電子記録応用基盤に関する
調査検討報告書 2010

-クラウド時代の安心安全な電子記録管理-

電子記録応用基盤フォーラム（eRAP）

平成 23 年 5 月

一般財団法人日本情報経済社会推進協会

序　文

本報告書は、一般財団法人日本情報経済社会推進協会の電子記録応用基盤フォーラムが平成22 年度に実施した、電子記録管理システムの調査、および電子記録管理システム構築のための電子署名等の基盤技術に関する調査検討の成果を取りまとめたものである。

現在、電子空間における情報の生成、利活用は様々な社会において急速に普及してきている。こうした中で、「情報の信頼性」、「安全な保管」、「安心できる取扱い」を保証できる仕組みを確立することが喫緊の課題といわれて久しい。

電子署名は IT 社会における重要な基盤技術のひとつであり、わが国でも電子署名を利用できる環境が整いつつある。しかしながら、わが国における電子署名の保有及び利用者の数は、韓国などアジアの国に比べても比較にならないほど少ない。その理由のひとつとして、電子署名の利用に関する多面的な検討が進んでいないことがある。また、「個人情報の保護に関する法律」が平成 17 年 4 月に全面施行され、また、平成 21 年 7 月には公文書管理法が制定され、国だけではなく社会全体における新しいレコードマネジメントの構築が叫ばれている。企業においても新しい法規制や国際競争力の維持・拡大の必要性から新しい電子記録マネジメントシステムの構築が叫ばれている。情報セキュリティに対する取組みも積極的に行われているが、電子記録に関する利活用面では不十分な状況にある。

このような状況を打ち破っていくためには、安全安心技術の活用が必要不可欠な分野において、システム設計側が電子署名や個人情報保護技術を安心かつ簡易に導入できる環境を整備するとともに、導入・活用事例を積み重ねていくことが重要である。

この主要な分野として、電子記録マネジメントがある。今、日本の企業に求められている重要な課題として、企業活動の効率化・透明化、企業秘密の流出防止があり、企業の競争力強化を内外で図る上において、電子記録マネジメントシステムの普及促進は必要不可欠である。電子記録応用基盤フォーラムはかかる状況に鑑み、ECOM 設立以来十数年にわたって蓄積された電子署名、タイムスタンプ、個人情報保護、ID 管理などITセキュリティに関するノウハウ･人脈を電子記録管理の分野に生かし、電子記録管理を推進してきた団体、企業、個人と連携をとり、また、ETSI や ISO などの国際機関と協調しながら、電子記録マネジメント基盤の確立と応用に向けた活動を行っている。

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 5 月

一般財団法人日本情報経済社会推進協会

目　次

まえがき

今年の3月11日に発生した、東関東・東北大地震とそれに続く津波により、多くの被害が発生した。一部の地域では、市町村が管理する書類や各企業が管理する書類が、紙媒体、電子媒体にかかわらず、流失や水につかるなどにより失われてしまった。このような、巨大な災害への対応はもちろんだが、日ごろから自然災害や人の手による不正行為によって、書類等のデータが失われたり、改ざんされたりすることのない社会を作っていかなければならない。

また、技術的な流れとして、「クラウドコンピューティング時代の到来」がある。クラウドコンピューティング（英: cloud computing）とは、ネットワーク、特にインターネットをベースとしたコンピュータの利用形態である。ユーザーはコンピュータ処理をネットワーク経由で、サービスとして利用する。従来のコンピュータ利用は、ユーザー（企業、個人など）がコンピュータのハードウェア、ソフトウェア、データなどを、自分自身で保有・管理していたのに対し、クラウドコンピューティングでは「ユーザーはインターネットの向こう側からサービスを受け、サービス利用料金を払う」形になる。ユーザーが用意すべきものは最低限の接続環境（パーソナルコンピュータや携帯情報端末などのクライアント、その上で動くブラウザ、インターネット接続環境など）のみである。実際に処理が実行されるコンピュータおよびコンピュータ間のネットワークは、サービスを提供する企業側に設置されており、それらのコンピュータ本体およびネットワークの購入・管理運営費用や蓄積されるデータの管理の手間は軽減される。このサービスを利用することにより、ユーザーは低いコストでデータを保管することが可能になったが、一方でデータの改ざんや漏えいに関する対策に不安がある。

そこでJIPDECでは、クラウドコンピューティング上でも、電子記録を安心して保管できる技術基盤の検討のため、平成22年4月にDUPC内に会員を集めて調査検討作業を行う電子記録応用基盤フォーラム（eRAP）を立ち上げた。このフォーラムは次世代電子商取引推進協議会（ECOM）の電子署名普及WGの流れを汲むものであって、ECOMが1996年に設立されて以来十数年にわたって蓄積された電子署名、タイムスタンプ、個人情報保護、ID管理などITセキュリティに関するノウハウ･人脈を電子記録管理の分野に生かし、電子記録管理を推進してきた団体、企業、個人と連携をとり、また、ETSIやISOなどの国際機関と協調しながら、電子記録マネジメント基盤の確立と応用に向けた活動を行うものである。

このeRAPでは、平成22年度から3年間の予定で電子文書を安全安心な形で預かるサービスに共通に使われる電子記録応用基盤の構築、運用ガイドラインの作成と、相互運用可能な相互運用実験環境を構築しようとするのである。

本報告書は、eRAPの平成22年度成果をまとめたものであり、4章の構成になっている。第1章では、ITのあるべき姿と電子記録応用基盤のあるべき姿について述べている。第2章では、大きく2つの項目について紹介しており、ひとつは、記録管理に関する先進事例の調査結果であり、もうひとつは、電子記録管理システムに対する要求仕様の整理であり、欧州委員会の推奨するMoreq2010をベースに作成したものを紹介している。3章では、電子記録管理システムを検討するために必須となる技術（電子署名、ID、秘密分散）について解説しており、特に電子署名は次世代電子署名と呼ぶべき新たな動きがあり、これについて解説を行っている。4 章では、今後の進め方について、簡単に説明を行なっている。

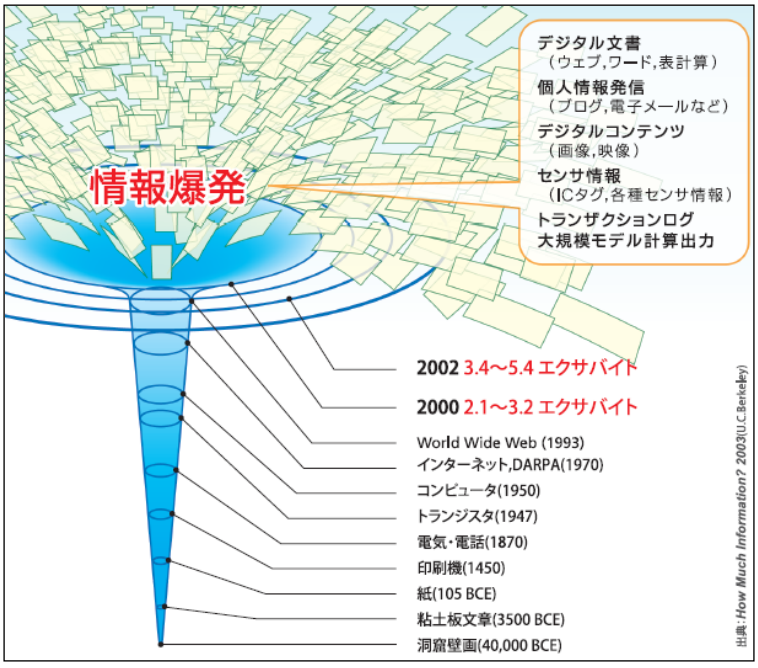
第１章　あるべき ICT 社会と安心安全な電子記録マネジメント

1.1　情報爆発

世界的にも急速な、IT（もしくは ICT）化の推進は論を待たない。その根底にあるものは単に合理化、効率化を求めるためなのだろうか？それは、未来への夢を拓くためだと考える人もあり、それゆえ多くの人々の好奇心を擽り、その結果多くの技術者や開発者を輩出し、国家レベルで競い合うように技術革新が加速している。

そもそも人類は、自らが面倒な計算を機械にやらせるべく電子計算機を発明し、それを高度化させ、ネットワークでつながることで変革し続けてきた。更に、そこで計算された計算結果やドキュメントの運用管理までも、電子計算機やネットワークに依存した。その結果として、莫大な量の電子データが世界中に存在することとなり、そのマネジメントに実社会の我々人類が苦しめられるという時代になっている。

高度情報化社会と言われて久しいが、この間に世界中で創出される情報量は爆発的に増大してきた。一方で、情報はヒト・モノ・カネと同等の経営資源として、その利活用の巧拙が成果に大きく影響しているのが現状である。また、情報の「カタチ」も紙から電子へと変貌したが、マネジメントの技術や手法の標準化が不十分な状態である。



まさしく「情報爆発」の時代において、氾濫する情報に翻弄されることがないように、IT をはじめとする社会基盤・インフラ技術の確立と標準化がワールドワイドで求められている。

翻って、コンピュータが商品としてこの世に登場した頃を振り返ってみよう。

現在の電卓よりも性能の劣るコンピュータが、とてつもない価格で取引され、現代からすると他愛も無い計算しかできなかった。しかし人類は、そこに大きな夢、可能性を見出していた。

それまで世界が経験していなかった、合理的で間違いや不正が無く、今までできなかったことができる、そんな未来への架け橋となることをコンピュータに期待していた。丁度、我々が子供の頃に故手塚治虫氏の SF 未来漫画を読んだときの感動のようなわくわく感と同様である。

果たして、人類の努力でコンピュータの性能は飛躍的に向上し、一方で価格は手頃なものになって、実社会に普及し活用が広まった。特にビジネスユースでは、日常的に処理していた業務をコンピュータに置き換え、業務効率と精度は格段に向上した。しかし業務上、日常的にできることに文明の利器を代用したことは、必ずしも本来の活用として正しかったとは断言できないのか

もしれない。

結果、コンピュータの活用は電算部門の独壇場となり、一般オフィスや家庭に普及するまでには、タイムラグが生じてしまう。加えてセキュリティに関しては、ID/PASS の仕組みは用意されていたものの、極論としては設定しなくても（電算部門の担当者しかオペレーションをしないため）脅威に晒されるリスクが低かった。そのため、そもそも導入のメリットを体感できない上に、セキュリティに対するリテラシーもこの頃は非常に低かったと言える。

現代に至る過程で、半導体技術、LSI，超 LSI、大容量メモリー、工作ロボット、様々な制御システム、視覚的で直感的な OS の出現、インターネットの急速な広まり等々、弛まない努力の結果、コンピュータと IT 社会は実社会に正に浸透した。現在、身の回りに仮にコンピュータや情報ネットワークが存在しなくなったら、大混乱が巻き起こることは誰もが否定しないほど深く普及・浸透している。

一方で、ウイルスやハッカーの脅威、個人情報に対する法制度や考え方の変化によって、情報セキュリティに対する認識にも変化が生じてきた。しかし、リテラシーが低かった頃の負の遺産から、セキュリティーシステム（暗号や認証等）自体が、誰もが簡単に使えるような所謂「枯れた技術」にはなっておらず、セキュリティと言えば結局のところ ID/PASS という認識にしかなっていないのが大方の現状である。電子的な署名や認証が普及しない根本はここにあるのではないだろうか？

より安全・安心な情報化社会を築き上げるためには、この現状を打破する必要がある。

我々人類の飽くなき欲求は、情報記録媒体を粘土板や石版そして木版や紙から電磁的記録に移行させ、更に記録した情報自体の利活用に優れたコンピュータの導入が爆発的に進み、更にコミュニケーションツールとしてのインターネットとの融合を行なってきた。つまり、デジタル化は情報記録メディアとしての革命だけに留まらず、コミュニケーションの在り方そのものにも大きな影響を与え、我々人類の社会基盤へも大きな影響を与え続けている。その過程で、我々はコンピュータの利用によるハンドリングの効率性を追い求めてきた。加えて、本来自らが責任主体として管理しなければならない情報自体を他者に委託するところまで合理性を進めてきた。しかし、その一方で当然のリスクとして、委託した相手の不手際や想定し得ない天変地異やアクシデント（時には政変やテロなども大きなファクタになる）での情報盗難や漏洩のリスクを受容しなければならなくなっている。

物理的な情報（書類・証憑等）だけならばまだ、被害は限定されるとも考えられるが、我々は現在情報化社会にあって、電子化情報の渦中にあり、センシティブな情報（たとえば個人の金銭情報や医療情報、経歴など）がコントロール下から離れ、ネット上に露出してしまうと事実上回収できなくなってしまう。

更に怖いのは、それが正しい情報なのか不正確な情報なのか検証しようもなく、ネット上で拡散していってしまうという事実である。

記録とは、歴史であり過去の証拠とも言える。個人に帰属する内容であれば秘匿したい情報もあり、企業でも国家でも一定以上のセキュリティを確保したい情報が多数存在している。デジタルの特性を考えると、新たな電子記録のマネジメントに一般も納得・合意できる道筋・手法が必要であり、安全・安心な情報化社会を構築していかなければならない。そして、これらの技術を幅広く普及していくためにグローバル社会の背景からも国際的な標準化が必須であると考える。

特に我が国においては、少子高齢化の加速に伴う情報へのアクセシビリティの確保（簡便な操作性）と環境対策の側面から求められるグリーン IT の推進という国家的な課題に対する取組みにも直結する非常に重要なテーマである。

電子記録応用基盤フォーラム（以下略称である「eRAP」と記す）は、電子記録マネジメントコンソーシアムを構成する各組織とも情報共有・連携しながら、これらのテーマに関して情報を収集し、課題検討を行い、提案・提言を整理してきた。

1.2 記録マネジメントの重要性

前述のように、相当程度コンピュータや IT 化が普及したと言える現代では、小規模・零細・個人事業主のレベルでも（あるいは一般家庭においても）、通常の社内業務で一台でも PC を導入していれば、必然的に原本やリストを電子データで作成することになっているはずである。それが、研究開発なのか、経理処理なのか顧客管理なのか、営業（販売）資料なのかはここでは問題としない。当然、その原本となる電子データを業務で利用することになれば、自ずとペーパーレス化が促進されているのは間違いない。企業内での文書を例に取れば 80%以上が電子化されているというデータ（出典：社団法人日本画像情報マネジメント協会／JIIMA“ECM 研究会”より）もあるほどで、もはや電子データや記録は、世間では普及も浸透もしている状況にある。

しかし一方では、法律上の要求や、単純なコンピュータへの疑念（というより紙媒体の安心感や利便性）等の理由で、未だに紙ベースの原本管理が要求される業種・業務も存在している。これらすべてを電子化すべきだということを提言するつもりはない。電子化でメリットが享受できるものを優先すれば良いのである。

セキュリティに関して角度を変えて見ると、各自が好きなように電子記録の管理をするのも、考えようによっては一定以上のセキュリティーレベルを確保できる可能性はある。しかし、その一方で社会としての合理性を考えると、そこには一定のルールに基づく方が、社会の構成員たる個々の利益が大きいのは言うまでも無い。

1.3 社会基盤としての署名・認証

電子記録マネジメントにおいて、そのセキュリティの重要性については、これまで述べてきたとおりである。詳細な説明は後段に譲るとして、ここでは、その技術や手法としての電子署名および認証について簡単に触れておく。

多くの人々にとって、電子署名・認証と言われても極めて馴染みの薄い単語で、ある意味 IT に携わる技術者や専門家の不親切な体質が露呈している面があり、活用が進まない遠因とも考えられる。

一般的な感覚で考えると、署名といえば契約書等にペンや万年筆で手書きサインする行為であり、パソコンのキーボードやマウスから法的に有効な電子署名ができるとは大多数の人は知らないのが実態であろう。また、「認証」という言葉も一般には聞きなれない単語で、見かけるとすれば工場の壁に「ISOXXXX 番認証取得」とか銀行の窓口で「本人認証が必要です」といった告知程度ではないだろうか。

しかし、こと IT 社会、IT システム、開発や研究に従事する側からするとどうしても利用者に理解していると言わせたい、そして是非とも活用を促し普及させたい踏み絵的な技術・ツールになっていると思われる。何故なら、電子署名や認証を知らないといわれてしまうと、電子情報マネジメントの入り口から躓くことになり、ほとんどの技術的なロジックが無に帰すからである。

更に、多くの人々が IT におけるセキュリティ技術に感心を示さないのは、暗号について理解しにくいという現実が横たわっているからである。要するに専門家の世界の話になってしまって、理解できないし、現状では理解したいという特段の動機も無いのである。誰にでも理解できるように説明できないのは、情報を提供する側の努力不足とも言えるが、理解する動機が無い（興味を持たない）のは、我々にとって非常に高いハードルとなっている。また、暗号化された情報自体の保護と、署名や認証についての話題がミックスされて説明されることが多く、聞いている側からすると、暗号の話が、いつの間にか本人認証の話になり、しかも最終的には署名の効力について話題になっていたりして、理解するための機会が混乱を招く結果となることも少なくない。

稚拙なたとえであるが、お蕎麦屋さんで、もり蕎麦を頼む。店員が、鴨南蛮ですね？と聞き返し、勝手にメモを取るのに呆れていると、提供されてくるのがカツカレー。そんな印象で、現状の IT は、一般人に非常に不親切で不適切（残存リスクを明確に理解してもらってない）だし、すぐに内容が理解できない。

更に言えば、実社会での運用と裁判等の事例を積み重ねていく中で、被告等を含めた裁判関係者全員が仮に IT に関して素人であったとしても、国民、行政、法曹界（裁判官、裁判員、検事、弁護士、学者等々）が、共通理解の下に判断ができるようなセキュリティ基盤になっていることが重要である。よって、前提となる IT システムなり IT 社会の抱える原理的な課題の明記と、より理解しやすい暗号の言及（情報保護手法・技術）、それをベースにした署名・認証についての噛み砕いた説明が必要である。そして、IT の技術的な背景や説明よりもその署名・認証を利用することで実現できること、利用者が享受できるメリットについての理解の促進をしなければならない。

特に既存技術等だけでは、「できないと諦めていた」ことが、実は社会にとっては非常に重要な機能だったりすることもある。IT を導入し効率化等の改善を行なってきた企業・組織等が直面している最近の課題は、まさに「現在の IT システムでは実現できないと諦めている機能等」の中に新たな IT の進化の方向性や可能性が潜んでいると考える。但し、ベースとなった技術等が誕生した際に留意事項として挙げられていた事項が、時間の経過や市場普及の過程で軽んじられてしまい、あるとき大きな問題を引き起こすことがある。（回転ドアの問題で有名になった「技術の系譜」という考えである）合理的で積極的な革新は非常に大事であるが、守るべきポイントはしっかりと守り、そこに改革を行なう際には、十分な検討と評価等を行うことも重要なことである。

1.4　重要情報の保護

比較的理解しやすい情報保護技術として、秘密分散技術（電子的割符）がある。この技術は世界でも日本が先行していると考えられ、JIPDEC の昨年の報告にも記載されている。原本の電子データを実際にビットレベルで分割していく処理を根底に置いている為、原本情報保護の原理が

非常に明快であること。更に、原本情報を分割し個々の割符（分割ファイル）を生成する際に、冗長等の工夫を加えると、例えば３つに分割していながら一つのファイルが消失してしまったとしても、残りの二つで原本情報を復元できる処理も可能となる。といった特性がある。結果として、原本情報の保護と同時に、緊急時のリカバリー・バックアップの機能も兼ね備えているのが、秘密分散技術（電子的割符）と言える。

前述のような割符生成のプロセスから原本情報の全体長が維持されていない為、生成された割符単体では原本復元に必要なビット数が不足している事実がある。これは割符という概念を実際のデータ処理に適用した結果生じた効能で、当然ながら原本情報が丸ごと容易に漏洩しない仕組みが自ずと構築される。しかし、ここで重要なことは、割符のセキュリティ上の存在意義ではなく、人類の叡智である情報を相互補完する。シェアする。という「割符」の概念で、電子的な重要情報の運用管理が実現できるようになる。という事実である。つまり、割符技術とは数学的な暗号技術とは異なり、あくまで「割符の概念で保護したい電子情報を運用管理する際に利用できる道具であり、対象の電子ファイルを分割・統合を行なうためのソフトウエアであり、それが日本発祥である」という事実が貴重なのである。

これまでの、集約型の情報管理において活用されてきた暗号技術と対極、すなわち管理対象とする情報自体を、関係当事者等で分散管理することで、原理的な安全性を担保する技術と手法である。

また、暗号技術における最大の課題である「暗号鍵管理・配布」関連する ID/PASS 管理、管理テーブル管理といった集約型のアキレス腱と考えられる部分に、一つの解決ルートを提供できる可能性のある技術であると考えられる。加えてロジックが理解しやすいことと、分割後のファイルをオフラインで物理的に管理させることもでき、人間として大事な情報を管理できるという「実感」を得られやすい。

さらに、情報を開示する際も、物理的に管理しているメディア等を自らの能動的な行為によって提供する仕組みにすることもでき、単に対象情報の安全性確保といった観点以外にも、法的見解の立場からも有意義な技術であり、手法である。これは、集約型と分散型の両極の技術が存在する日本から、双方をマージさせた新たな情報社会基盤を作り、広く世界の IT に発信できる可能性がある技術である。我が国にとっても構造改革に不可欠な IT の普及、そして、そこで得られたノウハウを活用した新たな日本の産業・商品・サービスの重要な構成技術になっていくとのではないかと考える。

例えば、デジタルデータの基本的な特性から来る脆弱性の一つが、データ消失問題である。近年の日本国内での大規模災害でも、地域情報・医療・行政・企業組織等のデータが災害の都度消失してしまい現場の混乱が発生し、中にはもう復元不可能な情報も多数存在する。

よって、地震等の大規模な自然災害が多い我が国においては、当該技術が昨今のクラウド等での応用に資するだけではなく、国民や企業、行政組織等での情報管理の場面でも、原本情報保護とバックアップ・リカバリーの役割を同時に満たす仕組みとして、広範な導入等が期待される。

1.5　これからの IT 化ビジョンと電子記録マネジメント

今後も多方面にわたって IT 化が推進されていくことは予想に難くない。この推進をさらに加

速させるためには、誰もが身を乗り出すような「何か」を具体化できることを示していくのが道筋の一つとしてあると考えられる。世界を俯瞰してみると IT 化が国家レベルで飛躍的に推進された国々が散見される。これらの国々の特徴は、国家的な経済危機を打破するために、意識的に IT を導入することによって国としての経営資源（人員・コスト・時間等）を他の分野へシフトさせたモデルである。既存実社会の仕組みにコンピュータを当てはめたモデル（既存業務の IT 化による効率化と合理化）と、既存の人手による実処理ではできなかった仕組み（新たな業務および国民サービスの提供）が融合している。

そこで我が国においても IT を活用したさまざまな業務改革に必要な技術・知的財産・アイデア・付加価値を持つ企業・個人を積極的に束ねて、今までに無いプロジェクトを検討してみてはどうか？

加えて、IT 分野における人材の育成強化も急務であり、国内ノウハウや人材が海外流出することに一定の歯止めをしなければならない。そのためにもプロジェクト内での知財対策と人材開発方針を明確にし、我が国の国際競争力の向上に寄与できるものにしていく必要がある。

このようなプロジェクトを推進していくために、マストな要件として、

- 明らかなマイナス提案は排除するものの、プラス思考の予算確保。
- 自戒も含め、所謂専門馬鹿の排除・・・論より証拠、やってみる・・・チャレンジ風土の醸成。
- 意思決定は、極論構成委員一人のアイデアであっても尊重するようなプロジェクトの推進。
- 一般公開による全てのプロセスと情報（技術的内容など知的財産に関連事項を除く）の国民共有。
- 国家的課題として、ISO 等の標準化を念頭においた中長期的なプロジェクト化。

などが考えられる。

また、目指すべきベクトルとしては、

１、既存社会の処理を単に IT に置き換えるような技術ではなく、大きな付加価値を求める。
２、IT に閉じた仕組みは専門的・技術的になり過ぎ、一般的に受け入れられないため回避する。
３、IT 社会と実社会がシンクロしている領域（誰でも何時でも何処でも）が、普及の条件である。

つまり前述した諸外国のように、IT 導入の目的が国家的な財政問題の解決を図るためという、市民も賛同せざるを得ないような深刻なモデルではなく、逆に社会が明るくなるような理由・動機であっても欲しいと考える。そして広く遍く活用される仕組みが構築されなければならない。

これらの背景を踏まえ、本報告書では前述の IT 社会と実社会がシンクロするトリガーとして、電子記録のマネジメント分野において課題克服に向けた事例を調査し、その事例から標準化や、セキュリティ意識の底上げのため提案を行いたい。更にこれらの提案の中から、次世代に継承できる仕組みやルール、そしてこれらのたたき台ともなるような技術的基盤の提案ができればと考えている。

そのための前提として、

- 本提案が、組織のトップマネジメントに対する具体的商材になるような検討が行われること
- 一般人にも理解されやすい内容であること（専門的、技術的過ぎないこと）
- 当面は国内標準の提言ではあるが、国際標準をも意識した内容であること
- 日本発の技術として世界へ発信できる内容であること

前項でも触れたとおり、電子記録マネジメントにおいて「誰もが理解」でき、「社会全体にメリットが循環」し、「国際社会でも通用」する仕組みを“eRAP”として提案したいと考える。もちろん、品質、満足度、コストパフォーマンスなどすべてにおいて、優位性を獲得できるような仕組みでなければならない。

しかしながら、現在のところ諸外国における動きが先行していることは否定できない。したがって、国際的な潮流との整合性に留意し、その胎動・動向を敏感に受け止めることが必須である。まずは電子記録マネジメント先進国の事例を調査研究し、その成果を真摯に受け止め、まずは標準化のモデルを検討しながら、最終的には国際的な思考モデルに影響を与えるような成果を出したい。

例を挙げるなら、

- 韓国における公認電子文書保管所と電子文書の利活用
- エストニアにおける電子政府システムと国民 ID 制
- ドイツ、デンマーク、ハンガリーにおける電子記録管理

上記のような各国の状況について、調査結果を含めた提言は後段にて詳述する。

一方、我が国においては電子記録マネジメントの必要性が、今後は関連する法体系からも強まることが予想される。これは以下の電子記録マネジメントコンソーシアムのステートメントを参考としたい。

「電子文書を利用するため、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った。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、現状は組織的な運用がなされていない、データの標準化が行われていない、証明すべき証拠の維持方法が規定されていない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、活用されていない状況となっている。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。」（2010/3/10 プレス発表より）

1.6　デジタル社会に向けて＜あるべき ICT 社会と安全安心な記録管理＞

確実に言えることは、利用者が素晴らしいと実感できる仕組みを提供しなければならない。これまで人類が経験してきた紙文化からデジタルとの共存段階を経て、更に大きく一歩を踏み出し、真に社会に受容される IT システムを実現し、実社会と法解釈上も高度に融合させることができる仕組みとする。その為には、根拠・証拠となる原本情報の安全安心な記録管理は必要不可欠な機能である。

証拠という文言を使うと、刑事・民事で解釈が異なってくるが、普遍なのは、我が国においては心象が非常に大きく影響を及ぼし、時には真実の資料等であっても証拠として採用されない場合もあるということ。よって、IT に詳しくない国民であっても、十分理解できる仕組みが必要

である。同様に、企業組織等での情報管理の場面でも、本当に有意義な事業継続計画に合理的な IT システムが導入されているのか、更に、組織の代表者として残存リスクを正確に把握し、その具体的な対処方策を適切に採用しているのか。等々といったことのコミットメントを、組織の代表者は求められる。ステークホルダーからすれば、当然の要求であり不可避な内容である。その際、本当に組織の代表者は残存リスクを正確把握し、且つ、実際に導入している情報管理・保護システムがどのようなものなのかを理解できているのであろうか。現状のセキュリティーシステムの実状を鑑みると非常に形式的であるとしか言えない。

我々は、IT に親しみの無い方々も十分に理解できる IT システムが、実社会と高度に融合することを切望する。そうなれば、その仕組み自体が、日本が世界に誇ることができる新たな産業の柱の一つに成長していける可能性を持てるようになるからである。理由は簡単で、そのような分かりやすく、実社会と高度に融合した仕組みは、世界中が未だ実現できていない仕組みだからである。

我々は本報告書を記述するにあたり、上記のような観点からの報告と同時に、この報告の中に日本の将来を明るく導く IT システム像の片鱗を、読者の皆様にお届けしようと活動した。諸外国の真似ではなく、日本独自でありながら、世界で通用し、更に広く利用される仕組みの萌芽を本報告書の中から見出し、育んでいく気風が創出できれば我々の活動は半ば報われると考える。最後になるが、そういった活動の中から、是非実現してもらいたいのは、中途半端な IT 化やペーパーレスではなく、究極の社会推進事業としてモデル地区を選定し、未来型社会の特区等の措置を行い、日本そして世界を牽引できるレベルの事業を具体化することである。なぜならば、既存（アナログ）文化や法制度・法解釈、しきたり等々のしがらみを断ち切ることができないからである。一例を挙げれば、人が何らかの証拠資料を手にしたとき、その見た目や風合い、手触り、紙の折れ具合、汚れ等々様々な情報を媒体から感じ取り、総合的にその資料の信頼性を判断する。しかし、十分にデジタル社会が成熟し、記述（情報）内容の正確性と、長期保管の際の安全安心も、もたらされたならば、記述された内容（情報）だけに注力してよい社会になる。つまりデジタル情報が完全に証拠として取り扱われる社会では、そのようなアナログの紙から受ける副次的情報は不要になり、紙を物理的に長期に渡り保管する必要はなくなる。しかし、現代社会はそこまでデジタル化が進んでいるとは言えず、それだけアナログ社会とデジタル社会との乖離は未だに大きいということである。

第２章　電子記録管理

2.1　電子記録管理の要件

2.1.1　電子記録管理の課題

ICT 技術の進展により、デジタル情報の作成、共有が進み、日常の業務におけるデジタル情報の重要性が高まっている。これにともない、技術、組織・運用、法的裏付けの観点からの信頼可能な情報や知識の展開・活用に対する指針や答えが求められている。

技術領域の課題としては、地理的に分散した、ビジネス上の重要かつ機密性の高い膨大な電子文書や電子記録を、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・運用の課題としては、業務プロセスの刷新と、電子化や紙文書との共存、保管方法の革新がある。電子文書や電子記録を意識してその保存、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。法律と規制の面では、特に、電子記録の適法性と信頼性を確保することが課題となる。

電子化のメリットは、①データの管理と保護を集中的に行える。②火災、洪水、凍結、カビの発生を回避できる　③物理的な保管コストがなくなる。また、④分散したオフィスという問題も回避できる。しかし、電子化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。電子記録管理システム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、生成からその活用、保管まで、全プロセスを自動化できる。

企業や組織は今、効率化、透明化、低炭素化が求められている。しかしながら現状は、事業活動の反映としての電子記録の活用が十分であるとは言えない。表 2.1 は、電子記録活用における問題を示している。企業レベルの記録管理（Enterprise Records Management, ERM）システムは、この問題の対策への解を与えるものでなければならない。

表 2.1　電子記録活用における問題

	問　題	原　因	対　策
1	見つからない	そもそも記録が存在しない	作成・取得基準、自動キャプチャ
2		破棄された（故意/過失/現場判断）	破棄基準、破棄記録
3		保管場所移動（散逸）	分類体系保守、Export/Import
4		検索キーが不明/不適切	分類基準、統制語管理、 検索キー自動設定（フォルダへの Drug & Drop 時に自動設定等）
5	選別困難 （検索結果過多）		
		不要文書に埋もれている	計画的な破棄（保存・処分計画）
6	役に立たない	関連情報の欠落	記録間の関係性情報付与、 パッケージ化、CASE 管理連携
7		リンク切れ	ユニーク ID 付与
8		信頼性不足 （コンテキスト不足）	来歴・脈絡情報付与、署名・タイムスタンプ

ERM システムについての一般的な定義はないが、ERM の機能は、欧米の政府や企業が定義する要件によって大枠は示されてきている。

ここで、文書、記録、記録管理について整理しておく。まず、文書と記録との違いを表 2.2 に示す。

表 2.2　文書と記録との相違点

文　書	記　録
重要あるいは非重要	決定や行為の重要な証拠
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

ISO 15489-1 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。この定義は全種類の記録（デジタル記録、紙の記録、物体など）を対象としている。また、記録とは商業行為、取引やその他の行為（契約など）の証拠であり、記録が正式であるためには以下が必要であるとしている。

真正性（当人が作成、送出していること）

信頼性（文書化された行為を正確に反映する、信頼可能な内容）

完全性（記録が一貫していて変更がないこと）

利用性（場所の特定、検索、提示、解釈が可能であること）

記録に加えて、ISO 15489-1 は記録管理について「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」と定義している。

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 15489-1 を基にすると、ERM システムは以下を提供する必要がある。

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

2.1.2　代表的な電子記録管理の要件仕様

電子記録管理の要件については、すでに幾つかの国際的な仕様が存在する。MoReq2、ISO 16175-2、DoD 5025.2 がその代表例である。表 2.3 に、代表的な電子記録管理の要件仕様の必須要件の比較を示す。ここで言えることは、必須要件のコア部分には大きな差はないということである。例えば、ISO 16175-2 や DoD 5025.2 にキャプチャに関する要件が定義されていないが、これは、外付けにするか内包するかの方針の違いであり、記録のライフサイクル管理の本質ではない。

実績の観点からは、欧州を中心に実績のある MoReq2 と米国の DoD 5025.2 が挙げられるが、本検討では、オープンな活動の結果としての仕様である MoReq2 を参考にすることとした。

