十分に検討されているシステムとは思えず、システムそのものに対して不信感を持ってしまう。

エストニアの IT の基盤のフレームワークを例に挙げれば、IT 基盤として eID や公開鍵基盤（PKI）、情報連携の仕組み、情報管理、地理情報などが、あげられている。

(3) アプリケーション

IT の基盤のフレームワークを利用してアプリケーションのシステム設計をすることにより、互換性がありかつ安価なシステムを構築することができる。

このため、ユーザニースに合わせた多くのアプリケーションシステムの出現が期待できる。

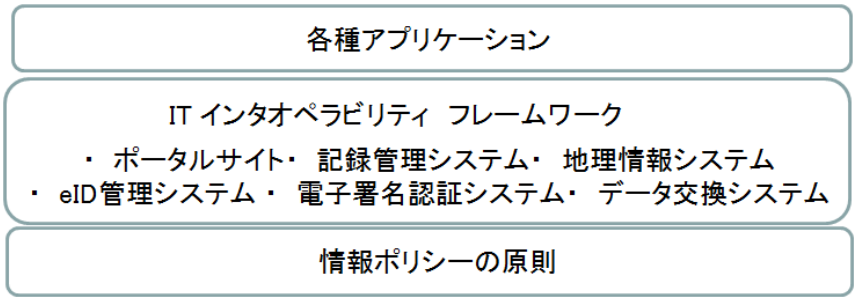


図 1.4.1 IT システムの階層

4.2 国民 ID 導入に関する課題の整理

IT 社会の恩恵を受けるには各セクタが保管する個人情報を連携して活用する必要があり、これを実現するための国民 ID の必要性、導入の方法について議論する必要がある。

現在利用されている基本 4 情報（氏名、生年月日、性別、住所）で個人を特定しようとする場合、名前に使われる漢字パターンのバリエーションが多いこと、漢字の読みのバリエーションが多いことから、情報が揺らぐ可能性が高い [榎並]。このため、年金システムでは個人が特定できない膨大な個人情報が発生してしまった。

また、行政の透明化が進んでいないこともあり、かなりの国民が行政を信頼していないこともあり、行政の電子化や国民 ID の導入により、国民の個人情報を行政が利用しやすくなることに不安を感じている人もいる。

すなわち、IT 化による効率化の効果は享受し、全国民を平等に取り扱うために管理することは必要だと思うが、IT を導入し国民に ID を振るのは、過剰管理、監視社会に繋がる可能性があると考えている。

また、住基ネット（住民基本台帳ネットワーク）がかなりの国民から強く反対されてきた理由はなにか、反対する人の意見を、2008 年 2 月 28 日　牧野二郎氏　講演資料より引用する。

① 住基ネットに携わる公務員等による個人情報の漏洩や不正利用の可能性
② ハッカーなどの不正侵入により、個人情報の流失や改ざんが起きる危険性
③ 住基ネットにかかる構築費や運用経費に対して、国民に提供されるサービスがあまりにも貧弱であり、コスト的に見合わない
④ 住民基本台帳法（以下「住基法」）の国会審議に際し、政府は稼動前に個人情報保護に「万全の措置を講じる」と約束し、同法の附則には「所要の措置を講ずる」との文言が入れられたが、個人情報保護法を未制定のままに住基ネットをスタートさせたことは、これらに反している
⑤ 国民総背番号制として国家による国民の監視・管理につながる危険性

これらの反対意見に対応するには、技術・制度・運用面から、分かりやすい説明を行っていかなければならない。

国民 ID の導入について、以下のとおり論点を整理する。

① 国民 ID の導入推進側の意見としては、
・ 行政コストの削減、行政サービスの向上のためには、バックオフィスの連携が必須。

・　基本4情報では、個人を特定しづらい（変形漢字、読み、姓の変更、住所の変更）。
・　暗号技術を用いることにより情報の漏洩に対応できる。
②　国民IDの導入反対側の意見は、
・　行政サービスの運営体制の中に犯人がいる場合の対応が不明確。
・　絶対に安全な完璧なシステムは無い。
・　将来日本が独裁体制になったときには、法律を無視して名寄せされてしまうか可能性がある。
③　第3者として
・　セクタ間の情報統合方法について国民の合意がない。
・　個人情報の活用について、法律やガイドラインが無い。
・　バックオフィスの連携について、無制限統合（行政が保管する全ての個人情報を統合可能）として議論されていて、無意味な議論が行われている。

そこで、反対側の意見を取り込んだ国民ID導入のための要件として以下の6点をあげる。

要件 1：個人情報の管理が明確で分かりやすい制度（法律やガイドライン）に従って運営されること。
要件2：個人情報の管理が中立的で信頼の高い組織によって運営されること。
要件 3：個人情報にレベルをつけあるレベルの個人情報については、セクタ間の情報提供は禁止すること。
要件 4：セクタ間の情報提供のしくみを明確にするとともに、個人情報を他のセクタに提供する時には本人への確認を基本とすること。
要件 5：本人の個人情報及び情報へのアクセスログをチェックでき、ミスやエラーを発見したときの対応方法が明確になっていること。
要件6：国家権力の暴走が危惧される場合は、セクタ間の情報提供を停止できること。

4.3　国民ID管理方式の整理

多くの国では、個人の情報を管理するために個人ごとにユニークな番号（ID）を用いている。個人にひとつのIDを宛てて、多くのセクタでそのIDを用いるモデルをFLAT MODELと呼ぶ。また、セクタごとに個人にひとつの ID を宛てるモデルを SEPARATED MODEL と呼ぶ。日本ではこの「SEPARATED MODEL」を採用している。

近年、電子政府など IT によるサービス向上が進められ、セクタ間の個人情報の交換の必要性が増してきたが、SEPARATED MODEL ではセクタ間の個人情報を対応づける方法がないため、これに対応できない。

そこで、SEPARATED MODEL のよさを生かしながら、セクタ間の個人情報の交換ができるモデルが検討されてきている。そのひとつが、オーストリアで実現しているモデルで、ひとつのIDから新たなセクタIDを生成するSECTORAL MODELであり、もうひとつがSEPARATED MODELで利用しているセクタ ID をそのまま利用し、ひとつの ID と各セクタのセクタ ID とのリンク情報を用いるLINK MODEL（注：ECOMの定義であり、一般的に使われているものではない）である。各方式の概

要を図 1.4.2 に示す。

以下に、4 つのモデルの長所、短所について説明する。

① FLAT MODEL

長所：一つの ID で個人情報を管理するため、システムが簡単になる。

短所：セクタ間の個人情報を集めやすくなり、政府の監視強化につながる不安がある。

② SEPARATED MODEL

長所：サービス（セクタ）ごとに ID をつけるため、ひとつのセクタの ID がもれても、他のセクタの個人情報をアクセスできない。

短所：セクタごとに独立して個人情報が管理されるため、情報連携によるサービスの提供はできない。

③ SECTORAL MODEL

長所：オーストリアで開発された方法で、一つの ID からセクタごとの IDn を発生させる方式で、セクタ間の個人情報を集めることができるとともに、ひとつのセクタの ID がもれても、他のセクタの個人情報にはアクセスできない。

短所：一つの ID からセクタごとの IDn を発生させるシステムが複雑である。

④ LINK MODEL

長所：一つの ID と各セクタの IDn を対応づけるテーブル（ID 連携テーブル）を持つ。ひとつのセクタの ID がもれても、他のセクタの個人情報にはアクセスできない。

簡単なしくみで実現できる。

短所:ID 連携テーブルが漏洩した場合、全てのセクタの個人情報にアクセス可能になってしまう。

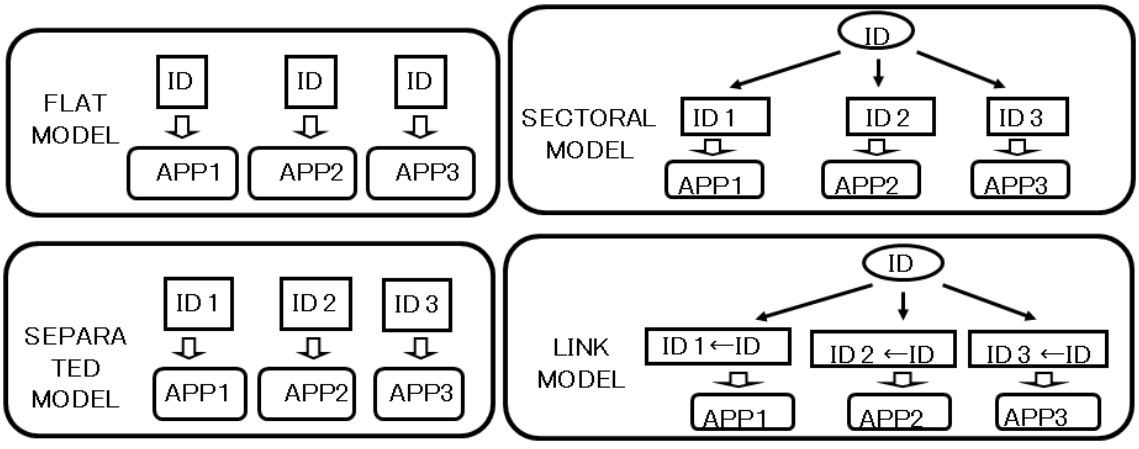


図 1.4.2 ID 管理モデル

つぎに、日本が採用している SEPARATED MODEL から FLAT MODEL、SECTORAL MODEL、LINK MODEL へ移行する場合の負荷について、以下に示す。

表 1.4.1 SEPARATED MODEL からの移行に伴う負荷

	長所	短所
FLAT MODEL	システムが簡単になる	国民に情報の漏洩、名寄せに対する不安感がある。 現システムからの移行のため、全てのデータへの ID の付け替えが必要。
SECTORAL MODEL	セクタ間の情報結合ができ、かつ、セクタ番号がもれても他のセクタに影響を与えない。	新たなシステムの導入が必要である。現システムからの移行負荷が大きい。
LINK MODEL	簡単なしくみで、 SEPARATED MODEL のセクタ間の情報結合が可能になる。	新たに、ID 連携テーブルが漏洩しないシステムの開発が必要。

次に、LINK MODEL の導入について、検討を進める。

4.4 LINK MODEL の導入検討

LINK MODEL について、4.2 で示した「国民 ID 導入のための 6 つの要件」への対応を検討するほか、表 1.4.1 で示した「新たに、LINK テーブルが漏洩しないシステムの開発が必要」への対応を検討した。

その結果、新たにこの ID 連携テーブルを「秘密分散技術を用いて分割管理する」ことにより、これらへ対応する方式を提案する。

4.4.1 秘密分散技術とは

秘密分散技術とは、秘密情報を分散化し、一般的には「シェア」と呼ばれる意味のない分散情報にすることによってセキュリティ強度を高める技術である。個々のシェアからは元の情報を一切類推することができないので、暗号化するのと同じように情報漏えいを防止することが可能である。また、暗号技術では、データや復号鍵を失くしてしまうと、復元ができなくなるといった問題もあるが、秘密分散技術を利用することにより、復元に必要なシェアの個数「しきい値」をあらかじめ設定しておけば、すべてのシェアを集めなくても復元することが可能であり、万が一の紛失や盗難、破壊の際にもデータ復旧に対応できる。さらに、本物のシェアでないと正しく復元できないということを利用し、シェアの真正性を検証することが可能なので、簡易な認証スキームへの応用も可能である。

秘密分散技術の一般的な利用方法として、情報漏えい対策への応用があげられる。一例を挙げると、社外秘にしておきたい電子ファイルや暗号鍵などを分散化して、セキュアに保管する方法である。この場合、分割されたシェアそのものは意味を持っておらず、また個々のシェアからは

オリジナルデータを全く類推不可能なので、情報漏えいを阻止することが可能になる。さらに「しきい値」の設定により、シェアの紛失の場合にも情報の復元が可能なので、データバックアップ機能を兼ねた情報漏えい対策として最適である。

このような秘密分散技術を用いて、以下のような「ID 連携テーブル」が考案される。

4.4.2 秘密分散技術を用いた ID 連携テーブル

まず、今回提案するシステム概要について説明を行い、次に「国民 ID 導入のための 6 つの要件」を満たすことができるか、考察する。

(1) システム概要

「国民 ID 導入のための 6 つの要件」を満たすシステムを構築するためには、セクタ間の情報交換が必ずひとつの組織を経由して行われることが必須であり、こうすることによって、アクセスコントロールやアクセスログを取得することができる。ここでは、秘密分散技術として、ID 連携テーブルを 3 つの「シェア」にし、2 つの「シェア」をもちいて ID 連携テーブルを復元する場合について説明する。

図 1.4.3 に、説明のための図を示す。

まず、構成について説明する。

① セキュリティ監視委員会

この委員会は、以下の構成と役割を持つ。

- 構成：オーストリアの方法が参考になる。オーストリアでは、各団体の推薦により、首相が任命する方法をとっている。
- 役割：システムの（部分）停止、セキュリティ監視センターの作業監視、新規サービスの認可

＜セキュリティ監視センター＞

セキュリティ監視委員会の元で、以下のシステムの監視を行う。

- 電子記録管理システム：個人情報がどこのセクタのどのシステムにあるかを管理する。
- 操作ログ管理システム：セキュリティ監視センターの要員が不正な行為を行っていないことを示すために、操作ログを記録する。この情報はセキュリティ監視委員会に提出する。
- アクセスログ管理システム：情報交換の要求や実施に関して個人情報をアクセスしたときのログを記録する。この記録は、本人に開示する。
- 秘密分散処理システム：ID 連携テーブルを 3 つの「シェア」にし、それぞれの「シェア」を、「本人」、「セキュリティ監視委員会」及び独立性の高い（場合によっては海外への設置も含む）「第 3 者機関」の管理下におく。

② 「シェア」の分散管理

例えば以下のような情報の管理に、秘密分散の「シェア」を利用する。

セクタ間で情報を提供するケース	利用する「シェア」
センシティブな情報の提供	本人、第 3 者機関
センシティブでない情報の提供	本人、セキュリティ監視委員会
本人が一度許可した情報の提供	本人、セキュリティ監視委員会 ただし、本人については自動回答とする

③　データ交換方式

エストニアの X-Road サーバ相当を用いることにより、アクセスコントロール、アクセスログを管理する［EST01］。

（ｉ）Security Server（SS）

あらゆるメッセージ（クエリー、サービス）をログに保存する特殊なファイアウォールとして構築される。つまり、長い時間が経過しても、過去の状況を復元できる。

アクセスコントロールは、組織と個人の 2 段階で行う。

（ⅱ）Adapter Server（AS）

XML 形式の X-Road メッセージを特殊なデータベース・クエリー言語（主に SQL）に変換し、クエリーの回答を XML 形式に戻すという、コンバーターの役割を果たしている。

(2) 動作概要

セクタ B がセクタ A にデータを要求する場合について説明する。

①　セクタ B がセクタ A の IDn の個人データをセキュリティ監視委員会に要求。

②　セキュリティ監視センターはセキュリティ監視委員会の指示により、IDn に対応するセクタ A の IDa を「シェア」2,3 を収集することにより作成。

③　セキュリティ監視センターは、IDa によりセクタ A より個人データを取得。

④　セキュリティ監視センターは、取得した個人データをセクタ B に送付。

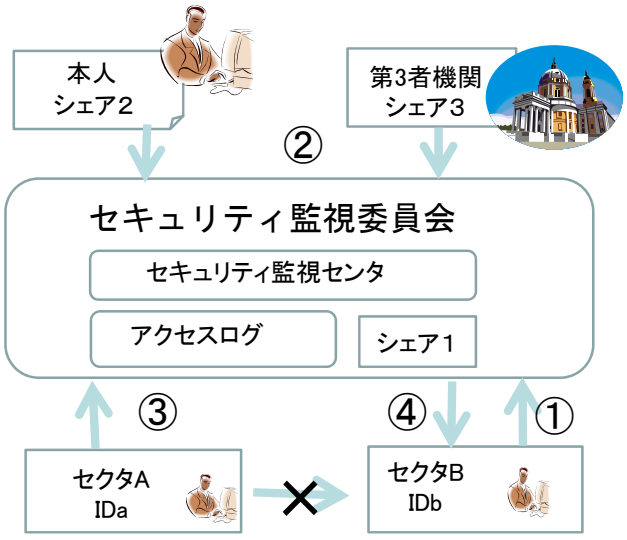


図 1.4.3 秘密分散技術を用いた ID 連携テーブル

(3) 「国民 ID 導入のための 6 つの要件」への考察

以下の要件ごとに提案のシステムが満たしているかを考察する。

［要件 1：個人情報の管理が明確で分かりやすい制度（法律やガイドライン）に従って運営されること。］

この要件を満たすためには、法律やガイドラインの形で、4.4.2(1)、(2)で説明した内容について、以下の項目について国民のわかりやすい言葉で明記する。

- 体制：セキュリティ監視委員会、セキュリティ監視センターの体勢と役割
- 利用する技術：秘密分散技術を含む、セキュリティを確保するために導入する技術を明記する。
- 運用：「シェア」をどのように本人に管理させるか等の詳細項目を明記する。
- 罰則：他のセクタから受け取った個人情報を保管するなどの、規則違反を行った場合の罰則を明記する。

