電子記録応用基盤に関する
調査検討報告書 2011

-電子記録マネジメントシステム要件とケースマネジメント-

電子記録応用基盤フォーラム（eRAP）

平成24年3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（JIPDEC）の電子記録応用基盤フォーラム（eRAP）が平成 23 年度に実施した、電子記録マネジメントシステムの利用状況調査、電子記録マネジメントシステム構築のための要件の検討、及び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。

平成 21 年 7 月に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電子記録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不可欠となりつつある。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平成 22 年 4 月に発足し、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･人脈を電子記録マネジメントの分野に生かし、電子記録マネジメントを推進してきた団体、企業、個人と連携をとり、また、ETSI（欧州電気通信標準化機構）や ISO（国際標準化機構）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、電子記録マネジメントシステムの発展の一助になれば幸いである。

平成 24 年 3 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

昨年の 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、書類や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（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。このサービスを利用することにより、ユーザ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 月に電子情報利活用推進部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。

本報告書は、平成 23 年度の eRAP の活動成果をまとめたものである。活動は、ビジネス検討 WG、システム検討 WG、技術検討 WG の 3 つの WG を発足して行った。本報告書では、6 つの章の構成になっている。

第 1 章と第 2 章はシステム検討 WG の活動成果であり、第 1 章では前年度検討した記録管理の 100 要件について、技術解説をつけるとともに分野ごとの要件及び成熟度対応の要件を紹介し、第 2 章では同一イベントで発生あるいは参照された書類を関連付けて管理するケースマネジメントについて紹介する。

第 3 章、第 4 章、第 5 章は技術検討 WG の成果報告であって、第 3 章では組織間での情報交換に必須なパッケージ構造の ETSI（欧州電気通信標準化機構）の方針に沿った提案を紹介し、第 4 章ではクラウド時代の認証、署名の新たな動きを紹介し、第 5 章では、ETSI 関連の活動について紹介を行う。

第 6 章はビジネス検討 WG の活動成果であり、記録管理の市場動向について文献調査の結果を踏まえ、記録管理についてのビジネスモデルをいくつか紹介する。

第１章　記録管理 100 要件の適用ガイド

1.1　記録管理に関する主要概念

記録管理の 100 要件は、MoReq2（Model Requirements for the management of electronic records）で定義されている 794 要件のうち、必須要件を中心に関連する要件を統合し、100 要件（実際には 101 要件）に集約したものである。

本章では電子文書管理システム（ERMS：Electronic Records Management System）の理解を進めるために、MoReq2 の仕様で定義される下記の 8 つの概念とその用語について解説を行う。

なお、説明文中の斜体表記の用語は、本節内で解説されていることを意味している。

- 記録と電子記録
- 信頼可能な記録
- 電子ファイル、サブファイル、ボリューム
- 分類体系
- クラス
- ERMS
- 記録のキャプチャ
- 利用者の役割

1.1.1　記録と電子記録

記録は以下から構成されると見ることができる。

- コンテント
- 構造
- コンテクスト
- 表示

コンテントは、記録のメッセージ（情報提供の内容）を伝達する、1 つまたは複数の物理的または電子的（またはその両方の）ドキュメントに存在している。ドキュメントは、将来の利用者がドキュメントとそのコンテクストを理解できるような形で保存される。このような視点からは、十分に管理された記録とは、ドキュメントのコンテントに加えて、構造に関する情報、及びコンテクストに関する情報を提供する*メタデータ*、並びに利用者への表示から構成されることが示唆される。

しかし MoReq2 では、*記録*という用語はメタデータを持たない情報提供の内容、すなわち記録を構成するドキュメントを意味するために使っている。表示は、記録のコンテント、構造、及び（*電子記録*の場合に）提示のためのソフトウェアとの組み合わせに依存している。

物理的記録の世界では、大多数の記録は紙の上にあって、ファイルに収められている。ファイ

ルは記録の 1 つまたは複数のボリュームから物理的に構成され、紙のフォルダに入れられている。手続き的管理によって、利用者が記録やファイル内でのその位置を変更することを防ぐ必要がある。

同様の概念が電子記録にも適用される。*記録*は、1 つまたは複数の電子ドキュメントから構成されている。これらの *ドキュメント*はワープロ文書、電子メール・メッセージ、表計算シート、動画や静止画、音声ファイル、その他のデジタル・オブジェクトのことがある。ドキュメントは取り込まれたとき、つまり ERMS に『*キャプチャ*』されたときに*記録*となる。キャプチャに際して*記録*は「分類」され、つまり属する*分類体系*の*クラス*に相応したコードが付加されて、ERMS による管理が可能となる。通例、*記録*はファイル内に配置されるが、そうでない場合もある（下記参照）。

保存を目的とした場合に、電子記録はしばしば複数の*コンポーネント*から構成されるという認識が必要になる。記録管理の『*ファイル*』と混同する可能性をなくすため、MoReq2 では IT 用語の『ファイル』を避けて『*コンポーネント*』という用語を使用している点に注意が必要である。

各*コンポーネント*はコンピュータのオペレーティング・システムが管理するオブジェクトであり、異なった形式のこともある。しかし、記録を構成するためには全部がそろって必要になる。また、すべての記録が複数の*コンポーネント*を持つわけではない。たとえば、多くのワープロ文書は 1 つの*コンポーネント*からだけ構成されている。複数の*コンポーネント*を持つ記録としては、テキスト、グラフィック、スタイルシートを伴ったウェブページの例がある。ウェブページが 1 つの HTML コンポーネント、多数の JPEG 画像コンポーネント、少数の CSS（Cascading Style Sheet）コンポーネントを含んでいることは珍しくない。

記録に必要不可欠な特性は、その情報提供内容が固定されていることである。その帰結として、*コンポーネント*間の関係を損なういかなる行為も、電子記録上で行うことは許されない。言い換えると、電子記録上で行うすべての行為は、その全*コンポーネント*間の正しい関係性を保つものでなければならない。そのため、たとえばどの記録でもそれを移動したりコピーしたりする場合には、全*コンポーネント*及びそれらの全関係性を保つ方法で移動またはコピーしなければならない。

1.1.2 信頼可能な記録

ISO 15489 では、「信頼可能な記録」とは以下のような特性を持った記録として説明されている。

- 真正性
- 信頼性
- 完全性
- 利用可能性

ISO 15489が説明するように、すべての記録管理システムは、それに保存された記録が信頼可能であることの保証を目的とする必要がある。

要約すると、信頼可能な記録は次の機能を持たなければならない。

- それが主張する内容であることを証明できる
- それを作成あるいは送信したと主張する人物によって作成あるいは送信されたことを証明できる
- 主張される時間に作成あるいは送信されたことを証明できる
- それが証明しようとする取引、行為、事実の十分で正確な表現として、その内容が信頼可能なために依存できる
- 完全であり改ざんされていない
- 検索、取り出し、表示、解釈が可能である

MoReq2 が示す要件は、MoReq2 準拠 ERMS に保存された記録が信頼可能であることを保証するように設計されている。しかし、これらの要件に適合することだけでは十分でなく、企業ポリシの存在と、それへの準拠も必要になる。

1.1.3 電子ファイル、サブファイル、ボリューム

紙の記録は一般に紙のフォルダに収容することにより、物理的なファイルに蓄積される。このような紙ファイルが、ある構造、あるいは*分類体系*へと収集される。ERMS では、あたかも電子的なファイルに蓄積し電子的なフォルダに収容するようにして、電子記録の管理を行うことができる。厳密には、電子的なファイル及びフォルダは実際の存在である必要はない。これらは、実際には何も「収容」しないという意味で仮想であり、事実上は記録に付与されたメタデータ要素によって構成されている。更に、多くの場合に電子システムにおいて、ファイルとフォルダを実際に区別する必要もない。しかし一般に、このような詳細は ERMS の利用者には見えない。ERMS のアプリケーション・ソフトウェアによって、利用者は、論理的にファイルに割り当てられたドキュメントを物理的に収容するかのようにフォルダを見て、管理することができる。このような利用者中心の視点が、MoReq2 では推進されている。従って、理解しやすいように MoReq2 では、記録を「収容している」ものとして電子ファイルを説明している。しかし、MoReq2 は電子ファイル管理の機能的要件を提供するものの、電子ファイルの概念の実装方法を規定するものではない。

状況によって、*ファイル*を*サブファイル*に分割するのが有用なことがある。*ファイル*の*サブファイル*への分割は「知的な」分割であり、（一般に）*記録*をどの*サブファイル*へ保存するべきか決めるための、人間による入力が必要になる。*サブファイル*は、ほとんどの場合に*ケース処理*の環境で使用される。たとえば土地販売に関するファイルで、販売にかかわるそれぞれのビジネス活動（広告、契約、弁護士との交渉など）に対してサブファイルを持つ。

従って*サブファイル*は、コンテントのタイプによる*ファイル*の分割である。その結果、*ファイル*内の一連の記録に対して異なった保存・廃棄のスケジュールを適用可能なようにして、*サブファイル*を使用できる。

*サブファイル*を使用するかどうかにかかわらず、*ファイル*を所定の慣例に従ってファイル・ボリュームへと「機械的に」分割する場合もある。この「機械的に」という語は、「ファイルの知的な内容ではなくサイズ、収容されている記録の数、時間間隔などにもとづいて」、それらの慣例の単純な順守を示唆している。このような方法は、処理しやすいサイズや重さに制限するという、紙ファイルの場合に起因している。電子ファイルの場合でも、評価や転送などの取り扱いを目的に処理しやすい大きさに制限するなど、この方法を継続できることがある。特に、長期間にわたってオープンされる場合や、収容する記録数が多くなる場合があるようなファイル管理では、この方法が適切になる。

ファイルとファイル・ボリュームとの区別は明白だが、その意味合いはそれほど明確ではない。これは、ファイルのボリュームへの分割を選択する意味合いは、実装のニーズによって異なるからである。

この相違は以下のように発生する。

- ファイルによっては一定期間のうちにクローズされるため、管理目的に使用される単位はファイルとなる（いくつかのボリュームがファイルを構成していても）。たとえば特定の小規模な調達、1プロジェクトのためのファイルなど
- ファイルによっては無期限の（あるいはほとんど無期限の）ライフスパンを持つため、管理目的に使用される単位はボリュームとなる。たとえば、地理的領域に関する記録のファイル、ポリシなど時間が問題にならない主題を扱うファイル、毎年新たなボリュームが開始される送り状ファイルなど

以下にクラス、ファイル、サブファイル、ボリューム、記録、コンポーネントの関係を図示する。

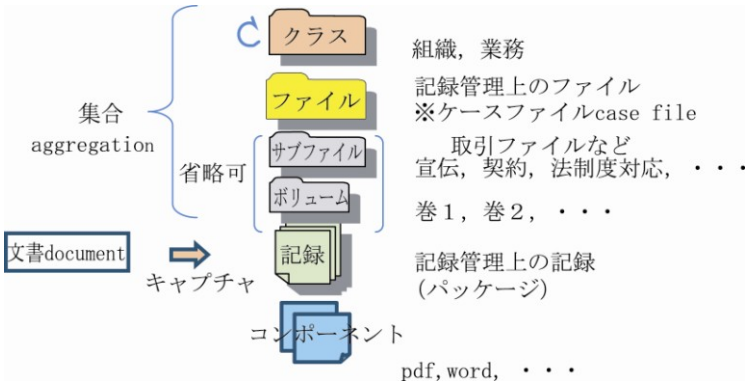


図 1-1　分類体系とファイル構成

1.1.4　分類体系

記録管理はファイルを構造的な方法で収集するが、優れたプラクティスは、この構造がビジネス機能を反映すべきことを示唆している。このような収集の表現が「分類体系」と呼ばれる。分類体系は一般に階層構造を持っており、MoReq2 では、この階層ビューに焦点を当てている。その他のアプローチは MoReq2 のスコープ外であり、階層的配置は MoReq2 準拠のための必須条件となっている。

実際には記録の集合であるにもかかわらず、*ファイル*が存在するかのように見えるのと同様に、分類体系階層の上位レベルも、*ファイル*や下位レベルの集合であるにもかかわらず、存在するかのように見えている。MoReq2 ではファイルの場合と同様、実装方法を規定することなしに階層のための要件を述べている。

*ファイル*は、階層構造のどのレベルでも存在できる。これを、仮想的な分類体系を表す「図 1-2　分類体系（Classification)」で示している。ここでは*クラス*と、最下位レベルの*クラス*に割り当てられた*ファイル*が示されている。この仮想体系は、実際の分類体系となるものよりも、かなりシンプルなものである。

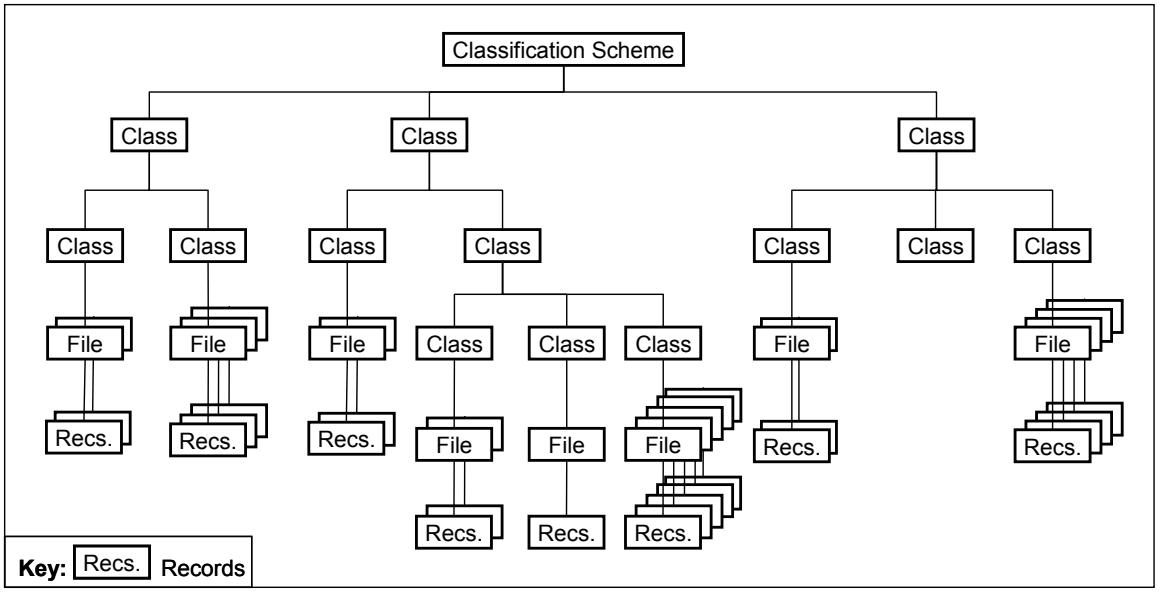


図 1-2　分類体系（Classification）

注：この図はレベル、ファイル、記録の考えられる選択された関係性を示すもので、可能なすべてのレベルや配置を表すものではない。

1.1.5　クラス

MoReq2 が使用する「クラス」は、IT 用語のオブジェクト指向のクラスを指すものではない。分類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言う。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。

視覚的に、階層構造におけるクラスは木の枝に相当している（木構造）。従って、木構造の、あるノードの下位に複数のノードを持つように、クラスも他のクラスを含むことがある。上記の例を続けると、「図 1-3　クラスの説明」の影付きボックスと太い線がクラスの例を示している。一番内側の点線内が最下層のクラスで、中心の点線内の最上位のクラスが中間ノード以下を示すクラス、一番外側の点線内の最上位のクラスが内側の各クラスを包含するクラスとなる。

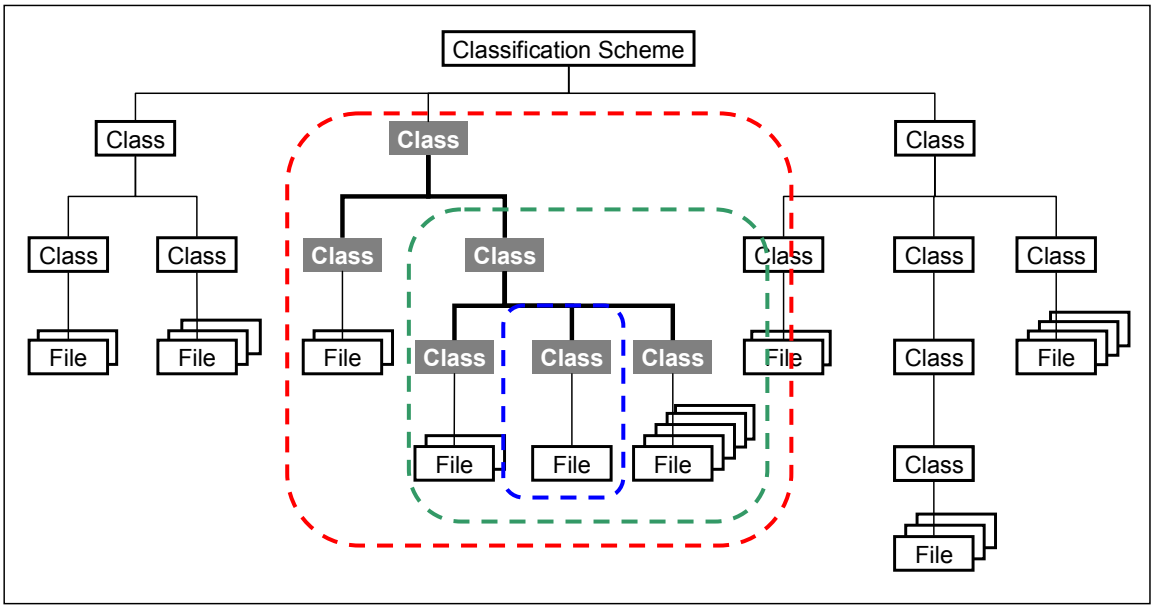


図 1-3　クラスの説明

MoReq2 では、あるクラスに割り当てられたすべてのファイル、記録などを意味するのにも、「クラス」という用語を使用している。これは、「ボトル」という語によって容器と、液体で満たされた容器の両方を表すのに似ている。この二重使用は意図的なもので、用語の適切な解釈はコンテクストから常に明らかである。

MoReq2 は、エンティティ間の関係を表すために「子供」と「親」という用語を使用している。あるエンティティの「子供」とは、階層中でその下に位置するエンティティである（言い換えれば子孫のエンティティ）。あるエンティティの「親」とは、階層中でその上に位置するエンティティになる。従って、たとえばクラスの子供が他のクラス、ファイル、あるいは(まれな場合に)記録のことがある。

MoReq2 では記録がファイルであることなしに、クラスに割り当てられる、あるいはクラスに直接に格納されることが可能である。これは MoReq2 の本文が説明するように、比較的まれな状況を対象にしている。

1.1.6 電子記録管理システム（ERMS：Electronic Records Management System）

ERMS はおもに電子記録を管理するためのアプリケーションだが、物理的記録の管理にも使用できる。

ERMS は、電子文書管理システム（EDMS：Electronic Document Management System）あるいはビジネス・アプリケーションと密接に統合されていることも多い。技術的には、ERMS は記録を管理し、EDMS はドキュメント（記録ではない）の管理を行う。しかし、特に日常的業務の支援においては、これらの機能性を分離することは難しい。

1.1.7 記録のキャプチャ

MoReq2 では、「記録のキャプチャ」は、ある記録をある ERMS へ入れることに関係したすべてのプロセスを意味する。つまり、登録、分類、メタデータの付与、ソース・ドキュメントの内容の凍結などを指す。より一般には、この用語は ERMS への入力や、メタデータ値など他の情報を保存することにも使われる。

業務過程で作成あるいは受領されたドキュメントは取り込まれたとき、つまり ERMS に「キャプチャ」されたときに記録となる。キャプチャに際して記録は「分類」され、つまり属する分類体系のクラスに相応したコードが付加されて、ERMS による管理が可能となる。また、ユニークな識別子も付与される。

多くの場合、キャプチャされたドキュメントは、ワークフローでよく起こるように業務プロセスと結び付くことによって記録となる。たとえばインボイスが発生すると、記録が自動的にキャプチャされる必要がある。または、正式に業務のプロセスに関与しないものでも、業務関連のドキュメントはすべて記録にするという方針が存在することもあるだろう。一方で、キャプチャの手順は利用者が選択的に開始するという場合もある。どのドキュメントを記録システムにキャプチャするかの判断は、規制環境、業務・説明責任の要件、記録をキャプチャしないことの危険性などの分析にもとづく必要がある。たとえば、政策問題を取扱う組織でのメモがあるとする。その組織では、重要とみなされるメモだけを記録とするように決めているだろう（会議の段取りに関するなど、重要でないメモは記録とならない）。ある状況では、下書きは重要とみなされ記録になることもあるし、逆に記録にはならない状況もあるだろう。MoReq2 は、これらどのような状況にも対応することを目的としている。言い換えると、MoReq2 は単に特殊利用のためや、アーキビストや監理者による専門的利用のための記録管理システムではなく、汎用的なオフィス・システムについて説明している。

1.1.8 利用者と監理者の役割

MoReq2 が用いるコンセプトでは、ERMS を使って仕事をする正式な許可を得た人間は、誰でも「利用者」を意味している。ERMS へのログインが認められている者は誰でも利用者であ

る。

しかし、ERMS の利用者の中には、純粋な「利用者」と、記録を監督・管理する役目をもつ「利用者[1]」、システムのメンテナンスを行う「利用者[2]」が存在する。そのため、MoReq2 は多くの要件を規定する場合に「役割（ロール）」という概念を使用している。

MoReq2 では、純粋な利用者の役割を「User Roles」、記録の管理、システムの管理を行う役割を「Administrative Roles」としている。そこで本書では前者を「利用者役割」、後者を「監理者役割」と呼ぶ。

1.1.9 監理者役割

監理者役割は、記録の管理そのものに関連した活動を行う。その関心は、記録の内容や業務のコンテクストよりも、エンティティとしての記録の管理である。監理者役割は ERMS のハードウェア、ソフトウェア、ストレージの管理も行い、バックアップの確認、ERMS の性能の管理も行う。

一方、組織によって、ERMS の実装形態は異なる。たとえば、小さな組織が実装する ERMS では監理者が１名のこともあるし、大きな組織では、それぞれが異なるアクセス許可を持った複数の監理者職を必要とすることもある。

多くの組織がこれらの役割に対し複数の人間を割り当てるだろうし、多くの組織で追加的な役割も規定されるだろう。

このような理由から、この汎用的仕様で具体的なアクセス・プロファイルを特定することは有用ではない。そのため、MoReq2 では「役割」という概念を用いている。

しかし要約すれば、MoReq2 が規定する「役割」は利用者プロファイルのようなものである。これは職や地位ではなく、何人かの利用者によって共有された、責任と職務上許可の集合と言える。

大きな組織では、監理者は、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いくつかの役割に割り当てられる。MoReq2 の“監理者”はいくつかの機能を有し、複数の役割に振り分けることができるようになっている。

複数の役割を有する“監理者”については、各要件上の役割及びその組織上の位置付けを明確にしておくことが必要である。

このため、本報告書においては“監理者”をシステムそのものの監理者とシステムに登録された内容の管理者の二つの役割を有しているものとした。

100 要件の“監理者”の役割、機能、組織上の位置付け、該当する要件は表 1-1 の通りである。

[1] 記録の管理者
[2] データのバックアップやリストア等を行う、日本で一般に言われているシステム管理者

表 1-1　監理者の役割

MoReq2の用語	役割	機能	組織上の位置付け	該当要件№
監理者	システム監理者	システムそのものの監理者	情報システム部門	4、26、79、80、82、84、86、87、88
	コンテンツ監理者	システムに登録されているコンテンツの管理者	各部門の責任者	2、10、11、15、20、27、29、34、35、37、52、58、60、81、90、91

1.1.10　利用者役割

利用者役割は、監理者役割と違って記録を扱うときにオフィスワーカーや調査員が必要とするような設備にアクセスする。これにはドキュメントの追加、記録の検索や取り出しなどが含まれる。利用者役割の関心は、記録の管理よりも、主にその内容である。言い換えれば、利用者役割は、記録が証拠を与えるような業務のプロセスに関心を持っている。

1.2　主要用語に関する追加解説

MoReq2 の仕様で定義される用語は記録管理分野で一般に使用される用法と一致しているが、一部に MoReq2 に特有な用法もあるため、概念説明に加えいくつかの用語について補足説明を行う。

1.2.1　メタデータ（metadata）

記録管理における記録のコンテクスト、コンテント、構造、更に時間経過におけるそれらの管理を説明するデータ（原典： ISO 15489）。

1.2.2　記録（record）

法的義務に従って、あるいは業務取引において、組織団体や個人が証拠及び情報として作成、受領、保持する情報（原典： ISO 15489）。

国固有のローカルな定義の適用もある。

記録は１つまたは複数の *ドキュメント*を組み込んでいることがあり（たとえば１ドキュメントが添付情報を持つ）、また、メディアやフォーマットにかかわらない。結果として、記録は１つまたは複数のコンポーネントから構成されることがある。ドキュメントの *コンテント*に加えて、記録はコンテクスト情報と、適切な場合に構造情報（たとえば記録のコンポーネントを説明する情報）も含む必要がある。記録の重要な特徴は、その変更が可能でないことである。