表 2.3　代表的な電子記録管理の要件仕様の必須要件比較

要件		MoReq2	ISO 16175-2	DoD 5015.2
分類体系及びファイル構成	分類体系の設定	3.1	3.1.3	2.2.1
	クラスとファイル	3.2	3.3.1-.2	2.2.2
	ボリューム・サブファイル	3.3	3.3.4	
	分類体系の維持	3.4	3.3.3	
セキュリティ	アクセス制御	4.1	3.4.1-.5	2.2.7
	バックアップ・リカバリ	4.3	3.8.4	2.2.9
	重要記録(vital)	4.4	3.8.4	2.2.6
	監査	4.2	3.x	2.2.8
保存及び処分	保存及び処分計画	5.1	3.6.1	2.2.2, 2.2.5-.6
	処分のレビュ	5.2	3.6.1	2.2.6
	移管，エクスポート，廃棄	5.3	3.6.2	2.2.6
キャプチャ及び記録の宣言	キャプチャ	6.1	3.1.1	
	合成記録(コンテナ)	6.1	3.1.6	
	記録のタイプ	6.4	3.3.1	2.2.2
	バルクインポート	6.2	3.1.4	3.2
	e-メール管理	6.3	3.1.7	2.2.4
	スキャニング/イメージング	6.5		
参照(識別)	分類コード	7.1	3.2	2.2.3
	システム ID	7.2	3.2	2.2.3
検索, 取り出し, 及び表示	検索及び取り出し	8.1	3.7	2.2.6
	表示：記録の表示	8.2	3.7.1	2.2.6
	表示：印刷	8.3	3.7.2	2.2.x
	表示：音声等の対応	8.4	3.7.4	
管理機能	モニタ及び通知	9.1	3.8.1	2.2.9
	報告	9.2	3.8.3	3.2
	変更，削除，リダクション	9.3	3.7.3	

注記：MoReq2、ISO 16175-2、DoD 5025.2 の各欄の値は、各々の仕様のなかの該当する項番である。
複数の要件にまたがって対応付けられる場合は代表的なもののみ示した。

MoReq2 は、企業記録管理（ERM）システムの一般要件のための包括的カタログである。この仕様は、ERM システムを使用する公共および民間部門の組織体を対象としている。

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（Donnees Lisibles par Machine）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。

2006 年には、DLM フォーラムは、MoReq からの強化版として「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（MoReq2）（Scoping report for the development of the Model Requirements for the management of electronic records (MoReq2)）」を公表した。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。現在(2011年3月現在)は、更にその強化版であるMoRTeq2010の策定段階にある。

参考までに、MoReq2、ISO 16175-2、DoD 5025.2のオプション要件比較を表2.4に示す。

表 2.4　代表的な電子記録管理の要件仕様のオプション要件比較

要件		MoReq2	ISO 16175-2	DoD 5015.2
オプション機能	紙・電子共存(ハイブリッド)管理	10.1	3.5	
	物理ファイル/記録の管理	10.1	3.4.8	
	物理記録の処分	10.2	3.6.3	
	文書管理及び共同作業	10.3	3.7.5	
	ワークフロー	10.4		3.2
	ケースワーク	10.5		
	コンテント管理との統合	10.6		
	電子署名・タイムスタンプ	10.7		
	暗号化	10.8		
	デジタル著作権管理	10.9		
	分散システム	10.10		
	オフライン及び遠隔作業	10.11		
	FAX 統合	10.12		
	セキュリティカテゴリ	10.13	3.4.6	4.1
非機能要件	利便性(ease of use)	11.1		
	性能及び拡張性	11.2		3.1
	システム可用性	11.3		3.1
	技術標準	11.4	3.1.5	2.1, 3.2
	法規制要件	11.5		
	データの外部委託・第三者管理	11.6		
	長期保存及び技術陳腐化	11.7		
	業務プロセス	11.8		

注記：MoReq2、ISO 16175-2、DoD 5025.2の各欄の値は、各々の仕様のなかの該当する項番である。
複数の要件にまたがって対応付けられる場合は代表的なもののみ示した。

2.1.3　主要 100 要件

MoReq2は、800の要件からなるモデル要件仕様である。要求は必須、推奨、オプションが混在していることから、ミニマム要件を抽出し、次の主要100要件として整理した。

(a)　分類体系とファイル構成

分類体系の設定

1.　ファイルや記録を階層化されたクラスによる分類体系で表現できること
　※ 全てのクラス，ファイル，サブクラス，ボリュームに説明（スコープノート）を入力できることが望ましい

［補足説明］

図2.1に、想定する記録の分類体系とファイル構成を示す。ここで、クラス（class）は、分類体系階層中の任意の点からそれより下のすべてのファイルまでの階層の部分をいう。クラスは、

クラスに割り当てられたすべての記録を意味するためにも使用する。

ファイル（file）は、それらが、同じ主題、活動あるいはトランザクションに関係があることからグループ化された記録のひとまとまりの単位であり、情報技術（IT）の用法とは異なる。サブファイル（sub-file）は、ファイルの知的細別であり、ケースファイル環境の中でしばしば使用される。

ボリューム（volume）は、サブファイルの細別であり、管理のしやすさを改善するために作成され、知的ではなく機械的に行われる。

記録(record)は、法的な責任の履行，又は業務処理における，証拠及び情報として，組織，又は個人が作成，取得及び維持する情報である（ISO 15489 の定義）。注:記録は 1 つ以上のコンポーネントから構成される。

コンポーネント（component）は、記録や文書を構成する、単独あるいは他のビットストリームに付随した個別のビットストリーム（distinct bit stream）であり、注:情報技術におけるファイルと同義である。記録管理上のファイルと混乱することを回避するために、別の用語を用いる。

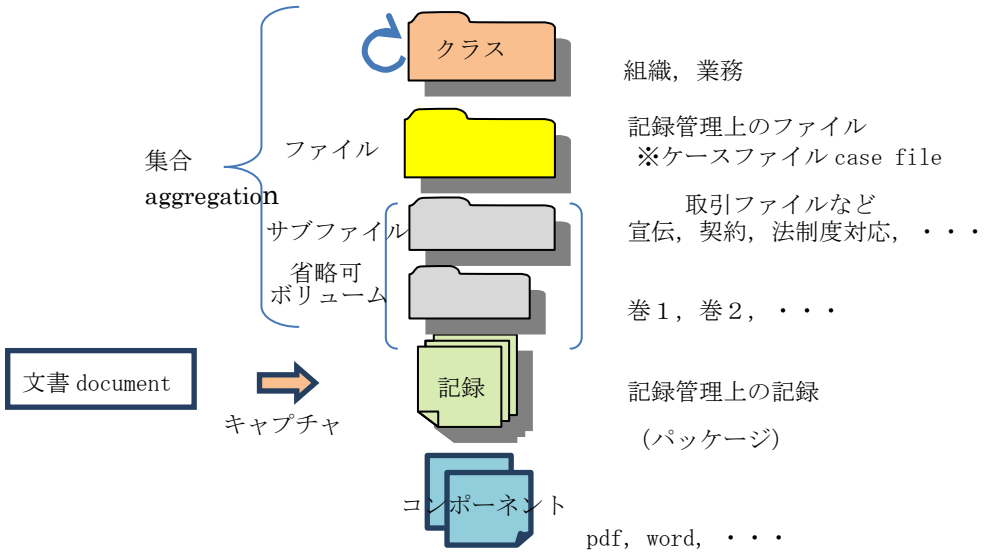


図 2.1　分類体系とファイル構成

2. 分類体系の管理は監理者だけに許されること
3. 分類体系の全て又は部分をインポートできること。分類体系をインポートするときは関連メタデータ，保持及び処分計画，監査証跡もインポートできること
4. 分類体系の全てまたは部分をエクスポートできることが望ましい。分類体系をエクスポートするときは監理者がエクスポートするメタデータを選べること。このとき監理者の選択で関連する保持及び処分計画，監査証跡もエクスポートできること
5. 別途規定される標準フォーマットでエクスポートすること
6. 分類体系の全て又は部分をコピーする場合は関連メタデータ，全ての保持及び処分計画を含むこと
7. 複数の分類体系が定義でき同時に使えること

クラスとファイル

8.　クラス又はファイルのメタデータ内に，開始日（open）及び終了日（close）を格納すること

［補足説明］

ファイルの生成（create）と開始（open）は分けて管理する（図 2.2 参照）。ファイルをあらかじめ生成しておくことはできるが、キャプチャされた記録やメタデータの格納は、ファイルの開始から終了の間でのみ可能である。読み出しはいつでも可能である。

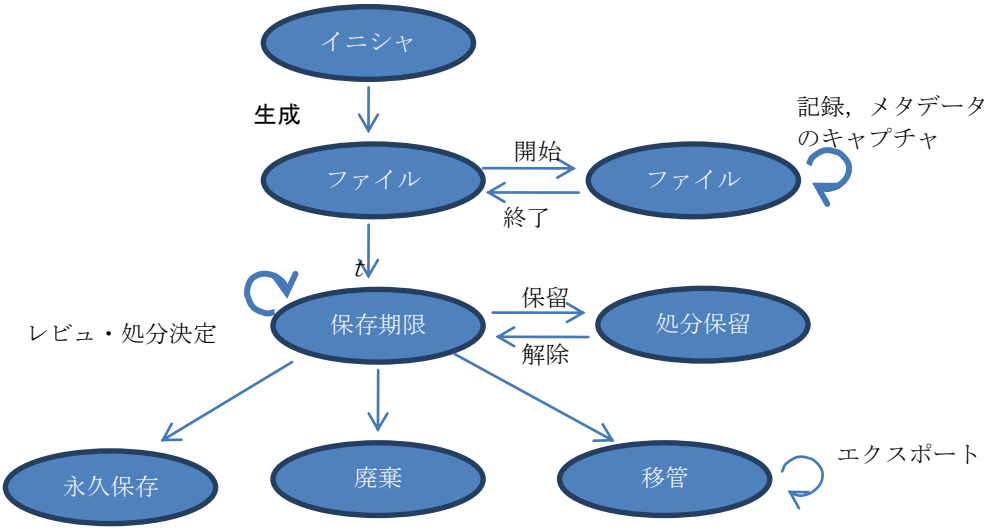


図 2.2　ファイルの開始・終了

9.　クラス又はファイルのメタデータ内に、新たなクラス，ファイル，サブファイル，ボリュームの作成日を格納すること

10. 新たなクラス又はファイルを開始(open)したときはメタデータを継承すること。継承したメタデータ値は許される範囲内で監理者が変更できること

ボリュームとサブファイル

11. サブファイルやボリュームを監理者が作成できないようにも設定できること

12. 新たなボリューム又はサブファイルを開始したときは，開始日をメタデータに格納し，上位集合のメタデータ値を継承すること

分類体系の保守

13. クラスの結合や分割ができること

［補足説明］

図 2.3 に分割と結合のイメージを示す。主に組織の統廃合に伴って発生する。

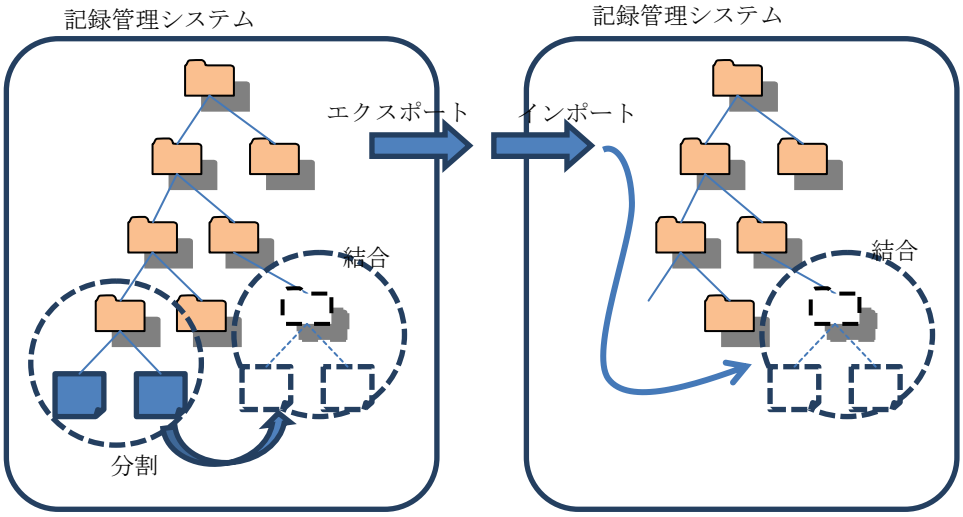


図 2.3　分割と結合

14. 再配置や再分類するとき，変更前の参照関係を保持すること（変更された体系に参照を付けること）また，新たな親クラスからの継承ができること
15. 記録が再配置またはコピーされる時に監理者にメタデータとしてその理由の入力を要求すること
16. 再配置又はコピー前の状態，及び再配置前のメタデータの値を記録すること
17. ユーザが関連ファイル間の相互参照を作成できることが望ましい
18. 記録の重複なしに記録に対する複数エントリを作成できることが望ましい
19. ユーザはファイルや記録のコンテキスト（脈絡、たとえば属するクラス）を認識できること
20. ファイルの検索用キーワードを変更するときは、変更前の状態の痕跡を履歴として残すとともに、監理者に理由の入力を求めること

(b)　コントロールとセキュリティ

アクセス

21. 識別され認証された認可(authorized)ユーザでない限りいかなる操作もできないこと

監査

22. 操作やその時刻情報を自動的にキャプチャし格納した監査証跡を保持すること
23. 監査証跡パラメタの変更，メタデータの変更，記録への注釈や変更，監理パラメタの変更が監査証跡に記録されること
24. アクセス制御の意図的違反行為をキャプチャし保存すること

バックアップとリカバリ

25. 自動バックアップを提供すること
26. 許可された監理者のみがリストア及びロールフォワードできること

重要記録

27. 重要記録を含むか重要記録として扱われるファイルや記録を監理者が表示できること。また，最早重要と扱われないファイルや記録を表示できること

［保続説明］

重要記録（vital record)は、緊急時および/またはその後に機能および/または組織の存続にとって不可欠な記録をいう。

28. フルバックアップと重要バックアップの２つの独立した操作ができること

(c) 保持と処分

保持及び処分計画

29. 監理者のみが保持及び処分計画を作成し維持（含，修正）できること
30. 保持及び処分計画の変更履歴を改変できないよう維持すること
31. 保持及び処分計画の変更は直ちに適用されること。変更理由は保存すること
32. 全てのクラス，ファイル，サブファイル，ボリュームは１以上の保持及び処分計画をもつこと。デフォルトの場合は上位エンティティの保持及び処分計画を継承すること

※記録のタイプにデフォルトの保持及び処分計画を適用できることが望ましい

33. 保持及び処分計画は保有期間及びトリガ事象または処分日，処分行為と理由を含むこと。処分行為として少なくとも永久保存，レビュに提出，自動廃棄，管理者承認後の廃棄、移管が許されること

※ 保持及び処分計画は説明と業務規程を含むことが望ましい

34. 保持及び処分計画に従って保存期間が満了した場合は自動的に処分決定プロセスを起動すること。自動処理は監査ログをとり監理者に通知すること。レビュが必要なときは監理者に自動的に通知すること
35. 監理者はレビュを委任することができること
36. 許可されたユーザによる処分保留が許されること。処分保留の適用及び解除の場合はその日付，許可されたユーザの ID，理由をキャプチャし保存すること

処分のレビュ

37. 計画が特定の期間に入ることを監理者に通知すること
38. メタデータと計画情報によりレビュプロセスを支援すること

※ 同じ記録のレンディション間のリンクを維持し処分行為を同時に行えること。レビュワが，廃棄，移管，更なるレビュ，永久保存のマーク付けをできること

※ 自動的にレビュ日のログが採れること

39. レビュ決定の理由を記録するためにレビュワがメタデータにコメントを入れられること
40. レビュ期間の理由を含むレビュワの決定の不変履歴を保持すること

移管，エクスポート，廃棄

41. 記録をエクスポートできること。記録を移管またはエクスポートする場合は全てのコンポーネントの関係を維持したまま移管またはエクスポートすること

42. 他のシステム又は他の組織に記録と関連メタデータと監査証跡情報を移管するよく定義されたプロセスを提供すること
43. エクスポートするメタデータ，監査証跡は選択できること。エクスポートまたは移管する場合はインプリシットなメタデータを含むこと
44. 宛先システムでの再適用のために，記録と一緒に保持及び処分計画，アクセスコントロールをエクスポートまたは移管すること
45. ポインタではなく完全な記録をエクスポートまたは移管すること。記録はキャプチャ時のフォーマット及びレンダリングされたフォーマットでエクスポート又は移管できること
46. 記録が廃棄されるときは全てのレンディションも廃棄されること（図 2.4 参照）
47. 廃棄または移管されたクラス，ファイル，サブファイル，ボリューム，記録のメタデータスタブを保存できることが望ましい。メタデータスタブは少なくとも廃棄日または移管日，分類コード，タイトル，説明，廃棄または移管理由，参照を含むこと

［補足説明］

メタデータスタブ（metadata stub）とは、その項目（item）が保持され適切に破棄された証拠の役割をするために、その項目が破棄された後に保持される、そのアイテムのメタデータの部分集合をいう。

(d) キャプチャ及び記録の宣言

キャプチャ

48. キャプチャプロセスはユーザに，記録のキャプチャ，分類体系への関連付け，ファイルと関連付けられた記録のためのコントロールと機能を提供すること
    ※ 対象はデスクトップ AP 出力（オフィス），e メール，音声，DB，PDF，ビデオ，Web ページ，blog，ソースコード，構造化データ（EDI），Wiki 等
49. キャプチャする記録が複数コンポーネントで構成されるときは関連を保存し 1 単位として管理すること
    ※ 保存や表示に必要なら一部をモディファイ（例えば，HTML ページのリンク先のグラフィックを取り込む）できることが望ましい
50. キャプチャ時に記録内の参照を変更する場合は，監査証跡に自動的に記録されること
51. 各コンポーネントのファイルフォーマット，バージョンは自動的にキャプチャしメタデータに格納する
52. メタデータ要素の幾つかの値は承認されたユーザと監理者のみが更新できる
53. 記録はキャプチャされたときに適切なクラス又はファイルに割り当てられること
54. 特定のファイル（フォルダ）にドロップされた記録に属性を自動付与することが望ましい
55. 記録のキャプチャ日時がメタデータ及び監査証跡として記録されること。自動キャプチャできないメタデータ入力をユーザに促すこと
56. クラス，ファイル，サブファイル，記録の複数キーワード又は語彙の割り付けを支援すること
57. 制御された語彙から選ばれるキーワード値及び他のメタデータ要素値を提供すること
58. キャプチャ時又はそれ以降にも追加の記述などのメタデータ登録ができること。監理者や権

限を与えられたユーザが記録のタイトルを修正する余地があること
※（組織のオプション）

59. 複数バージョンの文書をキャプチャした場合は全てを１記録とする，１つを特定，全て別の記録とするかを選べること
60. 監理者はクローズしたボリュームに（クローズ以前の日付がある）記録を追加できること。この時例外理由がメタデータに追記されると共に監査証跡に自動記録されること

バルクインポート

61. 記録のバルクインポートを実行すること
62. 他のシステムで生成された取引記録をキャプチャできること（バッチファイルなど）
63. バルクインポートの間に関連記録のメタデータを自動キャプチャできること。キャプチャしたメタデータはルールを使って検証すること
64. インポートされた記録の履歴を表す監査証跡記録をインポートすること。監査証跡記録をその監査証跡にインポートしないこと（別々に格納）

e-メール管理

65. 出入りするＥメールキャプチャ時自動的にメタデータ（日付，受信者，主題，送信者，署名など）を抽出すること
66. ユーザがドラッグによってＥメールをサブファイル，ファイル，クラスにキャプチャできることが望ましい
67. 添付を別の記録としてキャプチャする場合はメタデータ値のキャプチャ又は入力を要求すること
68. プロプラエタリフォーマットでキャプチャしたＥメールメッセージをオープンフォーマットで格納できること

記録タイプ

69. 記録タイプを定義しメンテナンスすること
※ 記録の特性（メタデータ属性，保存要件，アクセス制御，文書の種類など）を記述
70. 全ての記録は１つの記録タイプをもつこと

スキャニング及びイメージング

71. 少なくとも１つのスキャニングソリューションとの統合が可能なこと
72. OCR機能をもつときスキャンイメージとOCR結果のテキストは１つの記録として管理すること
73. イメージの注釈，注釈者，日付は記録として保持され変更と削除から保護されること

(e) 参照

分類コード

74. クラス，ファイル，サブファイル，ボリューム，記録，コンポーネントに分類体系の階層内

でユニークな分類コードを関連付けること

システム ID

75. 分類コード，クラス，ファイル，サブファイル，ボリューム，記録，レンディション，保持及び処分計画，文書に対してグローバルにユニークなシステム ID（UUID）を生成すること

［補足説明］

UUID (Universally Unique Identifier)は、16 バイトの数値で表される一意に特定可能な識別子である。ISO/IEC 11578、RFC4122 で規定されている。GUID はマイクロソフト社による実装例である。

(f) 検索，取り出し，及び表示

検索及び取り出し

76. アクセスが制限されているユーザにはいかなる情報も暴露しないこと

77. 記録やファイル，関連メタデータ（含、署名情報）を検索し取り出し，また表示できること。検索は、全文検索および属性検索が可能なこと

78. オリジナルフォーマットとは別のフォーマット（レンディション）を表示できること

［補足説明］

レンディションは、記録の本来ファイル形式とは異なるファイル形式による記録またはコンポーネントの発現をいう。例えば、所有者のファイル形式で生産された記録を、PDF/A あるいは XML のような標準形式にして格納するなど。

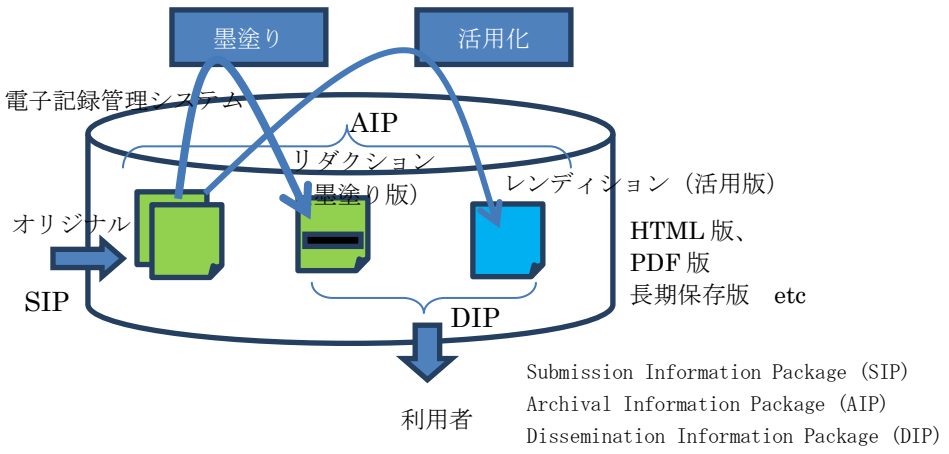


図 2.4　リダクションとレンディション

(g) 監理上の機能

一般監理

79. コンフィグ時に設定した値を監理者が再設定できること

80. ユーザと役割に対して監理者が機能を割り当てできること

報告

81. 監理者が定期的又は臨時の報告書を作成できるようにすること

※ 処分計画の成功及び失敗の結果，エクスポート処理の結果，処分作業，アクセス制御への試みやセキュリティポリシ違反行為，移管，エクスポート，廃棄，消去の失敗の詳細，インポート時の失敗の詳細など

変更，削除，及びリダクション（墨塗り）

82. 一旦キャプチャした記録を削除又は移動できないオプションをもてること。

※ 監理者が削除した記録はメタデータにマークされ記録内容とメタデータは隠され監査証跡に記録されること

83. 削除を破棄，移動を再構成とする代替をコンフィグオプションとしてもてること

※ メタデータもメタデータスタブを除いて削除される

84. 監理者は処分プロセスの外でクラス，ファイル，サブファイル，記録を削除できること

85. 利用者は削除候補のクラス，ファイル，サブファイル，ボリューム，記録をマークできること

86. 削除事象では削除を監査証跡に記録し監理者への報告を作成しコンテンツを削除し変更なら削除せず又他のファイルとのリンクをハイライトしメタデータの完全性を維持すること

87. 監理者はユーザが入力したメタデータ要素を変更できること。メタデータ要素への変更は監査証跡に格納されること

88. 監理者は，オリジナル記録が保存されている間に１以上のリダクションを作成できること。また，組織の要請でリダクション内の機微情報を削除又は隠すことができること

89. リダクションを作成した時は記録とリダクション内のメタデータに作成，日時，作成者，作成理由を格納すること

※ リダクションにオリジナルとの相互参照を格納することが望ましい

(h) オプション

物理的ファイル及び記録の管理

90. 監理者が物理的コンテナとして存在するクラスやファイルを識別できること

91. 監理者やユーザが物理的コンテナとしてのクラスやファイルのメタデータの入力や保守ができること

92. 場所，保管者，日付のログによるチェックイン/アウトで物理コンテナと記録の追跡を支援することが望ましい

物理記録の処分

93. 移管，エクスポート，廃棄が完了する前に物理的な移管，エクスポート，廃棄を確認すること

文書管理及び共同作業

94. 文書と記録を同じ分類体系且つ同じアクセス制御下で監理することが望ましい

95. 文書と記録を同じ分類体系下で監理するときは文書と記録を明確に表示すること

ケースワーク

96. ケースワーククラス及び非ケースワーククラスの為に異なるアクセス許可をもつケースワーカーの役割を構成できること
97. ケースファイルは特有のメタデータ要素で構成されること
98. 分類コードの替わりにケースファイル ID により取り出しや実行など正当なアクションがとれること

電子署名

99. キャプチャ時に電子署名と証明書をキャプチャし必要なら検証し保存できること。保存に際しては、長期署名措置が可能なこと
100. 電子署名された記録の検証メタデータを保存すること
101. エクスポート又は移管処理の間のファイル，記録，移管メッセージに第三者検証可能な電子署名を適用できることが望ましい

2.2 電子記録管理のアーキテクチャ

以下に、訪問調査を行ったデンマークの FESDⅡ、ハンガリーの Dossie、ドイツの ArcgiSafe、韓国の公認電子文書保管所（CeDA）の調査結果を紹介するとともに、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構築に向けたアーキテクチャの考察を行う。

2.2.1 デンマークの FESDⅡ

デンマーク（デンマーク王国）は、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）。また、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、1200 余あった市町村を 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 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、同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。

2.2.2 ハンガリーの Dossie

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 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。

2.2.3 ドイツの ArchiSafe

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。

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。

2.2.4 韓国の公認電子文書保管所（CeDA）

韓国では、2007 年から、原本性を保証する公認電子文書保管所（通称 ARC（Authorized Retention Center）または CeDA（Certified e-Document Authority））のサービスが始まっている。韓国の保管所は、電子商取引基本法第 2 条でその設置が定められており、第 31 条の 6（電子文書保管代行の効力）で、公認電子保管所が電子文書を保管する場合には、法律上の電子文書の保管が行われたものとみなすと規定されている。また、第 31 条の 7(電子文書内容の推定等)で、公認電子保管所に保管された電子文書は保管機関の中ではその内容が変更されていないことと推定および証明書に記載された事項は真正であることと推定すると規定されている。

韓国の公認電子文書保管所（以下、保管所という）の仕様は、認定機関の情報通信産業振興院（NIPA：National IT Industry Promotion Agency）によって策定された。保管所の技術規格として、5 つの規格が公開されている（いずれも原文はハングル）。

なお、公認電子文書保管所のアーキテクチャは、ISO14721（Reference Model for Open Archival Information System, OAIS）を参照している。

(a) インタフェース

利用者システムと公認電子文書保管所間の連携インタフェース技術仕様では、表 2.5 のメッセージが定義されている。このインタフェースを介して、利用者は、保管所への文書の登録（原本の登録）、検索、取得、第三者への文書発行、文書の廃棄、（原本性）証明書の発行/再発行、検証などを行うことができる。

表 2.5　利用者システムと保管所間の連携インタフェース

No	メッセージ	意味	備考
1	SubmitDocument	文書の登録（提出）	
2	GetDocument	文書発行	
3	DeliverDocument	第三者への文書発行	
4	GetDocumentByCert	証明書を使った文書の発行	
5	TransferDocument	文書の転送	
6	DeleteDocument	文書の廃棄	
7	ExtendRetention	文書のアーカイブ延長	
8	IssueCert	証明書の発行	
9	UpdateCert	証明書の更新発行	
10	VerifyCert	証明書の検証	
11	GetCert	証明書のダウンロード	
12	Search	検索	

(b) 情報パッケージ（付録２　参照）

電子文書の情報パッケージの目的は、公認電子文書保管所（以下「保管所」とする）を通じて流通する電子文書の全体的なプロセスを情報パッケージモデルの策定により電子文書の真正性を維持し、偽造・変造を防止することにより、電子文書の信頼性と完全性を図ることとしている。その背景には、他保管所のシステムおよび外部システムとの相互運用性を高め、保管所をベースとする e-ビジネスの活性化を図る狙いがある。

文書の真正性を維持するためには電子文書の構造、内容、業務の脈絡を保証する必要があり、これは電子文書をパッケージ化することにより確保している。実際の文書の内容とメタデータをまとめて関連付けたものを電子文書情報パッケージと呼び、文書を登録・移管あるいは保存・配布する物理的な単位となっている。

電子文書情報パッケージには次の種類がある。図 2.5 にそれぞれのパッケージの構造、表 2.6 にパッケージ構成要素、図 2.6 に証明書の構造の内容を記す。

① 提出用情報パッケージ（SIP; Submission Information Package）
　利用者のプログラムより提出され、受け入れられる文書。

② 保管用情報パッケージ（AIP; Archive Information Package）

保管所のシステムに登録されたれる電子文書。保管所のシステム内で一意の識別子を付与されて管理される。

③　配布用情報パッケ（DIP; Dissemination Information Package）

利用者の要請により保管用情報パッケージの一部あるいは全体を閲覧または発給するために構成される電子文書。配布メディアとパッケージのタイプ、メタデータの構成は利用者の要求により様々な構成が可能である。

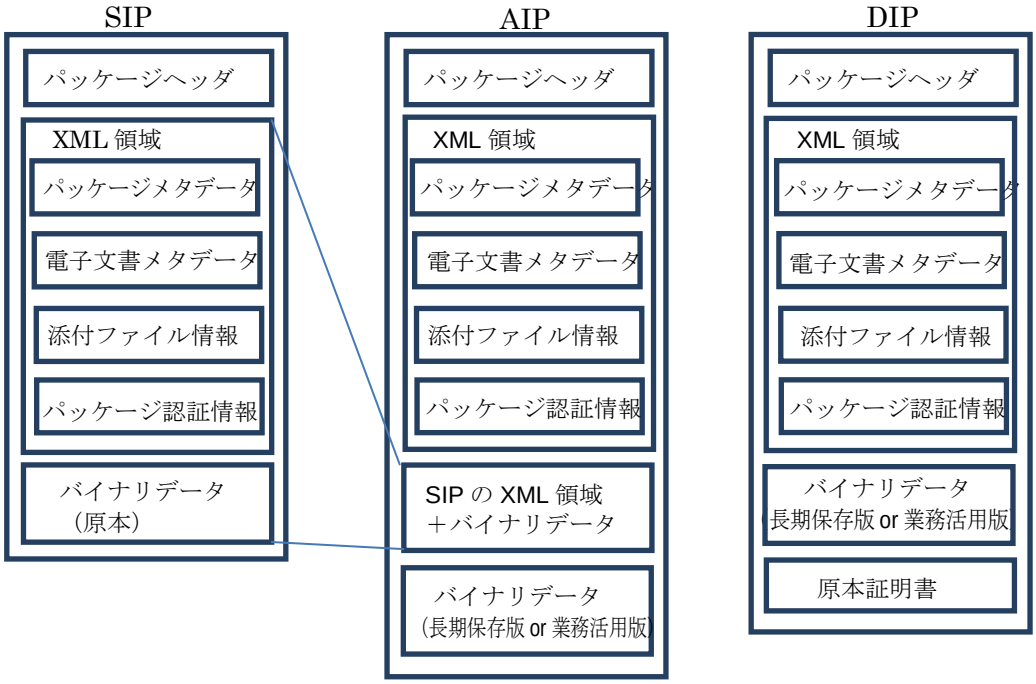
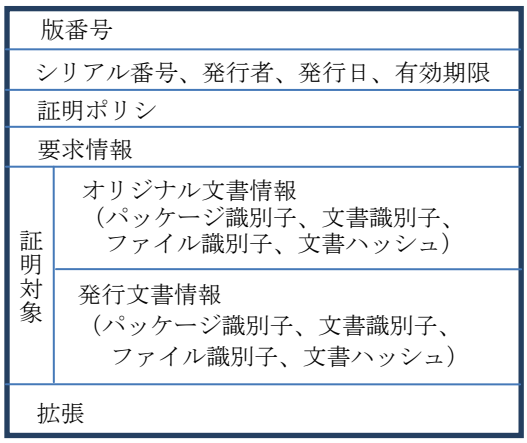


図 2.5　公認電子文書保管所のパッケージ構造



注記　証明書は、発行所によって署名される

図 2.6　証明書構造

表 2.6　パッケージ構成要素の内容

	構成要素	内容
1	パッケージヘッダ	版番号，種類，XML 領域１のサイズ，XML 領域２のサイズ，添付ファイルの個数，添付ファイルのサイズ
2	パッケージメタデータ	パッケージ識別子，保存タイプ区分，内容説明，電子文書の個数，XML 領域２のハッシュ値，ハッシュアルゴリズム，拡張領域
3	電子文書メタデータ	登録情報，分類情報，詳細情報，権限情報，保存情報
4	添付ファイル情報	添付ファイル ID，添付ファイル名，添付ファイルの作成日時，添付ファイルの説明，添付ファイルの容量，ソフトウェア（OS 環境，アプリケーション，版番号），添付ファイル認証（ハッシュ値，ハッシュアルゴリズム）
5	パッケージ認証情報	署名日時，署名，署名者 ID，署名者名，証明書情報（発行者，シリアル番号）
6	バイナリデータ	ファイル原本　｜　長期保存版　｜　業務活用版

(c)　保管所の移管（付録３　参照）

使用者の要求及び保管所の認証取り消しあるいは営業廃止などの事情により、電子文書を保管し続けることができない状況が発生した際、それまで保管中であった電子文書を他の保管所のシステムに安全かつ速やかに移管されるようになっている。

全ての保管所は、公認電子文書保管所移管の技術仕様を遵守し、保管中の電子文書を他の保管所に移管することができ、また、他の保管所が移管を要求する電子文書を受管できる必要がある。