［要件 2：個人情報の管理が中立的で信頼の高い組織によって運営されること。］

このシステムでは、セキュリティ監視委員会に依頼しなければ「ID 連携テーブル」を入手できないため、この要件は満たしている。

［要件 3：個人情報にレベルをつけあるレベルの個人情報については、セクタ間の情報提供は禁止すること。］

この用件については、別途個人情報保護法を改定するなどが必要である。

［要件 4：セクタ間の情報提供のしくみを明確にするとともに、個人情報を他のセクタに提供する時には本人への確認を基本とすること。］

「シェア」の一つの管理を本人とすることにより、この要件は満たしている。

［要件 5：本人の個人情報及び情報へのアクセスログをチェックでき、ミスやエラーを発見したときの対応方法が明確になっていること。］

このシステムでは、セクタ間の情報の受け渡しは ID 連携テーブルを用いることとしているため、必ずセキュリティ監視センターを経由する必要があるためすべてのアクセスログを保管し、本人に開示することができる。

［要件 6：国家権力の暴走が危惧される場合は、セクタ間の情報提供を停止できるようにすること。］

「シェア」の一つを独立性の高い（場合によっては海外への設置も含む）「第 3 者機関」の管理下におくことにより、この要件は満たせる。

4.5　今後の検討課題

現在の日本では、セクタを越えた情報の提供は実現してない。このため、確定申告においてはたとえ行政が管理しているデータであっても申請者が全て入力しなければならない。このような現実を打開するためには、各セクタが保管する個人データを連携するしくみが必要で、このためには国民 ID の導入が必須である。

本章では、「国民 ID 導入のための 6 つの要件」を整理し、この要件を満たす「秘密分散技術を用いた ID 連携テーブル」を提案した。

今後は、提案したシステムの実現性に向けた検討を続けるとともに、以下の項目についても検討を行う予定である。

(1) 国民 ID の詳細検討

生まれてすぐにつけたほうがいいのか／生涯固定がいいのか／秘密にする必要があるのか

(2) 提案システムの信頼性の確保

自身のデータチェックの仕組みは／自身へのアクセスログのチェックの仕組みは

(3) 事後処理では対応できないものは

ネットワークに接続しないデータは／最適なアクセスコントロールとは

［参考文献］

［榎並］榎並利博　「行政&情報システム」　2008 年 10 月号

［EST01］前田陽二、内田道久　「IT 立国エストニアーバルトの新しい風　2008 年 11 月　慧文社

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、昨年度に第一段階として、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。本年度も引き続き実施し、昨年と同一内容のアンケートに加えて、監査法人が紙保管を要請する理由を確認した。

1. 紙・電子文書管理の実態調査結果の概要

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に、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、アンケート形式で調査を行った。本アンケートでの文書管理の調査事例としては、昨年度に引き続き、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 2009 年 11 月 13 日から 12 月 11 日までである。

1.2 質問内容

表 2.1.1 に示す 3 つの観点から、アンケートを依頼した。その狙いは、次の通りである。

表 2.1.1 質問の観点と狙い

No.	観点	質問の狙い
1	全社	文書管理に関する全社的な組織、ルールの整備状況の確認
2	JSOX 文書	JSOX 文書の管理、利用ついて、「紙」、「電子」の取扱いの違いを含めた確認
3	IT インフラ一般	文書管理に関する IT インフラ、及び業務の電子化状況の確認

1.3 回収実績と業種

ECOM 会員企業 103 社にアンケートを依頼し、表 2.1.2 に示すように 29 社から回答を得た。

回答企業の業種については、表 2.1.3 に示すように、「情報」、「電力」、「サービス業」「機械」、「電気機器」、「銀行」、「通信」等であった。尚、JSOX への取組み状況については、表 2.1.4 に示すように、25 社がなんらかの形で、JSOX 対象もしくは関連企業となっており、その内、1 社を除き、24 社が JSOX への取組みを行っている。

表 2.1.2 ECOM 会員区分別　回答社数

	送付件数	回収件数	回収率
理事会員	6	2	33%
A 会員	41	13	31%
B 会員	56	14	25%
総数	103	29	28%

表 2.1.3 業種別　回答社数

No	業種	回収社数	No	業種	回収社数
1	情報	6	5	電気機器	3
2	電力	5	6	銀行	2
3	サービス業	4	7	通信	2
4	機械	3	8	その他	4

表 2.1.4 回答社の JSOX 関連状況

回答内容	回答数	比率
JSOX、及び米 SOX 対象上場企業	3	10%
JSOX 対象上場企業	13	45%
上場準備中	0	0%
JSOX 又は米 SOX 対象上場企業の関連会社	10	34%
上記に当てはまらない	4	14%
回答社数	29	

表 2.1.5 回答社の JSOX 取組み状況

回答内容		回答数	比率
1.	取組みを実施していない	1	4%
2.	取組み準備中	0	0%
3.	取組み中	0	0%
4.	ほぼ対応済み	3	12%
5.	対応済み	21	84%
回答社数		25	

1.4　アンケート結果サマリー

アンケート結果の特徴的なポイントをピックアップし、以下に記載する。

尚、【】内は関連する質問項目を示す。

1.4.1　全社に関する質問

(1) 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 1】

(2) 個人情報、情報セキュリティについては、規程の設定率は 9 割以上であるが紙文書、電子文書とも具体的な管理方法を示す規程、規則を設定している企業は 4 割以下である。【問 2】

1.4.2　「JSOX 文書」に関する質問

JSOX への取組みを実施している 24 社について、集計した。

(1) 文書化 3 点セット、整備状況 テスト報告書、整備状況 エビデンス、運用テスト テスト報告書、運用テストエビデンスの夫々に対し、社内原本の管理の仕方が異なっている。【問 4】

(2) 社内原本として、紙で保管している企業は、文書化 3 点セットについては 5 割、整備状況 テスト報告書については 6 割、運用テスト テスト報告書については 7 割であった、整備状況・運用テストのエビデンスについては、9.5 割であった。エビデンスに、紙保管を求めるケースが多い。【問 4】

(3) 紙を原本としている企業で、監査法人からの要請で行っている企業は 4～5 割であった。【問 4.5】

(4) 監査法人が紙保管を要請する理由としては、「監査法人が紙に慣れているから」が 4 割、「紙の方が、証拠性が高い」が 2～4 割、「貴社の電子管理規則の未整備」が 1～4 割であった。【問 4.6】

(5) 監査法人に紙提示を要請されている企業は、文書化 3 点セット、整備状況/運用テスト テスト報告書については 7 割、整備状況/運用テスト エビデンスについては、8.5～9.5 割とエビデンスの方が、要請率がやや高かった。【問 5】

(6) 監査法人が紙提示を要請する理由としては、「原本が紙だから」が 5～6 割、「監査法人が紙に慣れているから」が 2 割、「紙の方が、めくりが出来たり、見やすいから」が 1～3 割、「紙の方が証拠性が高い」が 1～3 割であった。紙を原本としたために、原本である紙を見せるよう要請しているケースが多い。逆に、言えば、電子文書を原本とすれば、紙提示を要請される可能性が大きく減る可能性を秘めている。【問 5.1】

(7) 電子データを原本としている場合、その原本性の確保手段としては、ワークフロー履歴を挙げる企業が 5～7 割、電子署名を挙げている会社は 1 社と少なかった。また、その他の手段を挙げている企業も 3～5 割あった。【問 7】

(8) 紙保管の基本的な管理方法として、入退出簿、保管キャビネットの施錠、保管キャビネットの施錠管理簿について確認を行ったが、「入退出簿あり」が 6～7 割、「施錠あり」が 4～7 割、「管理簿あり」が 1 割であり、まだ、管理レベルの底上げが不足していた。【問 9】、【問 10】、【問 11】

(9) 電子保管しているケースでのアクセス権管理では、アクセス権設定は全社行っているが、アクセス権設定のログ保管は 3～4 割、アクセスログ保管は 1～3 割であり、アクセスログ監査については 1 社に留まっていた。【問 13】

1.4.3 「IT インフラー般」に関する質問

(1) 「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 割に留まっており、前年と大差ない。【問 1】

(2) 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、備品購入申請、人事関連申請も電子化率が高く 7 割となっている。一方、稟議書、決裁書は一番遅れており、3 割である。尚、稟議書、決裁書以外は昨年と大差ないが、稟議書、決裁書については、回答社が昨年と異なっていることもあり、昨年の電子化率 6 割から後退している。【問 2】

1.5 アンケート結果から見る電子文書管理拡大への課題についての考察

紙で原本保管している企業の 5 割が、自主的に紙保管を選択している。また、残りの 5 割は監査法人からの要請によるものであり、電子文書管理の推進には「企業が電子管理を選択できるように環境を整備する」ことと「監査法人が電子を容認するように働きかける もしくは、仕掛けを準備する」ことの 2 面が必要である。

- 「企業が電子管理を選択できるように環境を整備する」については、「電子文書管理規程」の普及率が低いことなどから、実際にどのように電子文書を管理していけばよいかのガイドラインや事例が必要になる。
- 「監査法人が電子を容認するように働きかける もしくは、仕掛けを準備する」については、「監査法人が紙に慣れているから」、「紙の方が証拠性が高い」、「貴社の電子管理規則の未整備」について、具体的に、事例ベースで具体的な対応策や、誤解を解くなどの活動が必要であろう。【問 4.6】関連

2. H21 年度　紙・電子文書管理の実態調査結果の詳細

本章では、アンケート項目毎に以下の内容について記載する。

- アンケート質問内容
- アンケート質問　集計結果
  - ① 期待する姿：H20 年度　本 WG にて検討した民間企業での記録のあり方
  - ② 現実の姿の推定：H20 年度　本 WG にて推定した現実の姿
  - ③ アンケート結果（H21 年度）：H21 年度アンケート結果のまとめ
  - ④ 分析・意見等：アンケート結果に対する分析・意見等がある場合

2.1　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	41%
2. いいえ	15	52%
3. 回答なし	2	7%
アンケート回収社数	29	

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。

③ アンケート結果（H21 年度）：推定通り、CIO を設けている会社といない会社に差異はなかった。

【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。(複数回答可)

回答内容		回答数	比率
1.	文書取扱い規程	25	86%
2.	文書整理・分類基準	15	52%
3.	文書保管・保存基準	21	72%
4.	ファイル（紙文書）管理規程	14	48%
5.	機密文書管理規程	22	76%
6.	個人情報管理規程	28	97%
7.	示達・通達文書規程	12	41%
8.	電子文書管理規程	14	48%
9.	電子媒体取扱い基準	22	76%
10.	情報セキュリティ管理基準	29	100%
11.	その他	3	10%
12.	回答なし	0	0%
アンケート回収社数		29	

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、電子文書・電子媒体の運用に関する項番8、9については、2割程度しか保有しない。

③　アンケート結果（H21年度）：文書取扱い規程、個人情報管理規程、情報セキュリティ基準を設けている企業は9割以上あり、文書保管・保存基準、機密文書管理規程、電子媒体取扱い基準が次いで7割と多い。一方、電子文書管理規程、ファイル（紙文書）管理規程、示達・通達文書規程を設定している企業は4割である。

④　分析・意見等：推定より多いが、まだ、普及率は低い。

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	27	93%
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	0	0%
アンケート回収社数		29	

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。

③　アンケート結果（H21年度）：一部公開を含めると、全ての会社で、イントラネットでルールを公開している。

④　分析・意見等：推定より、進んだ段階にある。

問4　問2のルールの中での具体的な規程内容（複数回答可）

回答内容		回答数	比率（%）
1.	保管ファイル台帳の作成	14	48%
2.	ファイル管理者の設定	18	62%
3.	ファイル分類基準	11	38%
4.	ファイル背表紙記入基準	4	14%
5.	文書登録台帳の作成	13	45%
6.	文書保管・保存基準	25	86%
7.	文書廃棄基準	23	79%
8.	文書廃棄記録の義務付け	6	21%
9.	回答なし	2	7%
アンケート回収社数		29	

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：「ファイル管理者の設定」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。

③　アンケート結果（H21年度）：文書保管・保存基準、廃棄基準については8割以上の企業で設定されているものの、「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、設定している企業は4～6割であり、「ファイル背表紙」、「文書廃棄記録の義務付け」についての設定企業は1～2割と少ない。

④　分析・意見等：推定通り、紙の管理については具体的な管理手法の制定が不足している。

【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。

回答内容		回答数	比率（%）
1.	はい	24	83%
2.	いいえ	4	14%
3.	回答なし	1	3%
アンケート回収社数		29	

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。

③　アンケート結果（H21年度）：8割の企業で、管理ポリシー／ルールを決定している。

④　分析・意見等：設定率は推定よりやや低く、電子文書管理の基本であるだけに企業への啓蒙が必要である。

問6　電子文書の管理規則の中に以下のルールは入っていますか。(複数回答可)
なお、問6では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）	4	14%
2.	フォルダ管理者の設定	9	31%
3.	フォルダ分類基準	6	21%
4.	文書保管・保存基準	12	41%
5.	文書一覧表の作成（データベース化）	3	10%
6.	文書廃棄基準	12	41%
7.	文書廃棄記録の義務付け	6	21%
8.	文書毎への属性データ（メタデータ）の付与	4	14%
9.	回答なし	11	38%
問5　回答“1”の社数		29	

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：「フォルダ管理者の設定」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。
③ アンケート結果（H21 年度）：「フォルダの管理者の設定」についても、3 割しか規程されておらず、「文書保管・保存基準」、「文書廃棄基準を設定」を制定している企業が 4 割、その他の項目については2割以下であった。
④ 分析・意見等：推定を下回る段階であり、具体的な規則の設定が進んでおらず、企業が推進するにはガイドラインなどの普及が必要であると考える。

問7　アクセス権設定は誰が行いますか。(複数回答可)

回答内容		回答数	比率（%）
1.	全て情報システム部門	8	28%
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	10	34%
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	6	21%
4.	その他	4	14%
5.	回答なし	2	7%
回答社数		29	

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、管理者がアクセス権の設定はを実施する。
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。

③　アンケート結果（H21 年度）：項番 1 または項番 2 でアクセス権を設定している企業が 6 割あったが、項番 3（各部門に管理を任せている企業）も 2 割であった。

④　分析・意見等：推定通りではあったが、各部門任せになると JSOX のエビデンスとして、監査法人に電子文書を認めてもらうのは困難になっていると推測する。

問 8　2009 年度（2009 年 4 月～12 月）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	21%
2.	ない	21	72%
3.	回答なし	2	7%
回答社数		27	

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。

③　アンケート結果（H21 年度）：2009 年度だけでも、紙から電子情報への変更をおこなった企業は 2 割あった。

④　分析・意見等：各企業毎に、電子化の推進が進み始めている。

問 8-1、2、3

問 8 で「はい」と回答された方に、質問します。

①その具体的な業務内容、②切り替え時期、③切り替え理由

回答）

(1) ①文書の電子化（+外部保管）推進中、③検索性向上・省スペース等

(2) ①承認書電子化、②2009/4、③正確な記録の管理、業務処理の標準化

(3) ①情報セキュリティ事故報告書、②2009 年 10 月、③申請処理効率化のため

(4) ①業者への発注書、②2009/9、③効率化とコスト削減

(5) ①IT 統監査証跡、②2009/9、③保管スペース削減、検索高速化

(6) ①各種管理帳票、②2009/4、③環境負荷の削減

(7) 参考)　①契約書の電子化、②2007、③管理効率化の為

2.2　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	10%
2.	JSOX 対象上場企業	13	45%
3.	上場準備中	0	0%
4.	JSOX 又は米 SOX 対象上場企業の関連会社	10	34%
5.	上記に当てはまらない	4	14%
回答社数		29	