ERMS において、電子記録と物理記録の両方の管理が可能。

1.2.3 電子記録（electronic record）

電子形式の記録。

アプリケーション・ソフトウェアにより作成された結果、あるいはスキャニングなどのデジタル化の結果として電子形式をとることがある。

1.2.4 文書／ドキュメント（document）

1 ユニットとしての取り扱いが可能な、記録された情報やオブジェクト（原典：ISO 15489）。

ドキュメントは紙、マイクロフォーム、磁気メディア、その他の電子メディアの形をとることがある。またテキスト、データ、画像、音声、動画、その他の情報形式の組み合わせのことがある。1 つのドキュメントは、1 つまたは複数の*コンポーネント*により構成されることがある。

ドキュメントは、いくつかの重要な点で「*記録*」とは異なっている。MoReq2 では、記録としてキャプチャされていない、つまり分類、登録、変更防止ロックなどがされていない情報を意味するときに、ドキュメントという用語を使用する。定義中の「記録された」という語は、「*記録*」の特性を示唆するものではない。しかし、ドキュメントによっては「*記録*」となるものもある。

備考：文書と記録

要件 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」とあり、“文書”と“記録”を明確に分け、同一の体系で管理する場合はその区別を明示することが求められている。

しかし、記録管理の国際標準である ISO 15489 を JIS 化した JIS X0902-1 の用語の定義中に参考として「記録管理（records management）の管理対象は、記録（records）であるが、わが国で一般に使われている文書管理は、記録（records）のほかに文書（documents）をも管理対象としており、その範囲が広い。」と記述しているように、わが国では管理対象として“文書”、“記録”を明確に区別せず、“文書管理”の中で定義上の“文書”、“記録”を含めて管理する場合が多い。このため、MoReq2 の要件にあるような“文書”と“記録”の明確な区分及びその区分に応じた管理は、現状ではなじみにくいものであると考えている。

平成 23 年度の報告書[1] の“文書”、“記録”の定義を再掲する。

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。

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、及び適用可能な場合、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。

なお、JISX0902-1 では“文書”、“記録”を以下のように定義している。

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

記録（records）：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

1.2.5 コンポーネント（component）

この用語は標準的用法ではなく、MoReq2 固有の用法である。

コンポーネントは単独で、あるいは他のビット・ストリームとともに*記録*または*ドキュメント*を構成する、個別のビット・ストリームである。

「個別のビット・ストリーム」とは、IT 分野で通常呼ばれている「ファイル」を示している。ここでは、記録管理における「*ファイル*」との混同を避けるために、そのような「ファイル」という語を使用していない。概念として重要なのは、「コンポーネント」は別個の処理や管理が可能であるにもかかわらず、ある記録の内容の不可分な部分を構成している点である。

以下にコンポーネントの例を示す。

- ウェブページを構成する HTML 文書と JPEG 画像
- 記録が、表計算シートへの埋め込みリンク（ハイパーリンク）を持ったワープロ文書によって構成される場合に、そのワープロ文書及び表計算シート

コンポーネントは明確に区別が可能、つまり互いが別個である必要がある。もし、表計算シートへの埋め込みリンクでなくワープロ文書の中に表計算シートが埋め込まれていれば、その場合に表計算シートはコンポーネントとはみなさない。表計算シートが埋め込まれたワープロ文書が、1 つのコンポーネントから構成された 1 つの記録となる。

また添付情報のある電子メール・メッセージは、その保存形式によって 1 つのコンポーネント、複数のコンポーネント、または複数の記録とみなされる。

以下に添付情報とコンポーネントの関係例を示す

- メッセージが、その本文及び全添付情報を含む形式で保存されていれば、それらは 1 つのコンポーネントとなる
- 添付情報が電子メール・メッセージの本文とは別に保存され、その内部でリンクされている場合には、各添付物及びメッセージの本文がコンポーネントとなる
- 添付情報が電子メール・メッセージの本文とは別に保存され、その内部でリンクされていない場合には、各添付情報及びメッセージの本文は別個の記録となる。適切なプラクティスとして、これらの記録は互いに手動でリンクする必要があるだろう

1.2.6 ファイル（file）

同じ主題や行為、トランザクションに関係するためにグループ化された、「*記録*」の組織化ユニット（原典：ISAD(G)からの改変・短縮）。

これはファイルという語の記録管理上の用法である。IT 分野での通常の用法とは異なる。IT 分野でのファイルは MoReq2 においては、用語「*コンポーネント*」を使用する。

1.2.7 サブファイル（sub-file）

*ファイル*の知的認識における下位区分。

サブファイルは、ケース・ファイル管理環境で使用されることが多い。一般に各サブファイルには名前が付けられ、それぞれが「送り状」、「査定」、「通信」など、ケースの 1 事例における特定種類の記録（1 つまたは複数）の保存に使用される。しかしサブファイルは、同じ方法で、非ケース・ファイルの環境でも使用されることがある。

1.2.8 ケース・ファイル（case file）

本用語は MoReq2 の理解のために定義された語であり、ERMS で管理される他のファイルとケース・ファイルの違いについて、広く一般に認められた定義はない。

MoReq2 でケース・ファイルは構造化された、または部分的に構造化された方法で完全に、または部分的に実行される 1 つまたは複数の具体的なプロセスや行為の結果としてのトランザクションに関係したファイルであると定義される。

なお、ケース・ファイル内の記録は構造化されている場合もされていない場合もある。

次にケース・ファイルの主な特徴であるが、少なくとも部分的に構造化され、繰り返し可能なプロセスの結果として作成されることが挙げられる。

以下にケース・ファイルの例を挙げる。

- 許可の申請
- 所定のサービスに関する問い合わせ
- 事件の調査
- 規制上の監視

またケース・ファイルは典型的に、以下の特徴を持つ場合が多い。

- その内容のための予見的構造を持つ
- 数が多い
- 構造化されている、または部分的に構造化されている
- 既知で規定のプロセスにおいて使用され、管理されている
- 法律や規制にもとづき、特定期間の保管が必要
- 管理者の承認を得ることなしに、専門職、エンドユーザ、データ処理システムなどによるオープンとクローズが可能

1.2.9 ボリューム（volume）

*サブファイル*の下位区分。

この下位区分は、管理のために大き過ぎない単位を作成することによって、サブファイル内容の管理を容易にするために作成される。この下位区分は知的というより、機械的なものである（たとえば記録の数、数の範囲、時間間隔など）。

1.3 記録管理の成熟度

(1) 成熟度モデル

組織の記録管理が進まない理由の一つとして、組織の記録管理の現在の状態や目指すべき記録管理の状態が見えない、認識できないということがある。状態が見えることにより、どこに問題があるか、目標とする状態とのギャップはどこにあり、このギャップをうめるための具体的な対応を組織で計画し、進めていくことが可能となる。

このように、組織の現在の状態を見える化するための評価軸の設定や、PDCA サイクルを使った改善の仕組みを行うマネジメント手法は、他の分野で多くの試みが行われ、成功した事例が多くみられた。例えば、CMMI や JRMS（JIPDEC が作成したリスクマネジメントシステム評価システム）[2] などである。

特に、JRMS は JIPDEC が ISO 31000 のリスクマネジメントの規格を参考に、組織のリスクマネジメントの評価を行うために、組織のリスクマネジメントの状態を表す成熟度モデルを作成し、組織のリスクマネジメント評価に貢献した実績がある。

そこで、JRMS の成熟度モデルを参考に、組織の記録管理の成熟度を作成し、組織の記録管理の状態の見える化を実施することとした。

ただし、今年度は、成熟度モデルの作成のみを行うこととし、この成熟度モデルを使った組織の記録管理の評価のための評価軸等の作成は行わないこととする。

表 1-2 に、eRAP が提案する記録管理の成熟度モデルを示す。

表 1-2 成熟度モデル

成熟度の評価レベル		定義	摘要例
0	未認識・未対応	記録管理の対応が個人、組織とも行われていない	・記録を管理するという認識もなく、記録管理の対応方法について知識を持っている要員もいない ・紙の記録を中心に管理している ・記録管理に対する認識や対応は個人に依存している ・紙の記録を中心に管理している
1	個人ごとによる対応	記録管理の対応が個人ごとによる対応に留まっている	・記録管理に対する認識や対応は個人に依存している

成熟度の評価レベル		定義	摘要例
2	部門ごとによる対応	記録管理の対応が部門ごとに統一されているが、全組織で統一した対応は行われていない	・記録管理に対して、支店等の部門ごとに対応が定められ、文書化もされている
3	全組織による対応	記録管理の対応が全組織で標準化され、組織的な承認を得ている	・記録管理に対して、全組織としての対応が定められ、文書化もされており、手続き等も定められている
4	全組織による管理された対応	全組織での標準化された記録管理の対応に加え、記録管理が基準通り実施されているかを管理している	・記録管理のばらつきやぶれが、基準からの逸脱として把握されている
5	全組織による最適化された対応	全組織による管理された対応に加え、記録管理を組織として継続的に改善している	・全組織による最適化された対応

(2) 100 要件と成熟度モデルの関係

記録管理の 100 要件の各項目について、文書管理の成熟度モデルの各レベルに到達するための要件という視点で評価を実施した。

評価レベルは成熟度モデルのレベル 3～5 の 3 段階とした。各レベルとの関係は薄いが、記録管理システムが有しておくと望ましい機能については“オプション”と表記した。

なお、「主要 100 要件」は、単体の記録管理システムですべてを満たしている必要はなく、他システムとの連携によって要件を満たすことができる場合も、要件に適合していると考えてよい。

ただし、要件を満たしていないことをもって、記録管理システムとして不十分であるといことではないことはお断りしておく。

1.4 業務プロセス及び文書の類型毎の要件

「業務プロセス」は業務の流れを類型として捉えたものであり、今回は、表 1-3 の「商品開発プロセス」、「研究開発プロセス」、「日常処理プロセス」を設定した。

「文書モデル」は業務上作成される文書を類型化したものであり、今回は「企業統治モデル」、「内部統制モデル」、「マネジメントシステムモデル」、「営業情報管理モデル」、「技術継承モデル」、「知的財産保護モデル」、「物品製造モデル」、「設備情報管理モデル」、「建造物維持管理モデル」の 9 種を設定した。文書モデルの特徴及び代表的な文書については表 1-4 に示す。

それぞれの類型ごとに「主要 100 要件」の大分類単位で「必要」、「あった方が望ましい」、「必要性が低い」、の 3 レベルで評価した。記録管理の主要 100 要件の評価について表 1-5 に示す。

本検討の目的は、①記録管理システムの要件仕様である「主要 100 要件」に対し、文書管理の成熟度モデルのレベルで評価することによって、そのレベルに見合った記録管理システムが満たすべき要件を示すこと、②記録管理（レコードマネジメント）の視点から、上述した業務プロセスの類型または文書モデルに対し、記録管理システムにどのような要件が重要視されるかを示すことである。

本検討が記録管理システムを導入する際の要求仕様作成の目安となり、利用しやすい記録管理システムの構築の一助となると幸いである。

表 1-3　業務プロセスの類型

カテゴリ	説明（キーワード）	該当する文書モデル
商品開発プロセス	商品の企画、研究及び決裁に係る一連の文書 知的財産に関する文書が多い	マネジメントシステムモデル、知的財産保護モデル
研究開発プロセス	商品の企画、研究及び決裁に係る一連の文書 研究結果の蓄積＝長期保存が必要であり、その継承が求められる文書が多い	マネジメントシステムモデル、知的財産保護モデル、技術継承モデル
日常処理プロセス	毎日定例的に処理が必要なプロセス。会計処理など 適切な処理が行われたかどうかエビデンスとなる文書が多い	内部統制モデル、営業情報管理モデル

表 1-4　文書の類型

カテゴリ	文書類型	説明	文書内容
企業経営（外部）	企業統治モデル	組織の外部に対し、法的責任、社会的責任を果たしていることを担保するために重要な記録である 記録管理上、特にシステム登録後に変更、改ざんされていないことが重要になる	規定、マニュアル、株主総会議事録、取締役会議事録、取締役の職務執行に関わる記録、広報
	内部統制モデル	組織内部の会計処理が適正に行われていることを担保するために重要な記録である	帳簿、契約書、会計データ、納品書、発注書、請書

カテゴリ	文書類型	説明	文書内容
		記録管理上、特に記録がもれなく保存されていること、システム登録後に変更、改ざんされていないことが重要になる記録管理システムにはスキャニングデータとして登録されることが多いことが特徴である	
企業経営（内部）	マネジメントシステムモデル	組織の外部に対し、組織内のリスク対応や品質を保証するためのマネジメントシステムで必要かつ重要な記録である 記録管理上、作成・承認の時間などの証明に加えて、万が一の場合に即検索できることも重要である	品質計画書、作業報告書、実施報告書、業務手順書、業務分類、各種作成したリスト類
	営業情報管理モデル	現在進行している営業案件はもとより、過去の営業案件の蓄積や、その際に作成・提出したドキュメントの管理も重要である	営業日報、交渉議事録、連絡・対応記録、顧客要求事項の記録
	技術継承モデル	営業情報、技術検討経緯、設計記録など企業活動で蓄積された“情報資産”の集約と活用は、企業にとっての財産に繋がる	議事録、検討メモ、提案資料、入手資料、重要情報のURLなど
訴訟対応	知的財産保護モデル	知財保護のために、蓄えられた情報資産に対してのアクセス権、秘密保持の設定が重要になる	申請書、研究開発に発生した際のメモ・文書やラボノート
	物品製造モデル	品質保証（消費者保護）のために、製品設計・製造に関わる記録について、適切な保管管理が重要である。特に、製品寿命が長期間にわたるもの、取扱い不備による人命事故に繋がるものでは重要な記録となる	設計企画書、設計図、試験記録、販売計画、発送記録、クレームなど
維持管理	設備情報管理モデル	設備の安全運転と安定稼動のためには設計から設置・施行、性能試験、保守点検などのメンテナンスが不可欠である。その際の記録と保修工事をする際のもとデータとして、設備情報は重要な記録である また、万が一の事故、災害時には、復旧	設備設計書、設置計画書、取扱説明書、設計図、配置図、不具合記録、点検記録、監督官庁への提出書類など

カテゴリ	文書類型	説明	文書内容
		対策の初動に大きく影響するので、最新版の管理は必要不可欠となる	
	建造物維持管理モデル	施設の安全と予防保全のためには設計から部品製造、建設施行、耐用試験、保守点検などのメンテナンスが不可欠である。その際の記録と予防計画をする際のもとデータとして、施設情報は重要な記録である また、万が一の事故、災害時には、復旧対策の初動に大きく影響するので、施工当初の設計図の長期保存が重要になる	施設設計書、工事計画書、取扱説明書、設計図、機械配置図、不具合記録、点検記録監督官庁への提出書類など

表 2-5　記録管理主要 100 要件

成熟度モデルのレベル　3：全組織による対応、4：全組織による管理された対応、5：全組織による最適化された対応、
Op.：成熟度モデル各レベルとの関係は薄いが、記録管理システムが有しておくと望ましい機能
◎：絶対に必要、○：必要(有った方が望ましいを含む)、×：必要性が低い

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
(a)	**分類体系とファイル構成**															
	分類体系の設定				◎	◎	○	○	○	○	◎	◎	○	○	○	○
	1	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 ②※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	①:3、②:Op.	共通用語（概念）での階層管理のためには必要不可欠												
	2	分類体系の管理は監理者だけに許されること	3	コンテンツ管理者のみの変更権限として必要												
	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	3	システム更新など、システムの置き換え時に必要												
	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	3	同上												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
		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	Op.	標準フォーマットは別途定義												
	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	3	№4、5 と同様の意味												
	7	複数の分類体系が定義でき同時に使えること	4	全社で管理する場合は複数の分類体系が必要												
	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	3	ファイルについては、必要と考える。クラスについては、詳細な定義化が必要と考える（たとえば、暫定 PJ などの場合は利用可能な期間の定めが必要など）	○	○	○	○	○	○	○	○	○	○	○	○

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	3	－												
	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	3	あると非常に便利な要件である。時系列でファイルを保持するためには有効な要件である												
	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	Op.	ファイルデータの整合性を保つためには、コンテンツ管理者のアクセス権も必要	○	○	○	○	○	○	○	○	○	○	○	○
	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	3	あると非常に便利な要件。時系列でファイルを保持するためには有効な要件												
	分類体系の保守															
	13	クラスの結合や分割ができること	3	コンテンツ管理者の権限として必要	○	○	○	○	○	○	◎	◎	○	○	○	○

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	3	変更前の参照と同時に、変更も可能とする必要がある。特に、組織分割や法律・社内規定の変更などの場合は、一括変更ではなく、個別判断を要することが多い。												
	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	3	コンテンツ管理者の権限として必要												
	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	3	ファイル情報の履歴管理として必要												
	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	Op.	ただし、セキュリティ制約との調整が必要（本来閲覧権限が無い個人情報への参照作成をしてはならない）												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	Op.	時系列的に同名称のファイルの保持が必要な場合もある（第 1 回申請、第 2 回申請など）												
	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	3	セキュリティ制約との調整が必要（本来閲覧権限が無い個人情報への参照をしてはならない）												
	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	4	コンテンツ管理者の要件として、必要												
(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	3	全組織で標準化した記録管理のためには必須要件	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	4	ログ	○	○	○	◎	○	○	○	○	◎	○	○	○
	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	4	ログ												
	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	4	ログ												
	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	3	大規模システムの場合、利用不可時間が無いように考慮することが必要	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎
	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	3	全組織で標準化した記録管理のためには必須要件												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	Op.	組織として、事前に重要情報としての定義化が必要												
	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	Op.	№25 と同様の配慮が必要												
(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	4	全組織で標準化された記録管理を管理・監査するためには必須要件												
	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	4	同上												
	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	4	同上												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	3	必須要件												
	33	保持及び処分計画は保有期間及びトリガー事象または処分日、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、レビューに提出、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	4	上位については、参照機能の方が有効												
	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。レビューが必要なときは監理者に自動的に通知すること	Op.	データ管理者の要件として、必要												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	35	監理者はレビューを委任することができること	Op.	コンテンツ管理者要件としては必要だが、初期判断はユーザが行うことが一般的（ファイルごとの個別対応が必要）												
	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	3	コンテンツ管理者は上位権限者にのみ、委譲できる												
	処分のレビュー															
	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	4	処分期間に入ることを管理者に知らせる												
	38	メタデータと計画情報によりレビュー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、更なるレビュー、永久保存のマーク付けをできること	5	同じ記録のレンディション間のリンクを維持しながらの管理（難易度大）	○	○	○	○	○	○	○	○	○	○	○	○

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
		※自動的にレビュー日のログが採れること														
	39	レビュー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	4	全組織で標準化された記録管理を管理・監査するためには必須要件												
	40	レビュー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	4	同上												
	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	3	電磁的記録を移管する場合は必要												
	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	5	基幹システムとの連携を図ることが前提の場合、ファイル保管のシステムが複数存在することのリスク検証が必要	○	○	○	◎	◎	○	○	○	○	◎	○	○

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	3	文書管理機能を有するシステムを複数保持することについてのリスク検討が必要。次期システムへの移行時等には必要な要件（№3、4、5と関連）												
	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	3	文書管理システム単独の要件ではない												
	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	5	原則。完全な記録のエクスポート及び移管に対するリスク想定が必要。データ管理者以上の権限者による、選択・修正機能は必要（たとえば、部門横断でのエクスポートや移管の												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
				際、表現の整合や統一をはかる場合もある）												
	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	5	e-Discovery 対応では要求される要件												
	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	3	（各レンディションに要求さる廃棄期限管理と整合を取ることが難しい）												
(d)	**キャプチャ及び記録の宣言（※全組織で標準化した記録管理のためには必須要件）**															
	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	3	全組織で標準化した記録管理のためには必須要件	○	○	○	○	○	◎	○	○	○	○	○	○	○

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
		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	5	－												
	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	3	必須機能												
	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	3	必須機能												
	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	3	承認されたユーザ（コンテンツ管理者）による権限制限が必要												
	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	4	必須機能												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	3	必須機能。特に有効である												
	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	5	記録管理上、メタデータの入力を促す機能があると望ましい												
	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	3	辞書機能なども考慮する必要がある												
	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	3	辞書機能なども考慮する必要がある												
	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 Op.）	3	原則、権限を与えられたユーザ（コンテンツ管理者）のみの権限とする必要がある												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	5	ただし、データ管理者以上の権限者での選択が必要												
	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	4	完結したボリュームに対する変更の記録は、全組織で標準化された記録管理を管理・監査するためには必須要件												
	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	Op.	メタデータ構造の標準化が前提												
	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）	Op.	同上												
	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	Op.	同上												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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）	Op.	同上												
	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	Op.	メールは通信手段としての活用に専念すべきとの考えもある												
	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	Op.	コミュニケーション記録としての保管は必要だが、運用ルールを確実にしないと、情報が混乱するリスクと、ウイルス感染などのリスクも高い	○	○	○	×	×	×	○	×	×	×	×	×

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	Op.	添付資料をキャプチャする場合に、メールとの関連などのメタ情報のキャプチャまたは入力が求められることが望ましい												
	68	プロプラエタリフォーマットでキャプチャした電子メール・メッセージをオープンフォーマットで格納できること	Op.	№65と同様												
	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	3	記録管理の要件として、必要												
	70	全ての記録は1つの記録タイプをもつこと	3	全組織で標準化した記録管理のためには必須要件												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	3	入手手段をスキャニングとした場合、スキャニングデータが原本と同等のものとなる。このデータが重要な記録の場合は、タイムスタンプなども含めて記録化することが必要												
	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	3	全組織で標準化した記録管理のためには必須要件												
	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	3	電子化データの安全性確保のためには必須要件												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
(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	3	№17 と同様。ただし、セキュリティ制約との調整が必要(本来閲覧権限が無い個人情報への参照作成をしてはならない)												
	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	3	全組織で標準化した記録管理のためには必須要件												
(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	3	全組織で標準化した記録管理のためには必須要件												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	3	全組織で標準化した記録管理のためには必須要件												
	77a	検索は、全文検索及び属性検索が可能なこと	4	全文検索によるリスク（定型業務におけるノイズの増加）を考える必要がある												
	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	Op.	システムの利用目的により、必要機能か否かの判断が必要												
(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	3	システム管理者の要件として必要												
	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	3	同上												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	4	ログと理解。違法・不適切行為の監視は不可欠	○	○	○	○	○	○	○	○	○	○	○	○
	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 Op.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	5	厳格なデータ管理が必要な場合は必要	○	◎	◎	◎	○	○	○	○	○	○	○	○
	83	削除を破棄、移動を再構成とする代替をコンフィグ Op.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	3	データ管理者の要件として必要												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	Op.	処分プロセス外で削除が許されるケースのみ可												
	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	Op.	同上												
	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また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	5	特に、むやみな削除を防止する要件はあると望ましい												
	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	4	システム管理者の要件として必要。ただし証跡を遺すなどの管理が必要												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	Op.	情報公開法に基づく請求に対して、電磁的記録で対応する場合は不可欠												
	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	Op.	情報公開法に基づく請求に対して、電磁的記録で対応する場合を考慮するとあると望ましい												
(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	Op.	紙の文書管理をシステム上で行う場合は必須要件												
	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	Op.	同上												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	Op.	同上												
	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	Op.	運用での対応可												
	文書管理及び共同作業				×	○	○	○	○	○	○	○	○	○	○	○
	94	文書と記録を同じ分類体系かつ同じアクセス制御下で監理することが望ましい	Op.	－												
	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	Op.	－												
	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ため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	Op.	データ管理者の要件として必要												
	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	Op.	ケース・ファイルの活用が前提												

区分	No	要件	成熟度モデルのレベル	補足説明	商品開発プロセス	研究開発プロセス	日常処理プロセス	企業経営（外部）		企業経営（内部）			訴訟対応		維持管理	
								企業統治モデル	内部統制モデル	マネジメントシステムモデル	営業情報管理モデル	技術継承モデル	知的財産保護モデル	物品製造モデル	設備情報管理モデル	建造物維持管理モデル
	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	Op.	ケース・ファイルの活用が前提												
	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	Op.	電子文書を、法的証拠能力を有するものとして活用する場合は、重要な要件												
	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	Op.	同上												
	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	Op.	同上												

参考文献

[1] 電子記録応用基盤フォーラム　「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-」

[2] 財団法人日本情報処理開発協会　「リスク社会で勝ち抜くためのリスクマネジメント JRMS2010」

第２章　ケースマネジメントの適用

2.1　ケースマネジメント手法の導入

企業活動の記録、情報連絡、伝達の手段として、業務と関係付けて文書を管理することで、管理した文書の活用性が格段に増す。デンマークの「ケースマネジメント」は、その実施例である。本章では、企業に簡便に「ケースマネジメント」を導入することができるように、通常の文書管理システムのフォルダ構造をベースにした手法を考察する。

次に導入したケースマネジメントの効果について検討する。

デンマークの「ケースマネジメント」では、ケースに「属性」、「状態」、「関係」を紐づけています。フォルダの構造を利用する場合は、「ケース属性」、「ケース状態」、「ケース関係」をフォルダ自体に紐づける、もしくは、フォルダの下に配置するものとする。

実際、文書管理システムの中には、フォルダもしくはフォルダに紐づいたファイルの「属性」定義できるものもある。そのような場合は、この領域に「属性」、「状態」、「関係」を記述するものとします。図 2-1 に、フォルダの属性に「ケース属性」、「ケース状態」、「ケース関係」を関連付けたイメージを示す。また、ケースマネジメントにおけるアクセス管理では、ケースクローズ後の公開時において、図 2-1 のように、取扱者による更新・削除権限をなくすことが必要である。