移管対象となるデータは、各利用者別に保管を依頼した電子文書、初期登録証明書及び管理のための各種管理情報である。（表 2.7 参照）

表 2.7　移管データ

	移管データ	説明
1	電子文書	利用者が登録した電子文書の原文であり、TIP の形態に変換され、文書転送される。文書転送の必須対象情報である。
2	初期登録証明書	利用者が保管所に電子文書の登録を依頼した最初の時点で正常に登録されたことを証明するための構造体情報である。
3	利用者情報	両保管所間の協議のもと、電子文書の転送前に予め移管または登録されている必要がある。文書転送の選択的対象情報である。
4	管理情報	文書転送の選択的対象情報である。
5	電子文書に関する基本属性情報	パッケージ番号・登録日時・登録者・所有者
6	同、拡張属性情報	移管保管所及び管理される電子文書のタイプにより追加して定義される。
7	セキュリティ情報	電子文書に関するアクセス権限

2.2.5　訪問各国の電子記録保存システムの比較

今回調査した、デンマーク、ハンガリー、ドイツ、韓国の各々の電子記録管理システムの比較を表 2.8 に示す。

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。電子記録管理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管理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AdES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 2.8　訪問各国の電子記録保存システムの比較

項目		韓国	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

2.2.6　ビジネス記録の利活用基盤アーキテクチャの考察

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、欧州調査結果を参考にして、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アーキテクチャのあるべき姿を考察する。

(a)　安心・安全なシステムの観点から

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、日本ではタイムスタンプの法的裏付けがない。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。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といった、それ以前の問題がある）。

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。

[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。

[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。

(b) システムの相互運用性確保の観点

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。

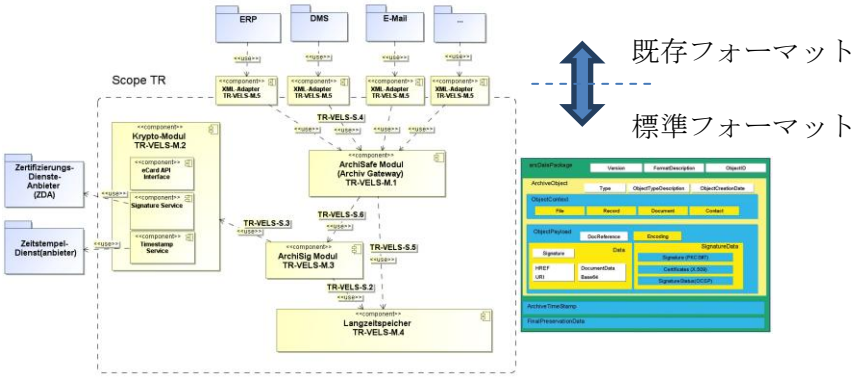


図 2.7　ArchiSig における互換性の考え方

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。

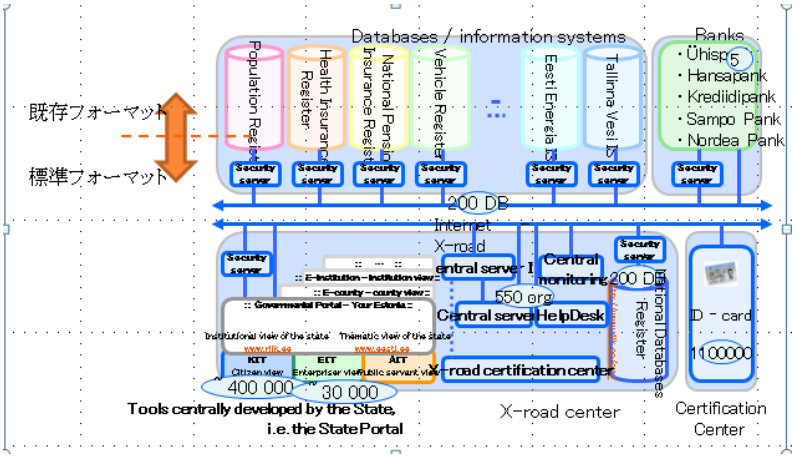


図 2.8　X-Road における互換性の考え方

[CASE の位置付け]

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（Shall）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 2.9 はデンマークの FESD II システムのアーキテクチャである。CASE、文書、アーカイブがコアとなっており、これは手本の非筒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。

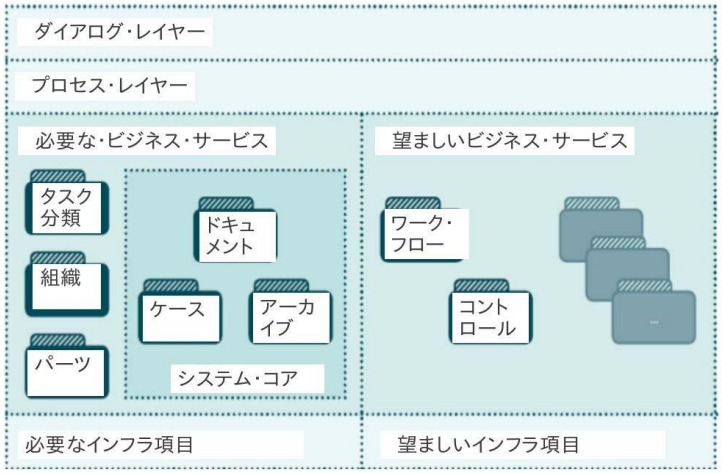


図 2.9　デンマークの FESD II システムのアーキテクチャ

[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。電子記録管理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 2.10 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。

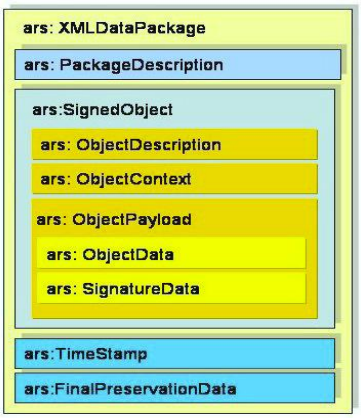


図 2.10　ArchiSafe のパッケージ構造

[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]

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も重要である。例えて言えば、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。

2.3　電子記録管理の実装

eRAP では，電子記録管理の実現に向け、あるべき姿としての要件を洗い出し、前述のように「2.1.3 主要 100 要件」としてまとめた。引き続き、現在，国内で実際に使用されている文書管理システムがどの程度主要 100 要件を満たしているか調査を行った。調査の目的は、現状のとのギャップを把握し、次年度以降の活動に反映させることにある。

ここでは MoReq2 と文書管理システムのオブジェクトとの対応を以下のように想定して調査を行った。

MoReq2	文書管理システム
Class	Folder
File	
Sub-file	
Volume	
Record	Document

図 2.11　MoReq2 と文書管理システムの分類体系

次に電子記録管理の要件に関して文書管理システムを対象に行った調査結果を報告する。

No	大分類	中分類	要件	調査結果※
1	分類体系とファイル構成	分類体系の設定	ファイルや記録を階層化されたクラスによる分類体系で表現できること ※全てのクラス，ファイル，サブクラス，ボリュームに説明（スコープノート）を入力できることが望ましい	○
2			分類体系の管理は監理者だけに許されること	○
3			分類体系の全て又は部分をインポートできること．分類体系をインポートするときは関連メタデータ，保存及び処分計画，監査証跡もインポートできること	△
4			分類体系の全てまたは部分をエクスポートできることが望ましい．分類体系をエクスポートするときは監理者がエクスポートするメタデータを選べること．このとき監理者の選択で関連する保存及び処分計画，監査証跡もエクスポートできること	△
5			別途規定される標準フォーマットでエクスポートすること	△
6			分類体系の全て又は部分をコピーする場合は関連メタデータ，全ての保持及び処分計画を含むこと	△
7			複数の分類体系が定義でき同時に使えること	○
8		クラスとファイル	クラス又はファイルのメタデータ内に，開始日(open)及び終了日(close)を格納すること	○
9			クラス又はファイルのメタデータ内に，新たなクラス，ファイル，サブファイル，ボリュームの作成日を格納すること	×
10			新たなクラス又はファイルを開始(open)したときはメタデータを継承すること．継承したメタデータ値は許される範囲内で監理者が変更できること	×
11		ボリュームとサブファイル	サブファイルやボリュームを監理者が作成できないようにも設定できること	△
12			新たなボリューム又はサブファイルを開始したときは，開始日をメタデータに格納し，上位集合のメタデータ値を継承すること	×
13		分類体系の保守	クラスの結合や分割ができること	×
14			再配置や再分類するとき，変更前の参照関係を保持すること（変更された体系に参照を付けること）また，新たな親クラスからの継承ができること	△
15			記録が再配置またはコピーされる時に監理者にメタデータとしてその理由の入力を要求すること	×
16			再配置又はコピー前の状態，及び再配置前のメタデータの値を記録すること	×
17			ユーザが関連ファイル間の相互参照を作成できることが望ましい	×
18			記録の重複なしに記録に対する複数エントリを作成できることが望ましい	○
19			ユーザはファイルや記録のコンテキスト（脈絡，たとえば属するクラス）を認識できること	○
20			ファイルの検索用キーワードを変更するときは，変更前の状態の痕跡を履歴として残すとともに，監理者に理由の入力を求めること	○
21	コントロールとセキュリティ	アクセス	識別され確証された認可(authorized)ユーザでない限りいかなる操作もできないこと	○
22		監査	操作やその時刻情報を自動的にキャプチャし格納した監査証跡を保持すること	○
23			監査証跡パラメタの変更，メタデータの変更，記録への注釈や変更，監理パラメタの変更が監査証跡に記録されること	△
24			アクセス制御の意図的違反行為をキャプチャし保存すること	○
25		バックアップとリカバリ	自動バックアップを提供すること	○
26			許可された監理者のみがリストア及びロールフォワードできること	○
27		重要記録	重要記録を含むか重要記録として扱われるファイルや記録を監理者が表示できること．また，最早重要と扱われないファイルや記録を表示できること	○
28			フルバックアップと重要バックアップの２つの独立した操作ができること	△
29	保持と処分	保持及び処分計画	監理者のみが保持及び処分計画を作成し維持（含，修正）できること	△
30			保持及び処分計画の変更履歴を改変できないよう維持すること	△
31			保持及び処分計画の変更は直ちに適用されること．変更理由は保存すること	×
32			全てのクラス，ファイル，サブファイル，ボリュームは１以上の保持及び処分計画をもつこと．デフォルトの場合は上位エンティティの保持及び処分計画を継承すること ※記録のタイプにデフォルトの保持及び処分計画を適用できることが望ましい	△
33			保持及び処分計画は保有期間及びトリガ事象または処分日，処分行為と理由を含むこと．処分行為として少なくとも永久保存，レビュに提出，自動廃棄，監理者承認後の廃棄，移管が許されること ※保存及び処分計画は説明と業務規程を含むことが望ましい	△
34			保存及び処分計画に従って保存期間が満了した場合は自動的に処分決定プロセスを起動すること．自動処理は監査ログをとり監理者に通知すること．レビュが必要なときは監理者に自動的に通知すること	△
35			監理者はレビュを委任することができること	△
36			許可されたユーザによる処分保留が許されること．処分保留の適用及び解除の場合はその日付，許可されたユーザの ID，理由をキャプチャし保存すること	△
37		処分のレビュ	計画が特定の期間に入ることを監理者に通知すること	△
38			メタデータと計画情報によりレビュプロセスを支援すること ※同じ記録のレンディション間のリンクを維持し処分行為を同時に行えること．レビュワが，廃棄，移管，更なるレビュ，永久保存のマーク付けをできること自動的にレビュ日のログが採れること	×
39			レビュ決定の理由を記録するためにレビュワがメタデータにコメントを入れられること	△
40			レビュ期間の理由を含むレビュワの決定の不変履歴を保持すること	×
41		移管，エクスポート，廃棄	記録をエクスポートできること．記録を移管またはエクスポートする場合は全てのコンポーネントの関係を維持したまま移管またはエクスポートすること	○
42			他のシステム又は他の組織に記録と関連メタデータと監査証跡情報を移管するよく定義されたプロセスを提供すること	×

43			エクスポートするメタデータ，監査証跡は選択できること．エクスポートまたは移管する場合はインプリシットなメタデータを含むこと	×
44			宛先システムでの再適用のために，記録と一緒に保持及び処分計画，アクセスコントロールをエクスポートまたは移管すること	△
45			ポインタではなく完全な記録をエクスポートまたは移管すること．記録はキャプチャ時のフォーマット及びレンダリングされたフォーマットでエクスポート又は移管できること	○
46			レコードが廃棄されるときは全てのレンディションも廃棄されること	○
47			廃棄または移管されたクラス，ファイル，サブファイル，ボリューム，記録のメタデータスタブを保存できることが望ましい．メタデータスタブは少なくとも廃棄日または移管日，分類コード，タイトル，説明，廃棄または移管理由，参照を含むこと	△
48	キャプチャ及び記録の宣言	キャプチャ	キャプチャプロセスはユーザに，記録のキャプチャ，分類体系への関連付け，ファイルと関連付けられた記録のためのコントロールと機能を提供すること	○
49			キャプチャする記録が複数コンポーネントで構成されるときは関連を保存し１単位として管理すること ※保存や表示に必要なら一部をモディファイ（例えば，HTML ページのリンク先のグラフィックを取り込む）できることが望ましい	×
50			キャプチャ時に記録内の参照を変更する場合は，監査証跡に自動的に記録されること	×
51			各コンポーネントのファイルフォーマット，バージョンは自動的にキャプチャしメタデータに格納する	○
52			メタデータ要素の幾つかの値は承認されたユーザと監理者のみが更新できる	×
53			記録はキャプチャされたときに適切なクラス又はファイルに割り当てられること	○
54			特定のファイル(フォルダ)にドロップされた記録に属性を自動付与することが望ましい	○
55			記録のキャプチャ日時がメタデータ及び監査証跡として記録されること．自動キャプチャできないメタデータ入力をユーザに促すこと	○
56			クラス，ファイル，サブファイル，記録の複数キーワード又は語彙の割り付けを支援すること	○
57			制御された語彙から選ばれるキーワード値及び他のメタデータ要素値を提供すること	○
58			キャプチャ時又はそれ以降にも追加の記述などのメタデータ登録ができること．監理者や権限を与えられたユーザが記録のタイトルを修正する余地があること（組織のオプション）	○
59			複数バージョンの文書をキャプチャした場合は全てを１記録とする，１つを特定，全て別の記録とするかを選べること	△
60			監理者はクローズしたボリュームに（クローズ以前の日付がある）記録を追加できること．この時例外理由がメタデータに追記されると共に監査証跡に自動記録されること	×
61		バルクインポート	記録のバルクインポートを実行すること	×
62			他のシステムで生成された取引記録をキャプチャできること（バッチファイルなど）	×
63			バルクインポートの間に関連記録のメタデータを自動キャプチャできること．キャプチャしたメタデータはルールを使って検証すること	×
64			インポートされた記録の履歴を表す監査証跡記録をインポートすること．監査証跡記録をその監査証跡にインポートしないこと（別々に格納）	×
65		e-メール管理	出入りする E メールキャプチャ時自動的にメタデータ（日付，受信者，主題，送信者，署名など）を抽出すること	△
66			ユーザがドラッグによって E メールをサブファイル，ファイル，クラスにキャプチャできることが望ましい	○
67			添付を別の記録としてキャプチャする場合はメタデータ値のキャプチャ又は入力を要求すること	×
68			プロプラエタリフォーマットでキャプチャした E メールメッセージをオープンフォーマットで格納できること	×
69		記録のタイプ	記録タイプを定義しメンテナンスすること ※記録の特性（メタデータ属性，保存要件，アクセス制御，文書の種類など）を記述	○
70			全ての記録は１つの記録タイプをもつこと	○
71		スキャニング及びイメージング	少なくとも１つのスキャニングソリューションとの統合が可能なこと	○
72			OCR 機能をもつときスキャンイメージと OCR 結果のテキストは１つの記録として管理すること	○
73			イメージの注釈，注釈者，日付は記録として保持され変更と削除から保護されること	×
74	参照	クラスコード	クラス，ファイル，サブファイル，ボリューム，記録，コンポーネントに分類体系の階層内でユニークな分類コードを関連付けること	○
75		システム ID	分類コード，クラス，ファイル，サブファイル，ボリューム，記録，レンディション，保存及び処分計画，文書に対してグローバルにユニークなシステム ID(UUID)を生成すること	○
76	検索，取り出し，及び表示	検索及び取り出し	アクセスが制限されているユーザにはいかなる情報も暴露しないこと	○
77			記録やファイル，関連メタデータを検索し取り出し，また表示できること．検索は，全文検索および属性検索が可能なこと	○
78			オリジナルフォーマットとは別のフォーマット（レンディション）で表示できること	○
79	監理上の機能	一般管理	コンフィグ時に設定した値を監理者が再設定できること	○
80			ユーザと役割に対して監理者が機能を割り当てできること	○
81		報告	監理者が定期的又は臨時の報告書を作成できるようにすること	×
82		変更，削除，及びリダクション(墨塗り)	一旦キャプチャした記録を削除又は移動できないオプションをもてること． ※監理者が削除した記録はメタデータにマークされ記録内容とメタデータは隠され監査証跡に記録されること	△
83			削除を破棄，移動を再構成とする代替をコンフィグオプションとしてもてること ※メタデータもメタデータスタブを除いて削除される	×
84			監理者は処分プロセスの外でクラス，ファイル，サブファイル，記録を削除できること	△
85			利用者は削除候補のクラス，ファイル，サブファイル，ボリューム，記録をマークでき	△

			ること	
86			削除事象では削除を監査証跡に記録し監理者への報告を作成しコンテンツを削除し変更なら削除せず又他のファイルとのリンクをハイライトしメタデータの完全性を維持すること	×
87			監理者はユーザが入力したメタデータ要素を変更できること．メタデータ要素への変更は監査証跡に格納されること	△
88			監理者は，オリジナル記録が保存されている間に１以上のリダクションを作成できること．また，組織の要請でリダクション内の機微情報を削除又は隠すことができること	×
89			リダクションを作成した時は記録とリダクション内のメタデータに作成，日時，作成者，作成理由を格納すること ※リダクションにオリジナルとの相互参照を格納することが望ましい	△
90	オプション	物理的ファイル及び記録の管理	監理者が物理的コンテナとして存在するクラスやファイルを識別できること	×
91			監理者やユーザが物理的コンテナとしてのクラスやファイルのメタデータの入力や保守ができること	×
92			場所，保管者，日付のログによるチェックイン/アウトで物理コンテナと記録の追跡を支援することが望ましい	×
93		物理記録の処分	移管，エクスポート，廃棄が完了する前に物理的な移管，エクスポート，廃棄を確認すること	×
94		文書管理及び共同作業	文書と記録を同じ分類体系且つ同じアクセス制御下で監理することが望ましい	△
95			文書と記録を同じ分類体系下で監理するときは文書と記録を明確に表示すること	△
96		ケースワーク	ケースワーククラス及び非ケースワーククラスの為に異なるアクセス許可をもつケースワーカーの役割を構成できること	○
97			ケースファイルは特有のメタデータ要素で構成されること	○
98			分類コードの替わりにケースファイルIDにより取り出しや実行など正当なアクションがとれること	○
99		電子署名	キャプチャ時に電子署名と証明書をキャプチャし必要なら検証し保存できること．保存に際しては，長期署名措置が可能なこと	○
100			電子署名された記録の検証メタデータを保存すること	○
101			エクスポート又は移管処理の間のファイル，記録，移管メッセージに第三者検証可能な電子署名を適用できることが望ましい	○

（※）○：要件を満たしている

△：一部要件を満たしている

×：要件を満たしていない

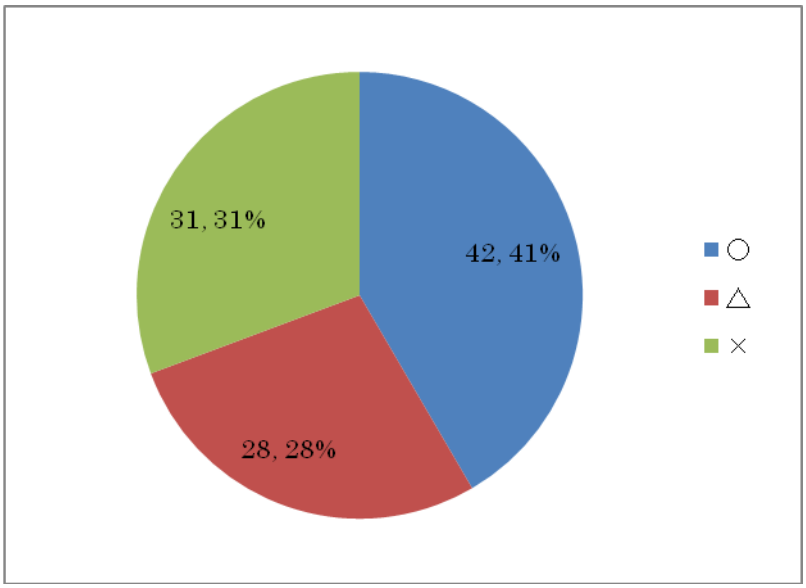


図 2.12　調査結果

調査結果として，日本国内で流通している文書管理システムの適応率は「○」、「△」合わせて69%(図 2.12)となった。

ただし、「×」となっている要件のほとんどは、以下の要因によるものだと考えられる。

・Moreq2 の要件は運用も含むサービス要件であり、システム単体では要件が満たせない

・Moreq2 の要件には，企業間での記録の利用のための要件が含まれているが、評価対象のシステムは企業内での記録の利用のためのシステムであること。

第３章　電子社会共通基盤

3.1　新たなステージに向かう電子署名

電子署名法が 2001 年 4 月 1 日に施行されてから 11 年が経過した。その間、電子署名に係る証明書として、公的個人認証サービスの電子証明書、商業登記に基づく電子認証制度の電子証明書、政府認証基盤の政府共用認証局が発行する電子証明書、地方公共団体組織認証基盤に係る認証局が発行する電子証明書、認定認証業務に係る電子証明書等が発行されてきており、保健医療福祉分野公開鍵基盤（HPKI）における電子証明書や JCAN ビジネス証明書などの新分野の証明書が発行されつつある。これに伴い、電子署名の利用分野も、公的分野、国税関係書類のスキャナ保存、医療情報システム、知財保護、電子契約・電子商取引、その他へと広がっている。[参考文献 1]

ところが、証明書の人口に対する普及枚数を見てみると日本の場合人口 12700 万人に対してせいぜい 140 万枚程度（1%強）であり、電子署名における他の先進国と比較すると桁違いに少ないことが分かる。このことは筆者らの直感にも適ったものであり、すなわち期待していたほど電子署名は普及してはいない。

表 3.1　各国の電子署名用証明書発行枚数

	エストニア	ベルギー	韓　国	オーストリア	デンマーク	スウェーデン	フィンランド
人口	約 134 万人	約 1058 万人	約 4846 万人	約 823 万人	約 551 万人	約 918 万人	約 532 万人
発行枚数《年》	約 105 万枚《2009》	約 850 万枚《2008》	約 1790 万枚《2008》	約 10 万枚《2007》	約 134 万枚《2009》	約 230 万枚《2009》	約 24 万枚《2009》
対人口比	約 80%	約 80%	約 37%	約 1%	約 24%	約 26%	約 5%

出典：電子政府ガイドライン作成検討会「セキュリティ分科会報告書」、2010 年 2 月

その原因は様々考えられるが（eRAP メンバで検討した結果を附録に示す）、これを打ち破り、電子署名を普及させる方向に導くことができそうな新たな動きがでてきている。本節ではそのような新たな動向として、モバイル環境やクラウド環境における PKI の活用について、主に米国で台頭してきた PKI にとらわれない次世代の電子署名サービスや非 PKI への対応を目指した韓国における電子署名法改正の動き、そして PKI における電子署名を更に利用しやすくするような標準化の動きについて紹介する。

[参考文献 1] 日本データ通信協会、“タイムスタンプ活用事例”、 日本データ通信、 2010 年 11 月号

3.1.1　モバイル＆クラウド時代の PKI 活用

(1)　クライアント環境の多様化

この数年で IT 環境が激変している。従来のサーバ＆クライアント PC の環境と、モバイルと言

えば i モード等の携帯電話が主流であった。それが近年ではサーバ環境はクラウド環境に進化し、クライアント環境としては新たに高機能なスマートフォンやタブレット（スレート）端末も加わり多様化している。つまり現在ではクラウド技術により提供されるサービスを、スマートフォンやタブレットやクライアント PC 等の多様化したクライアントから横断的に利用する環境が実現している。モバイルとクラウドの環境は前提として、常にまたは頻繁にネットワークに接続されている。ネットワーク上に展開されるクラウドサービスを多様なクライアントから利用するイメージとなる。

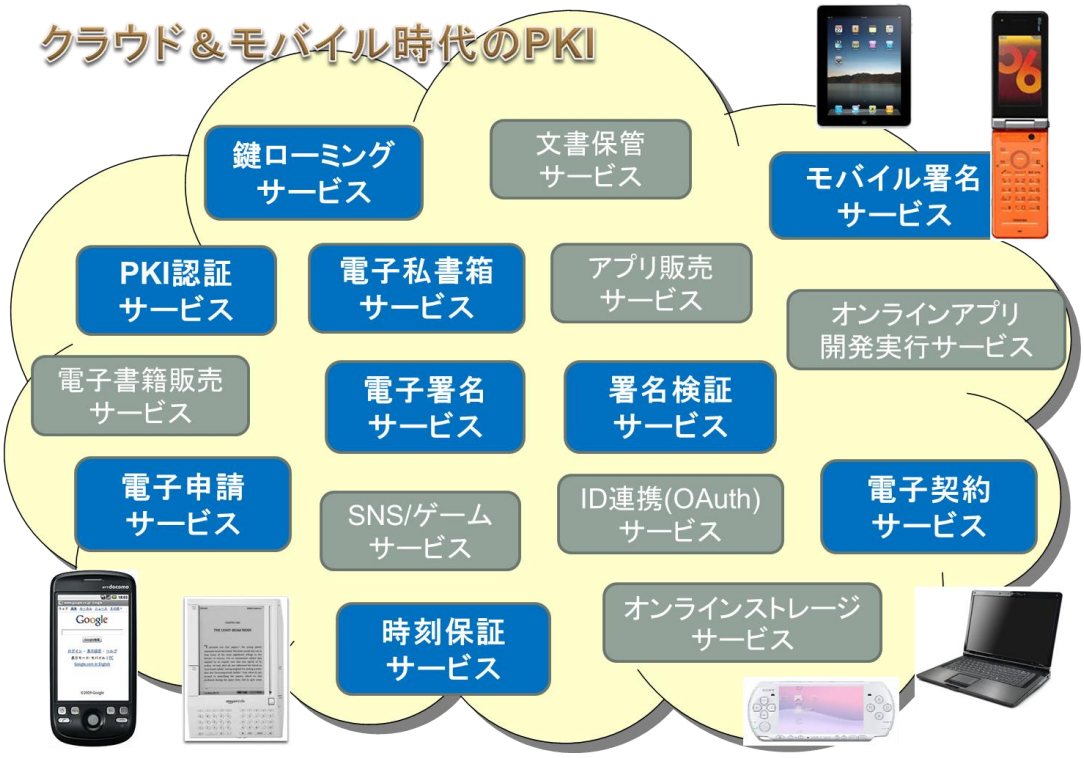


図 3.1　クラウド＆モバイル時代の PKI イメージ図

ネットワークを利用したクラウドや、モバイル環境で利用されるスマートフォンでは従来以上にセキュリティの必要性が求められている。しかしながら現実にはまだまだ電子署名や電子認証は各種の取り組みは始まっているものの普及途上にある。電子署名はアプリケーションの配布時には必須になりつつあるが、一般のドキュメントや電子データにおける電子署名の利用は普及が待たれる状況である。電子認証も ID とパスワードによる認証がまだまだ多い。しかしながら OTP（ワンタイムパスワード）や PKI 技術による電子認証の標準化も進んでいる。更に ID とパスワードによる認証だけでは無く他の認証技術と組み合わせる多要素認証も利用が進みつつある。

ここでは、モバイルとクラウドの環境におけるセキュリティ技術に関して PKI 系技術を中心に現状や課題をまとめることを目的とする。その前にクラウドの定義とモバイルの現状分析をまとめる。

① クラウドの定義

クラウドは NIST（米国国立標準技術研究所）の定義によると、SaaS・PaaS・IaaS の 3 種類のサービスモデルに分類できる。NIST はクラウドの特徴やサービス展開モデルの定義している（http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc）。

表 3.2 クラウドのサービスモデル定義（NIST）

サービスモデル名	概要
SaaS （Software as a Service）	ソフトウェアによりサービスを提供する。従来の ASP サービスも SaaS と言える。
PaaS （Platform as a Service）	ネット上にてソフトウェアの実行プラットホーム環境を提供する。新たな OS の提供に近い。
IaaS （Infrastructure as a Service）	計算資源やストレージ等のインフラを仮想的に提供する。ハードウェアの仮想化サービスである。

SaaS は ASP サービスもその 1 種と言えるが、一般に使われるソフトウェアサービスの提供が SaaS である。SNS（Social Network Service）であったり仮想ストレージサービス等多様なサービスが既に提供されている。PaaS と IaaS の違いは少し分かり難いかもしれない。IaaS はハードウェアを仮想化して提供するサービスと言える。仮想化することでハードウェアの故障から開放されると共に必要に応じた各種資源の増減が可能となる。現時点では IaaS サービス上に SaaS のサービスを提供する形態が多い。

一方 PaaS はクラウドを利用したソフトウェアの実行環境を直接提供するものである。Java 系の技術を使ったものが多いが、直接 API を提供することで仮想化に必要となる無駄が省け高速かつシンプルに SaaS のサービスの構築や提供が可能になる。PaaS サービス上での SaaS のサービス提供形態は今後増える可能性があるが現状ではまだ数は少ない。

利用者から見ると IaaS と PaaS の違いは直接関係が無い。SaaS としてのサービスのみを見て利用されることになる。

② クライアント分析

iPhone 以来急速にスマートフォンが普及している。更にスマートフォンと同じ OS（iOS や Android）を利用したタブレット（スレート）端末もこの 1 年で普及が加速している。これらは、従来のクライアント PC（ノート PC を含む）と携帯電話の間を埋める端末であり一部ではクライアント PC の代わりとしての利用も進みつつある。また別の見方をするとソーシャルサービス等での利用方法として、手軽に持ち運びが出来る高機能なクライアント端末としての可能性を秘めており新たな次元の端末としての利用が期待される。創造的な作業はこれからもクライアント PC が主に使われるが、単にサービスを利用するだけである場合にはスマートフォンやタブレット端末でも充分になってきている。スマートフォンやタブレット端末は家電のようにすぐに使えてシンプルな操作が実現でき安価である点が利点と言える。タブレット端末は既にオフィス内でも使われ始めている。

表 3.3　クライアント端末の分類

クライアント分類	近年の状況
デスクトップ PC	ノート PC の高機能化により徐々に少なくなっている。
ノート PC	モバイル的な利用ではタブレット端末やスマートフォンに移行。
タブレット端末	ノート PC の代わりにクラウドサービスの利用に使われはじめた。
スマートフォン	モバイル環境においてもクラウド利用が可能になる。
携帯電話	まだまだ使われているがスマートフォンに移行も増えてきた。

更に純粋なクライアントでは無いが専用の端末として電子書籍端末やゲーム機も高機能化とネット接続を前提にしつつある。

(2)　モバイル＆クラウド分野のセキュリティ技術の可能性

モバイルとクラウドの特長を踏まえてここでは主に PKI 技術をベースとした、電子署名と電子認証のモバイル＆クラウド分野における利用可能性を考察する。

スマートフォンやタブレット端末と言った新しいモバイル端末の出現により利用者は場所や時間を選ばず常にクライアント端末とネットワークインフラを利用してクラウド上のサービスの利用が可能となった。クラウド側がクライアント端末をどのように認証するのかはセキュリティ的に重要かつ不可避の要求であろう。現在多くのクラウドサービスは主に ID とパスワードを利用している。これに対して新たな標準として OTP や PKI 技術を利用した電子認証の技術や標準が広まろうとしている。まずはこの電子認証について考察する。

認証の次に署名についても考察する。署名に関しては海外では非 PKI 系のサービスが広がろうとしている。主に紙の契約書にペンで署名したものを電子的に可能にするサービスが多い。またクラウドサービスからの要求によりモバイル端末で電子署名を行うモバイル署名（Mobile Signature）も海外では使われている。これらを踏まえて非 PKI 系も含めた電子署名の可能性と課題についても考察する。

①　電子認証

現在コンシューマ向けの主なクラウドサービスはほとんどが ID とパスワードにより認証を行なっている。ID パスワードベースの認証技術は、OAuth（http://oauth.net/）や OpenID（http://www.openid.or.jp/）等のシングルサインオンの仕組みが標準化され広まろうとしている。ID とパスワードの仕組みは手軽であり便利ではあるが、ID もパスワードも単なる文字列の情報である為にフィッシングや電話等の口頭ベースで簡単に漏洩してしまう恐れがある。この為にビジネス用途としてはセキュリティ的に不安が残る。ID とパスワードに加えてハードウェアの利用や PKI 的な技術により、コピーが困難な別の認証を組み合わせる多要素認証や多段階認証の利用が好ましいと考えられる。

ID パスワード認証以外に考えられる認証方式としては、OTP（One Time Password）による

認証、PKI ベースの認証、モバイル機器の SIM による認証、生体認証等がある。これらを組み合わせて利用することが望ましい。

表 3.4　主な認証方式の分類

認証方式	特徴
ID パスワード認証	簡単便利であるが ID とパスワードが漏洩する可能性がある。
OTP 認証	専用ハードを利用することが多く安全だがコストがかかる。
PKI ベース認証	認証局等のインフラを利用すれば安全に認証が行なえる。 ただし秘密鍵や証明書の管理をきちんと行なう必要がある。
SIM ベース認証	モバイル機器に内蔵されている SIM を利用する。 場合によってはプライバシーの配慮も必要になる。
生体認証	生体を識別するハードが必要となる。

主にワンタイムパスワード等の認証系ベンダーが主体の業界団体が推進する規格である OATH（http://www.openauthentication.org/）では OTP 認証・PKI ベース認証・SIM ベース認証の 3 つの認証方式の利用に関して標準化されている。今後は OATH のような ID パスワード以外の認証の標準化普及を期待する。