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	1	4%
2.	取組み準備中	0	0%
3.	取組み中	0	0%
4.	ほぼ対応済み	3	12%
5.	対応済み	21	84%
回答社数		25	

（以降は、問 1(5)上記に当てはまらないを 4 社と問 2(1)と取組みを実施していないを集計から外した。）

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	0	0%
2.	文書化作業全社展開済み	0	0%
3.	整備状況評価パイロットプロジェクト実施済み	0	0%
4.	整備状況評価全社展開済み	1	4%
5.	運用テストパイロットプロジェクト実施済み	0	0%
6.	運用テスト全社展開済み	2	9%
7.	有効性評価パイロットプロジェクト実施済み	1	4%
8.	有効性評価全社展開済み	19	83%
回答社数		23	

【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。(複数回答可)

【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	11	11	19	11	17
		52%	58%	95%	69%	94%
2.	ファイルサーバ	7	6	4	6	5
		33%	30%	20%	38%	28%
3.	汎用文書管理システム	1	0	2	0	0
		5%	0%	10%	0%	0%
4.	J-SOX用文書管理システム	6	8	2	5	4
		29%	43%	10%	31%	22%
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)		14	14	8	11	9
		67%	65%	40%	58%	50%
回答社数		21	19	20	16	18

J-SOX 文書管理システムの内訳

		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
4.	J－SOX 用文書管理システム	6	8	2	5	4
		29%	43%	10%	31%	22%
4-1.	いわゆる汎用文書管理ソフト	1	1	1	1	1
		5%	5%	5%	6%	6%
4-2.	市販 J-SOX 専用機能付き文書管理ソフト	2	2	2	1	0
		10%	11%	10%	6%	0%
4-3.	自社独自文書管理ソフト	3	1	1	2	1
		14%	5%	5%	13%	6%
回答社数		21	19	20	16	18

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。

1.　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。

③　アンケート結果（H21 年度）：「紙」を原本とする保管比率は、文書化3点セット、テスト報

告書、エビデンスによって、異なっている。

- 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、JSOX 用文書管理システムの使用比率は整備状況では、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。

④ 分析・意見等：文書の種類（文書化 3 点セット、テスト報告書、エビデンス）によって、紙を原本とする比率は異なっている。特に、文書化 3 点セット、テスト報告書については、紙を原本としている比率は推定よりやや多かったが、エビデンスについては推定を大きく上回った。エビデンスについては、紙で保管している傾向が強い。

問 4.1　運用テストのエビデンスをサンプルする元になっている帳票類の原本が紙の場合について

運用テストのエビデンスの原本管理方法について教えてください。（複数回答可）

回答内容		回答数	比率（%）
1.	紙帳票（原本）を複写し、複写物（紙）を原本として保管	17	89%
2.	紙帳票（原本）をスキャニングして、電子文書を原本として、保管	3	16%
回答社数		19	

③ アンケート結果（H21 年度）:「紙帳票（原本）を複写し、複写物（紙）を原本として保管」している企業が 9 割、「紙帳票（原本）をスキャニングして、電子文書を原本として、保管」している企業が 1.5 割であった。

④ 分析・意見等：項番 1 を選択している企業のうち、監査法人から紙保管を指定されている企業は 5 割であった。項番 2 のように、原本が紙の場合でも運用テストのエビデンスとしては、電子文書が容認されているケースもあるので、項番 1 を選択している企業にも電子化の検討をお願いしたい。

問 4.2　運用テストのエビデンスをサンプルする元になっている帳票類の原本が電子の場合について、運用テストのエビデンスの原本管理方法について教えてください。（複数回答可）

回答内容		回答数	比率（%）
1.	電子文書・画面（原本）を印刷し、印刷物（紙）を原本として保管。	14	88%
2.	電子文書・画面（原本）を抜き出し、電子文書を原本として、保管。	4	25%
回答社数		16	

③ アンケート結果（H21 年度）:「電子文書・画面（原本）を印刷し、印刷物（紙）を原本として保管」している企業が 9 割、「電子文書・画面（原本）を抜き出し、電子文書を原本として、保管。」している企業が 2.5 割であった。

④ 分析・意見等：項番 1 を選択している企業のうち、監査法人から紙保管を指定されている企業は 5 割であった。項番 2 のように、原本が電子の場合、運用テストのエビデンスとしては、電子文書が容認されているケースもあるので、項番 1 を選択している企業にも電子化の検討をお願いしたい。

問 4.3　JSOX 文書を紙で原本を保管している方に質問します。
社内参照用に、原本とは別に、電子文書で保管していますか。

		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.	はい	11	9	5	9	4
		73%	64%	28%	64%	22%
2.	いいえ	4	5	13	5	14
		27%	36%	72%	36%	78%
回答社数		15	14	18	14	18

③ アンケート結果（H21 年度）：文書化 3 点セットは 7 割の企業で電子文書でも保管、テスト報告書は 6 割の企業で、電子文書でも保管している。

④ 分析・意見等：紙を原本としている企業でも、利便性への配慮から、社内参照用に、電子文書で保管をしている企業が多い。

問 4.4　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。（複数回答可）

回答内容		回答数	比率
1.	承認機能（決裁機能）	5	63%
2.	文書作成、テスト等工程の進捗報告・確認機能	5	63%
3.	テスト実績、テスト結果、評価判定の Web 入力	5	63%
4.	テスト実績、テスト結果、評価判定の一覧表示	6	75%
回答社数		8	

問4.5　問4で、紙保管と回答した方に質問します。
監査法人から紙保管を要請されていますか。

		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.	はい	8	6	8	7	8
		50%	40%	50%	47%	50%
2.	いいえ	8	9	8	8	8
		50%	60%	50%	53%	50%
回答社数		16	15	16	15	16

③　アンケート結果（H21年度）：監査法人から紙保管を要請されている企業は5割である。

④　分析・意見等：H20 年度調査では、8 割の企業が監査法人から紙での提示を要請されていたことから、監査法人の要請は保管に対してのものか、提示に対してのものなのかを判別するため、本質問を加えた。問5のアンケート結果からも監査法人は、紙保管は要請しなくても紙での提示を要求するケースがあることがわかった。

問4.6　問4.5で、監査法人から紙保管を要請されていると回答した方に質問します。(複数回答可)

		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.	監査法人が紙に慣れているから	3	2	3	2	3
		38%	40%	38%	33%	38%
2.	紙の方が証拠性が高い	2	1	3	1	3
		25%	20%	38%	38%	38%
3.	貴社における電子保管の管理規則が未整備であるため	2	2	1	2	1
		25%	40%	13%	13%	13%
4.	その他	2	0	2	0	2
		25%	0%	25%	0%	25%
回答社数		8	5	8	6	8

③　アンケート結果（H21 年度）：監査法人が紙保管を要請する理由として、「監査法人が紙に慣れているから」という理由が3～4割と一番多い、次に、「紙の方が証拠性が高い」、「紙の方が証拠性が高い」などとする理由が2～4割、また、自社の「電子保管の管理規則が未整備」であることを理由に挙げている企業が、1～4割ある。

⑤　分析・意見等：電子保管の推進のために、監査法人には、「監査法人が紙に慣れているから」と「紙の方が証拠性が高い」などの意見が少なくなるよう監査法人にも紙・電子文書双方を

中立に見ていただき、電子文書への理解を高めて頂くこと、企業には、「貴社における電子保管の管理規則が未整備であるため」との指摘を受けないよう IT インフラの導入だけではなく、運用規則や運用手順の整備して頂くことが必要である。

問5　監査法人への提示方法を教えてください。(複数回答可)

		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	12	12	13	17
		68%	71%	86%	72%	94%
2.	システム画面	3	4	1	4	6
		16%	24%	7%	22%	33%
3.	電子ファイル	10	9	2	10	5
		53%	53%	14%	21%	14%
回答社数		19	17	17	18	18

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

③ アンケート結果 (H21 年度):「紙」提出している企業が多いものの、文書種別により、その比率は異なっている。文書化3点セット、整備状況/運用テストのテスト報告書は7割が「紙」提出であるが、エビデンスについては、「紙」提出の比率がさらに、高くなり、整備状況では8.5割、運用手テストでは9.5割となっている。一方、システム画面または電子ファイルについては、文書化 3 点セット、整備状況のテスト報告書では 5 割、他のケースでも 2～3 割監査法人への提示に使用されている。

④ 分析・意見等:現在の提示の仕方は、システム画面や電子ファイルで、監査法人に提示するものと紙で提示するものが同一企業でも混在していると思われる。

問5.1　問5で、紙提示を要請されている方に質問します。(複数回答可)

		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.	原本が紙だから	6	7	10	8	10
		50%	64%	63%	62%	63%
2.	監査法人が紙に慣れているから	3	2	4	2	3
		25%	18%	25%	15%	19%
3.	紙の方がめくりが出来たり見やすいから	2	1	5	2	2
		17%	9%	31%	15%	13%
4.	紙の方が証拠性が高い	2	0	0	0	1
		17%	0%	0%	0%	6%
5.	その他	1	2	2	2	2
		8%	18%	13%	15%	13%
回答社数		12	11	16	13	16

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。

③ アンケート結果（H21年度）「原本が紙だから」という理由が5～6割と多い、次に、「監査法人が紙に慣れているから」・「紙の方がめくりが出来たり見やすいから」を理由に挙げている企業が、2～3割ある。また、「**電子保管の管理規則が未整備だから。**」、「**押印や画面のハードコピー等のハンドリングが容易**」を理由にあげる企業もあった。

④ 分析・意見等：「原本が紙だから」という理由は、監査法人は写しではなく、原本を確認する傾向がある考える。この意味では、紙を原本として保管しているケースでは、紙原本の提出を求められることになる。逆に、原本を電子文書とすれば、電子文書での提示が容認される筈であるが、監査法人への電子文書での提示の残の課題は、「監査法人の紙への慣れ」「紙の方がめくりが出来たり見やすいから」、「紙の方が証拠性が高い」とする意見をいかに解決または打破していくかである。

【原本作成】

問6　紙を原本としている場合押印していますか。(複数回答可)

		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	4	7	6	11	10
		57%	70%	67%	100%	100%
2.	書類への審査・承認等多段押印有り。	3	4	4	5	5
		43%	40%	44%	45%	50%
回答社数		7	10	9	11	10

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。

③ アンケート結果(H21年度):文書化3点セットについては、押印は6割、整備状況のテスト報告書・エビデンスついても押印は7割に留まっており、管理状況の甘さが見える。一方、運用テストについては、全ての会社が押印している。これから、運用テストについては、管理が厳密で、文書化、整備状況については管理が緩やかであることが伺える。尚、審査・承認等の多段の押印については、4〜5割の企業で実施している。

④ 分析・意見等:証拠性や原本性を考えた時、「紙」への押印は必須と考えるが、その押印の運用が必ずしも正しく普及していないと思われる。審査・承認などの多段承認の比率も低く、電子化した方が、管理が確実になるのと考える。

問7　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	4	4	2	4	2
		67%	67%	50%	50%	100%
2.	電子署名	0	0	1	0	0
		0%	0%	25%	0%	0%
3.	PKIに基づくタイムスタンプ	0	0	0	0	0
		0%	0%	0%	0%	0%
4.	その他	2	2	2	4	0
		33%	33%	50%	50%	0%
回答社数		6	6	4	8	2

① 期待する姿:3点セット、テスト報告書については、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。

③ アンケート結果（H21 年度）：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。

④ 分析・意見等：まだまだ、電子データの原本性確保の配慮は十分ではない。

【紙保管】

問 8　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	10	5	10	5	10
		77%	38%	59%	38%	59%
2.	部署別等分散管理	0	1	2	1	2
		0%	8%	12%	8%	12%
3.	事務局集中、部署別等分散管理 混在	3	7	5	7	5
		23%	54%	29%	54%	29%
回答社数		13	13	17	13	17

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

③ アンケート結果（H21 年度）：文書化 3 点セットは「事務局に集中管理」の企業が 8 割と期待する形に近い。テスト報告書については、「事務局に集中管理」が 4 割、「事務局集中、部署別等分散管理 混在」が 5 割となっている。エビデンスについては、「事務局に集中管理」が 6 割、「事務局集中、部署別等分散管理 混在」が 3 割となっている。

④ 分析・意見等：紙管理の場合、文書化は事務局中心で実施し、集中管理しやすいが、整備状況評価や運用テストとなると現場部門での確認作業が増えるので、管理が分散しがちである。この傾向は今回の結果からも明らかであり、集中管理には、紙管理を継続するよりも、電子保管を進めた方がよいと考える。

問9　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	10	7	11	7	11
		77%	64%	61%	64%	65%
2.	入退出簿なし	0	1	4	1	3
		0%	9%	22%	9%	18%
3.	入退出簿あり、なし 混在	3	3	3	3	3
		23%	27%	17%	27%	18%
回答社数		13	11	18	11	17

①　期待する姿：「保管場所への入退出管理」を管理している。

②　現実の姿の推定：「保管場所への入退出管理」は5割程度である。

③　アンケート結果（H21年度）：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おり、推定通りであった。

④　分析・意見等：「入退出管理」の重要性は認識されているものの運用の徹底にまで至っていない。

問10　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	5	5	9	5	9
		45%	42%	47%	42%	47%
2.	施錠なし	2	2	2	2	2
		18%	17%	11%	17%	11%
3.	施錠あり、なし 混在	4	5	8	5	8
		36%	42%	42%	42%	42%
回答社数		11	12	19	12	19

①　期待する姿：「保管キャビネトもしくはファル棚の施錠」をしている。

②　現実の姿の推定：「保管キャビネトもしくはファル棚の施錠」は9割程度である。

③　アンケート結果（H21年度）：「施錠あり」の企業が4割～5割で、「施錠あり、なし 混在」の企業が4割であった。

④　分析・意見等：「施錠」の重要性は認識されているものの運用の徹底にまでは至っていない。

問11　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.	施錠管理簿あり	0	0	2	0	1
		0%	0%	11%	0%	6%
2.	施錠管理簿なし	9	9	13	9	13
		82%	82%	68%	82%	72%
3.	施錠管理簿あり､なし 混在	2	2	4	2	4
		18%	18%	21%	18%	22%
回答社数		11	10	15	11	18

①　期待する姿：保管キャビネトもしくはファイル棚の施錠を「施錠管理簿」で管理している。

②　現実の姿の推定：「施錠管理簿」を利用する企業は3割程度である。

③　アンケート結果（H21年度）：「施錠管理簿」を利用する企業は0～1割であった。

④　分析・意見等：「施錠管理簿」の必要性すら認識されていていない状況である。

【電子保管】

問12　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	8	9	3	9	3
		89%	90%	50%	90%	50%
2.	部署別等分散管理	0	0	1	1	1
		0%	0%	17%	0%	17%
3.	全社集中、部署別等分散管理 混在	1	1	2	1	1
		11%	10%	33%	10%	33%
回答社数		9	10	6	10	6

①　期待する姿：全て、「全社集中管理」を実施。

②　現実の姿の推定：殆どの企業が「全社集中管理」を実施。

③　アンケート結果（H21年度）：文書化3点セット、テスト報告書については、「全社集中管理」を9割の企業で実施、エビデンスについては、5割の企業で実施。

④　分析・意見等：全社集中管理の方が、管理が行き届くので、エビデンスについても「全社集中管理」が進むことを期待する。

問13　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	10	10	9	11	7
		100%	100%	100%	100%	100%
2.	アクセス権設定のログ保管	5	5	3	5	2
		45%	27%	33%	45%	29%
3.	アクセスログ保管	2	3	1	3	1
		18%	30%	11%	27%	14%
4.	アクセスログ監査	0	1	0	1	0
		0%	10%	0%	9%	0%
回答社数		16	10	9	11	7

