22−H009

電子データ保存システム
に関する調査研究報告書

平成23年 3 月

財団法人 日本情報処理開発協会

この事業は、競輪の補助金を受けて実施したものです。
http://ringring-keirin.jp

22−H009

電子データ保存システムに関する調査研究報告書

平成23年3月

財団法人 日本情報処理開発協会

序文

本報告書は、財団法人日本情報処理開発協会が競輪の補助金を受けて実施した平成 22 年度情報化推進に関する調査研究等補助事業「次世代電子情報流通基盤の整備に関する調査研究」事業の一環である「電子データ保存システムに関する調査研究」の成果を取りまとめたものである。

今日、大半の文書は電子的に作成されており、これを紙の原本に替えて電子データで保存することのメリットは大きい。しかしながら、電子記録を管理及び利用するためには、紙の記録を管理及び利用する場合とは全く違う技術と運用が必要になり、これまで紙の記録で定着していた保存技術や保存のための運用方法の多くは、電子記録には適用できず、多くの組織は適切な解決策が見いだせない状態に陥っている。特に、中小企業などでは、費用的な面、人材面の理由から、企業が個々にシステムを導入して利用することは多くの困難が予想される。

そこで今年度は、利用者が安心して使うことのできる電子文書等のビジネス記録の利活用基盤の構築に向けた調査検討を行った。具体的な項目としては、記録管理としてのライフサイクル管理、電子署名やタイムスタンプの長期検証可能化対策、ユーザインタフェースの向上、署名目的の明示化（署名ポリシーの検討）に加え、誰もが安心して電子記録の保管を任せられる公認保管庫の検討など、多岐にわたった。

本報告書は、本年度実施した先進事例等の調査及び検討結果を紹介するとともに、これらの項目について、技術面、運用面、制度面から検討を行い、標準化、ガイドラインの作成、法制度の提案を行うものである。検討に当たっては、電子データ保存システム検討委員会を設置し都合 4 回開催した。

本報告書が、電子データ保存システムの拡大の一助になれば幸いである。

平成 23 年 3 月

財団法人日本情報処理開発協会

目　次

まえがき

我が国では、2000 年に電子文書の発生が紙文書を越え、今や電子文書は社会の隅々にまで浸透し、組織内外の活動は、電子文書を抜きにしては考えられない。今後は、電子文書を記録として活用・保存していくことによって、組織内外の活動のみならず社会全体の効率を向上させていくことができる。

これを実現していくために、2005 年には e 文書法が施行され、法令等で保存を義務付けられている文書を、一部の例外を除き、電子文書・電子化文書で保存できることになり、また、2009 年には公文書管理法が公布され、政府、公共機関で取り扱う記録の全体を規定した法律も制定された。

しかしながら、組織的な運用がなされていなかったり、データの標準化が行われていなかったり、証明すべき証拠の維持方法が規定されていなかったりするなど様々な理由から、電子的な手段による記録は期待されたとおりに取得、維持、活用されているとはいえない。

このような状況を打ち破っていくためには、記録の組織的なマネジメントサイクル、長期間データ維持のための方法、証拠性を担保するための見読性、完全性、機密性、検索性の維持方式、制度面の対応方法などを運用面や利用者視点で追求し、記録のマネジメント基盤を確立していく必要がある。

また、大企業では自社内に電子記録管理のためのシステム、運用要員の確保ができるかもしれないが、中小企業では電子文書保管のための設備費や人件費を割きづらい状況にある。一部のサービス事業者が実施している文書保管サービスを利用しようとしても、その事業者がサービスを停止した場合の預けていた電子文書の取り扱いに関しては、法律的に明確になっていない。

本事業は、安心して電子文書の原本を預けることのできる保管庫について検討を進めるものである。そのためには公的な電子保管庫についての基準を定め、認定制度等により運用面、設備面において一定レベル以上に達していることを保障する必要が強く求められる。さらに、制度を整備するとともに、電子署名やタイムスタンプが付されたデータのフォーマットの標準化、保管されているデータに関する付加情報の標準化が必要である。

今回、海外の事例を参考にすべく、欧州各国の状況調査を行った。

欧州では、欧州委員会委員会のもと「域内市場におけるサービスに関する欧州議会および理事会指令案（サービス指令案)」により EU 域内でのサービスの自由移動の実現を狙っており、EU 指令 2006／123「域内のサービスの自由移動を保証するサービス指令」では、加盟国は、2009 年 12 月 28 日までに同指令を国内法化することが義務付けられた。このような背景もあり、EU 内で IT の標準化を進めている欧州各国の中から、デンマーク、ドイツ、ハンガリーの 3 カ国への訪問調査を行うとともに、英国、エストニア、チェコについては、WEB を中心に調査を行い、欧州における電子文書管理の実態を調査した。

本報告書は 3 章の構成になっており、各部の概要は以下のとおりである。

第 1 章では、欧州が標準化を進めている、電子文書管理システムに対する要求項目である MOREQ2 についての最新の状況について紹介する。第 2 章では、調査した各国の状況について報告する。

今回調査した国の文書管理システムは、各国ごとにまだまだ進化を続けているところであるが、それぞれ現時点の状況について紹介する。

第3章では、電子データ保存システム検討委員会における委員からの提言について紹介する。

本報告のテーマについては、までほとんど調査、検討されていない分野であり、提言は多岐にわたっており、課題も多く出された。今後、日本における文書管理の標準の確立に向けて、粘り強く、調査検討を続けていく予定である。

第1章　欧州における記録管理の動向

本章では、欧州における企業文書・記録管理（Enterprise Document and Records Management, EDRM）システム標準仕様の目的と成果について主に文献[1-1]に基づいて説明する。最新の欧州企業文書・記録管理（EDRM）システムの標準仕様 MoReq2 は、企業記録管理（ERM）システムの一般要件を表したものであり、2001 年に発表された MoReq 仕様に基づいている。

最初に記録の定義と ERM の主要特性及び、ERM システムについて紹介する。次に、欧州で最も一般的な電子記録管理のための標準を概観し、また MoReq2 仕様、およびその目的、構成、内容を概観する。さらに、現在進行中の MoReq2010 についても説明する。

1.1　MoReq2 仕様の目的

インターネットの使用によって、デジタル情報を作成、共有、活用、保存する作業環境が高性能になるに従い、日常の業務においてデジタル情報を作成、共有、活用、保存する能力の重要度もかつてないほど高まっている。しかし、このような変化は「情報」、「コミュニケーション」、及び「知識」に対する理解に大きな影響を与えており、次のような重大な多くの疑問を引き起こしている。つまり、信頼可能な情報とは何か、効果的なコミュニケーションの方法とは何か、アーカイブにおいて知識をどのように展開、維持すればよいか。ビジネス・ソリューションを考える前に、この疑問について、テクノロジー、組織、政府という 3 つの領域それぞれで答えなければならない。

- テクノロジー領域の課題としては、地理的に分散した、ビジネス上の重大で機密性の高い膨大なデータを、どう取り扱い、保護するかの問題に対処しなければならない。
- 組織的な課題としては、業務プロセスの刷新と、伝統的なアーカイブ内の紙文書を取り扱い、保管する方法の革新がある。アーカイブがデジタルデータを意識しその保存、管理、検索、廃棄のプロセスを取り入れるためには、利用者の役割と責任の見直しも必要になる。
- 政府領域の課題は、電子アーカイブの実現に対する最大の障壁を表している。その最重要の仕事は、法律と規制の面で、デジタルデータの適法性と信頼性を確保することある。

電子アーカイブの主なメリットは、次のものがあげられる。

- データの管理と保護を、離れた場所にあるセンターから行える。
- デジタル形式の文書は、大勢の要員や、火災、洪水、凍結、カビの発生を招くような高温から守る大きな部屋などを特に必要としないため、物理的な保管コストがなくなる。
- 分散したオフィスという問題も回避できる。

しかし、デジタル・アーカイブを実現することの最大の理由は、完全に電子的なビジネス基盤の実現である。電子アーカイブに基礎を置いたビジネス情報システムによって、企業はビジネス活動の真正で法的な証拠としてのデータの取得、生成からその処理、分類、保管まで、全プロセスを自動化できる。

企業記録管理(ERM)システムは、このような必要性の結果として策定された。その主な目的は、電子および物理的記録の管理が可能なデジタル・アーカイブを構築するための、バックボーンの提供である。ERM システムは、その主な機能としてコンテンツの生成と取得、その格納、検索、

長期および短期の保存、および整理、廃棄を行う。今日そのようなシステムは、ペーパーレス・オフィスとも呼ばれる電子文書オフィスの構築に必要となってきている。ERM システムの主な役割は、情報の要求に対する応答時間の短縮、紙の冗長と重複の除去、また法律と規制という面でデジタルデータの適法性と信頼性を維持しつつ、記録管理サイクルから最終的に紙をなくすることである。

1.2 企業記録管理（ERM）システム

ERM システムについての一般的な定義はない。今日主に定義と言えるのは、企業コンテンツ管理システムのベンダーが定義する、電子記録管理製品の簡単な商品説明である。しかし ERM の機能は、主に各国の公文書館が定義する要件によって指示されている。このような要件は、アーカイブ内の物理記録を管理・構成するための、長い間の進化、伝統の結果としてもたらされている。そして、各 ERM システムの違いとは、主にアルゴリズムの具体化（セキュリティ・アルゴリズムなど）、技術サポート（他のシステムとの統合など）、付加的な機能（拡張オブジェクト・モデルなど）の差となっている。しかし、ERM システムの定義を考える上で近年に最もよく参照されるようになった文書として、ISO 15489-1:2001（ISO）標準[1-2]がある。

(1) 記録

ISO 15489-1 標準では記録を、「法的義務に従い、または商業取引の上で組織または個人が証拠および情報として作成、受領、維持する、全形式の記録された情報」と定義している。この ISO 15489-1 による記録の定義では、2 つの重要なポイントに注目しなければならない。まず第一に、この定義は全種類の記録（デジタル記録、紙の記録、物体など）に対して開かれている。第二に、記録とは商業行為、取引やその他の行為（契約など）の証拠である。ISO の定義によると、記録が正式であるためには以下が必要である。

・真正性（Authenticity）

真正な記録とは、次のことを立証できるものとする。

a）記録が主張しているとおりのものであること。

b）それを作成又は送付したと主張する者が、作成又は送付していること。

c）主張された時間に作成し、送付していること。

記録が真正であることを確実にするために、組織は、記録作成者に権限を与え、それがだれかを明確にすることが望ましい。許可のない記録の追加、削除、変更、利用及び隠ぺい（蔽）から確実に記録が守られるように、記録の作成、取得、送信、維持及び処分を管理する方針並びに手順を実施し、文書化することが望ましい。

・信頼性（Reliability　文書化された行為を正確に反映する、信頼可能な内容）

信頼のおける記録とは、その内容が、処理、活動又は事実が完全であると信じることができ、そして継続して起こるその後の処理及び活動の過程を証明し、かつ、よりどころとすることができるものをいう。記録は、関連する処理又は事象の発生時に、又はその直後に、事実について直接知っている個人によって、又は処理を行う業務で日常的に使われる機器によって作成されることが望ましい。

・完全性（Integrity）

記録の完全性は、その内容が完結していて変更されていないことを意味する。記録は、許可のない変更から守られなければならない。記録管理の方針及び手順は、記録作成後どんな追加又は注釈が許されるのか、どのような状況で追加又は注釈が許される場合があるか、だれに追加又は注釈を入れる権限があるのかを定めることが望ましい。どのような追加、注釈又は削除でも、それが明示され追跡可能になっていることが望ましい。

・利用性（Useablity）

利用できる記録は、所在場所がわかり、検索でき、表示でき、解釈できるものをいう。記録は、それを作り出した業務活動又は業務処理に直接関係するものとして、その後、提示できるものであることが望ましい。記録のコンテキストのつながりには、記録を作成し利用した業務処理の理解に必要な情報を含むことが望ましい。より広い業務の活動又は機能のコンテキストの中で、記録を見つけることが可能であることが望ましい。一連の活動を文書化した記録間のつながりを、維持することが望ましい。

文書と記録との違い、類似点を認識することが重要である（表 1.1）。

表 1.1：文書と記録との相違点（文献[1-1]の表を元に作成）

文書	記録
取り扱い可能な一片の情報	取り扱い可能な一片の情報
重要あるいは非重要	決定や行為の重要な証拠を表す
所有者（通常は作者）の管理下	組織の管理下
自由に変更が可能	変更は不可
自由に削除が可能	通常は削除不可

(2) 記録管理

記録に加えて、ISO 15489-1 標準は記録管理についても次のように定義している。- 「ビジネス活動および取引に関する情報の証拠を記録の形で取得および維持するプロセスを含め、記録を作成、受領、維持、使用、廃棄することの効率的で体系的な制御を行う、管理の分野。」

ERM システムは、電子形式または物理形式にかかわらず、すべての記録特性を確保しながら、記録の管理を行うシステムである。ISO 標準に従って、ERM システムは以下を提供しなければならない。

・完全で系統的、アクセス可能で保護された記録の信頼性
・権限制御システムによる保護された完全性
・法律、規制上の、および適切なビジネス要件への準拠
・適切なビジネス活動が反映された包括的範囲
・記録の体系的な作成、保存、管理

今日 ERM システムは通常、電子文書管理（Electronic Document Management, EDM）システムとの統合により、企業文書・記録管理（Enterprise Document and Records Management, EDRM）シ

ステムを形成している。これら 2 システムの相乗効果により、EDM の文書指向協働機能と ERM の分類、準拠、保存、整理、廃棄機能とが結合する。ERM システム内のケースファイルと、適切なケースファイル・ワークフローとの橋渡しとして、ビジネス・プロセス管理（Business Process Management, BPM）システムを使用できる。

ユーザー・インタフェースのカスタマイズや記録取得の自動化のため、電子書式（eForm）など他の技術も追加ツールとして使用できる。

ERM（または EDRM）システムは一般に、組織の全情報資産をライフサイクルにわたって管理する、企業コンテンツ管理（Enterprise Content Management, ECM）システムの範囲内に入る。

(3) 記録管理標準

各国の公文書館は間接的に ERM システムの機能を形成しているが、いまだ解決されていない機能性の問題が残っている。もっとも大きな問題は、各国の公文書館の間での、実行方法の違いである。欧州連合（EU）諸国間での、記録管理の実行方法は類似しているが、小さな相違はまだ残っているため、特定の機能について個々の実行方法が必要になっている。

さらに、ほとんど全 EU 諸国は、記録管理に対して自国の標準を規定している。EU レベルでの記録管理標準が存在しないため、主要な ERM ベンダーは主に英国の PRO/TNA 標準だけに対して、自身の ERM システムを認証するようになっている。これが、小さな EU 諸国でアーカイブのデジタル化を遅らせ、ひいては真の電子ビジネスの実現を遅らせている。

1.3 EU 諸国の記録管理標準

EU 諸国で最も一般的な記録管理標準を説明する[1-1]。

(1) DOMEA（ドイツ）

DOMEA コンセプト(電子ビジネスでの文書管理と電子アーカイビング(Document Management and Electronic Archiving in Electronic Business)、「ペーパーレス・オフィス・コンセプト」としても知られる）は、ドイツにおける電子記録実現のための最も重要なガイドラインである。これは組織コンセプト、要件カタログ、拡張モジュールの主要 3 部から構成されている。IT ベンダーは ERM システムを DOMEA に準拠して認証する義務はないが、ドイツ、オーストリア、およびスイスで 170,000 件の DOEMA ライセンスが承認されている。

(2) ELAK（オーストリア）

ELAK（Electronic Act）は、連邦内記録管理の簡素化および整理統合のための、オーストリア連邦政府プログラムである。DOMEA に加えて、ELAK コンセプトは ERM システムの要件および機能の、より技術的な詳細を説明している。さらに、公開入札募集で何を考慮する必要があるかの例を示している。

(3) Gever（スイス）

Swiss Gever は電子記録管理、および紙ベース記録管理の放棄を導入する、5 つの標準を集めたものである。5 つの標準は以下のとおりである。

・ビジネス管理、法的不履行に関連した方法と機能
・GEVER 連合ビジネス・モデル
・GEVER アプリケーションのサービス・カタログ
・GEVER メタデータ。

(4) Protocollo Informatico/CNIPA（イタリア）

CNIPA（行政における情報技術のための国立センター（National Centre for Information Technologies in Public Administration)）は、サービス品質の向上と行政コストの削減維持を図る情報システムの構築のために、イタリア行政を支援する政府機関である。CNIPA が公開する Protocollo Informatico は、文書管理のために行政が使用する、リソース・フレームワークとしての電子プロトコルを説明している。

(5) ReMANO（オランダ）

ReMANO は、オランダ行政機関における ERM システム・ソフトウェアの仕様カタログである。これは 2004 年に公表された。

(6) NOARK（ノルウェー）

NOARK-4 は、ノルウェーの公共機関すべてで使用される、ERM の機能要件仕様およびケース管理システムである。

(7) PRO/TNA（英国）

PRO/TNA 文書は、英国公文書館（Public Records Office, The National Archive）が策定した。その主な目的は、電子記録管理をサポートするための、政府省庁のベンチマーク機能を提供することにあった。PRO/TNA は EU における最も総合的、一般的な標準であったが、MoReq 仕様に置き換えられた。

1.4 MoReq2 仕様

EU には、各国の記録管理標準が多数ある。しかし EU 全体の標準がないため、欧州電子政府サービスの、行政、企業、国民への相互利用可能な配信を複雑なものにしている。i2010 電子政府行動計画（i2010 eGovernment Action Plan）[1-3]は、電子政府を通した国民・企業への具体的メリットの提供促進を主要目的のひとつとしているが、この状況はそれに相反するものとなっている。

政府機関のための ERM システム要件の包括的仕様が必要なことは、1996 年の DLM フォーラムで初めて明確な議題となった。DLM（Document Lifecycle Management）フォーラムは、欧州委員会が設立した学際フォーラムである。その主要目的は、- 加盟国との緊密な協力のもとで - 電子アーカイブの分野での、加盟国間および EU レベルでの幅広い協力の可能性を調査、促進、実現することにあった。

1999 年、DLM フォーラムは、「行政における電子文書・記録管理のための参照モデルを策定する」という行動計画を発表した。

仕様の策定作業は2000年に開始され、2001年に終了した。2001年に最初に電子化され入手可能となったMoReqは、2002年はじめに欧州委員会により INSAR（Information Summary on Archives publication、アーカイブに関する情報要約の公開）補遺として公表された。

この仕様は、ERM システムの機能性要件と非機能性要件を含んでいる。機能性要件は、以下のような項目を取り扱っている。

ERMシステム機能の概要、分類体系、制御とセキュリティー、保存と廃棄、記録の取得、検索、回復とレンダリング、管理機能、その他の機能。

メタデータ・モデルなどの非機能性要件は、環境に伴って大きく変化しうる。したがって、MoReq仕様は非機能性要件の概略のみを特定、説明している。

この仕様では、ERM システムは管理者・保管員（記録の管理に責任を負う要員）だけでなく、記録の作成、受け取り、検索に関与する、すべての一般オフィスや業務スタッフにも導入されるべきことを示唆している。そのため、MoReq 仕様は文書管理やケース管理など、記録管理に密接に関連した要件もカバーしている。しかしこれらの要件は、機能性要件に比べれば詳細度は低い。

1.5 MoReq2 プロジェクト

2006年に、DLMフォーラムは「電子記録管理のためのモデル要件策定のためのスコーピング報告書（Scoping report for the development of the Model Requirements for the management of electronic records：MoReq2)」を公表した。この文書は、旧版からの変更詳細の概要を述べている。このスコーピング報告書によると、MoReq2策定の全体的目標は、欧州を背景とする中での拡張された機能要件を開発し、以下によるコンプライアンス・スキームをサポートすることにある。

・これまでに重要となった分野の、MoReqからの強化と、要件の重要な新分野の明確なカバー
・機能要件が検査可能であることの確認と、要件への準拠に対して製品を検査可能な検査材料の作成
・要件が使用されうるさまざまな環境での適用を支援するための、要件のモジュラ化

MoReq2プロジェクトは2007年に開始され、MoReq2仕様が2008年の初めに正式に公開された。

(1) MoReq2 仕様

MoReq2仕様はERMシステムのための、必須および任意の、機能要件および非機能要件の集合である。必須機能はMoReq2への準拠のために強制であるのに対して、任意要件は望ましいが強制ではないERMシステム特性に対応している。必須および任意の要件は、コア・モジュール（MoReq2準拠のために必須のモジュール）とオプション・モジュール（ERM システム・プロバイダーは特定のオプション・モジュールのために追加のソフトウェア認証を選択できる）とにグループ化されている。コア・モジュールは、分類体系とファイル構成、制御とセキュリティー、保存と廃棄、記録の取得と宣言、参照、検索、回復と表現、ERM システム管理に関係した要件を内容としている。

オプション・モジュールは - 物理的(非電子的)ファイルおよび記録の管理、物理記録の廃棄、文書管理と協働作業、ワークフロー、ケースワーク、コンテンツ管理システムとの統合、電子署名、暗号化、デジタル権利管理、分散システム、オフライン／遠隔作業、ファックスの統合、セ

キュリティー・カテゴリである。

(2) メタデータ要件

メタデータ要件は、MoReq2 仕様のもうひとつの重要なパートを表している。ダブリン・コア・メタデータ基本記述要素集合（Dublin Core Metadata Element Set）を基本にした MoReq2 メタデータは、アクセス制限情報など、効果的な記録管理に必要な索引情報などのデータを含んでいる。可能な全種類の ERMS 実現のための、全メタデータ要件を定義するのは不可能なため、MoReq2 は、カスタム化と拡張の開始点として意図された最少限の要件を提示している。これらの最少要件は、ERM システムが取得および処理できなければならない、特定のメタデータ「要素」のリストと密接に関連している。

(3) 仕様のローカライゼーション

仕様のローカライゼーションについては、特別な注意が払われている。それぞれの国が、電子記録の管理に関し特別の要件を必要とすることが考えられるので、「第 0 章」が MoReq2 構造には組み込まれている。このチャプターは、ある国の特別なニーズを表すために使用できる。このチャプターによって MoReq2 仕様を拡張する場合の唯一の制限は、チャプターの内容が MoReq2 の残りの内容と相反してはいけないことである。

生み出される情報量の増加、また情報形式の多様性によって、電子記録の管理という課題はこれまでになく大きなものとなっている。新たなテクノロジーの具体化に対処し、また、法律および規制の面でデジタル記録の信頼性を実現するために、個々の国が電子記録管理のための仕様を導入し始めた。しかし、異なった仕様の多様性は、EU 諸国間でのデータの相互運用を難しくする。

MoReq2 は、記録管理ソフトウェアの標準および実施を、欧州全体で統一するプロセスの一歩前進を示している。これにより政府や企業は、その最重要の記録を管理するための、単一のアプローチが提供されることになる。このように MoReq2 は、政府行政、企業、国民の間での、より高い相互運用性の達成に大きく寄与するものとなる。このことは、欧州連合の i2010 電子政府行動計画の目標達成をも意味している。

1.6 MoReq2010

現在、DLM フォーラムにおいて MoReq2 を改定中である。改訂版は MoReq2010 と呼ばれており、次のような変更が計画されている（2011 年 2 月時点のドラフト）。

- 仕様の位置付けを、電子記録管理要件から記録システム要件（Model Requirements for records systems）に変更する。
- DLM Forum 認定試験センターの認証対象とする方針が打ち出され、これに伴い、仕様を ISO 15489、ISO 23081 準拠とすることを原則とした。
- 分類体系とファイル構成について、従来の階層型から非階層、シソーラス導入へとシフトし、階層型を既存との互換用とした。また、ファイル、サブファイル、ボリュームの区別を廃し、ISO 15489 に合わせて Aggregation に変更する。
- スキャニング、e メール、利用者管理は、スコープの対象外に位置付ける。

・バックアップ（機能要件）を事業継続（非機能要件）に位置付け直す。
　また、次の機能が追加された（主なもののみ記載）。
・認証に伴う評価の必要性から GUI、API が定義される。
・記録を構成するコンポーネントの管理が詳細に定義される。
・処分トリガを与えるインベントリが明確化される。
　更に、機能ブロック単位に版管理が行えるよう、仕様の構成の組み替えが行われる。

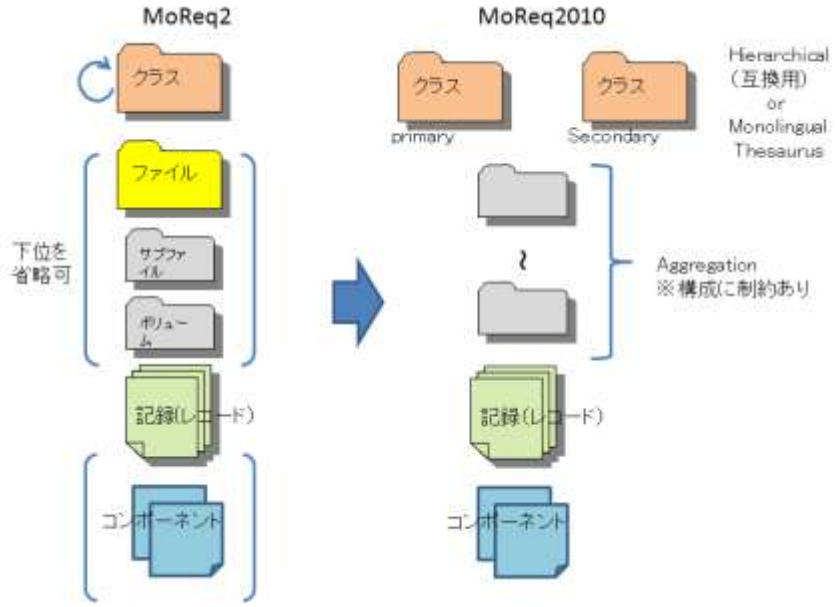


図 1.1：分類体系とファイル構成

【参考文献】

[1-1]″Electronic Records Management System Requirements″ M. Lukicic, V. Sruk, INFuture2009
[1-2]″ISO 15489: Information and documentation - Records management″, ISO 15489-1:2001(E).
[1-3] ″European Communities. i2010 eGovernment Action Plan″, Communication from the Commission, 2006

【参考】

ダブリン・コア・メタデータ要素セット（ISO-EVS 15386:2004）

ダブリン・コア（Dublin Core）は全タイプの情報リソースについて、そのメタデータ要素を記述するための標準である。これは非常に普及しており、たとえば OpenOffice 文書の意味的記述にも組み込まれている。この標準は、欧州でも一般的なものとなってきている。

以下に、記述の編集に有用と思われるダブリン・コア・メタデータをリストで示している。

要素名	識別子	定義	コメント
Title	Title	リソースに与えられた名前	通常、Title（タイトル）は、リソースが公式に知られる名前を指す。

Creator	Creator	リソースの作成に主たる責任を持つエンティティ	Creator（製作者）の例としては個人、組織、サービスなどがある。通常、このエンティティを示すためにCreatorの名前を使うべき。
Subject	Subject and Keywords	リソースのトピック	通常、Subject（主題）はキーワード、キーフレーズ、分類コードなどを使って表す。推奨される最良実践としては、統制語彙や公式の分類体系からの値を選択する。
Description	Description	リソースの説明	Description（説明）には以下が挙げられる（これらに限らない）：要約、目次、画像表現、リソースの自由形式の説明など。
Publisher	Publisher	このリソースを利用可能とすることに責任を持つエンティティ	Publisher（発行人）の例としては個人、組織、サービスなどがある。通常、このエンティティを示すために Publisher の名前を使うべき。
Contributor	Contributor	このリソースに寄与することに責任を持つエンティティ	Contributor（貢献者）の例としては個人、組織、サービスなどがある。通常、このエンティティを示すために Contributor の名前を使うべき。
Date	Date	リソースのライフサイクルにおけるイベントに関連した時間もしくは期間	通常、Date（日付）はリソースの作成や入手性に関連付けられる。Date 値の符号化に推奨される最良実践としては、ISO 8601 [W3CDTF]のプロファイルによる定義があり、YYYY-MM-DDの形式に従う。
Type	Resource type	リソースの性質もしくはジャンル	Type（タイプ）には一般的カテゴリ、機能、分野、内容の集約度などが含まれる。推奨される最良実践としては、統制語彙（例：DCMI Type Vocabulary [DCT]）からの値を選択する。
Format	Format	リソースの物理的あるいはデジタル的発現	通常、Format（フォーマット）にはリソースのメディアタイプ、大きさなどが含まれる。Format はリソースの表示や操作に必要なソフトウェア、ハードウェア、その他の装置を決定するために使用できる。大きさの例にはサイズや時間などがある。推奨される最良実践としては、統制語彙（例：インターネット・メディア形式 [MIME]）からの値を選択する。

Identifier	Resource Identifier	あるコンテキストでの、リソースへの一義的な参照	推奨される最良実践としては、公式の識別体系に従った文字列や数字によってリソースを識別する。 公式の識別体系にはURI（Uniform Resource Identifier）（URL（Uniform Resource Locator）も含む)、デジタル・オブジェクト識別子（Digital Object Identifier）(DOI)、ISBN（International Standard Book Number、国際標準図書番号）などがある。
Source	Source	現在のリソースが由来するリソースへの参照	記述されるリソースは、関連するリソースから全体的に、または部分的に由来する場合がある。推奨される最良実践としては、公式の識別体系に従った文字列や数字によって、関連するリソースを識別する。
Language	Language	リソースの知的内容の言語	Language（言語）要素の値に対して推奨される最良実践としては、RFC 3066 [RFC3066]の定義がある。ISO 639 [ISO639]標準に従ったこの文書には、2文字または3文字の言語コード、および必要に応じたサブコードが示されている。
Relation	Relation	関連するリソースへの参照	推奨される最良実践としては、公式の識別体系に従った文字列や数字によって、関連するリソースを識別する。
Coverage	Coverage	リソースの程度または範囲	通常、Coverage（対象範囲）には場所（地名や緯度経度)、時間区分（時代、日付、期間など)、管轄区分（例：行政主体名）などが含まれる。推奨される最良実践としては、統制語彙（例：Thesaurus of Geographic Names [TGN]）からの値を選択する。また適切な場合には、地名や時代区分名を、緯度経度、期間などの数値表現よりも優先して用いる。

第2章　欧州先行事例調査

EU 内で IT の標準化を進めている欧州各国の中から、デンマーク、ドイツ、ハンガリーの 3 カ国への訪問調査を行うとともに、英国、エストニア、チェコについては、WEB を中心に調査を行い、欧州における電子文書管理の実態を調査し、調査結果をまとめた。

2.1　調査概要

今回訪問調査を行ったデンマーク、ハンガリー、ドイツ、並びに Web 調査を行ったエストニア、英国、チェコに関して、各々の電子記録管理システム及びその環境について調査概要を以下に記す。

(1) デンマーク

デンマーク（デンマーク王国）は、人口 550 万人で、国連調査の電子政府ランキング（United Nations E-Government Survey 2010）は 7 位であるが、労働人口 290 万人のうち、39%が公務員といった特殊な状況にある（欧州の平均的な割合は 15%といわれている)。

デンマークは、電子政府推進と同時に、行政の大幅改革を断行し、108 あった県を 9 に、1388 あった市町村を 98 に統廃合している。このような背景は、記録管理の推進に大きく影響していると考えられる。

記録管理については、2002 年から CASE マネジメントを導入し、2004 年から電子記録管理システム FESD を導入し公共部門の記録管理標準化をはかったが、システムの柔軟性に欠けていたため、アーキテクチャをサービス指向（SOA）に切り替え、標準 I/F による統合と連携をはかり、2009 年から FESDⅡとして提供されている。

デンマークは、中央省庁、県、市町村が一体となって、記録管理も含めたシングルソリューションを目指している。実現には、中央省庁、県、市町村にまたがって適用する標準の存在が重要である。記録管理のための標準は、大きく技術標準とセマンティック標準の 2 つに分けられている。技術標準は、基本的には ISO や EU 標準の内から必要な標準を“選択”することであり、比較的容易である。一方のセマンティック標準は、例えば、教育に関する標準など、合意形成は困難が伴い、かつ見直しが頻繁に行われている。

FESDⅡの特徴としては、サービス志向（SOA）であること、CASE 管理に重点を置いていることがあげられる。署名やタイムスタンプは付与していない。

メタデータは、基本的に、ワードなどのプロパティに入っているメタデータ（作成者や作成日など）は使わず、別途データベース上でメタデータを管理している。署名、タイムスタンプ、他の文書との相互関係（本体と付属資料など）も全てデータベース上のメタデータとして管理される。データベースアクセスに関しては、更新の前と後のデータが CASE ファイルに格納される。

署名、認証に関しては、従来はソフトベースの電子署名や電子認証を行ってきたが、市民に秘密鍵も管理させることへの問題と、モバイルで使えないことに対する問題解決方法として、認証は ID、パスワードとテーブル方式に切り替え、秘密鍵はセンターサーバに置く方式に切り替えている（カナダのトゥルーパスと同じ発想)。

CASE ファイルは案件が終了するとクローズされて、5 年経過するとアーカイブス（公文書館）に送られる。

記録の再利用に関する工夫点としては、ケースタイプなどの分類方法と適切な名前付けに留意していることが挙げられる。

(2) ハンガリー

ハンガリー（ハンガリー共和国）は、人口 1100 万人で、国連調査の電子政府ランキングのベスト 20 には入っていないが、2010 年に東欧ではトップの座についた。労働人口 378 万人で、欧州の他の国に比べて人口に占める割合が少ないが、失業率は 10%にのぼる。

ハンガリー政府は、縦割り意識が根強く残っており、各省庁単位に要求事項が異なっているという現状である。そのなかで、Microsec 社が開発した記録管理サービス基盤である Dossie がデファクトとしての共通仕様の役を担っている。Microsec 社は、ハンガリー資本のハンガリーを代表する認証局（ハンガリーに 3 つある認証局の一つ）及びタイムスタンプ局を運営しており、電子署名に関する開発も行っている。提供するタイムスタンプは適格（Qualified）タイムスタンプを提供しており、欧州圏で適格タイムスタンプを提供しているのは、他に、ドイツ、イタリアがある。タイムスタンプの時刻源は、ドイツの標準時と GPS から得ている。ハンガリーは MKEH（ハンガリの国家標準計量機関）が UTC（Universal Time, Coordinated）を決定するネットワーク BIPM（International Bureau of Weights and Measures）に加入しているが、時刻情報を配信するには至っていない。

電子記録の保存サービスは、Dossie と呼ぶパッケージを単位に管理している。Dossie は、XML ベースのパッケージ構造をもち、任意のドキュメント（ワードや PDF など）、電子署名、タイムスタンプ、ダブリンコアメタデータから構成される。個々の Dossie は、Dossie 自身のハッシュ値（SHA256）で識別している。電子署名は、個々のドキュメント単位ではなく、Dossie 内のすべてのドキュメントとメタデータに対して付与される。適用される署名仕様は XML ベースのアドバンス電子署名（XAdES）である。

長期保存目的のタイムスタンプは、ドイツと同様、複数の署名付き文書にまとめてタイムスタンピングする LTANS の ERS（証拠記録構文、RFC 4998）を適用している。

電子保存サービスでは、文書保存受付時に署名の検証を実施している。検証が失敗した場合は保存を受け付けない。失効情報は OCSP で提供され猶予期間（Grace period）は 3 日である。一旦保存が受け付けられた後、猶予期間内で失効が判明した場合の処置については、現時点ではその扱いは明確には決まっていない。

なお、Dossie をベースとするサービスは、顧客との契約で 50 年までの保管ができる。

また、電子保存サービスのアベイラビリティは 99%（主として計画停止）であり、一方、認証局 CA とタイムスタンプ局のアベイラビリティは 99.99%を確保している。

(3) ドイツ

ドイツ（ドイツ連邦共和国）は、国土の面積が 35 万 7 千 km^2（日本の 94%）、人口が 8200 万人で、欧州各国のなかでは最も人口が多い（2 位はフランスで 61 百万人、3 位は英国で 60 百万人、4 位はイタリアで 50 百万人）。首都ベルリンの人口は 366 万人である。電子政府の 2010 年のラン

キングは、15 位である（日本は 17 位）。ドイツにおけるインターネット普及率は、75.5%で米国、英国、韓国、日本などの最先進諸国と同様の水準にある。

ドイツ政府は、2001 年 11 月に BundOnline2005 を発表し、2005 年に全ての行政サービスを電子化し、インターネットを利用して提供することを目標とした。フラウンホーファーSIT は、BundOnline2005 プロジェクトにおいて、電子署名方式 ArchiSig、その実装 ArchiSoft、署名付き文書のフォーマット変換ツール TransiDog、文書管理体系 ArchiSafe の提案に深く係ってきた。

電子文書保存に係る ArchiSafe の戦略は、オーストラリアのビクトリア政府提唱の VERS（ビクトリア州電子記録戦略）と ArchiSig に基づいている。VERS は電子記録の高信頼且つ本格的な保存を可能とする記録保持（Recordkeeping）の枠組みである。ArchiSafe システムの特徴は、XML によるデータパッケージの定義と、データパッケージに対するユニーク ID の付与である。データパッケージは、文書、管理情報（メタデータ）、電子署名、証明書、タイムスタンプが格納できるようになっている。ここに格納されるタイムスタンプ（前述の ArchiSig の成果）は、紙文書でよく見受けられる受付印を目指したものであり、データパッケージに格納される文書が署名されているか否かは問わない。また、署名時刻の表示（署名タイムスタンプ）はサーバの時計を使用している。なお、データパッケージに対するユニーク ID は UUID（Universally Unique Identifier）が使われている。

ArchiSafe と ArchiSig の成果は、BSI TR 03125（Reliable long term archiving of electronic documents）として標準化された。

BSI TR 03125 は、ドイツ政府の要求、基本仕様、eCard の API、証拠記録構文（ERS）、暗号アルゴリズム関係の構造（DSSC）に関する規定から構成されている。また、典型的なアーカイブシステムとして、E メールや ERP などのアプリケーション層、アーカイブミドルウェア層、ストレージ層の 3 層構造を想定している。アーカイブミドルウェア層での処理単位はオブジェクト、ストレージ層の処理単位はデータパッケージである。

BSI TR 03125 は、いろいろな枠組みを取り込んだ複雑な構造をもつため、今後広く受け入れられるかは未知数であり、政府も導入可否を検討中の状況にある。

ドイツの電子記録市場は、EU 指令により e-invoice（電子的な請求書）に電子署名が不可欠なこともあって、ドイツの電子署名関連市場の 2/3 は e-invoice である。しかし、インボイス全体に占める e-invoice の割合はまだ低く、大半は紙のままである。

(4) エストニア

エストニア（エストニア共和国）はヨーロッパ北部に位置し、九州よりやや大きい国土に、福岡市とほぼ同数の約 135 万の人々が住み、首都タリンには人口の約 30%にあたる 39 万 6 千人が住んでいる（一極集中により人口が密集していると言われる東京都でも約 10%である）。

エストニアの電子文書管理の特徴は、SOA アーキテクチャに基づく国家の IT 基盤としての X-Road と文書交換センター（DEC）である。エストニアは、技術的な相互運用性、セキュリティー、オープン性、柔軟性。拡張性を確保すべく国家の IT アーキテクチャとして SOA を全面的に導入した。

X-Road（XML の道）は、SOAP（Service Oriented Application Protocol）の交換をサービスするネットワークである。X-Road を利用することで、インターネットを介した安全なデータ交換を

可能にしている。

システム間のデジタル文書交換への移行は政府機関の効率を大幅に改善する。文書交換センター（Document Exchange Centre：DEC）は中央情報システムとして、各所に分散する記録管理システムを X-Road を介して結合する。センターの基本的な役目は文書(特にデジタル署名された文書)を転送することである。転送には 3 つの方法がある。