モバイル機器における PKI ベースの認証では、別途トラストアンカーをどのように管理するのかと言う点が課題となる。トラストアンカーの問題は後述する電子署名においても考慮が必要となる。スマートフォンでは iOS（http://www.openauthentication.org/）・Andoroid（http://developer.android.com/）・BlackBerry（http://ap.blackberry.com/jpn/）・Windows Phone（http://windows.microsoft.com/ja-JP/windows/products/windows-phone）等の多様な OS や実行環境がある。それぞれで PKI 的なインフラをどのように管理できるのか、出来れば統一した PKI 環境の実現が望ましい。モバイル機器は今後決済端末としての利用も拡大すると予想され、よりセキュアな機能やハードが実装されて行く可能性があり注目して行く必要があるだろう。

② 電子署名

電子署名と言えば PKI を利用した方式が一般的だが、海外では非 PKI 系の署名サービスである DocuSign（http://www.docusign.com/）や EchoSign（http://www.echosign.com/）が提供されている。一部電子署名を利用しているがほぼ同様の署名サービスとしては Adobe eSIGNATURES（https://esign.adobe.com/）や 2011 年 4 月にサービスを開始した SignNow（https://signnow.com/）等も提供されはじめている。非 PKI の署名はサーバ側で認証と承認を行ない、手書きサインのかわりに署名外観を埋め込むことで署名として利用している。日本国内では長期署名を利用した PKI 系の署名サービスも開始されている。国内外共に主に電子契約書に利用されている。電子署名の本来的な利用方法でありビジネス分野では手堅い成長が期待される。非 PKI 系の署名についてはすぐに日本国内で認められるものでは無いと考えられるが今後の海外動向はチェックして行く必要がある。

電子契約書以外では、クラウドサービスを運営する上で安心を与え安全を保証する為に利用ログ等の保管時に電子署名を利用することも必要になってくると考えられる。改ざんされていない

ことを保証するだけであれば電子署名以外にタイムスタンプの利用も考えられる。このようにクラウドのインフラを保全して行くには電子署名やタイムスタンプの技術利用は有効であると考えられる。利用者から見た場合には安全が保証されることで安心して利用して貰えると考えられるのでインフラレベルでの電子署名技術の利用も普及が望まれる。

PKI 的な電子署名技術を考える上で秘密鍵をどのように保管して管理するかと言う問題を解決する必要がある。クライアント端末が多様化することで一人が複数のクライアント端末、例えばデスクトップ PC とノート PC とスマートフォン等を組み合わせて利用することが考えられる。従来は各端末の OS 上に用意されている証明書ストアに入れて管理するか、IC カードや USB トークンに入れて管理していた。クライアント端末の数が増えるとその全てに秘密鍵を入れておくのは好ましく無い。一方で IC カードや USB トークンは専用のハードやドライバソフトが必要となり多様化したクライアントへの対応が難しい。これを解決できる技術としては、モバイル機器がサーバと通信を行い署名自体はモバイル機器だけで行うモバイル署名や、サーバ（クラウド）側で秘密鍵を管理するサーバサイド署名（鍵ローミング）等があるだろう。

モバイル署名はトルコの Turkcell 社が既に携帯端末を利用した Mobile Signature（http://www.turkcell.com.tr/en/AboutTurkcell/services/mobilesignature）として実現している。利用手順はサーバ側から送られてきたハッシュ値と署名要求を確認して署名を行なって結果をサーバ側に返すことで実現される。署名要求が遅れるサービスやアプリケーションであれば利用できる。欧州ではモバイル署名のような技術の標準化も進んでおり今後動向をチェックする必要があるだろう。またモバイル機器の内部にどのように秘密鍵を保管するかも検討が必要だろう。またモバイル機器を紛失した場合の対応も検討しておく必要ある。Turkcell 社のモバイル署名では PIN コードの入力が別途必要となっている。モバイルの視点から見るとモバイル署名は自然な利用方法と言えるかもしれない。

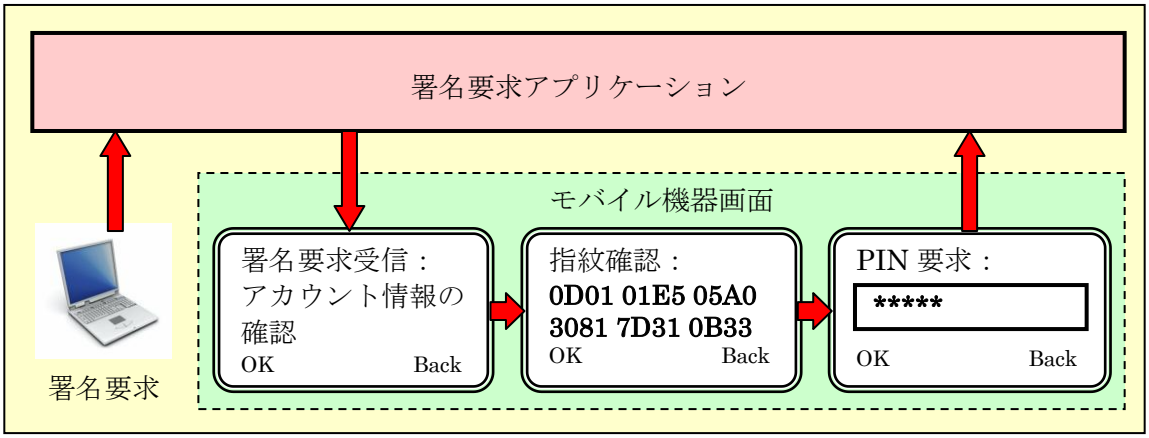


図 3.2　モバイル署名の利用手順

サーバサイド署名（鍵ローミング）は従来から使われている技術だがサーバの進化形であるクラウド環境においても有効な利用方法だと考えられる。サーバサイド署名では不正利用を防ぐ為に利用時の認証が非常に重要になる。ID とパスワード以外の認証も併用するような多要素認証

や多段階認証が望まれる。さらに正しく運用して鍵を不正利用されないようにする必要がある。ただしいたずらに認証を厳しくするのでは無く必要十分な認証として使い勝手の面も考慮する必要がある。認証や運用の問題がクリアできればクラウドと言う環境を考えた場合にはむしろサーバサイドで鍵を管理する方が自然な利用方法と言えるかもしれない。

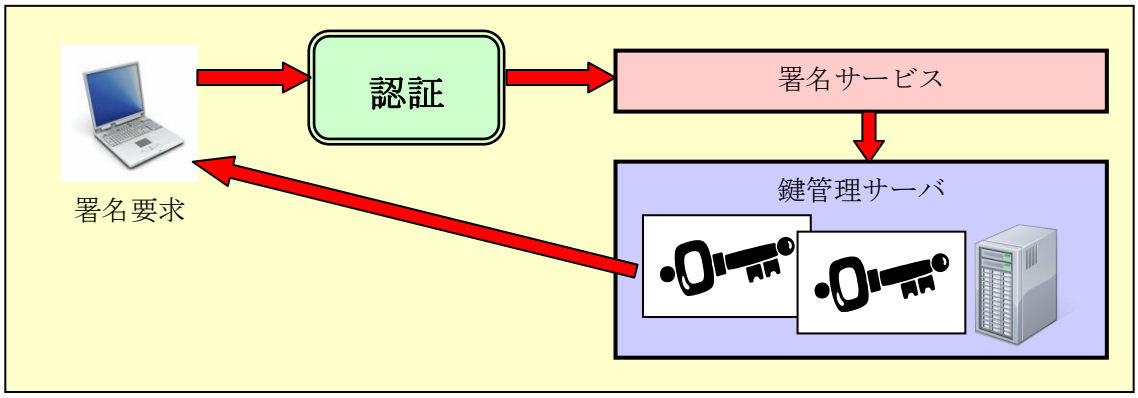


図 3.3　サーバサイドに鍵を置く鍵ローミング

スマートフォンのアプリ開発では電子署名を利用することで安心と安全を保証している。今後は電子書籍やその他のコンテンツ配信時においてもサービス提供者側が電子署名を付与することで安心と安全を保証できる可能性がある。電子書籍のフォーマットとして有望視されている EPUB（http://idpf.org/epub/30）は XML 形式であり既に電子署名の仕様も決まっている。残念ながら電子書籍を閲覧するソフトウェアが電子署名の検証に対応している例はほとんど無いのが現状である。今後はサービス提供者側が積極的に電子署名の利用を検討して行けるように情報を提供して行く必要があるのではないだろうか。PDF フォーマットに関しても PAdES により電子署名部の仕様が固まったことで今後の電子署名の利用促進が期待される。

ここに述べた以外にもクラウド分野では、Twitter（http://twitter.com/）や FaceBook（http://www.facebook.com/）等のソーシャルネットワークのサービスや、Dropbox（http://www.dropbox.com/）や Evernote（http://www.evernote.com/about/intl/jp/）等のオンラインストレージのサービス等が普及している。これらの新しいクラウドサービスにおいて電子署名の技術が応用できる可能性が無いか今後検討をして可能なら応用方法を提示してよりセキュアなサービス提供を促進したい。

(3)　新たな環境にむけて

従来はサーバとクライアント端末はほとんどが１対１の関係で済んだ。しかしながらモバイル機器の普及によりクライアント端末は多様化し一人で何台ものクライアントを保有する状況となった。またサーバ側もクラウド化してサービス間も連携して動作するようになり多対多の関係になっている。このように利用環境は変化しているが基本となる電子署名や電子認証の技術は継続して応用が可能であろうと考えている。新たな環境に向けて一度思考をリセットして新たなまたは従来通りの利用方法を今後検討し提案して行くことで電子署名分野の発展を目指したいと考えている。

モバイルとクラウドによるサービスは使いやすく無いと全く使われない。セキュリティは必要だが過度に適用や要求はせずに、必要十分なセキュリティの検討と実施が求められるだろう。

電子署名のサービスは表立っては電子契約等で利用されて行くことになる。しかしながら目に見えないバックグラウンドで安心安全を守る為の技術として電子署名等の PKI 系技術の必要性はむしろ高まっているように思える。今後は海外動向もチェックしつつ日本に合った電子署名の応用を考えて行く必要があると考えている。

3.1.2 次世代電子署名

PKI による電子署名は安全ではあるが非常に複雑であるため、PKI を使わない試みも行われている。本節では主に米国で台頭してきた、署名者が PKI を使う必要のない電子署名サービスとして、DocuSign、EchoSign、その他を、また韓国における PKI 以外の電子署名に法的効力を与えようという新たな試みについて紹介する。

(1) DocuSign

DocuSign（http://www.docusign.com/）は米国の電子署名サービスで、既に 500 万以上の署名者が毎年数百万のトランザクションで利用しているという。このサービスは Web サイトを通じて提供され、利用者は PC の他、iPhone や iPad より簡単にサービスを利用することができる。Salesforce や REALTORS といったサービスにも組込まれている。

電子署名を得るための手続きは次の通りである。

① 電子署名を相手（署名者）に要求する利用者（要求者）が、署名対象の電子文書を DocuSign のサーバにアップロードする。
② アップロードされた電子文書を確認し、電子文書上で署名領域を指定する。
③ すると DocuSign は署名者に対して署名対処文書へのリンクを含む電子メールを送信する。
④ 署名者は送付されたメールのリンクを辿り、DocuSign サーバを起動、署名対象文書が表示される。
⑤ 署名者は表示された署名対象文書を確認し、署名の表示スタイルと署名場所を選択する。
⑥ 署名つき文書を保存するとともに要求者にメールで送信する。

このように、署名者は予め公開鍵証明書の発行を受ける必要はない。電子メールの利用環境があればすぐにこの電子署名サービスを利用することができる。（ただし要求者は予めサービスにアカウントを登録しておく必要がある）

DocuSign サービスが TTP（信頼のおける第三者機関）として署名者と要求者を仲介し、署名対象文書の内容と署名者を保証する。ここでは PKI による電子署名技術は利用されておらず、DocuSign の TTP としての信頼性と、署名者のメールベースの認証によって電子署名の効果を成立させようとしている。

DocuSign サービス提供者が署名を偽造できてしまう構造と思われるために、日本における電子署名法では法的な要件が満たされないと判断されるであろうが、DocuSign は米連邦政府の Electronic Signatures in Global and National Commerce Act of 2000 (ESIGN) と Uniform Electronic Transactions Act (UETA)に準拠しているという。今後、世界的な流れとしては同様

のサービスの利用が拡大していく可能性も否定できない。

(2) EchoSign，その他

EchoSign（http://www.echosign.com/）も DocuSign とほぼ同様の米国の電子署名サービスである。こちらも 2009 年にはユーザ数が 100 万人を突破したとのことである。

処理手順は DocuSign とほとんど変わりはなく、やはり TTP としての信頼性と、署名者のメールベースの認証によって電子署名の効果を成立させようというものである。米連邦政府の電子署名法への準拠を謳っていることも同様であり、日本における電子署名法には準拠しないであろうこともまた同様である。

このほか、米 Adobe 社がベータ版ながら電子署名サービス Adobe eSIGNATURES（https://esign.adobe.com/）を提供している。このサービスでは、最終的に署名対象文書にサーバの PKI 署名が施されるところが DocuSign や EchoSign とは異なる。

また、米国の SignNow 社が 2011 年 4 月に電子署名サービス Signnow（https://signnow.com/）をリリースした。このサービスは署名者、要求者ともにアカウントを登録する必要がなく、更に容易に利用できることを特長としている。ただし、実在しないメールアドレスを利用しても署名が可能であり本人確認の面で疑問が残る仕様となっている。この点注意を要するものと思われる。

(3) 韓国の電子パッド署名

韓国では、電子パッドを使った手書き署名入力にある条件の下で法的効力を認めるような電子署名法の改定が計画されている。韓国の公認電子文書保管所（http://www.ceda.or.kr/Eng/）では、既に保管文書への利用者の署名を電子パッドを使った手書き署名入力としているケースも存在する。計画されている改訂では、このようなケースにおける条件を正式に法制化することによって安全性を維持しながら電子署名の利便性を高めようとするものと思われる。

改定案の詳細は明らかとなっていないが、公認電子文書保管所を運営する KTNET 社（http://homepage.ktnet.co.kr/servlet/ktnet?pgmid=engmain）の担当者からの情報によると、正当な電子署名と見做す条件として次の要素を考えているとのことである。

- 署名者と要求者が対面であること（非対面の場合は PKI による電子署名しか効力を認めない）
- 署名者が直接入力すること
- 署名対象となる情報の価値に依存させる（高価な情報の場合は PKI による電子署名しか効力を認めない）
- 本人性確認のため、署名動作を CCD カメラでの撮影、本人の携帯電話の利用、ID カードのコピー取得等と組み合わせて行なう
- タイムスタンプで署名の時期を保証する
- 大胆な試みであるが、国連の電子政府に関するランキングで第 1 位となった韓国の勢いを感じさせる動きである。

3.1.3 電子署名に係る新たな標準化動向

署名やタイムスタンプの検証者にとって認証局やタイムスタンプ局といった機関の信頼性をどのようにして判断するかは悩ましい問題である。欧州（EU）ではこの問題へのアプローチとしてTSL(Trusted Service Status List)と呼ばれる信頼点のリストを作成する仕組みを構築し運用を開始している。以下にTSLの概要を紹介する。

(1) Trusted Service Status List

TSLとは認証局などの信頼できる認証サービスプロバイダに関する情報をリスト化して公表する仕組みである。認証サービスプロバイダとはEU電子署名指令に基づくクォリファイド証明書を発行する認証局や、その他の認証局やタイムスタンプ局などを運用している事業者のことである。このリストにはこれらの事業者への認定や監査の状態などの情報も記載される。リストの形式には人が読める形式（例えばPDF）だけでなく、機械で処理可能な形式(XML)があり、システムやアプリケーションが自動で処理できるようになっている。TSLの技術仕様はETSIで標準化しており、その標準仕様に基づくガイドラインもEU官報で公表している。TSLはEU諸国が自国で運用している認証サービスプロバイダについて作成し公開することになっている。また、欧州委員会では各国のTSLが簡単に参照できるように、各国のTSLへのリンクを含んだcentral listを発行している。

TSLのような仕組みを導入した背景にはEU諸国の認証サービスプロバイダに対する信頼関係を築くための負荷を軽減する狙いがあると考えられる。EUではEU諸国間の電子商取引や電子申請をより活性化させるための基盤として電子署名を重要視しており、各国が扱う電子署名の水準がある一定になり相互運用が可能になるような枠組み作りに取り組んでいる。法的な枠組みとしてはEU諸国で策定される電子署名法の指針となっているEU電子署名指令があり、それを背景とした技術や運用に関する標準規格を策定している。EU諸国はこれらの枠組みをもとにして、それぞれの国の事情に合わせて電子署名に関する法制度やサービス、アプリケーションを構築している。実際に各国で運用される認証サービスプロバイダの種類や運用、本人確認など保証のレベルに差異はあるため、相手国の認証サービスプロバイダをいかにして信頼するのかという問題がある。特にEUのように多数の国との電子文書交換が想定される場合には、メッシュ構造のように各国がそれぞれの相手の国ごとに認証サービスプロバイダを評価していくことは非常に困難であり現実的ではなく、TSLという認証サービスプロバイダの評価スキームに関する統一的な仕組みを構築することが求められたと考えられる。EUがこれまで取り組んできた法的な枠組み、技術・運用に関する枠組みに加え、TSLは信頼に関する枠組みへのアプローチとしてとらえることもできる。

(2) PDFの長期署名(PAdES)とビジュアル化

PKIの仕組みは信頼点を信頼することを前提として、機械的に真正性を検証可能な仕組みであるが、実際の利用場面ではデバイスやサーバの認証など機械的な処理だけで完結するものもあれば、人間が署名やタイムスタンプ付きのデータをアプリケーション等で検証して表示された情報をもとに受け入れ可否を判断することもある。署名やタイムスタンプ、証明書の仕様は基本的に機械的に処理されることを目的としたものであり、人が見ても分かりやすいものではない。その

表示方法についてもこれといった標準や指針があるわけでなく各アプリケーションごとに独自に行っているのが実態である。しかし、最近では欧州を中心として署名や証明書の表示に関する標準策定の動きがある。人にとって分かりやすくアプリケーションによらない表示方法を構築することは、署名やタイムスタンプ普及促進のためにも重要な課題である。以下に表示に関する海外の標準化動向を紹介する。

① 長期署名(PAdES)

ETSI TS 102 778 として策定された PAdES により PDF で長期署名を実現することが可能になった。Acrobat X/Adobe Reader X より PAdES(Part2～4)がサポートされ、広く普及している Adobe Reader で検証や画面表示が可能になったことにより、長期署名の利用がより活発化することに期待できる。

この規格の Part6（Visual Representations of Electronic Signatures）では署名やタイムスタンプ、証明書の画面表示に対する要件や推奨について定めている。

また、技術標準ではないものの ETSI SR 003 232 という報告書では PAdES の署名データと印刷された紙文書を結びつける仕組みの提案と課題が記述されている。この提案は、電子データから紙へ印刷するときに、署名データのハッシュ値等を文字列やバーコード等で共に印刷することで、どの署名データから印刷されたかを分かるようにすることが狙いである。同報告書ではまだ概念的な構想の段階であり、この仕組みを実現するためには、元の署名データにはどのような情報を記述するのか、署名後に生成される署名の印刷データをどのように格納するか、など様々な課題を解決しなければならない。

② 証明書イメージ(Certificate Image)

証明書所有者に関する画像情報を証明書とリンクさせるための規格で、IETF の PKIX ワーキンググループでドラフトが作成されている。証明書の拡張領域に画像情報への参照情報や画像情報そのものを格納することができる。通常、証明書に記載される所有者の名称は識別名(DN)の形式で書かれており、証明書検証者にとって所有者を特定するために扱いやすい名称であるとは限らない。証明書検証の実行と共に証明書所有者に関する画像を画面上に表示することで判断しやすくする狙いがある。

3.1.4 署名やタイムスタンプの視覚化に関する議論

3.1.3 節で述べたように欧州を中心として署名やタイムスタンプの表示に関する標準化の動きがある。eRAP においても表示に関する問題に対してどのようなアプローチが可能であるか議論を行った。署名やタイムスタンプの規格と文書フォーマットの規格をあわせて考えていく必要があるため容易な問題ではなく、今後も検討を継続していく必要がある。ここでは今期の議論で得られた途中経過を紹介する。

表示方法は署名やタイムスタンプで一貫性のあるものであり、さらに、各文書フォーマットで可能な限り差異がないように共通化された方法であることが望ましいと考えられる。このような表示方法を実現することを目指して、現状では次のような案を検討している。

・CMS SignedData や XML 署名の署名属性(プロパティ)に署名のイメージ画像や表示情報（以降、これらを署名イメージ情報と呼ぶ）を格納する新しい属性を提案する。この方法であれば、タイムスタンプトークンも CMS SignedData であるためタイムスタンプにも適用できる。
・署名イメージは例えば署名者による手書きの名前、陰影、装飾のあるスタンプなどが考えられる。
・署名イメージ情報には実際に文書を描画したときに配置される署名イメージの場所（座標等）を含めることができる。
・署名イメージ情報は署名者（タイムスタンプの場合にはタイムスタンプ局）が作成する。
・署名イメージ情報は様々な形式の情報（例えば JPEG や PDF など）を含めることができる。

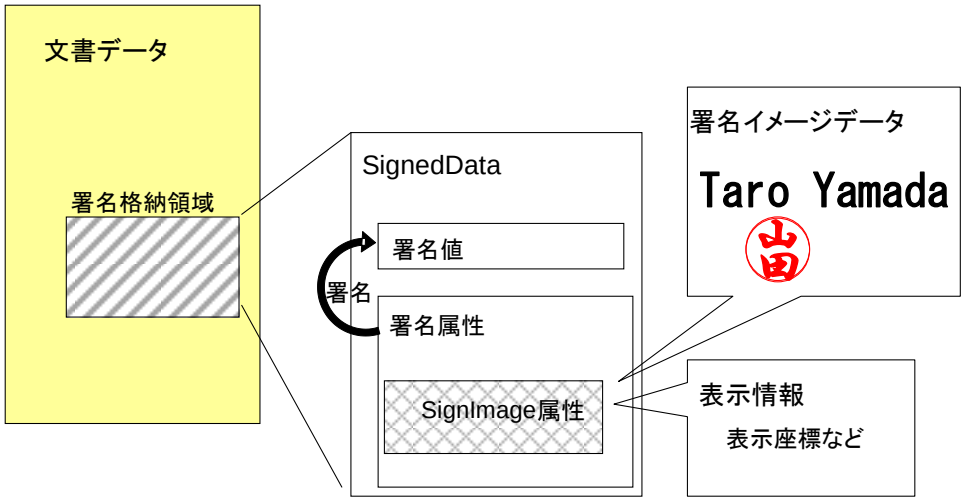


図 3.4　署名イメージ情報の属性

この考え方は IETF で策定中の Certificate Image と同様の発想である。Certificate Image は認証局のもとで証明書所有者を示す画像をリンクさせるのに対して、こちらの案では署名者自身が署名文書に署名イメージをリンクさせる考えである。

この案ではタイムスタンプ生成のときに起こりうる文書フォーマットの描画情報とタイムスタンプ時刻情報の生成順序の問題(*1)を回避できる可能性がある。

また、文書フォーマットの描画情報と署名マーク情報を分けることで文書のコンテンツと合わせて表示する方法だけでなく、コンテンツと署名のレイヤーを分けて署名マーク情報は別の枠組みで表示する方法なども提案できる可能性がある。

(*1) タイムスタンプ生成と表示情報生成の順序関係の問題
タイムスタンプを生成して文書データに格納するときには下記のような手順をとる。例えばPAdESがこの一例である。

1. 文書データ中の署名対象（タイムスタンプ対象）となる領域を抽出する。
2. 1.の領域に対してハッシュ生成を行い、タイムスタンプ局がタイムスタンプ情報を付加して署名を行う。タイムスタンプトークンが生成される。
3. 2.で得られたタイムスタンプトークンを元の文書データ中のある領域に格納する。

このとき、タイムスタンプに関する表示情報には、2.の署名生成時に決定されるもの（例えば、タイムスタンプ時刻など）があり、1.の段階では表示情報は確定できない。したがって、文書フォーマット中で表示情報を格納するには、その領域は署名対象外にする必要がある。しかし、3.の過程でタイムスタンプトークンと共に表示情報を文書フォーマットに追加した場合、表示情報は署名対象領域内の情報ではないため、不正な表示情報の追加と区別ができなくなるおそれがある（文書フォーマットによっては不正としてエラー表示される場合もある）。
上記の手順はタイムスタンプ生成のみの場合を示したが、署名タイムスタンプの場合でも同じ問題である。

今後、この案について検討を深めていくには、対象となる様々な文書やデータフォーマットと整合性を考慮しつつ、署名属性で定義すべき情報の内容を具体化していく必要がある。また、様々な文書フォーマットで共通化された表示方法を実現していくためにも表示に関するガイドラインなどの作成も視野に入れる必要があるだろう。

3.2 安全安心なID管理のために

記録管理のメタデータとして、「誰がいつどこで何を何のためにどのような方法で（5W1H）」行ったかの情報を付加する必要があるが、この「誰が」をどのように表記するかが課題としてある。また、記録管理情報をアクセスする場合のアクセスコントロールにも、「誰が」あるいはどのような「権限」を持っている人がアクセスすることが可能である、といった場合の個人を特定するための情報は必須である。

この、個人を特定する番号（ID）を利用する場合、国全体のID管理体系に合わせていく必要があると考えている。現在、内閣官房で個人のID管理方式の検討を行っているが、利用する立場からID管理に対する現状の個人情報保護やID管理方式の検討状況について整理し、今後検討すべき項目について提言を行う。

3.2.1 個人情報の保護

国民にIDを付番するときに、避けて通れないのがIDによる名寄せの問題、すなわち個人情報保護の議論である。そこで、はじめに個人情報保護法について簡単に解説する。

(1) 個人情報保護法の系譜

個人情報保護は、国際的には1980年のOECD「プライバシー保護と個人データの国際流通についてのガイドライン」をきっかけにOECD加盟国を中心に諸外国で法整備が進められている。

日本ではOECD8原則に準拠し、国の行政機関を対象とした「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が制定された。1995年に採択された「EU個人情報保護指令(EU指令)」では、第25条にてEU域外の各国と個人データを流通する際の規定が定められており、日本でもこれに対応することが必要になった。2000年に「個人情報保護法制に関する大綱」が決定され、これをうける形で主に民間部門を対象に「個人情報の保護に関する法律案」が国会に提出されたが、一部メディアの反発に合い、廃案となった。しかし、2003年に修正された同名の法案が国会に再提出され、5月に成立となった。2005年4月1日に全面施行が決定している。

OECDは、1980年に「加盟国は、国内法および国内政策の相違にもかかわらず、プライバシーと個人の自由を保護し、かつプライバシーと情報の自由な流通という基本的ではあるが競合する価値を調和させることに共通の利害を有すること、個人データの自動処理及び国際流通は、国家間の関係に新しい形態を作り上げるとともに、相互に矛盾しない規則と運用の開発を要請すること、個人データの国際流通は経済及び社会の発展に貢献すること、プライバシー保護と個人データの国際流通に係わる国内法は、そのような国際流通を妨げる恐れがあること、を認識し、加盟国間の情報の自由な流通を促進すること及び加盟国間の経済的社会的関係の発展に対する不当な障害の創設を回避することを決意し」(出展：外務省ホームページ「プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告(仮訳)」)「プライバシー保護と個人データの国際流通についてのガイドライン」の理事会勧告を採択した。

8原則は、以下のとおりである。

・収集制限の原則(合法的な手段により入手し利用者への通知・同意を得る)
・データ正確性の原則(個人情報は利用目的に即したものである)
・目的明確化の原則(利用目的に必要な範囲で正確・完全・最新である)
・利用制限の原則(要求された目的以外で利用してはならない)
・安全保護の原則(紛失・破壊・修正・開示等の危険に対し、合理的な安全保護措置が必要)
・公開の原則(個人データに係る開発・実施・政策は一般に公開される)
・個人参加の原則(自己データの存在を利用者がいつでも確認できる)
・責任の原則(管理者は上記を全うする責任を持つ)

上記勧告では、個人データの取り扱いに関して、これら8つの基本原則を示し、これを加盟国の国内法に含むことを考慮するよう求めている。

(2) 国内の個人情報保護の法制度

行政機関の保有する個人情報の保護に関する法（平成15年5月30日法律第58号）とは、行政機関における個人情報の取扱いについて定めた法律（略称は行政機関個人情報保護法）で以下に示す個人情報保護法関連五法の一つである。

・個人情報の保護に関する法律(基本法制)
・行政機関の保有する個人情報の保護に関する法律
・独立行政法人等の保有する個人情報の保護に関する法律
・情報公開・個人情報保護審査会設置法

・行政機関の保有する個人情報の保護に関する法律等の施行に伴う関連法律の整備等に関する法律

行政機関個人情報保護法では、「個人情報」の定義を「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。」としている。

また、「個人情報ファイル」とは、「保有個人情報を含む情報の集合物であって、一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの」としている。

個人情報の利用については、次の通り決めている。

「行政機関の長は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。

２　前項の規定にかかわらず､行政機関の長は､次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供することができる。ただし、保有個人情報を利用目的以外の目的のために自ら利用し、又は提供することによって、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。

一　本人の同意があるとき、又は本人に提供するとき。

二　行政機関が法令の定める所掌事務の遂行に必要な限度で保有個人情報を内部で利用する場合であって、当該保有個人情報を利用することについて相当な理由のあるとき。」

3.2.2　エストニアの個人データ保護法

比較のために、個人情報にその秘匿の度合いをランク付けしているエストニアの個人データ保護法を紹介しよう。

「個人情報」とは、「特定の自然人に関する情報、または身体的、精神的、生理学的、経済的、文化的または社会的な特徴、親族関係および交友関係に言及することにより特定可能な自然人に関する情報」とする。

(1)　個人情報の分類

エストニアでは、「個人情報」を「私的個人情報」と「機密個人情報」に分類して、扱いも異なる。なお、国民 ID や氏名は公共情報として、共有される。

①　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)　課税過程において個人に関し収集された情報（ただし、税金滞納に関する情報はこの限りでない)。

②　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（ただし、法律で規定された手続

きに基づいて登録された司法上の法人の構成員であることに関する情報はこの限りでない）

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) 犯罪に関連する事項に対する公開法廷の開廷前もしくは判決が下される前において犯罪を確認するため、刑事訴訟手続もしくはその他の手続きにおいて収集された情報、または公衆道徳もしくは個人の家庭生活および私生活を保護するために必要である場合、もしくは未成年者、被害者、証人もしくは裁判官の利益のために必要である場合。

(2) 個人情報の活用

「個人情報」の利用については、以下のとおりである。

本人の同意がある場合の個人情報の処理

① 個人情報の処理に対する同意とは、任意に行われ明示的に通知される本人の要望を示す意向であり、それによってかかる本人が自己に関する個人情報の処理に同意することを示すものを意味する。

② 主要処理機関または授権処理機関は、個人情報の処理に対する本人の同意を得る前に、以下の事項を本人に通知しなければならない。

1) 個人情報の処理の目的、

2) 個人情報の伝達対象として許可される人またはかかる人の分類、

3) 主要処理機関の名称またはその代表者の氏名および主要処理機関の事務所の住所、

4) 本人が個人情報の処理の終了および個人情報の訂正、ブロッキングまたは抹消を要求する権利を有する状況、

5) 本人が自己に関する個人情報を入手する権利を得る状況。

③ 本人の同意は、本人の生存期間中および本人の死亡後 30 年間有効であるものとする。ただし、本人が別途の決定を行っている場合はこの限りでない。

④ 本人は、自己の同意をいつでも撤回することができる。同意の撤回は、遡及効を有しない。かかる同意には、民法（RT I 2002, 35, 216; 2003, 13, 64）総則の意思表示に関する規定が追加的に適用されるものとする。

⑤ 紛争が生じた場合、本人は、自己に関する個人情報の処理に対する同意を行っていないと推定される。

⑥ 本条は、行政当局により個人情報が処理される場合には適用されない。ただし、本法第 4 条(3) 項に記載される機密個人情報の処理に関してはこの限りでない。

⑦ エストニアでは本人が死んだ後の個人情報の扱いにも言及している。

1) 本人の死亡後、当該本人に関する個人情報の処理は、当該本人の配偶者、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。ただし、個人情報の処理に対する同意を要しない場合または本人の死亡後 30 年が経過している場合はこの限りでない。

2) 本条第 (1) 項は、処理される個人情報が氏名、性別、生年月日および死亡日ならびに死亡

の事実のみである場合には適用されない。

3.2.3 個人 ID の管理方式

ここでは、ID 管理に関する技術、用語などの世の中の議論を整理する。

(1) 個人 ID 管理方式

日本では、自分が日本国民であることを証明するための身分証明書（ID カード）はなく、もっぱら自動車免許証、健康保険証、パスポートなどがその代用として用いられている。すでに 2003 年から日本の eID カード（スマートカードを用いた身分証明書）というべき住民基本台帳カードの配布が始まっているにもかかわらず、その知名度や活用機会は非常に低く、住民基本台帳カードの存在意義自体があいまいな印象を与えている。

これは、各省庁や銀行や病院等が保管している個人情報を連携するための仕組みがない（基本 4 情報が入っているが、年金番号事件でもありらかになったように、この中の氏名、住所の漢字に誤記入が多く、実際には情報連携には利用できない）ためである。こういった状況の中で、日本の ID 管理､及び eID カードがどのように整備されていこうとしているのか見守る必要がある。

(2) 個人 ID 番号とは

個人の ID 番号を各国が管理し、電子政府のサービスなどに用いている。この ID 番号は、以下の 3 つの番号に分類することができる。

① ユニバーサル ID

これは、各部門で同一の ID 番号を用いる方式である。ID 番号は、誕生日や出身地番号を利用して発生する方式をとっている国と、全く無意味な文字列を ID 番号として用いる国もある。

② ドメイン ID

これは、各部門で異なる ID 番号を採用する方法である。この場合、部門間の情報の連携は図れない。

③ ルート ID

これは、いわばユニバーサル ID とドメイン ID を組み合わせたもので、ルート ID と各ドメイン ID のリンクを行う方法であり、実現方法はいくつか考えられる。ルート ID は市民がその番号を知る必要もなく、たとえば無意味な長い文字列が安全なカードやサーバに記憶されていればよい。