① 期待する姿：全ての会社で、「アクセス権の設定」、「アクセスログ権設定のログ保管」、「アクセスログ保管」、「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」は行っているが、「アクセスログ権設定のログ保管」、「アクセスログ保管」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。

③ アンケート結果（H21年度）：全ての会社で、「アクセス権の設定」は行っているものの、「アクセスログ権設定のログ保管」は3～5割、「アクセスログ保管」は1～3割と推定より実施企業が少なかった。「アクセスログ監査」を実施している企業は1社に留まった。

④ 分析・意見等：電子文書管理を推進していくためには、「アクセスログ権設定のログ保管」、「アクセスログ保管」、「アクセスログ監査」の重要性を各企業に認識して頂くことが必要である。

問14　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	6	29%
2. いいえ	15	71%
回答社数	21	

③ アンケート結果（H21年度）：3割の企業で他に活用している。

④ 分析・意見等：JSOX文書を社内業務改善などの他の用途に利用している企業が少ない。

問15　問14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。

2.3　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	1	4	9	13
	4%	14%	32%	46%
部門文書管理システム	5	10	0	4
	18%	36%	4%	14%
全社共有サーバ	1	5	8	14
	4%	18%	29%	50%
文書管理システム（ECM等も含む）	5	9	1	7
	18%	32%	4%	25%
回答社数	28			

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状況に留まっている。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。

③ アンケート結果（H21 年度）：「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	23	79%
2.	経費清算	21	72%
3.	勤怠管理・勤怠申請	28	97%
4.	人事関連申請	23	79%
5.	備品購買申請	20	69%
6.	稟議書、決裁文書	9	31%
回答社数		29	

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

③ アンケート結果（H21 年度）：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。

④ 分析・意見等：推定通り、「稟議書、決裁文書」の電子化が遅れている。内部統制的な観点からは、「稟議書、決裁文書」の電子化は、内部統制の透明性の強化につながると考えるので、各企業には推進を目指して欲しい。

第３部　電子署名普及のための標準化提案

長期署名プロファイルが2008年3月20日にJIS†として発行されてからほぼ2年が経過する。

†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

第3部では、この間の長期署名に関連する標準化動向について紹介する。1章では、即刻上記JISを改定すべきと考えられる事項を改定案としてまとめた。2章では、長期署名プロファイルのISO標準化活動の状況を紹介する。3章では、ISOで標準化が進められているPDF長期署名(PAdES)を中心に、将来のJISの改定に結びつく可能性のある関連技術に対する標準化動向をいくつか紹介する。一方4章では、長期署名プロファイルが利用される可能性のある電子記録の長期管理について紹介する。

1. 長期署名プロファイル JIS 改定案

1.1 証拠記録の JIS への追加案

IETFが発行するRFC4998においてERS（Evidence Record Syntax、証拠記録）がASN.1により定義されている。これは、ECOMの平成20年度報告書「電子署名普及に関する活動報告2008(H21.3)」の「第3部 4. ERSのJIS長期署名プロファイルへの導入案」で示したとおり、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（証拠記録）の構文である。同報告書では、JIS X 5092:2008の表6に示される「(改ざん検知を可能とする情報)」にアーカイブタイムスタンプと並ぶ任意選択の要素として証拠記録を併記する形で追記することを、また、JIS X 5093:2008の表5に示される「(改ざん検知を可能とする情報)」にアーカイブタイムスタンプと並ぶ任意選択の要素として証拠記録を併記する形で追記することを提案した。

ASN.1でERSを定義するRFC4998の仕様検討と並行して、XMLでERSを定義する「Extensible Markup Language Evidence Record Syntax」が議論され、そのドラフト版が draft-ietf-ltans-xmlersとして第0版から第4版の計5版が公開されているが、2009年8月3日付けの最終版である draft-ietf-ltans-xmlers-04 は既に2010年2月3日に失効しており、その後ドラフトは公開されていない。このような状況を考慮し、ERSのJISへの追加案ては2008年度報告書記載のままとする。

1.2 その他の JIS 改定案

JIS X 5092:2008（CAdES）の表6において、全証明書参照情報群及び全失効参照情報群の要素を「必す（必須)」としている。一方、JIS X 5093:2008（XAdES）の表5では同要素をいずれも任意選択としている。これらの相違は参照するETSI規格の記述の相違に起因する。両JISでは証明書や失効情報の実データ（証明書群及び失効情報群の両要素）を必す（必須）としているため、全証明書参照情報群及び全失効参照情報群の両要素を必す（必須）とする必要はない。従って、JIS X 5092:2008においても両要素を必す（必須）ではなく任意選択に変更することを提案する。

2. 長期署名プロファイル ISO 標準化活動の進捗状況

電子署名普及 WG では、TC154 国内審議委員会を通じて、ISO/TC154 にて UN/EDIFACT や ebXML などの記録管理に応用できる長期署名フォーマットプロファイルの標準化を行う計画を進めている。

2008 年 11 月にはベルギーで開催された ISO/TC154 総会にて、長期署名プロファイルに関するニューワークアイテム提案（NWIP）を行った。そして、2009 年 7 月にドイツ、チェコ、中国、ベトナム、そして、日本の積極的参加 5 カ国が揃い、ニューワークアイテム（ISO/NP 14533 Long Term Signature profiles for EDI Data and Electronic Documents）として承認された この 5 カ国から代表者として選ばれたエキスパートで構成されたグループで長期署名プロファイルの草案作成を行い、2010 年 1 月にはワーキングドラフトとして委員会に提出した。2010 年 3 月現在では委員会原案（Committee Draft）の投票の段階にある。

長期署名プロファイルのワーキングドラフトは次の 2 つのパートから構成されている。

- ISO 14553-1 Information technology - Long term Signature Profiles - Part 1: Long term Signature Profiles for CAdES
- ISO 14553-2 Information technology - Long term Signature Profiles - Part 2: Long term Signature Profiles for XAdES

これらのドラフトは JIS X 5092:2008、JIS X 5093:2008 をベースとしている。しかし、ワーキングメンバーであるドイツから、本ワークアイテムのスコープが CAdES や XAdES のみに限定しているため、一つの署名ごとに一つのアーカイブタイムスタンプの方式では ISO 14721 のアーカイブシステムのモデル[1]への適合性について疑問があり、RFC4998 の Evidence Record Syntax (ERS) についてもスコープに入れて欲しいとのコメントがあった。

また、他のメンバーからは PAdES のプロファイルも検討したいとのコメントもあった。しかし、両者のコメントはワーキングドラフト提出の直前であったことと、ERS や PAdES のプロファイルの原案自体がまだない状況であることから、現段階では CAdES と XAdES のみの構成でワーキングドラフトとした。一般的な ERS のプロファイル策定は行っていないものの、電子署名普及 WG では、CAdES や XAdES へ ERS のタイムスタンプを格納するケースについては長期署名プロファイルの JIS 規格改定案として検討を続けていたため、その内容を今回のワーキングドラフトへ反映させることとした。将来的に ERS そのもののプロファイルや PAdES のプロファイルをどのように取り扱うか検討が必要だろう。

[1] ISO 14721 "Space data and information transfer systems - Open archival information system - Reference model"

3. 関連技術の標準化動向

3.1 PAdES（PDF 長期署名）の概要、経緯、動向

3.1.1 PDF 長期署名の経緯と動向

PAdES（PDF Advanced Electronic signatures）の標準化は、2005 年 10 月に標準化された ISO 19005-1(PDF/A)の次のバージョンである ISO/WD 19005-2 の検討が始まったことが発端となった。ISO 19005-1 は PDF1.4 を参照しており、署名に関する制約は特にはなかったが、ISO/WD 19005-2 は、Adobe 社の PDF1.6 仕様（その後 PDF1.7 にバージョンアップ）を参照していたことから、署名の観点から 2 つの問題があった。一つは、PDF1.6 仕様内に定義されている署名仕様が、当時既にデファクトとなっていた RFC シリーズによる署名仕様と異なる点があり互換性がなかった（つまり独自仕様であった）こと、今一つは、PDF/A（PDF Long Term Preservation）と謳いながら、長期署名対応の考慮がなされていなかったことである。具体的には、PDF の署名は内包(embedded)型の署名であり、且つ署名範囲を示すパラメータ（バイトレンジ）自身が署名対象となっているため、一旦署名されると、その後は、PDF に内包された署名に検証情報やアーカイブタイムスタンプを格納できないという問題があった。

ECOM では、平成 17 年度（2005 年度）の検討で、PDF1.6 仕様に極力手を加えずに PDF に内包された署名部分をいかに拡張するかの検討を行い、幾つかの対処案を挙げた（平成 18 年 3 月発行の報告書参照）。

平成 18 年度（2006 年度）は、対処案の実現性評価を行い、最終的に、検証情報やアーカイブタイムスタンプを格納した長期署名データを増分更新により添付ファイルとして付加する方式を、ECOM 案としてまとめた。この結果は、2007 年 1 月に開催されたコスタメサ会議に入力され、PDF における長期署名の必要性が認識されることとなった。

一方、PDF の本体である PDF1.6 について、2007 年の前半に大きな動きがあった。2007 年の 2 月に Adobe 社は、PDF 仕様の ISO 化をはかるべく、PDF 仕様を AIIM に譲渡した。その年の 5 月までに Acrobat 依存の仕様を汎用的な表現に書き換え、ISO 標準として体裁を整えたドラフトができた。これと並行して、長期署名の組み込みについて議論が行われ、長期署名を含む署名仕様に関しては、PDF/A、PDF/X、PDF/E などの PDF シリーズに共通の、長期署名を含む独立した仕様を作成することになった。

体裁を整えられた PDF1.7 ドラフトは 2007 年 7 月 2 日に、DIS 32000 としてファストトラックで投票にかけられ、12 月 2 日に投票が締め切られた。この投票に対し、フランスは、署名が Adobe 社固有の仕様であり、長期署名も考慮されていないことで反対投票を行った。この時、日本は、前述のように別仕様にすることに合意していたので、賛成投票を行っている。翌年開催された表決解決会議（Ballot resolution meeting）で、長期署名の発案者であるデニスピンカス氏とフランス AFNOR 代表として参加し、Adobe 仕様を、デファクトである RFC シリーズによる署名仕様に置きかえるべきであると主張して、PDF の提唱者であり ISO のエディタであるジムキング氏が大激論を行った末、長期署名を含む RFC シリーズによる署名仕様は、ISO の次の version に入れる

ことで、決着を見た。この結果、DIS 32000 は ISO 32000-1 として ISO 標準となり、その年の 7 月 1 日に発行された。また、長期署名を含む PDF 仕様は、ISO/WD 32000-2 として検討が開始されることになった。同年 3 月には、ISO と、ピンカス氏がメンバとなっている ETSI との間で PDF の長期署名を協同で検討することが合意され、EC の資金援助を受けて、3 年計画で ETSI の PAdES の特別タスクフォース（STF）が立ち上げられた。この STF で、ECOM 案を含む 3 方式の評価が行われ、最終的に PDF 本体に手を入れることが決まり、1 年半の開発機関を経て、2009 年 6 月に STF の成果が ETSI 標準 TS 102 778 として承認された。この成果は、2009 年 10 月の TC171/SC2 オーランド会議にインプットされ、ISO/WD 32000-2 に組み込まれた。現在は、ISO/CD 32000-2 として投票期間中にある。2011 年には標準化される見込みである。

3.1.2 PAdES 概要

PDF 長期署名の新しいプロファイルである PAdES(PDF Advanced Electronic Signature Profile)は、XAdES（ETSI TS 101 903 / JIS X 5093）や CAdES（ETSI TS 101 733 / JIS X 5092）と同じく現在 ETSI（欧州電気通信標準化機構）により ETSI TS 102 778 として公開されている。ETSI では PAdES プロファイルを ISO にフィードバックしており、いずれ ISO 32000-2（PDF2.0）へ反映される予定になっている。また XAdES/CAdES と同じく JIS 化についても検討がされるべきだろう。

本章では他の長期署名プロファイルと比較して PAdES の位置付けと、ETSI TS 101 778 の資料よりプロファイルの概要をまとめる。なお詳細な PAdES 仕様に関しては、ETSI の ETSI Publications Download Area（http://pda.etsi.org/pda/queryform.asp）にユーザ登録して「PAdES」にて検索すれば無料で PDF ファイルにて仕様を入手できるのでそちらを参照頂きたい。

3.1.2.1 PAdES 仕様構成

PAdES の仕様は現在 ETSI TS 102 778 の 1 から 5 までの 5 パートにより構成されている。Part1 が全体の説明であり、Part2～4 までが PDF 本体に対する長期署名プロファイルの説明であり、Part5 は PDF に埋め込まれた XML に対する長期署名プロファイルの説明となっている。

Part1:	**PAdES Overview**	a framework document for PAdES PAdES 全体の概要を解説している。最初に読むべきパート。
Part2:	**PAdES Basic**	Profile based on ISO 32000-1 既存の PDF 仕様（ISO 32000-1/PDF1.7）に基づく署名プロファイル。署名プロファイルとして PKCS#7（CMS）を利用。
Part3:	**PAdES Enhanced**	PAdES-BES and PAdES-EPES Profiles 署名プロファイルとして CAdES-BES/CAdES-EPES/CAdES-T を使った署名プロファイル。

Part4:	**PAdES Long Term**	PAdES-LTV (Long Term Validation) Profile 長期署名の為に新たに加えられた PDF 独自のオブジェクトを使って検証情報と、ドキュメントタイムスタンプを、PDF に埋め込む為の長期署名プロファイル。
Part5:	**PAdES for XML Content**	Profiles for XAdES signatures PDF に添付された XML ドキュメントや、XFA (XML Forms Architecture) として埋め込まれた XML フォームに対して、XAdES を使った長期署名プロファイル。

図 3.3.1 PAdES 仕様のパート構成

前ページのパート構成を関連と生成される PDF の種類からまとめると以下のようになる。なお正確には例 3 の PAdES for XML Content ベースの長期署名 PDF のうち Part4：PAdES Long Term を利用するのは XFA として埋め込まれる XML フォームの場合となる。XML の添付ファイルの場合には XAdES-X-Long や XAdES-A が使われる。

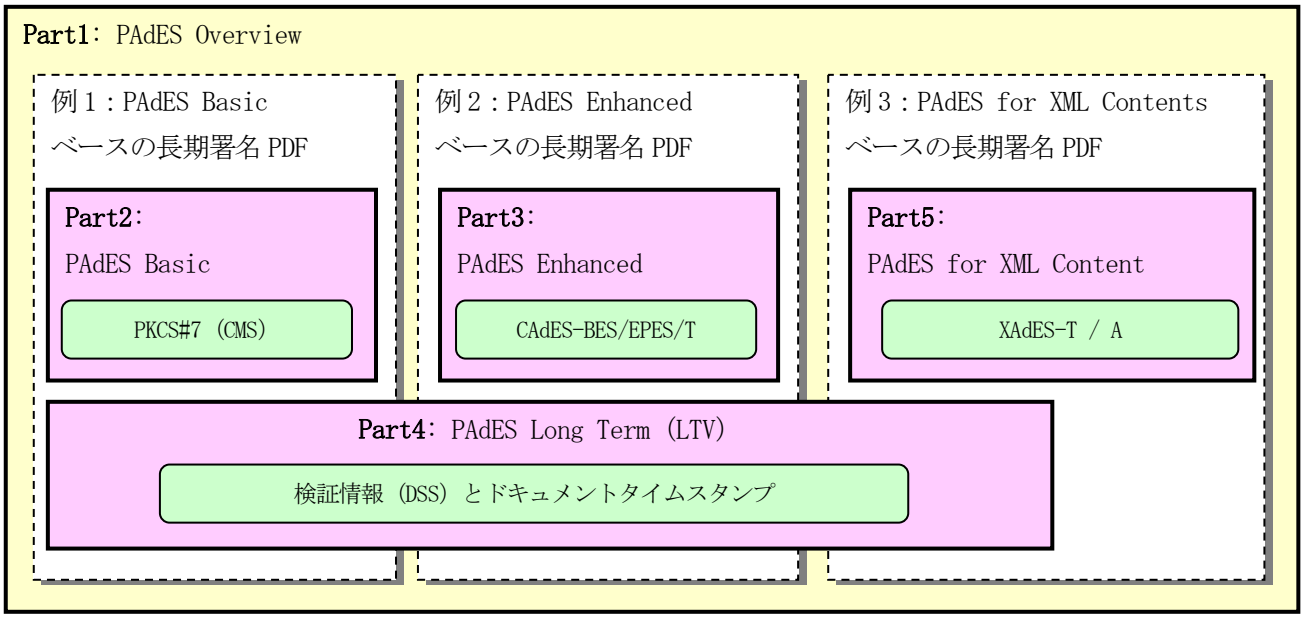


図 3.3.2 PAdES 仕様と PDF ファイルの関係

この関係図から興味深いのは Part3 では CAdES を、Part5 では XAdES を使っているにも関わらず、ES-X-Long と ES-A の部分に関しては Part4 の PAdES Long Term の仕様を使っている点がある。PAdES では、Part5 の XML の添付ファイルのケース以外では、検証情報は全て Part4：PAdES Long Term で規定されている新たな PDF オブジェクト DSS (Document Security Store) に保管される。