① 記録管理システムが用意されている公共機関の場合、その記録管理システムは DEC に接続されており、DEC が他の公共機関の記録管理システムへの文書転送を可能にする。

② 記録管理システムが公共機関に用意されていない場合、DEC が e メールによって文書を転送する。

③ ユーザーである市民が e メールで文書を DEC に送信し、DEC がその文書を適切な機関へ転送する。公共機関は市民に（直接に、または DEC を介して）e メールで返答する。

将来的には、DEC はレターだけではなく、法律文書、財務文書、インボイスなどの送信にも使われる。

記録管理システムの相互運用性、さらには公共機関間の自動的でセキュアなペーパーレスな文書交換のために、DEC のサポートに加え、転送された文書とそのメタデータの統一化が行われている。DEC を介した記録管理システム間のデジタル文書の交換では、XML（Extensible Markup Language)の文書形式が使われる。文書の内容の統一的なプレゼンテーションを保証するために、公共機関は DEC を介して転送される XML ベースの文書のプレゼンテーション形式を総理府とコーディネートし XML ベースのプレゼンテーション形式をデータベースに格納することによって、統一的なプレゼンテーション形式の再利用を可能にしている。

(5) 英国

正式な国名は、グレートブリテン及び北アイルランド連合王国（United kingdom of great Britain and Northern Ireland)。人口は 6179 万人で日本の 1/2、国土は、24 万 2 千 km^2 で日本の 2/3 である。労働人口は 2916 万人で、うち 13%が外国人労働者、民間部門労働者数は約 2300 万人、公共部門が約 600 万人である。

英国では、1838 年（日本では天保年間にあたる）に公記録法が制定された。現行法は 1958 年公記録法（Public Records Act）である。1958 年公記録法第 3 条は、公記録に責任を有するすべての者が永久に保存すべき記録の選別と安全な保管のための準備を行うよう義務づけている。

1998 年にはデータ保護法が制定された。データ保護法は、健康や国家安全保障など特別理由があるものを除き、個人情報を保持する行政上のすべての必要性がなくなった時点において当該情報を処分する必要があることを規定している。

2000 年には情報自由法が策定され（英国では、記録（records）と情報（information）は同じものとして理解されている)、公文書について、従来の 30 年という一般公開までの基準が廃止された。ただし、防衛、国家の安全、個人情報には例外が適用される。

文書管理のルール（規程やマニュアル類）については、2000 年情報自由法第 46 条に基づいて大法官が定める行為規範が2008年7月に改定され､その中で保存期間のガイダンスも定められた。あくまでもガイドラインであり、各省庁がその枠内で意思決定をする。また、永久に保存する必要のある公文書に関しては、公文書館が永年保存基準（acquisition policy）を作成し、公文書

館と各省庁が共同で選定方針を作成し移管を行う。

英国には、共通化された電子文書保存システムは存在しない。各省庁の判断で、予算に応じて必要なシステムを調達している。今回調査した各国が共通のシステムを提供しているのとは対照的である。

(6) チェコ

チェコ（チェコ共和国）は面積 7 万 9 千 km^2（日本の 5 分の 1 弱)、人口は 1050 万人である。2004 年 5 月に EU に加盟した。

電子政府の実現度については､ハンガリー､ポーランドとともに東欧ではトップクラスにある。

チェコでは、公共業務の領域で情報・通信技術を利用することは、当然のことと考えられていたが、テクノロジーの多用が、行政サービスの質や効率の向上を意味するわけではなく（近年では、小さな村から省庁にいたるまで、役所には最新の ICT 機器が備わっている)、国民が行政手続の簡素化という形で利益を受けることがなかった。

このため、法律、方策、および組織的な観点からプロセス全体と手段を見直し、国民、役人、法律、テクノロジー、予算、場所（窓口）のバランスがとれた電子政府へキサゴンと呼ばれるシステム戦略を策定した。

チェコにおける電子データ管理は、申請書類や要請を提出するための信頼可能な場所（Czech POINT)、行政機関からの応答を得るためのデータボックス、そして電子文書の長期保存（これが現在最も問題となっている）の 3 つの要素からなる。

Czech POINT は補助員付きの行政端末である。誰でも、全官庁および公共機関と簡単に電子的に通信できるようになる。

データボックスは、「電子運用と認定文書変換に関する法律（Act on Electronic operations andauthorized document conversion, No. 300/2008 Coll.)」に基づき、2009 年 7 月 1 日に初めて導入された。データボックスは全法人（公共機関と、企業登録に登録されている企業）に使用が義務付けられ､自然人と､企業家として登録している自然人は､要求した場合のみ使用できる。

データボックスは、電子メールとは異なり、ユーザーは公共機関自体とのみ通信が可能で、特定の役人や自然人/法人との通信にこれを使用できない。データボックスは､ユーザーと公共機関との間の通信を支援するために設計された電子ストレージであり、これを使用して、公共機関との間の文書の電子提出および受信を行う。この電子通信はハードコピーの送付という従来のシステムに置き換わり、行政をより効率的、低コスト、迅速にするものとなっている。現在、地域および中央の機関によって約 7,000 のデータボックスが、また法人および自営業の自然人によって約 250,000 のデータボックスが使用されている。行政上も、主に所轄公共機関の間で新形式の通信が行われている。

長期保存に関しては、現在、検討段階であり、さまざまな可能性が議論されている。その 1 つに、安全な保管庫（リポジトリ）を作る案がある。保管庫に保管の後、認証された機関が署名を検証しその文書を証明する。この機関はその証明書によって当該文書が変更を受けていない原本であることを保証する。

もう 1 つの可能性として文書の再署名があり、この場合には、証明書が失効する前に文書は再署名される必要がある。このような手続きは積極的保存(active preservation)と呼ばれている。

2.2 調査結果結果

2.2.1 デンマーク

2.2.1.1 デンマーク基本情報

北欧諸国の中で最も南に位置し、ヨーロッパ大陸と陸続きのユトランド半島と 500 以上の島々からなる。正式国名はデンマーク王国（英語表記は Kingdom of Denmark）であり、面積は約 4.3 万平方キロメートル（九州とほぼ同じ）の広さに人口は約 550 万人（北海道とほぼ同じ）の人が住む。首都はコペンハーゲン。

日本では、なだらかな国土で酪農が盛んなので農業国と思いがちだが、産業構造（GDP に占める割合：2009）から見ると、農業は 2%にも満たない。

表 2.1：産業構造

農業:	1.57%
工業.：	23.64%
サービス業:	74.79%

政府の下に、5 つの県（Regions）と 98 の市町村（Municipalities）がある。それぞれ役割が明確になっていて、市民サービスは市町村の役割になっている。予算配分は、政府(30%)、県(22%)、市町村（48%）となっている。

1970 年に県及市町村をまとめていく動きが始まり、108 あった県を 5 つの県にまとめ、1388 あった市町村は、98 まで少なくした。この目的は、市町村を役割を担える大きさ（人口）にすることであった。

表 2.2：市町村合併

	市町村	州/地方
1970 以前	1388	108
1970-2006	275	16
2007 以降	98	5

この結果、ほとんどの市町村は人口 3 万人を超えた。

表 2.3：市町村あたりの人口

住民数	市町村
0 - 20,000	7
20,000 - 30,000	18
30,000 - 50,000	37
50,000 -	36

もうひとつのデンマークの特徴は、デンマークは大きな政府（社会福祉など行政サービスを充実させる）を進めていて、次の表に示す通り常勤勤務者の約 4 割が公務員（政府 17.2 万人、県 11.97 万人、市町村 44.4 万人）と、パブリックセクターの役割が大きい。

表 2.4：常勤勤務者の雇用の割合（民間または公共）

雇用主	人数（常勤勤務者 2009 年調査）	割合
民間組織	1.361.800	61.0 %
公共組織	787.700	36.0 %
公共運営組織	66.600	3.0 %
公共関連組織合計	854.300	39.0 %
合計	2.215.100	100.0 %

常勤勤務者の男女の割合は以下の通りで、若干女性の方が少ない程度である

表 2.5：常勤勤務者の雇用の割合（男女）

	割合
男性	78.3
女性	73.1
平均	75.7

ちなみに、平均寿命は女性 80.50 才、男性 76.00 才である。

ブロードバンド・カバレッジは人口の 98%以上に達している。企業及び世帯の 98%以上が ADSL に接続可能となっている。ブロードバンド回線数は、2008 年 6 月末現在、約 200 万で、xDSL が約 125 万、ケーブルモデムが 54 万、FTTH が 9 万等となっている。

現在は、100MB のブロードバンドを島々を含めて全国に広げようとしている。

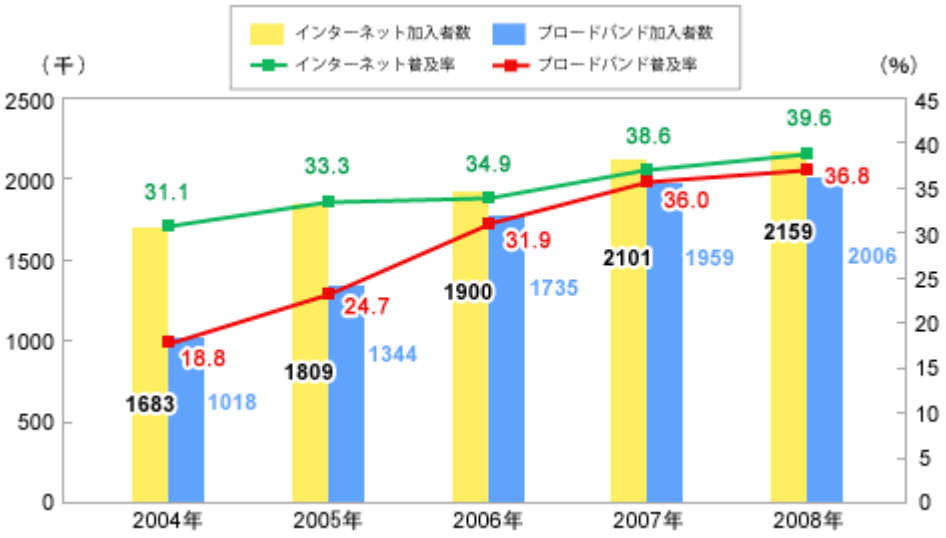


図 2.1：デンマークにおけるインターネットの普及（総務省 HP より引用）

出所：http://g-ict.soumu.go.jp/index.html

2.2.1.2　デンマークの電子政府

デンマークでは、国、県、市町村が参加する STS（Joint Committee for Cross Governmental Co-operation）中心になって環境、教育、健康などのシステムの検討を進めている。

一例として。中央省庁、県、市町村で共有できるよう公的なメールボックス e-BOX の標準化を行った。この作業ために、中央省庁、県、市町村それぞれ、40%、40%、20%の割合で費用を分担した。

電子政府サービスのいくつかを紹介する。

(1) 電子署名

デンマークでは 2003 年以来、無償で電子証明書の発行を行ってきた。

基本的には、ソフトウェア証明書であり、自分のパソコンに秘密鍵を格納して利用してきた。しかしながら、外出した場合、電子署名、認証ができないとの問題が出て、新たな電子署名利用環境（NEM ID）を構築し、サービスを開始した。

具体的には、電子証明書、私有鍵を政府が運営するサーバで管理し、その起動については、従来の ID、パスワードに加えキーカードを利用して認証する。キーカードとは 9 桁の数値列が多量に並んでいるカードである。利用時にはまず ID とパスワードを入力すると、4 ケタの数値列を送ってくる。キーカードからその数値列に続く 5 桁の数値を見つけて入力することにより認証を完了する。

認証後、サーバの電子証明書、私有鍵を用いて電子署名を行うことができる。このようなシステムでは、市民が私有鍵を管理する負担がなくなり、かつ自身の PC だけでなくモバイル端末からであっても公共端末からであっても、電子署名をすることができる。

電子証明書、私有鍵を政府が運営するサーバで管理する方法はカナダでも採用しているが、政府に対する信頼が必要である。

(2) 市民ポータル（Borger. dk）

市民主体の電子サービスを目指して構築された生活にかかわる公的サービスの窓口（Borger.dk）がある。これは、バックオフィスのデータ連携によるサービスであり、Borger.dkで該当する項目を選ぶと関連する法律や手続き方法まであらゆる政府提供の情報を閲覧することができる。また、この中のマイ・ページを設定することで、行政からの連絡や年金情報記録などの行政が保管する個人・家族の情報がひとまとめで閲覧できる。

2.2.1.3　電子文書管理

デンマークは約40パーセントが公務員であり、多くのことが国主導で動いている。電子文書管理においても、公共部門が中心に進めてきたが、第一フェーズが終わり大きく方針を変えた第 2フーズが進み始めた。

大きな流れは以下のとおりである。

2004－2008　ERMS（FESD）の公共の枠組みの標準化（Siloシステム）

2008－2009　ERMSのアーキテクチャーを検討

2009－2010　新たに SOA（Service Oriented Architecture）をベースとして検討（FESDⅡ）。サービスインタフェースとして、文書（Document）、ケース（Case）、アーカイブ（Archive）、階層（Classification）、組織（Organization）の標準を作成。

(1) 電子文書管理（FESDⅡ）について

FESDでは、システムに修正を入れるたびに莫大な費用がかかっていた。そこで、以下の通り方針転換をおこなった。

- クローズなFESD標準をオープンなOIO（デンマークの組織）標準にした。
- ERMSを中心に検討したシステムからいくつかのソリューションを連携し、協調させた。
- 一つの包括的なシステム（ERMC）から、オープンスタンダード、リファレンス・アーキテクチャーやコンポーネントとの連携を図れるようにした。

また、文書管理も含め、シングルソリューションを目指している。そのためには、中央省庁、県、市町村にまたがって適用する標準の存在が重要である。標準は、大きく技術標準とセマンティック標準の2つに分けられる。技術標準は、基本的にはISOやEU標準の内から必要な標準を“選択”することであり、比較的問題は少ない。一方のセマンティック標準は、例えば、教育に関する標準など、同意形成は困難を極め、頻繁に見直しが必要である。

そこで、システム上にプログラミングするのではなく、各業務を分析して処理手順（ケース）を作成し、そのケースに従った処理を行う環境としてSOAアーキテクチャー選択し、そのインタフェースを定めた。すなわち、文書の標準インタフェースによる小さなコンポーネントの集まりに方向を変えた。

このソリューションは以下のようなことを可能にする。

- 自身のデータと機能を公開することにより、他の it-solutions に用いられることがありえる。
- 他のit-solutionsのデータと機能を再利用する。

デンマークにおける文書管理は 2002 年から導入を開始したケースマネジメントと密接な関係にある。例えば、国民の 1 人から義足に対する補助申請案件が発生すると、その時点でその申請に対するケースファイルが作成され、様々な手続き書類、例えば Web からの入力データ、内部書類など、がタイムスタンピングされそのケースファイルに時系列的に格納される。タイムスタンプは、サーバ内の時計を使用している。また、デーベースアクセスに関しては、更新の前と後のデータがケースファイルに格納される。案件が完了し、案件ファイルがクローズされて、5 年経過するとアーカイブス（公文書館）に送られる。

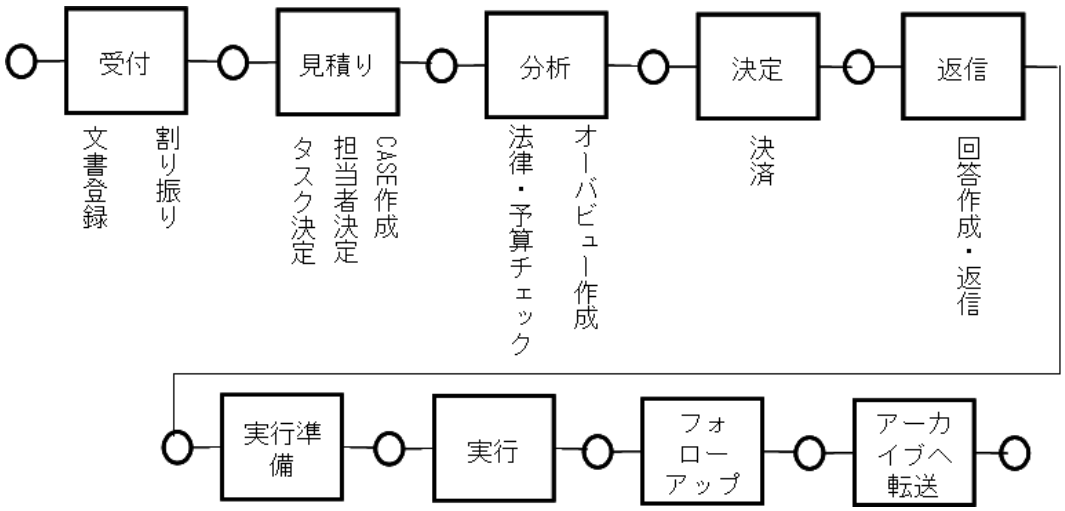


図 2.2：業務フローにおける CASE ファイル作成タイミング

ケースはケースタイプ（例えば、年金、建物購入、など）により分類され管理される。代表的な市町村を例にとると、アクティブなケースファイルは 800 万件に上り、1 日あたり 25 万件が処理されている。

記録の再利用に関しては、ケースタイプなどの分類方法と適切な名前付けに留意している。

長期保存に関しては、現時点では TIFF（つまり、イメージデータ）に変換して保存しており、PDF/A の適用はまだツールが一般的ではないので今後の課題である。

基本的に、ワードなどのプロパティに入っているメタデータ（作成者や作成日など）は使わず、別途データベース上でメタデータを管理している。署名、タイムスタンプ、他の文書との相互関係（本体と付属資料など）も全てデータベース上のメタデータとして管理される。

2.2.1.4　デンマーク文書関連仕様書概要

SOA（Service Oriented Architecture）の導入にともない、サービスインタフェースとして、文書（Document）、ケース（Case）、アーカイブ（Archive）、階層（Classification）、組織（Organization）の標準を作成した。その概要とそれらの全体を示した「ケースとドキュメントの一般サービス仕様書」の概要を紹介する。

(1) ケースとドキュメントの一般サービス仕様書[221-1]

①　本仕様書の目的

本文書は全てのケース/文書管理（ESDH）システムに通用されるパーツを説明する。つまり、

ケースとドキュメントの一般サービス仕様書は OIO 組織内で作成されているスタンダードの基準点になる。他の文書の概念やコンセプトは本文書で説明されている。

初めに、OIO 組織は 2009 年の一月に設立された。OIO 組織は国、県、区レベルのケースとドキュメントシステムの基準化を担当している。システムの基準化は様々なケースとドキュメントシステムを含む、例えば、ビジネス・システムとケース/文書管理（ESDH）システムなど。

具体的な任務は OIO の下のプロジェクト・グループが行う。

ここで言うビジネス・サービスとは、仕事の為の自動化されたプロセスである。そのプロセスはユーザー・インタフェースや統合インタフェースからアクセス可能である。ビジネス・サービスのインタフェースで、パラメータによってデータの保存、検索、リードができる。

インタフェースは既存のシステムにも新しいシステムにも対応する。インタフェースの完全な実装も部分的な実装も可能である。機能の追加も可能である。

以下のアプリケーション・モデルは 4 つのレイヤーに分かれている。ダイアログ、プロセス、ビジネス・サービス、インフラ。

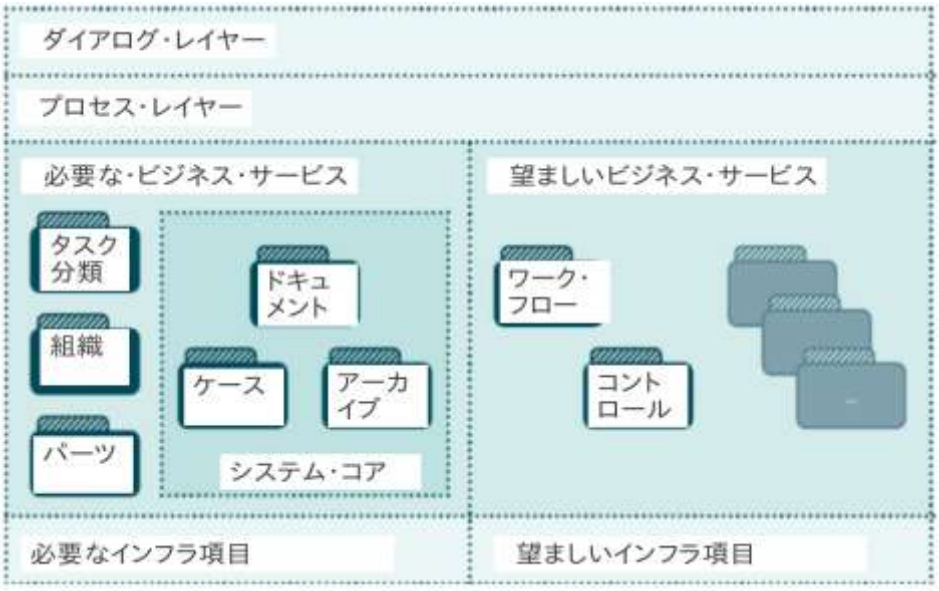


図 2.3：アプリケーションモデル

（デンマーク政府科学技術イノベーション省 IT 電気通信庁の資料を元に作成）

② サービス利用者とサービス提供者

システムは二つの役割を持っている。サービス利用者とサービス提供者である。例えば、ケース/文書管理（ESDH）システムはケースとドキュメントというビジネス項目を提供している。ビジネス・システムはケースとドキュメントというビジネス項目を利用している。（ビジネス・システムがケースとドキュメントのビジネス項目を提供する場合もある。）

サービス利用者と提供者の関係は以下のようになる。

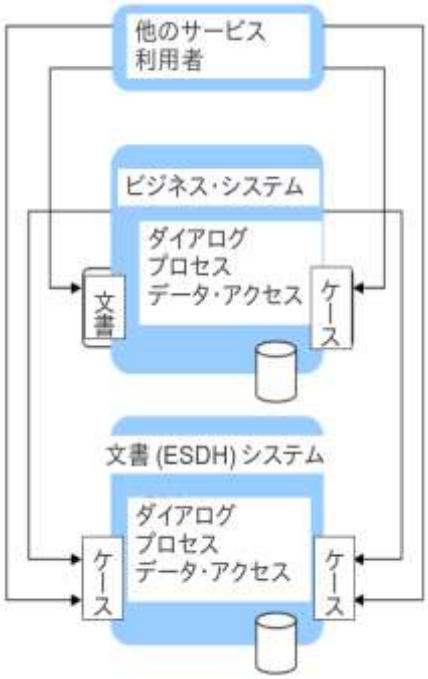


図 2.4：サービス利用者と提供者の関係

(2) SAG（ケース）のサービスインタフェース仕様書[221-2]

① ケース・ビジネス・サービスの目的

ケース・ビジネス・サービスの目的は組織のケースに関する情報を登録することである。

ケースというのは行政過程に関係のある文書の収集である。ケースという概念は ESDH のコア概念の一つであるが。普段は「ケース」は「文書」や「アーカイブ」という概念と一緒に利用されている。CMS システム、EDH システムなどで一つの「ケース」は複数の「文書」と相互運用性があるのが条件である。

② ケース・サービスインタフェースの目的

・ 既存のシステムの間のスムーズな電子ケース交換

・ ケースの送信/受信の基準化

・ 既存のケースを保管する ESDH システムとの相互運用性

③ ケースのサービスインタフェース

サービスインタフェースはケース担当者に機能を提供する。つまり、ケースの作成、エディット、削除、検索、拝見、リスト作成、引き取り、インポート。

サービスに対する条件（許可されている機能を発行することと、機能を関連させることを含む）を満たすことはサービス提供者に責任がある。

④ ケース

「ケース」というのは構造を持つ文献集である。ケースはあるプロセスの結果で、検索の為の構造を持つシステム（類別・分類）に登録されている。

ケースは組織の全ての文書と関係する。ケースには様々な面がある：

コンテンツ（業務過程）、関係（アーカイブ、関係者）、構造（分類など）。

ケースは同じ業務過程に対する文書でできている。一つの文書は複数のケースと関係してい

ると考えられる。ケースと文書に関係をつける為に、ジャーナル項目が利用されている。本スタンダードにある概念を用いて、関係の階層造を作ることが可能になる。

⑤　利用の実例

ケースの実例：

例 1：市民の申請によりケースを作成。

例 2：企業の登録の為のケース。

例 3：ある組織の複数の活動を含むプロジェクトに関するケース

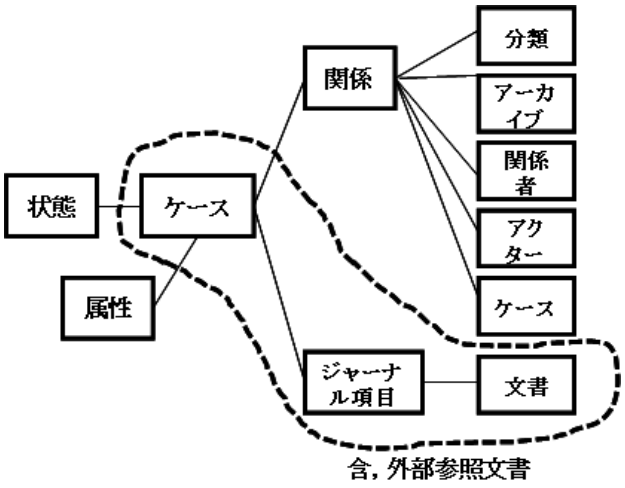


図 2.5：SAG（ケース）の構造

(3) 組織のサービスインタフェース仕様書[221-3]

ほとんどの組織に様々な管理システムが利用されている。組織と人事に関する情報は複数のシステムに入り、管理しないといけない。その為、組織や人事に対する情報共通交換の基準を提案する。

組織管理システムによって対象となる組織タイプが異なる。例えば、法律的な組織、マトリクス組織、安全保護組織等。この基準では多数の組織をカバーするのが目的である。既存のシステムとの相互運用性も目的の一つである。

組織には複数の動作者（Actor）が存在する。動作者はお互いに関係がある、そして動作者も外部の動作者（例えば、企業、人、官権）と関係がある。動作者とその関係を記述するのも本基準の目的である。

(4) ドキュメントのサービスインタフェース仕様書[221-4]

ドキュメント・ビジネス・サービスの目的は組織のドキュメントを記録する事である。ドキュメント・サービスに電子化ドキュメントとそれらのメタデータは保存されている。ドキュメントというのは構造があり、制限もある情報である。様々な情報媒体がある。例えば紙、デジタル媒体、ミクロフィッシュ等。ドキュメントにテキスト、絵、写真、画像データがある。

加えて、このサービスの目的は様々なビジネス・プロセスに利用される事である。例えば、ドキュメントの閲覧や文書交換。

ドキュメント・パーツ

ドキュメントはパーツ（部分）に分ける事ができる。例えば、あるレポートに三つ章がある。このような分け方によって、多数の動作者は同時に編集できる。

ドキュメント・パーツは合成ドキュメントでできている場合がある。例えば、一つのメールに二つファイルが添付されている：一個の画像データと一個のスプレッドシート。全ては一つのEMAIL mime-type というドキュメント・パーツとして扱われている。

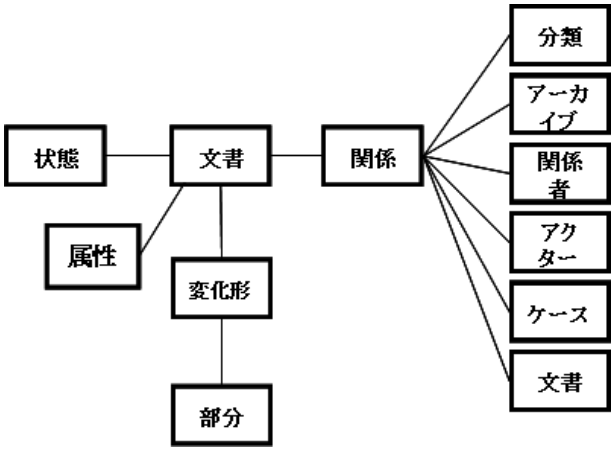


図 2.6：ドキュメントの構造

(5) アーカイブ構造のサービスインタフェース仕様書[221-5]

アーカイブはケースとドキュメントの集まりを示している。その集まりは論理的であるし、アーカイブの部分の間にも構造な関係ある。一つのアーカイブは複数の IT システムに保存されていると考えられる。

一つのアーカイブの資料は一つの分類システムを利用している。「進行」というステータスを用いて、異なるアーカイブステータスに区別を付けられる。

アーカイブは三つオブジェクト・タイプと関係ある：分類、作動者、アーカイブ

アーカイブ構造は「分類」というビジネス・サービスを利用し、アーカイブの構造を示している。

① バージョン管理

アーカイブのメタデータ変更は記録されている。つまり、属性、ステータス、関係の変更は全て検索可能である。アーカイブを検索する際に、アーカイブの日付けが重要である。

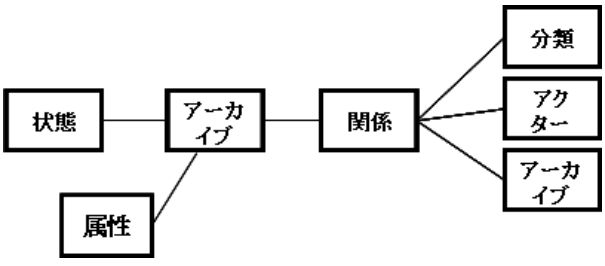


図 2.7：アーカイブ構造

(6) 分類のサービスインタフェース仕様書[221-6]

分類ビジネス・サービスは一般の ESDH(文書管理システム)をサポートする為に作られている。分類ビジネス・サービスは様々な異なる分類システムを含め、他のビジネス・サービスにクラス・マークやジャーナルキーを書き込める。

分類ビジネス・サービスは他の分類システムとマッピングができる。例えば、タスクやアカウント番号の間にリンクを作れる。だが、マッピングの為にセマンティックを設立しなければならない。

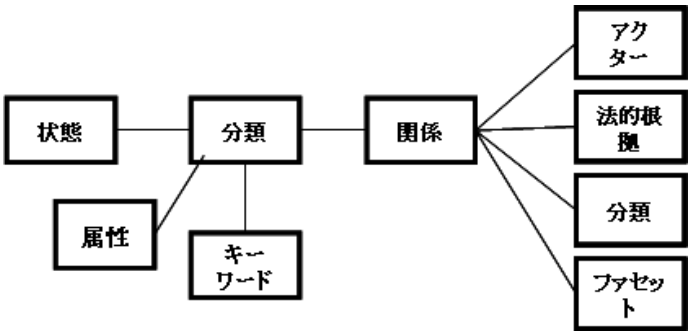


図 2.8：分類の構造

【参考文献】

[221-1] Generelle egenskaber for serviceinterfaces på sags- og dokumentområdet, Denne standard er godkendt af OIO-komiteen december 2009

[221-2] Specifikation af serviceinterface for sag, Denne standard er godkendt af OIO-komiteen december 2009

[221-3] Specifikation af serviceinterface for organization, Denne standard er godkendt af OIO-komiteen december 2009

[221-4] Specifikation af serviceinterface for document, Denne standard er godkendt af OIO-komiteen december 2009

[221-5] Specifi kation af serviceinterface for arkivstruktur, Denne standard er godkendt af OIO-komiteen december 2009

[221-6] Specifikation af serviceinterface for klassifi kation, Denne standard er godkendt af OIO-komiteen december 2009

2.2.2　ハンガリー

2.2.2.1　ハンガリーの基本情報

ハンガリー（正式な国名はハンガリー共和国）は、ヨーロッパ諸国の中で唯一アジア系民族の国である。1989 年 10 月 23 日のハンガリー共和国憲法施行に伴い、ハンガリー人民共和国が崩壊し多党制に基づくハンガリー共和国が成立した。体制転換以後、ハンガリーは一貫して「欧州への回帰」を最大の外交目標として掲げ、1999 年 3 月に NATO に加盟、2004 年 5 月には EU 加盟を果たした。2011 年前半には EU 議長国に就任の予定である。

ハンガリーの国土は 9 万 3 千 km^2 で、日本の 1/4 である。人口は 1001 万人（2009 年末現在、ハンガリー中央統計局）で、ポルトガル、チェコ、ギリシャなどの国々と同様、欧州のなかでは小規模に属する。人口の 2 割弱（170 万人）が首都ブタペストに集中している。労働人口は 387 万人と、人口の割に少ない。失業率は 10%である。一人当たり GDP は、12,914 ドルであり、名目 GDP は、1,287 億ドル、2009 年の成長率は－7%である。主要貿易製品は、機械、輸送機器、工業製品であり、輸出入の 25%をドイツに依存している。

IT 事情は、図 2.9 のように、インターネット加入数が 177 万加入、普及率は 17.7%となっている（2008 年現在）。

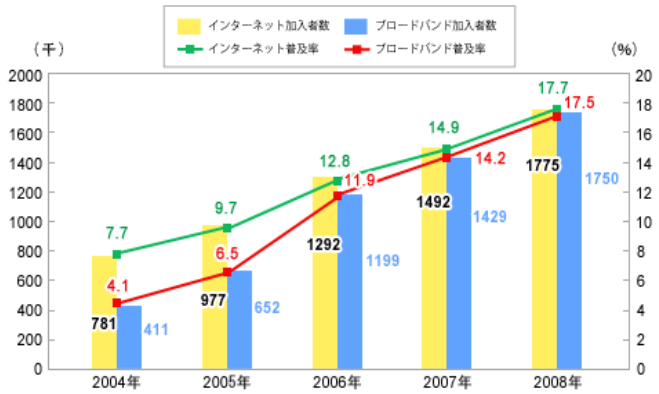


図 2.9：ハンガリーの IT 事情（総務省 HP より引用）

2.2.2.2　ハンガリーの電子署名及び電子文書保管所関連の法規制

ハンガリーの電子署名法 2001/31（Act 2001/31）は、4 つの電子署名関連信頼サービス（Trust service）を定義している。

(1) 認証サービス（証明書の発行と維持）
(2) タイムスタンピング
(3) 署名生成デバイスの規定
(2) 長期アーカイビング

各サービスは国家通信庁（National Communications Authority）の厳格な監督のもとに適格サービス（Qualified Service）として提供される。

信頼のおける電子文書保管に関しては、通商省（Ministry of Commerce）規則 114/2007 に従っ

て、次の方法のうちのいずれかである必要がある。

(1) 電子署名及び適格タイムスタンプ（例えば、AdES-T）の使用

(2) 認証されたクローズドなシステム

(3) EDI

上記(1)の、電子署名及び適格タイムスタンプの使用による場合は、もし保存期間が 11 年を超えるときは、署名検証に必要な全ての情報を集め、定期的にタイムスタンプを付与する（例えば、AdES-A）必要がある。自分自身で保存するか、適格保存サービス（Qualified archiving service）を利用するかは、いずれでも構わない。

2.2.2.3　適格保存サービス提供者の要件

適格保存サービスの法的要件は次の通りである。

(1) 適格認証局の要件を満たす

(2) ISO 9001 および ISO 27001 システムを取得している

(3) 公開されたポリシー（保存ポリシーと practice statement に従って運用されている

(4) 署名付き保存文書、または加入者からハッシュが提供可能な署名なし保存文書のいずれかである

(5) 署名付き文書がアップロードされたときは、署名を検証し、署名検証に必要な全ての情報を集め、適格タイムスタンプを付与する。署名に対する猶予期間は 3 日である。

(6) 署名の妥当性を維持するために、署名付き保存文書に対して適格署名と適格タイムスタンプを付与し、実施要領や通信局の規定に従って必要に応じて定期的にメンテナンスする。

(7) 認証された利用者は、99%の可用性で保存文書をダウンロードできる。

(8) 認証されていない利用者は保存文書にアクセスできない。

(9) サービス提供者の従業員は保存文書を読みだせない。

(10)加入者から要求があった時は、文書が保存され署名が正しいことを記載した署名付き文書や発行や、保存文書の永久的な削除を実行する

(11)サービス提供者は、保存文書の可読性維持を選ぶかもしれない

(12)サービスを終了するときは、保存文書を他のサービス提供者に移管しなければならない。

注　サービスを停止した場合の移管に関する制度は明確ではない。

2.2.2.4　保存パッケージ e-Dossie

ハンガリーにおける電子記録の保存サービスは、Dossie と呼ぶパッケージを単位に管理している。Dossie 仕様はハンガリーの標準にはなっていないが、デファクトとして利用されている。ハンガリー政府は、縦割り意識が強く、各省庁単位に要求事項が異なっているという現状である。そのなかで、デファクトの Dossie が共通仕様の役を担っている。

e-Dossie フォーマットの概要は次の通りである。（図 2.10 参照）

(1) フォーマットが XML で記述されている。

(2) 1 または複数の任意のファイル（ワードや PDF）が Base64 エンコードされている。

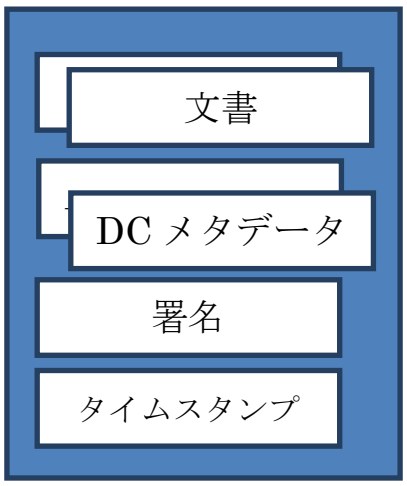
(3) 個別ファイルにダブリンコアメタデータが付与されている。

(4) 個別ファイルに XAdES 署名が付与されている。

(5) 全てのファイルと署名に対する外部 XAdES 署名が付与される。

個々の Dossie は、Dossie 自身のハッシュ値（SHA256）で識別している。長期保存目的のタイムスタンプは、ドイツと同様、複数の署名付き文書にまとめてタイムスタンピングする LTANS の ERS（証拠記録構文、RFC 4998）を適用している。

```
<es:Dossier ... >
<es:DossierProfile>...</es:DossierProfile>
<es:Documents>
  <es:Document>
    <es:DocumentProfile>...</es:DocumentProfile>
    <ds:Object>...</ds:Object>
    <ds:Signature>...</ds:Signature>
    <es:TimeStamp>...</es:TimeStamp>
  </es:Document>
  <ds:Signature>...</ds:Signature>
  <es:TimeStamp>...</es:TimeStamp>
</es:Documents>
```



署名(XAdES)は、Dossie 内の
全ての文書とメタデータに
対して一括付与

図 2.10：Dossie の構造（ハンガリーMICROSEC へのヒアリング調査に基づき筆者作成）

2.2.2.5　長期保存サービスの事例（Microsec 社）

Microsec 社は、ハンガリーにおける適格保存サービス提供者として登録された最初のサービス提供者である。現在判明している限りにおいては、実際に運用している唯一の適格保存サービス提供者である。本社は、マイクロソフトやキャノンなど 20 社を超える企業とともに、ブダペストの北に位置するテクノパークの中にある。

Microsec 社では、現在、1,400,000 ドキュメントを扱っており、主な顧客は、ハンガリー商工会議所の公証人、弁護士、電子的請求（e-invoicing）実施企業などである。主に、法務関係の文書の預かりを行っている。民間企業にも対応しているが、まだ民間での e-Invoice の利用が少ないため、そのボリュームは少ない。

なお、顧客との契約では 50 年までの保管ができることになっている。

(1) 保存ポリシー

Microsec 社の長期保存サービスの保存ポリシーは次の通りである。

① 要件は、ETSI TS 101 406 Policy requirements for certification authorities issuing qualified certificates に準拠する。

② 構成は、RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework に準拠する。

③ CA 鍵が維持されない、保存文書が管理されないという長期の保存を考えて、署名付き文書のみ保存する。

ポリシーの内容は次のようになっている。

1. はじめに
2. ポリシーの開示
3. 運用要件
   契約、アップロード、ダウンロード、保存証明書の発行、文書閲覧、文書削除、サービス停止
4. 設備、運用管理
5. 技術的なセキュリティ
   署名妥当性、文書の可読性の維持
6. コンプライアンス監査及び評価
7. その他事業、法的事項