(3) 運用モデル

つぎに、これらの ID を用いた個人 ID 番号の運用モデルを紹介する。

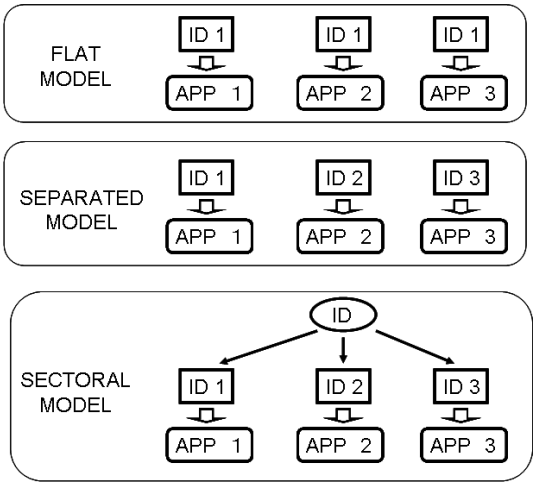
① フラット　モデル

ユニバーサル ID を用い複数のアプリケーションに同じ番号を使う方法である。欧州のいくつかの国はこれを採用している。エストニアを例にとって紹介する。エストニアでは出生届を提出すると、性別、生年月日、4 桁の番号からなる 11 桁の国民 ID 番号がつけられる。個人のデータはこの国民 ID 番号に関連付けられて記録されるためサービス間で個人情報を共有することができる。このため、電子政府サービスにおいてすでに登録した情報は入力画面に表示さ

れ、新たに入力が必要な情報だけを入力すればよい。エストニアでは個人情報のアクセスには公開鍵基盤による認証とアクセスコントロールが厳密に行われていて、かつ、個人情報へのアクセスログは管理され、本人のみが確認することができるしくみがあり、不正アクセスがあった場合の摘発を容易にしている。エストニア以外にもアイルランド、スペイン、スロベニア、イタリア、チェコ、デンマーク、フィンランド、ポーランド、フランス、リトアニア、ベルギーではフラットモデルが採用されている、あるいは、採用される可能性がある。

② セパレイテッド モデル

部門毎に全く関連の無い異なる番号（ドメイン ID）をつける方法である。組織間で連携がない場合、それぞれの組織のサービスはセパレイテッドモデルになる可能性が高い。アプリケーション間の ID の連携は無いため、ひとつのアプリケーションで利用される ID が外部に知られても他のアプリケーションの情報をアクセスできない反面、ユーザは他のアプリケーションですでに入力したものであってもアプリケーション毎に必要な情報を入力する必要があり、ユーザに負担がかかる。ドイツ、ハンガリー、スイス、イギリス、ポルトガルではセパレイテッドモデルを採用している。



③ セクトラル モデル

アプリケーション毎に異なる ID 番号を使うが、それらの ID 番号は一つの基本となる ID 番号から発生させる方式である。したがって、アプリケーションで使われるひとつの ID 番号を手に入れただけでは他のサービスで使われている個人情報を収集することはできない。また、サービス間の個人情報の共有は基本となる ID 番号を介して行うことができる。この場合、基本となる ID 番号の管理には、十分な注意を払う必要がある。このセクトラルモデルを採用しているのは、開発したオーストリアである。

オーストリアの ID 管理方式の特徴は 3 レベルの国民 ID 番号（ZMR-Zahl、SourcePIN、sSourcePIN）を連携して使うことである。

1） ZMR-Zahl

国民は出生後 CRR（Central Register of Residents）に登録される。登録時点で、CRR の内部ルールに従った国民 ID 番号（ZMR-Zahl）がつけられる。この番号は公開される番号であり一生変わらない。この番号に直接個人情報を結びつけることはない。

2） sourcePIN

ZMR-Zahl に対し暗号処理（3DES）を行うことにより、新たな数値列を得る。これを SourcePIN と呼ぶ。この数値列は市民カードに格納され、本人以外は知ることはできない。また、SourcePIN から ZMR-Zahl を推定することはできない。

この処理は、大統領が任命する 6 人の識者（裁判官、等）からなるデータ保護委員会（DPC：Data Protection Commision）のもとで実施される。

3) ssPIN（Sector-specific IDs）

ssPIN が実際にアプリケーションで使われる ID である。SourcePIN とアプリケーションを提供する各セクタ（例えば各省庁）に振られた SectorID を合成してハッシュ処理（SHA-1）を行い ssPIN を得る。これは、利用する毎に SourcePIN と SectorID から発生して利用する。なお、ssPIN から SourcePIN を推定することはできない。

このような仕組みにすることにより、アプリケーション毎に異なる ID（ssPIN）を利用することができ、万が一あるアプリケーションの ID（ssPIN）が外部に漏れても、他のセクタのアプリケーションには使うことができない。

一方、データ保護委員会（DPC）の許可を得ることにより、たとえば納税申告の場合など、関連する情報を統合利用して、把握した情報を納税者に提示することができる。

このように、国内でユニークな番号が入っている eID であれば、国のコードと結びつけることにより、世界でユニークな番号になる。

(4) 各モデルの比較検討

以下に、3 つのモデルの長所、短所について説明する。

① フラット　モデル

長所：一つの ID で個人情報を管理するため、システムが簡単になる。

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

② セパレイテッド　モデル

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

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

③ セクトラル　モデル

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

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

つぎに、日本が採用しているセパレイテッド　モデルからフラット　モデル、セクトラル　モデルへ移行する場合の負荷について、以下に示す。

表 3.5　セパレイテッド　モデルからの移行に伴う負荷

	長所	短所
フラット　モデル	システムが簡単になる	国民に情報の漏洩、名寄せに対する不安感がある。 現システムからの移行のため、全てのデータへの ID の付け替えが必要。
セクトラル　モデル	セクタ間の情報結合ができ、かつ、セクタ番号がもれても他のセクタに影響を与えない。	新たなシステムの導入が必要である。 現システムからの移行負荷が大きい。

(5) 関連用語の整理

ID 管理について、用語の整理ができていないため、混乱が生じやすい。そこで、これまで出てきた用語を含め、JIPDEC 内の検討で利用される用語の整理を行う。

① ID について

ID：アイデンテティ　ナンバーのことで、人や物、場所にユニークにつけられる番号

国民 ID 制度：国民の情報に番号を付けて管理する仕組みの全体

国民 ID：国民の情報に番号を付けて管理する仕組みで使われる ID。

社会保障番号：厚生労働省が進めている社会保障関連に共通に用いる ID

（社会保障と税に関する）番号／共通番号：内閣官房が進めている方式の中で、社会保障と税に関する分野に共通に使われる番号。

（国民）ID コード:内閣官房が検討を進めている方式で､住民票コードから発生させるコード。ルート ID として、各部門にリンクコードを発生する。

② ID の利用上の分類

＜他人に知らせるか否か＞

オープンな ID : 積極的に相手に知らせる ID で､保険証番号､社会保障番号､納税者番号など。

クローズな ID：自分だけが知っていればよい ID で、住民基本台帳コード など。

秘匿 ID : 本人も知ることのない第 3 者機関が管理する ID。「(国民) ID コード」がこれに当たる。

クローズな ID と秘匿 ID は、人に示す必要もないことから、無意味な長い文字列を使うことができる。

＜個人情報とひもづくか＞

ドメイン ID：オーストリア方式における ssPIN に対応するもので、個人情報がひもづけられる ID。(内閣官房の方式では、「利用番号」としている)

ルート ID：オーストリア方式における SourcePIN に対応するもので、ドメインごとの ID を作成するための ID のことを指し、個人情報とは直接ひもづけられない。

ハブ ID：ドメイン ID を連携するための ID で個人情報とは直接ひもづけられない。

3.2.4 ID 導入の際の検討事項

(1) ID を国民に配布する場合の課題として以下を検討する必要がある。(内閣官房 IT 担当室 2010 年 12 月資料より)

① 対象とする範囲

・国民 ID 制度において対象とする者（国民 ID コードの付番対象者）の範囲はどうするか。
例－日本国籍を有する者及び短期滞在者を除く外国人住民

② 一意性

・公平で正確な行政サービスの提供や行政事務の正確かつ効率的な実施の観点から、国民 ID コードは 1 人に対して 1 つのみ付番すべきか。

③ 悉皆性

・全ての者に対する確実な行政サービスの提供や行政事務の正確かつ効率的な実施の観点から、国民 ID コードは制度が対象とする全ての者に付番すべきか。

・全ての者に対する確実な行政サービスの提供や行政事務の正確かつ効率的な実施と整合性を確保しつつ、国民 ID 制度を利用したくない者のニーズに応える方法として、どのような方法があり、そのような方法とした場合にどのような問題が生じるか。
例－国民 ID コードには悉皆性を求めるが、それを利用して行政サービス等の提供を受けるかについては選択可能とする
－国民 ID コードの付番後に付番対象から外れることを可能とする

④　不可視性

・コードを盗み見されるリスクへの対策やコードが漏洩した場合に名寄せされるリスクへの対策等の観点から、国民 ID コードは第三者が目視できないものとするか。
例－コードに暗号化等の対策を施し、第三者が目視できない不可視のコードにする
－第三者が容易に目視できない番号（例：住民票コード）を国民 ID コードとする

⑤　可変性

・国民 ID コードで紐付けられた情報を時系列で容易かつ確実に遡ることを可能とし、また、情報システムの安定的、効率的な運用を確保するため、国民 ID コードを変更不可とするか。
・コードが漏洩した場合のリスクへの対策やコードを変更したい者のニーズに対応するため、国民 ID コードを本人の申請等により変更可能とするか。その場合、時系列で遡ることを可能とする方策や情報システムの安定的、効率的な運用を確保する方策として何があるか。

(2) ID 管理導入にあたっての要件（「電子署名普及に関する活動報告 2009」次世代電子商取引推進協議会 2010.3 発行より）

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

3.2.5　日本における今後の検討の進め方

将来の少子化社会に対応するには行政コストを下げる必要があり、国民の要求に対応するには行政サービスを増強する必要がある。この相反する要求に対応するためには IT 技術を用いた行政の自動化（AA：Administrative Automation（ECOM の定義））を進めることが必須である。この 10 年世界各国では電子政府あるいは電子行政の名の下で AA が推進されてきた。日本においても 2001 年に IT 戦略本部が立ち上り、電子政府の実現に向けた活動が始まってから約 10 年を経たが、一部のサービスを除き電子政府の利用拡大の見通しはたたず、今後の IT 戦略は混沌と

したまま方向性を失っているように見える。これは、「IT 推進のポリシー」や「IT 社会基盤のフレームワーク」など IT 推進方針に関する検討が不十分なままになっているためと考えられる。

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

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

日本において、この個人 ID の仕組みをこれまで導入できていない主な理由として、国民の不安に対して、十分な説明ができていないことによる。

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

そこで、これらの議論を進め、まず国民の不安を整理し、その不安に対応できる新たな個人 ID 管理のしくみを提案なければならない。

(1) IT 推進方針の必要性

ID 番号について検討する前に、何のためにどのような IT 環境を実現しようとしているのか、政治主導で国民に示す必要がある。eJAPAN 戦略の目標は曖昧であり、2005 年にその目標を達成したとは国民が思っていない。国内における IT 戦略の議論は、国民を巻き込んで進めるべきで、国民の理解を得ないで進めては、出来上がったシステムは結局使われないものになってしまう。そのいい例が住民台帳ネットワークである。そこで、IT 推進計画をわかりやすく説明していく必要がある。エストニアを例にとると、電子政府推進のステップは以下の 3 段階からなる。

① IT 推進ポリシーを決める

日本において、だれが、なぜ、何のために、どのように IT を推進していくのかのポリシーを分かりやすく説明する必要がある。

例えば、以下に示すようにエストニアの IT 推進のポリシーから一部を利用してそれに、日本なりの方針を加えてもいいのではないか。

1) 日本おける情報社会の発展は、公共部門が主導する形で、この原則にしたがい進むべき方向を戦略的に選択する。
2) 情報社会は、公共部門、民間部門および第三セクタの間の協力に基づいた、調整された方法で開発される。
3) 公共部門は賢明な顧客であり、公共調達において、革新的な実現方法に可能な限りの自由が残されることを保証する。

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

5) 公共部門は、既に存在している技術を利用し、IT 技術開発の重複を避ける。

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

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

8) （追加） 公共部門は移動時の紛失を避けるため、本人の要求がない限り個人情報の紙を含むあらゆる媒体へ出力は行わない。

② IT の基盤のフレームワーク

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

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

③ アプリケーション

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

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

(2) 法制度を作る

・戸籍登録の際に、住民票コードから国民 ID（ルート ID）を作成するよう法律に訂正を加える。国民 ID は生涯変更しないものとする。

・ルート ID を用いて連携テーブルで部門 ID の連携を図る方法、運営体制、罰則について法律として明確にする。

なお、オーストリアでは、セクトラルモデルについて法律（電子政府法）を作成している。

(3) 運営の体制を作る

日本のあらゆる行政システムの IT 化において以下の 2 点が重要である。

① 相互運用性

相互運用性を保つため、提案された行政システムが IT 基盤の枠組みを守っているか、開発に当たって事前チェックを行う仕組みを立ち上げる必要がある。

② 大規模システム開発体制

開発責任者は、一定以上の資格を持っていることにし、発注側の無責任な指示に従わなくてよい体制を作るなど、年金システム開発の轍を踏まないようにしなければならない。

(4) ID 管理の仕組みを考える

ID 管理の仕組みを考えるためには、先に説明した「ID 管理導入にあたっての要件」との整合性を検討しなければならない。

すなわち、「国民 ID 導入のための 6 つの要件」を満たすシステムを構築するためには、セクタ間の情報交換が必ずひとつの組織を経由して行われることが必須であり、こうすることによって、アクセスコントロールやアクセスログを取得し、管理することができる。まず、必要な構成について説明する。

① セキュリティ監視委員会（仮）

この委員会は、以下の構成と役割を持つ。

・構成：オーストリアの方法が参考になる。オーストリアでは、各団体の推薦により、首相が任命する方法をとっている。

・役割：システムの（部分）停止、セキュリティ監視センターの作業監視、新規サービスの認可人権団体からの参加が必要である。

＜セキュリティ監視センター＞

セキュリティ監視委員会の元で、以下のシステムの監視を行う。

・電子記録管理システム：個人情報がどこのセクタのどのシステムにあるかを管理する。

・操作ログ管理システム：セキュリティ監視センターの要員が不正な行為を行っていないことを示すために、操作ログを記録する。この情報はセキュリティ監視委員会に提出する。

・アクセスログ管理システム：情報交換の要求や実施に関して個人情報をアクセスしたときのログを記録する。この記録は、本人に開示する。

② データ交換方式

ID に紐付けられる情報の保管形式は部門により異なっている可能性があり、他部門との交換を行う際には、これらを標準フォーマットに変換する仕組みが必要である。エストニアでは X-Road という仕組みを導入してデータ交換の仕組みを実現している。この X-Road とそこで使われている 2 種のサーバ（Security Server（SS）、Adapter Server（AS））を導入することにより、アクセスコントロール、アクセスログを管理することができる。

1) Security Server（SS）

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

2) Adapter Server（AS）

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

(5) 日本における ID 管理の検討状況

これらの条件を念頭に、今の日本の動きを紹介する。

① 国の検討状況

高度情報通信ネットワーク社会推進戦略本部（第 53 回　平成 22 年 5 月 11 日）では、以下の重点施策が発表され、検討が本格的に進められている。

１．国民本位の電子行政の実現

(1)　情報通信技術を活用した行政刷新と見える化

【重点施策】

○行政サービスの中で、利用頻度が高く、週 7 日 24 時間入手できることによる国民の便益が高いサービス（例：住民票、印鑑証明、戸籍謄抄本等の各種証明書の入手等）を特定し、それらをオンライン又は民間との連携も含めてオフライン（例：行政キオスク端末）で利用できるようにする。

○社会保障の安心を高め、税と一体的に運用すべく、電子行政の共通基盤として、官民サービスに汎用可能ないわゆる国民ＩＤ制度の整備を行うとともに、自己に関する情報の活用については、政府及び自治体において、本人が監視・コントロールできる制度及びシステムを整備する。

○電子行政推進の実質的な権能を有する司令塔として政府ＣＩＯを設置し、行政刷新と連携して行政の効率化を推進する。その前提として、これまでの政府による情報通信技術投資の費用対効果を総括し、教訓を整理する。その教訓にもとづき、上記施策を含め、電子行政の推進に際しては、費用対効果が高い領域について集中的に業務の見直し（行政刷新）を行った上で、共通の情報通信技術基盤の整備を行う。クラウドコンピューティング等の活用や企業コードの連携等についても、その一環として行う。

この流れで、内閣官房が事務局として社会保障・税に関わる番号制度及び国民 ID 制度（以下「両制度」という。）における個人情報保護の仕組みに関する事項を検討するため個人情報保護ワーキンググループ、両制度で共通する事項のうち技術に係る事項を検討するため情報連携基盤技術ワーキンググループがそれぞれ設置し、今年の 2 月から検討を続けている。

その構成を図 3.5 に示す。その特徴は、以下のとおりである。

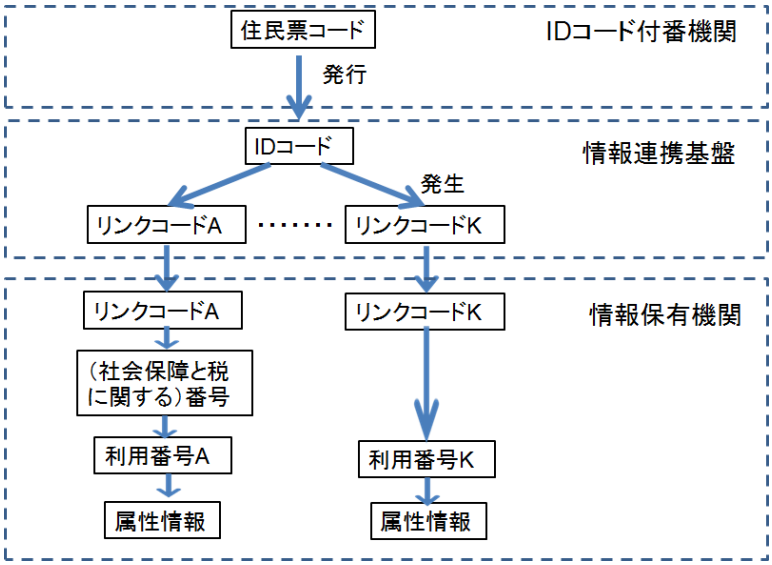


図 3.5　ID 管理方式（内閣官房モデル）情報連携基盤技術 WG 資料に基づき作成

a.　ルート ID として、住民票コードから生成した秘匿コードである「(国民) ID コード」を用いる。

b.「(国民) ID コード」から、個人の属性情報とのリンクを目的とした「リンクコード」をその都度発生させる。「(国民) ID コード」と「リンクコード」は双方向に発生できる。

c. 情報保有機関は、「リンクコード」、「(社会保障と税に関する) 番号」、「利用番号」、属性情報とひもづけて管理している。

d. 情報連携の流れ：属性情報＞＞利用番号 A＞＞リンクコード A＞＞ID コード＞＞リンクコード K＞＞利用番号 K＞＞属性情報

② JIPDEC（旧 ECOM）検討モデル（リンクモデル）

リンクモデルは、次世代電子商取引推進協議会で 2 年前に検討された方式であり、その構成を図 3.6 に示すとともに、特徴を説明する。

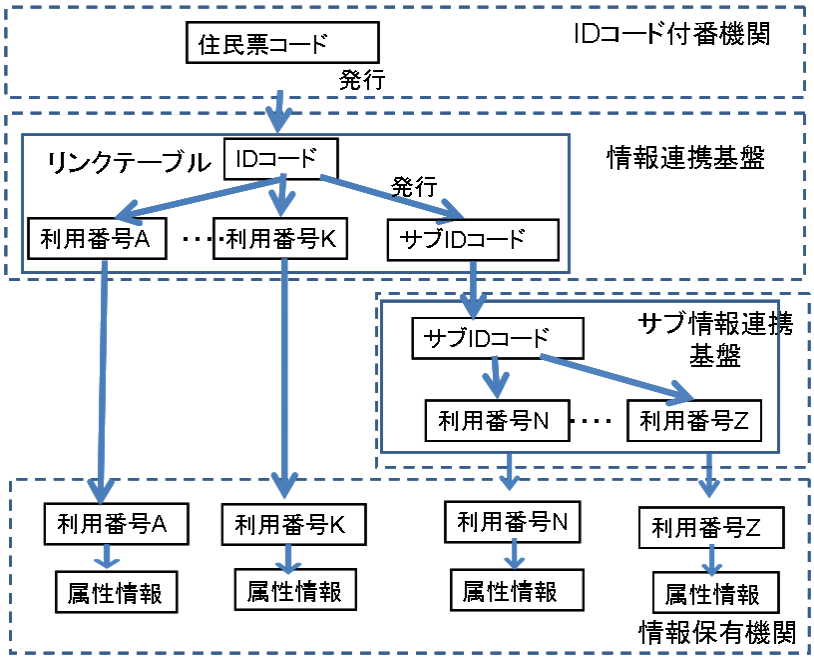


図 3.6 ID 管理方式（JIPDEC モデル）

a. 連携番号として、住民票コードから生成した秘匿コードである「(国民) ID コード」を用いる。

b. 「利用番号」と「(国民) ID コード」あるいは「サブ（国民）ID コード」と紐付けを行う「リンクテーブル」を作成する

c. 「リンクテーブル」を秘密分散技術により分散管理する。

d. 情報連携の流れ：属性情報＞＞利用番号 A＞＞ID コード＞＞利用番号 K＞＞属性情報

内閣官房の方式（図 3.5）に比べ、以下の特徴を持つ。

秘密分散技術を用いることにより「リンクテーブル」という簡単な方式で実現しているにもかかわらず、「リンクテーブル」の漏えいリスクを低く抑えることができる。

サブ情報連携基盤を作ることができ、極端にセンシティブな情報を扱う場合や、個人情報漏えいに対する基準の異なる民間などのセクタで ID を使う場合でも、柔軟に対応できる。

3.2.6 ID 活用にあたっての課題

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

近い将来、個人ごとに ID を持ち、文書管理に限らず多くのシステムで利用できる時代が来ることが望まれる。どのような ID 管理方式でも、暗号や秘密分散技術、法律や運用ガイドラインを整備することにより、安全に利用できるシステムの実現は可能である。

今後の課題として、電子文書特有の課題と一般的な ID 管理に関する課題を挙げる。

(1) 電子文書管理にかかわる課題。

① 電子文書にどの ID を記入するのか

これまでの議論は、各人の作業については、ドメイン番号/利用番号をサービスシステムで利用することを考えてきた。しかしながら、文書は必ずしもそのドメインだけで利用されるとはかぎらず、電子文書に記入された ID が、ドメインを超えて利用されることが考えられる。

このような場合に対応するため、文書を作成した時点でドメイン ID に加えドメインコードを入れるか、新たに、文書共通 ID 番号の導入を検討する必要がある。

② 文書作成時の本人の役職（属性）の確認

一つには、本人の役職をメタデータに自動的に入れるには本人の ID と役職データベースがリンクしている必要がある。また、文書作成時の役職の信頼性のために第 3 者の証明が必要になる可能性もある。

後になって、本人の役職を証明するための仕組み、それを保存するデータ形式なども検討する必要がある。

(2) ID 管理にかかわる課題。

① 国民 ID の詳細検討

ID 管理方式の検討も重要だが、どのような場面でどの従来システムと連携して用いるかを検討し、そのうえで「生まれてすぐにつけたほうがいいのか／生涯固定がいいのか／秘密にする必要があるのか」などの基本的な項目について決めていく必要がある。

② 信頼性の確保

「自身のデータのチェックの仕組み／自身のデータへのアクセスログのチェックの仕組み」については、必ず安全な方法で実現しなければならない。

③ 事後処理では対応できないものは

万が一でも漏えいしては困るデータについては、「ネットワークに接続しないデータとの連携方法／最適なアクセスコントロールとはなきか」などの検討を進める必要がある。

④ 国全体の情報管理システム

エストニアでは国政情報システムの全体を管理し国の IT 資源の最新状況を概観できるようなシステムがあり、同じ情報を複数の機関が管理する必要がない。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。

3.3　セキュリティの潮流を変える電子的割符

秘密分散技術(電子的割符)を活用した、重要・機密データの分散保管を実現するサービス基盤「J2ET(ジェッツ)エスクローサービス」を提供し、個人情報をはじめとするクリティカルな情報のエスクロー(預かり)及びディザスタ・リカバリ機能付きバックアップ・サービスを実現した。その概要について紹介する。

3.3.1　電子的割符について：『技術の背景と特徴』

秘密分散技術(電子的割符※1)は、個人情報・企業機密情報等の保管・移送手段として、これから広く普及が期待されるセキュリティ技術の一つである。この技術手法により企業・組織にとっては、従来のセキュリティ技術とは一線を画した機密情報保護や低コストでの保管システム構築の可能性が広がる。

※1: 電子的割符(でんしてきわりふ): 勘合(かんごう)貿易で用いられた勘合符のように、重要な情報を物理的に分割して管理・照合に使う「割符」の考え方を電子的に実現したものである。

(1)　特定 OS 非依存（オープンアプリ）で導入コスト安価：

企業にとっては、既存のシステム環境を大幅に変更することなく導入でき、特定のコンピュータ OS に依存することなく使用可能という、いわゆるエコ IT 情報利活用ツールであり、大企業だけでなく中小企業にもやさしいセキュリティ技術手法だといえる。また、機密データを分割して保存する際に、さらに秘匿性を高めるに、時空間情報を埋込むことも簡易に実現可能である。この事実は、様々な応用分野が期待でき、ある特定場所・特定時間の制限範囲の中でしか、機密データを復元できないという特徴を電子的割符に持たせることができる。

さらに導入コストやシステム更新コストについても、これまでの暗号システム導入や 2010 年問題等の暗号危殆化に伴う当該システム更新の必要がなく、半永久的に使用できるというメリットがある。

(2)　電子的割符（秘密分散技術）の特徴とは

従来からの暗号化技術と同じく情報秘匿化の手段であり、データを分割して分散保存する手法であるが、下記のような顕著な特徴を持つ。

分割した一片だけでは、元のデータは復元不能（一定個数以上の個片で復元）。

情報セキュリティ対策全般について適用が可能であり、安全保管だけでなく機密データ（個人情報等）の運搬時等における使用にも適する。

地域を超えた割符データ分散保存による BCP（事業継続計画）やディザスタ・リカバリ（災害対策）に有効である。

別々に保管した割符個片データ同士を結合することで、復元による認証効果もある(改ざん無証明⇒どちらか片方が改ざんの時は、原本復元不能)。

3.3.2　電子的割符の原理について

(1)　電子的割符の原理

電子的割符については、大きく分けて二つの秘密分散技術手法がある。

『完全秘密分散技術』（通常モード）とは、元本データを 2 個以上の複数個に分割保存する際に、元本復元のためには、分割した個片すべてが必要となる技術手法である（1 片でもなくなれば、復元不能となる手法）。

『閾値（しきいち）秘密分散技術※3』（リカバリーモード）とは、元本データを例えば 3 分割して、別な場所に分散保存する手法で、3 分割の上で、もし 3 片全部のデータが揃わなくても、（仮に 1 片が紛失となっても）、残りの 2 片で元本データが復元可能な技術手法である。

(2)　電子的割符処理の概要（電子的割符アプリケーションの果たす役割）

電子的割符化処理に伴う、当該割符化アプリケーションの果たす、実行内容を下記に示す。(図 3.7 参照)

単純にデータを複数分割ではなく、原本データをビット単位でランダムに分断。

その後，復元用の「青写真」を加え分割する。

それらを別々の場所・メディアに保存させる。

分割されたデータにはオリジナル・データと同じビットの並びは存在せず，分割データ単体では部分的にもオリジナル・データを復元は不可能となることはいうもでもない。

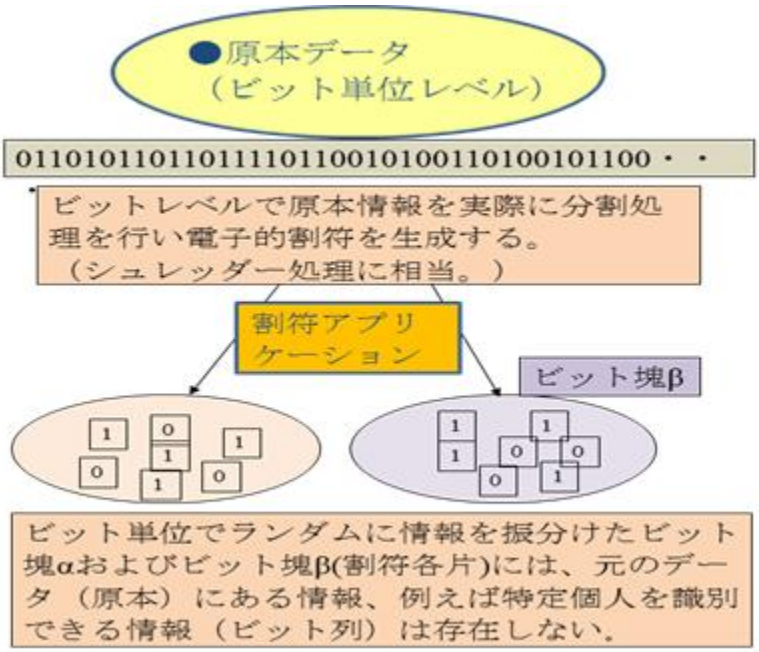


図 3.7　電子的割符化処理の概要

3.3.3 電子的割符を取り巻く環境について

(1) 行政側の対応

まず、政府機関等行政の対応についてであるが、NISC（内閣官房情報セキュリティセンター）から出ている、いわゆる政府統一基準への記載が挙げられる。

> 政府機関の情報セキュリティ対策のための統一基準(第 4 版)（抜粋）
> ＜電磁的記録の保護対策＞
> 【強化遵守事項】
> (f)行政事務従事者は,要機密情報である電磁的記録を移送する場合には,必要な強度の暗号化に加えて,複数の情報に分割してそれぞれ異なる移送経路を用いること。
> 「内閣官房情報セキュリティセンター（ＮＩＳＣ）　政府機関の情報セキュリティ対策のための統一基準」
> http://www.nisc.go.jp/active/general/kijun01.html
> 「政府機関の情報セキュリティ対策のための統一基準（2009 年 2 月版［第 4 版］）」

この「複数の情報に分割してそれぞれ異なる移送経路を用いる」を実現する方法の一つが「電子的割符」にあたるものである。

以上のように、行政側でも秘密分散技術（電子的割符）についての関心があり、適用について具体的な対応が示されている。

(2) 民間側の対応

次に民間側の取り組みとしては、「電子的割符ガイドラインの策定」が挙げられる。これは、電子商取引の民間推進団体である ECOM の情報セキュリティワーキンググループ傘下の秘密分散技術タスクフォースが策定したもので、電子的割符に関する、初めての準公的なガイドラインである。その内容としては、電子割符における各種の遵守事項やセッティングの際の注意事項等が記載されており、以下にそのガイドラインの記載例を示す。

> 「電子的割符ガイドライン（ECOM 秘密分散技術ガイドライン：2009 抜粋）」
> （ECOM　2009 年度情報セキュリティWG成果報告書「EC における情報セキュリティに関する報告」秘密分散技術検討ＴＦより）
> ①　復元に必要な割符片を第三者が容易に集められるような場所及び方法で格納しないこと
> ②　復元に必要な組み合わせ情報に第三者が容易にアクセスできないこと
> ③　復元を容易にするための情報を、そのまま割符に入れないこと

こういった、民間側からの電子的割符の普及における環境整備も、提供事業者側や導入企業側のニーズを受けて着実に推進されている状況である。

(3) 法的環境の整備

さらに、普及に関するさまざまな環境構築という点で大切なものに、法的環境の整備がある。この点に関しては、同じく ECOM 秘密分散技術ＴＦ成果物（2009：抜粋）としての「電子的割符に対する法的見解」が挙げられる。

これは、IT 関連分野で著名な、牧野二郎弁護士から ECOM 宛てに出していただいた「情報分散管理技術（電子的割符技術を利用した情報管理）に関する法的意見書」（2010.2 月）に記載されているものである。内容としては、機密情報保護における電子的割符の有効性を認めたうえで、「原本データを割符分割した単体としての電子的割符 1 片は個人情報とはいえない」というものである。もちろん条件として、分割された各割符単体が、容易に結合不能な条件下にあるというのが前提であることはいうまでもない。

この法的意見書の意味するところは、実際の判例が出ているわけではないけれど、大きな影響力があり、個人情報の保管企業にとっては、様々な意味で朗報といえる内容となる。

まず、電子的割符にして、個人情報を保管する場合において従来のように、必要以上に堅牢なセキュリティ保護は必要ないこととなる。なぜなら、割符化されたデータ一片は個人情報でなく単なる無意味データとなるため、ある意味通常データと同等のセキュリティ保護レベルでの保管にしても最低限、大丈夫だということになるからである。これにより、個人データの保管における手間やコストの大幅削減が可能であり、必要な時に原本復元を可能にする仕組み（例えば、当団体：JIPDEC による割符預かりサービス等）を備えておけば、これまでの暗号化に伴う、技術危殆化に関するシステム更新を気にすることなく利用可能である。まさにこれは、安全・安心で簡易な情報セキュリティ手法と言えることになる。

また、行政への報告対応や被害対策コスト・世間的評価・二次被害の発生防止等のポイントについて、企業側の負担が大きく軽減できる可能性が出てくる。

3.3.4 電子的割符預かり運用スキーム（機密性・可用性・完全性）について

(1) 記載例１：機密情報委託ビジネスモデル（閾値秘密分散：三分割）

以下の順に処理を行う。

1) 委託元で A.B.C に割符処理し、「割符 A」だけ委託先に送付する。
2) 「割符 C」を第三者（準公的機関）運用預かりセンターに預ける。
3) 委託先企業データ処理時のみ、「割符 C」をＤＣからダウンロード、手元の「割符 A」とで原本データを復元する。（認証とログ管理がポイントとなる。）
4) 通常時は委託元は「割符 B」のみ、委託先は「割符 A」だけ安全保存する。
   さらに長期署名やタイムスタンプ利用による原本保証（各片単位）も追加可能である。