また PDF 仕様としてのドキュメントタイムスタンプ辞書は、基本的に現在の PDF 署名の署名辞書とほぼ共通仕様になっている。その意味では ETSI TS 102 778 には明記されていないが、署名

無しでドキュメントタイムスタンプのみを付与することも可能だろうと予想される。つまり電子署名を付与するようにタイムスタンプだけを付与できる。もしドキュメントタイムスタンプのみを付与することが可能になると、知的財産保護の目的等への利用も考えられる。可能であれば今後このような運用形態も提案して行きたいと考えている。

3.1.2.2 なぜ PAdES が必要なのか

ISO 32000-1 には PKCS#7 を署名プロファイルとした PDF 署名の仕様が存在する。PKCS#7（RFC 2315）は CAdES のベースの CMS（RFC 3852）の更にベースとなった仕様である。CAdES を PKCS#7 の代わりに署名プロファイルとして利用すれば長期署名化ができるように思える。例えば XML 形式である ODF や OOXML に関しては同様に XmlDsig の代わりに XAdES を使えば長期署名化は基本的には可能となる。しかし PDF 署名には PKCS#7 の代わりに CAdES を単純に採用できない理由が存在する。

PDF 署名では署名対象の範囲を署名辞書の ByteRange エントリーにより指定される。以下に示すように通常は開始位置と長さをペアにして、PKCS#7 部の前後の領域を署名対象として指定することになる。

ByteRange [開始位置 1　長さ 1　開始位置 2　長さ 2]

開始位置はファイルの先頭からの直接位置指定となっている。ByteRange 自体も署名対象となっているので署名後に変更はできない。つまり署名時に決められた PKCS#7 用の領域は、後から拡大することができない。長期署名の仕様は検証情報とアーカイブタイムスタンプを重ねることで実現しているので、署名用の領域サイズが拡大できないと実現ができない。この為に CAdES-A を利用する事ができない点が問題となる。PAdES の仕様ではこの問題を、DSS オブジェクト（検証情報）とドキュメントタイムスタンプ（アーカイブタイムスタンプ）として、ファイルの最後に増分更新することで回避している。

3.1.2.3 PAdES と XAdES/CAdES との比較

XAdES と CAdES は細かな差異はあるが長期署名の仕組みとして大きな違いは無い。しかしながら PAdES のプロファイルはアーカイブタイムスタンプや、そもそも基本となるフォーマットが PDF と言う文書フォーマットである点等、XAdES/CAdES には無い特長や差異がある。以下に簡単にまとめる。

プロファイル	PAdES	XAdES	CAdES
ベース フォーマット	PDF (テキスト＋バイナリ)	XML (テキスト)	ANS.1/BER/DER (バイナリ)
ベース署名 プロファイル	PDF 署名 (ISO 32000-1)	XML 署名 (W3C 勧告)	CMS 署名 (RFC3852)
依存（参照）する プロファイル	CAdES (XAdES)	なし	なし
ES-A への対応	ドキュメント タイムスタンプ (文書全体が対象)	アーカイブ タイムスタンプ (指定順に要素を結合)	アーカイブ タイムスタンプ (指定順に要素を結合)
外観付き署名仕様	○ あり	× なし	× なし
採用可能な 上位プロファイル	(PDF)	ODF/OOXML 等	S/MIME 等

図 3.3.3 PAdES / XAdES / CAdES の比較

PAdES のベースとなっている PDF 署名では、外観付きの可視署名と外観なしの不可視署名の 2 種類が選べる。近年では署名や証明書のビジュアル化の検討も進んでおり、外観を付けられることは有利にはたらくかもしれない。XAdES/CAdES ではこれらを採用した文書フォーマット（ODF や OOXML 等）のレベルで、外観を付ける場合には対応をする必要がある。

3.1.3 PAdES 仕様概要

ここでは PAdES 仕様（ETSI TS 102 778）の構成に従って PAdES 仕様の概要をまとめる。

3.1.3.1 パート 1：PAdES オーバービュー

3.1.3.1.1 PDF 署名

ISO 32000-1（PDF1.7）では PDF 署名を実現する為に、署名辞書（Type エントリが Sig）と呼ばれるデータ構造が規定されている。署名辞書の ByteRange エントリーにより署名対象の範囲が決められる。

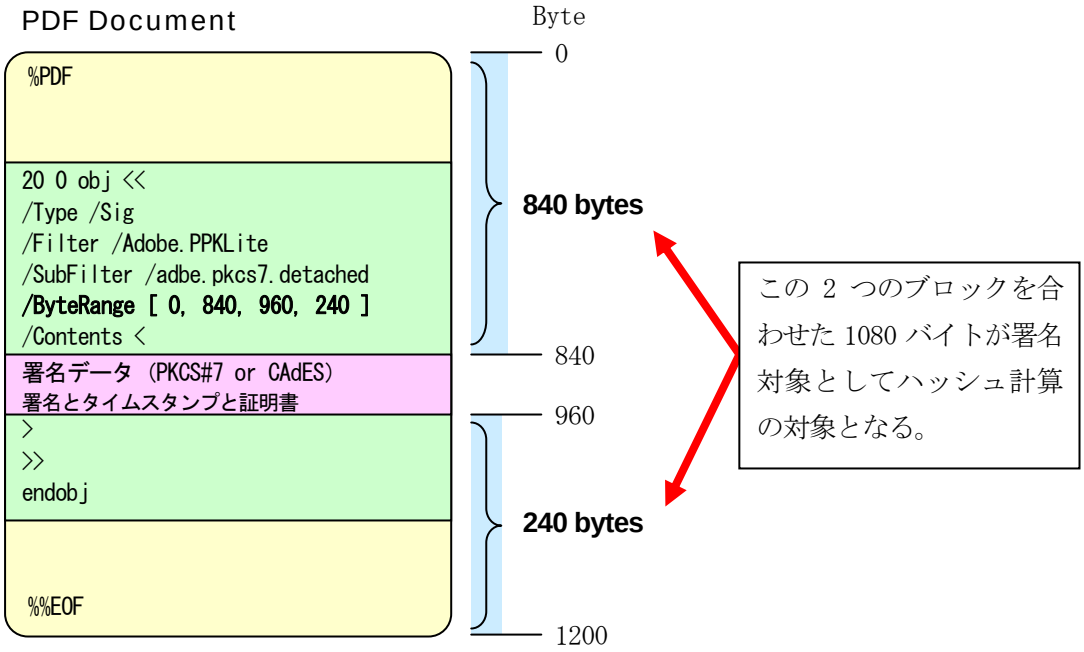


図 3.3.4 PDF 署名の構造例

この構造は PAdES Basic でも PAdES Enhanced でも共通となる。Contents エントリーに格納される署名データが、PAdES Basic では PKCS#7 に、PAdES Enhanced では CAdES になる。また署名辞書には Filter エントリと SubFilter エントリがあり SubFilter に、PAdES Basic では adbe.pkcs7.detached か adbe.pkcs7.sha1 を、PAdES Enhanced では ETSI.CAdES.detached を指定する必要がある。

PDF 署名のタイプとしては標準の PDF 署名以外に、MDP (Modification detection Permissions) と呼ばれるタイプもある。MDP 署名を行うと、署名者が文書を修正することについての許可 (Permission) を与えることができる。許可は「変更を許可しない」「フォームフィールドの入力と署名フィールドに署名を許可」、「注釈の作成、フォームフィールドの入力と署名フィールドに署名を許可」の 3 段階が指定可能となる。

3.1.3.1.2 PDF シリアル署名

PDF 署名は増分更新と呼ばれる仕組みによってバージョンを更新することでシリアル署名を実現している。増分更新とは既存の PDF 構造に新たな情報を追加して行く仕組みとなる。

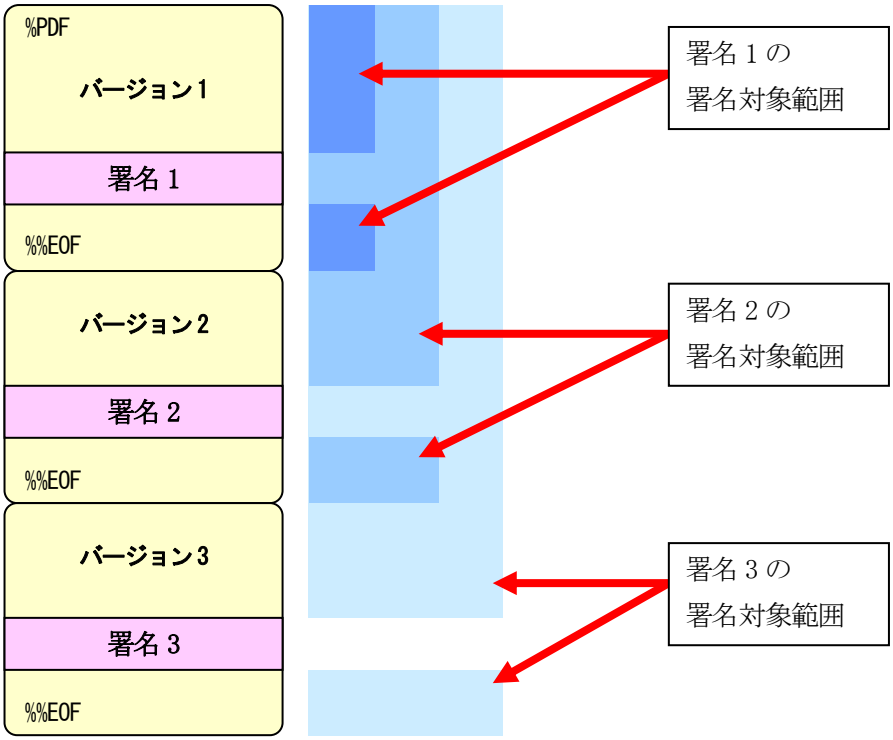


図 3.3.5 PDF シリアル署名の構造例

PDF シリアル署名の仕組みは、PAdES Basic と PAdES Enhanced にて利用可能となる。

3.1.3.1.3 ISO 19005-1：2005（PDF/A-1）

PDF には長期保管の為にフォントやカラープロファイルの埋め込み等をプロファイルとして定義した PDF/A（ISO 19005）仕様がある。長期保管と言う意味では長期署名とは深い関係のある仕様だと言える。現在の PDF/A-1（ISO 19005-1）はベースとして ISO 以前の Adobe PDF 1.4 の仕様を利用している為に、ISO 32000-1 の PDF 署名の全ての仕様は含まれない。PDF/A-2（ISO 19005-2）として ISO 32000-1（PDF1.7）をベースにまもなく更新される予定になっている。PDF/A-2 では PAdES の仕様が使えるようになるだろう。

3.1.3.1.4 PDF の中で使われる XML 文書

PDF の仕様では XML 文書を PDF の中に含めることができる。XML 文書の利用方法としては、添付ファイルとして生の XML 文書を埋め込む方法と、XFA Forms の入力フォームとして埋め込む方法、の 2 種類がある。PAdES for XML Content にて XAdES を使うことで長期署名に対応ができる。

3.1.3.2 パート 2：PAdES Basic（ISO 32000-1 に基づく PAdES）

PAdES Basic は、ISO 32000-1:2008（PDF 1.7）に対して新しい要素を規定することなく必須となる項目を定めたプロファイルとなっている。従って ISO 32000-1 の PDF 署名に対応している Adobe Acrobat 8/9 や Reader 8/9 をはじめとする PDF ビューワソフトにて表示や検証することが可能である。

PAdES Basic では PKCS#7 形式の署名データを利用するが、ISO 32000-1 では既に RFC 3161 形式のタイムスタンプトークンを PKCS#7 に含むことができる。以下主な要求事項をまとめる。

1. ISO 32000-1 仕様の 12.8 に準拠した PDF 署名に従うこと（shall)。

2. PDF 署名はその文書自身に埋め込まれること（shall)、ByteRange エントリがファイル全体を指し署名辞書に含まれること（shall)、ただし PDF 署名自体は除外する。

3. PDF 辞書は PKCS#7 のバイナリデータオブジェクトとして署名辞書の Contents エントリの中に存在すること（shall)。

4. PKCS#7 オブジェクトは RFC 2315 に準拠していること（shall)、最低 X.509 形式の署名証明書を含むこと（shall)。

5. PDF 署名にタイムスタンプと検証情報を含むべきである（should)、ここで言う検証情報とは証明書チェーンを構築する証明書であり、署名前に取得と確認されていること（shall)。更に検証情報は PDF 署名の signed attribute に含むこと（shall)。

6. もし提供されるなら任意の検証情報を PDF 署名の signed attribute に含むこと（shall)。

7. 署名証明書に関連した RFC 3281 の属性証明書を含むことは推奨されない(not recommended)。

8. 各 PDF`署名において署名者は 1 つ（SignerInfo は 1 つ）であること（shall)。

9. PDF リーダ（読込プログラム）は、指定された SubFilter フォーマットをサポートする限り、Filter で指定された署名ハンドラと異なる署名ハンドラを利用してもよい（may)。

10. ISO 32000-1 に記載の SubFilter のうち adbe.pkcs7.detached と adbe.pkcs7.sha1 のどちらかを使うこと（shall)。

11. タイムスタンプはできるだけ署名直後の時間に、信頼されたタイムスタンプサーバから取得して埋め込まれるべきである（should)。

3.1.3.3 パート 3：PAdES Enhanced（CAdES プロファイルに基づく PAdES)

PAdES Enhanced では、PAdES-BES または PAdES-EPES の 2 種類のプロファイルがあるが、それぞれ利用する署名データが CAdES-BES と CAdES-EPES である点が異なる。CAdES-T のプロファイルも利用されるが、これは CAdES-BES と CAdES-EPES で共通のプロファイルとなっている。

一部の署名属性はISO 32000-1の署名辞書とCAdESとで類似した意味を持つ場合がある。このような場合には署名辞書のアイテムがCAdESのアイテムより優先されるべきである（should)。以下主な要求事項をまとめる。

1. ISO 32000-1の12.8で定義されているPDF署名の仕様をPAdES Enhancedの仕様を除いて要求する（Requirements)。

2. SignedDataオブジェクトが署名辞書のContentsエントリの中に存在すること（shall)。ここで利用するCMSはCAdESに含まれる幾つかの属性を要求したプロファイルとなる。

3. ByteRangeエントリがファイル全体を指し署名辞書に含まれること（shall)、ただしPDF署名自体は除外する。

4. 署名辞書のSubFilterのキーとしてETSI.CAdES.detachedを使うこと（shall)。

5. 検証者は、指定されたSubFilterフォーマットをサポートする限り、Filterで指定された署名ハンドラと異なる署名ハンドラを利用してもよい（may)。

6. 署名辞書にはCertエントリは含まない（shall not)。

7. このプロファイルに含まれない非署名属性は他のプロファイルと共に使われない限り無視してもよい（may)。非サポートの署名属性の扱いは検証者の問題である。

8. タイムスタンプはできるだけ署名直後の時間に、信頼されたタイムスタンプサーバから取得して埋め込まれるべきである（should)。

これら以外に、CAdESの属性に関する細かな要求項目がPAdES Enhancedには含まれているので、詳細はETSI TS 102 778のPart3を参照のこと。