(2) アップロード

アップロードは、クライアント認証による SSL によってのみ可能となっている。

アップロード時、アップロードした e-Dossie のハッシュを算出し保存する。これは、受取の証拠になる。加入者は、署名された受取証拠を受け取る。

XAdES 署名（XAdES-BES、XAdES-T など）が付与された入方向（incoming）の e-Dossie 文書に対して、最新のハッシュアルゴリズムによるアーカイブタイムスタンプ処理を実施する（XAdES-A に対しても、追加のアーカイブタイムスタンプを付与する）と共に、そのハッシュを保存する。（図 2.11 参照）

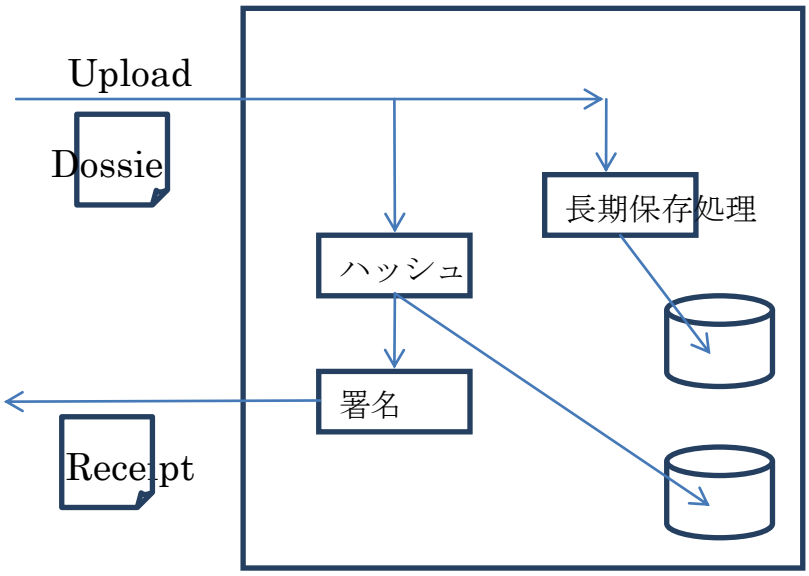


図 2.11：Dossie のアップロードとレシート（ハンガリーMICROSEC へのヒアリング調査に基づき筆者作成）

長期保存のタイムスタンピング関しては、XAdES-A と LTANS ERS の 2 つのベストプラクティスがある。

XAdES-A は、文書が定期的に更新される。ファイルごとにタイムスタンプが必要な替わりに、文書は相互に独立に保存できる。一方、LTANS ERS は、証拠記録が保存されるので、ファイルの更新はなく、タイムスタンプは 1 つで済むが、文書が相互に結び付いている。見方を変えると、アカウンタビリティ確保に向いているといえる。

Microsec 社のシステムは、アップロード文書の署名に対しては XAdES-A を適用し、XAdES-A 署名の保存には LTANS ERS を適用している。

注：ERS には MarcleTree 方式のハッシュが適用されることから、長期保存に対してタイムスタンプ更新は不要となる。

(3) 署名の検証

電子保存サービスでは、文書保存受付時に署名の検証を実施する。検証が失敗した場合は保存を受け付けない。失効情報は OCSP で提供され猶予期間（Grace period）は 3 日である。一旦保存が受け付けられた後、猶予期間内で失効が判明した場合の処置については、事例もなく、現時点ではその扱いは明確には決まっていない。

(4) 暗号化

アップロードされた署名付き文書は、加入者の公開鍵、または保存サービスの公開鍵で暗号化される。加入者は SSL によってドキュメントをダウンロードすることができ、そのドキュメントを復号することができる。

なお、保存サービスは、複数の信頼された従業員が深く関わり合う特別の手続き（秘密分散）によって秘密鍵を回復することができる。

また、ハッシュ・アルゴリズムや暗号アルゴリズム変更時に文書の復号が行われる。

(5) 可読性の維持

サポートするフォーマット仕様書をアーカイブとして保管している。オープンなフォーマットのみサポートされる。できるだけ、PDF/A が望ましい。

(6) 証明書

ハンガリーには 3 つの認証局がある。Microsec 社は、ハンガリー資本のハンガリーを代表する認証局及びタイムスタンプ局である。ハンガリーでは認証局事業者は同時にタイムスタンピング局事業者も兼ねている。Microsec 社の証明書の発行枚数は、1 万 5 千枚程度であり、その中の 1 万枚は弁護士に対する発行である。

(7) タイムスタンプ

タイムスタンプは、適格（Qualified）タイムスタンプを提供しており、年間 3,200 万回程度利用されている。欧州圏で適格タイムスタンプを提供しているのは、他に、ドイツ、イタリアがある。

タイムスタンプの時刻源は、ドイツの標準時と GPS から得ている。ハンガリーは MKEH（ハンガリの国家標準計量機関）が UTC を決定するネットワークに加入しているが、時刻情報を配信するには至っていない。

(8) 可用性

Microsec 社の電子保存サービスのアベイラビリティは 99%（主として計画停止）であり、一方、認証局とタイムスタンプ局のアベイラビリティは 99.99%を確保している。

以上

2.2.3 ドイツ

2.2.3.1 ドイツの基本情報

ドイツ（正式な国名はドイツ連邦共和国）は、国土の面積が 35 万 7 千 km^2（日本の 94%）、人口が 8200 万人で、欧州各国のなかでは最も人口が多い（2 位はフランスで 61 百万人、3 位は英国で 60 百万人、4 位はイタリアで 50 百万人）。首都ベルリンの人口は 366 万人である。失業率は 8.2%、一人当たり GDP は 40,832 ドル、名目 GDP は 3 兆 3300 億ドルで、成長率は、-4.7%となっている（2009 年 JETRO 調べ）。

毎年国連が調査している電子政府の 2010 年のランキングは、15 位である（日本は 17 位）。

ドイツにおけるインターネット普及率は、図 2.12 のように 75.5%で米国、英国、韓国、日本などの最先進諸国と同様の水準にある。

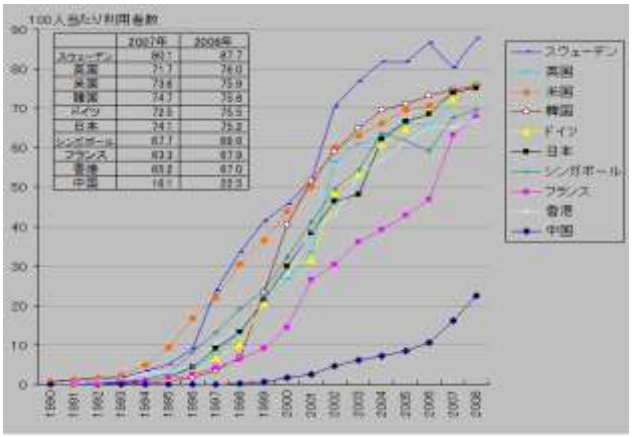


図 2.12：インターネット普及率の推移（文献[223-5]より図を引用）

2.2.3.2　長期保存に関係する法令

長期保存に関してドイツにおいては次の法令が関係する。。

・German fiscal code (Abgabenordnung)
・Data Privacy Law (BDSG)
・Works consitution act (BetrVG)
・Civil code (BGB)
・Commercial code (HGB)
・Principles for data access and verifiability of digital documents (GDPdU)
・Generally Accepted German Accounting Principles using digital systems (GoBS)
・Signature Law (SigG)
・Code of civil procedure (ZPO)

長期的にセキュアな文書の保存および長期的な使用可能性に対する署名法（Signature Law）の要件は次の通りである。

① 電子文書インフラは、少なくとも、電子文書の長期保管をサポートしなければならない。これは、長期間が経過した後でも、電子文書へのアクセスが妥当な労力と出費によって可能でなければならないことを意味する。

② 電子文書インフラは、法律的なセキュリティー（特に電子文書の真正性と完全性）を永続的に、ただし少なくともファイルの維持について法律で規定された期間が満了するまで、保証しなければならない。これは、画像と内容の両方が元の文書と整合していることが保証されなければならないこと、および電子署名された文書の場合、署名法第 17 条のいわゆる「再署名」が可能でなければならないことを意味する。

ArchiSafe プロジェクトの極めて重要な目的および原則は以下のとおりである。

③ 明確に解釈できて長期的に安定な、公表されているユーザー・データフォーマットの使用
④ 明確に解釈できて長期的に安定な、標準化された署名データフォーマットの使用
⑤ 暗号化アルゴリズムのセキュリティ適合性の考慮、およびセキュリティレベルが十分に高い電子署名（認定済み電子署名）の使用
⑥ 要求される検証データを業務運営に適した形式で保管すること

⑦　証拠となる署名のタイムリーな更新
⑧　技術構成要素が安定して入手可能であること
⑨　電子署名された文書の安全な変換
⑩　データ保護およびデータ信頼性の保証
⑪　電子署名された文書の保存および更新の際、冗長性を利用してセキュリティを増大させること
⑫　後の時点でデータを再利用可能にすること、拡張可能性を備えること、および標準化された経済的な手法および技術を適用することにより、費用効率を向上させること

2.2.3.3　Archi シリーズの推移

ドイツ政府は、2001 年 11 月に BundOnline2005 を発表し、2005 年に全ての行政サービスを電子化し、インターネットを利用して提供することを目標とした。BundOnline2005 プロジェクトにおいては、電子署名方式 ArchiSig、その実装 ArchiSoft、署名付き文書のフォーマット変換ツール TransiDog、文書管理体系 ArchiSafe などの一連の Archi シリーズ（Archi は、ドイツ語で Archive（保存）を意味する言葉）のプロジェクトが計画され実施されてきた。ArchiSig、ArchiSoft、TransiDog、ArchiSafe の各々のプロジェクトの関係を図 2.13 に示す。

ArchiSig は ArchiSoft に引き継がれると共に、その成果は IETF において LTANS（Long Term Archive and Notary Services）プロジェクトで標準化が進められている。また、ArchiSafe の成果は、ArchiSig の成果と共に BSI（Bundesamt für Sicherheit in der Informationstechnik、連邦電子情報保安局）から TR（Technische Richtlini、技術指令）として発行された。

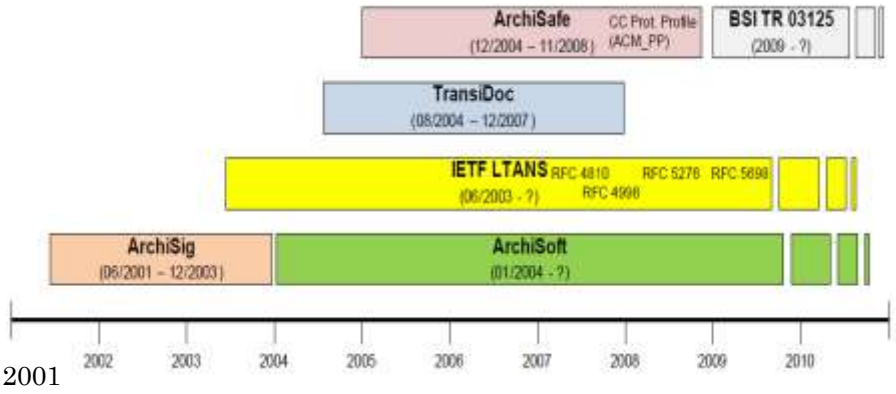


図 2.13：関連プロジェクトの関係（ドイツ FRAUNHOFER SIT 訪問時入手資料を引用）

(1) ArchiSig

ArchiSig では、電子署名の長期保存に関する検討が行われた。その特徴は、ETSI 標準の CAdES や XAdES とは異なり、電子署名文書一つ一つにタイムスタンプを付与するのではなく、複数文書に対して一括して一つのタイムスタンプを付与するところにある。検討成果は IETF の LTANS プロジェクトに入力され、4 つの RFC として発行された。

(2) ArchiSoft

前述の ArchiSig は、その実装を行う ArchiSoft プロジェクトに引き継がれ、ドイツ国内では複数のディストリビュータが製品を提供し始めている。具体的なディストリビュータとして、電子署名に関しては e.siqia 社 (http://www.esiqia.com/index.php?id=121)、一括タイムスタンプ方式に関しては AuthentiDate 社 (http://www.authentidate.com/) が挙げられた。

(3) IETF LTANS プロジェクト

IETF LTANS (Long-Term Archive and Notary Services) プロジェクトは 2003 年に立ち上げられ、これまでに次の RFC を発行している。

- RFC 4810 (Long-Term Archive Service Requirements)
- RFC 4998 (Evidence Record Syntax)
- RFC 5276 (Using SCVP to Convey Long-Term Evidence Records)
- RFC 5698 (Data Structure for the Security Suitability of Cryptographic Algorithms DSSC)
- Draft-ietf-ltans-xmlers (XML Evidence Record Syntax)
- Draft-ietf-ltans-ltap (Long-term Archive Protocol - LTAP)

(4) TransiDoc

TrabsiDoc は、署名付き文書のフォーマット変換の方法論の確立を目指すプロジェクトであり、2007 年末でプロジェクトが終了した。現時点では、対応アプリケーションや後継の活動はない。フォーマット変換に伴って、プロセスとして署名の正当性を引き継ぐことになるが、署名が数学的に引き継がれるわけではなく、署名を目で確認できないこともあり、公証人などに未だ受け入れられていない状況である。

注：紙文書をマイクロフィルムに変換して、マイクロフィルムを原本として扱えるのは、その変換プロセスが確立されているからであり、これと同様のアプローチをとろうとしている。

(5) ArchiSafe

ArchiSafe の戦略は、オーストラリアのビクトリア政府提唱の VERS（ビクトリア州電子記録戦略）と ArchiSig に基づいている。VERS は電子記録の高信頼且つ本格的な保存を可能とする記録保持 (Recordkeeping) の枠組みである。ArchiSafe システムの特徴は、XML によるデータパッケージの定義と、データパッケージに対するユニーク ID の付与である。データパッケージは、文書、管理情報（メタデータ）、電子署名、証明書、タイムスタンプが格納できるようになっている。ここに格納されるタイムスタンプ（前述の ArchiSig の成果）は、紙文書でよく見受けられる受付印を目指したものであり、データパッケージに格納される文書が署名されているか否かは問わない。また、署名時刻の表示（署名タイムスタンプ）はサーバの時計を使用している。なお、データパッケージに対するユニーク ID は UUID が使われている。

(6) BSI TR 03125 (Reliable long term archiving of electronic documents)

BSI TR 03125 の構成を図 2.14 に示す。

1. 序文
2. 規定範囲
3. 概要
4. 信頼できる電子アーカイブシステムの要件
5. アーカイブシステムの機能
6. 派生魏儒要件
7. IT アーキテクチャ
8. IT セキュリティポリシー
9. 適合と相互運用性
10. インストール
11. 要件の割当て

図 2.14：BSI TR 03125 の構成（文献[223-1]より図を作成）

このなかで、信頼できる電子アーカイブシステムの要件として、一般的な法的枠組み及び関連する法的枠組み並びに EC 法からの条件と、可用性、読み易さ（legibility)、完全性、信憑性（authenticity)、セキュリティ、秘匿性に関する信頼される電子記憶装置の機能要件が規定されている。

規定内容は、電子アーカイブシステムの基本仕様をはじめ、eCard の API、証拠記録構文(ERS)、暗号アルゴリズムのセキュリティ適合性のためのデータ構造（DSSC）にまで及んでいる。アーキテクチャ的には、典型的なアーカイブシステムとして、図 2.15 に示すように、E メールや ERP、文書管理システムなどのアプリケーション層、アーカイブミドルウェア層、ストレージ層の 3 層構造を想定している。アーカイブミドルウェア層での処理単位はオブジェクト、ストレージ層の処理単位はデータパッケージである。

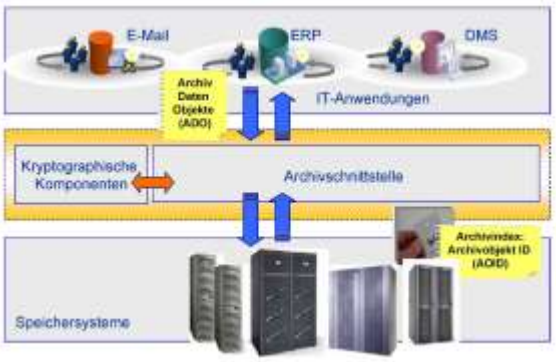


図 2.15：BSI TR 03125 による典型的なアーカイブシステム（文献[223-1]より図を引用）

現在、ドイツ政府は BSI TR 03125 導入の可否を検討中である。BSI TR 03125 は、いろいろな枠組みを取り込み結果として複雑な構造となっており、今後広く受け入れられるか否かは未知数である。

2.2.3.4　Archi シリーズの実装（Secript 社）

Archi シリーズの実装を行っている企業の 1 つであるドイツの Secrypt 社は、電子署名とタイムスタンプに特化したベンチャ企業であり、紙文書と電子文書の橋渡しをするユニークな技術をもっている。ドイツ政府は民間文書の電子署名に対する方針をもっていないことから、独自の判断で、証拠としての十分な対応を行うことによってスキャン済みの紙文書を廃棄できるツールを提供している。同社パートナは 14 社、ASP をはじめユーザは 50 社を越える。

(1) 電子記録市場への対応

e-invoice（電子的な請求書）については、EU 指令により電子署名が不可欠なこともあって、ドイツの電子署名関連市場の 2/3 は e-invoice である。しかし、インボイス全体に占める e-invoice の割合はまだ低く、大半は紙のままである。Secrypt 社製品が適用されている範囲での e-invoice は年 1.5 億枚とのことであった。

LTANS ベースのタイムスタンプについては、e-invoice、法廷関係（含、弁護士)、ヘルスケア分野で使われている。法廷関係では、ディレクトリ対して適用されている。ヘルスケア関係のガイドラインでは、必須ではないものの、適用が強く推奨されている。LTANS ベースのタイムスタンプの大半はインハウス利用とのことであった。

なお、ドイツには、電子記録保管サービス提供者は数社あり、なかでも（カメラやフィルムで有名な）Agfa 社がメジャである。

(2) 電子署名製品 DigiSeal

DigiSeal は、図 2.16 のように電子署名文書の内容を 2 次元バーコード（シークレットコードとも呼ばれる）で表示及するツールであり、電子署名付き文書を紙に印刷して交換及び保管することを可能とする。これにより、電子文書に対応できていない企業も紙文書で取引することができ、紙文書と電子文書の共存環境を構築できる。2 次元バーコードに備わる誤り訂正により、紙の破損や改竄からデータや署名を保護している（説明によれば 30%の情報が失われても復元可能とのことであった)。なお、2 次元バーコードは設定により、FAX レベルの解像度があれば送受できる。

DigiSea は、電子情報を格納する媒体が必ずしも電磁記録媒体だけではなく、紙も媒体に含め、かつそれを実装したところがユニークである。電子化を待つのではなく電子から紙に近づいて行くという発想は、商取引における電子化への切り札の一つになると考えられる。

図 2.16：電子署名付き文書（ドイツ SECRIPT 訪問時の入手資料を引用）

(3) LTANS ツール

LTANS は、一括してタイムスタンプを付与することから、インポート・エクスポートに課題があったが、Secript 社ではそれを解決して製品化を行っている。LTANS を推奨する理由として、CAdES や XAdES などはフォーマット毎に対応する必要があること、独自技術で、部分的なインポート・エクスポートを可能にたことを挙げていた。なお、ハッシュアルゴリズムの危殆化については、2 種類のアルゴリズムの同時提供と、バックグラウンドでの再ハッシュが可能との説明であった。

2.2.3.5 ArchiSafe

行政の中心的な生産現場はバックオフィスであり、その主な生産物はファイルである。電子方式による行政組織の導入によって、行政のさまざまな部門間でのデータと情報のスムーズかつ迅速な交換が可能になる。その主な利点は、デジタル化さ記録化された情報は機械が直接読み取れること、および遠距離であっても瞬時に転送できることである。

デジタル情報は本質的にバーチャルでる。電子ファイルが電子政府の基本的な前提条件であるためには、デジタル文書の真正性、完全性、機密性および可用性を長期的に、少なくとも法律で規定されたファイルの保存期間にわたって保証しなければならない。紙の書類と同様な証明機能を果たす必要がある。

電子文書インフラを導入しても、適切な電子アーカイブがなければ不完全な状態にとどまる。電子情報の長期的かつ法律的に安全な保管と維持は､適切な電子アーカイブによって保証できる。

ArchiSafe プロジェクトは、フラウンフォーファー協会の連邦物理・工学研究所（PTB）が中心となり、電子政府イニシアティブ BundOnline 2005 のスコープに沿って開発された。

(1) ArchiSafe の目的

ArchiSafe は、法律的に安全で改訂に耐えられる電子文書の長期保存（保管）統一基準をドイツ全体に導入することを支援および促進することを目的とする。ArchiSafe は、XML によるデータ交換（内容、記述データおよび署名データに関するデータ）の標準化形式を制定し、ソフトウェア参照アーキテクチャを実装することにより、連邦アーカイブを含む集中および分散いずれの電子アーカイブの導入と使用にも不可欠な基礎を構築する。

(2) ArchiSafe のアーキテクチャ

技術的観点では、ArchiSafe の概念は、サービス指向クライアントに適合する多層ソフトウェアアーキテクチャーに基づいている。

ArchiSafe の基本的な考え方は、信頼できる電子記録アーカイブシステムを既存のシステム（アプリケーション）からアクセスさせることにある。従って、既存のアプリケーションに対しては、アダプターを提供し、既存のインタフェースでアクセスできるように配慮している。これは、エストニアなどの、既存の電子アーカイブシステムにアダプターを前置し、アプリケーションからは新しいインタフェースでアクセスさせるアプローチとは対極に位置する。

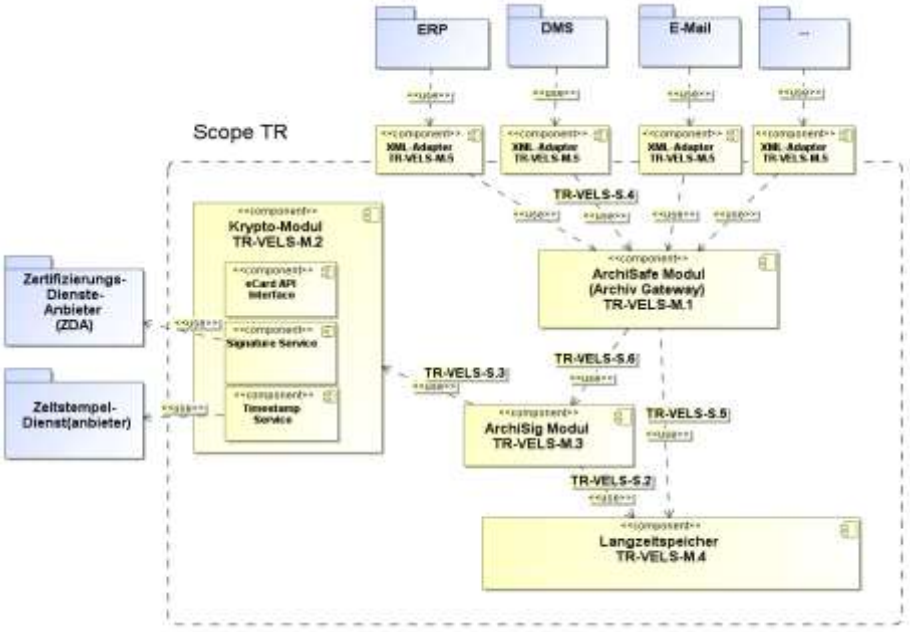


図 2.17：ArchiSafe のアーキテクチャ（文献[223-1]より図を引用）

いわゆる「案件関連手順」（たとえば文書管理あるいはファイル処理システム）は、プラットフォームとして、および文書管理、案件作成、長期保存のインタフェースのための先導システムとしての役割を果たす。案件関連手順は、電子アーカイブへの電子文書のファイリングを開始し、長期メモリーに保存されている文書の文書識別を管理する。これは、保存されている文書の文書識別が、ある案件の有効な処理のために保存されている文書インスタンスおよび処理データとリンクされていることも暗に意味している。

案件関連手順は、統一された保管インタフェース（保管サービス）を通じて、保管対象のオブ

ジェクト（文書、案件、ファイル）を長期メモリーに伝送する。電子文書を案件関連手順から長期保存システムに伝送する保管サービスは、システムに依存しないミドルウェア・コンポーネント（保管ハブ、図 2.17 参照）によって提供される。保管サービスは、標準化された文字セットとデータフォーマットを使用し、長期メモリーに保存しようとするデータオブジェクトの構文上および意味上の一致に基づいて、保管オブジェクトを確認および処理する。さらに保管サービスは、必要に応じて署名、証明書確認、タイムスタンプなどの暗号化機能を要求し、定義された XML スキーマに基づいて XML フォーマットを処理する。

標準化された保管オブジェクトの生成および保管サービスとの通信の開始は、専用のサービス・インタフェース（サービス・アダプター）で行われる。

保管サービスの中核は、定義済みのインタフェース（通信チャネル）を備え、案件関連手順および電子的長期メモリーにつながる XML プロセッサーからなる。さらに保管サービスは、署名サービス（電子署名の生成および／または検証）やタイムスタンプなどの追加的サービスを可能にする。

暗号化サービスは、案件関連手順から要求があったとき、長期メモリーに保存しようとする文書に署名するか、またはそれらの文書にタイムスタンプを付与する。さらに、案件関連手順から要求があったとき、署名された文書の署名および証明書を検証し、その検証データを保管サービスで利用できるようにする。保管サービスは、このデータを標準化された形式で保管オブジェクトの中に埋め込み、後の証明機能で利用できるようにする。

ArchiSafe プロジェクトでは、暗号化サービスは、連邦仮想郵便局（Federal Virtual Post Office）の中核システムを通じて提供される。

長期メモリーへの伝送は、必要に応じて、保存しようとする文書のタイムスタンプと組み合わせることができる。さらにタイム・スタンプサービスは、署名法（SigV）第 17 条に従って、電子署名された文書の再署名のために必要である。ここで、ArchiSafe プロジェクトは、法律的にセキュアで実績があるものとして分類されている Archi-Sig 手順を基礎として構築されている（http://www.archisig.de）。

最後に、真の長期メモリーシステムが最終段階に設けられ、その中には原則として元の文書および関連する案件メタデータだけが保存される。一意の文書識別（文書 ID、メタデータタグ）を割り当てることによって、長期メモリーシステムは、任意の時点かつ経済的に妥当な時間間隔で、案件関連手順から保存されている元データにアクセスできることを保証する。これにより、元の文書が法律的にセキュアな方法でファイリングされているにもかかわらず、長期メモリーシステムが案件固有のロジックによって過負荷にならないことが保証される。クライアントに適合するソリューションを実現するために、文書をそれぞれの案件関連手順に対する一意の識別とリンクさせることができる。この方法により、案件関連手順の中の許可の概念を通じて、保管データに無許可でアクセスされないことが保証できる。

案件関連手順の如何によらずに長期メモリーへのアクセスを可能にするために、補助的な検索および表示サービス（要求に応じて）を利用することができる。このサービスでは、長期メモリーに保存されているメタデータをデータベースによって冗長化しており、先導システムがダウンした場合に案件またはファイルを復元することができる。データおよび文書は、必要に応じて、表示（ビュワー）または後で利用可能な形でエクスポートできる。ただし、このようなサービス

を実装したために、法律に定められたデータ保護の規則が破られないよう注意しなくてはならない。

(3) 文書フォーマット

DOMEA 組織概念は、文書の長期保存には少数のフォーマットだけを適用すべきであると推奨している。長期メモリーの領域に最も多様なフォーマットを共存させると、法律に規定されたファイル維持期間中に、単一データ型を元のデータのとおりに忠実に再現することができなくなり、保存されている文書の真正性が失われるというリスクが増大する。

ArchiSafe では、DOMEA 概念に基づいて、保管しようとするデータのフォーマットに応じて以下の文書フォーマットを長期保存用として推奨している。

① 単純なテキスト情報

メタデータおよび特殊なシステムからのマスターデータには TXT（ASCII 7 ビット）

② コード化された文書（CI）

PDF フォーマット（PDF-A が望ましい）

この文書フォーマットはプラットフォームに関係なく使用でき、グラフィック情報に加えてテキスト情報も保存できるため、変換後にもフルテキスト検索が可能である。さらに、PDF フォーマットには電子署名埋め込みなどの有用な機能があるため、KBSt でも、CI フォーマットで提供されたテキスト文書の保管用に PDF を明示的に推奨している。これは、ISO 規格 19005-1「ドキュメント管理－長期的な維持のための電子ドキュメントのファイル形式－第 1 部：PDF ファイル 1.4（PDF/A-1）の使用」の公表によってより一層推奨されるようになった。

③ NCI フォーマットで入手できる文書

TIFF および／または PDF フォーマット

④ 保管対象のメタデータまたはデータセットに対するマークアップ言語

XML

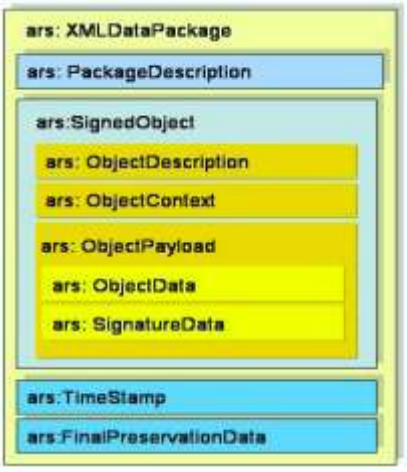


図 2.18：データ構造（調査結果から筆者作成）

(4) メタデータの構造

「電子政府アプリケーションのための規格およびアーキテクチャ（Standards and

architectures for E-Government applications)」では、メタデータおよび他のシステムとのデータ・インタフェースの記述と具体化を、原則として XML およびそれぞれの体系定義を通じて行うことを推奨している。

したがって ArchiSafe では、案件関連手順とアーカイブの間の通信にも、自己完結した保管オブジェクトの記述言語として XML を使用しているが、これは合意された XML スキーマを通じて記述されるため、後のアクセスに必要なすべての重要情報を含んでいる（図 2.18)。有効な XML スキーマによる記述を使用することで、とりわけ以下の利点が得られる。

① 保管オブジェクトは、電子的長期メモリーへの伝送前に、その構文の正確さを評価できる。
② メタデータを特に案件関連手順向けまたは特定の公共機関向けに拡張することは、XML スキーマの拡張および／または他の XML スキーマの組み込みによって、ほとんど労力をかけずに実現できる。

最も単純な場合、そのような保管オブジェクトは、バージョン番号およびそのオブジェクトに割り当てられた XML スキーマ・ファイルの表示のほかに、内容のデータ（オブジェクト・ブロック）を含むブロックと、場合によって 1 つまたは複数の署名ブロックとで構成される。オブジェクト・ブロック自体は、XML の中に埋め込まれた 1 つまたは複数の文書を含むことができる。各ブロックには前書きとしてメタデータが含まれており、その中に文書識別（文書 ID)、文書とその発生元の説明などを保存することができる。オプションとして、連邦アーカイブへの伝送のために、説明データのブロックが追加的に利用可能になっている。

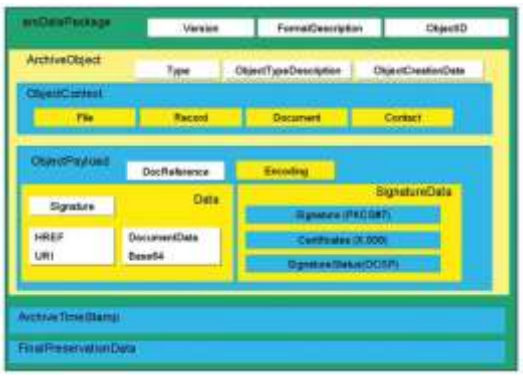
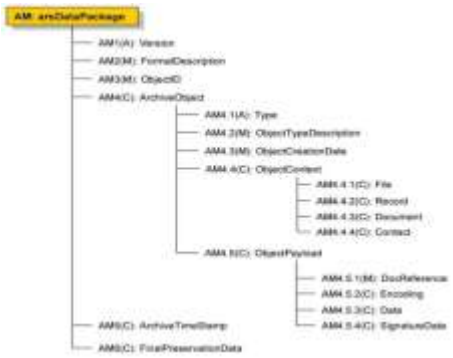


図 2.19：ArchiSafe メタデータの体系（文献[223-4]より図を引用）

文書自体に関しては PDF-A が標準として想定されているが、これは XML の中に埋め込む前にまずテキスト・フォーマット（Base64）に変換しなければならない。多くの記憶容量を必要とするバイナリ・データは、長期メモリーへのアクセスが頻繁に行われる場合、最終的に効率向上のためではなく、XML データ・フローの中で添付ファイルとして参照することを推奨する。この場合、オブジェクト・ブロックにそのバイナリ・ファイルへの参照を設けなければならない。すると、バイナリ・ファイルが追加的に保管される。さらに、ArchiSafe 概念によれば、実際の内容データ（文書の内容）も XML ファイルの内部および外部に複数の異なる文書フォーマットで保存できる。このような ArchiSafe 準拠 XML スキーマは、ARS（ArchiSafe 記録管理方針（ArchiSafe Record-Keeping Strategy）の「ARS XML データパッケージおよびメタデータ」に規定されている。



A：属性、M：メタデータ、C：コンテナー

図 2.20：ArchiSafe メタデータのツリー（文献[223-4]より図を引用）

(5) インタフェース

ArchiSafe によるアーカイブシステムは、前述のように 3 層構造となっており、アプリケーション層とアーカイブミドルウェア層、アーカイブミドルウェア層とストレージ層にインタフェースをもつ。BSI TR 03125 では、アプリケーション層とアーカイブミドルウェア層のインタフェースとして、表 2.6 に示す、XML アダプターと ArchiSafe モジュールの間のインタフェースを規定している。基本的なシーケンスは、先ず、ArchiveSubmissionRequest で XAIP ドキュメントを格納し、受取証（トークン）を受け取る。検索時は、ArchiveRetreivalRequest でトークンを提示することにより、対応する XAIP ドキュメントを受け取ることができる。

表 2.6：XML アファプターArchiSafe モジュール間インタフェース（ドイツ FRAUNHOFER SIT 訪問調査に基づき作成）

要求/応答	説明	主なパラメタ
ArchiveSubmissionRequest	格納要求	XAIP ドキュメント
ArchiveSubmissionResponse	格納応答	ステータス、トークン
ArchiveRetrievalRequest	検索要求	トークン
ArchiveRetrievalResponse	検索応答	ステータス、XAIP ドキュメント
ArchiveEvidenceRequest	証拠要求	トークン
ArchiveEvidenceResponse	証拠応答	ステータス、証拠記録（ERS）
ArchiveDeletionRequest	削除要求	トークン
ArchiveDeletionResponse	削除応答	ステータス
ArchiveDataRequest	データ要求	トークン or 格納場所
ArchiveDataResponse	データ応答	XAIP データ

ファイル、案件、および文書の間の関係は、もっぱら「保管された」オブジェクト、すなわち文書のメタデータを通じて関連付けられる。これは、ファイルまたは案件の設定は、最初に ArchiSafe ソリューションの外部、すなわち案件関連手順の中で具体化し保存する必要があることを意味している(つまり。ArchiSafeによるアーカイブシステムは、この件に関してdon″t care)。保管されたオブジェクトのメタデータを使用することで、長期メモリーに保存されている、ある

特定の案件またはファイルに属するすべての文書のリストを、いつでも動的に再コンパイルできる（たとえば検索を通じて）。

さらに、あるファイルまたは案件の設定および作成に関する情報を、別の文書によって長期メモリーに保存できる。このようにして、予定されている「単一」文書／オブジェクト・ソリューションも、任意の案件関連手順で使用できる。

このことに加えて、後のユーザは、それぞれ専用のファイル構造および案件構造を定義し、必要に応じてそのメタデータを ARS に入力することができる。ここで、ARCHISAFE プロジェクトは、ニーダーザクセン連邦州の IZN（情報技術センター）で集められた経験を基礎として構築されている。

ArchiSafe プロジェクトは 3 段階で開発された。第 1 段階では技術的概念およびデータ処理概念が開発された。これを基礎として、第 2 段階では PTB にパイロットが設置され、機能はまだ限られてはいるが、完全に稼働して特に PTB の電子文書インフラへの具体化と組み込みに関する経験を収集できるようになり、ARCHISAFE ソリューションを他の公共機関へのサービスとして提供することも可能になっている。

2.2.3.6　TransiDoc プロジェクト

電子署名の経年劣化問題に対するソリューションはすでに提供されつつあるが、署名された文書の安全な変換については、標準化とはほど遠い状況にある。目下のところ、この分野の最新技術について語ることは時期尚早である。署名された文書を法律的に安全に変換するためには、組織的な対策と技術的ソリューションを結びつける手段が必要である。

ドイツ経済技術省（German Federal Ministry of Economics and Technology）は、変換された文書の証明力を維持するためのコンセプトとソリューションを開発する目的で TransiDoc プロジェクトに資金を拠出した。このプロジェクトは数々の成果を上げている。

TransiDoc の最初の要件は、ターゲット文書の証明力、すなわち変換の結果がソース文書の証明力と比較できることである。これは、変換された文書がソース文書の代わりに後のフォレンジック的論証で使用できることを前提条件としている。ソース文書の提出は不必要になるべきである。

(1) 署名された文書の安全な変換に関する 10 の原則

TransiDoc プロジェクトによって、署名された文書の安全な変換に関する次のような 10 の原則が定義された。こうした要件は、電子的文書間の変換ばかりでなく、ソースまたはターゲットとしての紙の文書の変換にも対応する。

① 技術的ソリューションが望ましい。つまり、人的ミスを減らして経済効率を高めるために、標準化された技術的手順が使用されなければならない。

② 内容の承諾が保証されなければならない。ソース内容とターゲット内容間の承諾応答相関関係（agreement resp. correlation）についての必要な度合いは、それぞれの使用ケースの状況で決まる。たとえば、無効な署名のように、ソース文書の誤りや不完全性を記録する必要が要求される場合がある。変換の場合のいくつかのケースでは、内容を匿名にする

などのように、ソース内容の故意の変更が必要になる。

③ 作成者の認証、つまりソース文書の署名者の認証が行われなければならない。証明書と失効情報など、使用されたすべての検証データを含む認証結果は、記録されなければならない。手書きの署名は、慎重にスキャナで読み取られなければならない。必要であれば、作成者のその他の情報も収集されなければならない。

④ ソース文書とターゲット文書､すべてのプロトコル､変換で生成された検証結果について、データの完全性が保証されなければならない。

⑤ 変換の帰属性、つまり、変更の責任者は誰だったのかが検証できなければならない。変換の結果が電子的文書になる場合は、適切なセキュリティレベルの電子署名は変換の帰属性に達する。そうでない場合は、紙の書類は必要に応じて手で署名される。

⑥ 責任者の認証、つまり、変換は承認を受けた人物だけが実行できなければならない。責任者の ID、役割、承認が後で検証できなければならない。適切な証明、たとえば、電子署名のための属性証明書は、それぞれの使用ケースで決まる。紙の文書では、手書きの署名は公印で完全にすることができる。変換を行う機関は、法的規制に基づいて独自の承認コンセプトを開発しなければならない。

⑦ データの保護および機密が保証されなければならない。つまり、変換プロセスで使用または生成されたデータには、承認された人物だけにアクセスが許可される。電子署名を検証するために収集される個人データは、最小限必要な量に制限されなければならない。