(2) 記載例２：電子的割符＋時空間情報の運用スキームについて

① 機密情報の持ち出しフロー

1) ユーザは管理者にデータの持ち出し申請をする。
2) 管理者は依頼された復元場所を指定して、データを分割し、ユーザに渡す。
3) 分割の際、制約情報（時空間情報）を埋め込むものとする。

② 今回提案の特徴

上記の措置によって、

・復元場所を指定可能。指定場所以外では復元不可となる。
・管理者がデータの移動経路をトレースすることが可能となる。
・ポカミスをしても、指定した時間、場所等の条件がクリアできないと原本情報が復元されない

し、さらに許可された場所や、時間の範囲でのみ復元が可能という状況となる。

3.3.5 なぜ今、電子的割符預かりサービスなのか？

(1) クラウドネットワーク化の進展と種々の環境整備

秘密分散技術（電子的割符）自体は、すでに開発されてから 10 年あまり経過しており、いわゆる最新技術ではないが、最近、これを活用した新たなサービスが各企業等で検討され、各種の実証実験等が開始されている。そして既に新サービス提供を実施している企業も多く、これからサービスインする企業も増えてくると予想されている。

また、これらの割符サービスは、重要情報を分割で無意味な非重要情報化するため、クラウドネットワーク上に展開する複数のデータセンタに分散保管することを可能とする特徴がある。つまり、適切な単価での分散保管が可能なネット環境整備として、クラウド・ネットワークインフラが一層進展することにより、クラウド型電子的割符サービスが可能な基盤が構築される。また、前述のように、秘密分散技術（電子的割符）を取り巻く環境整備（ＮＩＳＣの政府統一基準表記・ECOM 秘密分散技術ガイドライン・同技術に対する法的見解等）により、電子的割符預かりサービスのニーズそのものの顕在化と準公的機関等の受け皿としての役割が必要となってきた。

(2) 通常のデータ預かりサービスの課題と解決策

割符化をしないままの、通常のデータ預り（ストレージ）サービスの課題としては、企業としてのセキュリティ確保の観点から、機密データそのものを外部へ預けることに対する不安感が、まず挙げられる。また、ディザスタ・リカバリ（災害対策）という点で、１箇所もしくは近辺での保管では、災害時にデータが復旧できないというデメリットとなり、事業継続性という観点では、サービスが予告なしに停止・変更になることがありえることも大きな課題である。

このため、今日のクラウドネットワーク時代における機密情報・個人情報の取扱い課題に対する解決策としては、JIPDEC のような準公的機関としての果たすべき役割として下記のような項目が求められている。

・民間の預かりサービスに比べ、中立性・安全性・事業の継続性が高い運用
・準公的機関としてのコスト対応⇒リーズナブルな価格対応
・第三者機関として、将来的に民間の割符預かり業者の認定スキームも視野

3.3.6 提供サービスの概要

(1) 「J2ET(ジェッツ) = JIPDEC/Japan Electronic Tally※2 エスクローサービス」提供事業

まず、財団法人日本情報処理開発協会(JIPDEC)は、2009 年度、経済産業省委託事業である「情報セキュリティ技術を使った情報利活用基盤構築に関する共同研究と実証事業」を実施し、その中で秘密分散技術(電子的割符)等に関する複数の実証事業を行った。この実証事業の成果から、JIPDEC では日本発の秘密分散技術(電子的割符)を活用した新たなサービスを企画・検討してきたが、本技術のより一層の普及及び本技術を活用したサービスの創出及び活性化のためには、準公的機関による基盤の提供が必要不可欠と判断し、その結果 JIPDEC において、本技術を活用したサービス普及のための基盤「J2ET(ジェッツ) = JIPDEC/Japan Electronic Tally※2 エスクローサービス」提供事業を 2010 年 10 月から開始し、2011 年 3/末までを実証事業期間として 2011 年度より本格的なサービス提供を実施した。

※Electronic Tally[※2]: 電子的割符を英訳したもの

(2) JIPDEC が提供するサービス基盤「J2ET(ジェッツ)エスクローサービス」の具体的内容及び本事業における JIPDEC の役割」

秘密分散技術(電子的割符)においては、前述のように生成される分割片がそれぞれお互いの一部分となるようなデータ構造となるため、それぞれ単体では原本の一部すら推測することが難しい、という特性を持つが、逆に、復元に必要な分割片を入手できれば比較的簡単に原本を復元することが可能という特性をも併せ持つものである。すなわち、秘密分散技術(電子的割符)の利活用のためには、復元に必要な分割片を容易に集められないような保管方法が重要となってくる。

そこで JIPDEC では、具体的に、

① 復元に必要な情報を原則、ユーザだけが知っている状況を作り出す

② 復元に必要な分割片を容易に集められない状況を作り出す

という 2 点を容易に実現できるようなサービス基盤を提供することとした。それぞれ、

① ユーザサイドでの「閾値(しきいち)秘密分散」実施基盤、

② 秘密分散により生成される 1 分割片の預かり基盤

となる。

1 つ目の「ユーザサイドでの閾値秘密分散実施基盤＝J2ET セキュア・ストレージサービス」：図 3.8（準公的機関としての直接バックアップ＋ディザスタ・リカバリ）は、3 分割片のうち 2 分割片を集めたら復元可能となるような秘密分散(閾値秘密分散)を実現するクライアント・アプリケーション・ソフトウェアと、本ソフトウェアを認証するためのサービスを提供する。本ソフトウェアにおいては、分割片の管理情報を原則ユーザしか知らない状態を作り出せるように、ユーザサイドで分割した分割片を、ユーザの意思で好きな場所に保管できる機能を提供することとなる。具体的には、JIPDEC が窓口となって、お客様の重要なデータを秘密分散技術を使って預かることで、バックアップおよびディザスタ・リカバリの機能を提供するようなサービスイメージとなる。

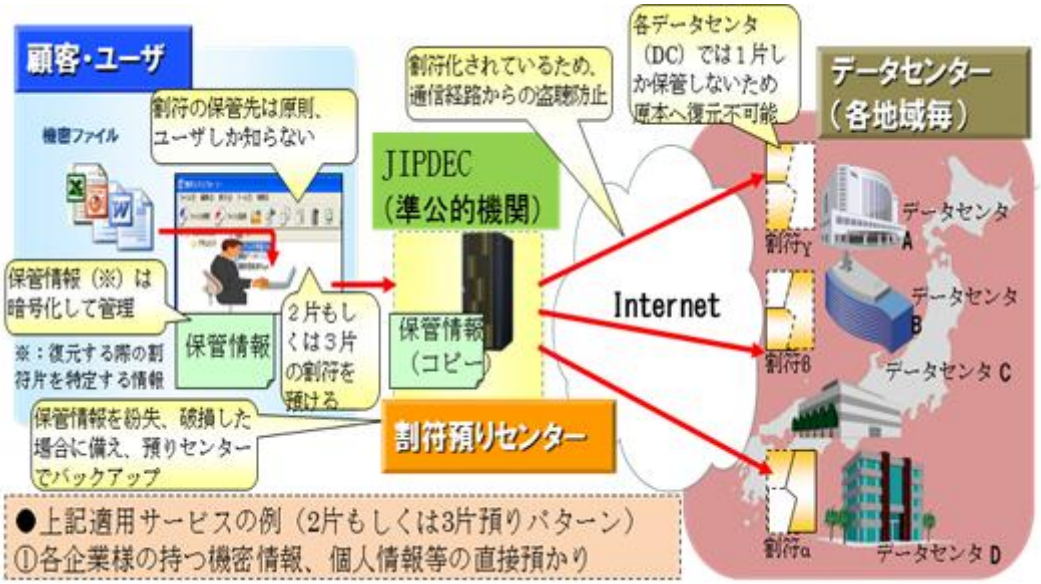


図 3.8　J2ET セキュア・ストレージサービス

2 つ目の「秘密分散により生成される 1 分割片の預かり基盤＝J2ET セキュア・バックアップサービス」図 3.9（事業者との連携による簡易バックアップ及びデータエスクロー）は、秘密分散された分割片の 1 つを JIPDEC が預かり、正式な復元要求があれば預かった分割片を引渡す機能を持つサービスを提供する。具体的には、他のサービス業者様が秘密分散技術を用いた預かりサービス等を実施するケースにおいて、JIPDEC がそのうちの 1 つを預かるようなサービスイメージとなる。

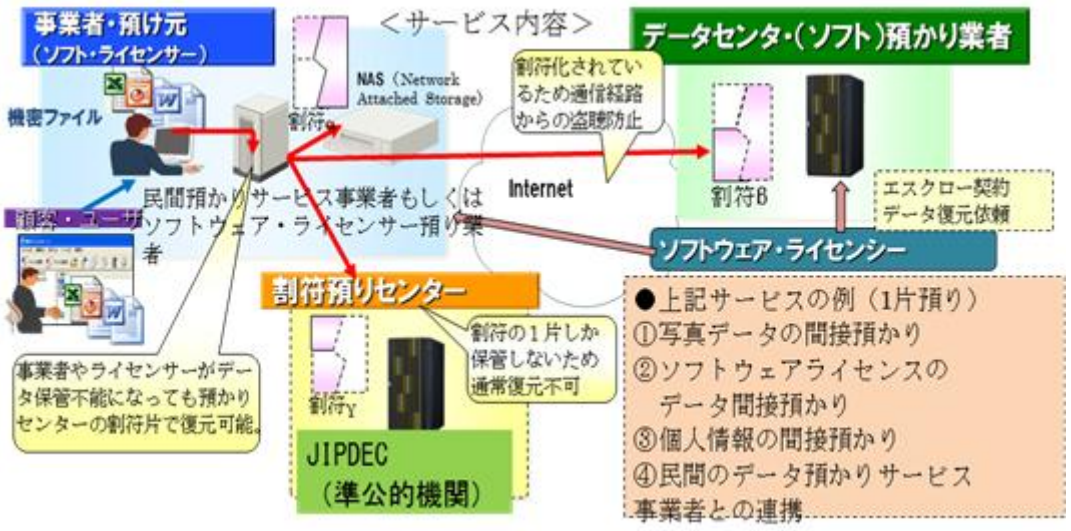


図 3.9　J2ET セキュア・バックアップサービス

3.3.7　まとめ

JIPDEC としては、秘密分散技術(電子的割符)を利活用するビジネスにおいて、将来発生するであろう問題への解決策を事前に考慮し、顧客企業における重要・機密情報（個人情報含む）の保管・取り扱いに対して、今回のサービスにより、コスト対策含めた新たな、しかも画期的なソリューションを提供できるものと考えている。

とくに電子的割符自体の特徴として、その導入企業にとって既存のシステム構成から見ても、とくに大きな管理負荷をかけずに運営でき、その導入コストも既存のセキュリティシステムと比較してかなりの削減を期待できるケースが多いというのが挙げられます。また、その保管対象データが割符化されて無意味情報となる観点から、余分な管理コストや対応業務も発生せずに、様々な法的環境整備という点からも長所として機能する可能性が高いと言える。

従って、大手企業の導入だけでなく、それほど規模が大きくなく、複雑なセキュリティシステム運営に不向な企業にとっても、「電子的割符」は、安全・安心でしかもエコなＩＴツールである。同時にその関連する情報システムについても、より簡便で簡易な利用が可能であるというメリットがあり、まさに、中小企業様に適した情報保護・管理システムであるということができる。

第４章　電子記録マネジメント基盤の今後の展開

本章では、2010 年度の活動結果を踏まえて、電子記録マネジメント基盤の中長期的な展望も含めた今後の展開について現時点での見通しを述べる。

4.1　電子記録マネジメント基盤の要件

2010 年度は、電子記録マネジメント基盤の要件案を策定し、実際の国内製品をもとに現状の実装とのギャップの見極めを行った。今後はさらに複数の製品について現状の実装を調査して確度を上げ、注力すべき項目を抽出するともに要件を確定する。

4.2　電子記録マネジメント基盤システム

(1)　電子記録マネジメント基盤システムの位置付け

ここでは、電子記録マネジメント基盤システムを、長期保存ストレージの存在を前提に、ID 管理基盤、署名・認証基盤、時刻認証基盤などの電子社会共通基盤と連携しながら業務アプリケーションに電子記録マネジメントサービスを提供するシステムとして位置付ける。

電子社会共通基盤は、さまざまなアプリケーション（及びその基盤）から利用されることが予想される。特にドメインをまたがったサービスを提供する場合は不可欠といっても過言ではない。個別のアプリケーションで対応するのは余りにも非効率である。電子記録マネジメント基盤サービスも例外ではない。

前章でも述べたように、電子記録マネジメント基盤システムは、記録の保存に加えて、記録の流通に必要なサービスを提供する流れになると考えられる。従って、土台としての保存基盤と、その上位層の流通基盤の 2 層構造を導入する。（図 4.1 参照）

図 4.1　電子記録マネジメント基盤システムの位置付け

(2) 保存基盤

保存基盤は、第三者による提供を含めて電子文書の安心安全な保存サービスを提供する部分である。ここでは、コアとなる記録のライフサイクル管理に加えて、登録した記録の原本性証明、長期に亙って記録の原本性を確保する原本性保存、及び原本性を確保した記録のフォーマット変換（原本性移行）を実現する必要がある。

このうち、原本性証明に関しては、既に韓国の公認電子文書保管所で実績を積んでいる。原本性保存に関しては、長期署名、媒体移行、長期保存フォーマットなど、JIS 化や ISO 化が先行している状況にある。原本性移行に関しては、紙から電子、電子から電子、電子から紙（またはマイクロフィルム）などの変換が考えられる。特に、電子から電子への変換については、ドイツの TransiDoc プロジェクトなどの報告はあるが、技術的に確立されているとは言い難い。署名やタイムスタンプの継承に関しては、更なる検討を要する。

第三者による提供においては、電子記録マネジメント基盤システム間のインターオペラビリティ（相互運用性）の確保が重要である。サービス停止に伴う他事業者のサービスへの移管が可能でなければならない。これは、インターオペラビリティに関して必要最小限の標準化が必要なことを意味している。

また、今や、非定型業務における記録が大半であることから、CASE マネジメントに即してコントロールが可能な CASE ファイルを提供する必要がある。CASE マネジメントとの連携に関しては、デンマーク政府の FESD Ⅱ が参考になる。

図 4.2 は、保存基盤のサービスイメージである。

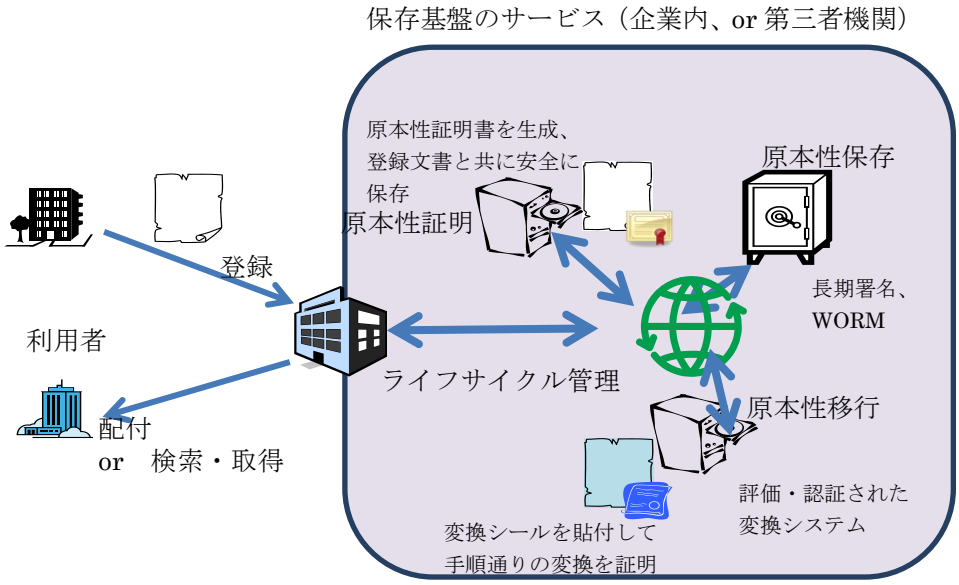


図 4.2 保存基盤のサービスイメージ

(3) 流通基盤

電子記録マネジメント基盤のなかの流通基盤のサービスについては今後広くコンセンサスを得る必要があるが、一案として、電子記録の流通に関するエビデンスをマネジメントする基盤であ

ると位置付けることが考えられる。言い換えると、電子記録に関して、何処で、何時、何をといったメタデータをキャプチャし、必要な時に流通の事実を検索できるようにするサービスを提供することである。モノに対応付けられた電子伝票が、何時、何処で発行され、何時、何処を経由して、何時、何処に到着したかを、メタデータとして管理することである。

図 4.3 は、流通基盤のイメージである。コアとなる仮称足跡管理サービスは、流通経路の動的管理、足跡としてのメタデータの収集とロギング（またはキャッシュ）、及び収集したメタデータの検索サービスを提供する。これにより、流通する特定の記録に関して、流通経路のトラッキング（発送元から宛先に向けての追跡）やトレースバック（発送元の逆探知）が可能になる。

流通証明は要求に応じて流通に関する証明（経路、場所、時間など）を行う。また、意味変換（セマンティック変換）は、ドメインをまたがる流通過程でのセマンティックの整合性を確保する。例えば、発行、中継、受取りといっても、どの時点を指すかはそれぞれのドメインによって異なることが考えられる。

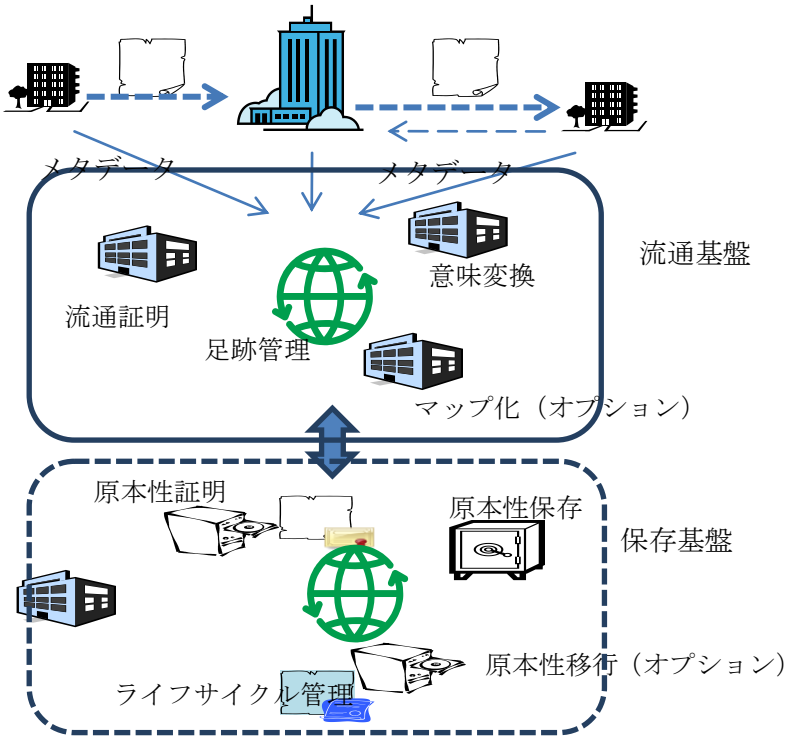


図 4.3　流通基盤のサービスイメージ

4.3　CASE マネジメントとの連携

CASE マネジメントに関連して、電子記録マネジメント基盤に求められることは、CASE マネジメントに沿ってコントロール可能な CASE ファイルを提供することである。ここでは、CASE マネジメントが適用される業務の対象として、プロジェクト管理や行政における事業などを想定する。

一般的な電子記録マネジメントにおいては（あるいは、ISO15498　記録管理では）、業務分類体系（BCS, Business Classification Schemes）に従ってファイルが定義されるが、CASE マネジメント環境ではより柔軟な対応が必要となる。すなわち、

・CASE ファイルを CASE（案件）ごとに紐付ける
・CASE ファイルは複数の組織の管轄下に置かれる可能性がある（動的に）
・CASE ファイルは複数の組織の関係者がアクセスする可能性がある（動的に）
ことを考慮する必要がある。
以下、CASE ファイルの特徴を示す。
・CASE ファイルにはプロジェクト内外との記録をすべて捕捉し格納する。
（含、メール、電話メモ、参照した過去の記録など）
・CASE ファイルを単位にライフサイクル管理（保持計画、廃棄、移管）を行う。
・CASE ファイルはその業務の責任者のみが生成でき、責任者が必要なメタデータを記述。
・CASE ファイルに格納した記録は保存期限満了まで削除でき。
・CASE ファイル内の記録は時系列が維持される。
・CASE ファイルを活用できるように、自動的に必要なメタデータが埋め込まれる。
・CASE ファイルは、担当者毎に必要なもののみ表示される。

図 4.4 に、CASE ファイルのイメージを示す。

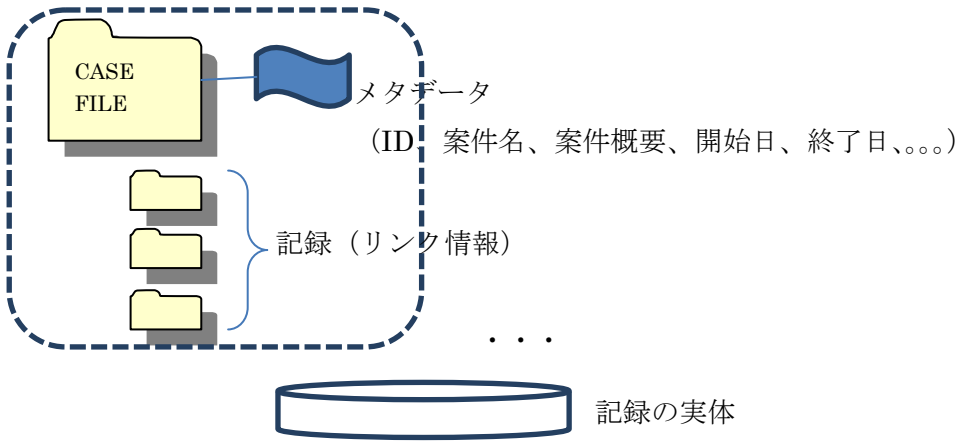


図 4.4　CASE ファイルのイメージ

4.4 情報パッケージ

電子記録マネジメント基盤へのアクセスは、何らかのまとまった単位で行う必要がある。ここでは、この単位をパッケージと呼ぶことにする。パッケージの仕様に関しては、韓国（公認電子文書保管所）、ドイツ(ArchiSafe)、ハンガリー（Dossie）などに実例がある。しかしながら、いずれも“記録”に関するパッケージングであり、分類体系におけるクラスやファイルに関しては対象外となっている（つまり、これらがサービス利用者側にあることが前提となっている）。これは、各々の電子記録マネジメント基盤システムが、単なる記録の格納庫に過ぎないことを意味している。

電子記録マネジメント基盤の目標は、マネジメントも含めた、インターオペラビリティの高いサービスの提供であり、このためには、クラスやファイルもパッケージングし、アクセスや移管を可能にしなければならない。

(1) パッケージの種類

表 4.1 に定義が必要なパッケージと関連インタフェースを示す。

表 4.1　定義が必要なパッケージと関連インタフェース

パッケージ / インタフェース	クラス	ファイル（CASE）	記録
生成/削除	○	○	
登録			○
配付			○
検索	○	○	○
移管	○	○	○

(2) パッケージフォーマット

原則的には、XML フォーマットとする。ただし、記録用の登録及び配付パッケージに関しては、PDF フォーマットも考慮する。

(3) パッケージ識別子

UUID を使用する。

付録１　用語（電子記録管理）

０．全般

管理上の役割（administrative role）
管理行為を認められたユーザに割り当てられる機能的な許可のセット。または、これらの許可をもつ人。

監理者（administrator）
組織内の記録管理方針の日常運用に責任をもつ役割。
注:大きな組織では、レコードマネージャ、アーキビスト、レコードオフィサーなど幾つかの役割に割り当てられる。

ユーザ（user）
ERMS を利用する任意の人。
注:監査人、管理者、事務所スタッフ、一般大衆のメンバーおよび外部人員を含む。

所有者（owner）
記録または集合に責任を負う人または役割。
注:法的な記録の所有者は記録を保持する組織である。

文書（document）
一つの単位として取り扱われる記録された情報，又はオブジェクト。
注:文書は、記録としてキャプチャされていない情報を意味する。

メタデータ（metadata）
記録のコンテキスト（背景・状況・環境），内容，構造，及びある期間の記録の管理について説明したデータ。

１．分類体系とファイル構成

分類（classification）
論理的に構成された規定，方法及び手順規則に従ったカテゴリによる業務活動及び／又は記録の系統的な識別及び配列。

分類体系（classification scheme）
クラス、ファイル、サブファイル、ボリュームおよび記録の階層的構成。

集合（aggregation）
クラス、ファイル、サブファイルあるいはボリューム。

クラス（class）
分類体系階層中の任意の点からそれより下のすべてのファイルまでの階層の部分。
注:クラスに割り当てられたすべての記録を意味するためにも使用する。

ファイル（file）
それらが、同じ主題、活動あるいはトランザクションに関係があることからグループ化された記録のひとまとまりの単位。
注:情報技術（IT）の用法とは異なる点に注意。

サブファイル（sub-file）
ファイルの知的細別。
注:サブファイルは、ケースファイル環境の中でしばしば使用される。

ボリューム（volume）
サブファイルの細別。
注:細別は管理のしやすさを改善するために作成され、知的ではなく機械的に行われる。

記録（record）
法的な責任の履行，又は業務処理における，証拠及び情報として，組織，又は個人が作成，取得及び維持する情報。
注:記録は１つ以上のコンポーネントから構成される。記録は、内容(content)に加えて、文脈上の情報、および適用可能な場合、構造情報(例えば記録のコンポーネントについて記述する情報)を含む。記録の重要な特徴はそれを変更することができないことである。

コンポーネント（component）
記録や文書を構成する、単独あるいは他のビットストリームに付随した個別のビットストリーム(distinct bit stream)。
注:情報技術におけるファイルと同義。別の用語を用いることにより記録管理上のファイルと混乱することを回避する。

２．コントロールとセキュリティ

重要記録（vital record）
緊急時および/またはその後に機能および/または組織の存続にとって不可欠な記録。

３．保持と処分

保持および処分計画（retention and disposition schedule）
スケジュール中に記述される、記録に認可された保持期間およびその後の処分作業を定義する形式上の道具。retention schedule とも呼ばれる。

処分（disposition）
処分権限又はその他の規定に基づいて文書化された，記録の保有，廃棄又は移管の決定に関係したプロセスの範囲。

処分保留（disposal hold）
記録の破棄および移管を防ぐ規則。

移管（transfer）
それらのメタデータと共に全電子ファイルを別のシステムに移動させるプロセス。

エクスポート（export）
別のシステム用に、それらのメタデータと共に電子記録のコピーを生成するプロセス。
注:記録は移管と異なりエクスポートの後にも ERMS に残る。

破棄（destruction）
記録を除去又は削除して，いかなる再生も不可能にするプロセス.

メタデータスタブ（metadata stub）
その項目(item)が保持され適切に破棄された証拠の役割をするために、その項目が破棄された後に保持される、そのアイテムのメタデータの部分集合。

４．キャプチャ及び記録の宣言

キャプチャ（capture）
(1) ディジタルオブジェクトの特定のインスタンスを記録または保存する行為。
(2) コンピュータシステムの中で情報を保存すること。
注:記録をキャプチャするとは、電子記録管理システム（ERMS）に記録を入れてオリジナル文書の内容を凍結することに関与するプロセスをすべて意味する。

登録（registration）
システムへの入力時に記録に独自の識別子を与える行為。

開始（open）
記録の追加を受理することができるよう、新しいファイル、サブファイルあるいはボリュームを作成するプロセス。

終了（close）
それがもはや記録の追加を受理することができないようにファイル、サブファイルあるいはボリュームの属性を変更すること。

バルクインポート（bulk importing）
他のアプリケーションから、それらのメタデータのうちの幾つかまたは全てと共に、電子記録のセットをキャプチャするプロセス。

記録タイプ（record type）
一般的レイアウト、コンテンツ、保管および処分の要件、および/またはメタデータなど共通の特性を共有する記録の種類。

５．参照

UUID (Universally Unique Identifier)
16 バイトの数値で表される一意に特定可能な識別子。ISO/IEC 11578、RFC4122 で規定。
注：GUID は MS 社による実装例。

６．参照、取り出し、及び表示

表示（presentation）
ERMS によって示されたユーザが参照することができる電子記録の発現。
注:画面表示、印刷、オーディオなどを含む。

７．管理上の機能

墨塗り（redact）
記録内の機微情報を隠すプロセス。
注:墨塗りは電子記録のコピー上で行なわれ、オリジナルの電子記録は影響を受けない。通常、情報の開示に対する制限に起因する。

墨塗り版、またはリダクション（redaction）
内容に追加や有意な修正を行わずに削除やマスク（墨塗り）が施された記録のコピー。

活用化（render）
活用版（レンディション）を生成する可視化プロセス。

活用版、またはレンディション（rendition）
記録の本来ファイル形式とは異なるファイル形式による記録またはコンポーネントの発現。注:例えば、所有者のファイル形式で生産された記録を、PDF/A あるいは XML のような標準形式にして格納するなど。

ファイル形式（file format）
人がアクセス可能な形式で表示することを可能にする記録またはコンポーネントの内部構造および/または符号化。

８．オプション

保管者（custodian）
記録を所持(possession)している人または組織的ユニット。

ケースファイル（case file）
具体的なプロセスまたは活動の結果として、構造化された（あるいは部分的に構造化された）方法でもって実行されたトランザクションに関するファイル。
注:ケースファイル中の記録は構造化されている場合も非構造の場合もある。

以　上

付録２　電子文書情報パッケージのための技術規格（抜粋）

電子文書情報パッケージのための技術規格（抜粋）
Technical Standard for Electronic Document Information Package

v1.20　2009年11月

1. 規格の概要

1.1　目的

「電子文書情報パッケージ技術規格(Technical Standard for Electronic Document Information Pakage)」は、公認電子文書保管所（以下「保管所」とする）を通じて流通する電子文書の全体的なプロセスを情報パッケージモデルの策定により電子文書の真正性を維持し、偽造・変造を防止することにより、電子文書の信頼性と完全性を図ることを目的とする。

また、電子文書情報パッケージの明確かつ適切な技術の規格化により保管所をベースとするe-ビジネスの活性化を図り、他保管所のシステムおよび外部システムとの相互運用性を高めることを目的とする。

1.2　適用対象および範囲

本規格は、保管所のシステムを開発しようとする企業（または機関）と保管所のシステムに文書を登録しようとする企業（または機関）を対象とする。また、保管所に電子文書を登録するプロセスから保存・流通・配布のプロセスまでを本規格の適用範囲とする。

また、電子文書の情報パッケージは国際標準であるISO14721を根拠とし、保管所の電子文書の管理のための一連のプロセスに必要なメタデータおよび諸要件は、国際標準であるISO15489とISO23018を参照した。

1.3　参照資料

□ ISO 14721: Space data and information transfer systems - Open Archival Information System - Reference model

□ ISO/TC 23081-1:2004

□ ISO 15489-1:2001(E)

□ 英国 PRO メタデータ標準: Requirements for Electronic Records Management System-Metadata Standard)

□ オーストラリア公文書館(NAA)電子記録管理のためのメタデータ(RMSCA)

□ 韓国大統領秘書室記録管理システム構築メタデータ定義書および説明書:2006

□ 韓国国家記録院, 記録管理システム革新のための ISP 事業: 2005

1.4　規格上の語彙

本規格において提示する規則の適用に関し、以下のタイプの語句を用いている。韓国語のみの

表現では不充分である場合には英文を併記した。

□ 必須要素：必ず本規格において提示する規則に従うべきときに用いる。規格に沿うためには厳密に従う必要があり、規則からの逸脱は認められない（英文: Must, Must Not）
- ～する。
- ～すること。
- ～しないこと。
- ～しない。

□ 推奨（選択）要素：本規格において提示する規則に従うことを奨めるときに用いる。この他の要素も差支えないが特に適していることを示す時に用いる。（英文: Should）
- ～するものとする。

□婉曲な禁止要素：規格の観点からは望ましくないが、絶対的な禁止ではない。（英文: Should Not）
- ～しないようにする。

□ 許容要素：規格の観点から認められることを示す。.（英文: May）
- ～できる。

2. 用語の定義

本規格の目的のため、用語を以下のように定義する。

1) 提出用情報パッケージ(Submission Information Package)：提出用情報パッケージは、利用者が保管所に登録するために生産・伝送するパッケージである。提出用情報パッケージは、メタデータと添付ファイルと利用者認証情報で構成される。
2) 保管用情報パッケージ(Archival Information Package)：保管用情報パッケージは、利用者が生産・伝送した提出用情報パッケージを安全に保存するため、保管所の内部で生産されたパッケージである。保管用情報パッケージは保存のために必要なメタデータと添付ファイルと保管所の認証情報で構成される。
3) 配布用情報パッケージ(Dissemination Information Package)：配布用情報パッケージは、保管所において保管している保管用情報パッケージを利用者の求める条件により閲覧あるいは発給をうけることのできる形態で生産し、利用者に伝送するパッケージである。
4) 電子文書(Electronic Document)：添付ファイルを紐づけする概念的な単位である。
5) 添付ファイル(electronic file)：実際の内容を収めた電子的形態のファイルで、情報パッケージの最小単位である。
6) アクセス(access)：利用者が情報をブラウズし、活用し、検索する権利・機会・手段をいう。
7) 変換(conversion)：文書を一つのメディアから他のメディアへ、またはあるフォーマットから他のフォーマットへ移し換える処理プロセスである。
8) 廃棄(destruction)：文書の再生が不可能となるように除去あるいは削除する処理プロセスである。