3.1.3.4 パート4：PAdES Long Term（PAdES-LTV)

PAdES Long TermではPAdES-LTVと呼ばれるプロファイルがある。PAdES-LTVはISO 32000-1へのLTV拡張として追加仕様がまとめられている。拡張される項目は、検証情報（証明書/CRL/OCSP）を保持するストアとしてDSS（Document Security Store）と、PDF署名の署名辞書をベースとしたドキュメントタイムスタンプ（Document Time-Stamp）の2つの追加仕様がある。

DSSは長期署名の仕組みで見るとES-X-Longに相当する。繰り返して適用が可能な点がXAdESやCAdESと異なる。DSSは、DSS辞書とVRI（Validation Related Information）辞書（オプショ

ン）とストリームオブジェクトとして埋め込まれる検証情報群、で構成される。DSS 辞書ではストアとして管理している全ての検証情報の参照を保持しており、VRI 辞書により特定の署名データに対する検証情報の参照を指定できる仕組みになっている。以下の例は PDF 署名が 2 つある（署名データも 2 つある）場合の DSS 辞書と VRI 辞書と各検証情報群ストリームオブジェクトとの関係を示している。これらは全て PDF の構造になっている。

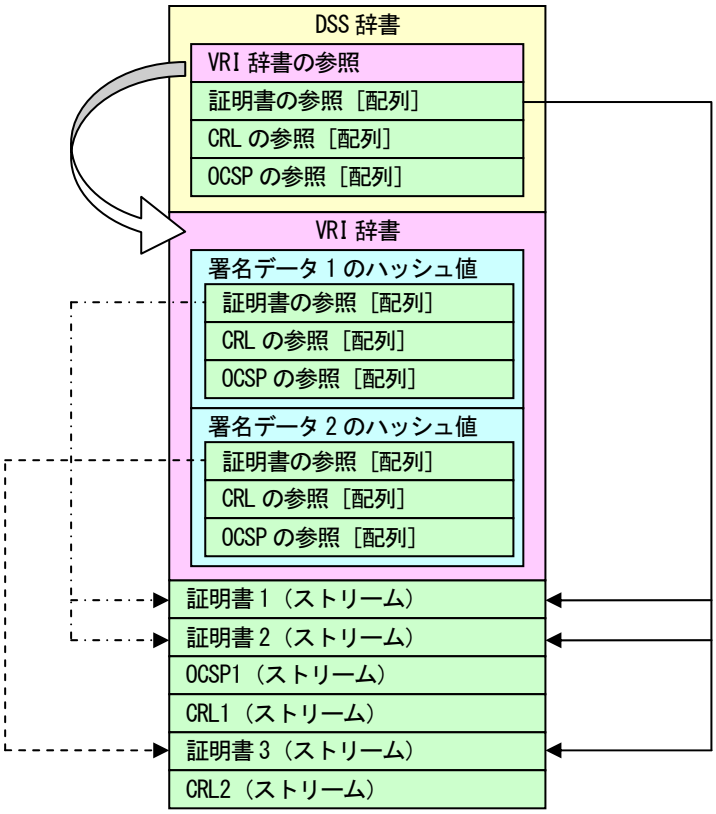


図 3.3.6 DSS と VRI の構造

VRI 辞書の署名データのハッシュ値と言うのは PAdES Basic と PAdES Enhanced の場合には、PKCS#7 や CAdES のバイナリデータ（つまり署名辞書の Contents エントリのデータ）のハッシュ値であり、PAdES for XML Content の XFA Forms の場合には C14N 正規化された XML 署名データのハッシュ値となる。

ドキュメントタイムスタンプは長期署名の仕組みで見ると ES-A に相当する。タイムスタンプのハッシュ対象となるのは PDF 署名の仕組みと同じく ByteRange で指定される文書全体になる。この点は署名対象や非属性要素を結合してハッシュ対象とする XAdES や CAdES と異なる。

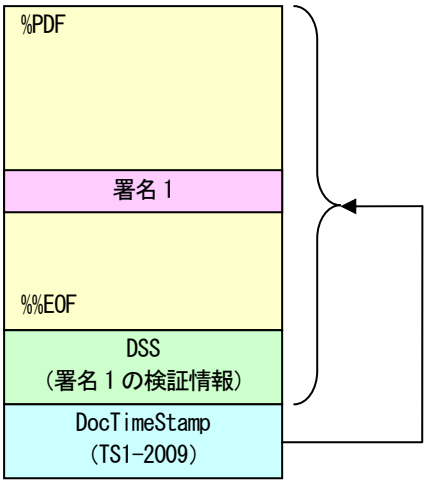


図 3.3.7 1 世代目の LTV

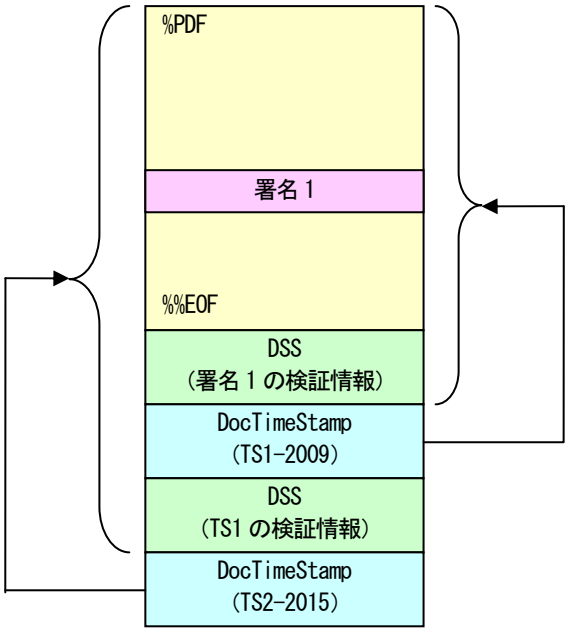


図 3.3.8 2 世代目の LTV

DSS とドキュメントタイムスタンプは増分更新の仕組みにより追加される。世代を重ねる場合には、直前のドキュメントタイムスタンプの検証情報を新しい DSS として追加した上で、新しいドキュメントタイムスタンプを追加する。

DSS とドキュメントタイムスタンプを使った、LTV の検証手順を以下にまとめる。

1. 最後のドキュメントタイムスタンプを検証情報と共に現在の時刻で検証する。
2. 内側のドキュメントタイムスタンプを検証情報と共にその前のタイムスタンプ時刻で検証する。
3. 署名と署名タイムスタンプを検証情報と共に最も内側のタイムスタンプ時刻で検証する。

3.1.3.4.1 ISO 32000-1 LTV 拡張：Document Security Store (DSS)

以下に DSS 辞書の表を示す。

DSS 辞書		
キー	型	値
Type	名前	（オプション）PDF オブジェクトのタイプ。存在する場合は **DSS**。
VRI	辞書	（オプション）署名 VRI 辞書。各エントリのキーは署名データの base-16-encode（大文字）の SHA1 ダイジェスト。**ノート 1** と**ノート 2** を参照。

Certs	配列	（オプション）間接指定されたストリームの配列。各ストリームには BER-encode された X.509 証明書（RFC 5280 参照）を格納。この配列の証明書は任意の署名検証に使われる。
OCSPs	配列	（オプション）間接指定されたストリームの配列。各ストリームには BER-encode された OCSP（Online Certificate Status Protocol）のレスポンス（RFC 2560 参照）を格納。この配列の OCSP は任意の署名検証に使われる。
CRLs	配列	（オプション）間接指定されたストリームの配列。各ストリームには BER-encode された CRL（Certificate Revocation List）（RFC 5280 参照）を格納。この配列の CRL は任意の署名検証に使われる。
ノート 1:	文書署名の場合は DER-encoded の PKCS#7（またはその派生形）のバイナリデータ（署名辞書の Contents エントリの base-16-decode の値）のダイジェスト。CRL と OCSP レスポンスの署名の場合は最初に BER-encode された OCTET STRING のダイジェスト。	
ノート 2:	XFA の XAdES 署名の場合は ds:Signature 要素の exclusive canonicalization により正規化を計算したダイジェスト。	

以下に VRI 辞書の表を示す。

署名 VRI 辞書		
キー	型	値
Type	名前	（オプション）PDF オブジェクトのタイプ。存在する場合は VRI。
Cert	配列	（オプション：空配列は不可）間接指定されたストリームの配列。各ストリームには BER-encode された X.509 証明書（RFC 5280 参照）を格納。この配列は、この署名の確認において使われた全ての証明書を含まなければならない。
CRL	配列	（オプション：空配列は不可）間接指定されたストリームの配列。各ストリームには BER-encode された CRL(Certificate Revocation List)(RFC 5280 参照）を格納。この配列は、この署名の証明書の検証において使われた全ての CRL を含まなければならない。
OCSP	配列	（オプション：空配列は不可）間接指定されたストリームの配列。各ストリームには BER-encode された OCSP（Online Certificate Status Protocol）のレスポンス（RFC 2560 参照）を格納。この配列は、この署名の証明書の検証において使われた全ての OCSP レスポンスを含まなければならない。
TU	日付	（オプション）この VRI 辞書が得られた日付/時刻。規則に従った PDF リーダの場合はこの時刻を無視して別の時刻を利用してもよい。TS エントリが存在する場合このエントリを使ってはいけない。ノート 1 を参照。

TS	ストリーム	（オプション）この VRI 辞書が得られた日付/時刻の BER-encoded されたタイムスタンプ（RFC 3161 参照）のストリーム。TU エントリが存在する場合このエントリを使ってはいけない。ノート 2 とノート 3 を参照。
ノート 1:	このキーの使用は、このプロフィールの推奨（recommend）ではない。他の実現例で使われる情報として用意されているだけである。そのようなものとしてこのプロフィールでは無視されなければならない。	
ノート 2:	このタイムスタンプの messageImprint フィールドのハッシュ値は、署名 PKCS#7 オブジェクトの encryptedDigest フィールドと同じである。	
ノート 3:	このキーの使用は、このプロフィールの推奨（recommend）ではない。他の実現例で使われる情報として用意されているだけである。そのようなものとしてこのプロフィールでは無視されなければならない。	

例 1：DSS 辞書と関連する情報

```
100 0 obj
<<
/Type /Catalog
/DSS 101 0 R
%other stuff here...
>>
endobj
101 0 obj
<<
/VRI 102 0 R
/OCSPs [103 0 R]
/CRLs [104 0 R]
/Certs [105 0 R 106 0 R]
>>
endobj
102 0 obj
<<
/4B783B9A6D0D69E4E881BFDF080835E896735416 << /OCSP [103 0 R] /CRL [104 0 R] >>
>>
endobj
103 0 obj
<<
/Length 3085 %whatever the length of the stream is
>>
stream
%OCSP data goes here...
endstream
104 0 obj
<<
/Length 909 %whatever the length of the stream is
>>
stream
%CRL data goes here...
```

```
endstream
105 0 obj
<<
/Length 1042 %whatever the length of the stream is
>>
stream
%Certificate data goes here...
endstream
106 0 obj
<<
/Length 960 %whatever the length of the stream is
>>
stream
%Certificate data goes here...
Endstream
```

例２：2 署名に対応した DSS 辞書

```
101 0 obj
<<
/VRI 102 0 R
/OCSPs [103 0 R 107 0 R]
/CRLs [104 0 R]
/Certs [105 0 R 106 0 R]
>>
endobj
102 0 obj
<<
/4B783B9A6D0D69E4E881BFDF080835E896735416 << /OCSP [103 0 R] /CRL [104 0 R] >>
/123456789ABCDEF987654321FEDCBA1234567890 << /OCSP [107 0 R] >>
>>
107 0 obj
<<
/Length 5012 %whatever the length of the stream is
>>
stream
%OCSP data goes here...
Endstream
```

検証に利用される検証情報の好ましい取得手順（優先順位）は以下となる。

1. DSS の中の署名 VRI 要素から参照されている検証情報。
2. DSS から参照されている検証情報。
3. 署名データ自身に埋め込まれている検証情報。
4. ローカルなリポジトリに保管されている検証情報。
5. オンラインソースから取得された検証情報。

ただし作成時において、旧バージョンの互換性を確保する為に、可能な限り署名データに検証情報を埋め込むべきである。

3.1.3.4.2 ISO 32000-1 LTV 拡張：Document Time-Stamp

ドキュメントタイムスタンプ辞書は、標準の署名辞書（ISO 32000-1 12.8 参照）と同じとなるが、以下の修正箇所がある。

Document Time-Stamp 辞書の為の table 252 の修正箇所		
キー	型	値
Type	名前	（オプション）PDF オブジェクトのタイプ。存在する場合は **DocTimeStamp**。
SubFilter	名前	（必須）Type の値が **DocTimestamp** であるとき、SubFilter の値は **ETSI.RFC3161** となる。SubFilter の値は、ストリームに含まれるデータのフォーマットを確認する為に用いられる。
Contents	バイト文字列	（必須）16 進文字列（Hexadecimal Strings）で表現された値。SubFilter の値が **ETSI.RFC3161** であるとき、Contents は RFC 3161 で定義された TimeStampToken である。TimeStampToken の messageImprint なフィールドの値は、ByteRange によって示される文書範囲のハッシュ値である。ハッシュ値が計算される前に、Contents エントリの為の領域が割り当てられていなければならない。
V	整数	（オプション）署名辞書フォーマットのバージョン番号。存在する場合にドキュメントタイムスタンプ辞書は 0 となる。 デフォルト値：0

次のキーはドキュメントタイムスタンプ辞書では存在してはならない。Cert, Reference, Changes, R, Prop_AuthTime, Prop_AuthType。

次のキーはドキュメントタイムスタンプ辞書では存在すべきではない。Name, M, Location, Reason, ContactInfo。これら情報が Contents に含まれる TimeStampToken の中ですでに存在するかもしれないので、これらのキーは無視しなければならない。

例：ドキュメントタイムスタンプ

```
1 0 obj
<<
/Type /Catalog
/Pages 2 0 R
/AcroForm 5 0 R
>>
endobj
2 0 obj
<<
```

```
/Kids [ 3 0 R ]
/Count 1
/Type /Pages
>>
endobj
3 0 obj
<<
/Type /Page
/Parent 2 0 R
/MediaBox [ 0 0 612 792 ]
/Annots 4 0 R
% other keys goes here...
>>
endobj
4 0 obj
<<
/Type /Annot /Subtype /Widget
/Rect [ 0 0 0 0 ]
/F 4 /P 3 0 R
/FT /Sig /T (Sig)
/V 6 0 R
>>
endobj
5 0 obj
<<
/Fields [ 4 0 R ]
/SigFlags 3
>>
endobj
6 0 obj
<<
/Type /DocTimeStamp
/Filter /Adobe.PPKLite
/SubFilter /ETSI.RFC3161
/Contents <00000> % values go here inside of ◇
/ByteRange [0 0 0 0 ] % values go here inside of []
>>
Endobj
```

3.1.3.5 パート5：PAdES for XML Content（添付ファイルとFXA）

3.1.3.5.1 添付ファイルXML文書のXAdESプロファイル

PDF ファイルの中に XML 文書を添付ファイルとして埋め込む場合は、XML 文書に対して XAdES 署名を付与することで対応する。埋め込み手順は以下となる。

1. PDF フレームワークの外で、XML 文書を生成して XAdES（XAdES-BES / XAdES-EPES / XAdES-T）により署名する。

2. 前述の XAdES 署名済み XML 文書を PDF に埋め込む。

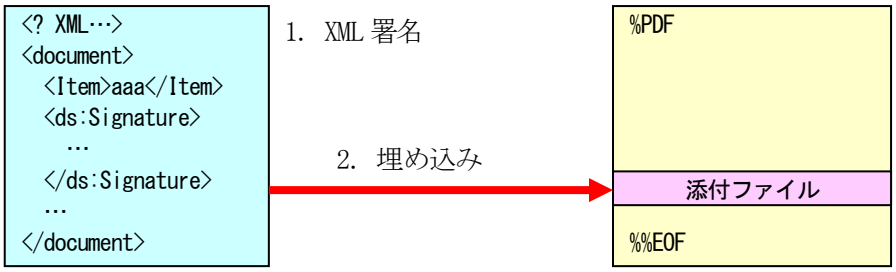


図 3.3.9 XAdES 署名済み XML 文書の PDF 埋め込み

XAdES を XAdES-C / XAdES-X / XAdES-X-Long / XAdES-A に更新する場合には以下の手順となる。

1. PDF に埋め込まれた XAdES 署名済み XML 文書を取り出す。
2. PDF フレームワークの外で、XAdES 署名を更新（XAdES-C / XAdES-X / XAdES-X-Long / XAdES-A）する。
3. 前述の XAdES 署名更新済み XML 文書を再度 PDF に埋め込む。