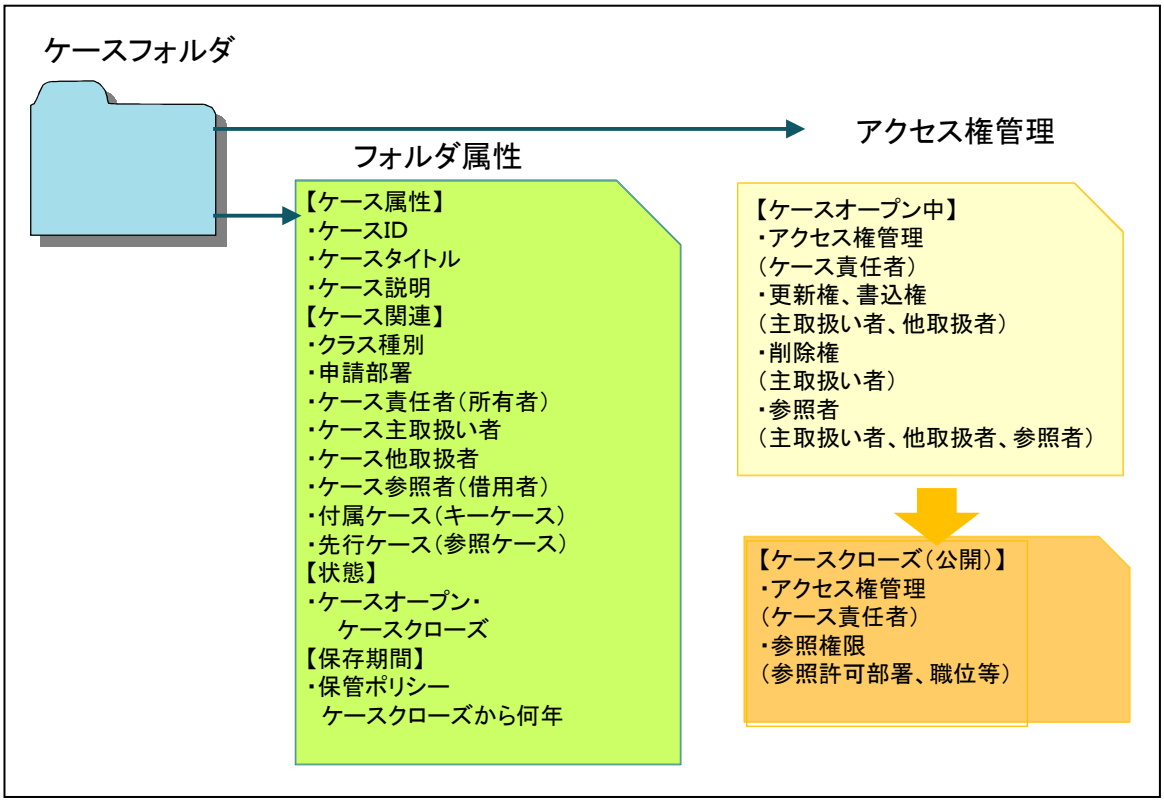


図 2-1　ケースフォルダの属性

表 2-1、表 2-2、表 2-3 に、「ケース属性」、「ケース状態」、「ケース関係」をフォルダ構造に適用した場合の簡易的な適用案を示す。なお、適用に当たっての必須区分については、M は必須、S は推奨で必須に準ずる。O は選択、X は不要を表す。

また、デンマークの「ケースマネジメント」では、文書（ドキュメント）を単独に管理し、ドキュメントリンクにてケースと紐づけているが、現状の国内で市販している文書管理システムでそこまでに機能を持っているものは見かけない。そこで、文書を単独で管理することは求めず、文書を最初に使用したケースフォルダの下に置くこととする。この文書を参照するケースフォルダ内に直接文書を登録するのではなく、リンク情報を記載することとする。ただし、ケース間で保管期限が異なる可能性のある場合は、そのコピー文書を参照しているケースフォルダにも置くものとする。

次に、企業活動におけるケースマネジメントにデンマークの「ケースマネジメント」を適用するに際しての主な留意点を挙げる。

- ケース責任者はケースの活動中とケース活動完了後のフォルダへのアクセス権を分けて設定する。
  - ケース活動中はケース活動推進のために必要な人・部署にのみ必要なアクセス権を付与する。
  - ケース活動完了後は、ケース内の文書への登録・更新・削除権限を他の人・部署に付与せず、予め定められた公開ポリシに従って参照権を与える。

- デンマークの「ケースマネジメント」では、行政処理という観点があり、ケース処理を要請している人を「所有者」と呼んでいるが、企業活動においては、「申請者」もしくは「申請部署」とする方がわかりやすい。
- 企業活動においては、組織変更が頻繁にあるため、個人に紐づけるアクセス権の付与を避けできるだけ、部署、職位による付与に努める。特に、部署については、部署名ではなく、部署コードのように職制変更の影響を受けにくい形態をとることが必要である。
- 保管期限管理

  電子文書管理システムおいては、文書の保管期限についても文書単位になっているものが多い。しかしながら、ケースマネジメントの場合は、ケースフォルダ単位で、保管期限を定めると保管期限管理が格段に容易になる。

  しかしながら、留意すべきは NDA 等の契約上で期限が過ぎた場合に、削除を求められている文書である。このような文書を他のケースから参照する場合は、必ず、リンク参照として当該文書を他のケースフォルダに文書をコピーして置くことは避けなければいけない。逆に言えば、そのような文書はコピー禁止として管理すべきである。

表 2-1　ケースマネジメントの属性（ケース属性）のフォルダ構造への適用案

名称	値	デンマーク ケースマネジメント		フォルダ構造　適用案	
		必須	説明	必須	説明
ユーザ向けキー	テキスト	Y	ユーザ向け ID	O	業務処理毎の ID 番号（追番）、フォルダ名に追加
ケース番号	テキスト	Y	自由なケース番号	M	業務名をフォルダ名として記す
ケースタイトル	テキスト	Y	公のケースタイトル。このタイトルは文書のオブジェクト名になる。	M	業務名をフォルダ名として記す
説明	テキスト	Y	ケースの説明（フリーテキスト）	M	・定常業務の場合は、外部に規程、説明があればよい ・非定常業務は、フォルダ毎に管理する
参考法令	テキスト	N	ケースを指す参考になる法律	O	定常業務の場合は、外部にリンクする規程、があればよい
非公開		N	ケースを非公開する決断。以下の 2 つの要素がある	O	各ケースについては、そのクラス毎に、元々の公開範囲を定める。ここでは、その公開の範囲を狭める場

名称	値	デンマーク ケースマネジメント		フォルダ構造　適用案	
		必須	説明	必須	説明
					合に使用する
代替タイトル	テキスト	Y	Y	O	－
参考法令	テキスト	Y	Y	O	－
代表ケース	Y／N	N	ケースが代表になる際のインデイケーター	X	－
廃棄コード	テキスト	Y	廃棄期間を表すコード	O	－
提出済み	Y／N	N	公共アーカイブに提出済	O	－

表 2-2　ケースマネジメントの「状態」（ケース状態）のフォルダ構造への適用案

名称	デンマーク　ケースマネジメント		フォルダ構造　適用案	
	値	説明 ケースの組織内過程	必須	説明 ケースの組織内過程
ステップ	開始	－	M	ケース活動開始
	情報収集	情報収集済み	O	－
	決定	決定済み。ケースへの追加が不可能になる	O	－
	依頼	アクターへの依頼済み	O	－
	活動完了	活動完了済み	M	ケース活動完了済み(主たる活動者)
	済み	ケースマネジメント済み	O	ケース責任者完了確認済

表 2-3　ケースマネジメントの「関係」（ケース関係）のフォルダ構造への適用案

名称	多重度	デンマーク ケースマネジメント		フォルダ構造　適用案	
		オブジェクトタイプ	説明	必須	説明
アーカイブ	1..1	アーカイブ	ケースを含む上階アーカイブ	O	－
主なクラス	1..1	クラス	分類システムに本ケースを指すメインクラス	S	同一業務については、それを明示するクラス名を割り当てる

名称	多重度	デンマーク ケースマネジメント		フォルダ構造　適用案	
		オブジェクトタイプ	説明	必須	説明
他のクラス	0..n	クラス	分類システムに本ケースを指す他のクラス	O	－
所有者	1..1	アクター	－	M	申請元部署もしくは申請者
責任者	1..1	アクター	－	M	ケースの責任者
主たる取扱者	0..1	アクター	－	M	ケースを推進する人
他の取扱者	0..n	アクター	－	M	ケースに文書を登録する人・部署
ケース借用者	0..1	アクター	ケースの借用者	M	自身のケースの進行のために本ケースの参照を許されている人・部署
対象	0..n	対象（パーツ）	－	－	－
付属ケース	0..n	ケース	本ケースの付属ケース	M	－
関係ケース	0..n	ケース	本ケースと関係あるケース	O	本ケースに先行するケース
関係ケース	0..1	ケース	本ケースの先例になるケース	X	－

2.2　ケースマネジメントの効果

ケースマネジメントにより文書単独での保存よりも格段に信頼度の高い文書の検索が可能になる他にも以下のような効果が期待できる。

- 大きな一つの目的のために、多くのケース処理が複雑に連動して処理されるケースにおいては、「付属ケース」に、大きな目的のケースを指定しておけば（ここではこれをキーケースと呼ぶ。）、このキーケースに関連したケースを検索し、それぞれの内容を検索することが可能になる。例えば、ケースフォルダの属性から表 2-4 のような関連表を作成する。これにより、次のような効果が得られる。
  - 進行中のキーケースの進捗状況とその活動の内容が判明する
  - 過去の類似例を調査する場合にどのような経緯でそのような結果が出されていったかを確認できる
  - 類似プロジェクトの場合には、先行して何を準備せねばならないかもわかる

- 文書の保管期限の観点から見ると各ケースの責任部署が個別に文書の廃棄をしたのでは、ケース全体としてはある時点で記録の一部を失い、全体としての管理ができなくなってしまう場合も生じ得るが、キーケースを管理することで、キーケースの管理が不要になるまでは、各ケースの廃棄も伸ばすという制御も可能になる。

表 2-4　ケースフォルダ関連表

No	当該ケース		付属ケース ID（キーケース）	先行ケース ID
	フォルダ名	ケース ID		
1				
2				
3				

2.3　ケース適用業務例（ソフトウェア受託開発）

ソフトウェア受託開発においては、各作業フェーズで様々な文書が作成される。

上位工程での成果物は下位工程への入力となり、そこで作成されたドキュメントは品質保証のエビデンスとして重要な役割を持つ。

以下、ソフトウェア受託開発にケースマネジメントを適用したモデルについて述べる。

(1)　前提とするモデル

独立行政法人　情報処理推進機構が提唱するエンタープライズ系プロジェクトの開発Ｖ字モデルを例にする。

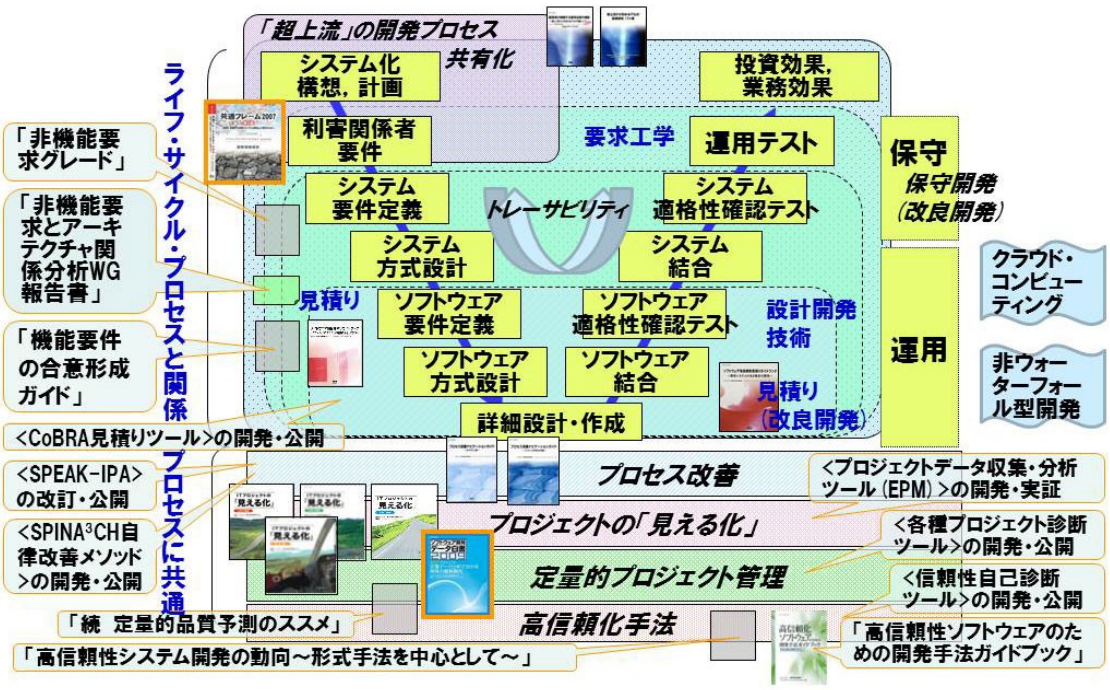


図 2-2　エンタープライズ系プロジェクトの開発Ｖ字モデル

（出典：IPA ホームページより引用）

(2)　条件設定

図 2-2 の中で、事例としてはシステム要件定義からシステム適格性確認テストまでをモデルとする。

また詳細設計・作成フェーズにおいて、協力会社に対してソフトウェア開発の請負契約を行なう場合を想定した。

2.3.1　ソフトウェア開発全般のケース適用

図 2-3 に、ソフトウェア受託開発におけるケース適用モデルを示す。

(1)　適用モデル図

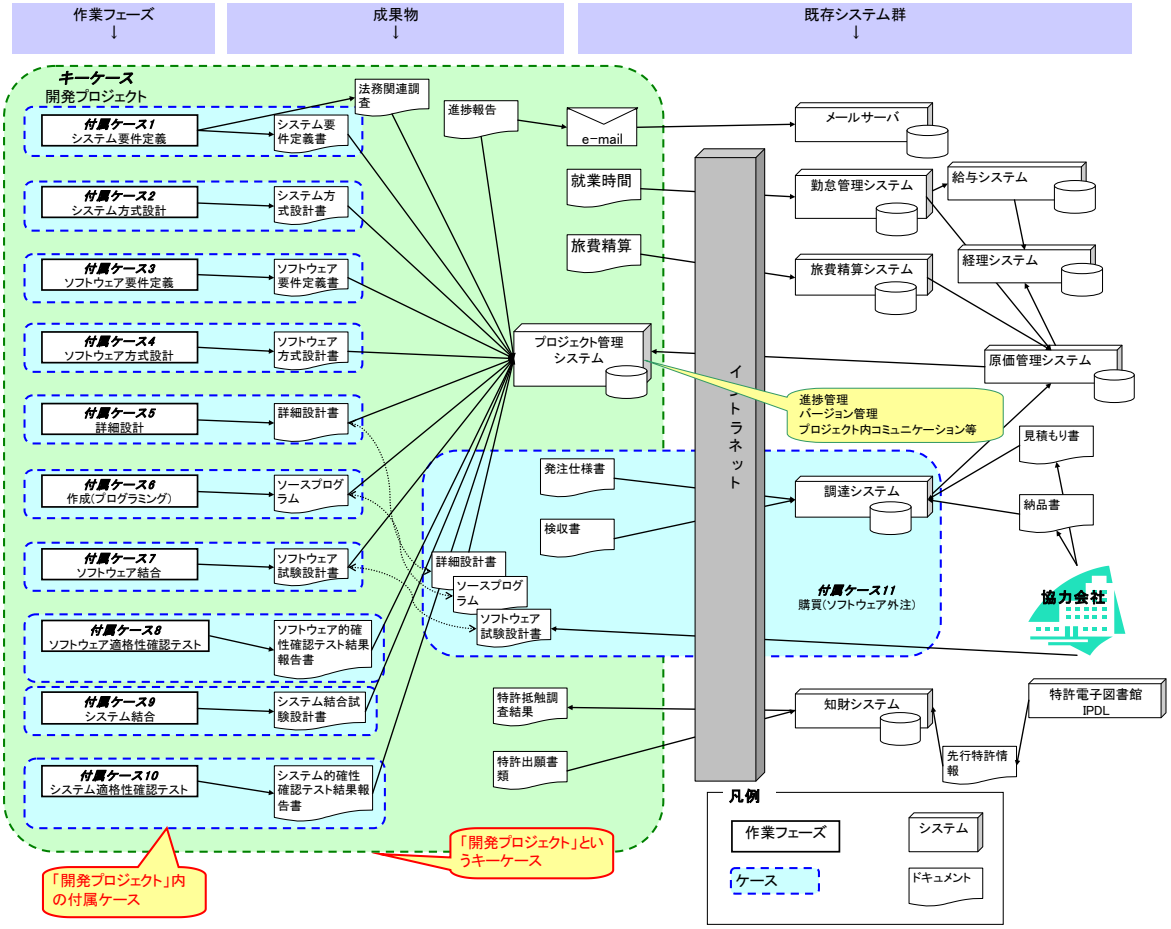


図 2-3　ソフトウェア受託開発におけるケース適用モデル

解説

①キーケースとして「開発プロジェクト」を定義

図中左側の角丸の大きな矩形がそれにあたる。

②キーケースに付属する「付属ケース」として 1～11 までを定義

これらの付属ケースのうち、1～10 は「図 2-2　エンタープライズ系プロジェクトの開発 V 字モデル」で示した V 字モデルの各作業フェーズに該当する。

ただし、付属ケース 11 については、図 2-2 には含まれない。

各付属ケースの中で設計、実装に伴うドキュメント作成と、意思決定が行われ文書がエビデンスとして作成される。

表 2-5　付属ケース一覧

項番	付属ケース名	内容
1	システム要件定義	システム要件定義書を作成する
2	システム方式設計	システム要件定義書を元にシステム方式設計書を作成する
3	ソフトウェア要件定義	システム方式設計書を元に、機能単位に分割し、個々の機能を実現するソフトウェアを定義したソフトウェア要件定義書を作成する
4	ソフトウェア方式設計	ソフトウェア要件定義書を元にソフトウェア方式設計書を作成する
5	詳細設計	ソフトウェア方式設計書に基づき、個々のソフトウェアについて詳細な設計を行い詳細設計書を作成する
6	作成（プログラミング）	詳細設計書に基づき、プログラミングを行う
7	ソフトウェア結合	作成されたプログラムが単体で正しく動作することを確認するために結合試験を実施する。そのためのソフトウェア試験設計書を作成する
8	ソフトウェア適格性確認テスト	ソフトウェア要件定義書を基に、ソフトウェアの適格性確認テスト結果報告書を作成する
9	システム結合	作成されたプログラムがシステムとして正しく動作することを確認するために他のシステムと接続しシステム結合を行う
10	システム適格性確認テスト	システム要件定義書を基に、システムの適格性確認テスト結果報告書を作成する
11	購買（ソフトウェア）	発注仕様書を元にソフトウェア外注を行う

③現在の企業の中には目的に応じて多くの「文書」を取り扱うシステムが存在する

プロジェクト管理システムを導入していれば、付属ケースで作成される多くの文書はプロジェクト管理システムで管理されるが、ケースとしては管理していない。

また、知財情報や進ちょく報告、プロジェクト遂行に必要な電子メールなどはそれぞれを管理するシステムなどで保持されるが、これはケース遂行の中での意思決定過程であったり、状態遷移の情報であり、ケースの管理対象にもなり得る情報である。

④現在、このような開発プロジェクト全体をケースと捉える文書管理システムは具体化していないと考えられる。今後ケースマネジメントを考えるとき、既存のシステムと融合しながら、ケースの切り口で文書を管理していく仕組みが必要になっていくと考えられる

2.3.2 ソフトウェア外注を含む詳細設計ケースの詳細化

図 2-3 のケース適用モデルについて、付属ケースのひとつである「付属ケース 5　詳細設計」を詳細化する。

ここでは、詳細設計業務の一部をソフトウェア外注と請負契約を結ぶ場合を考える。

図 2-4 に、「付属ケース 5 詳細設計」へのケース適用モデル図を示す。

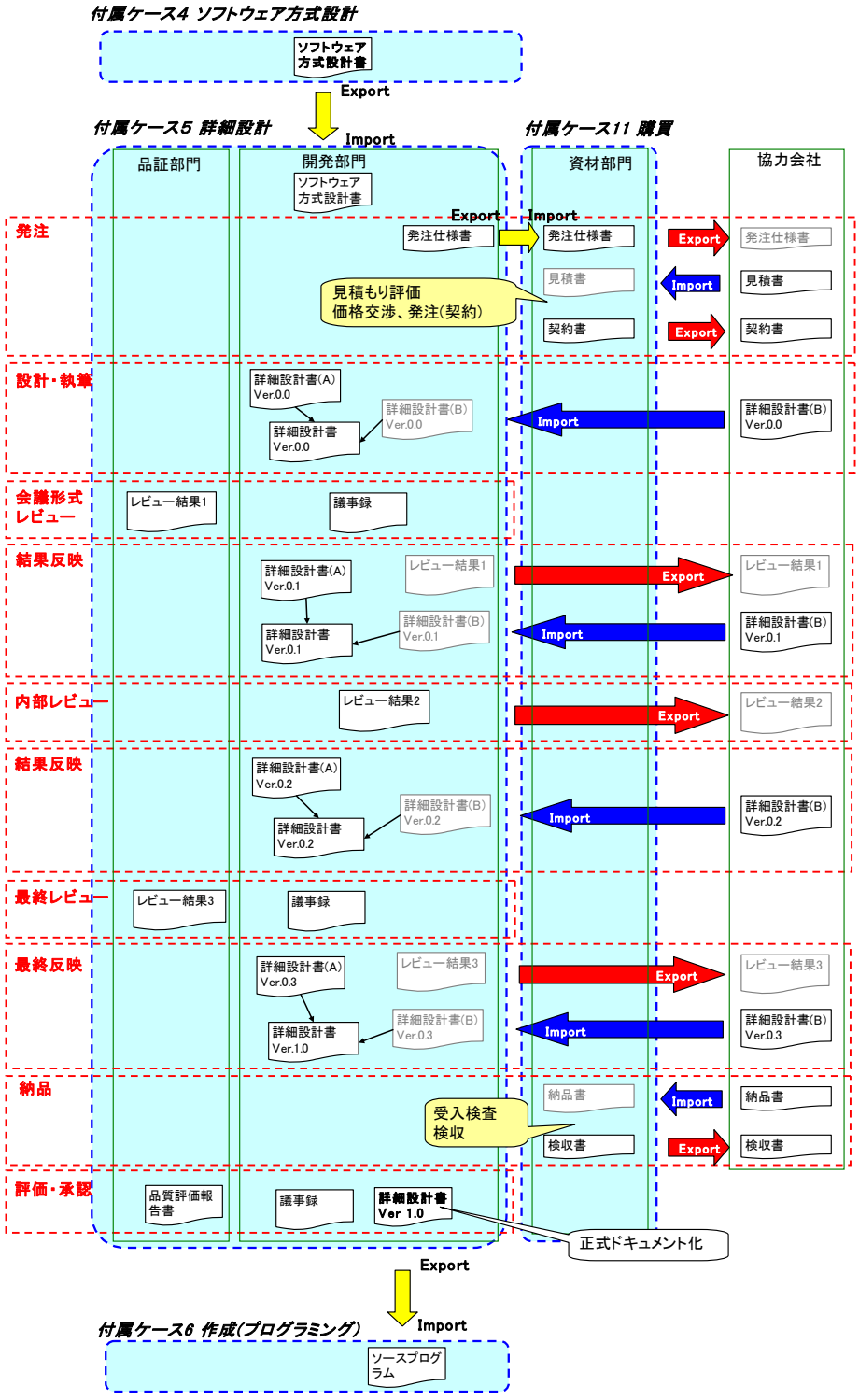


図 2-4　「付属ケース 5 詳細設計」へのケース適用モデル

解説

①ひとつの付属ケースの中でも複数の作業フェーズが存在し、そのフェーズ毎に様々なドキュメントが生成される

②文書は一部門で作成されるものではなく、複数部門、あるいは他社とも共有される

③ここではひとつの付属ケースを実現するために、複数の部門が関連している

「開発部門」が作成する文書を、「品質保証部門（品証部門)」によるレビューを重ねながら最終成果物としてまとめることを想定している。

またその過程で、「協力会社」に一部作業を依頼し、その成果物も取り込む形で最終成果物を作成する。その際、「資材部門」が「開発部門」と「協力会社」との仲介を行う。

④付属ケース 4 の成果物であるソフトウェア方式設計書が、本ケースの入力となる

その際、上位ケースからソフトウェア方式設計書が Export され、本ケースに Import される。

⑤本ケースの成果物である詳細設計書は、本ケースから Export され、下位付属ケース 5 作成（プログラミング）に Import される

⑥本ケース遂行の中で、協力会社に対し一部機能の設計を依頼する。この様子を付属ケース 11 購買として示した

⑦協力会社との文書の授受は Export／Import となる

⑧付属ケース 5 で作成される文書は以下の通りである

表 2-6　付属ケース 5 で作成される文書群

項番	文書名	作成者	内容	他ケースとの関連
1	発注仕様書	開発部門	協力会社への発注仕様	付属ケース 11 に Export
2	詳細設計書(A) Ver.0.0	開発部門	開発部門側が担当する部分の詳細設計書	－
3	詳細設計書(B) Ver.0.0	協力会社	協力会社側が担当する部分の詳細設計書	協力会社から Import
4	詳細設計書 Ver.0.0	開発部門	開発部門と協力会社の詳細設計書をマージしたもの	－
5	レビュー結果 1	品証部門	品証部門によるレビュー記録。品質確保に関するエビデンスとなる	協力会社に Export
6	議事録 1	開発部門	詳細設計レビューのエビデンス。また、付属ケースでの意思決定のエ	－