9) マイグレーション(migration)：文書をあるシステムから他のシステムへ、真正性・完全性・信頼性・利用可能性を保ちつつ移す行為

10) 長期保存版：10 年・20 年後にも特定のアプリケーションに従属せず電子文書の内容が確認できるフォーマットをいう。言い換えれば、当該フォーマットのアプリケーションソースが公開されており、そのアプリケーションのデベロッパーが消滅してもソースにより当該フォーマットを利用できるものをいう。これは、特定のアプリケーションに従属する電子文書の特性ゆえに必要な条件であるといえる。

11) 原本証明書：保管所が発給した電子文書の内容が、保管所に保管されている原本の電子文書の内容と同一であることを証明する保証書をいう。

3. 電子文書情報パッケージのモデル

3.1 電子文書情報パッケージの目的

保管所はユーザーが登録した電子文書を信頼性と完全性を維持したまま保管すること。このためには電子文書の保管に関連する業務プロセスとメタデータを有機的に関連付けられる体系が必要である。

保管所はユーザーが希望する時点まで電子文書を長期的かつ安全に保存し、これを利用可能であるように管理することが目的である。

保管所は電子文書の技術的環境の維持とともに、文書の真正性を維持することが必要である。真正性を維持するためには電子文書の業務の脈絡・構造・内容を保障する必要がある。

電子文書の保管と利用に関する設計は、一つのシステム内で構成されること。そして、このためには電子文書そのものが有機的な、断絶のない状態を維持する必要がある。このような形態を維持することにより、保管と利用のための一つの管理体系を構築し、これによりユーザーが希望する長期保存の条件を保障することができる。

結論として、電子文書により証明しうる業務の証拠性及び責任性、透明性を確保するための手段としての保管所の目的を保障すること。このため電子文書は業務の脈絡により有機的に関連付けられ、電子文書であるゆえに発生しうる時間の経過による電子的環境の陳腐化を防ぎうる技術的な変化が必須である。しかし、このような技術体系より情報そのものが信頼するに足るものであり、その情報を保障しうる確実な手段が必要である。これは電子文書をパッケージ化することにより確保できるものである。

3.2 電子文書情報パッケージの概念

電子文書は文書の内容と文書に関するメタデータにより構成される概念的な形態をいう。メタデータとは、電子文書の信頼性・完全性・可用性を満足させるため必要な文書の作成・登録・内容などに関する情報と、これを保管所のシステム内で保存及び活用管理するための情報により構成されるものである。

電子文書のメタデータは登録情報・分類情報・保存情報・構造情報・証明情報などにより構成される。

実際の文書の内容とメタデータをまとめて関連付けたものを電子文書情報パッケージといい、文書を登録・移管あるいは保存・配布する物理的な単位となる。

情報パッケージの構造を簡単にみていくと、

□ パッケージヘッダーは情報パッケージ全体の構造を指示する情報により構成されている。XML 領域のサイズ・バイナリデータの位置などに関する情報により構成されている。

□ XML 領域は情報パッケージに関するメタデータを記述する領域として、保存用情報パッケージの場合には 2 箇所、提出用情報パッケージと配布用情報パッケージは 1 箇所で構成されている。

□ バイナリデータ領域は実際の電子文書ファイルが添付される領域として、複数個の電子文書ファイルが添付される順序は電子文書内に含まれる添付ファイル情報の順序と同一である必要がある。

□ 原本証明書領域は電子文書の発給時、併せて発給される原本証明書が添付される領域として、配布用情報パッケージにのみ含まれる。

3.3 電子文書情報パッケージの種類

文書の管理プロセスにより提出用情報パッケージ(SIP)・保管用情報パッケージ(AIP)・配布用情報パッケージ(DIP)の形態に遷移し、管理される。

3.3.1 提出用情報パッケージ

提出用情報パッケージ(SIP; Submission Information Package)は、ユーザーのプログラムより提出され、受け入れられる文書の概念モデルをいう。基本的に電子文書と関連するメタデータ・ユーザーの証明情報により構成される。

3.3.2 保管用情報パッケージ

保管用情報パッケージ(AIP; Archive Information Package)は、保管所のシステムに登録され適切な管理措置により安定して保管される電子文書の概念モデルをいう。提出用情報パッケージを保管所のシステムに登録する時点で保管用情報パッケージが作成され、保管所のシステム内で一意の識別子を付与されて管理される。

XML領域1のメタデータは保管用情報パッケージを作成する間に情報を埋め込む領域である。XML領域2は保管所がユーザーから受け付けた提出用情報パッケージにあるXML領域をそのまま保管する領域である。XML領域2の役割は、ユーザーの電子文書登録行為につき否認を防ぐ役割をする。

XML領域1のメタデータは、本技術規格のメタデータリストにおいて定義されている通りに挿入すればよい。XML領域2のメタデータと重複してもXML領域1のメタデータは完結性を有したまま挿入する必要がある。すなわち、アプリケーションにおいて保管用情報パッケージのメタデータをバインドする場合、XML領域1のみを対象としてバインドし活用できるものとする。

保管用情報パッケージを作成するとき、提出用情報パッケージに添付されているファイル原本のうち、一つでも長期保存版に変換が可能であれば、原本の電子文書領域の他に長期保存版の電子文書領域を生成した後に、原本の添付ファイルを長期保存版に変換して添付する必要がある。このとき、提出用情報パッケージに添付されているファイル原本のうち、原本自体が長期保存フォーマットである、あるいはバイナリファイルであるなどにより変換が不可能であるか、必要の

ないファイルについては変換作業を省略のうえ原本ファイルをそのままの順序で含めるものとする。すなわち、原本の電子文書に含まれている添付ファイルの個数と、変換版の電子文書に含まれている添付ファイルの個数は同一である。

保管用情報パッケージ内には原本及び長期保存版の電子文書が存在するため、バイナリデータ領域に添付ファイルを含めるとき、まず原本の電子文書に含まれている電子文書のファイルを添付し、次いで長期保存版の電子文書に含まれている電子文書のファイルを添付するものとする。

万一、保管所のポリシー上長期保存版の電子文書が複数個である場合は、パッケージ内に含まれている長期保存版の電子文書の順序通りに電子文書のファイルを添付するものとする。

3.3.3 配布用情報パッケージ

配布用情報パッケージ(DIP; Dissemination Information Package)は、ユーザーの要請により保管用情報パッケージの一部あるいは全体を閲覧または発給するために構成される電子文書パッケージのモデルをいう。配布メディアとパッケージのタイプ、メタデータの構成はユーザーの要求により様々な構成が可能である。

3.4 パッケージヘッダー情報

パッケージヘッダー情報は、情報パッケージの全体構造をアプリケーションに指示する情報として、以下の情報により構成される。

番号	メタデータ	タイプ	桁数	備考
1	パッケージのバージョン	string	3	
2	パッケージの種類	string	3	
3	XML 領域 1 のサイズ	Long(4byte)	-	
4	XML 領域 2 のサイズ	Long(4byte)	-	
5	添付ファイルの個数	Short(2byte)	-	
6	添付ファイルのサイズ	Double(8byte)	-	配列の形態をいい、サイズは添付ファイルの個数を決定する
7	原本証明書のサイズ	Long(4byte)	-	

パッケージヘッダー情報は、XML形態で記載されず、プレーンテキストの形態で記載される。そのため、プログラムからは構造体を定義して用いることができる。

上記のメタデータを簡単に説明すると、

□ パッケージのバージョンは情報パッケージのバージョンを記述するものとみなす技術規格が改訂された場合、変更されたバージョンを使用し、本規格のバージョンは 1.1 として設定し、小数点第 1 位までのみ使用するものとする。(例：1.0, 1.5 など)

□ パッケージの種類は提出用情報パッケージであるか、保管用情報パッケージであるか、配布用情報パッケージであるかを区分する項目であり、SIP, AIP, DIP などに区分する。

□ XML 領域 1 のサイズはそれぞれの情報パッケージについてのメタデータを含む XML 領域のサ

イズを割り当てる。

□ XML 領域 2 のサイズは保管用情報パッケージ(AIP)において提出用情報パッケージ(SIP)に関連するメタデータを含む XML 領域のサイズを割り当てる。

□ 添付ファイルの個数は情報パッケージに挿入されている添付ファイルの全個数を割り当てる。

□ 添付ファイルのサイズは個々の添付ファイルのサイズを割り当てたもので、配列の形で規定し、添付ファイルの個数によりサイズを決定するものとする。すなわち、添付ファイルの個数が 10 個の場合、添付ファイルのサイズは 10 個の因子を持つ。

□ 原本証明書のサイズは DIP に含まれている電子文書の内容が電子文書の原本と同一であることを証明する原本証明書のサイズを割り当てる。

3.5 電子署名の範囲

電子署名の範囲はXML領域にのみ限り適用する。また、添付ファイルについてはハッシュアルゴリズムを用いてハッシュ値を生成した後にXML領域のメタデータに挿入するものとし、電子署名の範囲には添付ファイルを含めず、添付ファイルに関するハッシュ値のみ電子署名の範囲に含めるものとする。

保管用情報パッケージ(AIP)の場合にも、XML領域1のみを電子署名の範囲とする。その代わりにXML領域2を添付ファイルと同一の方式によりXML領域2に関するハッシュ値を生成してXML領域1のパッケージメタデータ(PackageMetaData)に挿入する方式を採るものとする。

配布用情報パッケージ(DIP)の場合には、バイナリデータに続いて添付される原本証明書がパッケージそのものの完全性及び否認防止の機能を提供するため、原本証明書のハッシュ値はXML領域のメタデータに挿入しない。

電子署名の生成方法は、enveloped方式とする。この方式は、電子署名値がエレメントをnullとし、次いでハッシュ値を生成し証明書の個人キーで暗号化のうえ生成、これをエレメントに挿入する方式である。

4. 電子文書情報パッケージのメタデータのタイプ

4.1 メタデータの全体リスト

下記の票は、本規格において定義する全てのメタデータリストの羅列であり、各パッケージごとに用いられるメタデータを“○”で表記した。

番号	メタデータの構成要素	パッケージ別生成の有無			備　考
		SIP	AIP	DIP	
ヘッダー情報(HeaderInformation)		O	O	O	
1	パッケージのバージョン (Version)	O	O	O	
2	パッケージの種類 (Type)	O	O	O	
3	XML 領域 1 のサイズ (XML1Size)	O	O	O	
4	XML 領域 2 のサイズ (XML2Size)	-	O	-	
5	添付ファイルの個数 (AttachFileQuantity)	O	O	O	
6	添付ファイルのサイズ (AttachFileSize)	O	O	O	
7	原本証明書のサイズ (CertificateSize)			O	
XML 領域					
パッケージメタデータ(PackageMetaData)		O	O	O	
8	パッケージ識別子 (PackageID)	O	O	O	
9	保存タイプ区分 (RetentionType)	O	O	O	
10	パッケージの内容説明 (Description)	O	O	O	
11	電子文書の個数 (DocumentQuantity)	O	O		
12	XML 領域 2 のハッシュ値 (HashValue)		O		
13	XML 領域 2 のハッシュアルゴリズム (Algorithm)		O		
14	ユーザー拡張領域	O	O	O	

	(Extensions)					
パッケージ認証情報(PackageAuthentication)			O	O	O	
15	署名日時 (DateTime)		O	O	O	
16	署名 (Signature)		O	O	O	
17	証明書 (Certificate)	発給者 (Issuer)	O	O	O	
18		一連番号 (Serial)	O	O	O	

19	署名者 ID (SignerID)			O	O	O	
20	署名者名 (SignerName)			O	O	O	
登録情報(RegisterInfo)				O	O	O	
21	電子文書識別子 (DocumentID)			O	O	O	
22	日時 (DateTimeInfo)	作成日時 (CreateDateTime)		O		O	
23		登録日時 (RegisterDateTime)			O	O	
24		要請日時 (RequestDateTime)				O	
25		受信日時 (ReceiveDateTime)			O		
26		発信日時 (SendDateTime)		O		O	
27	作成者 (ProductParty)	個人 (Person)	個人 ID (PersonID)	O	O		
28			個人名 (PersonIName)	O	O		
29		機関 (Organizati on)	機関 ID (OrganizationID)	O	O	O	
30			機関名 (OrganizationName)	O	O	O	
31		電子メール (ElectronicMail)		O	O		電子メールと住所・電話番号などは自宅あるいは会社などのタイプにより区分しうるが、会社系のタイプを優先して記述する
32		部署名 (DepartmentName)		O	O		
33		職位名 (PositionName)		O	O		
34		住所 (Address)		O	O		
35		電話番号 (PhoneID)		O	O		
36	受信者 (ReceiveParty)	個人 (Person)	個人 ID (PersonID)			O	
37			個人名 (PersonIName)			O	
38		機関 (Organiza ti on)	機関 ID (OrganizationID)	O		O	
39			機関名 (OrganizationNam e)	O		O	
40		電子メール (ElectronicMail)				O	- 同上

41		部署名 (DepartmentName)				O	
42		職位名 (PositionName)				O	
43		住所 (Address)				O	
44		電話番号 (PhoneID)				O	
45	要請者 (RequestParty)	個人 (Person)	個人 ID (PersonID)			O	
46			個人名 (PersonIName)			O	
47		機関 (Organizati on)	機関 ID (OrganizationID)			O	
48			機関名 (OrganizationNam e)			O	
49		電子メール (ElectronicMail)				O	- 同上
50		部署名 (DepartmentName)				O	
51		職位名 (PositionName)				O	
52		住所 (Address)				O	
53		電話番号 (PhoneID)				O	
54	関係者 (RelationParty)	個人 (Person)	個人 ID (PersonID)	O	O		
55			個人名 (PersonIName)	O	O		
56		機関 (Organizati on)	機関 ID (OrganizationID)	O	O		
57			機関名 (OrganizationNam e)	O	O		
58		電子メール (ElectronicMail)		O	O		
59		部署名 (DepartmentName)		O	O		
60		職位名 (PositionName)		O	O		
61		住所 (Address)		O	O		
62		電話番号 (PhoneID)		O	O		
63	業務手続の区分（テキスト） (BusinessProcessType)			O	O		

64	出典タイプの区分（テキスト） (SourceType)			O	O		
分類情報(ClassificationInfo)				O	O		
65	分類スキーマの区分 (ClasssificationSchemeType)			O	O		
66	分類スキーマ ID (ClassificationSchemeID)			O	O		
67	分類スキーマ名 (ClassificationSchemeName)			O	O		
68	分類コード (ClassificationCode)			O	O		
69	分類コード名 (Description)			O	O		
詳細情報(DetailInfo)				O	O	O	
70	内容説明 (DetailDescription)			O	O	O	
71	添付ファイルの個数 (AttachFileQuantity)			O	O	O	
72	電子文書形態のコード (DocumentForm)			O	O	O	
73	タイトル (Title)	メインタイトル (MainTitle)		O	O	O	
74		サブタイトル (SubTitle)		O	O	O	
75	インデックス (Index)	キーワードステップ (KeywordStep)		O	O		
76		キーワード (Keyword)		O	O		
77	電子文書のタイプ（テキスト） (DocumentType)			O	O		
78	言語 (LanguageCode)			O	O	O	
権限情報(RightsInfo)				O	O	O	
79	セキュリティ (Security)	セキュリティレベル (SecurityLevel)		O	O	O	
80		セキュリティレベルの説明 (SecurityDescription)		O	O	O	
81	利用 (Use)	ユーザー (User)	個人 ID (PersonID)			O	
82			個人名 (PersonIName)			O	
83		証明書 (Certificate)	発給者 (Issuer)			O	

84			一連番号 (Serial)			O	
保存情報(RetentionInfo)				O	O		
85	保存満了日 (RetentionExpiredDate)			O	O		
86	暗号化 (Encryption)	暗号化処理区分 (EncryptionType)		O	O		
87		証明書 (Certificate)	発給者 (Issuer)		O		
88			一連番号 (Serial)		O		
添付ファイルの情報(AttachFileInfo)				O	O	O	
89	添付ファイル ID (FileID)			O	O	O	
90	添付ファイル名 (FileName)			O	O	O	
91	添付ファイルの作成日時 (DateTime)			O	O	O	
92	添付ファイルの説明 (Description)			O	O	O	
93	添付ファイルの容量 (Volume)				O	O	
94	添付ファイルのフォーマット (Format)			O	O	O	
95	変換可能指示子 (TransformIndicator)			O			
96	ソフトウェア (Software)	OS 環境 (OperatingSystem)		O	O	O	
97		アプリケーション (Application)		O	O	O	
98		バージョン (Version)		O	O	O	
99	添付ファイルの証明 (Authentication)	ハッシュ値 (HashValue)		O	O	O	
100		ハッシュアルゴリズム (Algorithm)		O	O	O	

4.2 メタデータ集合情報タイプの定義

① パッケージメタデータ

管理番号	IP-ABIE-001
英文名	PackageMetaData
定義	パッケージ全体に関する情報を意味する。
目的	パッケージの識別情報およびパッケージ内に含まれる情報オブジェクトに関する全体的な説明を記述する。
根拠	- ISO 15489 完全性・真正性要件を充足 - ISO 23081 記録管理・記録そのものに関するメタデータの要件を充足
繰り返し数	1...1
利用条件	---
備考	---

② パッケージ認証情報

管理番号	IP-ABIE-002
英文名	PackageAuthentication
定義	パッケージの完全性を保障するための情報を意味する。
目的	パッケージ内に含まれる情報オブジェクトの真正性・完全性の立証を可能とするための根拠として役割をする。
根拠	- ISO 15489 完全性・真正性要件を充足 - ISO 23081 記録管理・記録そのものに関するメタデータの要件を充足
繰り返し数	1...1
利用条件	---
備考	情報オブジェクトの完全性値が含まれる XML 領域に関する認証及び完全性を保証することにより、結果として情報オブジェクトの認証及び完全性が保障される。

③ 登録情報

管理番号	IP-ABIE-003
英文名	RegisterInfo
定義	電子文書に関する固有の識別記号・日付などのような電子文書の作成と登録に必要な情報を意味する。
目的	全ての電子文書の SIP 生成段階及び AIP の管理段階においてこれらを固有のものとして識別し、電子文書客体の位置を把握し、あるいは参照するために活用する。
根拠	登録情報は電子文書及び各階層に関する固有の情報を付与し、電子文書客体を固有のものとして識別しうるようにし、SIP の生成により AIP 登録を行うときにも当該電子文書及び各階層に属するファイルなどについての必須情報を提供する要素である。 - ISO 15489 利用可能性・レコードの獲得と登録要件を充足 - ISO 23081 記録そのものに関するメタデータの要件を充足 - オーストラリア RMSCA の登録情報を充足
繰り返し数	1...1

利用条件	電子文書及び添付ファイルの識別子のタイプと形態は、ユーザーのプログラムにより一部が決定され、保管所において直接割り当てる。 また、この要素は内容情報を記述する諸要素とリンクされそれぞれが一貫したものであることを証明する必要がある。
備考	---

④　分類情報

管理番号	IP-ABIE-004
英文名	ClassificationInfo
定義	情報の業務機能をはじめ分類情報を意味する。
目的	情報オブジェクトが表現する業務機能との関係を記録することにより、タイトルが提供するものより、一層具体的な水準において接点を提供する役割をする。 ※各自の観点による様々な分類が可能である。
根拠	- ISO 15489 利用可能性の要件を充足 - ISO 23081 業務活動あるいはプロセスに関するメタデータの要件を充足
繰り返し数	1..*
利用条件	分類情報は情報オブジェクトの生成目的により決定され、情報生成の根拠となる。 また、この要素は情報オブジェクトが生成されるとき既に存在する分類スキーマの値を持つことがある。
備考	SIP により生成され AIP に登録される。

⑤　詳細情報

管理番号	IP-ABIE-005
英文名	DetailInfo
定義	電子文書の物理的構造と論理的構造である内容と関連した説明情報
目的	電子文書の構造及び電子文書が有する特性を文書化することにより、 DIP 提供時ユーザーに効果的な接点を提供し、その利用を促進させることができる。
根拠	- ISO 15489 真正性の要件を充足 - ISO 23081 記録そのものに関するメタデータの要件を充足
繰り返し数	1..1
利用条件	内容説明は登録情報を参照して表現できる。このように作成された内 容説明は、インデックスの抽出において参照できる。
備考	---

⑥　権限情報

管理番号	IP-ABIE-006
英文名	RightsInfo
定義	情報オブジェクトの利用及びアクセスを管理し、制限するための情報を意味する。

目的	秘密または非公開に分類された記録物を適切に管理するための要素として、情報オブジェクトのセキュリティレベル・公開の可否・閲覧範囲などの利用とアクセスに関する情報を記録し、情報オブジェクトへの不法アクセスを防止し記録の完全性を維持できるようにするためのものである。
根拠	- ISO 15489 完全性の要件を充足 - ISO 23081 記録そのものに関するメタデータの要件を充足
繰り返し数	0..1
利用条件	権限情報は認証された機関により修正されることがある。
備考	---

⑦ 保存情報

管理番号	IP-ABIE-007
英文名	RetentionInfo
定義	文書が作成された後、登録されて保管所のシステムにより文書が保管されるときに行われる全ての行為に関する情報
目的	内部／外部の環境の変化により保管所のシステムに保管されている情報になされる全ての保存履歴を提供することにより、文書を維持管理するために行われる全ての管理業務に確実な証拠を提供するため
根拠	- ISO 15489 真正性・完全性の要件を充足 - ISO 23081 記録そのものに関するメタデータの要件を充足
必須／選択	選択
繰り返し数	1..1
利用条件	保存行為はパッケージ単位で行われるものであり、パッケージに一貫して適用する。これによりパッケージ内の全ての情報が一括した保存行為に適用される。
備考	---

⑧ 添付ファイル情報

管理番号	IP-ABIE-008
英文名	AttachFileInfo
定義	作成機関または個人が作成したパッケージの対象である添付ファイルに関する情報である。
目的	パッケージ対象の添付ファイルに関する情報を明確にすることにより、パッケージ後も添付ファイルの内容が真正であり完全であることを立証するためである。
根拠	- ISO 15489 完全性・真正性の要件を充足 - ISO 23081 記録管理・記録そのものに関するメタデータの要件を充足
必須／選択	
繰り返し数	1...*
利用条件	---
備考	添付ファイルの認証は、認証についての行為が生じるごとに反復される。

5. 電子文書情報パッケージの検証

保管所をはじめ全ての電子文書情報パッケージの利用主体は、電子文書情報パッケージを利用

する前に検証作業を行うこと。

保管所は、提出用情報パッケージを受信し、これを保管用情報パッケージに変換するプロセス及び保管用情報パッケージを利用して配布用情報パッケージを生成するプロセス中に、それぞれの提出用情報パッケージについての検証を行うこと。

同様に利用者は保管所が発給した配布用情報パッケージを利用する前に、これについての検証を行い、万一、自身または他人が生成した提出用情報パッケージの内容を確認する必要がある場合でも、これについての検証を行うこと。

検証プロセスは情報パッケージの種類により若干の差があるものの、大きくは構造の検証・完全性の検証・内容の検証に区分できる。

ただし、各プロセスは必要により順序の入れ替え・統合または細分化が可能である。

5.1 構造の検証

情報パッケージの構造の検証は、検証の対象である情報パッケージが本規格において定義される情報パッケージの構造と各要素のtype及び値の請約範囲などを遵守しているかを確認する作業である。

検証システムは、情報パッケージの構造の検証時、本規格に伴い提供される情報パッケージのスキーマを参照し、検証の対象である情報パッケージが該当するスキーマを遵守しているかの有無を検証すればよい。

万一、情報パッケージの構造の検証が失敗すれば、検証システムは該当するエラーの原因を情報パッケージの利用主体に出力するものとし、情報パッケージの利用主体は当該情報パッケージを利用してはならない。

構造の検証プロセスは、各情報パッケージの種類に拘らず行う必要がある。

5.2 完全性の検証

情報パッケージの完全性の検証は、一般的に電子署名の検証とハッシュ値の検証に区分される。

電子署名の検証は、情報パッケージのXML領域1に添付された電子書名値を検証するプロセスであり、本規格に定義された要素であるSignatureについての検証を行うものとし、生成時と同様にW3C “XML-Signature Syntax and Processing“ (RFC3275)で記述された検証方法を準用して検証を行うものとする。

併せて電子署名に用いられた証明書の有効性確認の作業も電子署名の検証と同時に電子署名の検証プロセス中に必ず行うこと。

証明書の有効性確認作業は、公認証明体系の「公認証明書パス検証技術規格[KCAC.TS.CERTVAL]」を準用し検証する。

署名証明書の有効性検証に失敗した場合、情報パッケージの完全性を保証しえないため、検証システムは該当するエラーの原因を情報パッケージの利用主体に出力するものとし、情報パッケージの利用主体は当該情報パッケージを利用してはならない。ただし、署名証明書の有効性検証に失敗しても、電子署名の長期検証技術が適用され、当該検証技術により検証のうえ成功すれば、署名証明書の有効性検証の結果とは関係なく情報パッケージの電子署名検証に成功したものとして処理する。

長期検証技術は、本バージョンの規格においては扱わず、情報通信産業振興院または関連機関が提供する技術規格を準用するものとする。

電子署名の検証プロセスは、XML領域1についての完全性のみを保証し、XML領域1以外の主な領域値についての完全性の検証を行う必要がある。すなわち、XML領域2とバイナリデータ領域についての完全性の検証を行うこと。

全ての情報パッケージは、バイナリデータ領域について完全性の検証が行われ、保管用情報パッケージの場合には加えてXML領域2に対する完全性の検証を行う必要がある。

バイナリデータ領域に対する完全性の検証は、XML領域1の添付ファイル情報に含まれる各添付ファイルのハッシュ値と実際の添付ファイルのハッシュ値を比較することにより行われる。

すなわち、検証システムはバイナリデータ領域に添付された個々の添付ファイルをハッシュした後、XML領域1の添付ファイル情報に含まれる各添付ファイルのハッシュ値と比較してこれが同一であることを確認する必要がある。

これと同一に、検証システムは保管用情報パッケージに対しXML領域2の全体をハッシュした後、XML領域1のパッケージメタデータに含まれるXML領域2のハッシュ値と比較してこれが同一であることを確認する必要がある。

ハッシュ値を検証するプロセスと、電子署名を検証するプロセスは、必要により順序が変わることがある。

電子署名の検証およびハッシュ値の検証に失敗した場合、情報パッケージの完全性を保証しえないため、検証システムは該当するエラーの原因を情報パッケージの利用主体に出力するものとし、情報パッケージの利用主体は当該情報パッケージを利用してはならない。

5.3 内容の検証

情報パッケージの内容の検証は、検証対象の情報パッケージの各要素に記述された値が、本規格において提示した制約事項を遵守し、相互に矛盾がないかを確認する作業である。

情報パッケージに記述された各要素の値につき、情報パッケージスキーマにより検証可能な全ての制約事項についての検証、すなわち構造の検証プロセスにより確認しうる項目を除いた他の全ての項目についての検証を内容の検証ということができる。

例えば、datetime typeの諸要素間の前後関係・証明書の発給者を記述するときのDN形式の遵守の有無・添付ファイル情報において添付ファイルのサイズ値・datetime type要素において各時間単位の最大値超過の有無・電子メールの形式・情報パッケージに記述された主体の識別子についての検証が必要な場合、これについての検証、分類スキーマ区分値による分類スキーマID及び分類コードの設定・添付文書についての変換機能指示子値などは、本内容の検証プロセスにおいてエラーの有無を確認しうる。

この他にも、情報パッケージの各要素に記述された値が本規格の本文において提示した内容に違背し、もしくは各要素間に矛盾があれば、本内容の検証プロセスにおいて該当するエラーを確認できること。

情報パッケージの内容の検証に失敗した場合、検証システムは該当するエラーの原因を情報パッケージの利用主体に出力するものとし、情報パッケージの利用主体は当該情報パッケージを利用してはならない。

付録３　公認電子文書保管所の文書転送のための技術規格（抜粋）

公認電子文書保管所の 文書転送のための技術規格（抜粋）
Technical Standard for Documents Transfer between ARCs

v1.20　2009年11月

1. 規格の概要

1.1　目的

公認電子文書保管所（以下「保管所」）は、顧客が保管した電子文書について安定的かつ信頼性のある形で保管し、保管した電子文書をサービスに供するよう法的に「公認」されたサービス事業者である。よって、使用者の要求及び保管所の認証取り消しあるいは営業廃止などの事情により、電子文書を保管し続けることができない状況が発生した際、それまで保管中であった電子文書を他の保管所のシステムに安全かつ速やかに移管し、顧客（ユーザー）にサービスを提供する必要がある。

保管所は顧客に最適なサービスを提供するため、各事業者ごとに固有のシステムアーキテクチャー及び情報モデルを保有している。このように、相互に異なる情報構造を持つ保管所間で電子文書を円滑に転送するためには、これに必要な実行方法・実行手続・伝達される情報及び資料の範囲・構造などの標準案を提示する必要がある。

本「公認電子文書保管所の文書転送のための技術規格」（以下「本技術規格」）は、保管所のサービス事業者が円滑に電子文書を移管あるいは受管しうるようにするための基準案を提示するため作成された。

1.2　適用対象および範囲

全ての保管所は、本技術規格を遵守し、保管中の電子文書を他の保管所に移管することができ、他の保管所が移管を要求する電子文書を受管できる必要がある。

1.3　参照資料

□ ISO 14721: Space data and information transfer systems - Open Archival Information System - Reference model

□ ISO/TC 23081-1:2004

□ ISO 15489-1:2001(E)

□ 英国 PRO メタデータ標準: Requirements for Electronic Records Management System-Metadata Standard)

□ オーストラリア公文書館(NAA)電子記録管理のためのメタデータ(RMSCA)

□ 韓国大統領秘書室記録管理システム構築メタデータ定義書および説明書:2006
□ 韓国国家記録院, 記録管理システム革新のための ISP 事業: 2005
□ 韓国電子取引振興院, 電子文書情報パッケージのための技術規格: 2006
□ 韓国電子取引振興院, 電子文書証明書のフォーマット及び運用手続のための技術規格: 2006
□ 韓国電子取引振興院, ユーザーシステムと公認電子文書保管所間の連携インターフェイスのための技術規格: 2006

1.4 指針となる語彙

本指針において提示する規格の内容と関連して、次のタイプの文章と語句を用いている。韓国語のみの表現では不充分である場合には英文を併記した。

□ 必須要素：必ず本規格において提示する規則に従うべきときに用いる。規格に沿うためには厳密に従う必要があり、規則からの逸脱は認められない（英文: Must, Must Not）
▪ ～する。
▪ ～すること。
▪ ～しないこと。
▪ ～しない。

□ 推奨（選択）要素：本規格において提示する規則に従うことを奨めるときに用いる。この他の要素も差支えないが特に適していることを示す時に用いる。（英文: Should）
▪ ～すること。

□婉曲な禁止要素：規格の観点からは望ましくないが、絶対的な禁止ではない。（英文: Should Not）
▪～しないようにする。

□ 許容要素：規格の観点から認められることを示す。（英文: May）
▪～できる。

2. 用語の定義

イ）「移管」とは、保管所が独自に保管している電子文書を様々な必要性により保管・活用・管理サービスを中止し他の保管所へ登録・活用・管理を依頼するため、電子文書・初期登録証明書と管理情報を伝達することをいう。

ロ）「受管」とは、他の保管所が保管していた電子文書の移管を依頼する場合、この伝達を受けて顧客に登録・活用・管理サービスを提供するために保管所の情報構造に即して電子文書及び管理情報を登録することをいう。

ハ）「移管保管所」とは、保管していた電子文書を他の保管所に「移管」の依頼をする保管所をいう。

ニ)「受管保管所」とは、「移管保管所」の移管依頼を受け、電子文書を「受管」する保管所をいう。

ホ)「移管モジュール」とは、「移管保管所」が移管対象である電子文書の情報を保管所のシステムから抽出(export)し、受管保管所に伝達する作業を行うプログラムをいい、オンラインとオフライン方式の移管を全てサポートする。

ヘ)「受管モジュール」とは、「受管保管所」が移管保管所より移管要求の情報を受信した後、これを解析し受管保管所の保管所システムに保存する作業を行うプログラムをいい、オンラインとオフライン方式の移管を全てサポートする。

ト）移管情報パッケージ(Transfer Information Package,以下 TIP）は、保管所が保管している電子文書を他の保管所に移管するため、移管対象となる情報を電子文書の単位で構造化した情報パッケージをいう。移管情報パッケージはパッケージヘッダー・XML 領域 1・XML 領域 2（SIP の XML 領域）・電子文書の添付ファイル・初期登録証明書により構成される。

3. 電子文書の文書転送

3.1 概要

保管所は様々な事由により、保管中の電子文書を他の保管所に移管あるいは他の保管所で保管中であった電子文書を受管することがある。文書転送の作業は保管所において登録され保管中であった電子文書を他の保管所に移す作業であるため、ユーザーが電子文書を保管所に新規登録する過程とは異なり、初期登録の時点及び保管事実の証明・同一識別子の処理・ユーザー情報とのマッピング・管理情報の登録・何よりも多量の電子文書に関する処理など、考慮すべき事項が多い。

全ての保管所の文書保管設備の実現方式が同一でないことがあるため、本技術規格においては文書転送の対象・文書転送の手続・送受信プロトコル・パッケージフォーマットセキュリティの要件など、全ての保管所のシステムに適用可能な文書転送の共通事項につき規定しており、データのexportとimport手続など、文書保管設備の実現方式と関連する部分は移管保管所と受管保管所の協議のもとに適切な方式により実行することを提案している。

3.1.1 移管対象情報

移管対象となるデータは、各ユーザー別に保管を依頼した電子文書・初期登録証明書及び管理のための各種管理情報となる。

○ 電子文書：ユーザーが登録した電子文書の原文であり、TIP の形態に変換され、文書転送される。文書転送の必須対象情報である。

○ 初期登録証明書：ユーザーが保管所に電子文書の登録を依頼した最初の時点で正常に登録され

たことを証明するため「証明書フォーマット及び運営手続」技術規格に定義されたフォーマットにより発行された構造体情報である。受管保管所は TIP に添付された初期登録証明書につき検証を行った後、発給者及び署名者情報を除いたフィールドの内容をそのまま維持し、初期登録証明書を再度生成する必要がある。電子文書につき文書転送が再度発生したときは移管保管所より電子文書を受管したときに生成された初期登録証明書のみ文書転送の対象として移管する。万一、移管の時点で初期登録証明書に添付された電子署名の有効期間が満了していた場合は移管保管所は必ず有効な証明書を用いて初期登録証明書を更新した後に移管すること。文書転送の必須対象情報である。