⑧ ターゲット文書の長期使用性、つまり、ソース文書は明確に解釈できて標準化された長期保存形式でコンバートされなければならない。これは、長期にわたり文書が使用できることと、その内容の証明力を保護することの前提条件である。ターゲット文書には、変換された内容の他にもプロトコルと検証結果が含まれる。こうしたデータは、概要から最も細かい詳細に至るさまざまなレベルで提示されるように構造化されなければならない。ターゲット文書の提示は、さまざまな目的に適応できなければならず、この分野の専門家やさほど詳しくないユーザに対応できなければならない。

⑨ 変換のトレーサビリティ、すなわち、使用したシステムと操作した人物に関する情報を含めた変換ワークフロー全体が、フォレンジック評価できるように記録されなければならない。評価は変換システムと無関係に実施できなければならない。

⑩ 変換システムの信頼性、すなわち、変換プロセスでは、認定を受けたか十分な監査を受けたシステムだけが使用されなければならない。

上記の原則を考慮すると、文書の内容をコンバートするだけではこうした原則を満たすのに十分でないことは明らかである。形式を単にコンバートする場合でさえ、セキュリティを確実にするには、分析ステップなどの補足的なプロセスステップと組織的措置が要求される。こうした要件を識別するには、一般的な変換プロセスの手続き分析が役立つ。安全な文書変換を一連の高レベル変換フェーズとして以下に示す。このフェーズ・モデルは汎用である。すなわち、変換の種類に依存せず、幅広いアプリケーションに応用できる。必要なフェーズ、別のフェーズに包含するか結合させるフェーズ、フェーズが論理的に独立する場合に並列処理が可能なフェーズは、使用ケースで決まる。

(2) コンテキストへの中立性

セキュアな文書変換が何に存在するかを明確にするために、コンテキストに中立な一連の基本概念を導入する。このような抽象的概念は、以下の 2 つの理由によって必要となる。

まず第 1 に、特に法的分野において、多くの適用コンテキストは、それから文書変換のための特別な基準が得られるような、純粋な用語を持っている。このような概念は、変換の一般的分析では回避するべきものとなる。

第 2 に、変換をセキュアにする特性は、適用される領域および変換の目的によって大きく変わる。変換は、データの保護や機密性を理由として行われることがある。その必要性は、たとえば政府文書が法廷で使用され、前もってそれらの部分的な消去が必要な場合に発生し得る。しかし変換の結果が、結果の金銭的価値の面から評価される場合もあるだろう（さまざまな解像度でのデジタル画像など)。適用コンテキストは、具体的ケースにおいてセキュリティーを決定する。法的な規制や考慮は人の生活のほぼ全部分に、また特に、署名された文書のやりとりに関係するため多くの領域で重要となる。したがって、一方で多くの適用領域にまたがるよう十分に柔軟な、しかしもう一方ではそれらに依存しないような概念体系を得るためには、あるレベルの抽象化が不可欠となる。

これらの抽象化のもうひとつの目的は、人間が紙およびデジタルの文書をその意味に従って最終的に解釈し、評価する「現実世界」のコンテキストと、形式的分析に従うセキュアな文書変換の側面との、インタフェースを導くことである。これは形式化して自動化することの限界の線引きを可能にする。

(3) 変換の目的と趣旨

署名付き文書の変換は、ある趣旨を持ったソース文書の、ある趣旨を持ったターゲット文書への決定論的コンバージョンである。いかなる署名付き文書の趣旨も、与えられた適用領域のコンテキスト内で、あり得る利用の結合体として、すなわちその文書内で実現可能な使用法として実際的に理解されるべきである。原理的には、ターゲット文書の趣旨はソース文書のそれよりも大きい場合、小さい場合、または等しい場合があり得るが、それらの例外ケースを別にすれば、それぞれの趣旨が直接に比較可能なことはほとんどない。

変換の目的は、与えられたソースから、ある趣旨を持ったターゲット文書を得ることである。一般に、多くの場合に制限的な意味で、ターゲットの趣旨は部分的にソースによって決定されるだろう。この時点では、コンテンツと署名は双方とも趣旨に寄与し、したがって変換の目的をサポートすると同時に決定するものとのみなし、これらはまだ区別されていない。

他の変換は混合や組み合わせと考えられるという意味で、言及した 3 つの変換の特別ケースは基本的なものである。これらは、以下の 3 つの目的に対応する。

① ターゲットによって置き換わる場合には、ターゲットは―可能な限り―ソースと同一の趣旨を伝達していなければならない。置換文書の例として、紙文書の証明済みコピー（例証）がある。また、デジタル・ワークフローの前処理段階としての P→E 変換がある。たとえば文書を政府機関に提出する場合など､受信人のために文書の読みやすさを確保することは、データ形式の変換を必要とする場合が多い。

② 一定の利用に制限された部分コピーのみが要求される場合には、ターゲットの趣旨はソー

スのそれよりも小さい。

例としては、公的記録からの、指定目的のための証明済みの抜粋がある。また、データ保護を理由とした文書の匿名版がある。医療記録は、主治医への帰属可能性を保ちつつ、医学研究のために匿名化されることがある。

③ 変換は、ソースに対するターゲット文書のバロリゼーション（役割の引き上げ）を伴う、つまりソースの利用性を超えた、ある利用性を可能にすることがある。また、シンプルでしかし実際に関連のある例としては、後の使用のために空のフィールドを付加して、電子文書形式が新バージョンに移行することがある。代替フォントやその他の表現の付加により、文書が障害者にとってアクセス可能になることがある。

なお、コンテンツや署名の付加によるバロリゼーションは、ここで検討する変換の範疇に入らない。

(4) 忠実製、信頼性、安全性

ある目的を満たすために、変換は忠実性の適切な必要条件を満たさなければならなず、「必要な目的のためにコンテンツを忠実にコンバートすること」は、ソースとターゲットのコンテンツの 1 対 1 の一致とは対照的なことと理解されるべきである。忠実性は、署名を含めてソースとターゲットの全関連部分に関係する。ソース、ターゲット、変換の改訂可能な性質への参照は忠実性の概念の特質であり、それ自身をソースとターゲット間の意味論的意味の変更とは反対に置く。このような変更は現実の適用コンテキスト内に存在するため、形式的に把握することがほとんど不可能である。忠実性の評価のためにどの特質を調べなければならないかは、変換の目的に依存する。何を調べることが可能かは、ソースとターゲット文書そのものに依存している。

ソースとターゲットのデータ形式が、署名された全コンテンツを正しく表すために適切かどうかも、忠実性にとって最重要の問題である。これは、変換の法的監査を可能にするため必要であり、また、署名付きデジタル・データに対してはプレゼンテーション問題（見て確認したものが署名の対象（What You See is What You Sign ― WYSIWYS）の問題とも言われる）の適切な判断が必要になる。

適切なセキュリティー手段がなければ、忠実性の事後的な調査を行うことはできない。したがって、セキュアな変換に到達するためには、変換の目的に従いターゲットがソースに対して正しい忠実性を持つことを主張できる記録を保たなければならない。このような主張の信頼性とは、どのような種類の変換が起こったか、誰どのようにしてその忠実性を主張してきたか、また、変換と結果の評価について誰が責任を負うかを、後でたどれることを意味している。フォレンジック上の調査を可能にするには、ソースをすでに得ることができなくてもターゲットは目的を果たさなければならないという意味で、信頼性に対して高い基準を設定する必要がある。非再現可能性および廃れたデータ形式は、それらの最も重要な例である。

変換の忠実性を評価し、プロセスの最後でそれを証明することのできる事例はいくつかある。大規模なアプリケーションでは、変換システム自体が、一定のアルゴリズムがデータコンバージョンのために適用されたこと、また、たとえばソースの署名が適切に検証されたことを確証することができる。一方で、公証の場合には、権限を持つ者が忠実性を調査して、調査結果を書き留めて署名によりそれを裏付けることによって、信頼性を立証する必要がある。これまで導いた概

念をまとめると、以下のことが言える。

セキュアな変換は、ある目的のための忠実性の信頼性によって保証される。一方で、目的とはそれぞれの趣旨を伴ったソースとターゲット間のコンバージョンである。このシステム概念の中心的結果は、要求される趣旨の変更により目的が決定される場所で、適用コンテキストと変換プロセスが正確にリンクしていることとなる。ここに、セキュアな変換の形式化と実用化に対する、困難さが存在している。

(5) 文書変換プロセス

セキュアな変換のための必要条件を満たすには、文書のコンテンツをコンバートするだけでは十分ではない。シンプルな形式コンバージョンの場合でも、安全性を保証するには、そのためのプロセス段階の追加と組織的な手段が必要になる。このような必要条件を導き出すには、一般的な変換プロセスの手続きの分析が役に立つ。以下では変換の種類（紙文書→電子文書、電子文書→電子文書、電子文書→紙文書）に依存することなしに、変換を連続した段階として示している。これによって、特別なケースでは一部の段階は重要性が低く、他に包含されたり他と組み合わされたりすることがある、あるいは論理的に独立していれば並列化されることがあるという了解の下での、ハイレベルの変換段階の最大セットが得られる。図 2.21 はその概要を示している。

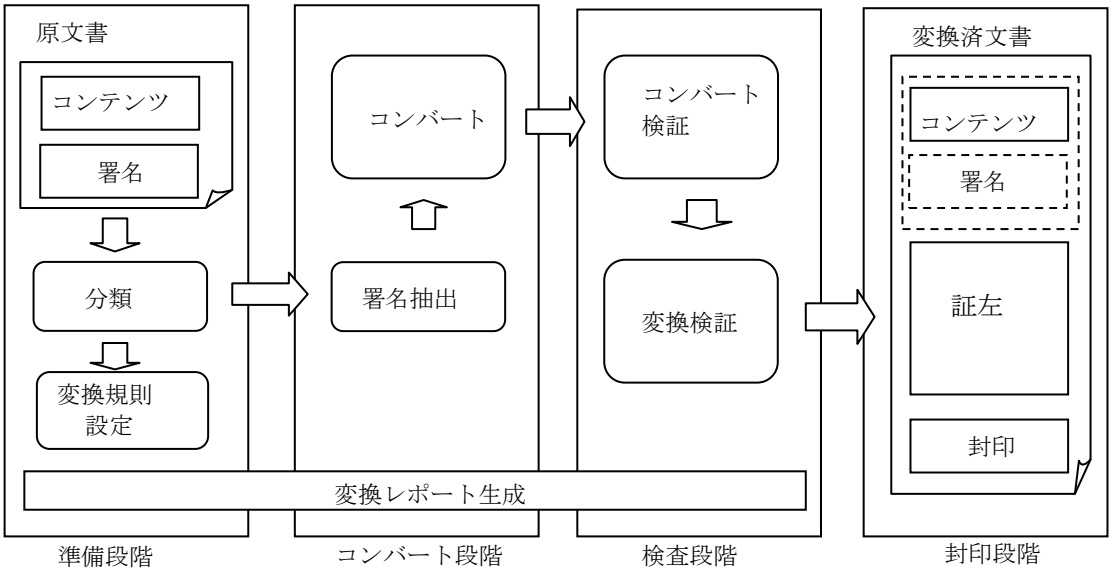


図 2.21：文書変換プロセス（文献[223-3]より図を作成）

① 準備段階

(a) 分類

最初の段階では、変換の目的を決定するためにソース文書を調べる。この分類は、ソースの関連特性を確定するだけでなくターゲットと変換の関連特性も確定し、要求される忠実性の達成のためにはこれを満たされなければならない。分類に続くのがルールで、これは、特に法的監査のためにプロセスからどのデータを保持しなければならないか、ターゲットに対しどのチェックを行う必要があるかという、信頼性が確立されるための方法を制御する。

分類は、要求される目的に対してソースがそもそも適切かどうかも判断する。その重要な例として、前述した署名付きデジタルデータのプレゼンテーション問題がある。これは、変換システムにおける提示コンポーネントへの要求を起こしたり、自動化に制限を与えたり、またはセキュアな変換を全く禁じるかもしれない。署名付きの紙文書であっても、注釈、取り消し、テキストの修正などの適切な処理を、完全に明確に指定しなければならない。より高次のレベルでは、たとえば一定数の署名が正しい場所にあるなど、ソースが満たすべき（法的）手続きが、そのソースが変換のために適格かどうかを決定する基準となることがある。

ソースと変換の目的を表す分類データとともに、ルールセットも分類の中心的な結果である。これは、後に続く全段階を制御する総合的なルールセットを表す、抽象的用語である。しかし、これは各々の特別な適用ケースにおいて組織的規定、技術的手段、責任の帰属、署名の検証と生成のためのルールなどの、非常に具体的な意味を持っている。

一般にルールセットは、機械処理が可能な命令と、人間によってのみ理解が可能な規範的指示との組み合わせである。場合によっては公証と同様に、すでに後者は既存の法的規制に関連付けられていることがある。特別な目的のための変換を伴う適用シナリオは多数あるために、特定領域のための一般的なルールセットを定義して、一般ルールを参照しそれを適切に特殊化するプロファイルに従って、それらを適応させることが実際的となる。このような一般的ルールセットは広範で、モージュール式であり、組み合わせ可能、パラメータ化が可能であることが望まれる。

変換の間に蓄積された情報を運ぶデータコンテナとしての変換記録は、純粋に技術的な理由だけでなく、たとえばコンバージョンのプロトコルや後の段階で実行される検査などの関係するメタデータを保存することによって、セキュリティを確立するためにも役立つ。変換記録の最初の項目は、ルールセットである。

変換記録は、関連するデータを相互に適切に結合するためにも役立つ。特に、

- ソースのコンテンツは全プロセスにわたって唯一に識別されなければならず、記録はそのための識別子を持っている、
- 同様に、ルールセットもプロセスにわたって唯一でなければならない、
- ターゲットのコンテンツの完全性と、そのソースのコンテンツとの関連を確保しなければならない、
- プロトコルおよび生成されるメタデータは、プロセスにわたって唯一性を保ち、純粋でなければならない。

閉鎖型の変換システムでは、記録は上述の対象を保存するシンプルなデータコンテナが可能だが、分散型プロセシングや純粋なセキュリティー要件によって、上述の結合やデータの完全性を維持するために、一部を暗号化でに安全にすることが必要な場合がある。

② コンバート段階

(a) 署名の抽出

署名抽出においては、ソースの署名を収集して、ソース署名として変換記録に加える。デジタル署名の検証、あるいは手書き署名の署名者の認証が必要か否かは、ルールセットが決定する。この場合に、ルールセットは検証ポリシーの指定、署名データ（タイムスタンプ、属性など）を記録にもたらすかの指定も行い、検証の結果も記録に加える。

(b) コンバート

この段階では、ルールセットのルールに従って、ソースからターゲットへの、コンテンツの適切なコンバージョンが行われる。ターゲットのコンテンツを除いて、コンバージョンプロトコルとエラーログを記録に加える。

③ 検査段階

(a) コンバート検証

すべてではないが多くのケースで、2 ステップの事後検査を変換プロセスに含めて、信頼性のレベルを上げることができる。これらのステップは、コンバートされたコンテンツの人間による検査、ターゲットとの自動比較、変換記録のデータの一貫性チェックなどが混ざって構成される場合があることを示すために、ここでは分析（assay）というあまり一般的でない用語を使用している。多くの場合にデジタル署名に結び付けられると理解されている、検証（verification）の概念と区別することにもなる。

最初のステップはルールセットの指示に従い、いかなる可能な方法によっても、コンテンツのコンバージョンの結果を分析する。上述のようにこれは、人が信頼可能な表示コンポーネントを使用してソース文書と変換されたコンテンツを比較することから、単に変換されたコンテンツの特定データ形式（XML スキーマなど）に対する構文的準拠をチェックすることまで、いかなることをも意味する。同様のチェックは、それがすでに暗黙的に署名抽出の間に行われていなければ、署名データに対して行われることがある。最重要のこととして、もし許容され、またコンバージョン分析が肯定的な結果をもたらせば、この時点でソースは変換プロセスから捨てられることがある。またその双方のための基準は、ここでもルールセットが指定する。

(b) 変換検証

最終のステップは、全体の変換プロセスの正確性をチェックする。たとえば分散型の変換システムでは、必要な全段階が行われていることの確認、あるいは変換記録の一定部分に対するハッシュ値の再照合が必要な場合がある。

④ 封印段階

2 つの分析ステップで肯定的な結果が得られると、変換記録が完了し、変換それ自体も終了する。しかしまだ、これらの結果を保証してセキュアな変換の最終目的を達成する作業が残っている。そのために、変換された文書に変換シールを貼付して、変換者による署名を行う。

ソースが後の比較のために得られない場合でも、変換の結果は保証されている必要がある。これが、変換プロセスで生成された関連データが持続的に信頼的にターゲットに結び付けられて、徹底した法的監査が可能でなければならない、主な理由となっている。変換の品質を帰納的に評価できる可能性は、ターゲットの証拠力のための重要な構成要素となる。これは以下の 3 つの下位目的の中に具体化されており、それらは変換シールの最も重要な目的を表している。

- 変換された文書、および他の記録されたデータの完全性の保証。
- 指定されたルールセットに従った変換の正確性の保証。
- 変換の変換エンティティへの帰属と、その事実の否認防止。

変換記録のどの部分を変換シールに転送する必要があるかの指示は、一般にルールセットが含んでいる。このシールは、変換プロセスがルールセットに則って正しく実行され、したがっ

てソースとターゲット間で要求される忠実性が達成されていることを保証する。技術的には、変換シールは暗号的にセキュアなデータコンテナと、変換記録および他の関連するメタデータから選択されたデータとして実現が可能である。これは常に、変換を行ったエンティティもしくは個人により（デジタル）署名されなければならない。

特に分析とシーリングの段階では、技術、セキュリティー、および法的な理由によって、人間による検査の必要性が生じることがある。変換システムの定期的な検査と結果のプロービングは、セキュアな変換システムのために、おそらく標準の組織的必要条件である。原本のコンテンツが構造化されていない場合には、部分的に変換そのものが手動で実行されなければならず、したがって結果も（独立して）人間が検査する必要がある。公証人の場合にあり得るように、ターゲットをシールする個人が担う法的責任は、ターゲットを検査する必要性を伴う。言うまでもなく、人間による干渉は、常にそれ自体のリスクを技術プロセスにもたらす。しかし、これは一般に避けられないことであり、たとえば前述のプレゼンテーション問題を考慮した信頼可能な表示コンポーネントや、署名者の信頼可能な端末などの技術が、セキュアなフェイルセーフの手段をサポートしなければならない。他にも悪意のある行為のリスクがあるが、たとえば公証/公的シールの過失または詐欺による使用に対する法的責任については、民事および刑事の法律がすでにカバーしている。

2.2.3.7　LTANS/ERS

IETF の作業グループ LTANS（長期アーカイブ保管及び公証サービス）で標準化された、RFC 4998「証拠記録・シンタックス」（ERS）は、時間のある時点でのデータの存在の長期的な否認拒否（non-repudiation）を支援するデータ構造（証拠記録）を定義している。

ERS は、データオブジェクトを単なるビット・ストリングと看做し（つまり、内部構造は Don't care）、それらにタイムスタンプを付与する構造を定義する。ERS はまとまった文書の保存に効果的であり、一方 XAdES-A は、個々の署名の長期的な有効性検証を必要とするような文書保存サービスに向く。

(1) LTANS ERS ハッシュ木の構築

詳細なアルゴリズムは RFC 4998 に記載されている。ここではその概略を述べる。

LTANS ERS のハッシュ木は次のように構築する（図 2.22 を参照）

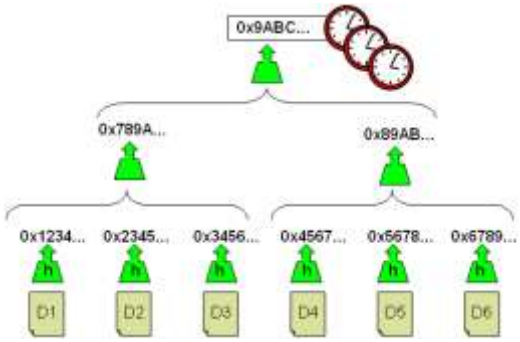


図 2.22：ハッシュ木（文献[223-6]より図を引用）

① 多くのデータオブジェクトがあると仮定する：D1、D2、D3、D4、D5、D6 など

② 各々のデータオブジェクトのハッシュを計算する：h(D1)、h(D2)、h(D3)、h(D4)、h(D5)、h(D6)

③ 「ハッシュ木」を作成する：

・ハッシュのグループを作り、ハッシュのグループに対して新しいハッシュを計算する:h[h(D1)、h(D2)、h(D3)]]そして h[h(D4)、h(D5)、h(D6)]

・これらの新しいハッシュのグループを作り、新しいハッシュのグループに対してさらにハッシュを計算する。h{h[h(D1)、h(D2)、h(D3)]、h[h(D4)、h(D5)、h(D6)]}

・1 つのハッシュ（図 2.22 参照）になるまで、グループ化とハッシュを繰り返す。

・いわゆる Merkle ハッシュ木が作成できる。最終ハッシュつまり木の根のハッシュは、各データオブジェクトのハッシュに依存することから、それは、すべてのデータオブジェクトの中のすべてのビットに依存する。

④ 根ハッシュへのタイムスタンプ

これにより、データオブジェクトすべてにタイムスタンプされる。ハッシュ木の根ハッシュ上のタイムスタンプは、木の葉の中の各データオブジェクトの存在を証明する。

⑤ タイムスタンプハッシュを更新する必要がある場合は再度タイムスタンプする。

常に、前のタイムスタンプにタイムスタンプを付ける。ERS では、タイムスタンプのこのチェーンをタイムスタンプチェーンと呼ぶ。

(2) ハッシュ木の更新

ハッシュアルゴリズムが危殆化する前に、ハッシュ木を更新する必要がある。つまり、新しいハッシュアルゴリズムによって新しいハッシュ木を構築する必要がある。

新しいハッシュアルゴリズムによる新しいハッシュ木の構築のために、全てのデータオブジェクトが必要となり、また、前のハッシュ木のタイムスタンプ鎖中のタイムスタンプも必要となる（その結果として、最初のタイムスタンプの有効性を証明することができる)。

この構造を格納するために、根ハッシュ上にデータオブジェクトとタイムスタンプを格納する必要がある。なお、データオブジェクトの全セットに基づいてハッシュを計算することができるので、必ずしもハッシュ木を自体格納する必要はない。

(3) ハッシュ木の縮退

ハッシュ木は、根ハッシュ上の最初のタイムスタンプの中で示された時点の、木の葉のすべてのデータオブジェクトの存在を証明する。しかしながら、単に 1 つの葉のデータオブジェクトの存在を証明するにも、すべてのデータオブジェクトを示さなければならない。

Merkle ハッシュ木は 1 つのデータオブジェクトに減らすことができる。

縮小手続きにでは、不必要なデータオブジェクトはすべてを削除することができる。また、根から希望の葉ノードおよびあるそれらの直接の子どもニーズまでのパス上のノードだけを示す。（図 2.23 を参照。）

縮退されたハッシュ木に基づいて、あるデータオブジェクトから根ハッシュ値を計算すること

ができることが実証されている。また、根ハッシュ上のタイムスタンプ鎖を確認することができる。

縮退されたハッシュ木は、ハッシュのリストとして表わすことができる。縮退されたハッシュ木のサイズは､データオブジェクトの数の対数に比例することから､これは効率的な構造である。

図 2.23 において､単に 1 つのデータオブジェクトの存在を証明する必要がある場合ハッシュ木は縮小することができる。また、根ハッシュは今までどおり縮小されたハッシュ木に基づいて計算することができる。

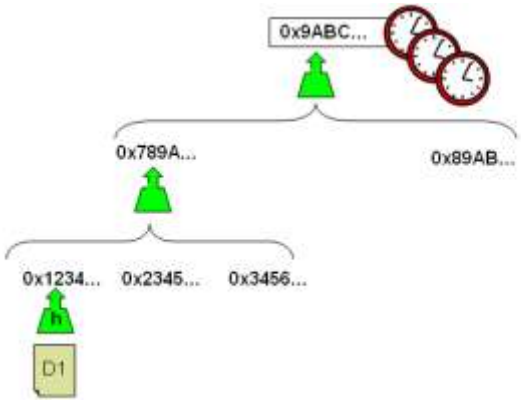


図 2.23：ハッシュ木の縮退（文献[223-6]より図を引用）

ハッシュ木を縮退できることは、この構造を非常に強力にします。

ツリー構造で、1 つのタイムスタンプだけが、すべてのデータオブジェクトの存在を証明することができる。(ハッシュ木の縮小によって）その一方で（比較的）小さなデータ構造と 1 つのデータオブジェクトの存在を証明することが可能となる。これは、LTANS ERS のツリー構造を正当化する。

(4) XAdES と LTANS ERS を利用した保存の比較

表 2.7 は、XAdES による保存と LTANS ERS による保存の比較である。

表 2.7：XAdES と LTANS ERS の比較（文献[223-6]とヒアリングにより作成）

XAdES-A	LTANS ERS
• 署名フォーマット	• ある時点でのデータの存在の長期的な否認拒否を支援するデータ構造
• 署名書類だけをアーカイブに保管するのにふさわしい	• 署名に注目しない • ガーベージイン・ガーベージアウト • タイムスタンプだけで動作する
• 署名検証の支援（それが CRL などのプレースホールダーを供給するとして）	• 署名に注目しない • 署名検証を支援しない • CRL は別のデータオブジェクトとしてアッ

	プロードされるか、あるいは AdES-X-L 署名がアップロードされる。
• 文書はそれぞれ独立して保存される	• ハッシュ木はすべての保存文書にリンク
• ドキュメントが独立して保存されているのでアップロードは単純	• 新しいデータオブジェクトが追加されるときは常にハッシュ木の再構築が必要 • したがって、新しい文書はバッチで追加すべきである
• 文書が独立して保存されているので、削除は単純です	• 個々のデータオブジェクトは削除することができる • データオブジェクトのハッシュはハッシュ木に残るが、問題は引き起こさない
• 1 つの署名の有効性を証明する情報はすべて付加されている	• 署名に注目しない • データオブジェクトの存在は縮退されたハッシュ木を使用して証明できる
• アーカイブ・タイムスタンプが追加された場合は常に、保存されていた署名ファイルは規則的に更新される • 読み取り/書き込みメディアが必要 • （あるいは、WORM を規則的に交換する必要がある）	• 保存されていたデータオブジェクトは修正されない • WORM でも動作可能
• 複数署名/文書が保存されている場合、一新のために複数タイムスタンプを規則的に集める必要がある	• 複数データオブジェクトが保存されている場合でも、一新のために 1 つのタイムスタンプだけでよい

［参考文献］

[223-1] "BSI TR-03125 Beweiswerterhaltung kryptographisch signierter Dokumente"

[223-2] "Legal Security for Transformations of Signed Documents: Fundamental Concepts?", A. U. Schmidt and Z. Loebl., EURO-PKI05

[223-3] "AUTHORISED TRANSLATIONS OF ELECTRONIC DOCUMENTS", J. Piechalski, A, U. Schmidt, ISSA06

[223-4] "Long-term security for signed documents: services,protocols, and data structures", T. Kunz, S. Okunick, U. Viebeg ,etrics2006

[223-5] "社会実情データ図録, http://www2.ttcn.ne.jp/honkawa/6300.html"

[223-6] "LTANS Evidence Record Syntax, Overview" István Zsolt BERTA,

2.3 Web 調査結果

2.3.1 エストニア

2.3.1.1 エストニアの基本情報 [1]

エストニアはヨーロッパ北部に位置し、西にバルト海を臨む、日本にとって「いちばん近いヨーロッパ」のひとつである。

九州よりやや大きい国土に、福岡市とほぼ同数の約 135 万の人々が住んでいる。人口密度は 1 平方㎞あたり 31 人で、日本の同 343 人と比較すると単純計算で一人あたり 11 倍以上の土地があることになる。しかしながら、首都には人口の約 30%にあたる 39 万 6 千人が住んでおり、一極集中により人口が密集していると言われる東京都でも約 10%であるから、それと比較しても、はるかに高い首都への人口集中である。

1992 年に旧ソ連から再独立後、政府は IT とバイオテクノロジーに資本を集中していくことを決定し、国民もそれを支持した。幸いにも、この政策は今日まで一貫していて、エストニアの成功の大きな要因になった。もうひとつの成功の要因としてソ連時代の旧システムに対する執着がないため、最新のシステムを導入することに対して既存のシステムの運用者側からの抵抗がほとんどなかったこともあげられる。

2004 年には欧州連合（EU）に加盟している。急速な経済的発展、寛大な税制、そして地理的条件にも恵まれ（バルト海地域の国の総人口は 9 千万人以上であり、エストニアの位置はその地域のほぼ中心､すなわちエストニアはヨーロッパの中で急成長している市場の中心に位置している)、エストニアは海外からの直接投資を集める中央・東ヨーロッパのリーダ的存在である。

エストニアは、教育レベルが高く相対的に賃金が安いことから、第一の貿易相手国であるフィンランドの情報産業の開発部門が多数進出している。そのため、情報産業も育ってきており、音声通話ソフトで有名な Skype Technologies 社はエストニアで創業された企業で、本社はルクセンブルクにおいているが、開発拠点はエストニアの首都タリンにある。

2.3.1.2 エストニアの IT

エストニアは IT 先進国といわれている。これは、国が IT 推進を第一の政策にあげたこともあるが､もうひとつの成功の要因として､X-Road を代表とする IT 基盤を国が構築したことにある。IT 基盤を利用することにより､サービス提供側にとってコストをかけずにアプリケーションを作成することが可能になった。

簡単に IT 推進の歴史を紹介してから、X-Road について紹介する。

(1) IT 推進の歴史

独立当初は、道路などの生活基盤や学校などの公共建築物もかなり整備が必要であった。しかし、インターネットの利用環境の整備に力を注ぎ、学校などでは、屋根の修理よりもパソコンの導入を優先したとさえいわれている。

① タイガーリープ（虎の躍進）プロジェクト

1996 年～2000 年にかけて、タイガーリープ（虎の躍進）プロジェクトが実施された。IT を使用した結果として経済が急激に発展したシンガポールに代表される東南アジア諸国のように、

IT を使用して虎のひと跳びのように先進国を追い越すことを目標に、すべての学校でインターネットを利用できる環境が整備された。同時に新しいスキルとして教師に対しインターネット教育を実施した。

② The Look@World プロジェクト

民間会社数社が 2002 年 4 月からエストニアの人口の 10%に当たる約 10 万人に対して無料でインターネット利用の基礎的な教育を行うプロジェクトを実施した。

トレーニングは、2 日連続（1 日 8 時間・計 16 時間）で実施した。

1 日目：コンピュータと OS（オペレーションシステム）に関する基礎知識

2 日目：インターネット使用の方法

③ WiFi 無料化の草の根運動

WiFi は業界団体の WECA（ワイヤレス・イーサネット・コンパティビリティ・アライアンス）が、無線 LAN の標準規格「IEEE802.11b」の互換性を保証するために定めた名称で、「Wireless Fidelity（ワイヤレス・フィデリティ）」の略である。この WiFi の利用環境を、レストラン、ガソリンスタンド、空港など多くの場所に構築し、外出先でも簡単にインターネットを利用できるようにしていった。

④ インターネット投票

エストニアは、2005 年の地方政府の選挙で初めて自宅からインターネットを介し電子的に投票を行い、世界の注目を集めた。エストニアはまた、国会総選挙（2007 年 3 月）でもインターネット投票を利用した。インターネットで投票した人はまだ少ないが、国民のほぼ全員が eID カードを持っていることで、こういったサービスが可能になった。

(2) X-Road：安全なデータ交換層

X-Road は国の情報システムのデータ交換層であり、X-Road アーキテクチャの構築は複雑なセキュリティソリューション（認証、マルチレベルの認証、高レベルのログ処理システム、タイムスタンプ付きの暗号化されたデータトラフィック、サイバー攻撃をサーバに警告するシステムなど）を X-Road 上に組み込むことを基本的な出発点とした。

X-Road プロジェクトの枠組みの中で、エストニアの e ガバメント・アーキテクチャーが開発された。

エストニアの e ガバメント・アーキテクチャーの概要を図 2.24 に示す。

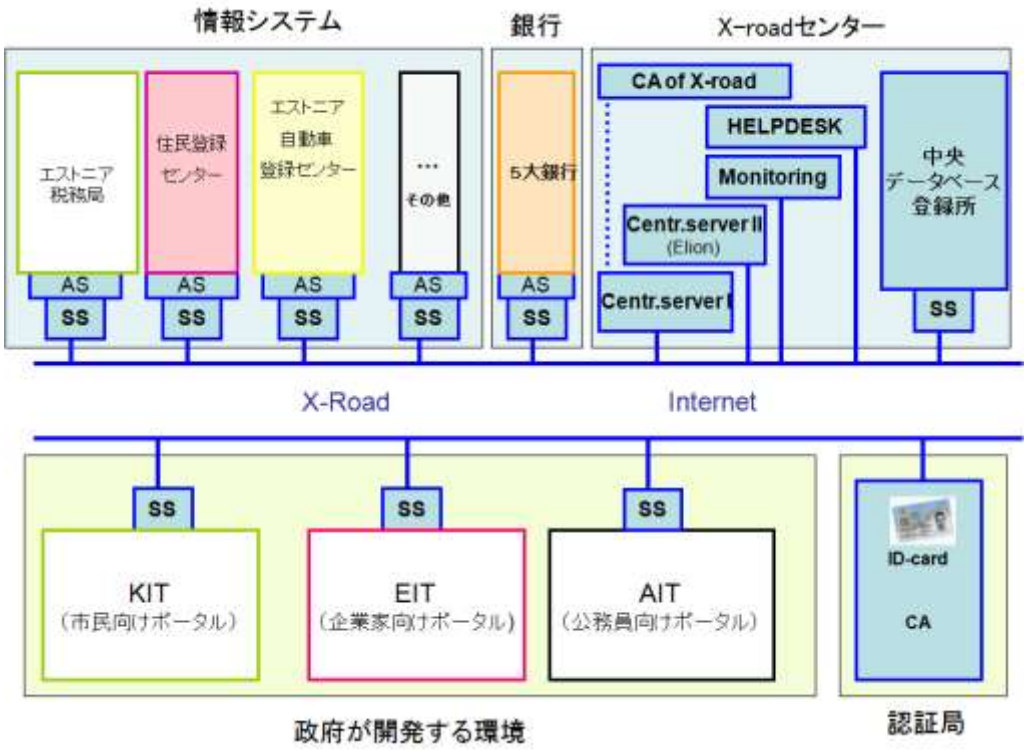


図 2.24：X-Road による情報交換の枠組み

e ガバメント環境の主なバックボーンは、分散サーバーおよび中央サーバーの X-Road ネットワークである。e ガバメント・プロジェクト自体は、X-Road インフラストラクチャー・プロジェクトと並行して発足し、ID カードや PKI のプロジェクトは、一部のバック・オフィス情報システムの開発と並行して発足した。もちろん、それまでに開発済みの一連の情報システムもある。基本的な構成要素について説明する。

① セキュリティー・サーバー（SS）

e ガバメントの本質は、さまざまな情報システムがセキュリティー・サーバー（SS）を介して通信できる点にある。SS は、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、たとえばサービスを誰がいつ利用したのかとか、特定の状況下でどのような意思決定が行われたのかなど、過去の状況を復元できる。

セキュリティー・サーバーでは、主に暗号化された形式でログが保存および保守管理される。たとえば、市民向けポータルのログには特殊なソリューションが備わっている。これらのログは、すべての市民が ID カードのキーを使用して閲覧できる。ただし、このキーを変更すると、キーの所有者を含むすべての市民がこれらのログを閲覧できなくなる。

② 民間銀行の役割

e ガバメント環境では、情報システムがサービス提供者とサービス利用者の両方の役割を果たす。エストニアの商業銀行（正確には Hansapank、SEB Eesti Ühispank、Sampo Pank、Krediidipank、および Nordea Pank）は、e ガバメントのスキーマで 3 つの異なった役割を果たしている。

第一に、これらの銀行では、市民の認証サービスを行うポータルを提供している。このポー

タルはｅガバメントに接続されている。これは、エストニアの全市民がeIDカードを所有しているわけではないが、人口の半数以上が既に商業銀行とインターネット銀行機能の契約をしているためである。これらの銀行で提供されている認証メカニズムは、eID カードに基づく認証と同程度の信頼性があり、ｅガバメント・サービスの利用に有効であると考えられている。

第二に、一部のサービスは有料であるため、これらの料金を支払うためのソリューションが開発されている。まず、一般市民は料金を銀行に振り込む。すると、その直後に電子サービスが自動的に開始される。

第三に、これらの銀行自体がデータや電子サービスの利用者であり、他の情報システムと同様にこの環境を利用している。

③　アダプター・サーバー（AS）

図2.24に、すべての情報システムがアダプター・サーバー（AS）経由でX-Roadのセキュリティー・サーバーに接続されている様子を示す。アダプター・サーバーは、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。現在使用されているデータ転送プロトコルはSOAPである。

④　中央サーバー

ネットワーク全体のすべての中央サーバー（中央の監視サーバー、認証サーバーなど）は、X-Roadセンターに接続され、そのセンターに置かれるため、実際にはX-Roadセンターがｅガバメント環境の中心である。X-Roadセンターでは、ｅガバメントのハードウェア、ソフトウェア、インターネット接続、合意などを管理する専門スタッフが採用されている。

⑤　エストニア認証機関（CA）

エストニア認証機関（CA）は、エストニアにおけるeIDカード、デジタル署名、および他のPKIのインフラストラクチャー要素関連の開発を担当する。

⑥　ポータルサイト

一般市民とｅガバメント環境の直接通信は、市民向けポータル、企業家向けポータル、公務員向けポータルといった一連の通信ポータル上で機能する。

市民向けポータルは一般市民と政府の間でｅガバメント・サービスを仲介する主なチャネルとなっている（www.eesti.ee）。このポータルでは、法律に従い、すべてのエストニア市民は、政府が市民に関して収集したデータの内容を知る権利を有する。

公務員向けポータルは、現在MISP（Mini InfoSystem Portal）として実装されている。このポータルは、約70の中央政府および地方政府の機関で使用されている。これらのポータルは、すべてｅガバメント・サービスのユーザー・マニュアルおよびサービス・ポータルとして利用可能な情報ポータルとして構成されている。

2.3.1.3　エストニアにおける電子記録管理の推進[231-2][231-3][231-6]

文書管理の開発は、国家事務局（State Chancellery）の記録管理部（Records Management Department）の担当である。同部門の主な業務には、公共部門の文書管理および保管、関連法規の原案作成、国家機関における文書管理の開発（電子文書管理への移行を含む）の調整などが含まれる。

公共部門の文書管理をより適切に調整するために、国家事務局の記録管理部では、2004 年春に記録管理者の協力ネットワークが設立された。同ネットワークの目的は、以下のとおりである。

・　国家機関の文書管理開発に関する知識の強化
・　公共部門における文書管理開発の全般的計画の改善
・　ノウハウ、ベスト・プラクティス、経験などの交流促進
・　国家機関の文書管理者間における連絡と調整の促進

協力ネットワークは、公共部門の電子文書管理戦略の草案作成において国家事務局をサポートしている。当面の主な戦略目標は、公共部門における迅速、簡単、かつ便利な文書管理を確保することである。

「エストニア情報ポリシーの原則（Principles of the Estonian Information Policy）2004～2006」、「2005 年および 2006 年の情報ポリシー行動計画」および「文書管理および保管の開発計画（Development Plan for Document Management and Archiving）2002～2005」を元に、国家事務局は、2005 年に電子文書交換プロジェクトを発足させた。このプロジェクトの目的は、以下のとおりである。