項番	文書名	作成者	内容	他ケースとの関連
			ビデンスでもある	
7	詳細設計書(A) Ver.0.1	開発部門	開発部門側が担当する部分の詳細設計書	－
8	詳細設計書(B) Ver.0.1	協力会社	協力会社側が担当する部分の詳細設計書	協力会社から Import
9	詳細設計書 Ver.0.1	開発部門	開発部門と協力会社の詳細設計書をマージしたもの	－
10	レビュー結果 2	開発部門	開発部門によるレビュー記録。品質確保に関するエビデンスとなる	協力会社に Export
11	詳細設計書(A) Ver.0.2	開発部門	開発部門側が担当する部分の詳細設計書	－
12	詳細設計書(B) Ver.0.2	協力会社	協力会社側が担当する部分の詳細設計書	協力会社から Import
13	詳細設計書 Ver.0.2	開発部門	開発部門と協力会社の詳細設計書をマージしたもの	－
14	レビュー結果 3	品証部門	品質部門によるレビュー記録。品質確保に関するエビデンスとなる	協力会社に Export
15	議事録 2	開発部門	詳細設計レビューのエビデンス。また、付属ケースでの意思決定のエビデンスでもある	－
16	詳細設計書(A) Ver.0.3	開発部門	開発部門側が担当する部分の詳細設計書	－
17	詳細設計書(B) Ver.0.3	協力会社	協力会社側が担当する部分の詳細設計書	協力会社から Import
18	詳細設計書 Ver.1.0	開発部門	開発部門と協力会社の詳細設計書をマージしたもの 最終成果物	次工程（付属ケース 6）へのインプット。本ケースから Export される。
19	議事録 3	開発部門	詳細設計レビューのエビデンス。また、付属ケースでの意思決定のエビデンスでもある	－

項番	文書名	作成者	内容	他ケースとの関連
20	品質評価報告書	品証部門	作成された成果物に対する最終的な品質報告	ー

このように、ひとつの付属ケースの中でも多くの文書が作成される。

これらは付属ケース実施過程で最終成果物に到達するまでの意思決定のエビデンス、将来、対外的に説明する必要（ここでは品質保証）事項のエビデンスである。

これらの文書を文書管理システムにより、付属ケースから紐づけられて参照できることで、記録として適切に管理できるようになる。

ケースマネジメントにより期待される効果

ソフトウェアの請負開発においてケースマネジメントを導入することで以下のような効果が期待できる。

(1) 証拠書類の維持・管理の精度向上

①品質保証

製造物に対する品質保証のエビデンス（設計、開発に関する資料と、その中での品質保証プロセスに関するドキュメント）の一括管理。

②契約

協力会社との契約、協力会社の製造物に関するドキュメントの一括管理。

(2) 文書の属人化防止

組織改変、人事異動などにより文書が散逸することを防ぎ、プロジェクトが遂行された当時の生々しい文書セットを保持し続けることができる。

(3) 同様ケースの再利用、活用

前述(2)により、成功、あるいは失敗の過去事例の振り返りでケース単位でドキュメントが一括管理されていることにより、検索の効率化など利活用が推進される。

参考文献

[1] 独立行政法人 情報処理推進機構　エンタープライズ系プロジェクトの開発 V 字モデル
http://sec.ipa.go.jp/std/ent.html

第３章　証拠性確保を重視したパッケージ構造

法的証拠性が重視される電子記録を利活用、保存、流通等するためのパッケージ構造を提案する。パッケージには電子記録、関連するメタ情報に加え、証拠性を確保するために電子署名等を含める必要がある。本章では、ETSI が電子データと分離型電子署名を一体化するために提案している ASiC（Associated Signature Containers）[7] を拡張した電子記録管理のためのパッケージ構造について紹介する。

3.1　はじめに

検索・共有・流用の容易性、通信による迅速なデータ配信、多重化による災害への耐性など、紙文書と比較して電子文書が多くの利点を持つことは言を待たない。

電子文書の欠点とされていた改ざんの容易性やその痕跡が残らないことに対しても、電子署名等の技術が解決策を与えている。

記録媒体の劣化やドライブ装置の世代交代による長期保存の困難性に対しても、一般社団法人電子情報技術産業協会（JEITA）が継続的マイグレーションによるデジタルデータの 100 年以上の保存を提唱しており[1] 、電子情報通信学会エレクトロニクスソサイエティの超長期保管メモリ時限研究会では 1000 年間のデジタル情報の保管を妥当なコストで実現する手段が検討されるなど、運用を含めた技術による解決が期待できる段階に近づいている。

また、e-文書法や厚生労働省のガイドライン[2] などの文書を電子で扱うための法制度や、デジタルデータの証拠性確保のために必要となるタイムスタンプサービスやその認定制度（財団法人日本データ通信協会「タイムビジネス信頼・安心認定制度」）などの社会インフラも整備されている。

南カリフォルニア大学の研究によると、2002 年にはデジタル情報がアナログ情報を上回り、2007 年には全人類が全世界中に保持している情報の容量は 295 エクサバイトの内、94%がデジタル情報であるとされている[3] 。この数値は「文書」に限らず種々のマルチメディア情報を含むものではあるが、電子文書の量が紙文書の量を大幅に上回っていることには疑いの余地がないであろう。

このように電子化が進展しているにもかかわらず、組織的な運用がなされていない、標準的な手段を用いていないなど、電子文書を記録としてマネジメントできていない。つまり電子記録マネジメント不在の状態にあると言える。

ここで言う電子記録マネジメントとは、組織による事業継続／発展、リスク回避、権利保護、説明責任などを達成し、それを長期にわたって維持することを目的とした、電子記録の取得、維持、活用等の仕組みであり、その実践である。eRAP では電子記録マネジメントを効果的に実現するための基盤として、電子記録マネジメント基盤を提案している[4] 。

電子記録マネジメントでは、特に権利保護や説明責任などへの適用においては、電子記録の証拠としての証明力が重視される。本章では、上記電子記録マネジメント基盤を想定し、証拠性の

確保を重視した電子記録マネジメントのための電子記録の取扱いの単位となるパッケージの構造を提案する。

3.2　電子記録マネジメント基盤

本節では、提案するパッケージ構造の前提となる電子記録マネジメント基盤について説明する。そのために、まず電子記録と電子記録マネジメントの定義を示した上で電子記録マネジメント基盤の概要について説明し、更に将来導入することを目指しているケースマネジメントについて紹介する。

3.2.1　電子記録

電子記録の定義は ISO 15489-1[5] に準じる。ISO 15489-1 によると、記録とは「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」である。

電子記録は証拠性を確保された状態の電子文書あるいは形式を問わないあらゆる電子データであり、証拠性（証拠としての証明力）を持つことが重要な性質となる。

3.2.2　電子記録マネジメント

電子記録マネジメントとは、組織による事業継続／発展、リスク回避、権利保護、説明責任などを達成し、それを長期にわたって維持することを目的とした、電子記録の取得、維持、活用等の仕組みであり、その実践である。この定義もやはり ISO 15489-1[5] に準じるものである。文献[4] では、MoReq2 に示された電子記録マネジメントに対する要件より抽出し整理した「電子記録マネジメントの主要 100 要件」を策定している。

3.2.3　電子記録マネジメント基盤

電子記録マネジメント基盤は、電子記録マネジメントの主要 100 要件に沿って電子記録マネジメントを実現する基盤（プラットフォーム）である[4] 。

電子記録マネジメント基盤の位置付けを図 3-1 に示す。

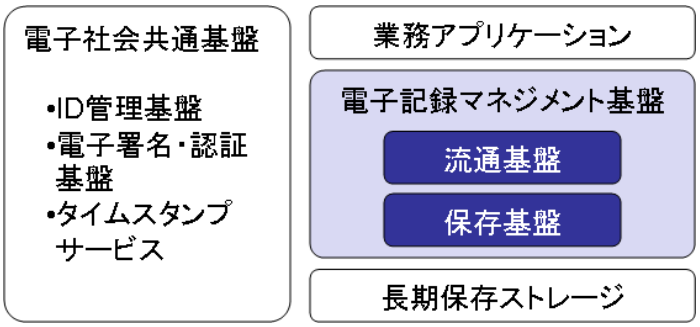


図 3-1　電子記録マネジメントシステムの構造と電子記録マネジメント基盤の位置付け

図 3-1 にあるように、電子記録マネジメント基盤は、電子記録マネジメントを実現する全体システムである電子記録マネジメントシステムの内部に位置する。その中で電子記録マネジメント基盤は、LTFS（Linear Tape File System）などの長期保存ストレージの存在を前提に、ID 管理基盤、電子署名・認証基盤、タイムスタンプサービス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に関わるサービスとして電子記録の保存と流通のためのサービスを提供する。それらサービスを実施する保存基盤と流通基盤が電子記録マネジメント基盤の構成要素である。

電子記録マネジメントシステム及び電子記録マネジメント基盤は複数存在することが可能で、1 つの電子記録マネジメントシステム／基盤より他の電子記録マネジメントシステム／基盤へと一部のあるいは全ての記録が移管される場合が考えられる。

3.2.4 ケースマネジメント

電子記録マネジメント基盤では、デンマーク政府が採用するケースマネジメントの概念を導入している。この概念の導入目的は、

- 決定過程を含めた記録の管理
- 記録の利活用の促進

である。

ケースマネジメントは、特定の案件に関する行動計画、実行者割り当て、行動記録などを動的にマネジメントする概念である。ケースを利用する業務としては、組織横断的なプロジェクトや行政における事業などを想定しており、従来の組織活動（縦割り）に対応した記録の管理から脱却し、組織横断的な記録の管理を実現することを想定している。

決定過程を含めた記録管理のためには、複数組織に跨る案件毎に対応する一連の業務と関連付けて記録を管理する仕組みが必要となる。

利活用促進のためには、様々な角度からの検索を容易とするために、記録の時系列的な並びと発生事象（作成、受取り、配布、参照など）、記録相互の因果関係、関係者などのメタデータを管理する仕組みが必要となる。

3.3 パッケージ

3.3.1 パッケージの参照モデル

パッケージとは、電子記録マネジメントにおける管理対象を単位ごとに一体化するためのデータ形式である。韓国の公認電子文書保管所、ドイツの ArchiSafe プロジェクト、ハンガリーなどで、パッケージを定義して記録管理を実施している。

パッケージの参照モデルが ISO 14721:2003[6] に定義されている。この参照モデル（OAIS の参照モデル）におけるパッケージの構造を図 3-2 に示す。

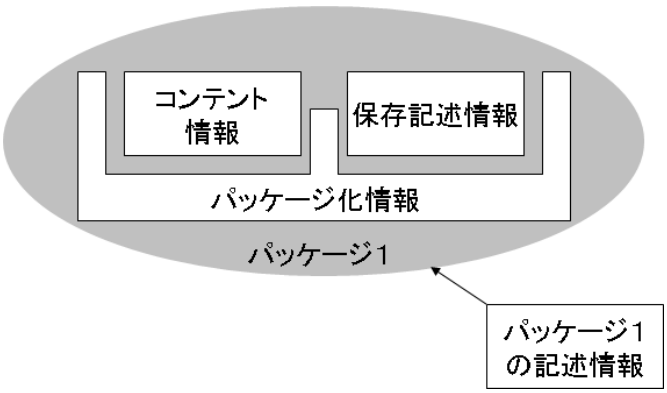


図 3-2　OAIS 参照モデル―パッケージ構造

パッケージは管理対象であるコンテンツとコンテンツに関する情報であるメタデータで構成される。図 3-2 において、コンテント情報（Content Information）は、管理対象であるコンテンツそのもの（Content Data Object）とコンテンツを可読とするための参考情報である表現情報（Representation Information）というメタデータで構成される。また、保存記述情報（Preservation Description Information）は、コンテンツの利活用や管理を容易とするためのメタデータである。パッケージ化情報（Packaging Information）は、コンテント情報と保存記述情報の物理的な結合のための情報であり、コンテンツに関するメタデータには含まれない。メタデータの詳細については次章に記述する。

ISO 14721:2003[6] における参照モデルでは図 3-3 に示すパッケージの種類を定義している。

図 3-3　OAIS 参照モデル―パッケージの種類

パッケージの種類として、保管・保存システムを中心として次の 3 種類が定義されている。

SIP：Submission Information Package（提出用情報パッケージ）

AIP：Archival Information Package（保存用情報パッケージ）

DIP：Dissemination Information Package（配布用情報パッケージ）

このモデルでは保管・保存システムから他の保管・保存システムへの移管が考慮されていない。

韓国の公認電子文書保管所におけるパッケージモデルは、OAIS の参照モデルを拡張し、TIP を定義している。

TIP：Transfer Information Package（移管用情報パッケージ）

TIP の位置付けを図 3-4 に示す。

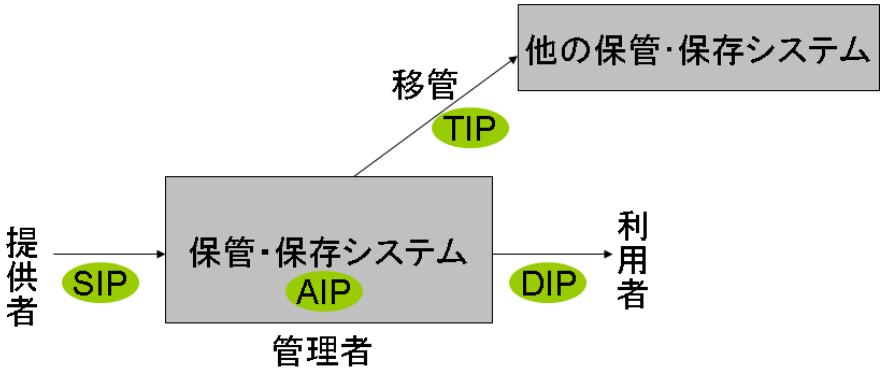


図 3-4　OAIS の拡張

3.3.2　ASiC（Associated Signature Containers）

ETSI では、コンテンツと電子署名あるいはコンテンツとタイムスタンプを一体化するためのパッケージとして ASiC（Associated Signature Containers）[7] を提案している。

ASiC の基本構造は次の通りである。

- フォルダにより階層化されたファイルを zip 圧縮したファイルである。
- コンテンツのメタデータ（署名を含む）を格納する META-INF サブフォルダを持つ。パッケージのタイプには大きく分けて次の 2 種類がある。
  - ASiC-S（簡易型 ASiC）：
    単一のデータオブジェクトと一つ以上の署名やタイムスタンプを含むパッケージ
  - ASiC-E（拡張型 ASiC）：
    複数のデータオブジェクトとそれぞれに対する一つ以上の署名やタイムスタンプを含むパッケージ

ASiC-E には、XML 型の長期署名（XAdES）[8] を含むものと CMS 型の長期署名（CAdES）[9] あるいはタイムスタンプを含むものがある。それぞれを図 3-5～図 3-7 に示す。

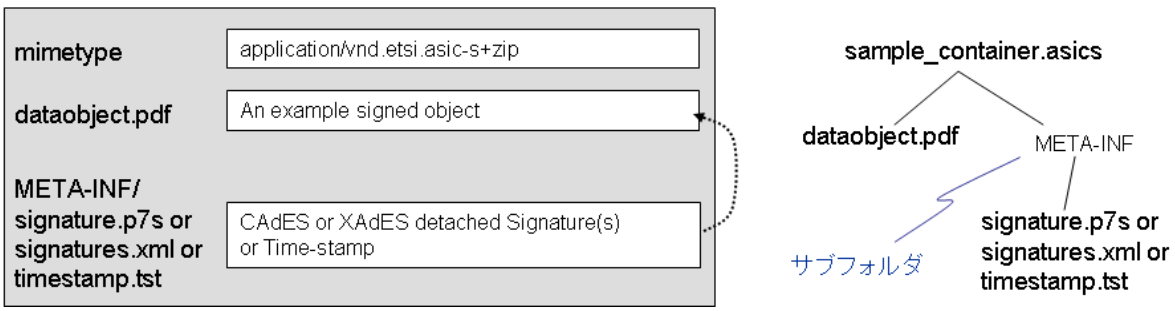


図 3-5　ASiC-S の構造とフォルダ構造の例

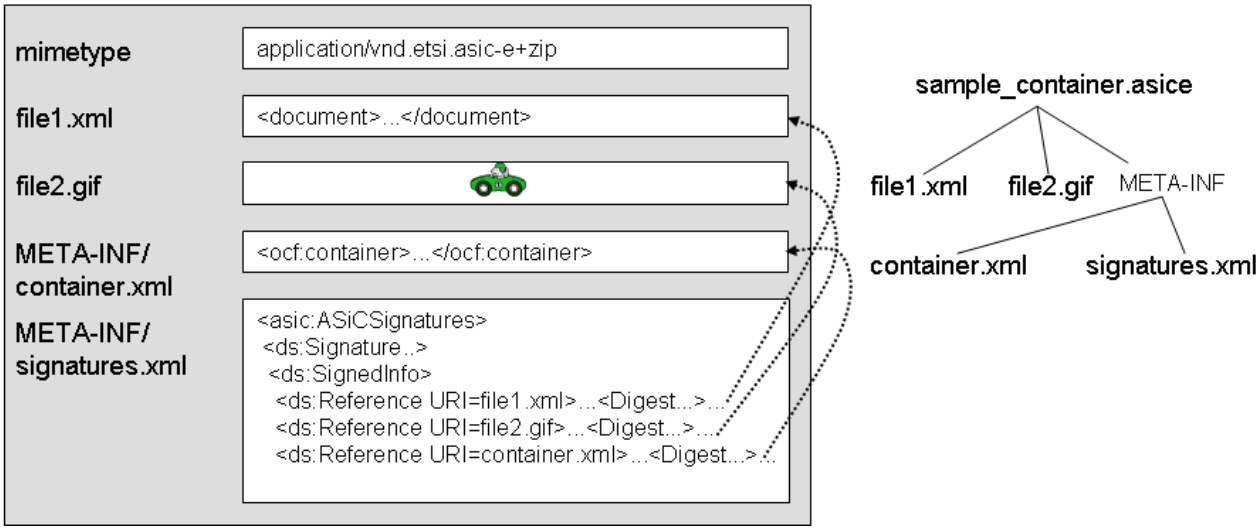


図 3-6　ASiC-E（XAdES を含む形式）の例

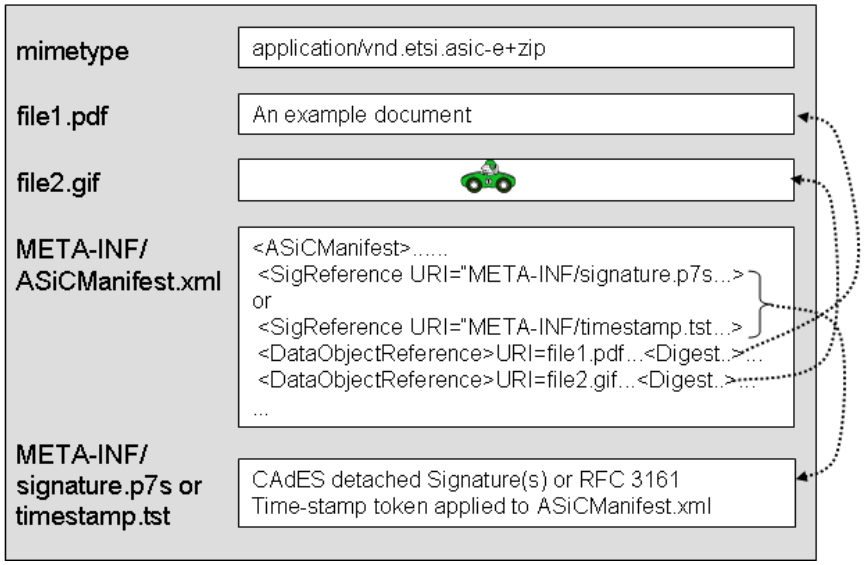


図 3-7　ASiC-E（CAdES またはタイムスタンプを含む形式）の例

ASiC-S や ASiC-E で付与された電子署名やタイムスタンプは、有効期間の超過や失効により、有効性を長期にわたって維持できない。ETSI ではその対策となる長期保存用のパッケージとして、ASiC-A（長期検証型 ASiC）が検討されている。ASiC-A の構造を図 3-8 に示す。

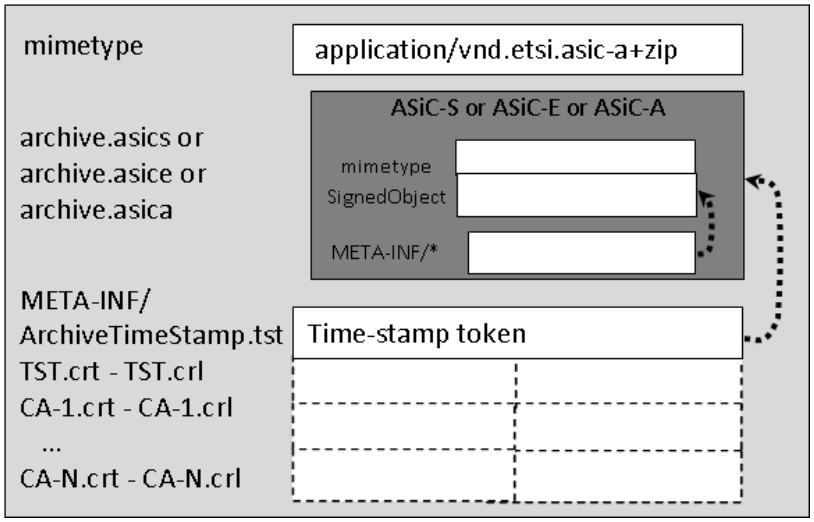


図 3-8　ASiC-A：長期検証型 ASiC の構造の例

3.3.3　証拠性確保を重視した電子記録マネジメントのためのパッケージ構造提案

証拠性確保を重視し、電子記録マネジメント基盤を前提として考案したパッケージ構造に対する要件を次に示す。

[要件 1] コンテンツの証拠性確保のためには、電子署名やタイムスタンプを伴わなければならない。証拠性を長期にわたって維持するためには長期署名をサポートすることが必須である。

[要件 2] 決定過程を含めた記録の管理を実践し、記録の利活用を促進するためには、長期署名以外のメタデータを格納できなければならない。

[要件 3] 電子記録マネジメント基盤に対して、記録の受取／保存／配布／移管を行うにあたっては、添付可能な、あるいは添付を必要とされるメタデータが異なることが考えられる。また、電子記録マネジメント基盤での管理期間中にメタデータが追記あるいは変更される可能性もある。メタデータが更新可能であることを考慮する必要がある。

[要件 4] メタデータ自体を記録の一部として証拠性を確保することを可能とすることも考慮する必要がある。配布や移管においてメタデータそのものの正当性を保証する必要がある場合の要件となることが考えられる。

[要件 5] 電子記録マネジメント基盤に対しては、記録の提出／保存／配布／移管が生じうる。それぞれの局面に対応したパッケージをサポートすることが必要である。

まず、[要件 1] に対応するために長期署名をサポートする構造とすることを前提とする。そのためには XAdES[8] や CAdES[9] 自体をパッケージの基本構造とすることも考えられるが、[要件 2] の長期署名以外のメタデータを含めるには XAdES や CAdES は適当な格納場所が用意されていない。そこで ASiC を基本構造とすることを考える。ASiC には 3.3.2 で示した異なる形式がある。管理対象が単一のファイルであれば ASiC-S を用いることができる。長期間証拠性を維持するためにはアーカイブタイムスタンプの追加付与が必要であるが、ASiC-S を用いた場合、

CAdESを利用した場合でもXAdESを利用した場合でも署名を格納するためのファイル(CAdESの場合 META-INF/signature.p7s、XAdES の場合 META-INF/signature.xml）を、アーカイブタイムスタンプを追加したファイルと置き換えることによって可能となる。

複数のファイルを管理対象とする場合は、ASiC-E（XAdES を含む形式）を用いることができる。同様に、署名を格納するためのファイル（META-INF/signature.xml）を、アーカイブタイムスタンプを追加したファイルと置き換えることによって、証拠性を長期にわたって維持することができる。

ところが、ASiC-E（CAdES またはタイムスタンプを含む形式）は適当でない。CAdES 及びタイムスタンプの対象データは ASiC において新たに定義された ASiCManifest.xml であり、本来の管理対象であるファイル（図 3-7 の file1.pdf と file2.gif）そのものではない。アーカイブタイムスタンプを取得する際には管理対象であるファイルそのものを含めて計算したハッシュ値を用いる必要があるため、管理対象であるファイルのハッシュ値のみを含む ASiCManifest.xml では十分ではない。

ASiC-A を用いることにより[要件 1] に対応することも可能と思われるが、[要件 3] を満たそうとすると、ASiC-A のアーカイブタイムスタンプの付与により、内部の ASiC-S、ASiC-E、ASiC-A の持つメタデータがアーカイブタイムスタンプにより固定されてしまい、更新できなくなってしまう。