○ ユーザー情報：両保管所間の協議のもと、電子文書の転送前に予め移管または登録されている必要がある。文書転送の選択的対象情報である。

○　管理情報：文書転送の選択的対象情報である。
電子文書に関する基本属性情報：パッケージ番号・登録日時・登録者・所有者

電子文書に関する拡張属性情報：移管保管所及び管理される電子文書のタイプにより追加して定義される

電子文書に関するセキュリティ（アクセス権限）情報

その他の情報

・連関関係情報：電子文書と分類スキーマ間の連関情報・電子文書及び属性情報と連関情報・証明書資料との連関情報

3.1.2　事前の準備作業

保管所が電子文書の文書転送を円滑に行うためには、次の事前準備作業を行うものとする。

○ 移管対象及び範囲を基準として移管・受管保管所間で協議
移管保管所は移管対象及び範囲を確定のうえ受管保管所との業務協議により移管要求に対する受容の可否を決定する

移管対象及び範囲が確定したら両保管所はこれに関する契約書を作成する。

○ 移管方式及び移管日程に関する協議
移管データの容量・要求日程・移管・受管保管所のシステム要件などにより移管のための具体的な方法につき協議

・移管データの容量及び処理期間などを主な基準としてオフライン方式またはオンライン方式を

決定

・文書転送の方式に関する最終決定は、移管データの容量あるいは処理機関だけでなく、移管・受管保管所が協議した日程及び保管所のシステム環境などにより両保管所が最終決定を行なうものとする

文書転送の対象情報及び情報構造に関する合意が必要

・移管が必要なユーザー情報構造
・ユーザー別の分類スキーマについての受容の可否及び受容時の移管方法
・電子文書に関するユーザーのアクセス権限水準に関する協議
・移管対象の電子文書の追加拡張属性情報の現況及び受管保管所の需要方法
・移管保管所が管理していた追加情報のタイプ及び移管の可否（例：電子文書間の連関関係情報など）に関する協議
・移管保管所が管理しない情報のうち、受管保管所が管理のため必ず必要とする付加情報がある場合、これに関する情報獲得の方法

ユーザーと受管保管所間の利用契約の締結及び登録。選択的な準備作業である

・受管保管所は、移管されるユーザーに関する情報をもとに、各ユーザー単位で利用契約を締結、登録する。

移管保管所のユーザー情報と受管保管所のユーザー情報間のマッピング情報を準備

・受管保管所は移管保管所のユーザーA が保有する移管対象の電子文書を受管保管所のどのユーザー情報に移管するかにつきマッピングした情報を準備する。

保管所間で管理方式の相違したデータに関して協議した処理方法により処理モジュールを準備

3.1.3　電子文書の移管手続

電子文書の文書転送は、①ユーザーの要求による移管　②移管保管所の営業停止による移管などがあるが、それぞれの移管のタイプにより文書転送手続において多少の相違がある。

①　ユーザーの要求による移管

使用者の要求による移管の場合には、使用者が受管移管所を指定して移管保管所に電子文書の移管を要求する場合であり、ユーザーが移管を要求する手続が先行して行なわれる必要がある。ユーザーの移管要求を受けた移管保管所は、対象となる受管保管所と移管対象の範囲及び方式・日時につき合意した後、合意した内容をユーザーに通知して移管に関する最終確認を行う。

ユーザーの最終確認を受けた後に移管保管所と受管保管所は移管のための実際のプロセスを進

めるものとする。

② 移管保管所の営業停止による移管

移管保管所の営業停止により、ユーザーの意図に関わらず移管が避けられない場合に、移管保管所は移管対象の電子文書及び範囲を把握した後、これをもとに受管保管所と電子文書の受管の可否を交渉するものとする。基本的に文書転送に関する合意が成立したら、移管保管所は各ユーザーに移管に関する進行状況を通知する。移管保管所と受管保管所は移管範囲及び方式・日時に関する追加の交渉を行なった後、合意した内容を改めてユーザーに通知し最終確認を受け、移管のための実際のプロセスを進めるものとする。

文書転送に関する初期の基本的な合意のプロセスが完了したら、電子文書転送のための実際の処理プロセスは次のように進められる。

3.1.3.1 電子文書の移管手続フロー

(1) 電子文書の移管の範囲を定義する。

○ 事前準備情報

移管対象となるユーザー情報及び電子文書の範囲を調査

移管・受管保管所及び使用者との合意により、移管保管所が提供した付加サービス情報に関する移管の可否を決定

○ 移管対象データ

電子文書原本・初期登録証明書

電子文書に関する属性情報（基本属性及び拡張属性）

電子文書に関するセキュリティ（アクセス権限）情報

その他付加情報（選択事項）

○ 連関関係情報：電子文書と分類スキーマ間の連関情報・電子文書及び属性情報と連関情報・電子文書及び証明書資料との連関情報

○ 付加サービス情報：保管所の特性によりユーザーに提供されていた付加サービス情報

(2) 移管・受管保管所は、移管日程及び方式につき合意し事前情報の文書転送または登録に関する準備作業を行う。

○ 先だって合意した移管範囲により、両保管所は移管の処理日程及び方式を論議し、これに関する合意を行う

○ 受管保管所は、移管対象のユーザーと電子文書の移管前にあらかじめ受管保管所と利用契約を締結するものとする。

○ 移管保管所より受管保管所にユーザー情報を移管または登録

○ 移管保管所のユーザー情報と受管保管所のユーザー情報の間で、予め電子文書転送のためのマッピング情報を定義しておくこと

○ 受管保管所にユーザー単位の分類スキーマ情報を登録（受管保管所の既存の分類スキーマに再分類する場合には、このプロセスは省略されることがある）

○ 受管保管所は、移管保管所のユーザーの分類スキーマと受管保管所において受管ユーザーが用いることのできる分類スキーマの間にユーザー単位でマッピング情報を定義する必要がある

○ 移管・受管保管所間で合意した移管情報の範囲及び方式により、これまで保有していた文書転送モジュールをカスタマイズする

(3) 電子文書移管情報の export

○ 移管対象の電子文書を定義してこれを検索する。

○ 移管対象の電子文書・証明書及び管理情報などを本技術規格の「3.2 文書転送の情報構造」において明示したフォーマットに即して export する

○ 顧客の要求により暗号化して保管中である電子文書は、必ず復号化の作業を行うこと

○ 移管の時点で初期登録証明書の電子署名の有効期間が満了していれば、移管保管所は必ず有効な証明書を用いて初期登録証明書を更新すること

(4) 移管データの伝達

○ export した移管要求メッセージをオンラインまたはオフラインの方法によりセキュリティが適用される方式により受管保管所に伝達する

(5) 電子文書情報の Import

○ 受管保管所は、移管保管所より移管要求メッセージを受け、これを解析した後受管保管所の構造に即して登録し、初期登録証明書を生成する

○ 顧客の要求により暗号化する必要のある電子文書は、暗号化の作業を行い登録

(6) 電子文書の廃棄

○ 移管プロセスにおいてエラーが発生した電子文書については、原因を把握した後、問題点を修正・補完して(3)～(6)のプロセスを再度行う

○ 電子文書に関する移管が完了した後、移管保管所は移管電子文書が確かに移管されたかを確認して対象の電子文書を廃棄する

(7) ユーザー情報

○ 移管プロセスが廃棄作業まで完了したら、移管保管所はユーザーに移管の事実を通知

○ 移管保管所は、ユーザーの要求時にユーザーに移管証明書を発給する

○ 受管保管所は、ユーザーに初期登録証明書を発給する

3.1.4 文書転送の方法

移管保管所と受管保管所は、電子文書の量と処理期間などを考慮して両保管所間の協議によりオフラインまたはオンラインでの処理の可否を決定する。

3.1.4.1 オンライン/オフラインの文書転送の方法

オンラインとオフラインの文書転送は、データを伝達する方式及び伝達のための文書転送メッセージの構造において若干の違いがあるだけで、全体的な処理フローはほぼ同一である。

伝達されるメッセージの構造において、オンライン方式は移管対象となる複数のTIPをSOAP Attachmentプロトコルにより一つのメッセージ内にembeddingする構造をとる反面、オフライン方式の場合にはPortable保存装置にTIPを独立的に保存してRequest Messageでこれに関する位置情報を保有するreferencing構造をとる（情報構造の詳細は「3.2 文書転送の情報構造」を参照）。

このようなメッセージ構造の他に最も大きな違いは、exportしたデータを伝達する方式の違いであるといえる。オフライン方式の移管は移管しようとする移管メッセージをPortable保存装置に保存し、入出力装置が封印された状態で車両などの方法により直接伝達し、オンライン方式はSOAP通信を用いて移管・受管保管所のシステム間で直接的に連携して伝達する。

3.2 文書転送情報の構造

3.2.1 概要

保管所間で電子文書の文書転送のために用いるメッセージは要求メッセージ(RequestMessage)と応答メッセージ(ResponseMessage)の二つのタイプにより構成される。それぞれのメッセージは文書転送システムが解析して処理しうるようにするため、移管保管所は本規格において定義する要求標準により要求メッセージを生成して受管保管所に送信し、受管保管所は本規格において定義する応答標準により応答メッセージを生成して移管保管所に伝達する必要がある。

3.2.2 メッセージパッケージング

電子文書の文書転送のタイプにはオンライン／オフラインの方法がある。メッセージパッケージングは文書転送のタイプによりパッケージングの方法に若干の違いがある。

3.2.2.1　オンラインメッセージパッケージング

オンライン文書転送の方法は、移管保管所において移管対象となる電子文書を文書転送規格により要求メッセージを生成した後、通信プロトコル(http, socket)を用いてオンライン上で電子文書を自動伝達し、受管保管所は要求メッセージを処理した後、応答メッセージを同様の方法で生成して移管保管所に伝達するタイプである。

オンライン文書転送メッセージのパッケージ構成は、ヘッダー情報及びボディ情報をSOAP Envelopeを用いてパッケージングした後、添付文書であるTIPをSOAP Attachment方式によりパッケージングし、最終的にはメッセージの全体情報をオンライン転送プロトコルのパッケージング方式を用いてパッケージングする。すなわち、各種ヘッダー情報・メタ情報及びTIP情報が一つのメッセージに含まれるパッケージとして構成され送受信する方式である。

3.2.2.2　オフラインメッセージパッケージング

オフライン文書転送の方法は、移管情報を移管媒体（Storage, DVD/CDなど）に収録して送受信する方法である。移管保管所は三つの移管電子文書情報である①移管総合情報ファイル②移管要求メッセージ③移管文書ファイルを生成し、生成されたメッセージを移管媒体に収録して受管保管所に伝達する。受管保管所はオフラインで伝達された移管媒体に保存された移管情報から電子文書を抽出して保管所の保存所に登録する。

3.2.2.3　SOAP パッケージング

移管・受管要求及び応答メッセージは、基本的にSOAPパッケージングによりEnvelopingされた後、メッセージの伝達方式がオンラインあるいはオフラインであるかによりSOAPパッケージングされた情報のMIMEタイプとしてMulti-MIME（オンライン）あるいはSingle-MIME（オフライン）を用いる。

文書転送メッセージのパッケージングは次の明細による。

◦ Simple Object Access Protocol (SOAP) 1.1 [SOAP]

◦ SOAP Messages with Attachments [SOAPAttach]

3.2.2.3.1　SOAP with Multi-MIME

オンライン文書転送メッセージをパッケージングする方法として、メッセージ内のContent-Type MIMEヘッダーは必ずSOAPメッセージを含むMIME本体部分のMIMEメディアタイプと同一のタイプ属性を持つ必要がある。[SOAP]明細によればSOAPメッセージのMIMEメディアタイプは“Multipart/Related" “text/xml"値を持たねばならない。

メッセージパッケージの最上位部分をルートコンテナというが、Content-Type MIMEヘッダーを持つ。ルートコンテナのContent-Type MIMEヘッダーには“Multipart/Related”及びboundary, startが常に存在する。

メッセージの本体部分をヘッダーコンテナという。ヘッダーコンテナのMimeヘッダー領域にはContent-TypeとContent-Lengthが必ず含まれる。MIME Content-TypeヘッダーはSOAP明細に準じて“text/xml"を持たねばならない。Content-Typeヘッダーは”charset"属性を含むこともある。Mime Conetent-Lengthヘッダーはヘッダーコンテナ内に含まれるSOAP Envelopeメッセージのバイト単位のサイズ情報を持つ。

ヘッダーコンテナはMIMEの本体部分として一つのSOAPメッセージが含まれる。

SOAPメッセージは SOAP HeaderとSOAP Bodyに区分される。SOAP Header領域には文書転送メッセージに関するセキュリティヘッダー(Security Header)とメッセージヘッダー(Message Header)が含まれ、SOAP Body領域には要求メッセージ(RequestMessage)と応答メッセージ(ResponseMessage)が含まれる。

メッセージの添付部分をペイロードコンテナという。ペイロードコンテナは[SOAPAttach]明細によりパッケージングされ、文書転送メッセージ内には必ず一つ以上のペイロードが含まれる。ペイロードコンテナにはTIPが含まれる。各ペイロードコンテナのTIPはSOAP Body内のTIPInfoにより参照される必要がある。参考としてTIPInfoはペイロードコンテナのContent-ID情報を持つ。

ペイロードコンテナのMimeヘッダー領域にはContent-TypeとContent-Lengthが必ず含まれる。MIME Content-TypeヘッダーはSOAP明細に準じてペイロードの文書タイプ(Media Types：RFC 2046に定義されたMedia Type)による値を(ex."text/xml", "application/octet-stream" ...)持たねばならない。Content-Typeヘッダーは”charset"属性を含むこともある。Mime Conetent-Lengthヘッダーはヘッダーコンテナ内に含まれるTIPのバイト単位のサイズ情報を持つ。

3.2.2.3.2 SOAP with Single-MIME

オフライン文書転送メッセージをパッケージングする方法として、オンラインメッセージのパッケージング方法からルートコンテナとペイロードコンテナ領域が省略される。よって、メッセージパッケージはnon-multipart形態でパッケージされる。

オフラインメッセージは一つのヘッダーコンテナにより構成され、ヘッダーコンテナのontent-Type MIMEは“text/xml"メディアタイプとcharset属性を持つ。ただし、オンラインパッケージで要求されるパラメータであるstartパラメータ・boundaryは存在しない。

ヘッダーコンテナはMIMEの本体部分として一つのSOAPメッセージが含まれ、その情報はオンラインの場合と同じである。

オフライン方式において文書転送の伝達物であるTIPは文書転送メッセージに含まれず、別途の移管媒体に保存される。このように、別途の移管媒体に保存されたTIPはSOAP Body内の

TIPInfo要素によりその位置情報が参照される。

3.2.3 移管情報パッケージ

文書転送のための電子文書情報パッケージは、電子文書の内容と電子文書に関するメタデータ、すなわち文書転送される情報の信頼性・完全性・可用性を満たすために必要な電子文書の作成・登録・履歴・内容などに関する情報と、これを移管保管所のシステム内から受管保管所のシステムに安全かつ持続的に保存及び活用管理するための情報により構成される。

3.2.3.1 文書転送情報の基本構造

TIPは電子文書を移管する保管所において生成され、受管する保管所に伝達される電子文書の概念モデルをいう。文書転送情報の基本構造はヘッダー情報(1..1)・XML領域1(1..1)・XML領域2(1..1)・ファイル原本(1..*)・初期登録証明書(1..1)により構成される。

3.2.3.1.1 パッケージヘッダー情報

パッケージヘッダー情報は、情報パッケージの全体構造をアプリケーションに指示する情報として、以下の情報により構成される。

番号	メタデータ名	タイプ	サイズ	備考
1	パッケージのバージョン	String	3byte	
2	パッケージの種類	String	3byte	"TIP"
3	XML 領域 1 のサイズ	Long	4byte	
4	XML 領域 2 のサイズ	Long	4byte	
5	添付ファイルの個数	Short	2byte	
6	添付ファイルのサイズ	Double	8byte	配列の形態を持ち、サイズは添付ファイルの個数を決定する
7	初期登録証明書のサイズ	Long	4byte	

パッケージヘッダー情報は、XML形式により記述されず、各メタデータの定義された形式により単純連結して記述される。

上記のメタデータを簡単に説明すると、

□ パッケージバージョンは情報パッケージのバージョンを記述するもので、本技術規格が改訂される場合、改訂されたバージョンを用い、本規格のバージョンは 1.0 と設定し、小数点第一位までのみ用いるものとする。(例：“1.0”)

□ パッケージの種類は提出用情報パッケージ（SIP)であるか、保管用情報パッケージ（AIP)であるか、配布用情報パッケージ（DIP)であるか、移管情報パッケージ(TIP)であるを区分する項目であり、TIP の値を用いる。

□ XML 領域 1 のサイズは TIP についてのメタデータを含む XML 領域 1 のサイズを割り当てる。

□ XML 領域 2 のサイズは TIP についてのメタデータを含む XML 領域 2 のサイズを割り当てる。

□ 添付ファイルの個数は文書転送情報パッケージに挿入されている添付ファイルの全個数であり、TIP に添付される原本文書の合計個数を割り当てる。

□ 添付ファイルのサイズは個々の添付ファイルのサイズを割り当てたもので、配列の形で規定し、

添付ファイルの個数によりサイズを決定するものとする。すなわち、添付ファイルの個数が 10 個の場合、添付ファイルのサイズは 10 個の因子を持つ。

□ 初期登録証明書のサイズは TIP に含まれている原本文書の内容につき、移管保管所が発給した初期登録証明書のサイズを割り当てる。

3.2.4 電子署名の範囲

3.2.4.1 文書転送メッセージの電子署名

文書転送メッセージに関する完全性の検証及び否認防止のため、移管保管所及び受管保管所は文書転送メッセージに電子署名を加えること。

文書転送メッセージに対する電子署名は、W3Cにおいて推奨する“XML Signature Syntax and Processing"プロトコルを遵守したWS-Securityプロトコル(WS-SecurityプロトコルV1.1）に記述された形式により生成され、電子署名情報を収録した<Signature>項目はSOAP Headerの下位項目として記述される。

署名対象は実際の送受信メッセージを含むSOAP Bodyの部分である。

そして、文書転送メッセージ全体に関する完全性の検証及び否認防止のため、ペイロードコンテナの部分に添付された各TIPのハッシュ値を生成してSOAP Bodyに挿入する必要がある。

3.2.4.2 パッケージの電子署名

TIPに対する電子署名の範囲は、XML領域1にのみ限定する。電子署名の生成方法は W3C “XML-Signature Syntaxand Processing“ (RFC3275)のenveloped signatureフォーマットを遵守して生成すること。

そしてXML領域2（すなわちSIPのXML領域）の完全性の検証のため、これに関するハッシュ値を生成した後、XML領域1のパッケージメタデータ(PackageMetadata)に挿入する必要がある。

TIPに添付される電子文書の添付ファイルに関する完全性の検証はXML領域2（すなわちSIPのXML領域）に含まれる添付ファイルのハッシュ値を用いて行い、XML領域2に関する完全性の検証は、XML領域1のパッケージメタデータに含まれるXML領域2のハッシュ値を用いて行う。

3.3 オンライン文書転送段階別の処理方法

3.3.1 概要

システムの連携によるリアルタイムな電子文書の移管である場合、通信プロトコルはSOAP Bindingをサポートし、メッセージパッケージングの構造は「3.2文書転送の情報構造」により生成される。

要求メッセージは、オンラインで伝達するが、応答（結果）メッセージが必ず同一のSOAPプロトコル（連携モジュール）により伝達される必要はない。移管要求に関する処理が終了したら受管保管所はこれに対する応答メッセージを生成した後、オフラインまたは電子メールの添付ファイルにより伝達することができる。

3.3.2　エラーの処理方法

移管保管所は移管要求メッセージを送信した後、受管保管所より受信確認に対するメッセージを受信できない、あるいは送信失敗メッセージを受信した場合、移管要求メッセージを再転送して受管保管所が移管要求メッセージを正常に受信したかを必ず確認する必要がある。

受管保管所も、移管要求に対する処理完了後、結果メッセージを受管保管所に伝達したら、必ず結果メッセージの受信の有無を確認して移管保管所がこれを正常に受信したことを確認すること。

受信した応答メッセージでFailCountが1以上である場合、移管保管所は失敗した電子文書に関する失敗コードを把握してデータエラーであるかの如何を確認した後、それぞれの失敗状況に即して措置するものとする。

3.3.3　オンラインのセキュリティ処理方法

オンラインで伝達される移管要求メッセージ及び応答メッセージにつき、移管・受管保管所は、電子署名値により相手方の保管所に関する証明及びメッセージの完全性などについての技術的検証及び以後の否認防止機能を行う必要がある。

また、移管要求メッセージ及び応答メッセージに関する機密性を保証するため、該当メッセージの機密性を保証しうる技術を適用する必要がある。

オンライン上におけるメッセージ転送のセキュリティは「ユーザーのシステムと公認電子文書保管所間の連携インターフェイス技術規格 v1.10」の「4.2.5 転送セキュリティ」と同一のセキュリティ基準を遵守する。

3.4 オフライン文書転送段階別の処理方法

3.4.1　概要

全ての保管所は、オフライン上で電子文書を移管する機能を必ず提供する必要があるが、オフラインで電子文書を移管するためには移管保管所が固有のシステム構造により管理していた電子文書及び初期登録証明書・その他管理情報をシステム及び言語独立的な情報構造（「3.2.3 文書転送要求メッセージ」）の形態でExportし、受管保管所は反対にこの情報を読み取り受管保管所内部のシステム構造に即してImportする必要がある。

3.4.2 オフライン処理段階

3.4.2.1 移管保管所の事前準備作業

(1) 基礎情報の伝達

移管保管所は、保管していた電子文書に関する移管要求が発生したら、ユーザー及び受管保管所と電子文書の文書転送に関し合意する必要がある。基本的な合意が成立した状態で、移管保管所は移管対象に関する情報及び移管方式に関し具体化のため、移管につき移管対象となる電子文書に関する総合的な情報を取り合わせ、これを受管保管所及び各ユーザーに伝達し、これに対して追加の確認を受ける。移管対象の電子文書に関する総合的な情報は、次の構造に取り合わせたうえで伝達するものとする。この情報は、移管を準備する段階において受管保管所及びユーザーに移管対象に関する基礎情報を伝達するための目的で一時的に発給されるが、この段階においてサービスが中断したわけではないため、移管対象となる電子文書・証明書に関する全体件数及び全体容量の情報は多少の差が生じることがある旨を通知する。

○受管保管所に伝達する内容

項目					データ値	備考
総合情報	移管保管所情報	保管所 ID				
		保管所名				
		住所				
		連絡先(Tel)				
		移管担当者	氏名			
			住所			
			連絡先(Tel)			
			連絡先（携帯電話）			
	移管対象使用者数					
	移管対象情報の容量					
	移管対象電子文書の総件数					
	移管作業開始予定日					
使用者別移管情報	企業 A	企業移管総合情報	移管対象使用者数			
			移管対象情報の容量			
			移管対象電子文書の総件数			
		機関使用者別情報	使用者（イ）	使用者名		
				所属部署（チーム）		
				連絡先(Tel)		
				連絡先（携帯電話）		
				電子メール		
				移管対象電子文書の総件数		
			使用者（ロ）			
	使用者 A	使用者名				
		所属機関				
		連絡先(Tel)				
		連絡先（携帯電話）				
		電子メール				
		移管対象電子文書の総件数				

	使用者 B 情報伝達媒体	...		
		タイプ		タイプ（CD, DVD, WORM Storage, SAN Storage, DAS など）
		メーカー		
		モデル名		
		全体容量		
		連携インターフェイスモジュール提供の有無		

※ DAS: Direct Attached Storage, SAN: Storage Area Network, NAS: Network Attached Storage

○ユーザー（企業ユーザー）に伝達する内容

項目				データ値	備考
総合情報	移管保管所情報	保管所 ID			
		保管所名			
		住所			
		連絡先(Tel)			
		移管担当者	氏名		
			住所		
			連絡先(Tel)		
			連絡先（携帯電話）		
	受管保管所情報	保管所 ID			
		保管所名			
		住所			
		連絡先(Tel)			
		受管担当者	氏名		
			住所		
			連絡先(Tel)		
			連絡先（携帯電話）		
	移管対象使用者数（企業内使用者情報）				
	移管対象情報の容量				
	移管対象電子文書の総件数				
	移管作業開始予定日				
使用者別移管情報	使用者 A	使用者名			
		所属機関			
		連絡先(Tel)			
		連絡先（携帯電話）			
		電子メール			
		移管対象電子文書の総件数			
	使用者 B	...			

○ユーザー（一般ユーザー）に伝達する内容

項目				データ値	備考
文書転送保管所情報	移管保管所情報	保管所 ID			
		保管所名			
		住所			
		連絡先(Tel)			
		移管担当者	氏名		
			住所		
			連絡先(Tel)		
			連絡先（携帯電話）		
	受管保管所	保管所 ID			

	情報	保管所名			
		住所			
		連絡先(Tel)			
		受管担当者	氏名		
			住所		
			連絡先(Tel)		
			連絡先（携帯電話）		
移管対象情報の容量					
移管対象電子文書の総件数					
移管作業開始予定日					

(2) 移管範囲及び方式に関する合意

オフライン移管の場合には、特別にある種のPortable保存装置を用いるのか、保存媒体への封印はどのような方式で行うのか、保存媒体の輸送手段は何を用いるのか、などを加えて合意する必要がある。

3.4.2.2 移管保管所の Export 手続

移管保管所は、移管媒体の最大保存容量を基準として移管データを分割してExportするものとする。保存媒体の容量により保管所間の電子文書の移管が一度で完了しないこともあるため、保存媒体は次の情報データが存在する。

① 移管総合情報ファイル

移管保存媒体内にある全体の情報を総合したInformationファイル

物理的に一つの移管保存媒体内にあるTIPに関するメタ情報ファイル

項目				繰り返し	Type
総合情報	移管保管所の情報			1..1	
		保管所 ID		1..1	
		保管所名		1..1	
		住所		1..1	
		連絡先(Tel)		1..1	
		移管担当者		1..1	Structure
			氏名	1..1	
			住所	1..1	
			連絡先(Tel)	1..1	
			連絡先（携帯電話）	1..1	
	移管対象使用者数（保存媒体あたり）			1..1	
	移管対象情報の容量（保存媒体あたり）			1..1	
	移管対象電子文書の総件数（保存媒体あたり）			1..1	
	移管要求日			1..1	
	要求メッセージファイルの総件数（保存媒体あたり）			1..1	
	移管要求メッセージファイル			1..∞	
		要求メッセージのファイル名		1..1	
		メッセージファイルの容量		1..1	
使用者別移管情報	企業 A			0..∞	Structure
		企業移管総合情報		1..1	
			移管対象使用者数	1..1	
			移管対象情報の容量	1..1	
			移管対象電子文書の総件数	1..1	
			機関ユーザー別の情報	0..∞	Structure

				ユーザー名	1..1	
				所属部署（チーム）	1..1	
				連絡先(Tel)	1..1	
				連絡先（携帯電話）	1..1	
				電子メール	1..1	
				移管対象電子文書の総件数	1..1	
	個人ユーザーの情報				0..∞	Structure
		ユーザー名			1..1	
		所属機関			1..1	
		連絡先(Tel)			1..1	
		連絡先（携帯電話）			1..1	
		電子メール			1..1	
		移管対象電子文書の総件数			1..1	
付加情報	情報伝達媒体				1..1	Structure
		Serial No			1..1	保存媒体の識別番号
		タイプ			1..1	タイプ（CD, DVD, WORM Storage, SAN Storage, DAS など）
		メーカー			1..1	
		モデル名			1..1	
		全体容量			1..1	
		連携インターフェイスモジュール提供の有無			1..1	

② 移管要求メッセージファイル

移管要求メッセージに対するSingle-Mime Packaging

移管要求メッセージファイルとTIPファイルは物理的に異なるファイルに分離される

一つの保存媒体に対する移管要求メッセージが二つ以上存在可能

TIPに関する情報を収める移管要求及び応答メッセージ構造は「3.2文書転送の情報構造」に記述された構造を参照

③ 移管文書ファイル

実際の電子文書を含むTIPファイルで、保存媒体に位置する

移管要求メッセージファイルに含まれず別途のファイルとして存在

移管総合情報ファイル・移管要求メッセージファイル・移管文書ファイルの位置する保存媒体間の関係を 1：n：1 として表現しうる。

移管モジュールはExport作業を行うとき、保存媒体の可用保存空間の1/10以上を残しておくため、受管保管所が受管完了後に応答メッセージを記録しうるようにする。

3.4.2.3 移管データの伝達方法

exportが完了した移管媒体は、物理的な運送手段により相手方に伝達され、移管保管所により保存媒体の入出力装置が封印された形態で伝達される。受管保管所の担当者は、移管データが収録された保存媒体の伝達を受けたら、移管保管所の封印状態を確認した後、受信確認に対する確認書を移管保管所に伝達する。

3.4.2.4　受管保管所の Import 手続

受管保管所は保存媒体を受信したら保存媒体を受管モジュールがインストールされたサーバーに接続し、情報をImportする。

Import手続は次の通りであるが、各移管要求メッセージに対する応答メッセージは移管要求メッセージ別にそれぞれ生成され、移管保管所に伝達される必要がある。

○ Import手続

移管総合情報ファイルを読み取り媒体内に記録された移管要求メッセージファイル全体の総件数を確認し、各ファイルに関する情報をもとに要求メッセージファイル単位で処理を開始する。

各要求メッセージファイルのメッセージヘッダーにある電子署名値の有効性を検証することにより、メッセージに関する証明及び完全性の検証を行う。

要求メッセージ内の電子文書単位でTIPファイルの位置情報及びハッシュ値などの属性情報を抽出する。

保存媒体からTIPファイルを抽出して要求メッセージから抽出した属性情報と比較し検証を行う。

TIPファイルに関する構造の検証・電子署名の検証・電子文書のハッシュ値検証・初期登録証明書の検証などを行い、移管対象の電子文書の完全性を確認する。

電子文書及び関連情報を受管保管所の電子文書保管構造に即して登録する。

一件の電子文書の登録が正常に完了したら、受管保管所は登録された電子文書につき初期登録証明書を発給する。

受管モジュールは処理された結果をもとに移管要求に対する応答メッセージを生成する。

生成された応答メッセージは、移管要求メッセージを収録した保存媒体に保存した後、再度受管保管所の封印手続を経て封印する。

受管保管所は封印された保存媒体と処理内訳情報を物理的な運送手段により移管保管所に再度伝達する。

3.4.3　オフラインのセキュリティ処理方法

オフラインで伝達される移管要求メッセージ及び応答メッセージにつき、移管・受管保管所は、は、電子署名値により相手方の保管所に関する証明及びメッセージの完全性などについての技術的検証及び以後の否認防止機能を行う必要がある。

また、移管要求メッセージに対する機密性を保証するため、伝達される電子文書に対する暗号化作業を行った後、保存媒体に保存する。電子文書を伝達するための保存媒体は物理的な侵害行為を防ぐためセキュリティキャビネットなどにより最大限に保護され、侵害の有無を確認しうるよう封印作業を行う必要がある。

ただし、電子文書に対する暗号化の作業はユーザーとの合意により決定し、機密性を必要とする重要な電子文書でない場合には処理時間の短縮のため省略できる。

規格沿革

バージョン	制定・改訂日	制定・改訂内訳
v1.00	2008 年 5 月 9 日	・制定
v1.10	2009 年 11 月 4 日	・添付ファイルの個数をバグのため 2byte に修正 ・誤りのある語彙を削除 ・オンライン文書転送要求メッセージにつき同期／非同期応答メッセージが可能であるとの内容を明確にした

メンバリスト

事務局

前田陽二　　財団法人　日本情報処理開発協会
木村道弘　　財団法人　日本情報処理開発協会
大崎　宏　　財団法人　日本情報処理開発協会

顧問　（五十音順）

大山永昭　　東京工業大学
辻　秀一　　東海大学

編集メンバ（五十音順）

役　割	氏　名	所　属
ビジョン委員会　委員長	保倉　　豊	グローバルフレンドシップ株式会社
基盤技術委員会　WG 主査	宮地　直人	有限会社ラング･エッジ
基盤技術委員会　WG 主査	佐藤　雅史	セコム株式会社
基盤技術委員会　委員長	宮崎　一哉	三菱電機株式会社
システム委員会　委員長	三原　　真	富士ゼロックス株式会社
ビジョン委員会　副委員長	高畑　勝人	凸版印刷株式会社
オブザーバ	合原英次郎	財団法人　日本情報処理開発協会

上記以外のメンバ

役　割	氏　名	所　属
委員	青木　正博	東芝ソリューション株式会社
委員	石原　達也	東芝ソリューション株式会社
委員	能勢健一朗	東芝ソリューション株式会社
委員	小林智恵子	東芝ソリューション株式会社
委員	高田　慎也	日本電信電話株式会社
WG 副主査	石本　英隆	日本電信電話株式会社
幹事	溝上　卓也	株式会社日立ソリューションズ
委員	鷲尾元太郎	三菱電機株式会社
委員	杉崎　　元	三菱電機株式会社
委員	小池　正通	富士ゼロックス株式会社
委員	太田　浩平	凸版印刷株式会社
委員	濱谷　卓美	凸版印刷株式会社
委員	金子　　剛	NRI セキュアテクノロジーズ株式会社
委員	森本伊知郎	NRI セキュアテクノロジーズ株式会社
有識者	西川　康男	ARMA 東京支部
有識者	佐藤　　均	東京医療保険大学

電子記録応用基盤に関する調査検討報告書 2010-クラウド時代の安心安全な電子記録管理-
電子記録応用基盤フォーラム（eRAP）

平成 23 年 5 月 20 日　第 1 刷発行
発　行：一般財団法人日本情報経済社会推進協会
〒105-0011　東京都港区芝公園 3-5-8　機械振興会館
TEL 03-3436-7500　FAX 03-3436-7570　　http://www.jipdec.or.jp/
印　刷：株式会社美行企画

ISBN978-4-89078-017-4
C3004