・　省庁の文書管理システム間のインタフェースの作成
・　省庁の情報システム間の相互運用性の確保
・　省庁における電子文書管理の割合の増加
・　電子文書手続の開発

その結果、省庁のさまざまな文書管理システムで、データ交換層 X-Road を介して文書を交換できるようになる。

省庁間の電子文書交換を可能にするには、文書管理システム間のインタフェースを開発する必要がある。2005 年初頭に行われた調査によると、各省庁では、機能や実装が異なるさまざまな種類の文書管理ソフトウェアが使用されている。電子文書交換プロジェクトの発足に対する国家機関の対応は、各機関に電子文書管理およびデジタル署名が導入されるか否かにかかっていた。

電子文書交換のための文書管理システムを各省庁で準備するには、更なるソフトウェア開発をソフトウェア開発者に委託する必要があった。

①　電子文書交換プロジェクト開始

プロジェクトの基本目標の定義と現状の把握を目的とし、2005 年夏にある調査が行われた。この調査では、省庁の文書登録機関に保管されているデータを元に、国家機関の間で交換される文書の総量、電子文書管理の割合、メタデータの構造などが分析された。

さまざまな文書管理システムの相互運用性を確保するには、プロジェクトの準備段階で、以下の要素を編集、テスト、および実装する必要がある。

・　電子文書管理およびデジタル文書の保存に必要なメタデータの標準リスト
・　XML 形式の共通の文書テンプレート

開発プロジェクトは、以下の 2 段階に分けて実施される。

2005 年に実施された試験運用プロジェクトでは、さまざまな文書管理システム間のインタフェースを作成することによる、電子文書交換アプリケーションの開発と、内務省、財務省、国防省の 3 省庁が使用する Postipoiss という文書管理ソフトウェアと、国家事務局が使用する GoPro という別の文書管理ソフトウェアの、異なるソフトウェアを使用する文書管理システム

間でテストされた。試験運用に関わった機関は、国防省、財務省、国家事務局、内務省などである。

2006 年のプロジェクトの第 2 段階には残りの各省庁も参加した。この年には、Amphora、Livelink、Postipoiss、Sharepoint、GoPro、Webdesktop といった文書管理システムのインタフェースが開発され、X-Road を経由する複数の異なる文書管理システム間において自動でセキュアな文書交換がテストされた。この文書交換は多機関間協定に基づいて行われた。次の段階としては、県、各省庁の管轄下の行政機関などのプロジェクトへの段階的な参加が予定されている。

DEC のより幅広い導入は始まったばかりであった 2006 年 11 月には、約 60 の機関がほぼ 500 の文書を DEP 経由で交換していた。DEC を使用すると、特定の機関で使用されている文書管理ソフトウェアにかかわりなく、ペーパーレス文書交換を公共部門に段階的に導入でき、送信されるデジタル文書の整合性を保証し、長期的保管の事前条件を作成することができる。

2007 年 10 月の初頭、エストニア政府は政府機関におけるペーパーレス事務管理への移行をスピードアップすることを目的として「記録管理のための統一ベースに関する規則」を改正した。この結果、各省庁と総理府は 2007 年 12 月 3 日までに記録管理システム間でデジタル文書を交換できるようにすることを義務づけられた。県庁、各種委員会、検査庁についてはこのタイムリミットは 2008 年 5 月 5 日になっている。(3 つの省だけは例外的にもっと長い移行期間を許されている。)

改正された規則では、X-Road 文書交換センターを通じ、国際的に認められたデータ交換標準である XML (Extensible Markup Language) を使ってデジタル文書を交換することになっている。システム間のデジタル文書交換への移行は (機関ごと、文書のタイプごとに) 段階的に行われる。地方自治体やその他の組織については、事務管理のレベルや利用できるリソースは一様ではない。デジタル文書交換への移行期間が長く設定されているのはこのためである。すべての政府機関に同じ条件を設定するのは適切でない。移行はさまざまな措置によってサポートされる。

また、ペーパーレス事務管理への移行に向けて、記録管理とシステム間のデジタル文書交換の要件がいくつか変更された。この結果、記録管理は統合プロセスの一部として処理されるようになった。デジタル文書は統一的なデータ構造の文書形式をベースとして作成し、文書管理のメタデータにリンクしなければならない。メタデータは文書のコンテキスト、内容、構造、管理履歴を記述し、(文書が破棄されるか、またはアーカイブに移送されるまで) 文書のライフサイクルのすべての段階でその文書が本物であり、改ざんされておらず、使用できることを保証する。

② 電子文書交換プロジェクト狙い

eGovernment に対する欧州連合のビジョンは、「グッド・ガバナンス (優れた統治) の手段としての eGovernance の効率向上」である。eGovernance は今まで主に公衆のためのより効率的なサービスを意味していたが、行政の合理性やガバナンスの効率向上、透明性の確保、および参加型民主主義の比重も大きくなってきた。文書管理の観点からは、グッド・ガバナンスはコスト効果の高い合理的な資料の利用、行政プロセスの簡素化、サービスの可用性と質の向上、文書管理システムの相互運用性の改善を意味する。

文書管理システムの相互運用性は、これらのシステムでデジタル文書を相互にやり取りおよび管理できることを指す。文書管理システムでは、中間的な書面や通常の郵便などを介さずに情報を交換する。これらのシステムには、一般市民や企業を対象としたネットワーク・サービスの利用や処理を行うためのプロセスが組み込まれる。

中央政府および地方政府の各機関で文書管理システムの相互運用性を実現するには、以下の活動が必要となる。

・データ交換環境で文書およびデータ転送を保証するための、X-Road の活用。あらゆる文書管理システムに、中央の文書交換拠点とのインタフェースが必要となる。
・文書管理システムにおける、XML ベースの文書説明、および文書編集のメタデータの作成。
・あらゆる公共部門の文書管理システムと一般市民の IT 環境の間で、一般市民や企業家からの申請を受信し、その申請に応答するといった通信能力が必要である。

文書管理システムの相互運用性は、国家事務局とエストニア国立公文書館（National Archives of Estonia）が担当することとなった。

③　文書管理システムの相互運用性

組織間の相互運用性は、以下の原則に基づく。

・相互運用可能な機関は、すべて具体的な技術アーキテクチャを持つ自立した組織である。
・機関どうしの接続は、すべて多元的な合意に基づくものである。可能な限り、2 者間での合意は回避する。
・国家の相互運用性に関する枠組みに参加する、民間部門の団体および非政府系組織は、自らが作成または入手した情報および/またはデータの所有権を持つ。国家情報システムのデータは、国家に所有権が属する。データの構造および内容は、主たるデータ処理者または正式なデータ処理者として個々のデータを管理する組織が、責任を持って管理する。
・データ交換においては、法的な制約や組織の能力を考慮する。
・相互運用可能な機関は、利用者の承認を得た上で情報を交換する。

公共部門の情報システムの相互運用性を確保するために、公共部門がいくつかのインフラストラクチャー・コンポーネントの開発および保守を担当する。これらのコンポーネントの調整は、国家情報システムの調整を担う省庁が担当するが、インフラストラクチャー開発については、原則的に民間部門に外注する。中央のインフラストラクチャー・システムの機能は、国家機関が保証するかまたは民間部門への個別サービスの外注により保証する。公共部門の各機関にとって、データ交換層 X-Road などの中央コンポーネントの利用は必須である。

④　サービス指向アーキテクチャー（SOA）

国家の IT アーキテクチャーの詳細を検討する上で、サービス指向アーキテクチャー（SOA）の原則に従う必要がある。

サービス指向アーキテクチャーの場合、他の情報システムで利用できる、いわゆる「サービス・インタフェース」を通じて、さまざまなシステムから多様な情報サービスを提供する。これらのインタフェースの説明には、サービスの識別や使用に関する十分な情報が記載されていて、サービスを利用するシステムがサービスを提供するシステム内部のアーキテクチャーやプラットフォームなどについて一切「知る」必要がないようにしなければならない。

SOA の場合、サービス公開者と実際のサービス提供者が必ずしも同じでなくてもよいが、サ

ービス利用者の観点から見れば、両者の違いは分からない。

SOA のアプリケーションで使用するテクノロジーに関しては、特に制限はない。

国家の IT アーキテクチャーの基礎となるものは、以下のとおりである。

- 技術的な相互運用性
- セキュリティー
- オープン性
- 柔軟性
- 拡張性

国家機関が効率的に機能し、一般市民が高品質なサービスを受けられるようにするには、高品質情報の可用性が前提となる。情報は、特定のプロセスの過程で特定の出来事が発生した結果として作成され、国家の登録機関や情報システムに保存される。

国家にはさまざまな情報システムおよび登録機関がある。情報社会のある基本原則に従い、国家情報システムで作成された情報は、情報の流れを円滑にするために、許可されたすべての人物が自由に利用できなければならない。一般市民、国家機関、企業家などが、同じように情報を必要とする場合がある。

2.3.1.4　文書交換センターの構築

国家事務局は、エストニアの公共部門の文書管理の発展を調整する公的機関として、文書管理システムの相互運用性を最優先事項の 1 つと考えている。2005 年、国家事務局は、紙ベースのやり取りに終止符を打つ目的の下、省庁間の電子文書交換プロジェクトを立ち上げた。このプロジェクトでは､省庁の文書管理システムがインタフェース接続されるため､相互運用性が確保され、公共部門での紙を使用しない文書交換への段階的な移行の道筋ができる。各省庁のさまざまな文書管理システムは、特別に設計された文書交換センターにより、セキュアなデータ交換環境 X-Road で文書を交換できる。

2005 年初めには、初期の状況を把握するため、各機関の文書登録簿に反映される文書交換に基づく調査が実施された。文書量の分析により、試験運用プロジェクトに参加する省庁を選択する際の基準が確立された。メタデータのマッピングも、メタデータ構成の統一準備となった。この調査では、電子形式の文書構成にもかかわらず、省庁間および省庁管轄の行政機関間のやり取りはまだ主に紙ベースであることがわかった。

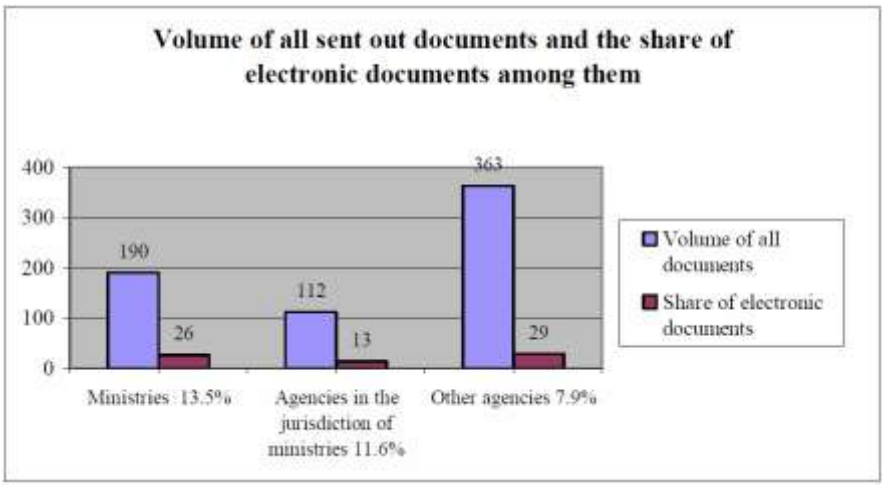


図 2.25：送付された全文書の量とその中での電子文書の割合（文献[231-2]より図を引用）

各機関のメタデータ・コンポーネントの構成を統一し、情報システム間の文書と情報の交換をサポートし、複数の情報システムで詳細な検索を同時に実行できるようにマッピングされたメタデータの要覧が作成された。

要覧の作成にあたっては、メタデータの以下の特徴が考慮された。

・再利用性 － 文書管理のために作成されたメタデータは他の生活分野でも再利用でき、他の活動分野のメタデータ規格に準拠する必要がある。
・多層性 － アーカイブ記述の国際標準によると、文書管理では多層的な記述を使用する。
・モジュール性 － メタデータは文書管理イベント別のグループで表示され、組織によって 1 度に 1 つ使用される場合や、他のメタデータ・スキームと組み合わせて使用される場合がある。

メタデータを用いる場合､すべての組織で一定量のメタデータ･コンポーネントが必須となる。追加メタデータも推奨されるが、文書管理要件によって各組織が導入時に決定できる。

エストニアは、「Estonian IT Architecture and Interoperability Framework」に定められている原則に従い、情報システム間の通信に必要な接続回数を大幅に減少でき、この接続の管理を容易にする多機関間協定に基づくアーキテクチャー実現に向けて前進している。公共部門文書管理システム間のペーパーレス文書交換も同じ原則に基づいている。

2006 年､エストニア情報科学センターは､X-Road での文書管理システム間で XML ベースのセキュアな自動データ交換を可能にする文書交換センターを導入した。

文書交換センターを経由する文書交換を図 2.26 に示す。

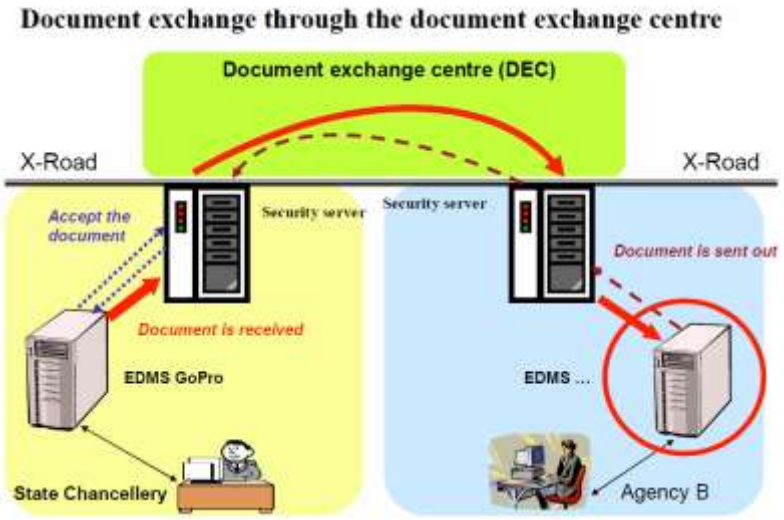


図 2.26：文書交換センターを経由する文書交換（文献[231-2]より図を引用）

(1) 文書交換センター（DEC）

システム間のデジタル文書交換への移行は政府機関の効率を大幅に改善する。文書交換センター（Document Exchange Centre：DEC）は中央情報システムとして、各所に分散する記録管理システムを X-Road を介して結合する。センターの基本的な任務は文書(特にデジタル署名された文書)を転送することである。転送には 3 つのやり方がある。

1) 記録管理システムが用意されている公共機関の場合、その記録管理システムは DEC に接続されており、DEC が他の公共機関の記録管理システムへの文書転送を可能にする。
2) 記録管理システムが公共機関に用意されていない場合、DEC が e メールによって文書を転送する。
3) ユーザーである市民が e メールで文書を DEC に送信し、DEC がその文書を適切な機関へ転送する。公共機関は市民に（直接に、または DEC を介して）e メールで返答する。

将来的には、DEC はレターだけではなく、法律文書、財務文書、インボイスなどの送信にも使われる。

記録管理システムの相互運用性、さらには公共機関間の自動的でセキュアなペーパーレスな文書交換のためには、DEC のサポートに加え、転送された文書とそのメタデータが統一されていることが求められる。このため、DEC を介した記録管理システム間のデジタル文書の交換では、World Wide Web Consortium（W3C）と総理府（文書要素とメタデータに関するガイドライン）が推奨する統一的なデータ構造体である XML（Extensible Markup Language）の文書形式が使われる。文書の内容の統一的なプレゼンテーションを保証するために、公共機関は DEC を介して転送される XML ベースの文書のプレゼンテーション形式を総理府とコーディネートしなければならない。コーディネートされた XML ベースのプレゼンテーション形式をデータベースに使用することによって、統一的なプレゼンテーション形式の再利用が可能になる。

電子記録管理への移行は一朝一夕のプロセスではない。公共機関間の電子文書交換に加えて、公共機関の電子記録管理内部での調整、公共機関の作業プロセスやそれに関連する記録管理プロセスの最適化なども必要になる。記録管理手順のための統一的ベースに関する改定規則には、電子記録管理への移行のためのコーディネーションに向けて省庁と総理府のタスクが設定されてい

る。総理府は公共機関の電子記録管理への移行を計画、組織化し、ガイドラインを作成することになっている。移行をできる限りスムーズにするために、総理府は他の政府機関と協議して、必要なソフトウェアを開発、調達するほか、トレーニングの実施、記録管理のベストプラクティスの導入、記録管理手順の相互調整も行う。

DEC の機能性は文書形式には依存しておらず、文書の種類を制限することもない。将来的には、DEC は以下のオンライン・サービスを提供する予定である。

・文書の手配
・処理サービス
・文書に関する DEC の内部手順
・文書管理機能
・照会および通知サービス;
・システムの管理手順

(2) メタデータの管理

メタデータの管理は記録管理の一部であり、いろいろな機能や目的に関係する。メタデータは構造化された（あるいは部分的に構造化された）情報であり、文書の作成、登録、分類を可能にする。文書へのアクセスや単一ドメイン内での（あるいは複数のドメイン間での）文書の保管と分離もメタデータによって可能になる。メタデータによる文書の定義は、該当の文書を登録して記録管理システムの中に入れ、その文書に対するコントロールを確立したときにはじめて行われる。新しい操作を実行したとき、あるいは何らかの変更を行ったときには、そのときの状態をベースとして新しいメタデータが文書または文書セットに追加される。メタデータは複数のシステムで使用でき、別の目的のために再利用することもできる。文書のライフサイクルの進行中にその文書に関連していたメタデータは現在のタスクでその文書が使われなくなっても必要になることがある。たとえば、将来の分析やその他の目的（たとえばアーカイブ）のために該当の文書が保存される場合である。

上述の規則は、単一の記録管理システム内で複数の公共機関のために同時に記録管理を行うことを見込んでいる。このため、小規模な公共機関は記録管理システムの創出にかかわるリソースを節約できる。記録管理システムはこうしたやり方をサポートし、文書の分類のためのさまざまな自律的システムの使用に備えていなければならない。

(3) 個人情報の管理[231-7]

エストニアでは、個人情報は守るだけでなく、利用についても検討されている。

個人情報は「Personal Data Protection Act（個人情報保護法)」によれば、機微の程度により 3 つのランクに分けられる。(第 1 章第 4 条)

① 氏名、個人 ID 番号

社会的情報であり、利用に制限はない。

② 私的個人情報

1) 家庭生活の詳細を明らかにする情報、

2) 社会扶助または社会福祉の給付申請を示す情報、
3) 個人が被っている精神的または身体的苦痛を示す情報、
4) その他

③ 機密個人情報

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
2) 民族的または人種的起源を示す情報、
3) 健康または障害の状態に関する情報、
4) 遺伝情報に関する情報、
5) 性生活に関する情報、
6) 労働組合の組合員であることに関する情報、
7) その他

個人情報のランクにより、取扱う時の手続きが異なる。

・個人情報の主要処理機関は、私的個人情報を一定の基準に基づき容易に入手できるときは、かかる個人情報の処理について情報保護監察局に通知しなければならない。(第 4 章第 21 条)
・個人情報の主要処理機関は、機密個人情報の処理をおこなう場合、情報保護監察局に登録しなければならない。(第 5 章第 24 条)

なお、本人の同意は、情報主体の生存期間中および情報主体の死亡後 30 年間有効であるものとする。本人が死亡した後は、本人の配偶者、父母、祖父母、子、孫、兄弟姉妹の書面による同意がある場合に限り認められる。(第 2 章、第 12 条、第 13 条)

2.3.1.5 国の情報システム管理システム (RIHA) [231-4]

RIHA は各種公共機関に散在する国の情報システムのコンポーネントを明確に把握し、さらにどのようなコンポーネントが必要なのか、どうすればこれらのコンポーネントの利用を最適化できるかを明らかにすることができる。重要なのは、RIHA の関係者全員 (ターゲットグループ) がそれぞれの役割と責任に応じた機能を理解し、システムの鍵となる目標の実現に貢献することである。

記録の保守管理だけでなく、情報システムのライフ・サイクルで発生するその他すべてのプロセスにおけるメタデータや情報を構成する必要がある。つまり、システム構築のニーズの定義から、その構築の決定、システムの開発、完成、再編成に向けた調達の取りまとめに至るまで、ライフ・サイクル全体を通じて情報を収集するということである。

RIHA では、すべてのオブジェクトを検索できる。X-Road に参加している情報システムや機関は、行政分野 (省庁) ごとに構成されている。RIHA の基本データは、すべての市民がアクセスできるよう公開されている。

(1) 背景および目的

エストニア IT 相互運用フレームワークは、国政情報システムを市民中心かつサービスをベースにしたものにすることを目的とする。情報システムは、全住民とさまざまな組織にサービスを提供する単一の論理的統一体に統合しなければならない。それには、国内の明確なルールと取り決

めに合意する必要がある。

論理的統一体としての国政情報システムを開発するには、国内の既存情報システムとデータベースを1カ所で概観する必要がある。すなわち、あらゆる国政情報システムとそれらが提供するサービスについてのメタデータを備えることが重要である。そのような概観が可能になるように、現在、国政情報システム管理システム（RIHA）が開発されている。このシステムの目的は、あらゆる国政情報システム、その管理者とサービス提供者、サービス、サービス利用者、分類、および分類管理者に関するメタデータを収集することである。

エストニアでは、データベースの構築とメンテナンスがデータベース法（Public Information Act）によって規制されている。情報システムの管理者は、この法律に従ってデータベースと情報システムをRIHAに登録するとともに、提出したメタデータを確実に更新することが義務付けられている。

RIHAの機能は、システムが国政情報システムの全体を表し、国のIT資源の最新状況を概観できるように拡張される。これは、国のさまざまな機関が持つ国政情報システムの既存の構成要素、今後さらに必要な構成要素、利用可能な資源、およびそれらの最適利用の可能性を1カ所で概観するための唯一の方法である。

(2) RIHAのターゲット・グループ

RIHAのターゲット・グループが、自らの役割／責任に応じた展望を持ち、システムの主なオブジェクトが統一的に取り扱われるのを保証することが重要である。

RIHAは、情報システムの管理者と国のIT調整に責任を負う人々の両方が使用するツールになる。情報システムの管理者は、他の機関の情報システムとサービスに関する情報のほか、必要な連絡窓口の情報もRIHAから入手できる。そのため、新たなサービスを作り出したり、既存サービスを広げたりする提案ができるようになる。

RIHAは以下のターゲットグループのためのツールとなる。

1) 政府機関の情報システムの管理者およびメンテナンス責任者。
2) 国の情報システムが提供するサービスの利用者。
3) 情報システムに使用されている分類の管理者およびメンテナンス責任者。
4) 国の情報システムに関する情報の受け手となる私法上の法人と個人。
5) 国の情報システムの調整機関としての経済通信省。
6) 国の情報システムの中央での管理者およびメンテナンス責任者としての経済通信省。
7) 統計データの収集責任者および分類方法作成コーディネータとしての経済通信省。
8) 個人情報保護の監督機関としてのデータ保護検査庁。
9) エストニア社会に関する情報の保存と利用に責任を持つ国立アーカイブ。
10) 政府機関の職員のツールとなる国の情報システムのサービスデスクおよびエストニア情報科学センターのサービスデスクのスタッフ。

国政情報システムの調整に責任を負う人々は、RIHAを通してモニターできる各種情報システムのユーザー統計とデータ・フローによって、国政情報システムの相互運用性を確保するためのシステムの開発と資金調達要件に関する意思決定を行うことができる。また、あるシステムが国の

IT 要件に適合しているかどうかをチェックして、必要に応じて関連するコメントと提案を情報システム管理者に示すことができる。

さらに、RIHA は以下の公共団体のためのツールになる。

- データ保護検査官室（個人情報を処理する情報システムの監督に関連）
- エストニア統計局（分類システムと統計調査の仕様との調整に関連）
- エストニア公文書館（保存する価値がある対象の決定に関連）

その上、RIHA はサービス利用者にとって重要な情報源になり、サービス利用者は国政情報システムを概観し、どのサービスが利用者に開放されているかを調べ、新たなサービスの作成を提案できるようになる。

(3) RIHA の主要なオブジェクトとそれらの間のリンク

RIHA の主要なオブジェクトには以下が含まれる。

① 組織に関して

RIHA には、組織の役割に関する一般的なデータと情報が含まれる。組織は、情報システムの管理者として、自らが管理する情報システムとリンクされているからである。管理している情報システムを通してサービスを提供する場合、組織はサービス提供者の役割も持つ。さらに、組織が他の情報システムのサービスを利用する場合は、サービス利用者の役割を持つ。

組織が分類体系の要件に従って分類を定め、それを他の組織が利用できるようにしている場合、その組織は分類管理者としても機能することがある。

② 情報システムに関して

RIHA には、その法的根拠、ドメイン、データ構成（システムの基本データを含む）、データのセキュリティー・クラス、情報システムと X-Road の結合に関するデータ、システムのアーキテクチャーとデータ取得プロセスに関するデータなどの一般的なデータが含まれる。

③ サービスに関して

RIHA には以下のデータが含まれる。X-Road サービスが WSDL フォーマット（入力と出力の記述）で記述されている場合はサービス記述、サービス提供方針（どのような原則に基づいて、誰に対して、どのような目的でサービスを提供するか）、およびサービスの品質指標（サービスの可用性、信頼性、効率、セキュリティー・クラスなど）。サービスは、それを提供する情報システムを通してサービス提供者およびサービス利用者とリンクされている。

④ 分類に関して

RIHA には、分類のメタデータと分類自体が XML ファイルの形で含まれている。その代わりに、システムが分類管理者の環境へのリンクを持ってもよい。その場合、分類は XML ファイルとしてダウンロードできる。

情報システムとサービスのセマンティック記述は、その概要記述の重要な構成要素になっている。セマンティック記述を生成するには、オントロジー（特定のドメインの用語を定義し、それらの間のタクソノミー（関連が階層構造で表される分類）を示す辞書）を作成する必要がある。

用語の記述は、人間が読めるフォーマット（HTML および XMI スキーマ）と機械可読フォーマット（OWL および XMI スキーマ）の両方で示さなければならない。

2.3.1.6　eNotary - 公証人のための情報システム[231-2][231-3]

情報システム eNotary（e 公証人）は公証証書を作成するためのコンピュータソフトウェアであるが、同時にデジタルアーカイブの土台ともなり、契約作成に必要なデータの取得と入力に際して公証人を助ける他の登録レジスタとのやり取りも可能にする。たとえば、個人の ID コード（または名前）を契約当事者詳細情報のボックスに入力すると、eNotary が住民登録レジスタのデータの中からその個人を見つけ出し、他の空白ボックス（名前、居住地、ID ドキュメントのデータ、婚姻の有無）を自動的に埋めてくれる。登録された不動産番号を入力すれば、eNotary は電子的な土地レジスタ（Land Register）に基づいて該当の不動産に関する他の情報（住所、エリア、所有者、負担やその他の制限、進行中の申請手続き）を探し出し、表示する。さらに地籍局（Land Cadastre）の Web サイトから該当の不動産の地図を見つけ出し、追加できるようにする（地籍局の Web サイトは文化保護や自然保護を理由として当該不動産に課せられている制御の情報も収めている）。当該土地の利用目的に関するデータも見つかる。商業登記所（Commercial Register）の情報に基づいて商業禁止区域になっていないかどうかチェックし、代理権を調べることもできる。

公証人は eNotary システムの一定の機能の使用を義務づけられている。現在のところ必須となっているのは、公証行為や供託金の eNotary への登録のほか、申請、契約、情報をレジスタに送る際に eNotary を使用することなどである。次のステップとして、保存しなければならないドキュメントをすべてデジタル公証アーカイブに保管することも義務づけられる予定である。

(1) eNotary の機能

- 契約当事者や契約対象に関するデータを他のレジスタから見つけ出す。
- 公証人の日程表を保管する。
- 公証行為を登録する。
- 公証証書の作成を助ける。
- 公証人料金と国庫料金の計算を助ける。
- 公証人料金請求書と国庫への支払い要求書を作成する。
- 公証人に供託された金額の勘定の管理を助ける。
- 契約に関するデータを他の国家レジスタに送信する。
- 契約を関連データと一緒にデジタル公証アーカイブに保存する。
- 公証統計を作成する。
- 公証人の会計士を助ける。

(2) eNotary の仕組み

契約のテンプレートは情報システムに用意されており、必要な情報はマウスを数回クリックするだけで別のレジスタから手に入れることができる。契約への署名が完了したら、公証人はデジタル署名された契約書のコピーを作成し、デジタルアーカイブに保存する。契約書のデジタルコピーはアーカイブだけに保存されるわけではない。デジタルアーカイブに保存された契約あるいはその契約の一部のデータは eNotary によって電子的に他の関係する登録レジスタ（土地登記所、登録局、遺言レジスタ）に転送される。契約のデジタルコピーは先買権などを持つ政府機関に転

送されることもある。

土地登記所（land registry department）の作業もずっと簡単になった。情報は土地登録情報システムのそれぞれ適切な場所に自動的に入力されるため、紙の書類からコンピュータに入力する必要はなくなった。紙の登録簿はなくなった。契約の登録に関する質問への回答は土地登記所や登録局から電子的に返される。データはいろいろな部門でクロスして使われ、他の政府機関でも作業プロセスの効率がアップする。

今日では、登録申請の 100%が電子形式で転送されている。

(3) 経緯

eNotary プロジェクトは 2004 年に始まった。プロジェクトを委託したのは公証人会議所（Chamber of Notaries）であり、実行したのは登録情報システムセンター（Centre of Registers and Information Systems：RIK）である。プロジェクトは 3 つの関係組織から編成され、コーディネーションと監督は司法省に任された。3 組織からなる運営グループに加え、作業グループも創設された。作業グループは、司法省と RIK の代表者に加え、いくつかの公証人オフィスの公証人やその他のスタッフから構成された。作業グループはシステムの機能を決定し、開発の過程で発生する問題を解決する。プロジェクトを成功させたのは、作業グループの熱意と責任感だといえる。プロジェクトの推進にとって、たえまないフィードバックと提案、その迅速な実現は不可欠の要素だった。

(4) eNotary の利点

プロジェクトの関係者たちは、シンプルに、スピーディに、効率的に作業を進めるという共通の目標に向かって力を合わせた。公証人が望んでいたのは、国の登録レジスタや情報システムからいわゆる単一のコンタクトポイントを通じてできるだけ速く、できるだけ簡単に情報を取得することだった。(土地登記所、商業登記所の登記部門、行政と立法政策にかかわるその他の機関を管轄している）司法省は、紙の書類による申請をデジタル化し、登記のビジネスプロセスを効率化することを望んでいた。RIK は司法省の管轄下にある IT システムの開発と管理を担当しており、登録レジスタをより効率的に、よりシンプルに、よりセキュアに、よりイノベーティブにすることを望んでいた。

これらの関係者の協力の結果、eNotary システムが完成し、土地登記所や商業登記所などの司法庁の情報システムへのインタフェースが確立された。司法省管轄の情報システムにとどまらず、eNotary は環境省やその他の省のデータベースにもつながっている。

公証人のもとで契約書を作成しようとしている人物がほんとうにその人物なのか。公証人に提出されたパスポートは本物か。偽造パスポートではないのか。無効のパスポートや盗まれたパスポートではないのか。eNotary を使えば、こうしたことをごく簡単にチェックできる。カスタマのパスポートの有効性、パスポートの写真、署名のサンプルはすべて直接に市民権・移民庁（Citizenship and Migration Board）と住民登録レジスタ（Population Register）から入手できる。これらをカスタマの顔やカスタマが提出したドキュメントと照合することによって、偽造パスポートの利用やその他の不正行為は非常に難しくなる。不動産を購入したくても、売り手の側に悪意がないとも限らない。別の公証人オフィスですでにその物件を売却しているかもしれな

い。幸い、公証人には eNotary という強力な武器がある。eNotary を使えば、不動産売買の契約を結ぶ前に土地登記を調べて、該当の物件の売買があったかどうかをほぼリアルタイムでチェックできる。

2.3.1.7　セマンチックの相互運用性の定義[231-5]

セマンティックの相互運用性とは、ある情報システムが別の情報システムから受信したデータを十分に利用できる機能のことをいう。セマンティックの相互運用性は、ソフトウェア・システムの使用方法、使用目的、および背景が異なれば、表現やコーディング方法、意味合いなども異なるため、理解するのが難しい。

セマンティックの相互運用性は、すべてのソフトウェア・システムで同様の要件や標準を確立することでは実現できない。なぜなら、そのような要件や標準を確立するのは非現実的で合理性を欠くからである。セマンティックの相互運用性の実現は、他のソフトウェア・システムとのインタフェースを構築しなければならないソフトウェア・エンジニアおよび開発者の仕事を容易にする作業として取り組む必要がある。

セマンティックの相互運用性の実現は、かなり組織的、社会的、教育的な性質の問題である。まず、互いの活動分野に対する理解を深め、データ構造やプロトコルに関する適切な文書を作成し､そのような文書の検索を容易にするために､システム専門家に対するサポートが必要である。

これらの文書に保存されたデータを公開するために、情報システムでは、言語や辞書、分類、規則から複雑なオントロジーに至るまで、さまざまなツールを利用する。情報システムのソフトウェアおよびハードウェアと同様、それらのセマンティック・アセットについても触れる必要がある。

(1) セマンティックの相互運用性アセット

セマンティックの相互運用性アセットは、シンタクティック・アセットとセマンティック・アセットに大別される。2 つの情報システム間におけるセマンティックの相互運用性を確保するには、それらの間にセマンティック・ゲートウェイが必要となる。セマンティック・ゲートウェイでは、セマンティックの変更により、情報システム間で互いのデータを十分に利用できるようにする必要がある。国家情報システムのセマンティック・ゲートウェイは、セマンティック・レベルでのシステムの相互接続を容易にするための、一連の多元的な合意および規則である。

シンタクティック相互運用性アセットには、XML スキーマ、メタデータ・スキーマ、コア・コンポーネントなどがある。データ・スキーマの発行およびメタデータの定義に関する原則は、国家レベルで規定する必要がある。シンタクティック・レベルの相互運用性は、セマンティックの相互運用性を実現するための第一歩であり、XML スキーマのリポジトリーを作成することで実現できる。

セマンティックの相互運用性におけるセマンティック・アセットは、情報システムの相互運用性を保証するために作成された情報リソースを表す。セマンティックの相互運用性におけるセマンティック・アセットは、以下のとおり分類される（この分類は、IDABC 作業文書「IDABC Content Interoperability Strategy（コンテンツの相互運用性に関する戦略)」に基づくものである)。

- 一般辞書

- 類語辞書
- 用語辞書
- 分類辞書
- マッピング・テーブル
- オントロジー
- サービス・レジスター

(2) セマンティックの相互運用性保証を担う組織

セマンティックの相互運用性は、主にデータベース、サービス、アプリケーション、領域などの高品質の文書化にかかっている。セマンティックの相互運用性を確保する組織の主な目的は、このような文書の開発および定期的な更新を調整することである。標準、一般辞書、類語辞書、用語辞書などを工夫することで、セマンティックの相互運用性を改善できる。同時に、法律でこれらのセマンティック・アセットへの参照を行うことができる。更に、必要に応じてそのような参照の利用を義務付けることも可能である。

国家情報システムのセマンティックの相互運用性保証を担う組織の発展は、以下の原則に従って行う。

- 中央の調整者の役割はエストニア経済通信省の国家情報システム局に任命し、そのスタッフにセマンティックの相互運用性設計者を含める必要がある。
- あらゆる主要分野において、各部門の文書の作成、更新および変更の作業を行う専門家グループを形成する必要がある。これらの主要分野は、程度の差はあれ省庁の行政分野と一致するため、あらゆる省庁の専門家グループを設立し、これらのグループに個々の辞書関連文書の編集と保守の作業を任命するのが得策である。
- セマンティックの相互運用性を実現するのに相互の合意のみでは不十分な場合は、部門間の作業グループを立ち上げる必要がある。このようなグループの目的は、ある分野のデータ・オブジェクトを別の分野のデータ･オブジェクトに変換/修正するための手順を作成および保守管理することである。
- 国際的な舞台では、セマンティックの相互運用性に関する IDABC 作業グループの作業にエストニアが参加するのが望ましい。この作業グループの目的は、各国の情報システム間におけるセマンティックの相互運用性のための 2 者間合意とセマンティック・ゲートウェイを確立することである。他国の情報システムとの接続を確立するためのプロジェクトを実現するには、両当事者を代表する 2 国間の専門家グループを設立する。

(3) セマンティックの相互運用性に関するアーキテクチャーの要件

システム･アーキテクチャーを計画する際､セマンティックの相互運用性を容易にするために、以下のガイドラインを考慮する必要がある。

- データ交換には、HTTP または HTTPS プロトコル経由の XML 形式を採用する。
- 使用する XML 形式は分かりやすいものとし、不要なタグや詳細事項などの煩わしいデータを含まないものとする。
- 使用する XML 形式を、開発者に理解しやすいように文書化する必要がある。

- XMLテキストによりメイン･アプリケーションと通信し､ユーザーに必要なHTMLを生成する、あるいは（WAP、SMS、デスクトップ・ソリューションなど）その他何らかの方法でインタフェースを実現する、独立したアプリケーションとして、プレゼンテーション層を構築する必要がある。
- メイン･アプリケーションの適応可能なセマンティクスをサポートしないHTMLテキストを直接生成することは避ける必要がある。

セマンティック相互運用性の実現はかなりの程度まで組織、社会、教育の側面に関係する。まずさまざまな分野のシステムスペシャリストをサポートすることを通じて、異なる分野の活動の相互理解を促進し、データ構造とプロトコルのドキュメンテーションの編集につなげ、さらにこうしたドキュメンテーションの検索を容易にする。情報システムに保存されている知識のパブリッシングに使われるツールはシステムによって異なる。言語、辞書、分類法から複雑なオントロジーに至るまで、ツールは一様ではない。

2.3.1.8　セマンティック的相互運用性のアーキテクチャ

セマンティック的相互運用性 - 交換されるデータを同様に理解し、その適切な使用を行う - は、データベース内における、データのセマンティック的記述のためのシステムと、要求されるオペレーションにおいて使用される入出力データを必要とする。このようなシステムのアーキテクチャは、以下の原則を基礎とする。

(1) 再使用の原則 - あるデータ要素またはオペレーションは一度だけの記述を行い､他のいかなる使用においても元の記述を参照する。
(2) データ要素／オペレーションの、シンプルで標準的な編集、管理、検索。

セマンティック的相互運用性のアーキテクチャは、以下のコンポーネントが構成する（下図参照)。
(1) ドメイン･グロッサリー - データ要素とオペレーションのセマンティクスの中央記述。記述は､「土地調査」などのドメインに分類されている。セマンティック的記述には、言語としてOWLを使用する。記述は、国家情報システム（RIHA）の管理システムに格納する。
(2) データベースとオペレーションのセマンティック的記述 - 一つ一つのデータベースまたはオペレーションと、そのコンポーネント、および存在する場合に、ドメイン・グロッサリー内のそれぞれのエントリへの参照を含む。記述には、言語としてWSDL、SA-WSDLなどを使用する。記述は、国家情報システム（RIHA）の管理システムに格納する。