次に[要件 2] に対応するには、ASiC の基礎となる形式である OEBPS Container Format（OCF）1.0[10]の”metadata.xml”オプションを利用する。このファイル内に各種メタデータを記述し、META-INF フォルダの下に格納することが可能である。

上記より、ASiC をベースとした証拠性確保を重視した電子記録マネジメントのためのパッケージ構造案を図 3-9 に示す。

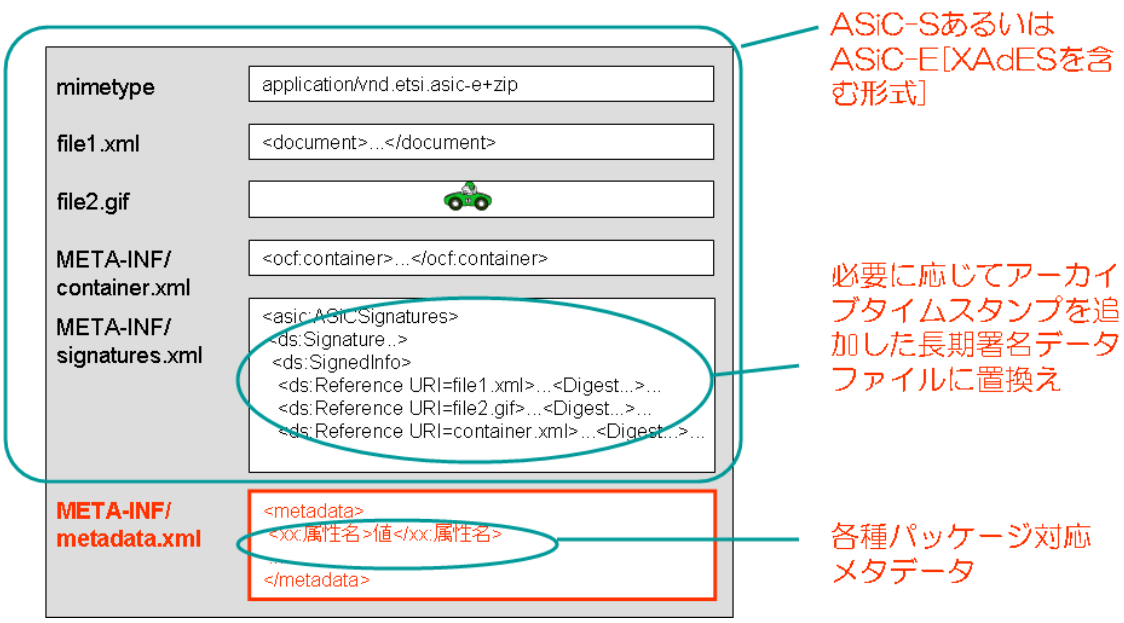


図 3-9　ASiC をベースとした電子記録マネジメントのためのパッケージ構造案

[要件 3] への対応については前述した。図 3-9 の構造を見ればわかるようにメタデータは長期署名の対象範囲外にあるため、更新可能である。

[要件 4] は[要件 3] とは反対にメタデータを長期署名等の対象とする必要がある。このとき、メタデータのみを対象とすることには意味が無く、コンテンツとの関連を含めて対象としなければならない。そのためには図 3-10 に示すように、パッケージをコンテンツとして更にパッケージに格納する方法をとればよい。

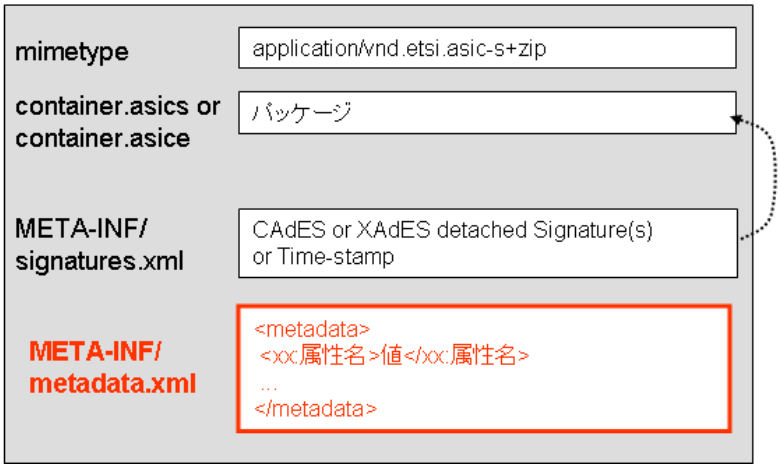


図 3-10　メタデータ自体を記録としたい場合のパッケージ構造例

[要件 5] に対応するためには、図 3-9 に示したパッケージ案をもとに、提出用、保存用、配布用、移管用のメタデータを定義すればよい。これについては 3.4 に記述する。また、配布用あるいは移管用にメタデータを含めた正当性を保証する必要がある場合、図 4-10 に示したパッケージのパッケージとして、電子記録マネジメント基盤の電子署名等を付与することを基本とすることが考えられる。

なお、図 3-2 の OAIS 参照モデルにおけるパッケージ構造との関係を整理すると、次のように対応付けられる。

- パッケージ化情報：zip のファイル形式として管理する情報と mime type が相当する。
- コンテント情報：署名の対象となるファイルの内容が Content Data Object に相当し、拡張子を含むファイルに関する属性が表現情報に相当する。
- 保存記述情報：META-INF フォルダ以下のファイルの情報が相当する。

3.4　メタデータ

3.4.1　メタデータモデル

メタデータについては 3.3.1 に示した OAIS 参照モデルでも触れたが、記録管理におけるメタデータの全体像を示すメタデータモデルが ISO 23081-2:2009[11] で定義されている。その中で、図 3-11 に示すように 6 種類のメタデータを定義している。

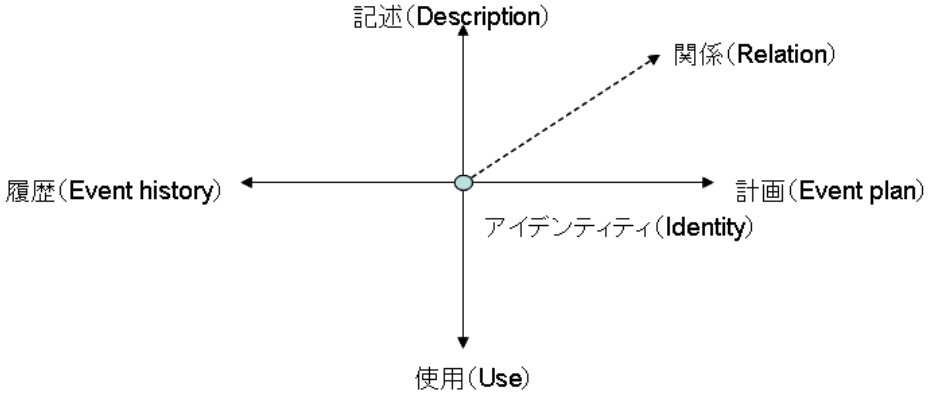


図 3-11　メタデータの種類と関係

6 種類のメタデータの概要を次に示す。

- アイデンティティ（Identity）: タイプ、階層的に管理される場合の階層、登録識別子など、コンテンツを特定するためのメタデータ
- 記述（Description）: タイトル、分類、概要、保管場所、裁判管轄地、外部で用いるためのユニークな識別子（ユニーク ID）など、利用すべきコンテンツであるか否かを決定するためのメタデータ
- 使用（Use）: 技術的な使用環境、アクセス方法、権利、想定する使用者、使用言語、チェックサムや電子署名などの完全性を保証するデータ、など、長期にわたってコンテンツを利用するために必要なメタデータ
- 計画（Event plan）: コンテンツを管理するための作業等のイベントに関するメタデータ。イベントのタイプ／優先度／実行日時／実行者、トリガーとなる事象などの要素となるメタデータをまとめたもの
- 履歴（Event history）: コンテンツ及びメタデータに対して過去に生じたイベントを示すメタデータ。イベントの識別子／発生日時／タイプ／内容／実行者などの要素となるメタデータをまとめたもの
- 関係（Relation）: 関係の識別子、タイプ、開始／終了日など、他のコンテンツとの関係を示すメタデータ

3.4.2　電子記録マネジメントのためのパッケージで考慮すべきメタデータ

3.3.1 に記したとおり、SIP、AIP、DIP、TIP の 4 種類のパッケージにつき、それぞれのパッケージの役割から採用すべきメタデータを検討する。

(1)　SIP

コンテンツの提供者が電子記録マネジメント基盤に対して登録するためのパッケージである。提供者のみが知る情報や、提供者の主張したい内容に関わるメタデータを含むべきである。従って、アイデンティティ、記述、使用に関わるメタデータのほとんどについては登録時に提供者が

指定する。

一方で、登録後に判明する情報を含むことはできない。登録識別子や保管場所がそれに相当する。

保存期間などの計画、作成に関わる履歴、登録済みの他のコンテンツとの関係を登録時に指定しても良い。

(2) AIP

電子記録マネジメント基盤内で保管・保存するためのパッケージである。基本的に全てのメタデータを保持する。登録識別子や保管場所はここで追加される。登録識別子とは別にユニークIDを付与することも必須としたい。

また、計画、履歴、関係の保持／更新は必須である。

登録者が付与した完全性保証データがSIPに含まれていた場合、その保持及びその長期保証は必須である。もしもSIPにこのデータが含まれていなかった場合は、コンテンツの存在時刻を証明するために電子記録マネジメント基盤が別途タイムスタンプ等の完全性保証データを付与する必要がある。

(3) DIP

利用者にコンテンツを配布するためのパッケージである。アイデンティティ、記述に加え、使用に関わるメタデータは必須である。ただし、単に参照するために利用する場合など、完全性保証データが不要である場合もある。

計画、履歴、関係については必要に応じてあるいは権限に応じて含めるか否かを判断することとなる。

(4) TIP

電子記録マネジメント基盤から他の電子記録マネジメント基盤にコンテンツを移管するためのパッケージである。基本的に電子記録マネジメント基盤内で管理している全てのメタデータを含める。また、移管されたコンテンツが正しいものであったことや移管時期を証明できるようにするために、電子署名及びタイムスタンプを用いた完全性保証データを付与することは必須と考えられる。

上記を表 3-1 にまとめる。

また、電子記録マネジメント基盤を中心としたパッケージの関係を図 3-12 に示す。

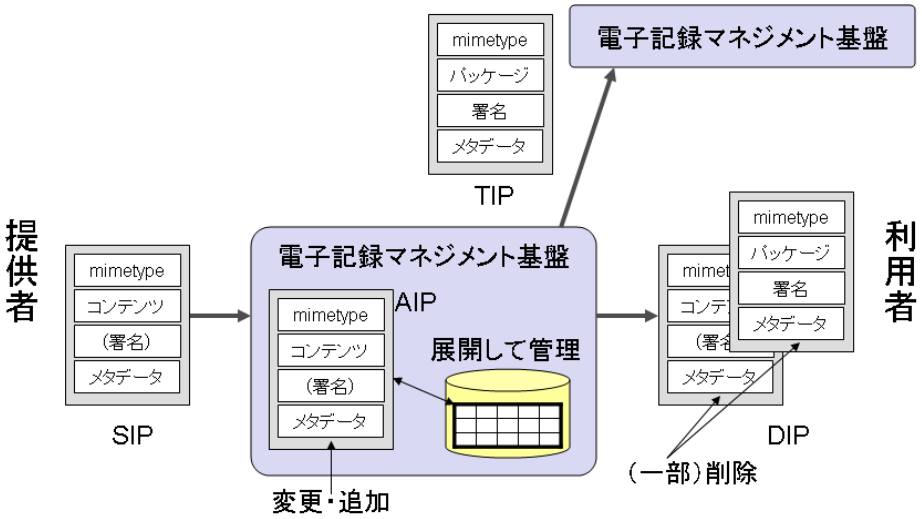


図 3-12　電子記録マネジメント基盤を中心としたパッケージの関係

表 3-1　各パッケージとメタデータの関係

○：必須、△：オプション、－：該当なし

			SIP	AIP	DIP	TIP
アイデンティティ	タイプ		○	○	○	○
	階層		○	○	○	○
	登録識別子		—	○	○	○
記述	タイトル		○	○	○	○
	分類		○	○	○	○
	概要		○	○	○	○
	保管場所		—	○	△	○
	裁判管轄地		○	○	○	○
	ユニーク ID		△	○	○	○
使用	使用環境		○	○	○	○
	アクセス方法		○	○	○	○
	権利		○	○	○	○
	使用者		△	△	△	△
	言語		○	○	○	○
	完全性保証データ		△	○	△	○
計画	イベント	タイプ	△	○	△	○
		優先度	△	○	△	○
		実行日時	△	○	△	○
		実行者	△	○	△	○
		トリガー	△	○	△	○

			SIP	AIP	DIP	TIP
履歴	イベント	識別子	△	○	△	○
		発生日時	△	○	△	○
		タイプ	△	○	△	○
		内容	△	○	△	○
		実行者	△	○	△	○
関係	他の実体	識別子	△	○	△	○
		タイプ	△	○	△	○
		開始日	△	○	△	○
		終了日	△	○	△	○

3.5 おわりに

電子記録マネジメント基盤を想定し、パッケージ構造及びパッケージが保持すべきメタデータを示した。メタデータに関してはその方向性を示すに留まった。今後、ドイツや韓国の例も参考にしながら、詳細を検討したい。

また、今回パッケージの対象としたコンテンツは「記録」を想定したもので、ケースマネジメントにおける「ケース」を対象とするものではない。電子記録マネジメント基盤ではケースマネジメントの概念を導入することとしているため、個々の記録だけではなく記録が一連の関連付けられるケースを対象としたパッケージ構造やメタデータを検討する必要がある。複数のコンテンツを扱え、更に階層化も可能な ASiC を基本とすれば、ケースに対応するパッケージを定義できると考えている。

証拠性確保を重視した今回の検討では、長期署名による真正性の確保を中心に検討してきたが、同時に秘匿性を検討する必要もあるであろう。登録者が電子記録マネジメント基盤の管理者にコンテンツを開示したくない場合や、Stuxnet 等に代表される新しいタイプの攻撃への対策のために電子記録マネジメント基盤としてコンテンツやパッケージを暗号化することが考えられるからだ。長期署名と暗号化の両立、長期保存に対応した暗号鍵の管理や更新、暗号アルゴリズムの更新などが課題となる。

参考文献

[1] 一般社団法人 電子情報技術産業協会　「データマイグレーションの必要要件」
http://home.jeita.or.jp/is/committee/tech-std/std/data_migration_201101.pdf

[2] 厚生労働省　「医療情報システムの安全管理に関するガイドライン 第 4.1 版」
http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf

[3] University of Southern California　「How Much Information Is There in the World?」
http://uscnews.usc.edu/science_technology/how_much_information_is_there_in_the_world.html

[4] 木村道弘、前田陽二、辻秀一　「クラウド時代の情報流通基盤」　情報処理学会、第 118 回 情報システムと社会環境研究発表会、IS118-05(2012).

[5] ISO 15489-1:2001 Information and documentation -- Records management -- Part 1: General

[6] ISO 14721:2003 Space data and information transfer systems -- Open archival information system -- Reference model

[7] ETSI TS 102 918 v1.1.1 (2011-04): Electronic Signatures and Infrastructures (ESI) ; Associated Signature Containers (ASiC)

[8] ETSI TS 101 903 V1.4.1 : XML Advanced Electronic Signatures - XAdES

[9] ETSI TS 101 733 V.1.7.4 : CMS Advanced Electronic Signatures - CAdES

[10] International Digital Publishing Forum, OEBPS Container Format (OCF) 1.0 日本語版, http://naoki.sato.name/ocf/ocf_1_0_spec_ja.html

[11] ISO 23081-2:2009 Information and documentation -- Managing metadata for records -- Part 2: Conceptual and implementation issues

第４章　署名・認証の新しい流れ－クラウド時代の PKI

4.1　クラウドを取り巻く現状

2011 年度は「クラウド」と言う言葉が広く一般に定着した年と言えるであろう。それには幾つか要因があるが、SNS（ソーシャルネットワークサービス）をはじめとするクラウドサービスと、スマートフォンに代表されるモバイル利用可能なネットワークデバイスの普及が、コンシューマ分野においてもエンタープライズ分野においても進んだことが大きな要因と考えられる。

一方で「クラウド」とは何かを知らずともクラウドを利用できる面があり、その可能性や特長を把握することが難しい。本章ではクラウドについての状況をまとめると共に、ECOM 時代から現在の eRAP まで取り組んできた電子署名・電子認証の分野における可能性を考察しまとめることを目的としている。

SNS の利用者は増加しており、その ID 数（アクティブユーザ数）が各 SNS の強みでありビジネスモデルの根幹になっている。Facebook、Google、Yahoo!等は IdP（ID プロバイダ）として各種認証 API を提供することで第三者における SNS 連携クラウドサービスの開発を推進している。Google、PayPal、VeriSign、Verizon など米企業 7 社は、企業及び政府機関のサイト向けのオープンなオンライン ID 認証フレームワークの構築を目的とした非営利団体 OIX（Open Identity Exchange）[1] を立ち上げており、Google 等が認定プロバイダとなっている。米国では SNS が着実に IdP への道を歩み始めていると言えるだろう。

4.2　クラウドの定義

まず「クラウド」の定義を行う。NIST（米国国立標準技術研究所）ではクラウドを SaaS・PaaS・IaaS の 3 種類のサービスモデルに分類している[2] 。

表 4-1　NIST によるクラウドのサービスモデルの定義

略称	名称	意味
SaaS	Software as a Service	ソフトウェアを実行してサービスを提供。従来の ASP サービスもこの一種
PaaS	Platform as a Service	ネット上におけるソフトウェア実行プラットホーム環境の提供。Java 等の API を提供
IaaS	Infrastructure as a Service	CPU（計算資源）やストレージ等のインフラの仮想的な提供

しかしながら現実問題として昨今ではこれらのサービスモデルを組み合わせて利用されるケースが増えており単純な分類は難しい。ここではNISTにて5つに分類されるクラウドの特徴をベースに独自の定義を行う。色々な定義があると思われるが大きく分けて以下に示す3つに整理した。

①利用者やサービスに対して必要なリソースが必要な時に動的に提供される。
②標準化された手順によりスマートフォンやシンクライアントからの利用も可能。
③サービスはAPIを提供しAPIを組み合わせることで新たなサービスが構築できる。

①は仮想的にOSやサービスが稼働するシステムを提供することを示している。従来のサーバ・クライアント型のシステムではサーバは物理的に存在しており能力を増強するにはハードウェアを追加する必要があった。しかし急激に利用者が増加した場合に対応することは難しく、逆に平素は過剰なハードウェアを保有する必要があり効率が悪い。これをクラスタ化されたサーバ上に構築された仮想マシン（VM）の上で動作させることでハードウェアの追加無しに必要なだけ動的にリソースを確保可能となる。これが一般のクラウドのイメージに一番近い定義であろう。

②は利用者のメイン端末がPC（パーソナルコンピュータ）からスマートフォンのようなネットワークデバイスに移行したことから生じた状況である。標準化された手順と言う点が重要であり、サービス構築時にクライアントの種類に依存せず利用できることが望まれている。現在では同じサービスであってもまだPCからの利用とスマートフォンからの利用では手順やサービス提供形態が異なるケースも多く見受けられる。例えばスマートフォンではそのサービス用の専用アプリケーションが提供されることが多い。今後HTML5等の普及により改善される可能性がある。

③はサービスを構築する際に全てを自前で用意せずとも必要となる機能を別途提供されている別サービスと連携して利用することを示している。マッシュアップと呼ばれる。サービスを直接利用者に提供するのではなく別のサービスに対してAPIを提供するようなサービスも考えられる。API公開もクラウドの重要な要素であると考える。

以上の①②③いずれか1つに該当するだけでも広義のクラウドと呼べるが、本章では全てに該当するような狭義のクラウドとして考察を行う。

4.3 クラウドにおける認証技術

クラウド以前のサーバ・クライアントの仕組みでは独自に管理されたIDとパスワードを使った認証か、SAML（Security Assertion Markup Language）やLDAP（Lightweight Directory Access Protocol）により管理されたIDによる認証が使われていた。SAMLやLDAPでは別途サーバ設定が必要になり、自由にSP（サービスプロバイダ）が利用できなかった。ただしこれは

SAML や LDAP が劣っていると言うことではない。エンタープライズ用途や学術用途のように自前でサーバを用意して利用者（ID）が管理されているケースでは、SAML や LDAP の仕組みの方が有効である。所属組織が明確な利用者は所属組織が立てた IdP を利用すれば良い。

コンシューマ用途では SNS を IdP として利用するケースが一般化してくると考えられる。IdP 独自の API も提供されているが、OpenID や OAuth と言った新しい認証の標準も生まれている。これら新しい認証技術の特徴は REST（Representational State Transfer）と呼ばれる HTTP 通信と XML 等の一般的な技術だけで実現された、オープンな認証を利用できる点が特徴となる。

OpenID は認証を OAuth は認可を得意としているがこの 2 つの標準を利用した OpenID Connect with OAuth 2.0 [3] [4] がまもなく標準化される予定になっている。多くの IdP で OpenID Connect による認証 API が提供されるようになると期待される。標準化によりサービス提供者は複数の IdP を使った認証の利用が可能となる。なお OpenID の用語では、IdP を OP（OpenID Provider）と、SP を RP（Relying Party）と呼んでいる。

4.4 トラスト・フレームワーク

OpenID Connect のような標準化が進みサービスが増えてくると利用者はどのように SP や IdP を信頼するのかと言う問題が生じてくる。PKI ではトラストアンカーとしてルート証明書を利用することでトラスト・フレームワークを確保してきたが、クラウドの SP や IdP に対しては TFP（Trust Framework Provider）を利用することでトラスト・フレームワークを実現しようと言う動きがある。TFP はポリシ策定者から認定を受け、認定監査人から監査を受けることで信頼性を確保する。

米国では政府が TFP を認定し、TFP が IdP を認定することになっている。TFP としては ICAMSC（Identity, Credential and Access Management（ICAM）Subcommittee）[5] が、TFPAP (Trust Framework Provider Adoption Process) [6] によって OIX や Kantara Initiative を認定している。これら TFP により審査承認された IdP として Google、Paypal、Verizon 等がある。

RP（SP）は認定 IdP リストを取得することで、接続しようとしている IdP が信頼できることを確認した上でデータ連携を行える。信頼された認証を利用する上で今後もこのようなトラスト・フレームワークの動向には注目する必要があるだろう。また後述する PKI 系サービスにおいてもどのように信頼できるかと言う面でトラスト・フレームワークの考え方は重要である。例えば検証を行うサービスは既に技術的には可能だが、そのサービスが信頼できないと検証結果も信頼できないことになる。

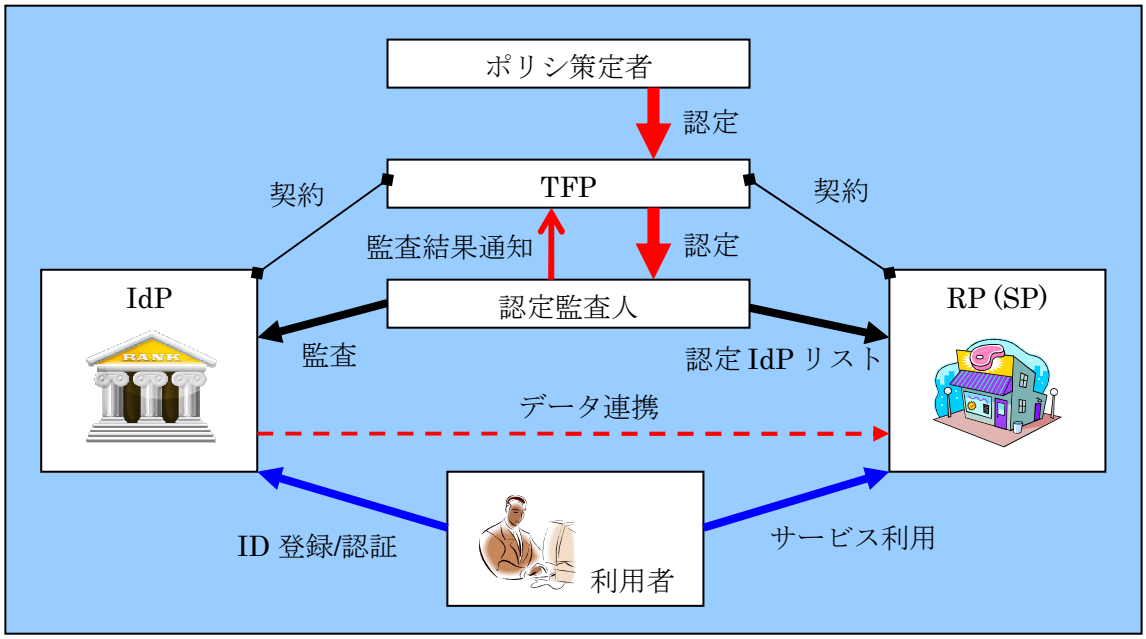


図 4-1　トラスト・フレームワークの例

（参考：Open Identity Trust Framework [7]）

4.5　SNS の動向

SNS の Facebook の全世界月間アクティブユーザ数は 2012 年 2 月 1 日付け情報では 8 億人以上となっている[8] 。また Twitter もアクティブユーザ数が 1 億人を超えている[9] 。利用者は全て ID を持っておりこれら SNS では既に日本の総人口を超える数の ID 管理が行なわれていることになる。これだけ大規模な ID 管理が実現できたのもクラウドの仕組みがあったからこそと言える。