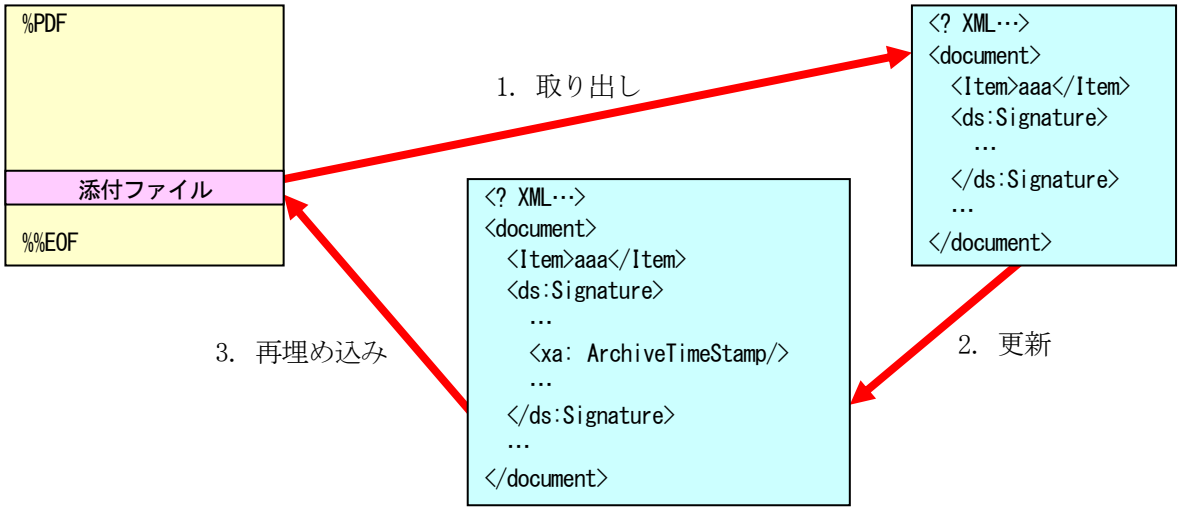


図 3.3.10 XAdES 署名済み XML 文書の更新と PDF 再埋め込み

3.1.3.5.2 XFA Forms の XAdES プロファイル

入力フォームとして XFA Forms を利用した場合には以下の 2 つのプロファイルがある。

1. 基本 XAdES フォームの基本プロファイル。（XAdES-BES / XAdES-EPES / XAdES-T）
2. 長期署名 XAdES 署名のプロファイル。PAdES-LTV の DSS / VRI 辞書を使う。（XAdES-X-Long / XAdES-A 相当）

この 2 つのプロファイルで、XFA forms の XML データのみへの XML 署名と、XFA forms の任意

の XML データへの XML 署名の、2 つのシナリオに対応ができる。以下は XFA フレームワークの例。

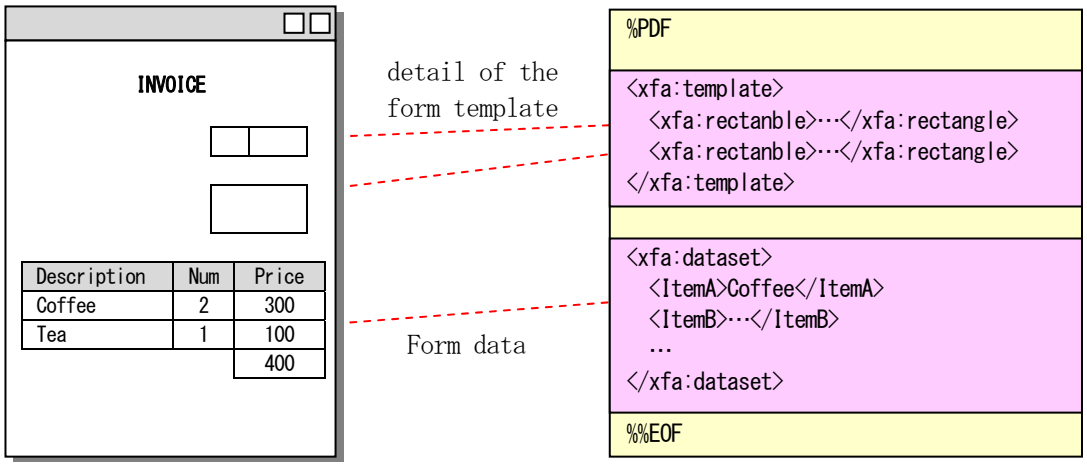


図 3.3.11 XFA フレームワークの例

XFA の入力フォームに入力した後で、XFA のデータのみまたは任意のデータに XAdES 署名（XAdES-BES / XAdES-EPES / XAdES-T）を付与した例を以下に示す。

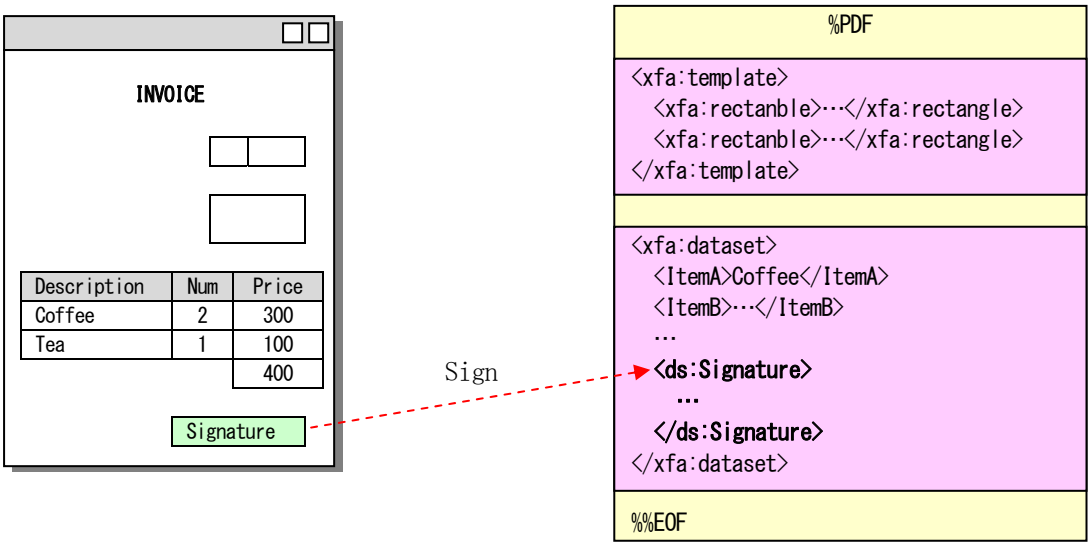


図 3.3.12 基本 XAdES フォームの基本プロファイル

XFA Forms への XAdES 署名（XAdES-BES / XAdES-EPES / XAdES-T）後に、PAdES-LTV の DSS 辞書と VRI 辞書を使って検証情報を埋め込む例を以下に示す。これで ES-X-Long 相当になる。更にドキュメントタイムスタンプを付与して ES-A 相当にも更新できる。

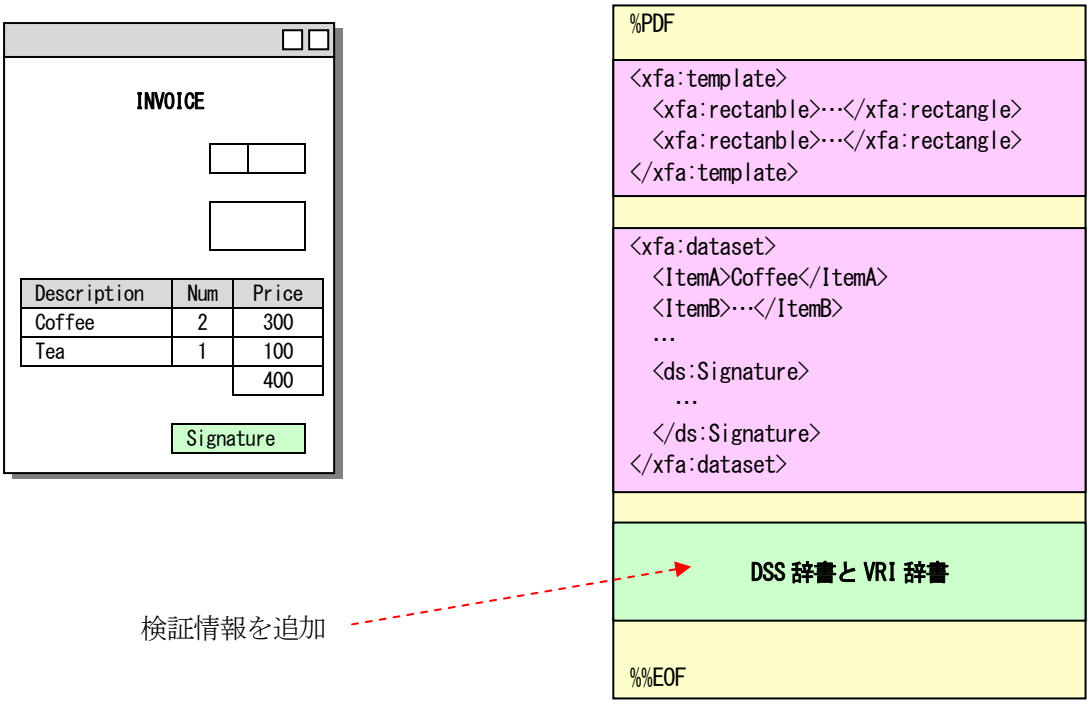


図 3.3.13 長期署名 XAdES 署名のプロファイル（PAdES-LTV の DSS / VRI 辞書を使う）

なお XAdES の要素に関する細かな要求項目が PAdES for XML Content には含まれているので、詳細は ETSI TS 102 778 の Part5 を参照のこと。

3.1.4 おわりに

PAdES は文書フォーマットとしては初めての長期署名仕様である。外観も含めて PDF と言う一つの仕様の中で全てが完結できるメリットは大きいのではないだろうか。反面 PAdES のプロファイルは CAdES や XAdES のプロファイルにも依存しており実装の難易度は上がっているとも言える。良い面も悪い面も色々あるが、PDF に対する一般のニーズは高く XAdES や CAdES にできなかったことが、PAdES では実現できるのでは無いかと期待がかかる長期署名プロファイルである。ISO 32000-2 や PDF/A-2（ISO 19005-2）としての実現が待たれる。

3.2 証明書や署名のビジュアル化

証明書や署名を検証するとき、システム上で証明書や署名の内容を自動判定するようなケースもあれば、検証者が検証ソフトウェアで表示される検証結果を見たり、さらに、証明書や署名の情報を見ることで受け入れ可否を判断するケースもある。

しかしながら、証明書や署名などのデータフォーマットは主に機械的に処理されることを想定しており、データフォーマットの各フィールドの内容は実際に人が見て判断するには適したものであるとは言いがたい。また、これまで検証結果の表示に関して標準規格やガイドラインもなく、各ベンダーがそれぞれ独自の方法で行ってきたため、表示される内容の詳細度や表現もソフトウェアにより異なり、検証者は使用するソフトウェア毎に確認方法を変える必要があったり、検証

者が参照したい情報が特定のソフトウェアでは得られないといった問題が生じる可能性もある。

このような状況は日本だけでなく海外でも同様であり、証明書や署名のビジュアル化に関する標準を策定しようという動きが見られている。

IETF ではCertificate Image というドラフトが作成され標準化へ向けて検討されている。これは、証明書の拡張に所有者本人を示す画像情報（画像フォーマットやPDF、SVG 等）のデータや参照情報を記載するものであり、RFC3709（Logotypes）の拡張として提案されている。

ETSI においても証明書や署名のビジュアル化に関する検討が進められている。この検討にはCertificate Image を作成しているメンバーも参加している。近くに PDF 署名の表示に関する規格が策定される予定である。

OASIS ではVisible Signature Profile としてDigital Signature Service（DSS）で署名の表示に関する操作を可能にするプロファイルを策定する計画である。

このように証明書や署名の表示に関する提案が各団体でなされており、それらが標準化された場合には日本も影響を受ける可能性がある。今後もこれらの標準化動向を継続して調査し、日本の検証ソフトウェアの普及状況と照らし合わせて、日本における標準やガイドライン策定の可能性について検討する必要があるだろう。

3.3　暗号アルゴリズムの安全適合性ポリシ

暗号アルゴリズムは脆弱化する可能性を持っている。電子署名の生成／検証時、データを暗号化／復号時に用いる暗号アルゴリズムの安全性を考慮することは極めて重要である。RFC5698:Data Structure for the Security Suitability of Cryptographic Algorithms （DSSC）は、過去、現在、未来を含む各時点における暗号アルゴリズムの安全性を機械的に判定するための「安全適合性ポリシ（Security Suitability Policy)」のデータ構造を定義する。署名生成あるいは検証ツールで安全適合性ポリシを検証することにより、署名の生成時あるいは検証時などの時点において、署名で使われている暗号アルゴリズムが脆弱化していないかどうかを確認することができる。暗号アルゴリズムの安全性評価は信頼のおける機関（NIST、Cryptrec など）が行うことを想定している。安全適合性ポリシには署名を付与することができ、署名を検証することにより安全適合性ポリシが信頼できるものか否かを判断することができる。

安全適合性ポリシの主なユースケースは次のとおりである。

①署名文書の長期保存

最も重要なユースケース。タイムスタンプの更新の手がかりとする。

②署名の生成・検証

署名の生成時には、利用する暗号アルゴリズムの安全性の判断に用いる。署名の検証時には、検証時点で、長期署名の場合にはタイムスタンプが付与された時点で、署名やタイムスタンプに用いられた暗号アルゴリズムが安全なものであったか否かを判断するために用いる。

③安全情報提供サービス

安全適合性ポリシそのものを暗号アルゴリズムの安全性に関する情報として提供する。

④再暗号化

秘匿のために暗号化していた保存データを、用いられている暗号アルゴリズムが脆弱化する前

により強力な暗号アルゴリズムで再暗号化するための判断基準として用いる。

安全適合性ポリシは XML と ASN.1 で定義されている。その大まかな構造を以下に示す。

安全適合性ポリシの要素	要素の説明
バージョン	安全適合性ポリシのバージョン。規定値は 1.
言語	記述言語。規定値は英語。
ポリシ名	安全適合性ポリシの名称。
発行者	安全適合性ポリシの発行者。
発効日時	安全適合性ポリシの発行日時。
次期更新日時	安全適合性ポリシの次回更新予定日時。オプション。
用途	評価対象の暗号アルゴリズムの用途。オプション。
アルゴリズム群	評価対象の暗号アルゴリズムに関する情報の並び。
アルゴリズム ID	暗号アルゴリズムの ID。
安全性評価	暗号アルゴリズムの安全性に対する評価。
パラメータ	暗号アルゴリズムに付随するパラメータや鍵長。オプション。
有効性	暗号アルゴリズムが安全な期間。
開始日時	暗号アルゴリズムが安全となる日時。
終端日時	暗号アルゴリズムが安全性を消失する（した）日時。
拡張領域	安全性評価に関する拡張領域。オプション。
関連情報	暗号アルゴリズムに関する情報。オプション。
拡張領域	暗号アルゴリズムに関する拡張領域。オプション。
署名	安全適合性ポリシに対する発行者による署名。オプション。

4. 電子記録の長期管理ガイドライン

4.1 背景

ECOM は、2000 年から電子署名文書の長期保存問題について調査・検討を重ねてきた。長期保存を阻害する主な要因は、記録媒体の劣化、署名危殆化、ファイル非互換などであるが、昨今の関係者の認識の高まりや標準化の進展もあり、表 3.4.1 に示すように、技術的な対応策が確立されてきた。しかしながら、現状は、電子文書を原本とした運用に移行しつつあるとは言い難い。社会は、企業活動に透明性、効率性を求めている。電子文書は正式な記録としてもっと活用されるべきであるが、依然として原本は紙の文書のままである。