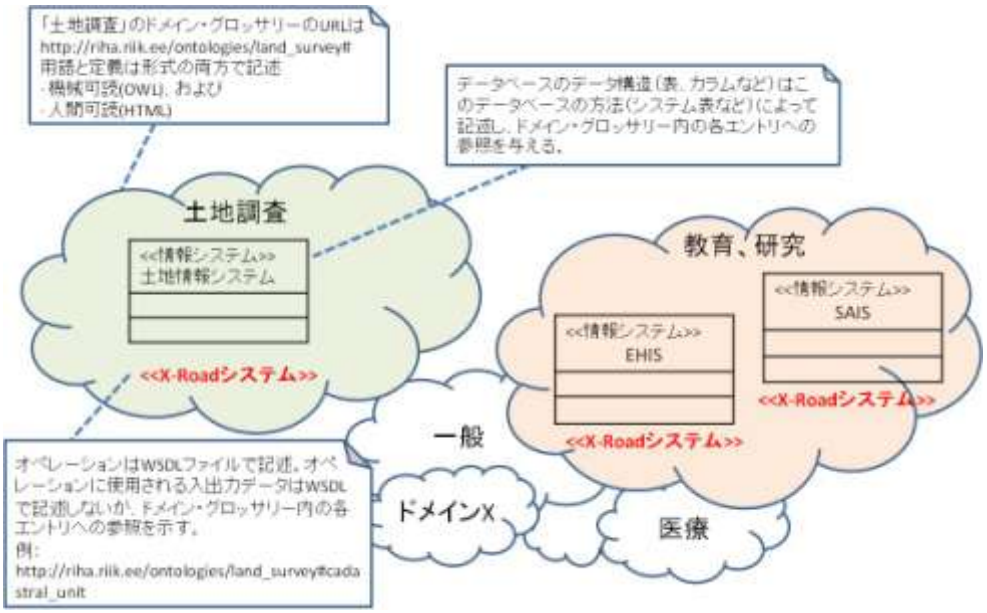


図 2.27：セマンティック的相互運用性のアーキテクチャ（文献[231-5]より図を引用）

ウェブサービスおよびドメイン・グロッサリーの記述場所の候補：

(1) 分散アーキテクチャ - 各データベースごと
(2) 集中型アーキテクチャ

記述を含めて各オペレーションが唯一であるべきと仮定すると、オペレーションをそれぞれのデータベースとともに WSDL ファイルで記述するとともに、容易なアクセスのためデータを集中的に格納することは合理的である。ドメインの用語は、集中的に記述するべきである。データベースの記述と、オペレーションの入出力データ要素は、中央グロッサリーへの参照を含む必要がある。

セマンティック的記述は、以下の情報リソースのために必要である。:

・情報サービス
・データベース

もうひとつの考慮は、メタデータを情報リソース内に格納する（WSDL はセマンティック的記述を含む）か、またはその外か（あるデータベース・フィールドのセマンティック的記述はドメイン・グロッサリー内に置き、記述されるリソースはメタデータ・エントリへのリンクを含み、その逆はない）の問題である。一般に回帰性の記述（通常はデータ要素）をリソース外（ドメイン・グロッサリー内）に格納し、また、オペレーションが一般的に唯一と仮定すれば、オペレーション関連の記述をリソース内に格納することが推奨される。

記述を情報リソースの外に格納することは、さらなる作業 - リポジトリの構築と維持、記述者の動機付けと監督 - を必要とする。リポジトリの構築について詳しくは、ISO/IEC11179 標準を参照。その一方で、記述はどこでも入手可能になり、より多くの監督者が求められるために、このアプローチでは記述者の意欲が増すことが考えられる。

2.3.1.9　セマンティック的記述の一般的な編集／公開プロセス

図 2.28「セマンティック的記述の一般的な編集／公開プロセス」は、一般的記述を編集および公開する業務プロセスの一般的な概要を、UML アクティビティ図で示している。コメントには前提条件と事後条件が含まれる。

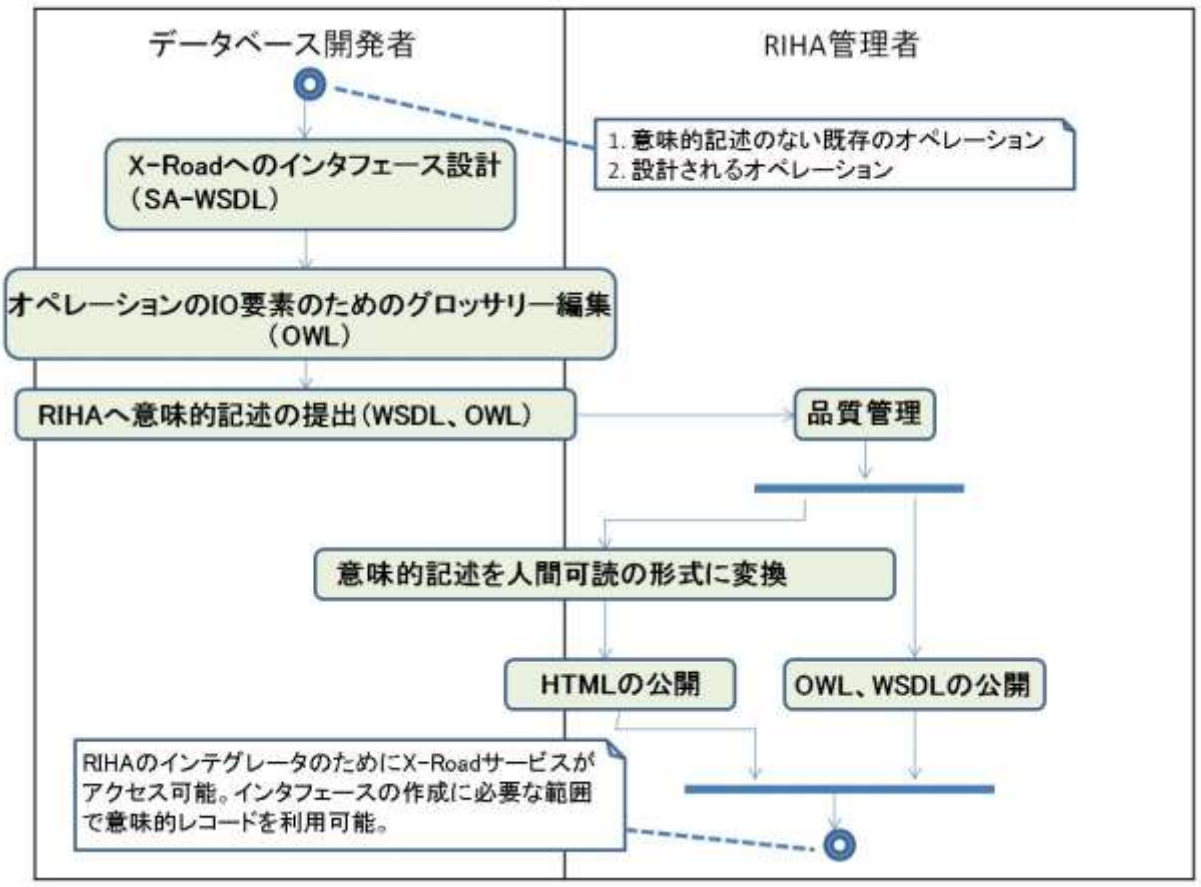


図 2.28：セマンティック的記述の一般的な編集／公開プロセス（文献[231-5]より図を引用）

[参考文献]

[231-1]「IT 立国エストニア――バルトの新しい風」前田／内田　2008 年 10 月　慧文社

[231-2] Information Technology in Public Administration of Estonian yearbook 2005, Ministry of Economic Affairs and Communications, 2006

[231-3] Information Technology in Public Administration of Estonian yearbook 2007, Ministry of Economic Affairs and Communications, 2008

[231-4] "Administration system for the state information system" http://www.ria.ee/27313

[231-5] "Methodology for the Semantic Interoperability of Databases and Operations Performed by Databases", Ministry of Economic Affairs and Communications Department of State Information Systems Version 1.2　2007-04-08

[231-6] Estonian Interoperability Framework, Ministry of Economic Affairs and Communications, 2006

[231-7] Personal Data Protection Act, 1996

2.3.2 英国

記録管理には幾つかの流儀がある。本調査では、英国における記録管理の慣行、電子記録の保管方針、業務分類とケースファイルの関係、電子環境における評価選別並びに最終処分の方法などについて文献調査を実施するとともに、英国における関連用語の定義と標準についてまとめた。

本文献調査は主として、英国公文書館から発行さている次の実施要領を中心に実施した。これらの文献は、行政機関を対象としたものであるが、適切に用語を読み替えることにより民間での記録管理にもおおいに参考となるものである。

- デジタル記録の保管方針（Custodial policy for digital records）
- 入手及び最終処分方針（Acquisition and Disposition Strategy）
- 業務分類体系の設計（Business classification scheme design）
- 記録の選択に関する一般ガイドライン（General guidelines for the selection of records）
- 最終処分スケジュール（Disposal scheduling）
- 評価選別方針（Appraisal policy）
- 2000年情報自由法第46条に基づいて公開される記録の管理に関する大法官の実施要領(Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of information Act 2000)

2.3.2.1 英国の基本情報

英国（正式な国名は、グレートブリテン及び北アイルランド連合王国（United kingdom of great Britain and Northern Ireland）は、人口6179万人で日本の1/2、国土は、24万2千km^2で日本の2/3である。首都はロンドンで、人口は775万人である。労働人口は2916万人で、うち13%が外国人労働者である。民間部門労働者数は約2300万人、公共部門が約600万人である。失業者総数245万人で労働人口の8.4%が失業中である。一人当たりGDPは40,832ドル、名目GDPは2兆1,731億ドル、成長率は-4.9%（2009年）である。

英国では、インターネットやブロードバンドサービスはほとんどADSLかケーブルによって提供されており、光ファイバは普及していないという特徴がある。端末販売ショップ大手の「カーフォン・ウェアハウス」や、サッカーのプレミア・リーグを独占的に放送している有料衛星放送事業者の「BSkyB」等も、「BT」の回線を借りてブロードバンドサービスを提供しており、ブロードバンドサービスの加入者は年々増加、料金も年々低下している（図2.29参照）。

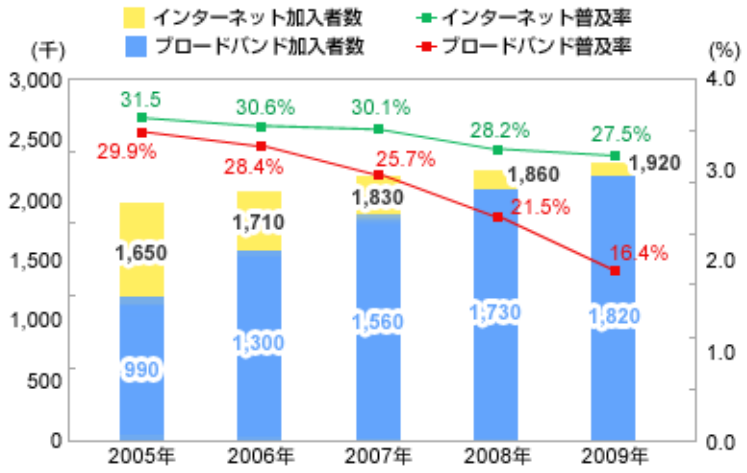


図 2.29：英国のブロードバンドおよびインターネット加入者数数（総務省 HP より引用）

2.3.2.2　推奨される記録管理の慣行

「2000 年情報自由法第 46 条に基づいて公開される記録の管理に関する大法官の実施要領」（以降、記録管理の実施要領という）では、記録と情報の管理が不完全であると、公的機関に次のようなリスクが発生するとしている。

- 情報が不正確または不完全なため、決定基盤が揺らぐ。
- サービスに一貫性がなくなり、水準が低下する。
- 証拠として要求される情報が利用できなかったり、信頼できるものではない場合、財務上または法律上の損失が発生する。
- 法的要件やその他の規制要件、所属する部門に適用される基準を満たすことができなくなる。
- 機密情報を適切なセキュリティ水準で処理することができず、不正なアクセスや最終処分を許す可能性がある。
- 組織の業務継続にとって重要な情報を保護できず、業務継続の計画が不適切になる。
- 必要以上に長期にわたって記録とその他の情報を保管することにより、無駄な費用が発生する。
- 記録を探すのに時間がかかる。
- 以前に対処して解決した問題をもう一度検討しなければならなくなり、時間が無駄になる。
- 上記のすべての結果として、国民の信頼を裏切り、機関の信頼性を落とす。

記録管理の実施要領では、また、公共機関に推奨される正しい慣行について、次のように記されている。

① 記録管理をサポートする組織上の取り決めを適切に用意しなければならない。
② 記録管理方針を個別の方針としてか、より広範な情報管理方針または知識管理方針の一部として、正しく設定しなければならない
① 業務上、規制上、法律上、責任上の目的に必要となる記録を維持することを保証しなければならない
② 必要に応じて記録の保管と検索ができるシステムに記録を維持しなければならない

③ 保管する記録の種類と保管場所を把握し、記録が要求される限り利用できることを保証しなければならない。
④ 記録が安全に保管され、記録へのアクセスが管理されていることを保証しなければならない
⑤ 特定の記録を維持するのに必要な期間を定め、記録がそれ以上必要なくなるときに最終処分し、記録をそれ以上維持しない理由を説明できなければならない
⑥ 他の機関と共有する記録、または他の機関が代わって保存する記録が、要領に基づいて管理されることを保証しなければならない
⑦ 要領の遵守を監視し、記録管理プログラムの全体的な有効性を評価しなければならない

2.3.2.3 電子記録の保管方針

(1) 背景

デジタル環境では、多くの記録に対して業務上の必要性が急速に低下するため、記録の保存が課題となる。アーカイブ目的を含めた記録の二次的目的を従来形式の記録の場合よりも早い時期に識別することが必要である。さらに、後の業務で記録を使用するかどうかは、適切な記録の同様の識別に左右される。このことは、主に最終処分スケジュールを通して実施される組織の記録管理方針にとって重要になる。

紙の記録は基本的な特定の環境条件が満たされれば長期にわたって保存できるが、デジタル記録を利用可能に保つには積極的な関与が必要になる。メディアは致命的な劣化を被る前に刷新が必要であり、オブジェクトの論理形式は、さらに新しい形式かオープンな形式に移行させる必要もある。個人が保存するか共有作業スペースに保存される記録を、組織の方針に基づいて有効に保つ必要もある。

デジタル記録の保存は比較的安価で、その費用はますます低下しているが、長期間の管理は積極的な操作が必要なため高くつくように思われる。だからと言ってもはや紙を選択する理由にはならない英国に於いては、大量の紙の記録の最終処分は 25 年目に評価を受けるまで保留されるが、デジタル記録ではこれは選択されない。「電子記録の保管方針」では、公文書機関が長期的な業務目的と、公文書法およびその他の法律に定められた義務の両方を果たすことを確実にするために、デジタル記録を維持する責任を明確にすることによって、この問題に対処しようとしている。

また、「評価選別方針」では、デジタル記録を作成した時点かその直後に永久保存するかどうかを識別する必要性は、こうした記録を早い時期にアーカイブに移行する可能性を生み出すと述べている。

公文書法 3 条と情報自由法 46 条のいずれも、記録の最終処分の適切な管理を要求している。これは、業務上の正しい慣行の主要目的でもある。

(a) 公文書法 3 条

ここには次のように書かれている。このセクションに従って実施される調整に基づき、永久保存の必要がないと評価された公文書は廃棄されなければならない。または、大法官以外の人物が記録の責任者である場合は、その他のどのような方法で処分するにも大法官の承認を必要とする。

(b) 情報自由法 46 条

ここには論議を次のように発展させている。

① 情報の自由（FOI）の下では、記録の最終処分及び記録のライフサイクルにおいてアーカイブに移管される時点か廃棄される時点としてここでは定義される － は､政府機関によって正式に採用された、適切な権限のある職員によって実施される明確な方針に基づいて行われる。

② 最終処分待ちで完結した（closed）記録の保管は、環境、安全性、物理的構成に関して認められた標準に従わなければならない。

③ 各機関は、記録を永久保存に選択するような職務と、他の記録を保持しなければならない期間を概略的に示す選択方針を維持しなければならない。選択方針は、電子記録を含めたすべての記録をカバーする最終処分スケジュールの裏打ちまたは関連づけを必要とする。最終処分スケジュールは、連続または収集に基づいて調整され、すべての記録に対して、たとえば、x 年後に評価、y 年後に廃棄など、適切な最終処分行為を示さなければならない。

④ 機関によって永久保存に選択され、もはや定期的に使用されない記録は、適切な保管設備とパブリック・アクセス施設を備えたアーカイブ機関にできる限り早く移管されなければならない。

⑤ 永久保存に選択されず、管理上のライフサイクルの終点に達した記録は、その記録に記された機密性または安全性のレベルに必要な方法と同じ確実な方法で廃棄されなければならない。記録の廃棄に関する参照、説明、日付を示す記録は、記録管理者が維持して保管しなければならない。最終処分スケジュールは、こうした記録の基礎を構成するものとなろう。

(2) 早期評価選別の役割

評価選別による記録の価値は､今までは作成から 5～10 年目と 25 年目にファイルごとに行う評価に関連して判断されてきた。評価選別方針では、この方法はデジタル記録には不適切であり、デジタル環境ではアーカイブの選択を含め、一般の政府機関が通知する記録価値にもっと幅広いアプローチが必要であると述べている。具体的には、マクロ選別は、業務またはアーカイブ目的で記録の価値を識別するガイドとして、政府全体または組織全体で職務を分析することを奨励する。その理由は、最も重要な職務で作成される記録を識別することにより、ファイルごとの精査の必要性や時間経過による“歴史的視点”なしに評価選別を決定する手段が提供されるからであるとしている。ガイダンスを示す最終処分スケジュールの作成と業務分類体系の設計も、評価選別のこの幅広い観点を採用している。

このことは、評価は今までより早い時期に行わなければならず、できるだけ部局の最終処分スケジュールに組み入れなければならないことを意味する。記録が作成される時点の適切な最終処分スケジュール並びに適切な命名および分類手順を規定するガイドラインによって、できる限り多くの記録がカバーされなければならない。

2.3.2.4　ケースファイルに固有の課題

(1) ケースとは

ケースとは、「ある事項（事実、状況など）の発生または存在のインスタンスまたは事例」のことであり、この一般的な辞書的定義は、英国中央政府の記録管理/アーカイブ環境に関する従来の理解の検証を支援するために役立ってきた。これまで、記録は政策の実施の日常的なインスタンスよりもアーカイブとして重要かつ貴重であるとみなされ、公共政策の策定に関するケースと記録は明確に区別されてきた。

(a) ケースファイルに対する職務アプローチの影響

これをうまく説明するために、ケースの定義は、アーカイブの問題としてではなく、記録のライフサイクル（作成組織における記録の作成と編成）のアクティブな業務フェーズに基づいた定義に変える必要がある。

ケースワーク組織は、ケースファイルを使用して、何らかの側面に関して同じサブジェクト（記者、患者、被告、または被害者など）を有するトランザクションの要素またはトランザクションのグループを統合する。ケースファイルの内容が、さまざまな活動および/または職務に属することがある場合、これによって機能アプローチとのパラダイムの衝突が生じる。この問題に関しては、いくつかの一般的な誤解があった。

(b) 衝突の解決

職務アプローチの非常に厳格な解釈の 1 つでは、BCS は、電子環境で従来のケースファイルを重複させる可能性がある。

紙の環境では、(特に上位レベルで)長年にわたり職務ベースの BCS が存在していた。しかし、便宜上、同じ個人、組織などに関連するトランザクションを含む記録は、まとめて保管された。事実上、記録には、政府が扱っているエンティティの ID によって、独自に索引が付けられた。（特に、カスタマーインタフェースでサービスのレベルを管理する必要性の観点で）この利点は非常に大きく、無視することはできなかった。

最終的に、電子環境での論理的結論は、このようなシナリオにおける記録が（紙の環境で実現可能であった解釈よりも厳格な活動およびトランザクションタイプの解釈に従って）個別の場所に属し、個々の項目間の共通メタデータリンクからなる代替的なケース「ビュー」によって結合されるというものである（現在では、これが可能である)。これは、前述したように、電子環境では、同じ情報の複数のビューをサポートできるためである。

(c) 「仮想ケースファイル」の入力

「仮想ケースファイル」は、主要な BCS ビューとは異なるアセンブリ内で、他の記録に対するメタデータ全体またはポインタ/制御コピーから構成される。評価/処分/アクセス制御およびその他の記録管理プロセスを確実に一貫して実行するために、BCS からケースファイルに職務をマッピングすることにより、職務アプローチを使用することができる。従来のワークフロー・プロセスを設計し直して、新しいプロセスからの記録が記録の職務上の分類およびこの種類のメタデータの収集に基づいて形成されるように、ケースファイルの作成を回避することもできる。

これは、純粋な職務アプローチであり、すべての業務環境におけるすべての利害関係者にと

って魅力的ではないことがある。

(d) 問題は何か

特定の問題は、ケースワーカー、作成組織のその他の者、またはおそらく住民が記録の「配置」(アーカイブに関する用語では、この代わりに、記録の「アセンブリ」または構造が使用される。) を簡単には理解できないによって発生する。

これらの問題は克服できないものではないが、システム設計と変更管理に関する要求が高くなる。これらの問題に対処できる場合は、大量のトランザクションシステムおよび評価/処分に対するその他の分野で、著しい利益が生じる。

(2) ケースワークシステムの業務分類スキーム

BCS 内のトランザクション資料の主要な構造化原則としてケースを保持することを決定した民間団体では、計画段階で対処する必要がある重要な課題がいくつか生じる。

(a) レベルの数および自己索引記録

通常、ケースには、ほとんどの目的のために最適であり、EDRMS の直接環境の外部で生成される識別子 (「ID」) が割り当てられている。これは、ペーパー環境での組織の業務ニーズに適合させるために発展した。以下に ID の例を示す。

・EDRM 環境とさまざまなレベルで統合されたケース管理アプリケーションからの ID
・住民の個人名
・企業の登記簿など、権限のある情報源からの組織名または参照番号
・フォルダ命名の構造化要素としてのケース ID (またはその他)

ケースはいくつかのわずかに異なるトランザクションから構成される可能性も高いことを考慮に入れると、ケースには、これらの記録を分類するために、おそらく BCS と同数のレベルは不要である。

(b) その他の分類の問題

BS ISO 15489 は、すべての記録を BCS 内に配置することを要求している。これにより、ケースファイルが分類スキームの「下位」領域内に (ほとんどの業務の目的のために自己索引を利用できるため、比較的少数のレベルで) 存在する可能性がある場合でも、その領域自体は分類スキーム内に配置されることが要求される。

(c) 職務構造内のケースファイル

職務原則に基づいて構築された BCS 内に従来のケースファイルに相当する電子記録を適合させることは可能である。しかし、厳格に言えば、このスキームはおそらくハイブリッド構造である。この最も一般的なタイプは、上位レベルでは職務アプローチを使用し、下位レベルではその他の原則 (サブジェクトなど) に基づいている可能性が高い。

2.3.2.5 業務分類体系 (Business Classification Scheme) の維持管理

以下では、「業務分類体系の設計」に収容されている業務分類体系の維持管理についてその概要を記す。

(1) システム管理者の役割

BCS の作成またはインポート、および処分規則、ユーザー・プロファイル、アクセス制御などの継続的な維持管理に加えて、システム管理者は、非常に重要な役割と、時には非常に手間のかかる役割を有する。システム管理者は、長期にわたり、EDRMS 内の BCS の整合性の維持に責任を負う。

EDRMS は、多くの記録管理プロセスを自動化する機能を提供する。一連の『Requirements for ERMS』は、管理者がこれらの機能を特定し、実装するために役立つことがある。たとえば、EDRMS には、大量のメタデータを自動的に収集してから、BCS を通じて下方に継承させる機能がある。これによって、一貫性を高め、データ入力に必要なキー操作の量を減らすことができる。また、これによって、共通の処分ルールまたはアクセス制御を BCS の領域全体に適用できる。

記録レベルでは、これは業務活動の証拠を収集するための重要な側面である。個々の記録の場所と属性を含むメタデータのほとんどは、フォルダへの記録の宣言に基づいて、自動的に収集される。

関連する業務活動を記録している BCS の領域に、同じ処分スケジュールとアクセス制御属性を割り当てることができることも、非常に役立つ。しかし、一般に、通常のエンド・ユーザーに負担を押しつけて、管理者の作業を軽減しようとすることは避けるべきである。

(2) 業務分類スキームの再編成

前述したように、BCS は組織の記録に関する唯一のビューである。シソーラスの用語、『政府カテゴリー・リスト』、サブジェクト（または、サブジェクトが主要な構造のために使用されている原則ではない場合は職務）に従って、追加の論理構造を表現する多くの方法がある。

このようなカテゴリー自体が高度に構造化されている場合、主要な分類として上記の基準に従って、記録を再編成することが理論的に可能である。このプロセスの大部分を自動化できる場合もある。

時間の経過により、組織は、BCS 構造を大幅に変更する必要があることに気付く場合がある。これは、法令環境、利害関係者の期待の変化、または作業慣行の発展が原因となることがある。厳格でない構造の方が簡単に実装できるように思われるかもしれないが、その維持管理と開発は、時間の経過に伴って困難になる可能性がある。BCS の再編成が必要になった場合、厳格でない構造は、新しい構成にマッピングすることも比較的困難である。

または、構造があまり厳格ではない場合でも、BCS がその目的を十分に達成していないと判断される限り、1 つの「ビュー」から別のビューへのマッピングを決定して、情報の体系的な再編成を実現することが可能である。また、主要な分類を形成するために「格上げ」されるスキームの構造の厳格性が低いほど、多くの作業が必要になる。

一般に、高度に構造化された、または厳格な業務分類スキーム（おそらくシソーラスによってサポートされ、強制される）に基づいて記録を分類する方が簡単である。ERMS と組み合わせて使用する（ERMS 間で移動する）場合、このプロセスのほとんどは自動化することもできる。

(3) レガシー記録

紙の記録を含むレガシー記録から ERMS 実装へのマッピングに対しては、類似原則が適用される。

(a) 電子記録の構造化アセンブリ

レガシー・システムが電子的であり、何らかの論理的構造が存在し、その構造が保持されている場合(たとえば、エクスプローラ、一部の文書管理システムなど)、これは最も簡単である。これは、おそらく ERMS ソリューションにインポートすることができる(これは、『Requirements for ERMS』の一括インポートのセクションに関係する)。これには、サブクラス、フォルダ、記録を含むクラス全体のインポートが伴うことがある。

ここで、「含む」とは、場合によってはある程度の自動化により、受取側のシステムで再アセンブリできるように、(通常はリレーショナル識別子を通じて)リレーショナル構造を維持するという意味である。

複雑化の要因となるのは、適切な分類スキームの永続化のみを推奨すべきであるということ、および前述したように、フォルダと記録を移行するときに、分類原則の変更に関して複雑なマッピング作業が必要になりうるということである。

このような作業中にフォルダの編成が変更されることがありうるが、記録の集合をフォルダ内に分解することは推奨されない。記録の集合は、個々の記録およびそれぞれの証拠価値のコンテキストの重要な部分であり、その分解は、記録管理の重要な原則に反する。再編成されたフォルダに対する以前の参照の保管に関しても検討すべきである。

分類スキームを交換するために、簡単に格上げすることができる代替的な分類「ビュー」(たとえば、職務スキームの事後結合サブジェクト索引など)が既存の BCS (「ファイルプラン」)に含まれる可能性は低い。このため、レガシー・システム内のフォルダを新しいシステム内のフォルダにマッピングする方法を評価するために、複雑なマッピング作業が不可欠になる。通常、これはフォルダ間レベルで実施される。明らかに、資料の量が多いほど、作業の負担は大きくなる。

(b) DMS およびスキャニング・ソリューションからのメタデータ

スキャンされた画像に関連し、文書管理システムに保持されるメタデータは、比較的アクセス不可能であることが多い。第 1 に、メタデータの量と性質はさまざまであり、豊富さ、収集の適切性、品質に関して記録管理メタデータとは異なる。リポジトリ内のデジタル・オブジェクトに付属するメタデータ・セット全体を構造化されたアセンブリとしてエクスポートできる ERMS とは異なり、DMS のエクスポート機能はまったく一貫していない。

また、技術的アーキテクチャが、メタデータにアクセスするための障害となることがある。(ERMS の場合のように)個別にアクセスできるメタデータベースを備える代わりに、メタデータは、非常に専有的な形式で、文書に付属する文書リポジトリ内のファイルに格納されることがある。同じサプライヤーの次世代製品に移行する場合を除き、一部のケースでは、メタデータをまったく抽出できないことがある。

(c) 物理的記録に関連するメタデータのインポート

紙環境のファイルプランを形成するメタデータは、登録データベースから ERMS にインポートできる可能性がある。多くの専有 COTS ERMS パッケージは、ERMS リポジトリに格納できない個々のオブジェクト(大規模なプランなど)または物理的なフォルダ内のレガシー記録のいずれであるかにかかわらず、物理的なオブジェクトを管理できる。これは、ERMS で明示的に作成されるメタデータのみに該当する。生成されたデジタル電子環境で必要なメタデータに相当するも

のの大半は、その記録と共に物理形式で格納される。

その他のメタデータが存在するが、アクセスできない場合がある。メタデータを標準形式（カンマ区切り変数）で表現できる場合、アプリケーションレベルではなく、表からエクスポートを実行することができるが、製品によってエクスポート機能は異なる。

(d) 代替的な戦略

特に記録が長期間にわたって保管される可能性が低い場合、レガシー記録に対する実際的なアプローチの方が適切である場合がある。たとえば、分類スキーム内にノードを作成して、これ以上オブジェクトが追加されない「無効」（クローズ）領域として、既存の構造上に、レガシー記録のための場所を形成することができる。

2.3.2.6　電子記録の評価選別

評価選別は、もはや価値のない記録から継続する価値の記録を区別し、選別からもれた記録を除外できるようにするプロセスである。「評価選別方針」は、英国政府内の記録管理条件の変化、特にデジタル記録の普及に対処するために策定され、確実で一貫した評価選別決定を可能にする戦略を策定して実施するためのものであるとしている。

- 部局の業務目的とアーカイブ目的に対して持続的価値のある記録に中身を制限する記録管理システムの効率性を維持する。
- 長期的価値またはアーカイブ価値のある記録が識別され、その保管のために準備が行われることを確実にする。

「評価選別方針」では、評価選別の時期、目的、スタッフ配属、範囲の現在と将来について表2.8のようにまとめている。

ここで、グリッグシステムとは、部局が記録を管理できるようにした効果的な手段として、ジェームズ グリッグ卿（Sir James Grigg）が委員長を務める部局記録に関する王立委員会（Royal Commission on Departmental Records）でまとめられ、文書の保管および保持義務に関する法的立場の無計画性を改めた1958年の公文書法の基礎となった。この法律は公文書を定義し、公文書の保管と管理について国立公文書館と部局の間および部局内の義務を指定し、歴史的記録を国立公文書館へ移管する時期（30年目）とパブリック・アクセスの権利（1967年公文書で50年から30年に修正）を定めた。

表2.8：評価選別と評価の移行

	現在	将来
評価選別プロセスの要素	グリッグシステムによる評価	評価選別（デジタルおよびハイブリッド記録） 評価選別＋評価（紙とその他の記録）
評価選別基準の適用時期	第1評価 （完結（closure）から5年後）	任意の時期、ただし、 (a) 電子記録 ・ファイル計画を通して作成される前

	第 2 評価 （記録の最初の日付から 25 年後）	・すでに最終処分が決まったフォルダへのファイリングを通した作成時 ・半現用記録の保存への移行時 ・さらに永久的な保管への移行時 (b) 紙の記録 ・現行の時期と同じだが、早期の第 2 評価が適切になる可能性あり ・関連付けられている電子記録の評価時
評価選別基準の適用理由	第 1 評価は、記録を将来の業務で使用する可能性を評価（＋歴史的価値の認識） 第 2 評価は、記録の歴史的価値を評価	業務およびアーカイブ評価選別価値は付録 2 に定義されている。
評価選別基準の適用者	第 1 評価は、部局の業務単位か、部局の記録センターの第 1 評価担当者の個別グループ：国立公文書館によるいくつかの抜き取り検査 第 2 評価は、国立公文書館の直接監視による部局の第 2 評価担当者の個別グループ	これらの業務単位は今までどおり作業に係わるが、その方法は異なる。特定の記録または記録のセットに関する決定は、組織または職務に関係する記録のすべてかその広範囲の分析の前に行われる。この最初のプロセスは、業務とアーカイブ目的の両方に対してさらに共同的な努力を必要とし、国立公文書館のクライアント担当者、評価担当者、過去と現在の商用利用者の専門知識が必要になる。
アーカイブ評価選別基準が適用される記録の範囲	他の部局または部門で同様ないし関係ある記録に対して行われた決定を限定的に認識しながら個別に評価される記録の各グループ	新しい方法では以下が奨励される。 (a) 1 つまたは複数の組織が同じ職務の中で作成するすべての記録を考慮 (b) 政府内に類似または関連した記録のある場所を認識 (c) 記録のタイプと記録を作成する機関のタイプに対する共通/汎用選択基準の策定

2.3.2.7　電子記録の最終処分

最終処分スケジュールの計画は、組織の情報および記録資源の管理を確立して維持するために重要である。すべての情報が永久に保存できるわけではない。

情報は資産であると同時にリスクでもあり、情報を所有する組織に責任を課し、適切で確実な

管理を要求する。このバランスを正しく保つには、“その情報が必要なのはいつまでか”という問題に対処することを組織レベルで決定することが必要になる。情報のニーズが相容れずに対立する場合は、解決策が必要になる。多くの組織がこうした問題に取り組まなければならない理由は他にもある。特にデータ保護法（Data Protection Act）と情報自由法（Freedom of Information Act）は、個人のデータと記録の適切な管理について、さらに厳しくて新しい義務を課している。

以下では、「最終処分スケジュール」に記載された、電子記録の最終処分の要点を記す。

(1) 最終処分、保持、破棄、評価

最終処分、保持、破棄、評価は、本質的に同じ概念を異なる面と用語法から眺めた用語である。英国では、電子的環境のアーカイブ慣行により、“最終処分”を“保持”より優先させる。“最終処分（Disposal)”は、廃棄（destruction）を意味するだけではなく、永久アーカイブへの移管を含めた意味合いを含んでいる。記録の最終処分の決定ができない場合は、後日の“評価(Review)”に先送りすることができる。“保持(Retention)”は、記録を維持すべき期間を一般的に意味する。したがって、普通は最終処分期間を表し、そのように表現される。これらの用語はどれも意味は概ね同じである。

(2) スケジュール

スケジュールに関する管理上の主な利用は、スケジュールに含まれたルールに従って維持すべき記録のカテゴリーをグループ化/リスト化（すなわち“スケジュール”）し、リストに含まれた記録にこうした最終処分基準を適用する論拠を密接に結びつけることにある。

今までに登録されたファイルシリーズでは、それはスケジュールに含まれるシリーズになる。これは管理上も便利であり、記録の最終処分の透明性と監査能力も最大限になる。

最終処分スケジュールは、一般的に、トリガ、期間、その期間の最後に取るべき行動の組み合わせである。いくつかの状況（特に電子的環境）では、スケジュールは１つ以上のステップで構成される。

代表的なトリガは、フォルダ/フォルダ・パートの開始（opening）と完結（closure)、フォルダ/フォルダ・パートの開始（opening）である。ここで注意しなければならないのは、アーカイブ記録は作成から 30 年経過するまでに国立公文書館か承認された別の公文書記録所に保管することが公文書法に規定されていることである。最終処分の活動は、一般的に、“廃棄”、“アーカイブに移管”（電子的環境では、“エクスポート”と“廃棄”活動に分離)、または“評価”である。

(3) フォルダの通常の管理単位

一般的に、記録を管理するほとんどの目的で使用される管理単位は、フォルダ（“ファイル”）かフォルダ・パートである。一般的に、最終処分は紙の環境では登録シリーズレベルで理解されて管理されてきた。これを電子的環境で計画するには、業務分類体系設計、電子記録管理システム（ERMS）の最終処分機能、MoReq（電子記録管理のためのモデル要件）規格から派生した“クラス”エンティティの理解が必要になる。

電子的環境に関しては、このガイダンスはERMS機能要件（Functional requirements for ERMS）の用語法とエンティティ・モデルを使用する。したがって、トリガがパートのメタデータに関係

している場合、パートの実行は異なる時間に発生するが、フォルダ・パートは時間によるフォルダの区分に過ぎず、個別のスケジュール/最終処分ルールを適用してはならない。

電子的環境を含めた最終処分活動にとって、フォルダの集合体の完全性が厳格に監視されることは特に重要である。そして、フォルダから記録を場当たり的に削除すること（“除草”とも言われる）は実行されない。最終処分スケジュールの目的の１つは、個人の好みに基づいてではなく、合意された基準に基づいて最終処分が実行されていることをはっきりと示すことである。

特に物理的環境では、従来の形式ではない記録をフォルダに簡単に集めることができない場合がある（マップ、プラン、ビデオテープ、アナログ・フィルムなど）。こうした記録については、適切な方法、すなわち、その内容、形式、取り合わせを説明して適宜な最終処分ができる方法で最終処分スケジュールを使用し、依然として最終処分方針の管理下に置かれなければならない。

(4) 電子的環境における最終処分

電子記録管理ソリューションが整っているデジタル形式の記録では、フォルダ内にどのようなオブジェクトでも含めることが論理的に可能なはずである（ERMS のオブジェクトリポジトリに実際に含まれていない物理オブジェクトへの参照を含む）。以下、ERMS 環境に要求されるオプションと、そうした状況で最終処分を管理する方法について概説する。

(a) 非デフォルト Record_type 要件

“一般 ERMS 機能要件”には、記録管理の基本的原則を不均衡に損なうことなく、個人データの管理をさらに促進するための特別な機能が含まれている。

極度に制限されたタイプのドキュメントに対して、フォルダ自体を処分する前にフォルダ（非デフォルト record_type ドキュメント）内で特定の記録を処分[廃棄]することが許可される。予測されるシナリオは、内容は同じ集合体の一部を形成するが、極端に長い期間（たとえば、老齢退職手当）とはるかに短期の価値（たとえば、年間実績報告書/訓練関連）の両方の記録がある個人ファイルである。

但し、集合体原則（aggregation principle）のこの緩和は、データ保護法の遵守を促進するためだけに考案され、さらに幅広い使用は想定されていない。これを拡大すると、記録の集合体の完全性を損ない、国別標準と国際標準に従う記録システムの運用に支障を来す恐れがある。

(b) 電子記録の廃棄方法

削除とは、電子記録の完全な廃棄を最終的に意味しなければならない（そして、物理的記録の安全な最終処分の電子版である）。実際には、ほとんどの技術的環境において、電子記録のインスタンスを削除することは、オブジェクトへのオペレーティングシステムやアプリケーションのリンクを除去するだけで、保管メディアの同じスペースが何度も再利用されているときは実際に削除されない。

データ保護法は、情報が普通の方法で検索できないことを確実にするために適切なステップを取ることを要求している。国立公文書館の見解によると、バックアップが適切に管理される場合は、ほとんどの環境では普通の検索手段を除去することで十分である。

ERMS 要件は、米国国防総省の ERMS 要件（“expungement”とも呼ばれる）のように廃棄する内容を 5 回上書きすることを指定していない。但し、英国政府の高度なセキュリティ環境では 5 回上書きが求められることは十分に考えられる。

(c) ハイブリッド環境管理

“ERMS 機能要件”の物理的/ハイブリッド環境に関するオプション・モジュールを参照する必要がある。特に注意が必要なのは、非必須要件とその実施方法である。この要件が満たされないと、ERMS 外部の物理オブジェクトが実際に廃棄されることを確実にするために別の手順の導入が必要になる。

(d) 統合 ERDM ソリューションにおける未宣言文書の処分管理

EDRM（電子文書記録管理）ソリューションでは、すべての電子文書が正式記録として宣言されるわけではない。未宣言文書が無期限に保持されないように工夫する必要がある。

論理的には、ユーザーが正しく訓練を受けていれば、未宣言文書のライフサイクルは短いはずで、記録に対して最終処分期間として識別されるよりもはるかに短期間の後に削除が可能である。ERMS 機能要件の“文書管理（Document management)”モジュールには、これをサポートする要件が含まれている。