SNS の多くは認証や属性利用（認可）の API を公開しており IdP としての地位を築きつつある。SP（サービスプロバイダ）は IdP と連携することで認証や ID 管理を行う必要が無くなる。更に SNS を使ったプロモーションやマーケティングも盛んになっており、一種のエコシステムが構築されつつある。

クラウド上のサービスを利用する際にサービス毎に ID 管理を行うと、利用者の利便性も損ないパスワードも多数登録する必要があり望ましくないと言う方向に向かいつつある。その意味では IdP が ID 管理をして認証の API を提供することが一般化してきた。何かクラウドサービスを利用する際には Facebook、Google、Yahoo!、mixi 等の ID と認証が要求されるケースが増えつつある。

4.6 複数 IdP 間の連携問題

個人所有のスマートフォンを仕事に使うようなケースが今後増えると予想される。従業員の私物であるデバイスを業務に利用することは BYOD（Bring Your Own Device）と呼ばれ、導入が検討されている。実現する為には、組織のシステムの外にいる利用者が組織内のサービスをどのように安全に利用するのかと言う問題を解決して行く必要がある。これには外部にある IdP と組織の IdP の連携も 1 つの方法であろう。

逆に個人情報保護の観点からは複数の IdP 間で名寄せが行えないようにする必要もある。OpenID では RP（SP）毎に異なる ID を割りふる PPID（Private Personal Identifier）の仕様を利用することで、名寄せが出来ない ID の実現が可能となる。

どのようなケースで IdP 間連携が必要であり、どのようなケースでは IdP 間連携を防ぐ必要があるのか、検討した上で利用する必要がある。OpenID Connect 等の新しい仕様では連携するにしてもしないにしても、柔軟な対応が可能となっている。

4.7 エンタープライズ分野の IdP

企業では社員を管理しているシステムを保有しているケースがあるが、これはそのまま IdP として利用できる可能性がある。既に企業がプライベート認証局として、証明書を社内向けに発行している例もあるようであり、今後 IdP として積極的に外部サービスとの連携が行なわれる可能性がある。

従来の社員等の管理を行なうシステムは SAML で構築されているケースが多かった。これは OpenID のプロトコルゲートウェイを間に挟めばそのまま OpenID の IdP として利用することも可能となる。もちろんその逆も可能である。

認証レベルによって利用できるサービスを使い分けることも必要になるだろう。例えばスマートフォンにより外出先から ID とパスワードによる認証を受けた場合は参照のみを許可して、社内において IC カードや多要素認証を利用した場合にはよりセキュアなサービスが利用できるようなケースが考えられる。

4.8 クラウドと IdP による PKI の可能性

ここまで見てきたようにクラウドサービスの多くでは IdP による認証が前提となってサービスが提供される。認証には ID とパスワードを使う以外に PKI 証明書（含 IC カード）や多要素認証等のレベルが存在する。認証レベル（LoA：Levels of Identity Assurance ／ OMB M-04-04 定義［10］）が高ければよりセキュアな高レベルの利用が可能となる。このようにクラウド認証を前提とした環境において従来の PKI の世界がクラウドにてどのように再定義できるかを考察

してみた。まずはPKIの基本要素がクラウドにおいてはどのように対応が可能かを表4-2にまとめた。

表 4-2　従来の PKI 基本要素のクラウドにおける再定義

PKI 基本要素	クラウドにおける再定義
登録局 Registration Authority	利用者の確認や登録は IdP の役割である その意味で IdP は登録局になり得る
認証局 Certification Authority	認証をうけた ID に対して証明書の発行を行うサービス IdP が兼ねても構わない
ディレクトリ Directory Service	従来の LDAP ベースのままでも良い 別途サービスとして提供しても良いと考えられる
証明書有効性検証局 Validation Authority	OCSP（Online Certificate Status Protocol - RFC2560）だけでは無く SCVP（Simple Certificate Validation Protocol）のようなオンライン失効確認 署名検証も含め検証局としてのサービス提供も考えられる

通常IdPは利用者の確認を行なっている。メール到達性だけで確認しているIdPもあれば携帯電話等でより厳密に本人確認を行なっている IdP もある。Facebook では本名での登録が必要となっており本名では無いと判断されるとアカウントが停止される。しかしながら実際問題として、犬や猫の Facebook アカウントも存在が確認できる。IdP を登録局として利用するには、IdP によるより一層の本人確認が望まれる。TFP による審査はその 1 つの回答になるだろう。

ディレクトリサービスは LDAP 等のサーバにより提供されている。これはそのままクラウドからも利用可能である。LDAP以外のインターフェイスでも同様のディレクトリサービスのAPIを実現できた方がクラウドでは使いやすいかもしれない。

証明書有効性検証局は例えば GPKI[11] ／LGPKI[12] にて提供されている証明書検証サーバのイメージが近い。証明書の検証だけでは無く署名検証も行なった署名検証サーバとしてクラウドのサービス提供をすることにも意味があると考える。現在一般には署名検証及び証明書検証は検証者のクライアント（PC）上で行なっているが、証明書ストア環境やネットワーク環境の違いにより隣り合ったPCでも検証結果が異なるケースがあり、PKI利用の難易度を上げているように思える。検証手順を確認できるクライアントでの検証はこれからも必要ではあるが、信頼された署名検証サービスが提供可能であれば検証をより使いやすくして PKI 利用を促進できる可能性がある。

認証レベルが信頼できるレベルであれば、鍵ローミングとしてクラウド上に署名用の秘密鍵を保管するサービスも考えられる。保管された秘密鍵はクライアント上のアプリケーションから利用しても良いし、別途クラウド上の署名サービスと連携することも考えられる。また PKI 基本要素で説明した証明書有効性検証局に署名検証も含めた検証サービスも考えられる。

表 4-3　クラウド上で実現が期待される新 PKI サービス

PKI サービス	機能
ID プロバイダ IdP（RA／CA）	登録局と認証局を兼ねる 認証局は別サービスとしての提供も可能である
鍵保管サービス Key Roaming	サーバ側（クラウド上）に秘密鍵を保管／管理するサービス 認証を受けた利用者に利用を許可する
署名サービス Signature Service	鍵ローミングのサービスと連携して署名を行うサービス 文書ファイルやデータファイルに署名が行える
検証サービス Verification Service	署名検証と証明書検証を行うサービス 安定した検証環境で簡単に検証できる

従来の電子署名（PKI）ではクライアントは PC にほぼ限定できた。通常は証明書と秘密鍵を PC にインストールするか、IC カードや USB トークンに入れて PC に接続して利用していた。基本的に秘密鍵はクライアント側にあると言う前提であったと言える。現在では 1 人でも PC 以外にスマートフォンやタブレット等のネットワークデバイスも同時に利用している。従来通りクライアントに秘密鍵をインストールすると複数の秘密鍵を管理する必要がある。これは管理的に望ましく無い。むしろ信頼できる認証が実現できるのであれば秘密鍵もクラウド（サーバ）側に置いて管理した方が良いと言う考え方もあるだろう。

また利用者が直接これら PKI サービスを利用するのでは無く、クラウド上に構築されたワークフローのサービスから PKI サービスの API を利用するケースも増えてくるだろう。Windows の Azure では既にワークフローの構築が可能であるし、Amazon もまだ米国のみであるが 2012 年 2 月 23 日に AWS（Amazon Web Services）から利用できるワークフローサービスとして SWF（Amazon Simple Workflow Service）[13] を発表している。例えばワークフローの最後で署名サービスの API を使って署名を行ったり、検証サービスの API を使って申請されたドキュメントの署名を検証したりと言った利用方法が考えられる。クラウドにおいて複数の API を使って新しいサービスを構築することをマッシュアップと呼ぶが、PKI サービスはマッシュアップに利用されてこそ真価を発揮するのではないかと考えている。

以上を踏まえて現状の PKI 要素も加えたクラウドと IdP を使った電子署名（PKI）サービスのイメージを以下に図 4-2 としてまとめた。利用者（またはフレームワーク等のサービス）から見ると登録と認証後には、署名サービスと検証サービスが見えるだけで、後は全てバックグラウンドで自動的に行われる。

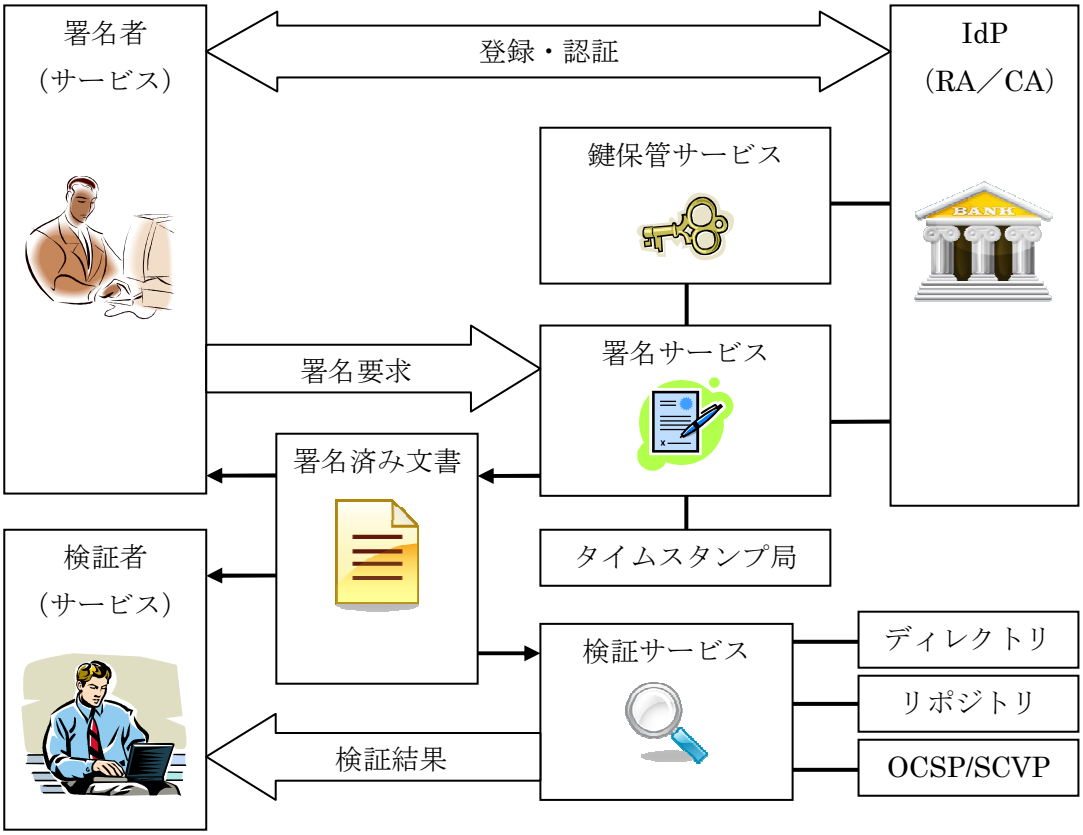


図 4-2　クラウドにおける新しい電子署名（PKI）サービスのイメージ図

4.9　認証と PKI

電子認証に PKI を利用した IC カード等を利用することで認証レベルを上げることが出来る。また無線 LAN にクライアントが接続する際に PKI 証明書を利用する EAP-TLS と言う認証プロトコルも利用されている。このように認証にも PKI を使うことでより信頼性の高い認証を実現できる。一方において認証用の PKI 証明書は証明書の発行者と検証者が同じでも構わない。電子署名の利用では署名者と検証者が異なることを想定しているのでトラストアンカーが重要になる。この点では電子署名と電子認証に要求される PKI の仕組みは異なると言える。

認証用の PKI 証明書を利用して高い認証レベルを実現した上で、鍵保管サーバに置かれた秘密鍵を使い電子署名を行うような利用方法が可能となれば、クラウド時代にマッチしたサービスが提供できる可能性がある。認証用と署名用の PKI 証明書を使い分けすることが重要と考えている。

4.10　まとめ

2012 年度は OpenID Connect 等の標準化も終わりいよいよクラウドと認証が普及すると予想されている。複数のサービスがマッシュアップされることで新しいサービスも普及して行くと考えられる。米国においては Adobe 社が EchoSign を買収しており[14] クラウドにおける電子署名

の利用に向けて動きが出てきている。また SignNow [15] は iPhone や Android 用の署名アプリケーションもリリースして電子署名サービスを提供している。ただし米国の電子署名は日本の状況には合致しない問題もあり、日本国内に向けた電子署名クラウドサービスの普及に期待したい。その為にはPKIの世界ももっとクラウドやIdPや認証を利用した新しいスタイルに生まれ変わる必要があるのかもしれない。

参考サイト及び文献

[1] OIX（Open Identity Exchange）
http://openidentityexchange.org/

[2] NIST Definition of Cloud Computing
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[3] OpenID Connect
http://openid.net/connect/

[4] OAuth 2.0
http://oauth.net/2/

[5] Identity, Credential and Access Management
http://www.idmanagement.gov/pages.cfm/page/
IDManagement-Identity-Credential-and-Access-Management

[6] TFPAP（Trust Framework Provider Adoption Process）
http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf

[7] What is a Trust Framework?
http://openidentityexchange.org/what-is-a-trust-framework

[8] Facebook, Inc. 株式上場の目論見書による
http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm

[9] Twitter、アクティブユーザ数が 1 億人を超えたと発表 - ITmedia ニュース
http://www.itmedia.co.jp/news/articles/1109/09/news027.html

[10] 以下より OMB M-04-04 (2003 年 12 月)の翻訳 PDF が入手可能
http://www.ipa.go.jp/security/publications/nist/

[11] 政府認証基盤(GPKI)
http://www.gpki.go.jp/

[12] 地方公共団体組織認証基盤(LGPKI)
http://www.lgpki.jp/

[13] Amazon Simple Workflow Service
http://aws.amazon.com/jp/swf/

[14] Adobe、電子署名技術の EchoSign を買収 - ニュース：ITpro
http://itpro.nikkeibp.co.jp/article/NEWS/20110719/362524/

[15] SignNow
https://signnow.com/

第５章　署名・タイムスタンプに関する国際連携

5.1　ETSI 標準化動向

欧州では電子署名指令 460[1] により、EU の署名規格の軽量化と再編成、期限切れとなっている CEN の標準文書（CWA：CEN Workshop Agreement）の更新や破棄、ETSI の技術標準（TS：Technical Specification）の統合や、より理解しやすく利用を促進できる TS の簡素化など、これまでの複雑化している電子署名に標準の見直しが行われている。この指令に対して ETSI では次の 4 つの新しい STF（Specialist Task Force）を立ち上げている。

- STF425 フレームワーク（Electronic Signature Standardization in Rationalised Framework）

  この STF は電子署名の製品やサービスの開発や利用を容易にするための電子署名標準のフレームワークを策定することが目的である。最初のフェーズとして、電子署名関連の既存標準の棚卸と標準のフレームワークの検討を行っている。フレームワークの方針として、①ビジネスオリエンテッド／ビジネスドリブンであること、②オプション要素の削減、③アセスメントガイドを提供すること、④テスト仕様とテスト環境の提供、⑤法律へ適合することが挙げられている。新しいフレームワークではこれまでの CAdES、XAdES、PAdES といった各仕様に新しい番号体系による付番が検討されている。今後、検討を法的枠組み（Legal Framework）や信頼の枠組み（Trust Framework）に広げて行く予定である。

- STF426　プロファイル Quick fixes to electronic signatures profiles

  この STF は CAdES、XAdES、PAdES、ASiC（アソシエート署名）のベースラインプロファイルを策定している。ASiC については 5 章で解説しているので参照されたい。

  長期署名（AdES）のプロファイルについては Commission Decision に合わせて短期と長期に分ける方針で検討されている。長期を“署名検証を考慮すべき保存期間”と再定義することで次の 4 つのレベルに整理する予定である。
  - ST レベル（短期）AdES-ES プロファイル
  - T レベル（短期）AdES-T プロファイル
  - SL レベル（長期）AdES-XL プロファイル
  - SLA レベル（長期）AdES-A プロファイル

- STF427　スタンダード Quick fixes to electronic signatures standards

  既存の標準について相互運用性の問題を抑止するための修正を行っている。認証局（CSP：Certificate Service Provider）の適合性評価（conformity assessment）要件及びガイダンスの策定、相互運用性のある適格証明書のプロファイルの策定、署名検証手順の策定、署名アルゴリズムの保守などの検討が行われている。

- STF428　プラグテスト Quick fixes to testing of electronic signatures standards
  XAdES ベースラインプロファイルの準拠性テストのテスト仕様の策定とテストツールの提供、PAdES や ASiC のプラグテストイベントの準備などが行われている。PAdES プラグテストは 2011 年 11 月に開催された。PAdES プラグテストについては 5.3 節で紹介している。2012 年 3 月には XAdES プラグテストが実施された。

これまでに多くの標準規格を策定してきた EU の電子署名の標準化活動は見直しと再編成の段階に入ってきており、今後の活動への大きな転換点になると考えられる。長期署名 JIS 規格（JIS X 5092、JIS X 5093）の参照規格である CAdES や XAdES についてもベースラインプロファイルや署名検証手順の策定などが予定されており、JIS 規格への影響も含めて今後も継続的なフォローが必要である。

5.2　TSP 適合性評価

信頼サービス提供者ステータス情報リスト（TSL）は、認証局等の信頼モデルの 1 つで、基準を満たした認証局をリストアップし公開する方法である。TSL には、認証局やタイムスタンプ局などを提供する信頼サービス提供者（TSP）の名前と認証情報が掲載される。EU 諸国では、2011 年 1 月から運用が始まっているが、信頼サービスであるか否かの判断が各国任せであったことからレベル差が生じた。このため、リストに掲載する信頼サービス提供者（TSP）の適合性評価要件とガイダンスを策定することとなった。

5.2.1　TSP 適合性評価モデル（conformity assessment model）

TSP 評価スキームとしての適合性評価モデルを図 5-1 に示す。構成要素は、適合性評価機関を認定する各国の認定機関（accreditation body）、適合性評価機関、信頼サービスステータス通知機関である。適合性評価機関は評価者（assessor）を擁する。適合性評価機関に対する認定条件として、ISO/IEC 270001 への適合が要求され、監査要件として ISO 17021（または EN 45011）への適合が要求される。

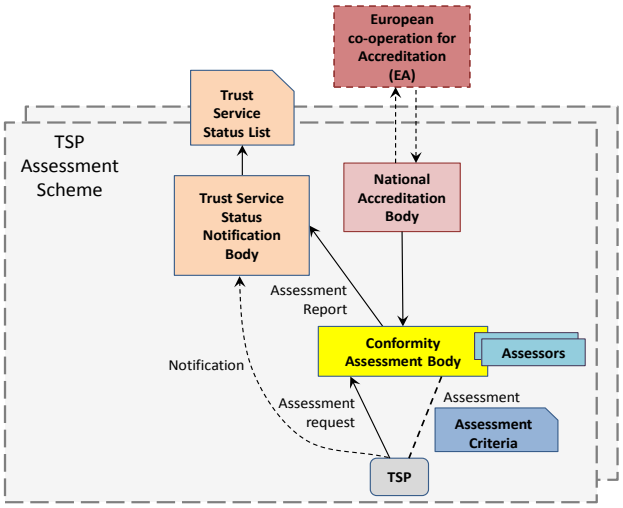


図 5-1　TSP 適合性評価モデル

（出典：Workshop on TSP Conformity Assessment 2012.1.24）

5.2.2　適合性評価及び再評価（conformity assessment、re-assessment）

適合性評価の流れは、評価基準（assessment criteria）に基づいて、書類審査に引き続き実装審査が行われ、評価結果が TSP と通知機関に報告される。報告機関は、これを信頼サービスステータスリスト（TSL）に掲載する。TSL には報告機関の署名が付与される。

適合性評価及び再評価の頻度は以下の通りである。危殆化可能性報告（notification of potential compromise）に関するインシデント動向監視（surveillance）が新たに追加されたことが特筆される。

- 3 年毎の適合性評価
- 年 1 回の監査
- 危殆化可能性報告に関するインシデント動向監視

5.2.3　TSP 適合性評価に関する新たな標準体系

今後発行される、TSP 適合性評価関連の標準は次のような体系になる。

- EN 19 403 General requirements and guidance for Conformity Assessment of TSPs
- EN 19 413 Conformity Assessment for TSPs Issuing Certificates
- EN 19 423 Conformity Assessment of TSPs providing Time-Stamping Services
- EN 19 433 Conformity Assessment of TSPs providing Signature Generation Services
- EN 19 443 Conformity Assessment of TSPs providing Signature Validation Services
- EN 19 602 Trust Service Status Lists Format
- EN 19 612 Trusted Lists Format

なお、欧州標準（EN）を基礎とする共通アプローチの採用並びにセキュリティインシデント及び現時点でのベストプラクティスに関する各国のスキーム間の調整は、今後の課題となっている。

5.3 EU-US 電子署名ワークショップ

2012 年 2 月 9 日、米国バージニア州マクリーン市 Hilton ホテルの Ballroom にて 米 Adobe 社主催による EU-US 電子署名ワークショップが開催された。このワークショップの目的は情報と経験の共有や、将来の共同プロジェクトなどの可能性を探ることである。米国から各機関（Department of Homeland Security、National Institute of Standards and Technology、Department of Justice、Department of Treasury、Federal Network Agency など）をはじめ 50 名を超える参加があり盛況であった。EU 及び US 双方からの最新状況説明、及びパネル討論（会場からの質問に対して、パネリストが回答）が行われた。

モデレータは ETSI ESI（Electronic Signatures and Infrastructures）議長の Riccardo Genghini 氏と米 Adobe 社の Leonard Rosenthol 氏が務めた。

EU からの報告には次のようなトピックスがあった。

- セキュア、シームレス、クロスボーダー、e インタラクションを目的に EU Directive を 2012 年 6 月頃に改訂予定である。電子調達やサービスが加わる。EU 成長の支援が急務である。
- EU 電子署名指令 460 への対応は、2013 年までに標準化を終了し 2014 年からインプリメントを開始する。
- コーナーストーンは、PDF/PAdES、SSCD、TSL、Digital Identity
- E-CODEX（e-Justice Communication via Online Data Exchange、欧州内のリーガル情報の交換）は、異なる署名方式の相互運用のためにゲートウェイで署名の変換を実施（ゲートウェイがトラストトークンを発行）する。
- PEPPLE（Pan-European Public Procurement Online、欧州内オンライン調達）は、署名検証の複雑さの回避策として署名検証サーバを提供する[3]。

US からの報告には次のようなトピックスがあった。

- 大学、研究機関、省庁で署名は使われている。例えば、Stanford 大学の成績証明書の 45% はデジタル署名である。
- 署名に対する考え方が、EU と US とで全く異なる。EU は手書き署名の代替であるが、US での位置付けはエビデンスとしてのトランザクションの証明である。
- US はブリッジを介して CA が相互に繋がっている。EU は TSL なので EU との相互接続に課題がある。日本の GPKI のお手本になったブリッジ相互接続が地道に整備されている。

[3]日本の GPKI は当初から同様のサーバを提供している。

パネル討論では本人を特定するための ID、適格証明書（Qualified Certificate）の価値、そもそもの署名の対象などについて EU-US 間で活発な討論が行われた。

- ID proof（証明）について

  EU 各国間の ID の連携についての検討が始まった段階であり今後の課題である。Civil law の問題、異なる登録方法の問題、ポリシの問題もある。

- 適格証明書の価値について

  EU は適格証明書を要求しているが適格証明書が要求される場面は 1%にも満たないのではないだろうか。US はリスクに応じて使用する証明書のレベルが複数あっても良いという立場である。ユースケースやビジネスモデルにもよる。

- 署名の対象について

  ドキュメント中心の考え方とプロセス中心の考え方がある。EU はドキュメントへの署名、US はプロセス実行に対する承認行為として署名を行う（承認ボタンへのクリックでもよい)。

上記のように、EU と US では署名や認証に対する考え方が大きく異なっている。これまでの eRAP の活動では主に EU における電子署名の標準化動向の調査を行ってきたが、ワンクリック承認など、実践的な US の署名・認証事情について今後更なる調査が必要である。

5.4 ETSI PAdES プラグテスト

2011 年 11 月 24 日から 2011 年 12 月 9 日[4]にかけて ETSI 主催の PAdES Plugtest 2011 が開催された。 PAdES Plugtest 2011 は PAdES 規格（ETSI TS 102 778）の相互運用性の問題を検証することを目的とした実証実験である。2008 年より実施されている XAdES/CAdES Plugtest と同様のインターネットを介した非対面のリモートプラグテストとして実施された。PAdES を対象としたプラグテストは今回が初めてとなる。日米欧合わせて 17 カ国 36 組織（うち日本からは 6 社）が参加し、過去のプラグテストに比べて大規模なものであった。参加者の業種にはセキュリティ製品ベンダーやサービス事業者（認証局やタイムスタンプ局など）だけでなく、行政機関や大学も含まれていた。