昨年度及び今年度のアンケート調査の結果にあるように、文書は電子的に作成されても、必ずしも原本としては管理されていない。問題は、次の 3 点に集約されると考えられる。

・電子化後の紙文書を捨てても後々（法的に）問題ないのかどうかが分からない
・紙文書の方が扱いやすい（めくりやすい、読みやすい）
・電子文書を原本として管理することに不安がある

表 3.4.1 長期保存の阻害要因と対応策

<table>
<tr><td>長期保存の阻害要因</td><td>記録媒体劣化</td><td>署名危殆化</td><td>ファイル非互換</td><td>災害など</td></tr>
<tr><td>対処方針</td><td colspan="3">問題が発生する前に適切な措置を行い、問題の発生に至らないようにする（＝リスクの先だし）</td><td rowspan="4">従来対策を踏襲</td></tr>
<tr><td>課題</td><td>記録媒体の劣化検知</td><td>再検証に必要な情報の保存</td><td>特定ベンダ依存からの独立</td></tr>
<tr><td rowspan="2">解決策</td><td>・高品質記録媒体の選択
・定期検査と媒体移行
ISO/IEC 10995
JIS Z 6016</td><td>・長期保存フォーマット導入
・長期運用タイムスタンプ局選定
JIS X 5092
（ISO/CD 14533-1）
JIS X 5093
（ISO/CD 14533-2）
ETSI TS 102 778</td><td>・長期保存ファイル形式導入
・既存システムの移行
ISO 32000-1
ISO 19005-1
ISO/IEC 26300
ISO/IEC 29500</td></tr>
<tr><td colspan="3">文書管理プロセス構築
ISO 15489（JIS X 0902-1）</td></tr>
</table>

4.2 電子記録マネジメント

記録の管理、すなわち、記録として残すべき文書の管理に関しては、既に国際標準 ISO 15489-1,-2 が存在する。ISO 15489-1,は既に、JIS X 0902-1 として JIS 化されている。この標準

には、図 3.4.1 のような記録管理プロセスとコントロールが定義されている。

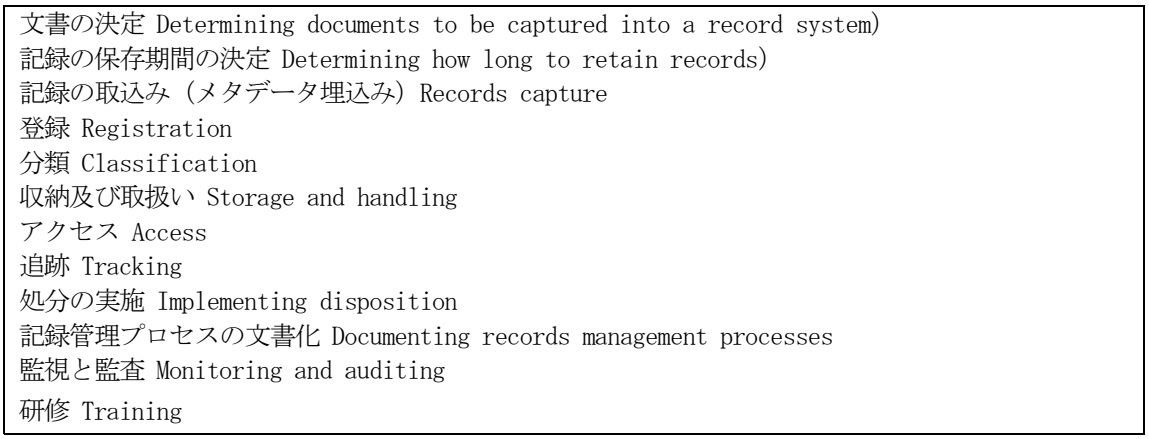


図 3.4.1 記録管理プロセスとコントロール

電子文書を原本として管理するためには、更にそれなりの仕組みが必要となる。電子文書は紙文書と異なり、さまざまな構成要素によってシステム的に成り立っているため、見読性、完全性、機密性、検索性、真正性、識別性の確保が必要である。

・見読性　使用に係る機器に直ちに表示
・完全性　滅失、毀損、改変、消去防止
・機密性　（個人情報などの）漏洩防止
・検索性　記録の体系的構成
・真正性　何時誰が作成したかの特定
・識別性　管理対象の特定

注記：共通課題研究会の報告書では、電子文書を紙文書と同等に扱う要件として見読性、完全性、機密性を挙げている。その後の、文書の電磁的保存等に関する委員会報告書では、これらに検索性が追加された。e 文書法に伴う政省令は、更に真正性を求め、公文書管理法では、保存管理の観点から記録の識別性を求めている。

電子記録を管理するには、これらの要件を満たすプロセスとコントロールを具体化し、記録管理システムとしてマネジメントして行かなければならない。前述の“紙が捨てられない”問題は、各ドメインの文書がどの程度の要件（技術的、運用的）を満たせばよいかについての基準やガイドラインが存在しないところにあると考えられる。

また、電子記録を管理するためには（紙文書も同じであるが)、対象となる電子記録を管理するための管理情報が必要である。これは、一般にメタデータと呼ばれている。

図 3.4.2 はメタデータのイメージである。電子文書は実体がなく目に見えないことから、これらのメタデータを実感として捉えにくい面もあるが、各々のメタデータの役割は次の通りである。

いうまでもなく、相互運用性を確保するためには標準化が欠かせない。

・ID　管理対象文書の識別
・来歴・入手経路　文書が作成された根拠、入手文書の由来や入手経路の明確化
・動作環境　文書を正しく表示・印刷するための環境条件の提示
・業務コンテキスト　稟議ルート、決裁者の提示
・ライフサイクル　登録から破棄までの間のフェーズ管理
・物理マッピング　格納場所へのポインタ
・保存コンテキスト　必要な長期保存処置
・権利　アクセス制御
・索引　検索用インデックス
・相互関連　文書ファイル（フォルダ）としての括り

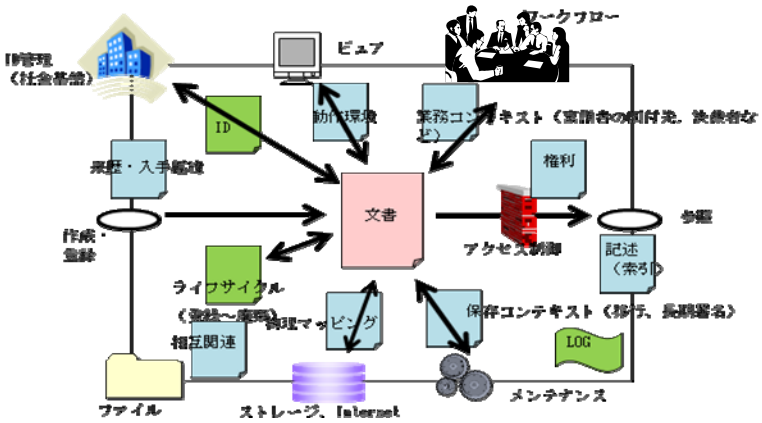


図 3.4.2 メタデータのイメージ

文書の作成・登録時、保管時、参照時のフォーマットは、それぞれの処理に適したものが選択されることになる。図 3.4.3 は、ISO 14721 Reference Model for Open Archival Information System (OAIS) で定義されているモデルである。

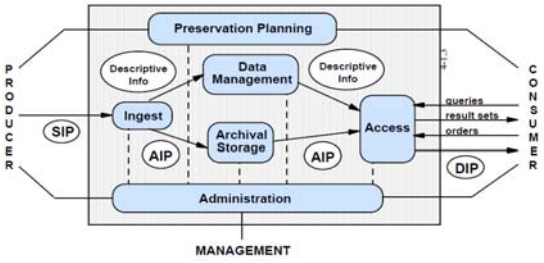


Figure 4-1: OAIS Functional Entities

図 3.4.3 OAIS モデル

図 3.4.4 は OAIS における情報パッケージの概念図であり、表 3.4.2 はパッケージに含まれるメタデータである。情報パッケージがどの様な実装になるかは別にして、参考にするのに値する

構造である。

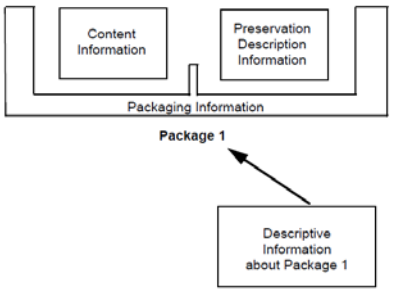


Figure 2-3: Information Package Concepts and Relationships

図 3.4.4 情報パッケージの概念図

表 3.4.2 パッケージに含まれるメタデータ

パッケージ化情報		コンテント情報と保存記述情報のパッケージ化
コンテント情報	コンテント	保存対象データそのもの
	表現情報	フォーマット、コードなど
保存記述情報	参照情報	識別番号
	コンテキスト情報	作成理由など
	来歴情報	起源、出所、その後の変更など。イベントを記録（含権利関係）
	不変性情報	チェックサム
記述情報		目録

4.3　記録に関するマネジメントシステム標準の動向

記録に関しても、他の、品質マネジメントシステム標準（ISO 9000）や環境マネジメントシステム標準（ISO 14000）などと同じ様な、マネジメントシステム標準（MSS と云う）が策定されつつある。記録に関するするマネジメントシステム標準は、現在、国際標準化過程にあり、審議が順調に進めば、数年後には ISO 30300 シリーズとして国際標準化される見通しである。標準のタイトルは記録マネジメントシステム標準であるが、内容的には電子記録をメインとした標準である。他のマネジメントシステム標準と同様、目標を定め、プロセスを定義し、PDCA をまわすことにより、自ら設定した目標を達成することになる。

ISO 30300 シリーズの構成を図 3.4.5 に示す。

ISO30300 ファミリー
30300　基本と語彙
30301　要件
30302　実装ガイド
30303　評価ガイド
30310　認定要件
関連標準
ISO 15489 記録管理
ISO/TR 26122　ワークプロセス分析
ISO TR 13008　変換と移行プロセス
ISO TR 13028　電子化実装ガイド
ISO TR 13069　リスク評価
ISO 23081 記録のためのメタデータ

図 3.4.5 ISO 30200 シリーズの体系

この体系のなかで、30300“基本と語彙”は、このシリーズの全体構造と用語（ターミノロジ）を定義し、30301“実装ガイド”及び30310“認定要件”は、それぞれ、記録のためのマネジメントシステムの要件、及びマネジメントシステムの認定要件を定義している。また、30302“実装ガイド”及び30303“評価ガイド”は、PDCA をまわすためのガイドラインを規定している。

ISO 15489“記録管理”のような、プロセスの実装に関する標準は、関連標準としてシリーズに組み込まれている。

4.4　電子記録マネジメントコンソーシアム

電子記録マネジメントは、対象ドメインや技術要素が広範にわたることから、一つの団体で全体をカバーする検討は困難である。このため、ECOM が関連する団体に声掛けし、関連団体が結集して、電子記録マネジメントを推進する活動のための組織「電子記録マネジメントコンソーシアム」を立ち上げることとなった。(4 月 27 日設立予定)

設立に向けての準備委員会は、当初、ARMA 東京支部、次世代電子商取引推進協議会（ECOM)、社団法人ビジネス機械・情報システム産業協会（JBMIA)、社団法人日本画像情報マネジメント協会（JIIMA)、タイムビジネス協議会（TBF）の 5 団体で発足し、その後、社団法人電子情報技術産業協会（JEITA)、財団法人日本情報処理開発協会（JIPDEC）からの参画を得た。8 月 31 日の第一回の準備会の開催から、都合 8 回の準備会を開催し、各団体が認識している、電子記録の問題や課題を共有すると共に、コンソーシアム設立に向けて、設立趣旨書及び会則案を策定した。

コンソーシアムの推進体制案は図 3.4.6 の通りである。コンソーシアムの会員は、コンソーシアムの活動に賛同する業界団体またはその下部組織、関連行政機関、その他、コンソーシアムが特別に認める機関である。

コンソーシアムは、関連する団体の活動を尊重し緩やかに結束する形態とした。総会の下に幹事会を置いて運営に関する議論を行い、技術的な検討は専門部会で行う。専門部会は、各団体による主管制とし、部会長と事務局を分担する。成果物は、コンソーシアム会員間で共有できることとするが、著作権の扱いは、その専門部会を主管する会員の団体の規則に従うものとした。

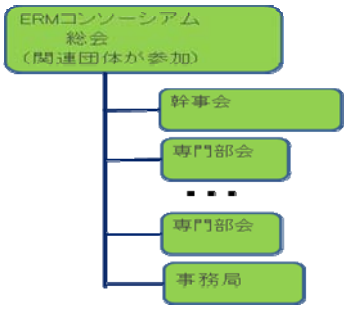


図 3.4.6 コンソーシアムの推進体制

コンソーシアムでは、当面、以下を目標として活動することを計画している。図 3.4.7 は全体スケジュール案である。

・電子記録マネジメント基盤のモデル化と要件定義
・電子記録マネジメント基盤システムの運用ガイドの策定
・電子記録の管理情報（メタデータ）の標準化
・電子記録マネジメント基盤の普及啓発

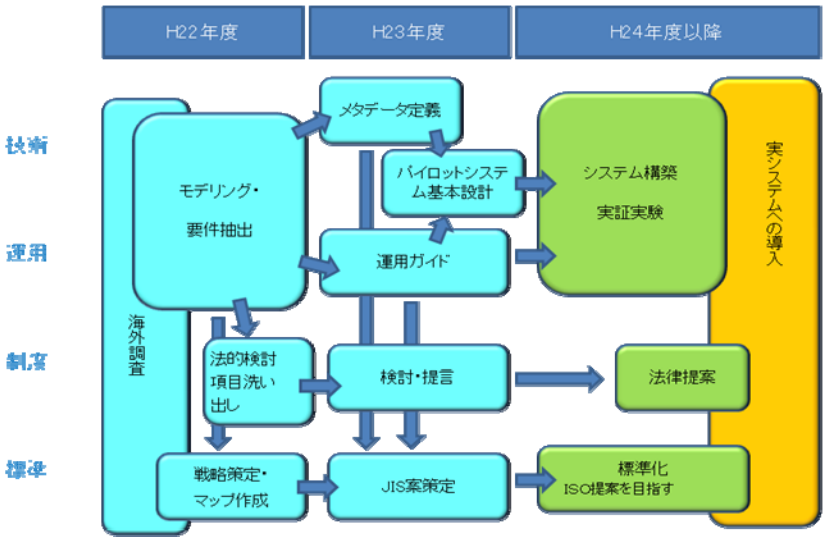


図 3.4.7 コンソーシアム活動の全体スケジュール案

5. 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	次世代電子商取引推進協議会　客員研究員
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
副主査	宮崎　一哉	三菱電機株式会社
幹　事	佐藤　雅史	セコム株式会社
幹　事	橋本　正一	日本電信電話株式会社
幹　事	政本　廣志	日本電信電話株式会社
幹　事	宮地　直人	有限会社ラング・エッジ
委　員	松本　泰	セコム株式会社
委　員	松山　博美	富士通株式会社

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
幹　事	高尾　美由紀	みずほ情報総研株式会社
委　員	浅野　敬	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	上田　勝	電気事業連合会
委　員	勝岡　義博	株式会社NTTデータ
委　員	小池　正通	富士ゼロックス株式会社
委　員	小林　英彦	東芝ソリューション株式会社
委　員	島　　成佳	日本電気株式会社
委　員	田村　雅之	三菱電機株式会社
委　員	永島　清	株式会社NTTデータ
委　員	芳賀　悟	エントラストジャパン株式会社
委　員	宮澤　慎一	セコム株式会社
委　員	保倉　豊	グローバルフレンドシップ株式会社
委　員	鷲尾　元太郎	三菱電機株式会社
委　員	和田　宗樹	株式会社帝国データバンク
オブザーバ	西川　康男	ARMA　東京

禁　無　断　転　載

電子署名普及に関する活動報告 2009

平成 22 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

この資料は再生紙を使用しています。

ISBN978-4-89078-684-8 C2055