(e) 完全な ERM を使用しない最終処分の管理

ERM 環境の外では、最終処分管理はさらに複雑で問題を引き起こす可能性がある。組織の方針と一致した、確固とした構造を持ち、監査可能で透明性のある最終処分は、ERM 業務ケースの重要な部分を占める。これに加え、最終処分を業務分類計画と調整し、統合された自動方式で両方を管理できる可能性はない。

国立公文書館は、ERMS の完全な機能が必要のない場合、電子記録と電子文書の管理に関する次のようなガイダンスを作成している。

①電子メールを管理する方針を作成するためのガイドライン

②LAN で MS Office 97 を使用した電子文書管理

③電子記録収集の一覧を編集するためのガイダンス

④情報資産の評価、つまり電子記録の一覧の評価選別

Web サイトとデータベース/データセットなど、とりわけ要求が厳しくて複雑に見える環境がいくつかある。こうした技術的環境における最終処分管理のための別の指針は、特定のガイダンス（Web リソース管理（Managing web resources））に含まれる。

⑤複製についての業務ルールによるコピー管理の徹底

⑥もはや必要がないか記録集合体に入れられたオブジェクトの削除手順

⑦ネットワーク・ドライブや電子メール・ボックスからオブジェクトを処分するために、IT 部門がデータ除去スクリプトを実行することも考慮できる（記録の正しい取得を保証する組織の方針と手順と併せて検討しなければならない)。

(5) 合意

記録の最終処分スケジュールについて意見を求める必要がある関係者は、たとえば以下のように数多くいる。

①［営業］業務責任者

②上級管理職

③IT 責任者（セクション 7 で説明した理由と、バックアップと最終処分の問題に特に関係する IT 業務活動に関する理由による）

④関連する規制団体

⑤［公文書機関に対する］国立公文書館クライアント責任者（国立公文書館の入手方針で定められた操作選択方針も、公共および専門協議段階の対象になる）

⑥他の公共団体（たとえば、共通して記録を所持する中央政府機関は、不必要な重複を回避するためや、情報の自由（FOI）要求の効率的な処理を支援するために連絡が必要になる場合がある。）

⑦セクション6で説明されている考慮事項を正しく評価するには、法的助言が必要な場合もある。

この協議プロセスは、入念な記録文書、特に、決定された処分期間に対する関係者の合意の正式な承認記録が必要になる。

2.3.2.8　長期に保存すべき記録の選択

保管するに値しない記録を保管するには継続的に高いコストがかかるが、さりとて記録の破棄は元に戻すことのできない行為である。「記録の選択に関する一般ガイドライン」は、永続的な価値のある記録を比較的簡単に特定するために、部門記録担当役員（Departmental Record Officers：DRO）を支援し、不適切な破棄や正当な基準に基づかない選択を防止することを目的に発行された。

1660年より前に作成されたすべての記録、年次報告書、主要な部門の機関の議事録と配布文書の一連の記録。部門の法律、または部門が主導する法律の作成に関連する文書、内閣府の公式の歴史で引用された文書、またはその作成において参照したことが知られている文書、法令に基づいて永続的に保管しなければならない記録（必ずしも国立公文書館に保管する必要はない）に分類される記録は、いずれにしても保管しなければならない。

問題はそれ以外の記録である。以下、題材として、政府機関における記録の取得方針、目的、収拾すべき記録のテーマ、記録の重要性を評価するために次の情報、選択される可能性が高い記録の例などの関係を概観する。他の組織においても、アナロジーとしてこれらの関係を参照することは有用であると思われる。

なお、このガイドラインでは、選択される記録は、後述の基準のほか、次の条件も考慮する必要があるとしている。

(a) 単独で使用されることは少ないが、その部門および他の部門によって選択された他の記録とともに頻繁に使用される。

(b) 作成された目的とは関係しない調査のために定期的に使用される。

また、特定の形式の記録を「保持する」法定要件は、通常、作成し、積極的に使用されている間に記録を保持する要件であり、記録を永続的に保管する義務ではないことに注意する必要がある。

(1) 取得ポリシーと収集テーマ

このガイドラインのなかの、取得ポリシーの章では、記録の取得に関して次のような目的を定めている。

・英国政府の主要な政策と活動を記録すること
・国家と国民との対話および国家と物理環境間の相互作用を文書化すること

これらの目的は、次のテーマに関連する記録を収集することによって達成される。

(a) 国家の政策および行政プロセス
(b) 政策の策定および中央行政官による公共資源の管理
(c) 経済の管理
(d) 外交および国防政策
(e) 裁判および治安維持
(f) 社会政策の策定および実行
(g) 文化政策
(h) 国家と国民との対話および物理環境に対する影響
(i) 正式な国境外の個人、共同体、組織に対する国家の対応に基づいて文書化される英国の経済、社会、人口統計上の状況

ガイダンスの作成とレビューの実施に際して、DRO とレビュー担当者は、選択する記録が、1つ以上の選択テーマに当てはまることを確認する必要がある。

(2) 評価のための情報

情報の質および量と記録の重要性を評価するために次の情報が考慮される。

(a) 内部行政の記録に関する運用選択ポリシーに規定されている、部門、その組織および手続きの歴史的側面
(b) 政策と法律の策定および解釈と、(さらに限定的に言えば) その実施
(c) 記録が既知の事項に多くの情報を追加する場合は、注目すべき出来事または人物
(d) 政治、社会、法律、または経済の歴史における主要な出来事、展開、または動向
(e) 科学、技術、環境、または医療に関する研究開発
(f) 地域または地方の状況 (地方から情報を入手できると予想することが合理的でない場合、中央で情報を保管することが便利な場合、または多くの地方の情報が地方で保管されていないことが確認されている場合)
(g) 統計および定量的研究による人口統計、医療、社会、文化、経済の歴史および歴史地理学

なお、次は、レビューで選択される可能性が高い記録の例を示す。

(a) 理事会および委員会の文書、刊行物および灰色文献 (グレー・リテラチャー)、内部行政の記録に関する運用選択ポリシーに規定されている、文書の発行元に関連する記録
(b) その部門に従属している、または緊密に関連しているが、情報公開法の対象ではない機関からの報告書およびその他の文書の写し
(c) 部門が主導的な役割を果たした一次的または従属的な立法につながる文書、大臣への提出文書、内閣または閣内委員会に対して資料を準備する過程で作成されたすべての草稿を含む文書などの主要な政策文書
(d) 主要な政策の策定、実施、または解釈の過程で作成された文書。たとえば、政策の大幅な変更を反映した文書、部門の主な職務およびプログラムに焦点を当てた文書、部門と他の公共分野または民間分野間の対話、特に統計、報告書または要約など、他の場所で簡単に

発見または編さんされない特定の情報など

(e) 部門の廃止された活動または中止されたプロジェクトに関連する記録

(f) 注目に値する出来事および有名な事件や、同時代の強い関心または議論を引き起こしたその他の出来事に関係する文書

(g) 科学、技術、環境、または医療の研究開発の比較的重要な側面に関する記録

(h) 地域または地方にとって非常に重要であるが、地方で入手できない情報を含む記録や、国全体またはその広域を対象とする重要または便利な概要情報に当たる記録

(3) 他の場所で保管されている情報

(a) DRO と CM は、レビュー対象である記録内の情報の全部または一部が、次のいずれかの形式で入手できるかどうかを検討する必要がある。

①出版された著作物など、比較的コンパクトな形式または入手が容易な形式

②当該部門、その地域事務局、地方事務局および研究機関、その他の部門、国立公文書館(TNA)、またはその他の公記録保管所に保有され、永続的な保管のために選択された、または今後選択されるその他の記録

③TNA またはその他の公記録保管所に保有されている他の部門の記録

(b) 情報が公開されたことが明らかではないが、比較的簡単に確認できると思われる場合（年次報告書または国会の質疑への回答に含まれる場合、またはよりコンパクトな形式でその他の方法により保有されている場合)、この確認を行う必要がある。代替的な情報源を探すために、過度な時間を費やす必要はない。

(c) 単なる情報提供のために当該部門の他の部署または他の部門によって配布された文書のみが記録に含まれる場合、その管理上の有用性が終了するとともに、この記録は排除されなければならない。このような文書が、原本の通信または覚書から切り離せない場合は、保管または破棄の決定は、この追加資料の行政上または調査上の価値に基づいて下す。

(d) 部門間委員会の議事録と配布文書を含むファイルは、通常、主導的役割を果たした部門で保管される。このようなファイルは、その中に重要な部門の文書が含まれる場合を除き、その場所にかかわらず、管理上の有用性が終了したときに破棄される。ただし、DRO は、指導的役割を果たした部門で、記録が引き続き保管されているかどうかを確認する必要がある。

(e) 部門内に、配布された報告書など、重複する、または類似している一連の記録がある場合は、通常、一部のみの保管を検討する。その他の記録は、最初の記録を補完するために使用できる場合、または異なる順序で配置され、独自の情報的価値を有する場合を除き、破棄する。

(f) 通常、TNA は、別の保管所内にすでに移転されている、または保有されている記録について、情報が重複しているかどうかを助言することができるようにする。代替的な情報源を探すために、過度な時間を費やす必要はない。

(4) その他留意点

(a) 通常、永続的な保管のために選択するファイルのすべての部分を保管する必要がある。ただし、これによって、重複した資料またはその他の一時的な資料が大量に保管される場合、このような資料から構成される部分は破棄しなければならない。

(b) 保管のために選択したファイルがサブファイルに関連付けられている場合、そのサブファイルは必ずしも保管する必要はない。各ファイルは、そのメリットに基づいて取り扱わなければならない。

(c) 永続的な保管のために選択される多くのファイルには、重複した資料、またはその他の一時的な資料が含まれる。消去するプロセスの中でこのような資料を簡単に削除できない場合は、その場所に残しておくべきである。ほとんどすべての場合、除去プロセスは費用効率が高くない。

2.3.2.9 専門教育

英国では、記録管理の専門人材を大学で育成（フランス、オーストリア、ドイツは、国や国立公文書館が育成）しており、研究機能も持っている。記録管理の専門課程は、ロンドン、リバプール、ウェールズ、グラスゴー、ダンディー、ノースアンブリア、ダブリンの 7 大学に大学院レベルの学科があり、定員は 7 大学合わせて凡そ 200 名である。なかでも、グラスゴー大学はデジタル保存に強みがある。

英国には、アーカイブや記録管理に関する特別の資格制度はなく、大学院を修了したことをもって資格を得たものと見做される。専門人材を必要とする組織は官民あわせて 2 千あり、企業、行政いずれも人材不足の状況にある。

ロンドン大学に関しては、ドクターコースに 6 名、マスターに 30 名、ディプロマに 10 名、サティフィケートに数名在籍している。カリキュラムは次のように構成され、各科目は（中世の文献を除き）紙と電子の両方を扱っている。

［必須科目］

・アクセスポリシーと実践
　記録とアーカイブへのアクセスを保証する意義、政策、利用など。
・アーカイブ
　整理学、分類。デジタル文書の整理法、主なシステムパッケージの内容を含む。
・国際専門コンテキスト（留学生のみ）
　アーカイブに関する国際的な比較分析。
・マネジメントスキル
　オフィス管理、人事管理、戦略計画、財務、会計、資金調達
・保存
　保存、修復管理の基礎。書庫のリスク管理、災害リスク、セキュリティを含む。
・アーカイブおよび記録管理の原則
　分類、ライフサイクル理論、評価選別、保管の実践、情報管理、ナレッジ管理など。
・1500 年以降のアーカイブの講読と解釈
　文献の解釈、理解。法的、行政的背景の理解。
・記録管理
　記録の作成から保存廃棄、移管までのライフサイクル管理。

［選択科目］

・高度な保存
・データベースシステム分析と設計
・人文領域のデジタルリソース
・電子出版
・英語歴史的なフレームワーク
・中世英語（12 世紀～16 世紀）のアーカイブ
・歴史参考文献

2.3.2.10　用語定義と適用標準

(1) 用語定義

①最終処分

記録を廃棄すべきか、永久保存のための保管サービス機関へ移管すべきか、または提出すべきかどうかに関する決定と、その決定を実施すること。

②最終処分スケジュール

記録のタイプを識別し、廃棄、永久保存の指定、さらなる審査への提出までのそれぞれの維持期間を指定するスケジュール。

③記録の維持

本要領の文脈では、記録の維持とは、文書と他のタイプの記録を作成するごとに、そして、受け取った資料を処理するごとに、公的機関の活動を記録することを含む。

④メタデータ

記録が作成された状況、その構造、それまでの管理方法に関する情報。メタデータは、デジタル・システム内のイベント・ログ・データといった記録を表すことができる。また、タイトルと場所などのような、デジタル・システムから管理されるか記録表またはカード索引によって管理される紙媒体のファイルを表すこともできる。

⑤公文書記録所

保存に選択されているが国立公文書館へ移管されない公文書の受理、保存、公開に指定された保管組織。指定権限は、大法官によって国立公文書館館長（Chief Executive of The National Archives）または適切な先任者に委譲されている。

⑥提出

1958 年公文書法に基づいた取り決めで、永久保存として選択されていない記録は国立公文書館によって適切な機関に提出される。

⑦公文書

1958 年公文書法または 1923 年（北アイルランド）公文書法の対象となる記録。政府の省庁とその行政機関、一部の特殊法人、裁判所、国民保険機関（NHS）、軍隊の記録は公文書である。地方自治体の記録は、イングランドとウェールズでは公文書ではないが、北アイルランドでは公文書である。

⑧記録

証拠として作成、受理、保有される情報と、法的義務の遂行または事務処理における組織または個人ごとの情報のこと。

この定義は、BS ISO 15489-1:2001 情報および文書化 - 記録管理 - パート 1：総論（Information and documentation - Records management - Part 1: General）に依る。

⑨保持

1958 年公文書法に基づく取り決めで、公的機関は指定された公文書の移管を決められた期間延期することができ、その期間の終わりまで公文書を保持することができる。

⑩記録システム

記録とその他の情報を含む情報システムまたは処理システムで、紙ベースのシステムかデジタル・システムになる。例としては、通信ファイル・シリーズ、デジタル記録管理システム、ケース管理システム、金融システムなどの機能別システムなどがある。

(2) 標準

〔英国規格協会〕

- BS ISO 15489-1, 情報および文書化 - 記録管理 - パート 1：総論（Information and documentation - Records management - Part 1: General
- BS ISO/IEC 27001: 2005, 情報技術、セキュリティ技術、情報セキュリティ管理システム、要件（Information technology. Security techniques. Information security management systems. Requirements）
- BS ISO/IEC 27002: 2005, 情報技術、セキュリティ技術、情報セキュリティ管理システム、実施要領(Information technology. Security techniques. Information security management systems. Code of Practice)
- BS 10008 電子情報の証拠としての重要性および法的有効性 - 詳述（Evidential weight and legal admissibility of electronic information - Specification）
- BS 8470:2006, 機密資料の安全な廃棄、実施要領（Secure destruction of confidential material. Code of practice）
- BS 4783, データ処理と情報ストレージで使用するメディアの保管、移動、維持（Storage, transportation and maintenance of media for use in data processing and information storage）

〔国立公文書館〕

英国では、国立公文書館館長（Chief Executive of The National Archives）は、政府の知識および情報機能に対する専門職の責任者として、あらゆる形式の記録のライフサイクル全体をカバーする管理基準を設定する。基準はガイダンスとツールキットによりサポートされる。政府機関に対する助言は、他の公共部門も使用することができる。基準とガイダンスは国立公文書館の Web サイトに掲載されている。

http://www.nationalarchives.gov.uk/services/default.htm?source=services

また、記録管理のメタデータに関する基準は、Govtalk に掲載されている。

http://www.govtalk.gov.uk/documents/Records_management_metadata_standard_2002.pdf

〔中央政府〕

・ 国立公文書館による上記の基準とガイダンスに加え、保護記録 22 が内閣事務局（Cabinet Office）によるデータ処理ガイダンスの対象になる。
http://www.cabinetoffice.gov.uk/mediacabinetoffice/csia/assets/dhr/cross_gov080625.pdf

〔地方自治体〕

・ 記録管理協会（Records Management Society）は、地方自治体のための最終処分および情報監査に関するガイドラインを公表している。
http://www.rms-gb.org.uk/resources.
・ 地方自治体協議会（Local Government Association）とウェールズ地方自治体協議会（Welsh Local Government Association）は、保護記録のためのデータ処理ガイダンスを公表している。
http://www.idea.gov.uk/idk/aio/9048091

〔継続教育および高等教育〕

・ 情報システム合同委員会（Joint Information Systems Committee、JISC）Infonet は、情報管理インフォキット（Infokit）を作成している。
http://www.jiscinfonet.ac.uk/information-management

〔学校〕

・ レコードマネージメント協会（Records Management Society）は、学校のための記録管理ツールキットを公表している。
http://www.rms-gb.org.uk/resources/848

〔警察〕

・ 内務大臣（Home Secretary）は、警察情報の管理に関する実施要領を公表している。
http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/CodeofPracticeFinal12073.pdf?view=Standard&pubID=224859
・ これをサポートするガイダンスは、警視総監全国センター（National Centre of Policing Excellence）が警察長協会（Association of Chief Police Officers）に代わって作成している。
http://www.npia.police.uk/en/8492.htm
http://www.crimereduction.homeoffice.gov.uk/policing21.htm

〔国民保険機関（National Health Service、NHS〕

・ 保健省（Department of Health）は、NHS のための実施要領を公表している。
http://www.dh.gov.uk/enPublicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

〔免除の適用〕

・ 情報自由法適用免除（FOI exemption）に関するガイダンスは、情報自由法と EIR 両方の規制機関である情報コミッショナー事務局（Information Commissioner's Office）が公表している。
http://www.ico.gov.uk/tools_and_resources/document_library/freedom_of_information.

aspx

- 法務省（Ministry of Justice）
  http://www.justice.gov.uk/guidance/foi-exemptions-guidance.htm
- EIR 例外に関するガイダンスは、環境・食料・農林省（Department of the Environment, Food and Rural Affairs）が公表している。
  http://www.defra.gov.uk/corporate/opengov/eir/guidance/full-guidance/pdf/guidance-7.pdf
- 国立公文書館
  公文書へのアクセス（Access to Public Records）:
  http://www.nationalarchives.gov.uk/documents/access_manual.pdf
- 公開前に紙および電子文書から免除情報を編集するためのガイドライン
  http://www.nationalarchives.gov.uk/documents/redaction_toolkit.pdf

［参考文献］

[232-1] "Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000", Ministry of Justice,2009
[232-2] "Business classification scheme design Ver. 1.0", The National Archives, OCTOBER 2003
[232-3] "Acquisition and Disposition Strategy", The National Archives, 2007
[232-4] "Custodial policy for digital records Ver1.0", The National Archives, 2005
[232-5] "Appraisal Policy Version 1", The National Archives, 2004
[232-6] "General guidelines for the selection of records Ver1.0, The National Archives, 2006
[232-7] "Disposal scheduling", The National Archives, 2004

2.3.3 チェコ

チェコ共和国の電子政府および電子文書管理について紹介する。チェコでは大規模に電子政府を推し進めており、国、地方、市町村の行政機関、法人、また国民にも大きな影響を与えている。例えば、行政と第三者（国民、法人）間のコミュニケーションに利用される「データボックス」は日本で検討された電子私書箱に対応するもので、最終の目標は、チェコ国行政の完全な電子化にある。

利用しやすい電子行政を進めるとともに、利用者に対する準備と周知という問題も提起している。

2.3.3.1 基本情報

チェコ共和国は面積7万8866km^{2}であり日本の5分の1弱の国土に、約1050万人が住んでいる。

2004年5月にEUに加盟している。

2.3.3.2　電子政府への取り組み[233-1]

チェコ共和国での電子政府への取り組みは、統合化情報システムの実現を担当するチェコ情報システム局（State Information System Office）の設置とともに、1996 年に本格的にスタートした。1999 年には、情報社会の発展に向けた最初の政策である、チェコ情報政策（State Information Policy、SIP）が採択された。2003 年は、パイロット・プロジェクトである行政ポータル（Public Administration Portal）がスタートし、さらに情報科学省（Ministry of Informatics）が設置された。これにより、行政の電子化が促進されることになった。情報科学省は 2007 年に内務省（Ministry of Interior）と併合された。

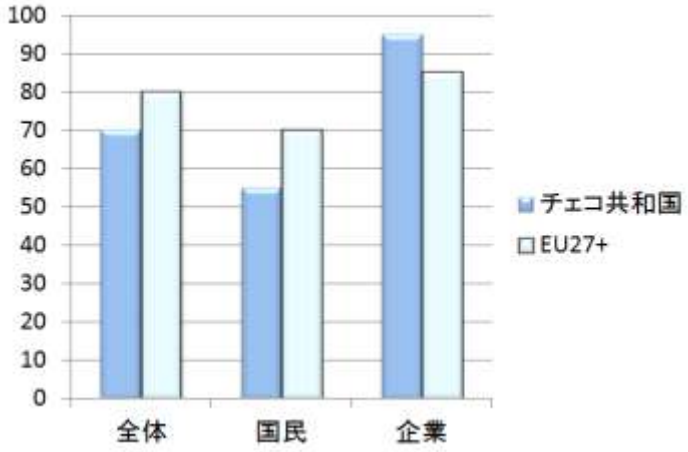


図 2.30：チェコ共和国におけるオンライン化状況（文献[233-1]より図を引用）

(1) 電子政府戦略

電子政府は構築途上であり、今後、すべての国民に対して平等な環境、機会を構築していかなければならない。また、行政サービスと地域の各種情報を適切な方法で全ユーザーグループに提供しなければならない。

これらの理由のために、行政のための統一フレームワークが 2007 年に採択された。「電子政府ヘキサゴン」と呼ばれるこのフレームワークでは、行政の全側面の機能が定義されている。

バランスの取れた電子政府の諸機能を達成するための総合的手段が、eGON と呼ばれている。本当に機能する電子政府のために、何をしなければならないのかを説明している。

以下の章では、このシステム概念（ヘキサゴン）および eGON を説明する。

(2) 効果的で利用しやすい電子政府（電子政府ヘキサゴン）

公共業務の領域で情報・通信技術を利用することは、当然のことと考えられている。しかしテクノロジーの多用が、行政サービスの質や効率の向上を意味するわけではない。最近では、小さな村から省庁にいたるまで、役所には最新の ICT 機器が備わっている。

しかしながら、国民は行政手続の簡素化という形で利益を受けることがなかった。この状況は、テクノロジーが過大評価されるとともに、他の側面が犠牲になったことによって引き起こされていると考えられる。そのため、法律、方策、および組織的な観点からプロセス全体と、考えられる手段を見直す必要があった。その結果として用意されたのが、行政に影響する全側面が統合さ

れた、電子政府ヘキサゴンというシステム戦略である（図 2.31）。このヘキサゴンの各頂点は、以下を表している。

① 国民：
- 政府および法律行為の準備プロセスに関与
- 電子的意見手続きの可能性

② 役人：
- 腐敗との戦い
- 能力の向上
- 行政役人としての倫理規範の励行

③ 法律：
- 過剰な官僚主義をなくすための複雑な分析
- 新たな法律行為の管理、経済、社会的な影響
- その環境上の影響

④ テクノロジー：
- 選択課題の完全に電子的な実行

⑤ 予算：
- 行政課題の実施コストの適切な判定
- 無駄のない方法
- 支出の透明性と効率性の向上

⑥ 場所：
- 行政への窓口場所（ワンストップ・ショップ）のネットワーク - Czech POINTs
- インターネットを介した安全なアクセス

テクノロジーはこの概念では、他のパートに依存した 1 パートでしかない。

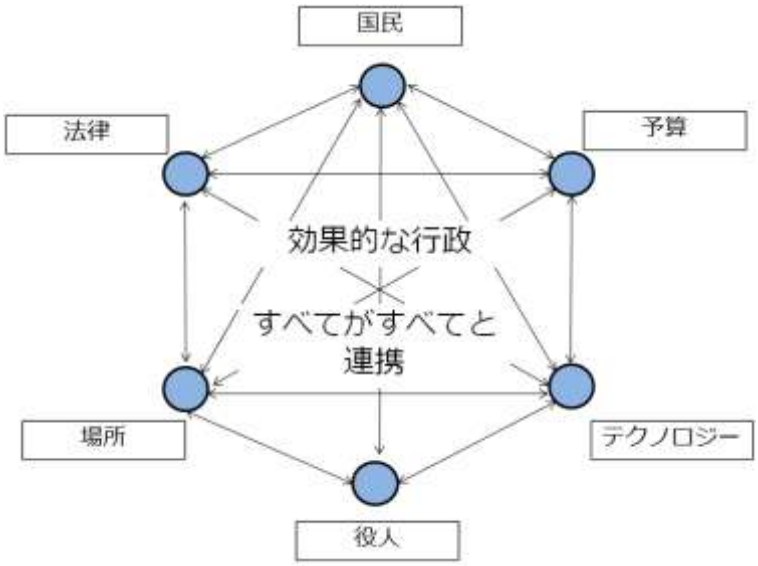


図 2.31：電子政府ヘキサゴンの図示（文献[233-1]の図を元に変更）

(3) 分かりやすい手段 - eGON

まえがきで紹介した「障壁のない欧州」への着手は、電子政府に関連した障壁を除去することも意味している。すなわち、電子政府では、さまざまなデータベースや公共情報源から入手可能な全データを収集して当局に提出する責務を、市民から政府へと移すことが望まれる。電子政府は国民に、また国民に近いところへ良質のサービスを提供するため、4 つの基本プロジェクトから成る大きな変化を経験する。

1 つ目の e プロジェクトは Czech POINT で、これは国民と行政間における汎用の窓口ポイントである。

2 つ目の e プロジェクトは KIVS で、行政のための通信基盤をを取り扱っている。

3 つ目の e プロジェクトは eBox（データボックスとも呼ばれる）で、電子政府法に関連し、市民へのサービス提供を促進し､それらをより安価に､より効率的にする目的で導入が決定された。

4 つ目の e プロジェクトは、中央レジスターであり、最新の情報のみを保持し、それらの情報は正しいとみなされる。

それぞれの e プロジェクト具体的には以下のとおりである。

① Czech POINT（ワンストップ・ショップ）
- 国がレジスタに保管する、エントリの検証済みコピー
- すべての大きな自治体、地方機関、国有郵便局、商工会議所へ（総計 2,200 以上のカウンター）
- 紙文書の認定変換、行政機関への全種類の申請、他の行政項目から証明付き情報を入手

② 行政用の通信基盤
- 行政機関の間の相互接続 - 統合体
- 行政機関と市民との間の接続
- 認証のレベルに従った、情報へのアクセス
- 運用の最初年における具体的な削減 - データ：5%、音声：7%

③ 電子政府法
- 電子的提供のための統一システム
- 「データボックス」を介した提供
- 電子通信の利用者個人を識別するための統一システム
- 紙から電子文書へ、およびその逆の認証された変換

④ 公共行政のための基本レジスター

基本レジスターに関する包括法は現在、省庁間の意見手続きにある
- 住民の登録
- 個人の登録（法的人格を持つ全エンティティー）
- 領地の識別、住所、不動産の登録
- 権利義務の登録

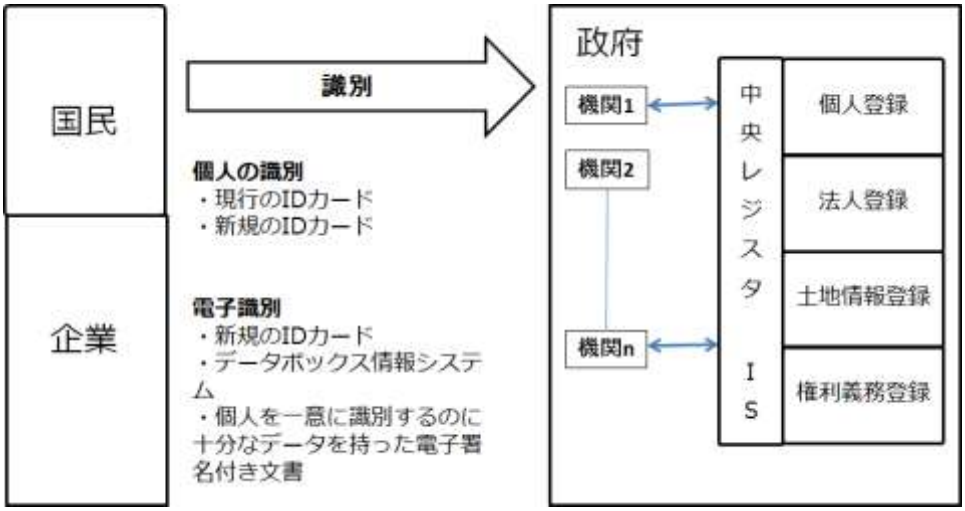


図 2.32：シンボル eGON の意味（文献[233-1]の図を元に変更）

新しい基本レジスターのための、および一方で国民／企業との、もう一方で政府機関との連絡、通信のための新アプローチを、図 2.32 で示している。

EGON というシンボルは、すべての者が利用できアクセスできる行政への到達方法を示している。

(4) チェコ共和国電子政府サービスの現在の利用状況

電子政府サービスは、それを使用する人がいて初めて有益なものになる。チェコでは、国民よりも企業部門のほうが、はるかに電子政府サービスの利用に前向きである。日本と同様、国民はより保守的であり、このことがすべての国で問題となっている。

現在の第一の問題は、全利用者の準備不足、知識不足がもたらしている。例えばある調査では、利用しやすい行政のシンボルである eGON は、チェコ居住者の 10%しかその意味を知らなかった。その多くは知識を持った若年層（18～44 歳）、および大学教育を受けた者だった。行政の事業をひとで表現する方法は非常にシンプルであり、分かりやすいと受け取られるはずたったが、人々へのプロモーションが不十分であった。同じ調査では、Czech POINT に対する質問も行っている。この場合には、比較的ましな状況となっている。2008 年には、50%が Czech POINT のことを聞いたことがあり、これは倍以上の増加を示している。Czech POINT の知識を持っていたのは、その大部分が大学教育を受けたインターネットユーザーである若年層（18～44 歳）であった。最寄の Czech POINT がどこかは、回答者の 28%が知っていた（2007 年には 10%しか知らなかった）。どのような施設が Czech POINT を提供するかは、知識を持つ者の 5 分の 3 が知っていた。その大部分は大学教育を受けた有知識者、プラハの住民、およびインターネット利用者となっていた。しかし、Czech POINT の実際の利用者となるともっと低い。チェコ住民の 10%しかこの設備を利用していなかった。またデータボックスは、新しい未経験のものとして受け取られていた。

それでも、データボックスについてある程度知ってる者は人口の 4 分の 1 に上り、その多くが大卒者および企業家となっている。公的文書をデータボックスを通じて配信できる可能性を便利と受け取る人は 36%いるが、しばらく時間が経過した後にレターが配信される場合には、利用意欲は低い（26%）。

「行政機関との電子通信に対する国民の準備度（Citizen preparedness for electronic

communication with public administration offices)」調査の結果は、国民はまだ電子政府に対して懐疑的だが、状況は好転していることを示している（図 2.33)。

電子通信を最も利用しているのは、主に大卒の若年層（15～29 歳）である。

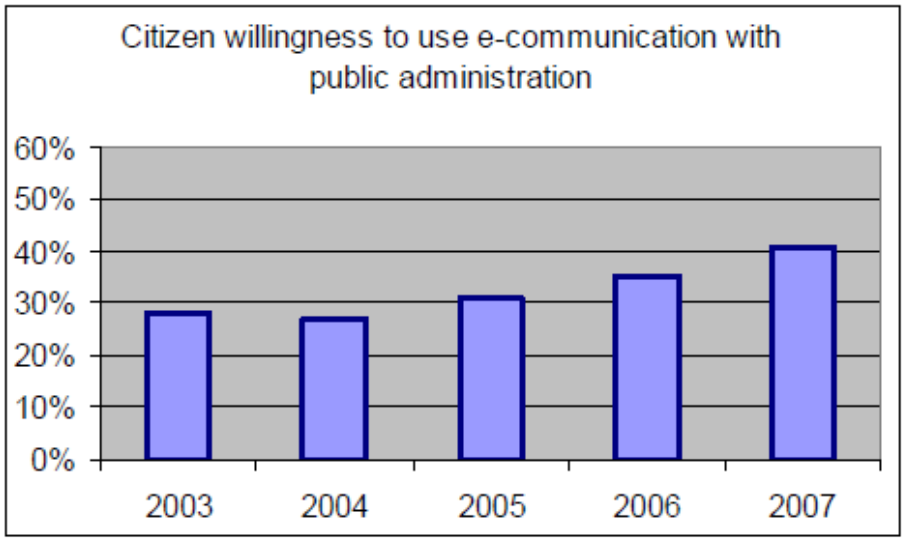


図 2.33：行政サービスで電子通信を利用することへの国民の意欲度（文献[233-1]より図を引用）

2.3.3.3　電子データ管理

上記の例は､電子政府サービスの利用を楽観的に示している｡この例を現実のものとするには、行政は 3 つの重要なツールを強化する必要がある。まず 1 つめに必要なツールは、申請書類や要請を提出するために信頼可能な場所（Czech POINT）である。行政機関からの応答を得るための、データボックスも必要になる。3 つめのコンポーネントとして挙げなければならないのは文書の電子化方法で、これが現在最も問題となっている。これら 3 つのパーツについて、以下でより詳しく説明する。

(1) 行政の窓口

官庁や公共機関とのコミュニケーションのためにもっとも便利な方法は、それが 1 つの場所、近くの場所から行えることである。そのための解決方法は、誰でも全官庁および公共機関と簡単に電子的に通信できる、汎用窓口の密度の高いネットワークを発達させることである。このような窓口場所を Czech POINT と呼び、これは「チェコ国提出・証明・情報端末（Czech Submission, Verification, and Information National Terminal)」を意味している。これは補助員付きの行政設備で、補助員は市民が登録所からの抄録を申請したり受け取ったり、申請書や文書を提出するのを補助する。これらの窓口場所は今後、他のサービスのを追加するため拡張されることになっている。この窓口は電子政府の一部として、1 つの場所からの、簡素化された行政とのコミュニケーションを促進する。また、過剰な官僚主義の低減が、これの付加価値となっている。これのサービスや機能は、徐々に拡大される予定である。

現在のところ、窓口場所はデータの検証や、文書および証明書（不動産登記、犯罪記録、会社登記などからの抄録）の公証を含めて、公共および非公共の情報システムにあるデータへのアク

セスを手助けしている。このサービスを、企業家登録への書類提出のために使用できる。また新しいサービスとして、このプロジェクトは公共調達手順に入札したい者の資格証明のための抄録を手助けしたり、ドライバー・ポイント登録の抄録を配布したりする。この設備は、理想的な行政窓口ポイントとしての自治体役場、郵便局、海外のチェコ大使館、公証役場、商工会議所などで設置されることになる。

将来的には、これの運営管理者は、サービスへのアクセスを Czech POINT 設備からだけでなく、便利であればインターネットを介しても可能にすることになる。多くの人が、各種の登録所から基本抄録を得るためとして、この場所を認識している。国民は、全く不必要にいろいろな機関をまわって何時間も待ったり、それらに出かけて行かなくてすむ。誰も、地方の土地登記所からの文書が必要なとき、休暇を取らなくてよいようになる。国民は、特定の登録所からの抄録を要請するために、本人が（郵便局や地方の役場にある）1 箇所の汎用窓口場所に出頭する必要がある。

(2) データボックス

データボックスのプロジェクトは、別の公的電子ツールを取り扱っている。

データボックスは「電子運用と認定文書変換に関する法律（Act on Electronic operations andauthorized document conversion, No. 300/2008 Coll.）」に基づき、2009 年 7 月 1 日に初めて導入された。この日付以来、データボックスは全法人（公共機関と、企業登録に登録されている企業）にとって強制使用となった。自然人と、企業家として登録している自然人は、要求した場合のみデータボックスを使用できる。

データボックスは、電子メール・ボックスとは異なっている。ユーザーは公共機関自体とのみ通信が可能で、特定の役人や自然人/法人との通信にこれを使用できない。データボックスは、ユーザーが公共機関とコミュニケートするのを援助するために設計された電子ストレージである。これを使用して、公共機関との間の文書の電子提出および受信が可能になる。従って、この電子通信はハードコピーの送付という従来のシステムに置き換わり、行政をより効率的、低コスト、迅速にするものとなる。

データボックスを使用して誰から誰に電子文書を送れるか					
所属		所轄の公共機関（中央/地方）	法人	（データボックスを持つ）個人の自営業	（データボックスを持つ）個人
	所轄の公共機関（中央/地方）	○	○	○	○
	法人	○	×	×	×
	（データボックスを持つ）個人の自営業	○	×	×	×
	（データボックスを持つ）個人	○	×	×	×

図 2.34：データボックスを介した通信方法（文献[233-1]の図を元に変更）

データボックスは、行政を簡素化、改善し、低コストにすることを目的にしている。データボックスは、サービス済み配信という新システムによって、処理が迅速に行われるようにする。つまり、このシステムではデータボックスに置かれた全配信は、置かれてから 10 日後にはサービス済みになっている。また上記の法律は、紙の文書と電子文書の両方が等しくみなされることも規定している。また、データボックスは別の電子ツールに接続されていて、これが紙に書かれた文書から電子文書への、またその逆方向の認定変換を行う。これは、公証人や地区／地域機関が電子署名を使用して行う。このような電子化文書には、変換の元になった原本と同じ法的地位が与えられる。この特別な電子文書は、情報へのアクセス許可、その流通、処理、アーカイブ保管、結果的損失などの問題も解決する。このプロジェクトでは地域および中央の機関によって約 7,000 のデータボックスが、また法人および自営業の自然人によって約 250,000 のデータボックスが使用されている。行政上の観点から見ると、主に所轄公共機関の間に新形式の通信設備ができたことになる。

データボックスに関係した今後のリスクはリスク・ダイアグラムとして表すことができ（図 2.35)、これを使ってリスクが階層型にカテゴライズされる。各リスクはそれぞれ、ただ 1 つのリスク・カテゴリーに属しており、各リスク・カテゴリーはそれぞれ、他のただ 1 つのリスク・カテゴリーに属している。あるリスク・カテゴリーが、同時に 1 つ以上のリスク／リスク・カテゴリーの上位に存在する場合もある。

このモデルは、あるリスクに関連したさまざまな状況を含むことがある。またそのリスクに対して、キーポイントとなる成績指標、およびリスクに対して実行する戦略を割り当てることができる。さらに目標、重要な要素、戦略やリスクに対する組織的な責任も付け加えられる。