[4]プラグテスト実施中に期間は 12 月 19 日までに延長された。

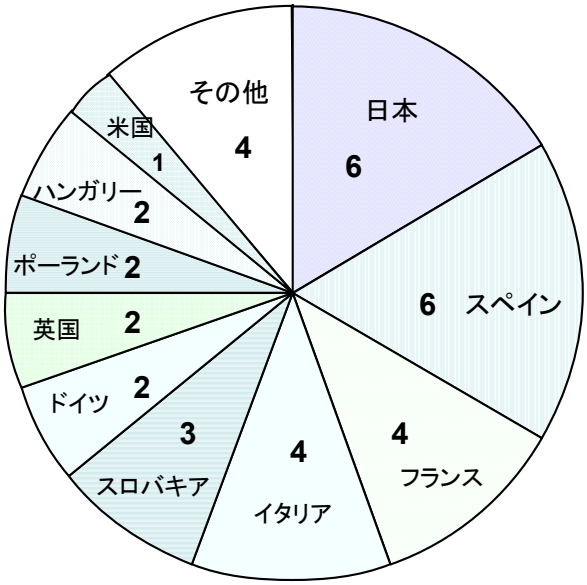


図 5-2 ETSI PAdES Plugtest 2011 参加者（国別）

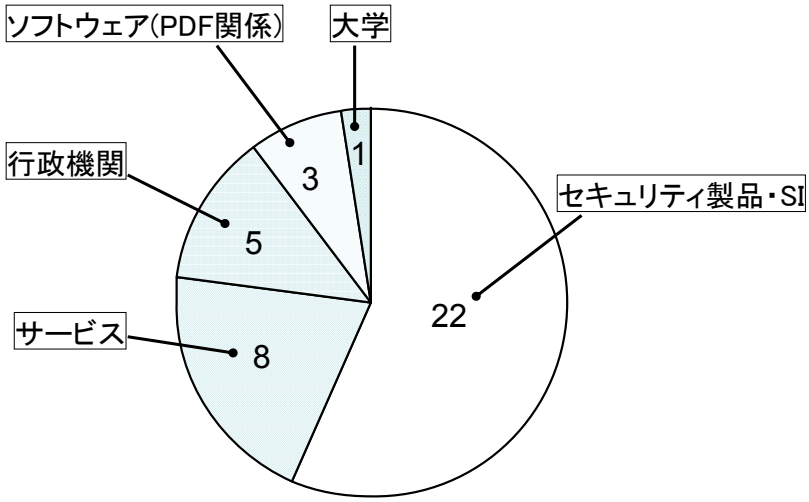


図 5-3 ETSI PAdES Plugtest 2011 参加者（業種別）

プラグテストには、各参加者が PAdES のテストデータを生成し、それを互いに検証しあうポジティブテストと、プラグテスト事務局が作成した異常系のテストデータを参加者が検証するネガティブテストがある。ポジティブテストは PAdES-Basic、PAdES-BES、PAdES-EPES、PAdES-LTV、PAdES-XML、PAdES-XFA の各仕様から計 41 項目のテストケースが用意された。PAdES-LTV のテストには署名者の署名を含まないタイムスタンプ（DocumentTimeStamp）のみのテストも追加された。ネガティブテストは PAdES-Basic、PAdES-BES の異常系のテストケースが 22 項目用意された。異常系テストには例えば署名対象の範囲が不正であるものや、失効された証明書を用いたものなどが含まれている。参加者は全てのテストケースについてテストを実施する必要はなく、各参加者のソフトウェアがサポートしている機能に関連するテストケースのみ選択して実施すればよいことになっており、ベーシックなデータ形式のテストケースほど参加者が多く、利用頻度の低いオプション属性を含んだテストケースは参加者が少ないなど参加者

の数にばらつきが見られる。中にはほとんどの参加者が実施しなかったテストケースもあった。

テスト中に明らかになった問題については専用のメーリングリストで議論が行われた。主な話題としては次のようなものがあった。

- PAdES に格納する SignedData のエンコーディング

  PAdES 規格では署名データのエンコーディングを DER に限定しているが、プラグテストの参加者の約半数が BER を使っていた。多くの参加者が BER を使用していることから、DER のみに対応していた参加者が BER の署名データも読み込めるように修正したことでテストを継続した。

  PAdES のベースとなっている PKCS#7 や CAdES といった標準規格では署名データのエンコーディングとして BER を使用することもでき、従来の汎用的な PKCS#7 や CAdES のライブラリ等は BER で署名データを出力することもある。多くの参加者が BER を使用していた理由も PAdES の実装にこのような汎用ライブラリをそのまま適用したためであると推測される。

  このように新しい規格がベースとなる規格に制約を加えて参照することによって、一から新規に実装する場合には実装の負担が軽減される一方で、ベース規格との互換性を失うことによってこれまでに蓄積された過去の資産を利用することに制限を与えてしまうという問題も生じてしまう。

- PAdES における ContentTimeStamp の必要性

  PAdES の DocumentTimeStamp で同じ役割を果たせるので署名データ内に格納する ContentTimeStamp は必要ないのではないかという意見があった。

- VRI の扱いについて

  PAdES には署名の検証情報を格納するための領域として DSS と VRI があるが、VRI がオプション要素であるため、これを無視した実装を行っている参加者があった。検証側としては VRI と DSS の両方をサポートする必要があり、VRI の検証情報に不足があっても、それを理由にエラーとすべきではない。また、VRI がオプション要素であることから実際には役に立たないことも考えられるため不必要な要素でないかという意見もあった。

- VRI のキー生成方法

  VRI の辞書のキーとなる署名データ（SignedData）のハッシュ値の対象とする範囲が参加者により異なっていた。Contents フィールドの 0 パディングを含んだ全体をハッシュ対象にする参加者と、0 パディングを除いた SignedData のみをハッシュ対象とする参加者に分かれた。0 パディングを含むべきか否かについて深く議論はされなかったものの、プラグテストの過程で 0 パディングを含める方法に修正する参加者もあり、結果的に多くの参加者が 0 パディングを含める方法をとっていたようである。

上記の課題は PAdES 規格にフィードバックされるべき内容も含まれているため、今後の eRAP の活動においても修正の必要性や修正案を検討し ETSI へコメントしていくことが必要である。

プラグテストのテストケースやテストデータ、テスト結果は非公開となっている。しかし、より多くのソフトウェアやサービスの相互運用性を高め、電子署名の普及を促進するためにも、プラグテストで使用したテストケースやテストデータを公開していくことが望ましい。今後の活動で ETSI へテストデータの公開を要望したいと考えている。

2012 年 3 月 14 日から 28 日にかけて XAdES ベースラインプロファイル（ETSI TS 103 171）を対象とした XAdES プラグテストが開催される予定（報告書執筆時）である。

5.5 長期署名 ISO 標準化

2009 年より ECOM 電子署名普及 WG で進められていた長期署名プロファイルの ISO 標準化プロジェクトは eRAP の活動に引き継がれ、現在も進行中である。ISO/TC154 にて標準化が進められており、ドラフト作成のワーキングメンバーは提案元である日本に加え、積極的な参加を表明したドイツ、チェコ、中国、ベトナムの 5 カ国で構成されている。エディタはセコム IS 研究所の佐藤雅史氏が担当している。ISO ドラフトの原案は長期署名プロファイルの JIS 規格（JIS X 5092、JIS X 5093）をベースとしており、次のパートから構成されている。

- ISO 14533-1 Information technology - Long term Signature Profiles - Part 1: Long term Signature Profiles for CAdES
- ISO 14533-2 Information technology - Long term Signature Profiles - Part 2: Long term Signature Profiles for XAdES

2012 年 3 月現在ではすでに DIS（Draft International Standard）の投票を終え、FDIS（Final Draft International Standards）のステージにある。いよいよ最終投票のフェーズに入っている。DIS 投票の結果では各国から様々なコメントがあった。その多くはエディトリアルな内容であったが、中には長期署名プロファイルの要件定義の変更を求めるものもあった。しかし、その要件定義への要望は参照規格の定義に反していたり、長期署名プロファイルの目的から逸脱するものであったため対応は見送られた。最終的に FDIS として提出したドラフトはこれまでのものと技術上の変更点はなくエディトリアルな修正にとどまっている。最終投票の結果は 2012 年内に判明する予定である。

参考文献

[1] STANDARDISATION MANDATE TO THE EUROPEAN STANDARDISATION ORGANISATIONS CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES APPLIED TO ELECTRONIC SIGNATURES

第６章　電子記録に関するビジネス提案

本章では、電子記録に関する具体的なビジネス創出に向けたビジネス提案を行う。ビジネス提案を行うにあたり、今後の市場拡大を目的に、1 企業のみが行うビジネスではなく、複数の企業が強みを生かしたビジネスを創出することも検討する。更に、東日本大震災の復興や国への提案を含めたビジネス提案も行うこととした。

(1)　クラウド上の記録管理保管サービス

①電子記録マネジメント基盤（ERM-Base）準拠電子記録保管クラウドサービス

0.前提
● ERM-Base が電子記録管理システムの標準である ● 自社とは、eRAP 等
1.事業概要（誰に、何を提供し、どこで稼ぐか）
記録（証拠となる電子データ、例：契約書）を大量にもつ組織に、安全・安心・信頼・安価に記録を保管する ERM-Base 準拠の電子記録保管クラウドサービスを提供する。 ERM-Base は、組織にスピード・グリーン・効率性・透明性・安全性・持続性・創造性を実現し、事実上のデファクトである MoReq2、ISO 15489（記録管理）、及び最新の技術や海外のトレンドを参考に電子記録管理システムの標準として JIPDEC、ERMC（電子記録マネジメントコンソーシアム）が作成・普及しており、以下の特徴がある。 ● 記録の真正性、信頼性、完全性、利用性を保証・提供 ● 原本証明書・流通証明書の発行 ● 電子記録のデファクトや規格を参考に作成 電子記録管理の標準である ERM-Base を利用することにより、以下のメリットがある。 **◆サービス利用者** サービスを利用する組織は、現在、特に組織に求められるスピード・グリーン・効率性・透明性・安全性・持続性・創造性を実現できる。 ERM-Base を満たしたサービスは、記録を安心・安全・信頼・安価に保管するばかりでなく、流通させるための仕組みや、サービス間での相互運用性の保証、グローバルな企業活動でも利用することができる。 **◆サービス提供者** システムの調達を多くの選択肢から行うことができ、安く基準を満たしたサービスを提

供できる。

グローバルなサービス展開も可能。

◆システム作成ベンダ

システム作成を行うベンダは、1 から基準を満たすシステムを作る必要はなく、現在あるシステムに基準を満たすように足りない機能を付け加えることによりシステム提供が可能である。

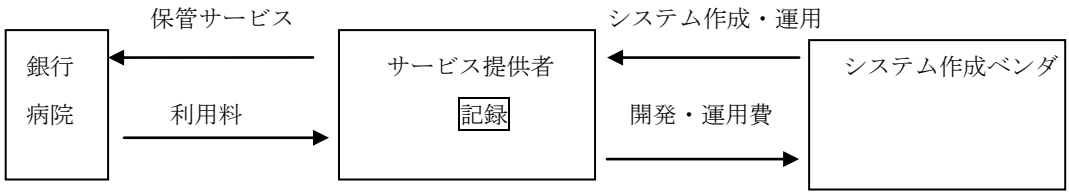
2.サービスの内容（サービスのメニュー、ラインナップ、体系など）

① 電子記録の保管・流通サービス

② 紙のスキャニングサービス

③ 税務監査など（他に、契約時に印紙代を払わないなど）に対応できる紙でなく電子のみで記録を管理するための電子記録管理のトータルソリューションサービス

3.ビジネススキーム（自社、その他主要プレーヤー、顧客の間でサービスをどのように企画・開発・提供を行い、どこからお金を得るか）



4.事業企画の背景・自社の強み

◆背景

現在、組織は、スピード・グリーン・効率性・透明性・安全性・持続性・創造性を求められている。

これらを実現するためには、紙中心の記録管理ではなく、電子記録による安価で標準となる電子記録管理サービスが必須である。

現状は、どのように管理すれば安全・透明性があるかなどの基準もなく、依然として紙での管理か、各社ベンダが個々に作成した相互運用性が確保されていない電子記録管理サービスを使っている。

そこで、ERM-Base 準拠した電子記録保管サービスを立ち上げることにより、上記問題を解決する。

◆自社の強み

- 記録管理システムの標準である ERM-Base を利用している
- ERM-Base に対応可能なシステムが存在する
- ERM-Base を深く理解し、直ぐに活用できる

5.事業の魅力点

◆自社にとっての魅力点

- 今あるシステムを活用して、ビジネスをすぐに、かつあまりコストをかけずに展開できる
- 安心・安全な社会、組織活動を実現でき、公益に寄与する

◆顧客にとっての魅力点

- 安全・安心・信頼・安価に記録を保管することでき、組織のスピード・グリーン・効率性・透明性・安全性・持続性・創造性を実現することができる
- 相互運用性があるサービスである

◆事業者にとっての魅力点

- 安全・安心・信頼・安価な電子記録管理サービスを提供できる

6.市場分析とターゲット設定

◆ターゲット規定と規模

- 医療、金融・保険、国・地方公共団体など

◆ターゲットの属性・特徴

- 記録を大量に抱えている、あるいは今後大量に発生する業務を抱えている組織

◆ターゲットの持っているニーズや課題

- 膨大な記録から必要な情報をみつける、記録管理を効率化、安くしたい組織
- 記録を正しく管理し、自らあるいは第 3 者に組織活動が正しく行われていることを証明したい組織

7.競合分析

◆競合サービス・他社取り組み状況

- 国内では、電子記録管理サービスを行っている業者が少なくとも 10 社以上ある。
  電子記録に電子署名・タイムスタンプを付与し、真正性や存在証明を電子記録に提供している
  また、電子記録管理を全社で取組み、税務、契約に関する記録の原本を電子のみで行うためのトータルソリューションサービスを実施している企業が複数存在する

◆他社に比べた自社優位性

- ERM-Base を使っている
- ERM-Base の特徴（デファクトの要件を使っている、相互運用性がある）

8.事業成功のポイント

- 安価にサービスを提供できるか
- サービスの提供だけではなく電子記録導入に伴うトータルソリューションを実施し、税務、契約の書類を電子化し、印紙税をただにするなど、利用者にメリットを出せるかどうか
- ERM-Base が記録管理システムの標準となるかどうか

②特許事務所様向け電子化包袋保管サービス

1.事業概要（誰に、何を提供し、どこで稼ぐか）

特許事務所が保管している特許出願や商標出願等に関わる文書は、同じ案件の文書であっても、紙文書（例：FAX 出力など）と（デジタルボーンの）電子文書が混在することがある。

そこで、紙文書はスキャンして電子化文書とし、（スキャンした）電子化文書と（デジタルボーンの）電子文書とを案件毎に統合管理可能な電子化包袋をデータセンターで保管する電子化包袋保管サービスを提供する。

特許事務所は特許庁への書類提出を出願人の代理として行うことが多く、特許事務所は書類提出前にその書類の内容確認を出願人に依頼する。特許事務所から特許庁へ提出する書類には法定期限がある書類があり、法定期限がある書類を対象とした期限管理が必須となっている。

そこで、この案件毎の期限管理の支援を目的とし、特許事務所-特許庁の間、特許事務所-出願人の間の案件毎の進捗状況の可視化を含む期限管理サービスを、電子化包袋保管サービスに連携させて提供する。

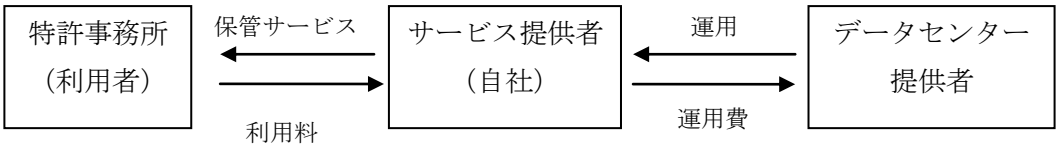
サービス利用者である特許事務所には次のメリットがある。

(1) 災害などにより特許事務所に被害が発生した場合であっても、（データセンターに被害がなければ）特許出願や商標出願等に関わる文書の紛失を防止できる。
(2) 特許事務所の各担当者が、案件毎の進捗状況を容易に確認できる。

2.サービスの内容（サービスのメニュー、ラインナップ、体系など）

① 紙文書のスキャン/登録ツールの提供
② 電子化包袋の保管・閲覧サービス
③ 案件毎の進捗状況確認サービス

3.ビジネススキーム（自社、その他主要プレーヤー、顧客の間でサービスをどのように企画・開発・提供を行い、どこからお金を得るか）



4.事業企画の背景・自社の強み

◆背景

書類保管の災害対応が今まで以上に重要視されてきた。

◆自社の強み

電子化文書と電子文書を統合管理可能なソリューションを展開している。

5.事業の魅力点

◆自社にとっての魅力点

- 開発済みのシステムを活用できる

◆顧客にとっての魅力点

- 災害などにより特許事務所に被害が発生した場合であっても、（データセンターに被害がなければ）特許出願や商標出願等に関わる文書の紛失を防止できる
- 特許事務所の各担当者は同時期に複数の案件を担当するが、案件毎の進捗状況を容易に確認できる

◆事業者にとっての魅力点

- 利用者に長期間利用していただくことを期待できる

6.市場分析とターゲット設定

◆市場の規模と成長性

- 国内特許出願数は、2000 年から 2006 年の間、毎年約 40 万件

◆ターゲット規定と規模

- 参考）　日本弁理士会会員の弁理士(自然人)数：約 9,000 名（2011 年 10 月）

◆ターゲットの属性・特徴

- 案件毎に文書を管理する必要があり、売上げが案件数の量に依存すると思われる

◆ターゲットの持っているニーズや課題

- 保管している文書の災害対応

7.競合分析

◆他社に比べて自社優位性

電子化文書と電子文書を統合管理可能なソリューションを展開した実績がある。

8.事業成功のポイント

保管している文書の災害対応の必要性の訴求と、案件毎の進捗状況管理の費用対効果の訴求。

(2) 電子署名、秘密分散技術等を利用したサービス

①文書の長期保存対応マイグレーションサービス

0.前提
● JIS 化された長期署名フォーマットを利用した証拠能力を有する電子文書の普及 ● 自社とは eRAP 会員等
1.事業概要（誰に、何を提供し、どこで稼ぐか）
電子的に文書を保存している（またはこれから保存を予定している）企業において、原本性の担保が必要な文書を対象に、長期署名フォーマットである JIS X 5092:2008（CAdES）、JIS X 5093:2008（XAdES）、または ISO3000-2 （PAdES）等に対応した文書に変換・保存するサービスを提供する。 現在、文書を電子データで保存・管理している企業は多数あるが、文書をエビデンスとして残す場合において、証拠能力を必要とする場合がある。（例えば、J－SOX 法等の会計に関する記録等） それらの企業をターゲットに、保存している電子文書の原本性を担保するため、または、現在は紙で運用しているエビデンスとしての文書を電子化するために、長期署名フォーマットに対応した文書に変換・保存するサービスを提供する。 署名に利用する電子証明書の発行やタイムスタンプ局の利用等も含め、ワンストップサービスで提供する。 現在、運用で原本性をカバーしている文書等をシステム化することで、より確実に原本性を担保できるとともに、運用コストの削減が期待できる。
2.サービスの内容（サービスのメニュー、ラインナップ、体系など）
長期署名フォーマットに対応した文書に変換・保存するサービスとしては、以下のサービスを想定。 ● 企業内の既存電子文書を長期署名フォーマット対応文書に変換・保存するマイグレーションサービス ● 既設文書管理システムに長期署名フォーマット対応文書に変換・保存する機能のアドインサービス ● 紙文書のスキャンニングサービス、及び長期署名フォーマット対応文書で保存するサービス ● 長期署名フォーマットに対応した文書を保管・管理するクラウドサービス

3.ビジネススキーム（自社、その他主要プレーヤー、顧客の間でサービスをどのように企画・開発・提供を行い、どこからお金を得るか）

クラウドやオンプレミス等の形態にとらわれず、単純に長期署名フォーマットに対応した文書化するサービスと位置付けられるため、主要なプレーヤーは以下となる。

導入企業：→データセンター事業者：サーバ等をデータセンターに設置している場合（クラウドの場合を含む）
→認証事業者：電子署名に利用する電子証明書を発行する認証サービス事業者
→タイムスタンプ局：タイムスタンプを付与するタイムスタンプ事業者
システムベンダー：上記のプレーヤーと連携し、ワンストップサービスで提供する。

4.事業企画の背景・自社の強み

◆背景

電子文書は容易に改ざんができてしまい、エビデンスとしての証拠能力は低く、法的なエビデンスとして利用できないことが多い。そのため紙の文書を原本として保管しておく必要がある等、二重管理をしている場合があり、紙による管理は運用コストがかかる傾向にある。そのため、証拠能力のある電子文書の普及が必要である。

◆自社の強み

旧 ECOM の時代から、長期署名フォーマットの JIS 化や相互運用性の実証実験等、紙文書電子化の普及に努めて来ている。

5.事業の魅力点

◆自社にとっての魅力点

- 収益の向上
- 顧客の事業に貢献し信頼を勝ち得る

◆顧客にとっての魅力点

- 既設の電子文書の有効活用、及び既設の文書管理システムを有効活用することによる低コストでの導入
- 運用コストの削減、及び監査に対応するための準備作業の削減
- 原本性担保のための紙文書の電子化による省スペース化、管理コストの削減

◆事業者にとっての魅力点

- 自部門のサービス利用率向上による収益の向上

6.市場分析とターゲット設定

◆市場の規模と成長性

運用コストの削減、及び省スペース化が求められており、市場規模は拡大・成長していく可能性が高い。

◆ターゲット規定と規模

電子データに原本性を求める民間企業、国、地方自治体、財団法人等全て

◆ターゲットの属性・特徴

電子データに原本性を必要としている

◆ターゲットの持っているニーズや課題

既存の電子文書の原本性を担保したい。または、紙を電子化しても原本性を担保したい。

7.競合分析

◆競合サービス・他社取り組み状況

長期署名フォーマットに対応した電子文書の保管・管理のサービスを行っている業者は多数有り、また、ソリューションとして提供している業者も多いが、各企業等のニーズはまちまちであり、企業のニーズに合ったものが必要である。

◆他社に比べて自社優位性

シンプルに長期署名フォーマット対応文書に変換・保存する機能を提供することで、様々な企業のニーズに対応することができ、また、ワンストップサービスで提供することにより、ユーザの利便性が向上する。

◆自社優位性を維持するための考え方（競合障壁）

データセンター事業者、認証事業者、タイムスタンプ事業者とのアライアンス。

8.事業成功のポイント

まずは、長期署名フォーマットである JIS X 5092:2008（CAdES）、JIS X 5093:2008（XAdES）、または ISO3000-2 （PAdES）で保存した電子文書が、法的なエビデンスとして有効なものとして認められるかどうかが成功のポイントとなる。

また、できるだけ安価にサービスを提供できるか、導入することによる運用コスト削減等の対投資効果が見えることも成功のポイントと考える。

②正規品の識別による模倣品撲滅サービス

0.前提
● 特許庁、経済産業省及び関連する省庁の後援 ● 非接触 IC チップ（ミューチップ）技術の応用 ● IC リーダー・ライター取扱い企業の協賛 ● 繊維メーカの協賛（IC チップの製品への接着をブランド企業と検証） ● 自社のブランドの衣類・雑貨・時計等を製造・販売しているメーカの協賛

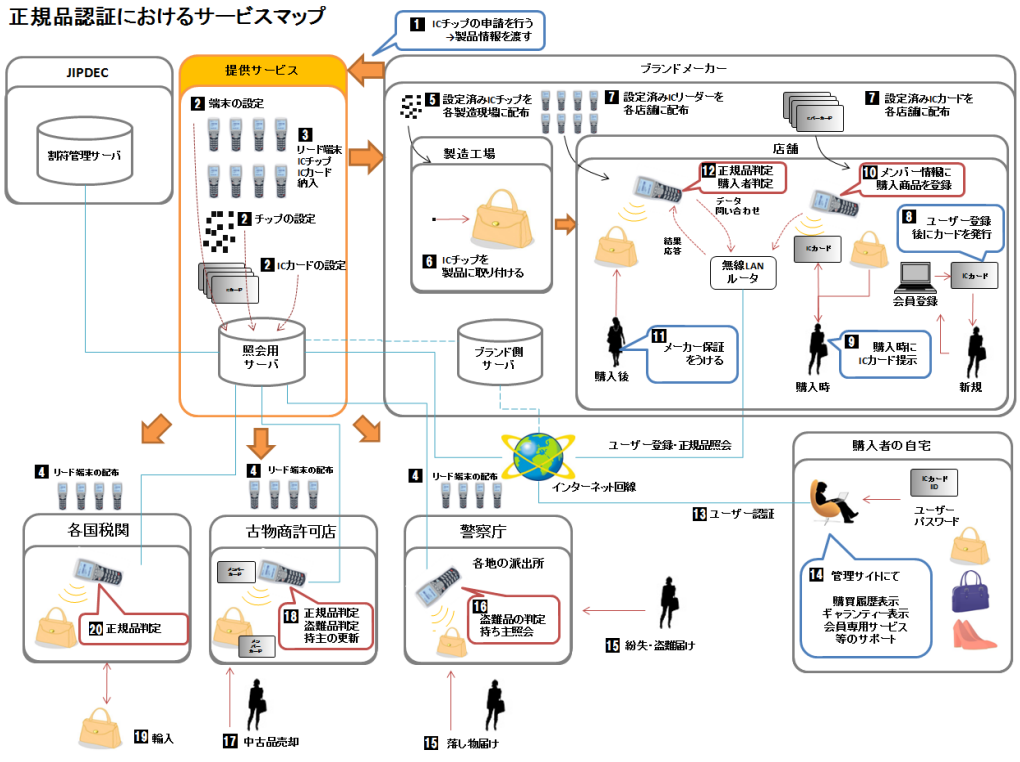
1.事業概要（誰に、何を提供し、どこで稼ぐか）

国内の衣類・雑貨・時計等のブランド分野の、各メーカを対象とし、IC チップ・IC カードを応用して正規品を認証するサービスを提供する。

警察庁、税関、古物取扱い許可店等と連携することで、盗難品や模倣品の抑制ができ、ブランド購入者へは、ユーザ認証カードを提供し、秘密分散技術を用いて、購入品と個人を結びつける事を可能とする仕組みを構築する。