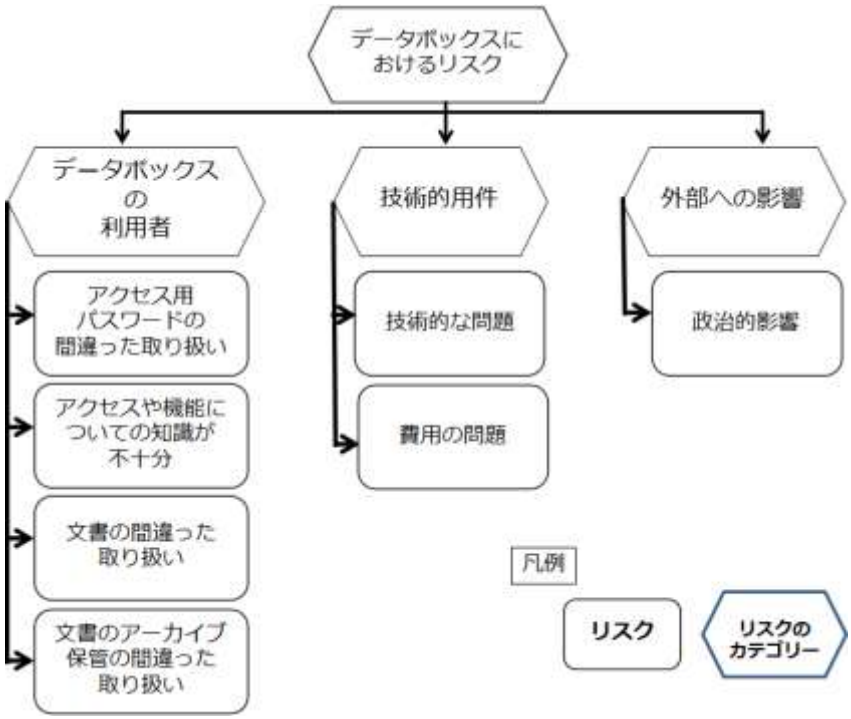


図 2.35：データボックスに対するリスク・モデル（文献[233-1]の図を元に変更）

(3) 電子文書

文書の新しい処理法は、電子メディアとして、考慮しなければならない 5 つの側面を持っている。

- 技術的側面としては、生成、配信、保管のための ICT 技術の使用法がある。
- 人的側面としては、新たな作業方法を使うための積極性と能力への妨げがある。
- 組織的観点では、組織は電子文書を取り扱うための規則を決める必要がある。
- 法的側面には、電子文書を紙文書と同等の法的正当性を持った等価物として受け入れることがある。
- 政治的側面は政府政策を変えられるため、前述の全側面に影響を与えることができる。

文書は書面、音声、視覚、その他いかなる方法で保存された情報でもあり得る。しかしアナログまたはデジタルにかかわらず、各々の文書にはその作成者がある。また、耐久性と一貫性は、文書の最重要の特性である。紙文書のシステムは、何百年にもわたって発展してきた。印判を押した署名付きの紙文書は、すべての文明化したコミュニティーで真性かつ信用できるとしてみなされている。紙文書は長期間にわたって読める状態を保つため、紙文書のただひとつの問題は、その安全な保管である。

文書に対する基本的要件は、紙の形で容易に満たすことができる。

・可用性：文書はいつでも使用できる必要がある。
・機密性：文書の秘密性の維持を保証できること。
・完全性：文書が変更されていないことを確認できなければならない。
・信頼性：文書の作者が既知であり、証明される必要がある。

電子文書の場合は、これらの要件を満たすのが難しいため、いくらかの法的、技術的障壁がまだ存在しており、それを解決する必要がある。

① 可用性、可読性、機密性

利用可能な文書は全情報が読み取り可能なように、適切なデータ形式で適切なデータ・メディア上に保存しなければならない。

電子文書の機密性は、要求された情報のあるデータベースへの、ユーザーによる許可に関係している。問題は、ユーザー・アカウントのあるデータベースが時間が経た場合、ユーザが抵抗することができなくなくなることである。すなわち、将来には文書の保護が期限切れになり、その文書が公開されるような状況が起こりうる。ユーザーによる許可が、文書内に置かれるようにする必要がある。

② 完全性、信頼性、法的な有効性

オンライン取引を導入するために、政府はその国の法律が、電子文書の有効性を認識するかどうかを考慮しなければならない。法律によれば、証明済みのデジタル署名によって署名されているか、または証明済みのデジタル社印、および同時に証明済みのデジタル時刻印がが押されていれば、文書は受け入れられる。この場合には、時間の経過によって問題が起こりうる。証明書はある時間の後に失効し、また、認証局は廃止される場合がある。時間経過における文書アクティビティーの問題は、非常に複雑である。文書はたとえば 20 年後に開封されることもあり得るし、

その文書は、過去の時点で有効だった署名により署名されたことが明らかでなければならない。このような状況で保証を確保する方法として、さまざまな可能性が議論されている。その１つに、データセーフとして働く機密のリポジトリを作る案がある。そこでの保管の後、電子文書は証明済みの機関によって処理される。この機関は署名が有効な時点で文書を受け付け、その文書を証明する。電子文書の信頼性を検査する間に、この機関はその証明書によって、当該文書が変更を受けていない原本であることを保証する。

もう１つの可能性として文書の再署名があり、この場合には、証明書が失効する前に文書は再署名される必要がある。このような手続きは積極的保存(active preservation)と呼ばれている。

③　情報のオーバーロード

他にも、どのような情報が保存する価値があるのかという問題もある。大量の情報と変化によって、役人はその生産性を維持するのが難しくなり、また意思決定の際に、現在の全要素を確実に考慮することも困難になる。特定の文書は法律に基づいて保存する必要があるが、運営上の性格を持っていても、時間が経つとその重要性がなくなる文書も多くある。従来の世界では、無用の情報は自然と消えてゆく。電子文書はより簡単にアーカイブされるため、諸機関はどの情報を保存する必要があるか決めるための、情報監査を受ける必要がある。さらに、政府関連機関はデータを分析して、それを「アクショナブル・インフォメーション」に変換するためのテクノロジーを用いる必要がある。情報は系統的で明白な、利用可能な方法で提示されない限り、知識に寄与できないからである。効果的で分析的な能力を創出するには、政府の指導者はテクノロジーやデータに投資するだけでなく、組織的文化、業務プロセス、および職員の振る舞いを変化させる、運営革新にも投資しなければならない。

2.3.3.4　課題

国民は電子ツールの助けを借りて行政機関とコミュニケートする意思があり、この意思はさらに高まっている。このような傾向を利用するのは有用で、また必要なことである。しかし、国民に用意がある一方で、行政とのコミュニケーションに電子ツールやサービスが実際に利用されているのかの問題がある。コミュニケーションのための利用意思と、実際のコミュニケーションとの差は、大まかに見て３倍ある。現在のところ、国民と行政機関の間の電子的コミュニケーション方法として成功しているツールは、Czech POINT サービスである。このサービスが同時に、電子政府の伝道者、既存の機能と新たな機能の仲介者、電子政府サービスの長所とメリットの広報役としても働けることは重要である。現在の電子政府プロジェクトである、データボックスの設置と中央レジスターの再構築は、国民から積極的な反応を得ている。

しかし、これら新たな機能性は主に行政機関職員の部門で伝えられているだけで、国民の間での、このトピックに関する周知度は低い。このことは、一般市民による、これらの利用を遅らせる可能性がある。これらの新行政サービスについて周知度が低いことは、国民が新行政サービスの枠組み内での、その個人データのセキュリティーに関して不安を抱く理由になる可能性がある。空間意思決定でのデータボックスの利用は、特に地方機関の観点からは役立つものの、国民の観点からの利益度は低い。

電子文書の法的有効性は、いまや紙文書におけるのと同等である。しかし、紙文書の持つ基本

特性は、電子文書によって簡単に実現することはできない。その状況はまだ明確ではないが、電子政府サービスの真の利用のためにはその解決法が必要である。

【文献】

[233-1] ″eDocument in eGovernment″ STANISLAVA ŠIMONOVÁ, HANA KOPÁČKOVÁ
WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, Issue 1, Volume 7, January 2010
[233-2] ″Czech Republic Country Report″ ENISA, January 2010

【付録】

関連の法律　出典［233-2］

［データ保護／プライバシーに関する立法措置］

データ保護法（Data Protection Act、No. 101/2000）が、2000 年 4 月に、国民のプライバシーの権利の保護を目的として採択された。この目的を達成するため、本法では、個人情報の処理に関する権利と義務を規制している他、個人情報の他国への移管条件も明示している。また、各個人が公共団体や民間団体が保有している自身の個人情報を入手並びに訂正することも認めている。本法は、個人情報保護局（Office for Personal Data Protection）によって執行されている。

［電子通信に関する立法措置］

『電子通信並びにその他の法改正に関する法令（Act on Electronic Communications and on Amendment to Other Acts)』が、2005 年 2 月 22 日にチェコ議会で採択され、2005 年 5 月 1 日より施行されている。本法は、EU の電子通信に関する規制の枠組み（EU Regulatory for Electronic Communications）を国内法に置き換えるものである。

［電子署名に関する立法措置］

電子署名法（Electronic Signatures Act、No. 227/2000）が、2000 年 6 月 29 日に採択され、2004 年に改正されている。本法は、各種個別条例と共に、電子署名に法的価値を明確に与えるために、電子署名のためのコミュニティの枠組みに関する EU 指令（1999/93/EC）を置き換えるもので、民法の各種規定を改正するものである。

指令（1999/93/EC）の置き換えに加えて、本法では、2 種類の国独自の手法（電子マークと適格タイムスタンプ・トークン）についても定めている。電子マークは、自然人と法人の両者に対して発行可能な適格システム証明書に基づく。電子マークは電子署名と同じ技術をベースとしているが、電子署名と違って、電子署名は、情報システムなどによって自動的に作成することも可能である。適格タイムスタンプ・トークンは、ETSI TS 102 023 に準拠して発行される。

［電子政府に関する立法措置］

① 情報社会サービスに関する法令（Act No. 480/2004 Coll., on Certain Information Society services）が、2004 年の終わりに承認されている。本法では、スパムに対処すると共に、伝達情報のコンテンツに関するプロバイダーの責任を限定している。本法は、電子商取引

の発展の妨げとなる障害を除去するための政府の取り組みに追随している。

② 電子的な行為および文書変換の認可に関する法令（Act No 300/2008 on Electronic Actions and Authorised Document Conversion）が、2008 年 7 月 17 日に採択され、2009 年 7 月 1 日より施行されている。本法では、電子文書とハードコピー文書に同じ法的地位を与え、ハードコピー文書の変換を認め、認定電子署名の使用に関する規定を明示している。

③ 電子政府法（eGovernment Act）の目的は、国民、企業、公的機関の間のやり取りを簡素化すると同時に、大幅な節約を実現することにある。本法では最初に、ハードコピー文書の電子フォーマットへの変換を予見している。電子変換に紙版と同じ法的地位を持たせるためには、認可を受けた機関（公証人、地方機関、市町村当局）が原文を変換する必要がある。

さらに、本法では、各電子文書には、認定電子署名に加えて、文書の署名日時を示すタイムスタンプを付与する必要があるとしている。公的機関とのやり取りでは、認定電子署名は、公文書の証明において自筆署名と同じ価値を持つものとする。

本法に盛り込まれているもう 1 つの革新的な技術が、公的機関との間でやり取りされたすべての電子通信の個人記録簿である、いわゆる「データ・ボックス」である。チェコ共和国内の法的実体はすべて、2009 年 11 月までにデータ・ボックスをそれぞれ設置して、使用できるようにする義務を負うものとする。各データ・ボックスは、パスワードで保護され、アクセスするには認定電子署名が必要である。自然人は、自身のデータ・ボックスを任意で開き、そこに含まれている文書を公的機関とのやり取りに使用することができる。

［機密情報の保護に関する立法措置］

機密情報の保護に関する法令(Act No. 412/2005 on the Protection of Classified Information)。本法では、機密情報とする情報を決定する際の原則、機密情報へのアクセス条件、機密情報の保護に関するその他の要件、国家機密に関わる行為並びにそれらの履行および関連する国家管理の実施に関する条件を規定している。

［危機管理に関する立法措置］

危機管理並びにその他の法改正に関する法令（Act No. 240/2000 Coll., on Crisis Management and Amendments to Certain other Acts、危機法（Crisis Act))、統合緊急通報システム並びにその他の法改正に関する法令（Act No. 239/2000 Coll., on the Integrated Emergency System and Amendments to Certain other Acts, as Amended)、さらに、危機管理に関する政府規制（462/2000 Coll.)。

2.4 調査のまとめと考察

以下では、今回の欧州調査のまとめと、利用者が安心して使うことができる電子文書等のビジネス記録の利活用基盤の構築に向けた考察を行う。

2.4.1 訪問各国の電子記録保存システムの比較

今回訪問調査したデンマーク、ハンガリー、ドイツの各々の電子記録保存システムの比較を表2.9に示す。併せて、韓国の公認電子文書保管所の現状を参考のために掲載する。

システムのアーキテクチャについては、いずれもサービス志向となっており、インタフェースはSOAPを適用している。電子記録保存システムの定義範囲はそれぞれ異なる。デンマークのシステムはCASE管理の一部までをカバーするのに対して、ハンガリーやドイツのシステムは低レイヤの、いわゆる文書保管に限定している。具体的には、CASEという管理対象を電子記録保存システムの中で定義するか、外付けとして位置付けて、連携のための仕組み（連携のためのメタデータ）を用意するかという違いである。

各システムに共通する項目として、文書にユニークなIDを付与し、このIDで文書やパッケージを管理していることが挙げられる。

パッケージ構造については、各システム独自に仕様を定義しているが、大きくは2つの流れがある。デンマークの FESDⅡがデータベース上で仮想的なパッケージを定義しているのに対して（つまり、関係性の定義だけがある）、ハンガリーのDossieやドイツのArchi Safeでは、論理的な構造をもっている（つまり、入れ物を用意して、その中に文書やメタデータなどを入れる構造をもっている）。欧州全体がXML志向であることもあって、メタデータはXMLで記述されるところが共通している。

長期保存に関しては、流動性の高い文書に対しては、個々の文書にタイムスタンプを付与するCAdESやXAdESに基づくタイムスタンプを、ストックされる文書には一括タイムスタンプ方式であるLTANSを用いるという使い分けがなされている。

表2.9：訪問各国の電子記録保存システムの比較（調査結果から筆者作成）

項目		韓国（参考）	デンマーク	ハンガリー	ドイツ
システム/プロジェクト		CeDA	FESDⅡ	－	ArchiSafe
保存対象文書		私文書	公文書	公文書/私文書	公文書
利用者		個人、企業	政府機関、個人（ポータル経由）	現時点では法曹関係中心	政府機関（予定）
アーキテクチャ		OAIS準拠	SOA	Dossieのネスト構造	独自3層構造
要件定義		法律で規定	中央、県、市町村横断的委員会で決定	省庁別縦割り要求	プロジェクト独自
技術	文書ID	階層型、保管所IDを認定機関が管理	UUID	ハッシュ（SHA256）	UUID
	パッケージ構造	OAISを拡張	メタデータで関連付け	独自形式（Dossie）	独自形式（XML）

	メタデータ	ISO23081 を拡張	ISO23081 を拡張	独自形式 (Dossie)	独自形式 (XML)
	長期保存	(AdES)、WORM	署名なし、TIFF	AdES、LTANS	AdES、LTANS
運用		事業者	民間に委託	官民協同	(未定)
標準化		NIPA (認定機関) が仕様提示	管理面、技術面の 7 分野の政府標準	デファクト標準	連邦政府標準 BSI TR 03125
備考		記録の保管＋流通にシフト	CASE 対応		導入政策未決定

2.4.2 ビジネス記録の利活用基盤のあるべき姿

日本には､今回訪問調査対象とした､基盤となる電子記録保存システムは存在しないことから、以下では、欧州調査結果をもとに、利用者が安心して使うことができる電子文書等のビジネス記録の利活用基盤のあるべき姿を考察する。

ビジネス記録の利活用基盤にとって重視すべき点は、3 つある。第一は、安心・安全なシステムの提供である。言うまでもないが、企業または組織の重要な電子記録が安全に保存され、電子記録を安心して活用できるものでなければならない。

第二は、システムの相互運用性確保である。企業内、更には企業間で電子記録の流通を可能にするためには、さまざまなアプリケーションから、必要な記録が保存された電子記録保存システムを自由にアクセスできる必要がある。そのためには、必要最小限の標準化は欠かせない。

第三は、真の業務効率化に寄与することができるシステムである。電子化しても電子記録保存システムが、単なるファイルの保管庫では業務効率化は望めない。真の業務効率化に寄与するには、業務プロセスと密接に連携するシステムであることが求められる。グリーン IT 推進は、真の業務効率化を実現して初めて現実のものとなる。

以下、各々について考察する。

2.4.2.1 安心・安全なシステムの提供

電子記録保存システムは IT システムの一環であり、IT システムに求められる、いわゆるセキュリティ要件を満たすことは最低限必要である。この意味でのセキュリティ要件に関しては、電子記録保存システムに限った問題ではないので、ここでは触れない。

安心・安全の観点から、電子記録保存システムとして考慮しなければならない問題（これは、紙の記録も同じであるが）は、ISO15489-1 にあるように、電子記録の真正性、信頼性、完全性、利用性の確保である。

［真正性］

今回の調査によって得られた知見として、真正性の確保については、文書への署名やタイムスタンプも重要であるが、記録の作成、取得、送信、維持及び処分を管理する方針並びに手順を文

書化し実施することもまた、同じように重要である。もっとも、日本では署名やタイムスタンプに関して、次のようなそれ以前の問題がある。

① タイムスタンプの法的裏付けがない。また、ドイツのように、認証局が事業を停止した際に、他の認証局がその業務を引き継ぐなどの法律がない。日本では、電子署名法が施行されたのち、タイムスタンプや電子署名に関する法律の充実は、十分進んでいるとはいえない。

② 欧州では、電子署名の効果や検証方式を署名ごとに定める「署名ポリシー」の標準ができつつあり、署名を効果的に利用できる環境は整いつつあるが、日本では対応できていない。

欧州各国では、紙の文書の時代から管理面が整備されていたという土壌はあるが、各国とも電子文書についても必要なルールが整備されている。特に英国は、記録の入手、保管、評価選別、最終処分に関する方針、分類体系の設計や記録の選択に関するガイドライン、実施要領などが体系的に整備され、かつ TNA（英国国立公文書館）によって公開されており非常に参考になる。

日本では、参考となるガイドラインもなく、一部の例外的な企業を除き、電子文書に対してはこの対応が立ち遅れているのが現状である。

［信頼性］

次に、信頼性であるが、ISO15489-1 にあるように、これは活動過程の証明であり、電子記録保存システムが業務フローと密接に関係付けられていることが求められている。80%の文書は、企業または組織の非定型な業務から発生するといわれている。欧州各国での非定型業務への対応の流れは、CASE マネジメントであるといえる。

電子記録保存システムと CASE マネジメントの連携方法には対局をなす 2 つの方法がある。一つは、デンマークが採用している方法であり、電子記録保存システムが CASE マネジメントに必要な機能を取り込んでいる。いま一つは、ドイツや英国が取り入れている方法で、電子記録保存システムは、CASE マネジメントとの連携に必要なリンクだけを用意し、上位のアプリケーションで対応するという方法である。

いずれの方法を採用するにせよ、デンマークの仕様は CASE ファイルの管理や記録と CASE の関係付けなど、参考になる点が多々ある。

［完全性］

完全性は、その内容が完結していて変更されていないことを意味する。記録は、許可のない変更から守られなければならないが、記録作成後どんな追加又は注釈が許されるのか、どのような状況で追加又は注釈が許される場合があるか、だれに追加又は注釈を入れる権限があるのか、追加、注釈又は削除をどのように明示し、かつ追跡可能にするかは、記録管理の方針と手順の問題となる。署名やタイムスタンプに加えて、権限管理が重要となる。

情報の流通を考えると、権限管理は局所にとどまらない。電子記録保存システムと ID 管理や ID 連携とのかかわりが非常に重要なテーマとなるが、今回調査した範囲では、日本の現状にとって参考になる事例は見当たらなかった。

［利便性］

最後に利便性であるが、より広い業務の活動又は機能のコンテキストの中で、記録を見つけるという点に関しては、業務分類体系もさることながら、前述のように 80%が非定型業務であることを考えると、デンマークのような電子記録保存システムに CASE マネジメントを取り込み、CASE

と記録を関連付けることによって、一連の活動を文書化した記録間のつながりを維持する方法は一考に値する。

また、プライバシーについては、日本では個人情報保護法で守られているが、個人情報を活用するとなると、個人情報保護法が障害となっている。

例えばエストニアでは、データ保護法に個人情報の扱いを 3 つのレベルに分け、かつその利用についても、法律に記述している。

2.4.2.2　システムの相互運用性の確保

今回調査した範囲ではあるが、電子記録保存システムはいずれもサービス志向であり、これは大きな潮流であると解釈できる。

［インタフェース］

相互運用性の観点からみると、今回調査した範囲では 2 つの考え方があることが分った。一つはドイツの ArchiSig プロジェクトの考え方で、電子記録保存システムにアダプタを前置し、既存のアプリケーションに対してインタフェースの互換性を保証している。

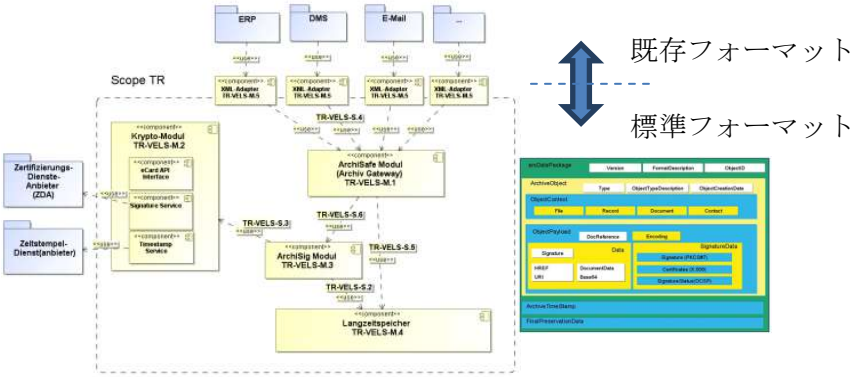


図 2.36：ArchiSafe における互換性の考え方（文献[223-1]より図を作成）

いま一つは、エストニアの X-ROAD で採用された考え方で、電子記録保存システムにアダプタを前置することまではドイツの ArchiSig プロジェクトと同じであるが、狙いは逆で、既存の電子記録保存システムに対してインタフェースの互換性を保証している。業務プロセスを再構築することが前提になっている考え方であるといえる。

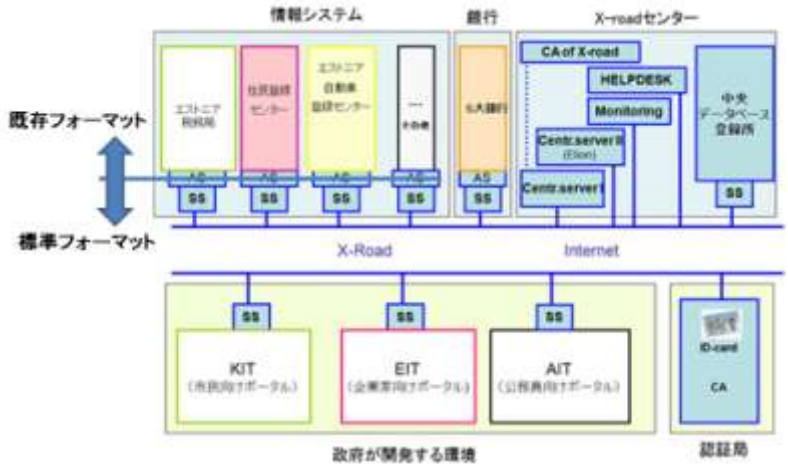


図 2.37：X-Road における互換性の考え方（図 2.24 に加筆）

［CASE の位置付け］

今回調査した各国の電子記録保存システムは、欧州における記録管理の動向で述べた、電子記録管理に関する雛形要件の MoReq2 が基礎となっている。電子記録保存システムが提供するサービスのレベルに関しては、CASE を取り込むか否かで大きく異なるが、これは、MoReq2 での位置付けと同様、基本部分と CASE 対応のオプション部分があると解釈すると整理できる。

今後、非定型業務領域へのシステムの適用を考えると、CASE は、必須（Shall）、または必須ではないが提供することが望ましい（Recommended）という位置付けになると考えられる。図 2.38 にデンマークの FESDⅡシステムのアーキテクチャを再掲する。CASE、文書、アーカイブがコアとなっており、これは手本の一つになると考えられる。ここで、ダイアログレイヤーは、利用者との Web インタフェース、プロセスレイヤでは案件対応の業務プロセスが動作する。

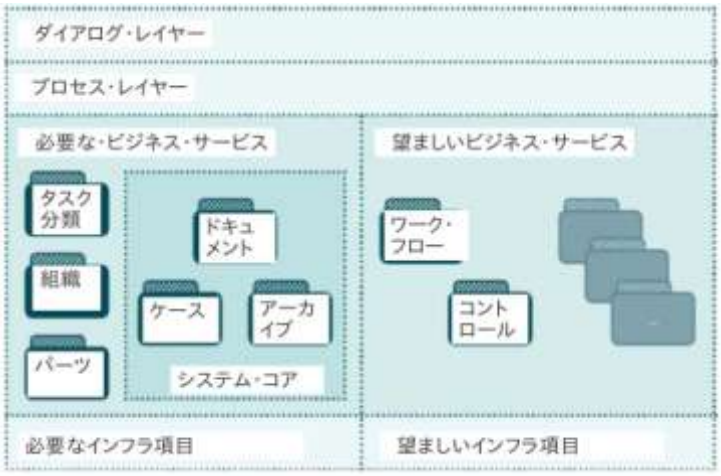


図 2.38：デンマークの FESDⅡシステムのアーキテクチャ

［パッケージ］

相互運用環境においては、電子記録保存システムが電子記録をハンドリングする単位はパッケージとなる。電子記録保存システムの利用者にとっても提供にとっても相互運用性保証の単位となる。パッケージはまた、システム間での記録の Export/Import の単位ともなる。今回の調査範

囲では、メジャな、つまり大勢を占めるような、パッケージ仕様は見当たらなかったが、いずれもセマンティックレベルでは非常に似たものとなっている。これは、前述の各国の電子記録保存システムの比較で述べた通りである。

図 2.39 に ArchiSafe のパッケージ構造を再掲する。パッケージは XML で記述され、タイムスタンプ（LTANS による一括タイムスタンプ）で保護されている。

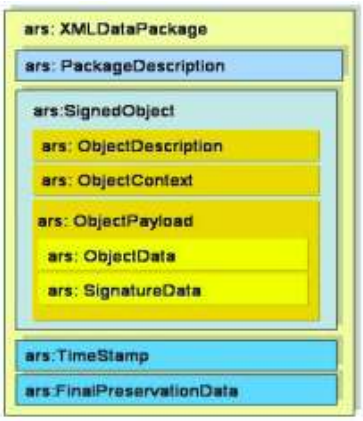


図 2.39：ArchiSafe のパッケージ構造（調査結果から筆者作成）

［ユニーク ID］

パッケージの ID については、今回調査対象の各システム（Dossie を除く）に導入されている ISO 標準の UUID を適用することで問題ないと考えられる。

［セマンティックの相互運用性］

もう一つ重要なことは、セマンティックな相互運用性、つまり用語とその対象との対応づけである。例えばある国の「ナース」が一部の医療行為を許されていると、日本語と対応づける場合「医師」となってしまう。セマンティックな相互運用性については、日本においても、貿易関係など、一部進んでいるところもあるが、日本語の問題でもあり、官民連携した検討を行う必要がある。

2.4.2.3　真の効率化への寄与

この件は非常に難しい問題を抱えている。電子記録保存システムを導入したからといって業務の効率化が図れる訳ではない。デンマークやエストニアの例を見るまでもなく、業務の改革、組織の再編、記録の電子化の相乗効果として効率化が実現できている。また、高度な専門人材の存在も欠かせない。

ここで、業務の改革そのものの議論は、本調査検討のスコープを外れるが、記録の電子化に関して、日常業務のルール、電子化に対するリテラシの向上、専門人材の育成については、ベストプラクティスを学び取ることができる。

［電子化推進の観点］

今回の調査での印象では、欧州は行政を中心に情報の管理・利用を電子文書に移行しようとし

ている。BtoG に関連する業務における文書の扱いは官主導になることから、民間だけでの電子文書への移行は困難である。

現在は、移行期間であり、例えばデンマークでは市町村の市民からの受付等は、インターネット以外に、FAX 及び紙での提出が半数を超えるが、窓口業務としてそれらを電子化して、バックオフィスには、紙が回らないようにしている。

日本では、e 文書法で「電子的に管理しても構わない」文書の種類が広がっただけで、積極的に電子文書を利活用する動きは目立っていない。

［教育の観点］

英国では、「2.3.2.9　専門教育」で説明した通り、記録管理の専門人材を大学で育成（フランス、オーストリア、ドイツは、国や国立公文書館が育成）しており、研究機能も持っている。記録管理の専門課程は、ロンドン大学をはじめ 7 大学に大学院レベルの学科があり、定員は 7 大学合わせて凡そ 200 名である。デジタル保存を扱うグラスゴー大学のような大学もある。

エストニアにおいても、eGOV アカデミーが中心になって、国内だけでなく、周辺の国に対する教育支援を行っている。

一方、日本においては、学芸員、図書館司書の資格がある程度で、電子文書の管理に関する資格はもちろん、高校大学のカリキュラムとしても取り上げられていない。最近になって学習院大学や岐阜女子大学においてデジタルアーカイブを担当できる人材の教育を行っている程度である。

第3章　提言

情報の保管、流通、活用といった面から考えると、現在は文字の発明、紙の発明、印刷技術の発明に続く、大きな変革の時代を迎えている。

これまで述べてきたように、欧州各国では従来の紙を媒体として進めてきた社会（紙文書社会）から、電子的な媒体とインターネットを駆使した社会（電子文書社会）への移行のため、多くの試行を重ねてきている。

日本においても、文書の作成および社内（組織）での流通については電子化が進んでいるが、社外との正式文書の交換や保管については、まだまだ紙が使われているケースが多い。

これまで、平成 13 年の情報公開法、公文書管理法、平成 17 年ｅ文書法などが成立しているが、これらはいずれも、情報の保管、流通、活用は紙文書社会を前提としており、電子文書の保管も許容するという立場にとどまっている。すなわち、電子文書の保管、流通、活用が一応可能になってはいるが、電子文書の安全かつ効率的な利用環境が整っているとはいいがたく、積極的に紙文書社会から電子文書社会に移行しようとするものにはなってない。特に、欧州でも問題としてあったのだが、紙文書社会にくらべて電子文書社会では、情報が跡形なく消えてしまう可能性があることから、情報を電子的に保管することに対して不安が大きいことも、移行の促進を阻んでいる。

こうした不安を払しょくするとともに、電子文書の活用を促進するために今後必要なものとして、安全で信頼性の高い電子データ保存システム及び同システムの保存データを高い信頼性のもとで安全に活用するシステムがあげられる。以下、このようなシステムの実現に向けて早急に検討すべき項目について、技術面、運用面、制度面から提言を行う。

3.1　制度面での提言

(1) 個人情報の活用を推進するための個人情報保護法の見直し

電子文書保存において、個人名や職責など個人情報をメタデータに利用することになるが、個人情報保護法に触れるのか、利用者にとって不安な面がある。

そこで、電子文書保存における個人情報の扱い、本人への利用確認方法の明確化などの電子文書保管における個人情報の扱いに関する制度あるいはガイドラインを策定し、利用者が安心して使えるシステム及び環境を実現すべきである。

(2) 電子文書保存サービス業者に対する認証制度

①　電子文書保存サービス事業者について、認定制度を作り、(可能な範囲で) 民事訴訟上の推定規定も設けるべきである。サービス事業者に可能なことは、対象文書の受領日時と、対象文書の内容だけであって、対象文書の作成者等に係る成立の真正は、作成者等の電子署名を用いる。

②　原本は改ざんされないよう確実に保存しなければならないことを、法律に明記すべきである。このためには、電子署名のように改ざんを検知する仕組みに加え、改ざんされない仕組み（Write Once Read Many）の利用を明記する。

③　電子化文書の保存にあたって、紙文書を原本として保存する必要をなくす法制度を拡充すべきである。特定の条件を満たす環境で電子化された場合、ある期間を経過した後、紙の保存を不要とする制度を拡充することが必要である。

④　電子文書における原本の定義を明確にした上で、認定電子文書保管所に預けた文書を原本とするための制度があってもよいのではないか。この場合原本とするための、特定の条件を満たす環境の認定制度が必要となる。

(3) 電子署名法の改定・タイムスタンプの法制度化

電子文書の長期保存のためには、電子署名、タイムスタンプが有効な技術として使われている。

日本では、電子署名法も施行から 10 年近くたっているが、まだ大幅な見直しがされていないために、いくつか問題が上がっている。

・現在、タイムスタンプに係る法律がないため、時刻に関する真正性の保証が行われていない。タイムスタンプを広く普及させるため、タイムスタンプに関する法律を作るべきである。

・電子署名・タイムスタンプ　特に、長期対応への国の担保も法律に含めるべきである。例えば、民間の認証局がサービスを停止した場合の対策なども法律に含めるべきである。

・文書保管などの場合、個人ではなく、企業職責による署名が必要になってくる。すなわち、個人の責任としてではなく、役職として作業を行う場合が多いため、現在の自然人に対する証明書だけでなく、企業職責に対する証明書を検討すべきである。

(4) グリーン IT 推進に関連した電子文書推進の制度の検討

紙文書から電子文書への以降は、低炭素社会の実現にとっても、極めて有効なものである。

実際、韓国では、国のプロジェクトであるグリーン IT 推進の中に、ペーパレス社会の実現を取りこんでいる。日本でも「電子データ保存」を低炭素社会を目指した施策の一環として位置付けることにより、文書の電子化を推進するともに低炭素社会の実現に貢献することが可能であると考えられる。なお、低炭素社会実現への寄与を前面に打ち出すことにより、経営者にとって電子化に取り組むインセンティブにもなると思われる。

3.2　運用面の提言

(1) 教育及び資格制度の作成

日本において、情報教育は大学、高校では積極的に推進されているが、その一環である電子データ管理教育は、いまだ十分とは言えない状況にある。電子データ管理教育の不足が、日本における電子文書の進展を妨げる要因の一つになっており、早急な改善が望まれる。

電子データ管理教育の推進にあたっては、以下の 3 点に重点を置いて検討すべきである。

①　電子データ管理者教育を高校・大学と連携して行う。

②　社会人ユーザを対象とした資格制度を作る。

③　専門家の要件／コアコンピタンスに向けた教育・資格制度。

(2) 中小企業が利用しやすい運用

大企業においては、電子文書保存のための設備や要員を確保することは可能であるが、中小企業に専用設備や専門要員の設置等の負担を求めることは難しい。

従って、中小企業にターゲットを当てた電子文書保管サービスの利用方法とそれを実現するビジネスモデルを検討すべきである。この場合、単に保管だけでなく、どのように情報が活用できるかがポイントとなる。

(3) 日常業務の中での電子化

日常業務において、他社、あるいは他組織から紙で書類を受け取ることは多い。その紙を受け取った段階で電子化し、日々発生する取引情報の電子化を推進するべきである。この場合、電子化作業を TTP（信頼できる第 3 者機関）で行う場合は問題ないが、社内組織で行う場合の社内規定、業界規定を検討すべきである。

(4) 情報流通のルール作成

範囲・期間を限定して、特定の相手へ開示することを可能にしていくことが、必要と考える。例えば、監査、デューデリジェンス（M&A における対象会社の調査）を外部の弁護士や会計士が行う場合に、保管されているデータの一部を、一定期間だけ、弁護士・会計士等に開示することにより、監査等の場所的制約を緩和する仕組みを提供すべきである。

(5) 価格設定の検討

現在の電子公証制度は日付情報の付与に 700 円、保存に 300 円を要する[1]など、日常的な使用のためには高額である。したがって、電子データ保存システムの利用を促進するためには、電子公証制度にくらべて、極めて低廉な料金を設定すべきである。

3.3 技術面に関する提言

(1) パブリッククラウド活用の検討

電子文書保存システムの運営コストは、同システムの普及発展の大きな要素である。運営コストを下げるためには、クラウドコンピューティング環境の活用が必要である。低価格化にあたっては、特に、海外の安価なパブリッククラウドを利用することが有効であるが、このようなクラウドを安全かつ高信頼に使うためには「パブリッククラウド高度利用技術」の確立が必要となる。

具体的なテーマとしては、例えば、暗号や秘密分散方式の活用、及び、利用者サイドでの暗号化、復号、及び鍵管理等を行うメカニズムの実現を検討すべきである。

(2) 相互運用性の確保

相互運用性の確保は必須である。

特に文書保管サービス業者のサービス停止に伴うデータの委管を可能にすることは、電子文書

[1] http://www.koshonin.gr.jp/de2.html

保存サービスでは必須であり、標準のパッケージ構造を決めると共に、代表的な非標準との変換ツールも検討すべきである。

(3) 表現方法の統一化の検討

電子文書保存の際のメタデータに入れるべき各種情報の表現方法の統一化を図るべきである。この表現方法の統一化については、財務諸表に使われる用語などすでに多くの分野で検討が進んでいるが、電子文書保存の際に必要となる

3.4 その他の提言

(1) 残存リスクの見える化

社内の文書保存媒体（電子、紙、マイクロフィルム、など）および保存状況から、どういったリスクがどの程度残っているのかを示す、見える化技術を導入すべきである。

残存リスクの明示の度合いは､データ保管サービス業者の評価にも使えるようにすべきである。

(2) 世界戦略を立てるべき

データ保管システムは、利用者が多分野にわたり、世界各国でニーズがあることから、Google Docs などとの違いを明確にしながら、利用できる基礎技術が本当に自国にあるのか、差別化要素を多分に持っているのか、この技術であるが故に可能なことは何か、他の技術との親和性はどうか、等を考え、世界戦略を立てる上で必要な事項の検討に至急、取りくむべきである。

(3) 海外製品・食品の輸入時の安全に関するデータ・ドキュメントの電子提出

TPP（環太平洋戦略的経済連携協定）への参加が検討されているが、導入条件としてユーザを守るためにも海外製品・食品の輸入時に安全テストの評価結果を電子データで受け取り改ざんが行われないように、信頼できる第 3 者機関が保管する仕組みを早急に検討する必要がある。

(4) 提供者にメリットのある情報提供モデル

情報を開示する側が、自ら進んで開示するビジネスモデルを構築してもよいのではないか。すなわち、開示した情報を、管理側が運用し、その運用で益が出ると配当とか利子のように、その情報を開示した者に益の一部が実際に振り込まれるものである。

これであれば、最初から情報の利活用を前提とした情報提供であるため、当事者間で事前の合意が容易であり、面倒な法的な確認も相当省略できる。従来、個人情報保護等で問題となっているような個人から情報を奪い管理するモデルを脱却し、個人に積極的に情報を開示させ、運用委託させるようなビジネスモデルに頭を切り替えて考えるべきである。

平成 22 年度電子データ保存システム検討委員会　委員名簿

		氏名	所属・役職
1	委員長	辻　秀一	東海大学　情報通信学部　組込みソフトウェア工学科 教授　工学博士
2	委員	保倉　豊	グローバルフレンドシップ株式会社　代表取締役
3	委員	溝上　卓也	株式会社日立ソリューションズ　経営企画統括本部
4	委員	宮地　直人	有限会社ラング・エッジ　代表取締役
5	委員	佐藤　雅史	セコム株式会社　IS 研究所 基盤技術ディビジョン　ネットワークセキュリティグループ
6	委員	宮崎　一哉	三菱電機株式会社 情報技術総合研究所　情報システム構築技術部
7	委員	西川　康男	ARMA 東京支部　理事長
8	委員	今別府　昭夫	株式会社ジェイ・アイ・エム　代表取締役社長
9	委員	牧野　二郎	牧野総合法律事務所　弁護士
10	委員	宮内　宏	ひかり総合法律事務所　弁護士
11	事務局	大崎　宏	財団法人日本情報処理開発協会　電子情報利活用推進センター 副センター長
12	事務局	木村　道弘	財団法人日本情報処理開発協会　電子情報利活用推進センター 主席研究員
13	事務局	前田　陽二	財団法人日本情報処理開発協会　電子情報利活用推進センター 主席研究員

平成２３年３月発行

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３－５－８
機械振興会館内
ＴＥＬ　０３（３４３６）７５００

印刷所　新高速印刷株式会社

東京都千代田区神田岩本町 15 番地 4　山上ビル東館 1F
ＴＥＬ　０３（６２０６）８９５８

23-H009