IC チップ・カード・リーダーライターへ初期設定を行い、各メーカ、警察庁、税関、古物取扱い許可店等へ販売を行う。

各ブランドメーカにおいては、購入したICチップを製造段階で製品に組み込み、購買ユーザへは購入したICカードを提供することで、警察庁、税関、古物取扱い許可店、購入者側で、正規品であることと、購入者を結びつけてもらう事を可能とし、これらのサービスに利用料を支払うことで、ブランド価値、購買層へのサービスレベルの向上を図る事が出来、模倣品の抑制につながるものと考えられる。



2.サービスの内容（サービスのメニュー、ラインナップ、体系など）

① 正規品情報登録サービス。
② 会員情報登録サービス
③ 正規品照会サービス
④ IC チップ発行サービス

3.ビジネススキーム（自社、その他主要プレーヤー、顧客の間でサービスをどのように企画・開発・提供を行い、どこからお金を得るか）

eRAP 参画企業は、電子割符を用いたブランド購入者と商品の識別システムを提供する。具体的には、認証システムの開発・保守・サーバ運用、IC チップ・IC カード・IC チップリーダーの機材開発と機材の提供によるサービスを考えている。必要に応じて、認証システムの技術的検証や導入後のアフターフォローの体制を構築する。各関係省庁においてはサービスの重要性の呼びかけ、導入促進のための支援活動を行う事でサービス拡大が可能と考えている。

主な納入先としては、国内で自社ブランドを製造するメーカ各社、警察庁、税関、古物取扱い許可店等があげられる。

収益については、メーカ各社から、製品の製造段階で埋め込む為のICチップ、購入者へ提供する IC カード、専用の IC リーダーを購入しネットワークを通じて照合できるサービスの利用費。関係省庁、税関、古物取扱い許可店等から、専用ICリーダーの導入費用とネットワークを通じて照会できるサービスの利用費を想定している。

4.事業企画の背景・自社の強み

◆背景

模倣品を間違って買ってしまう被害が多発しているため、被害が拡大している。

近年、技術力の向上や取締強化に伴い摘発を逃れようと模倣手口の巧妙化が進んでいる。具体的な手口についてみると、「見た目はそっくり作り、商標を付けずに販売」や、他の模倣手口もあり、巧妙な模倣手口の多様化がみられる。

国や企業をあげての具体的な仕組み作りや、購買層へ認知拡大等によって、被害を抑制する事が一定の効果を上げると考えられる。

◆eRAP 参画企業の強み

参画企業においては、IC チップ等の最先端技術を保持し、WEB におけるサービス実績やシステム運用におけるコンサルティング実績を持ち、これらのサービスの実現に向けた組織構成が可能と考えられる。

5.事業の魅力点

◆参画会員にとっての魅力点

正規品の照合 ID を管理する為の、各種システムの販売による収益や、各ブランドショップにおける WEB 上でのインターフェースとプログラム開発における収益を期待できる。

◆顧客にとっての魅力点

模倣品とのサービスとの差別化を明確にでき、ブランドを展開する企業とブランド購入者との結びつきを作ることでリピーターを増やす事が期待できる。

水際（税関）での模倣品の抑制を期待でき、ブランド市場における模倣品の被害額の減少を見込む事ができる。

◆事業者にとっての魅力点

一連の正規品保障サービスについて eRAP や国が後援することで、自国のみならず、他国に対してもコアコンピタンスとなる事が期待できる。

6.市場分析とターゲット設定

◆市場の規模と成長性

日本国内の高級品の市場は約1兆9500億円となっており、世界売上高に占める日本のシェアは11%となっている。

◆ターゲット規定と規模

日本国内に展開している高級品の 10%に正規品証明のサービスが適用され、販売価格の3%程度が当サービスの利用料に当てられると仮定すると、国内で年間約 58 億円程の事業規模が想定される。また、海外展開も視野に入れ、国内と同等の割合で導入された場合、年間約 500 億円程度の事業規模への成長が見込まれる。

◆ターゲットの属性・特徴

国内に流通している雑貨分野におけるブランドメーカ。バッグ、財布、時計等の小物を扱う業者をターゲットとする。

◆ターゲットの持っているニーズや課題

模倣品が多く出まわることによって商標権が侵害されており、模倣品の質の向上により、正規品でなくても手軽に同程度の品物を安く手に入れられるといった、購買層のブランドに対する意識の低下が見られる。

指輪、ネックレス等、宝飾品への直接の取り付けは、デザイン的に不可となるケースが想定される為、その場合は外箱への取り付け、または別の手法を用いるかは要検討である。

7.競合分析

◆他社取り組みに比べた優位性

個人情報と結びつけることにより、所有者の特定や、盗難時の個体識別が可能となる点である。

関係省庁が公認するサービスとして認知拡大することで、利用シーンの拡大が見込める。

◆自社優位性を維持するための考え方（競合障壁）

eRAP 連動企画案として関係省庁との窓口を開き、公認認証方法（サービス）としての認可を得る事が有効と考えられる。

商品の製造段階にて仕組みを組み込むことで、商品から購買者を特定したり、購買者から購入商品を特定するといった事を可能とできるため、一度仕組みを取り入れると、継続して利用する事が想定できるが、商品の製造工程にICチップ導入が困難となる事も想定される。

8.事業成功のポイント

比較的導入してもらいやすい、価格設定が必要と考えられる。

- 各企業の協力要請や導入手順の簡素化が必要と考えられる
- テストケースとして、1ブランドを対象にサービス展開を実施、モニタリングをすることで、安定的なサービス運用へとつなげる事が必要と考えられる
- 国が推奨するサービスとして認められ、ターゲットとなる業界に認知してもらうことが重要と考えられる

③東北地方太平洋沖地震（東日本大震災）後の証拠保全新社会基盤構築事業

1.事業概要（誰に、何を提供し、どこで稼ぐか）
1.事業コンセプト 甚大な被害を与えた東日本大震災後の復旧・復興・創生は我が国にとって巨大な試練であるが、ここで純国際技術や知財を有効に活用した未来志向の新たな先進的情報社会基盤を実現できれば、その仕組み自体が新たなサービス事業として成長し、将来の日本の貴重な輸出産業にまで発展する可能性がある。粘り強く試練に対処し、未来への希望の芽を育み開花・結実させることを事業として具体化していく。 **2.事業概要（誰に、何を提供し、どこで稼ぐか）** 国家（間接的に国民）に対して、電子割符の最新機能を活用した新たな情報社会基盤を構築し、その上位に究極の本人特定を可能とする情報社会基盤のサービスと、法的にも原本と認められる電子データの運用管理サービスをアプリケーションとして実現し、そのサービス提供対価を国家から支払いを受けることを当面の本事業の基本とする。
2.サービスの内容（サービスのメニュー、ラインナップ、体系など）
電子割符（秘密分散技術）の特性、更に最新の機能を活用した先進的な情報社会基盤を構築し、その管理対象情報として本人特定情報や原本情報等を設定し、サービスを国家が主体となって提供する。スキームやサービス詳細は、勉強会や eRAP との意見交換等により修正していく。
3.ビジネススキーム（自社、その他主要プレーヤー、顧客の間でサービスをどのように企画・開発・提供を行い、どこからお金を得るか）
本件に関連し、最新版の電子割符と機能を用いて被災地復興に関する先進的情報社会基盤の検討と実現に関して、複数の企業が協議を一部開始している。この会は、前述のように当該事業の具体化に向け、関連する有識者や一部行政も交えた勉強会等の準備をしているので、そこでの検討内容と eRAP との意見交換等から最終決定する。
4.事業企画の背景・自社の強み
◆背景 電子割符が、阪神淡路、新潟中越、十勝沖、そして今回の震災・津波と毎回電子割符が真っ当に社会基盤に組み入れられていたら、データ復旧を含め対処が確実にできたと思うことが繰りかえされてきた。再び同じ悔しさを味わいたくないし、被災者の皆さんに同じ思いをさせたくない。そして、IT 立国、知財立国、世界最高水準の電子政府の具体化に寄与する社会システムとして、新たな日本の象徴的事業とすることを狙う。

5.事業の魅力点

◆顧客（国家・地方行政等）にとっての魅力点

デジタルデータの持つ脆弱性の補完を、素人でも理解しやすい技術を活用して課題解決できる。更に、個人情報に関しても、世界でも最先端の管理の仕組みを実現でき、戦略的輸出産業として成長していく可能性を持てる。

◆事業者（本事業を実施する者）にとっての魅力点

既存IT システムのように、大きなリスクを事業者やエンドユーザのどちらかが負うようなモデルではなく、関係者が情報を分散管理して、相互保管することでサービス提供者とサービス利用者とで管理責任もシェアできる。更に、割符（シェア）単体では、原本情報が出てこないことから、保有時、移送時、保管時に容易に完全な情報漏洩が発生しない。この仕組みをきちんと割符を用いて対処すれば、政府機関の情報セキュリティのための統一管理基準解説書記載の秘密分散技術を用いる記述、つまり機密性 2 や 3 への対処に準拠した対応も実現できる。更に、割符の特性を鑑みれば、機密性のみならず、完全性、可用性も高度に満たしていることも自明であるので、そのあたりを更に勉強会と eRAP での検討成果を段階的に市場周知させていくことで、当該事業に携わることが今後の新たなビジネスに直結していくことを実体験しつつ、先進的ノウハウを吸収していくことができる。

6.市場分析とターゲット設定

◆市場の規模と成長性

国内＋海外＋他の情報（まずは、要機密情報）への応用事業＋周辺サービス・コンサル等

◆ターゲット規定と規模

初期：国民全員、行政機関すべて

◆ターゲットの属性・特徴

初期：国民全員、行政機関すべて

◆ターゲットの持っているニーズや課題

国家としての機能遂行・BCP に必要。最高度の個人情報の運用管理。

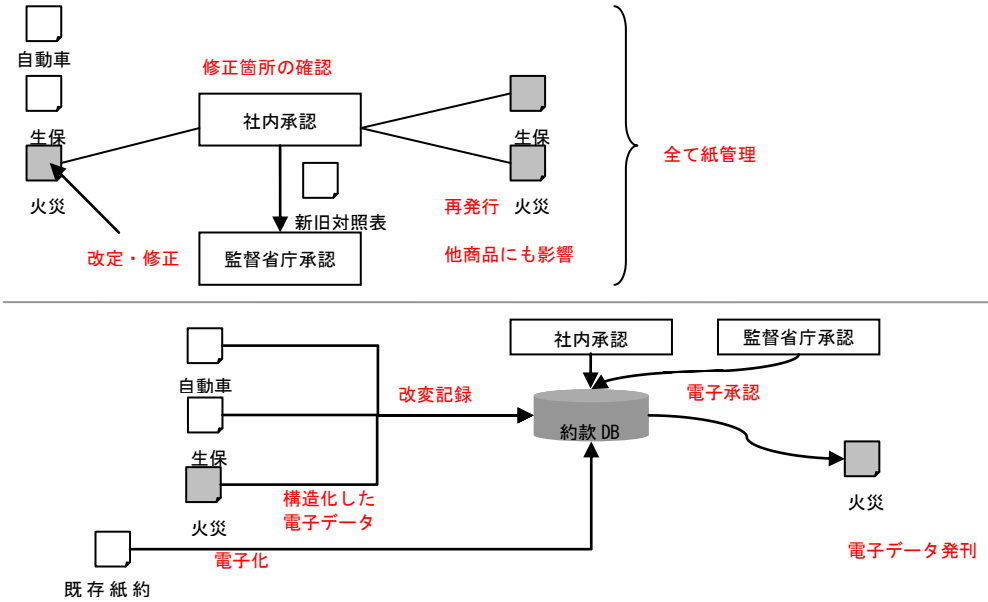
憲法上の国民の権利要求対処・・・サービス業としての行政の顧客満足度を向上させる。

民間へのノウハウの応用事業展開。

7.事業成功のポイント
すでに技術は安定している。実名を秘匿すべき導入事例等も含め、実績も十分にある。あとは真に社会的な象徴的要求事項で導入事例を構築し、ブランディングを行なう。特に日本として世界に展開できる日本ブランドとIT立国、知財立国、世界最高水準の電子政府の具体化に寄与させる。更に、応用ビジネスをパートナーとで展開する。パートナーは、厳選し、競合になる可能性を極力排除し、今回の取り組みに対し初期リスクを負う主体への配慮を行ないつつ、真に連携できるパートナー各社とでノウハウを共有し市場シェアを確保する。海外展開に関しても、同様。上記パートナーや現地有力企業との子会社等を活用する。但し、地域・業種・業界で総代理店的な機能を委託する可能性もある。並行し、知的財産に関して前述のパートナー各社とパテントプールの組織を準備し、積極的な知的財産戦略も行なう。国内のみならず、海外にも事業成果を展開することを前提とし、部品提供ではなく、商品・サービス提供を行い、知財立国、IT 立国日本の新たな輸出産業として成功させる。

(3)　電子記録マネジメントに関する支援、コンサルティングサービス

①金融・保険約款文書の電子化に伴う制作工程の合理化と承認記録管理

1.事業概要（誰に、何を提供し、どこで稼ぐか）
商法により規律されていた保険契約に関する一般的な契約ルールを定める保険法が、社会経済情勢の変化に対応し、平成22年に約100年ぶりに抜本改正され、保険法として制定された。e-文書法も追い風となり、法律改正を機に契約約款内容の抜本的な見直しと電子約款が流通し始めた。 従来より、保険約款の作成は各保険部門で下書き、制作部門で清書、マージ、監督省庁へ認可依頼など、全ての文書は紙で管理。商品の多品種化により、約款改定に伴う修正・公正・認可作業の影響範囲が広がり、各部門、監督省庁の業務負担となっている。また、制作物の特性から過去の制作物、制作者、改定、承認者など制作に纏わる全ての記録を残す義務があり、紙書類、過去データが散乱している状態である。 

2.サービスの内容（サービスのメニュー、ラインナップ、体系など）
①　構造化文書データの作成、既存紙文書のスキャニングサービス ②　文書データの作成・改変履歴管理 ③　案件毎の進捗状況確認サービス

3.ビジネススキーム（自社、その他主要プレーヤー、顧客の間でサービスをどのように企画・開発・提供を行い、どこからお金を得るか）
顧客：　金融・保険業界 自社：　約款情報の構造化、電子データ制作、スキャニングサービス、DB構築

その他：電子署名、タイムスタンプサービス

4.事業企画の背景・自社の強み

◆背景

顧客保護の観点から保険約款の簡易化、平明化が義務付けられている。

環境保護の観点から発行頻度の高い約款の電子化が普及しつつある。

◆自社の強み

長年にわたり保険業界の取引関係があり、文書レイアウトデザイン、文書データ制作に取組んできた。

ドキュメント管理システムを有している。

5.事業の魅力点

◆自社にとっての魅力点

- 比較的、簡易にスタートできる。
- 得意先の電子データを管理することで、継続的な受注が見込める。

◆顧客にとっての魅力点

- 専門人員（校正マン）の確保、属人的な文書管理からの開放
- 制作作業におけるミスロス削減、作業負荷低減。
- 監督省庁の承認作業のスピードアップ

6.市場分析とターゲット設定

◆ターゲットの属性・特徴

保険、クレジット、銀行など

7.事業成功のポイント

紙文化からの脱却。先ずは既存の紙ドキュメントの整理、及び最適な文書構造化のコンサルティング。

監督省庁の電子承認の受入。

ドキュメントの署名、証拠性の重要さ、危険意識を煽る

②共用ファイルサーバの容量対策及び電子化文書・電子文書の的確な運用体制の構築

1.事業概要（誰に、何を提供し、どこで稼ぐか）

◆誰に

- 業種、規模を問わず電子文書・電子化文書の管理が課題となっている企業・団体
  特に組織階層が深い企業、電子文書管理のルールがない企業、個人情報など機密性が高い情報を多く扱う企業、いろいろな情報（ドキュメント）を相互参照する業種（不動産管理など）を想定した。

◆何を提供するか

- サーバの使用容量の削減
- 業務プロセスで使用する文書の電子的な活用の推進支援
- 電子文書・電子化文書の的確な運用
  （電子文書管理ルール、記録管理システムの導入支援、電子化文書作成など）

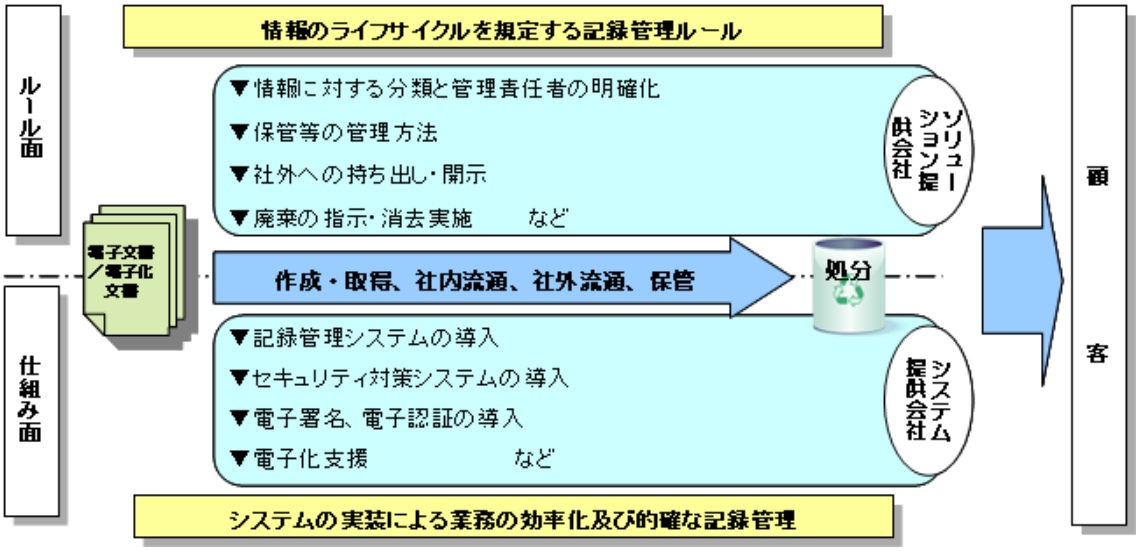
◆どこで稼ぐか

- ファイルサーバの容量対策をきっかけとして、その先の電子文書・電子化文書のセキュリティの強化、的確な電子文書・電子化文書管理に向けた仕組みの構築（運用方法・システム化）の支援を目指す。これらを会員企業各社の得意分野を持ち寄り、顧客にとって効果的・効率的な付加価値の高いサービスを総合的に提供することによって収益性の向上を図る。

2.サービスの内容（サービスのメニュー、ラインナップ、体系など）

① サーバ内データのインデックス分析・ヒアリング
② サーバ内データの整理案の提示
③ 電子文書・電子化文書の運用提案（電子記録管理ルール、システム導入、セキュリティの強化など）
④ 必要に応じた整備作業支援（組織が有する紙文書、電子文書、電子化文書など媒体に関わらない情報資産の整備・運用支援）

3.ビジネススキーム（自社、その他主要プレーヤー、顧客の間でサービスをどのように企画・開発・提供を行い、どこからお金を得るか）



4.事業企画の背景・自社の強み

◆背景

- 共用サーバの容量の問題、電子文書・電子化文書の管理は企業において大きな課題となっている。

  共用サーバ内の情報の乱雑さに困っているという話は、日々の営業活動の中でよく耳にすることである。一時的な容量対策・整理を行ったとしても、日常的に適切な管理を行う仕組みを導入しなければ根本的な解決にならない。

  一方、昨今の電子文書・電子化文書の有効活用、標準化、規格の制定などが進展しつつある。

  身近な課題であるファイルサーバの整理を行うことをきっかけとして、組織の記録管理の仕組みの見直し、昨今の情勢を鑑みたシステムの導入などを目指した提案とした。

  なお、記録管理の仕組みの見直しにあたっては、紙や電子、マイクロフィルム等それぞれの媒体の特徴を活かし、組織の実態に即した効率的な組織運営を支えるものとする。

◆自社の強み

- これまで特にシステムにこだわらず、顧客の有する情報の調査、ヒアリングなどをもとに顧客の業務分析、情報管理の提案、システム導入支援（要求仕様の検討、基礎データ作成など）を行ってきた。本提案においても顧客ニーズに適したソリューションを提供できること。

① 現在約 90 万件に及ぶファイルデータを有する組織の日々の登録、更新されるファイルデータの維持管理及び保存庫預入ファイルの貸出返却業務、ファイル廃棄処理とデータ照合を約 20 年にわたって実施していること。

② プラント事業者において約 150 万図面の保管管理及び年間約 10 万回の図面差替え作業を行い、長年にわたって設備の維持・管理を支える的確な記録管理を行っていることなど、これらの経験を活かしたサービスを提供できること。

- サービスの提供にあたって、①汎用的なソリューションの提供ではなく、お客さまのニーズに沿った個別のソリューションを提供すること、②現場の声を重視し、実在するドキュメントの把握、実際の業務フローの把握を行い実効性のあるものとすること、③導入時点だけの一過性の支援ではなく、運用段階でも継続的にフォローし続けることを心がけ、「お客さまが保有する情報の価値を最大限に高めていくこと」を目指していること。

5.事業の魅力点

◆自社にとっての魅力点

- 運用段階までいくとメンテナンス、スキャニング実施など継続的に顧客と関わっていくことができる可能性がある。

◆顧客にとっての魅力点

- 電子文書・電子化文書の整理を通じて、データ容量の減少による管理コストの削減
- 電子文書・電子化文書の的確な運用によって、企業が有する情報資産の有効利用・コスト削減

◆事業者にとっての魅力点

- 会員企業の協力による総合的なサービスを提供することで、顧客にとって一貫性のある付加価値の高いサービスを提供できること。

6.市場分析とターゲット設定

◆ターゲットの持っているニーズや課題

課題：氾濫する電子記録の的確な管理・運用

7.競合分析

◆自社優位性を維持するための考え方（競合障壁）

- 会員企業が総合的にサービスを提供することの効果、付加価値の高さをアピールしていくこと。

8.事業成功のポイント

- サーバ容量対策をきっかけとして、その先の電子文書・電子化文書の整備・運用の提案に結び付けていくこと。

メンバリスト

事務局（敬称略、五十音順）

大崎　宏　　一般財団法人日本情報経済社会推進協会
木村道弘　　一般財団法人日本情報経済社会推進協会
前田陽二　　一般財団法人日本情報経済社会推進協会

顧問（敬称略、五十音順）

大山永昭　　東京工業大学
辻　秀一　　東海大学
米丸恒治　　神戸大学大学院法学研究科

編集メンバ（敬称略、五十音順）

役　割	氏　名	所　属
委員	保倉　　豊	グローバルフレンドシップ株式会社
委員	佐藤　雅史	セコム株式会社
委員	能勢健一朗	東芝ソリューション株式会社
委員	溝上　卓也	株式会社日立ソリューションズ
委員	小野　成志	株式会社フォーク
委員	倉持　　勉	富士ゼロックス株式会社
委員	三原　　真	富士ゼロックス株式会社
委員	杉崎　　元	三菱電機株式会社
委員	宮崎　一哉	三菱電機株式会社
委員	宮地　直人	有限会社ラング･エッジ
オブザーバ	樽美　康一	東京レコードマネジメント株式会社
オブザーバ	松尾多計志	東京レコードマネジメント株式会社
オブザーバ	太田　浩平	凸版印刷株式会社

上記以外のメンバ（敬称略、五十音順）

役　割	氏　名	所　属
委員	川城　三治	グローバルフレンドシップ株式会社
委員	宮澤　慎一	セコム株式会社
委員	石原　達也	東芝ソリューション株式会社
委員	石本　英隆	日本電信電話株式会社
委員	高田　慎也	日本電信電話株式会社
委員	児玉　　剛	株式会社フォーク

役　割	氏　名	所　属
委員	塩川　淳史	株式会社フォーク
委員	棚沢　優介	株式会社フォーク
有識者	西川　康男	ARMA 東京支部
有識者	佐藤　　均	東京医療保健大学
有識者	佐藤　伸一	株式会社 PFU
オブザーバ	森川　　淳	経済産業省
オブザーバ	守山　速飛	経済産業省
オブザーバ	宍倉　勝仁	シヤチハタ株式会社
オブザーバ	柳原　孝志	日本ガードタイム株式会社
オブザーバ	浅川　慶洋	株式会社ワンビシアーカイブズ
オブザーバ	金井　　智	株式会社ワンビシアーカイブズ

電子記録応用基盤に関する調査検討報告書 2011

-電子記録マネジメントシステム要件とケースマネジメント-

電子記録応用基盤フォーラム（eRAP）

平成 24 年 3 月 30 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

〒106-0032　東京都港区六本木 1-9-9　六本木ファーストビル内

TEL 03-5860-7557　FAX 03-5573-0561　　http://www.jipdec.or.jp/

印　刷：株式会社美行企画

ISBN978-4-89078-027-3
C3004

JIPDEC